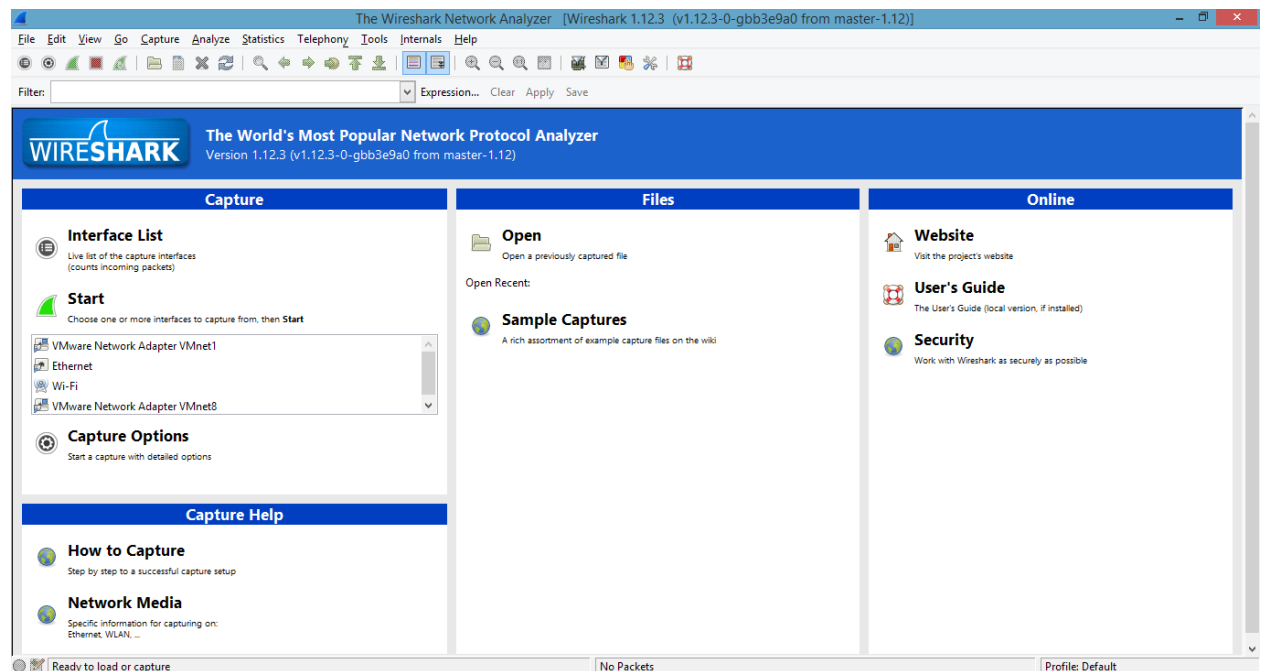


Chapter 1: Getting Started with Wireshark - What, Why, and How?

```
Sniffer Commands
=====

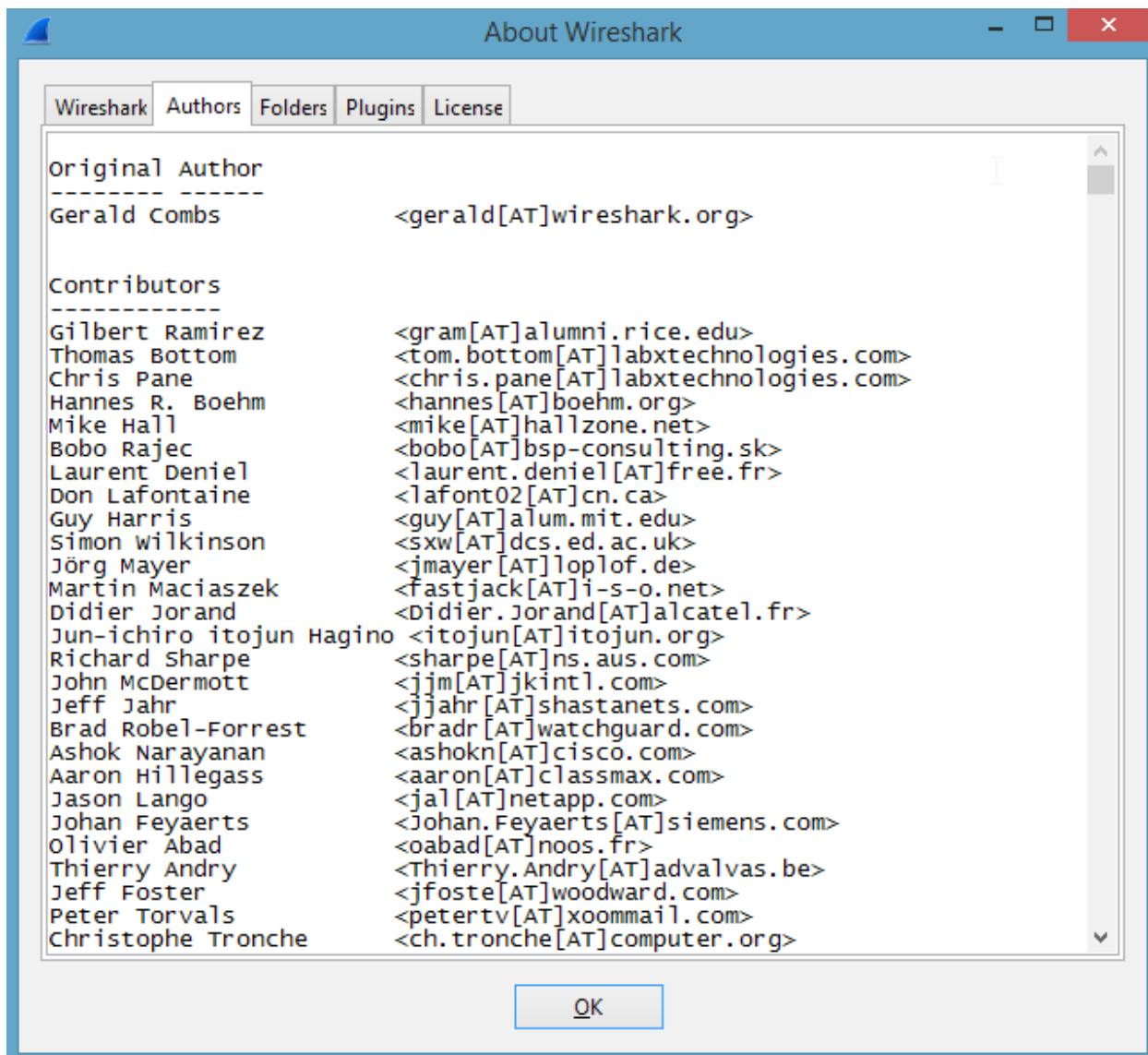
Command      Description
-----
sniffer_dump  Retrieve captured packet data to PCAP file
sniffer_interfaces Enumerate all sniffable network interfaces
sniffer_release Free captured packets on a specific interface instead of downloading them
sniffer_start Start packet capture on a specific interface
sniffer_stats View statistics of an active capture
sniffer_stop  Stop packet capture on a specific interface
```



Custom window title (appended to existing titles):

The Wireshark Network Analyzer [Piyush Verma for PACKTPUB] [Wireshark 1.12.6 (v1.12.6-0-gee1fce6 from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help



Filter: Expression... Clear Apply Save

ip.address == 192.168.1.1

ip.addr == 192.168.1.1

Save Filter as...
http.request.method == GET and ip.src == 192.168.20.130 GET Requests from 130

Capture



Interface List

Live list of the capture interfaces
(counts incoming packets)



Start

Choose one or more interfaces to capture from, then **Start**

- VMware Network Adapter VMnet1
- Ethernet
- Wi-Fi
- VMware Network Adapter VMnet8



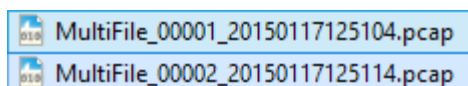
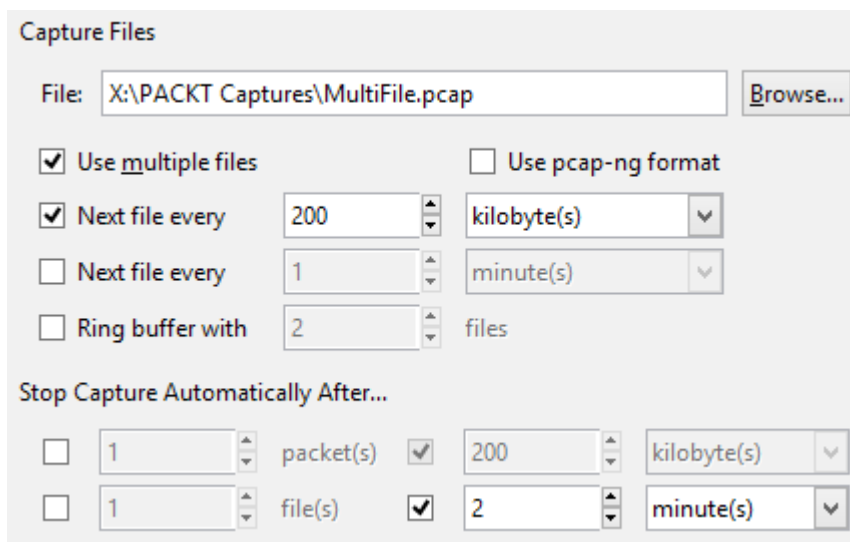
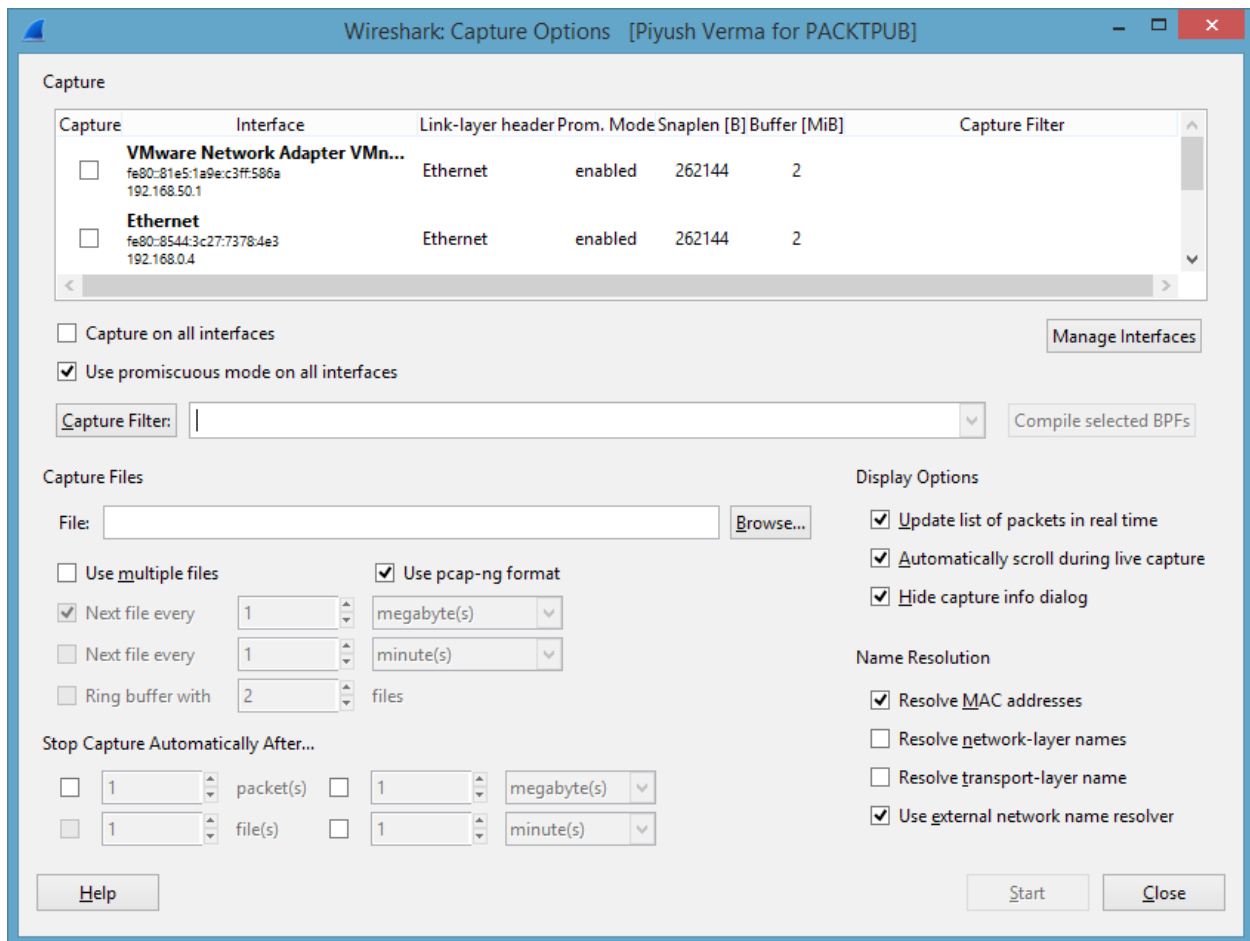
Capture Options

Start a capture with detailed options

Wireshark: Capture Interfaces

Device	Description	IP	Packets	Packets/s	
<input checked="" type="checkbox"/> VMware Network Adapter VMnet1	VMware Virtual Ethernet Adapter	fe80::81e5:1a9e:c3ff:586a	46	5	Details
<input type="checkbox"/> Ethernet	Realtek Ethernet Controller	fe80::8544:3c27:7378:4e3	0	0	Details
<input type="checkbox"/> Wi-Fi	Microsoft	fe80::a196:c707:a71e:de0f	835	17	Details
<input type="checkbox"/> VMware Network Adapter VMnet8	VMware Virtual Ethernet Adapter	fe80::70:d72d:5d28:cf84	61	10	Details

Buttons: [Help](#) [Start](#) [Stop](#) [Options](#) [Close](#)



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:

[X:\PackT WNS\WNS\Chapter 1\TelnetCapture.pcap \(11 kB\)](#)



Sample Captures

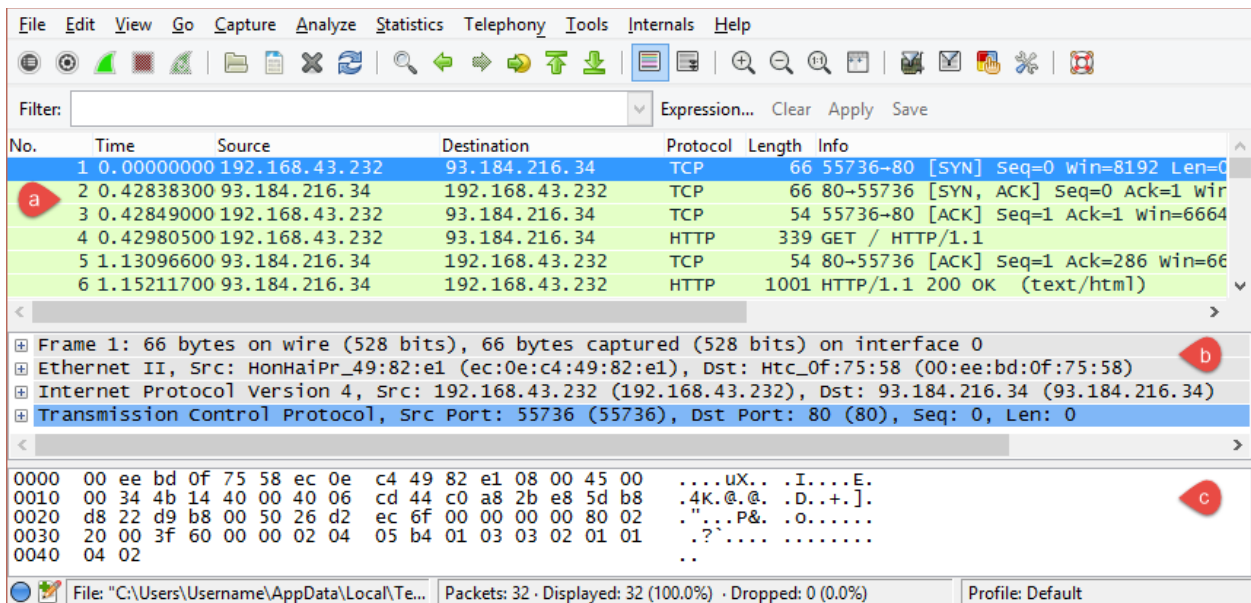
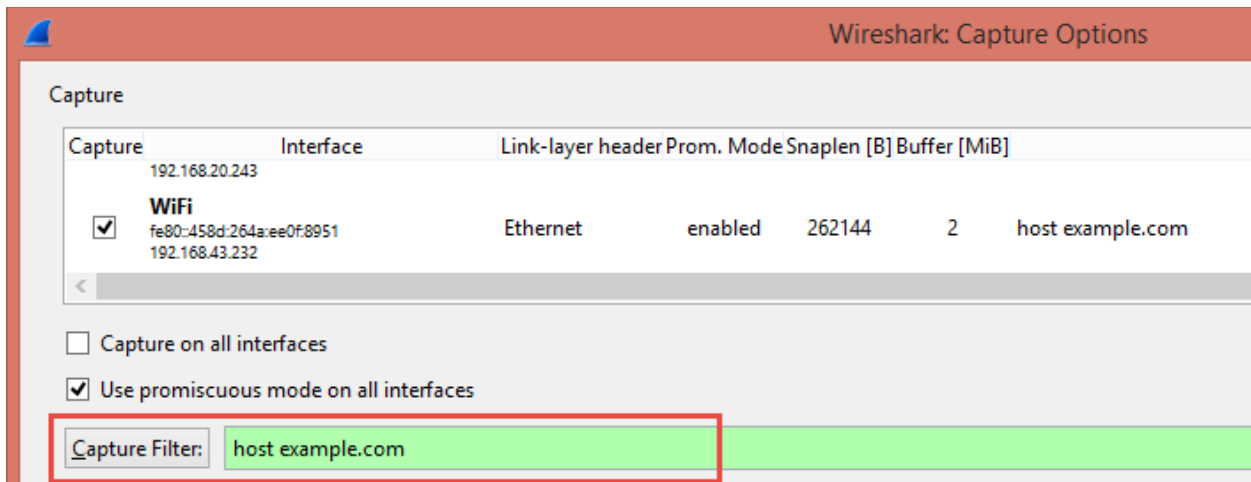
A rich assortment of example capture files on the wiki

Maximum recent files:

File: "D:\PACKT Captures\MultiFile_00002_20150117125114.pcap" 129 kB 00:01:49 | Packets: 483 · Displayed: 483 (100.0%) · Load time: 0:00.010 | Profile: Default

Device	Description	IP	Packets	Packets/s	
<input type="checkbox"/> Ethernet	Realtek Ethernet Controller	fe80::fca8:d134:33cf:8e07	0	0	Details
<input checked="" type="checkbox"/> WiFi	Microsoft	fe80::458d:264a:ee0f:8951	901	6	Details

[Help](#) [Start](#) [Stop](#) [Options](#) [Close](#)



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.43.232	93.184.216.34	TCP	66	55736->80 [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
2	0.428383000	93.184.216.34	192.168.43.232	TCP	66	80->55736 [SYN, ACK] Seq=0 Ack=1 win=33320 Len=0 MSS=1360 WS=2 SACK_PERM=1
3	0.428490000	192.168.43.232	93.184.216.34	TCP	54	55736->80 [ACK] Seq=1 Ack=1 win=66640 Len=0
4	0.429805000	192.168.43.232	93.184.216.34	HTTP	339	GET / HTTP/1.1
5	1.130966000	93.184.216.34	192.168.43.232	TCP	54	80->55736 [ACK] Seq=1 Ack=286 win=66640 Len=0
6	1.152117000	93.184.216.34	192.168.43.232	HTTP	1001	HTTP/1.1 200 OK (text/html)
7	1.202033000	192.168.43.232	93.184.216.34	TCP	54	55736->80 [ACK] Seq=286 Ack=948 win=65692 Len=0

!(ip.addr == 192.168.1.1)

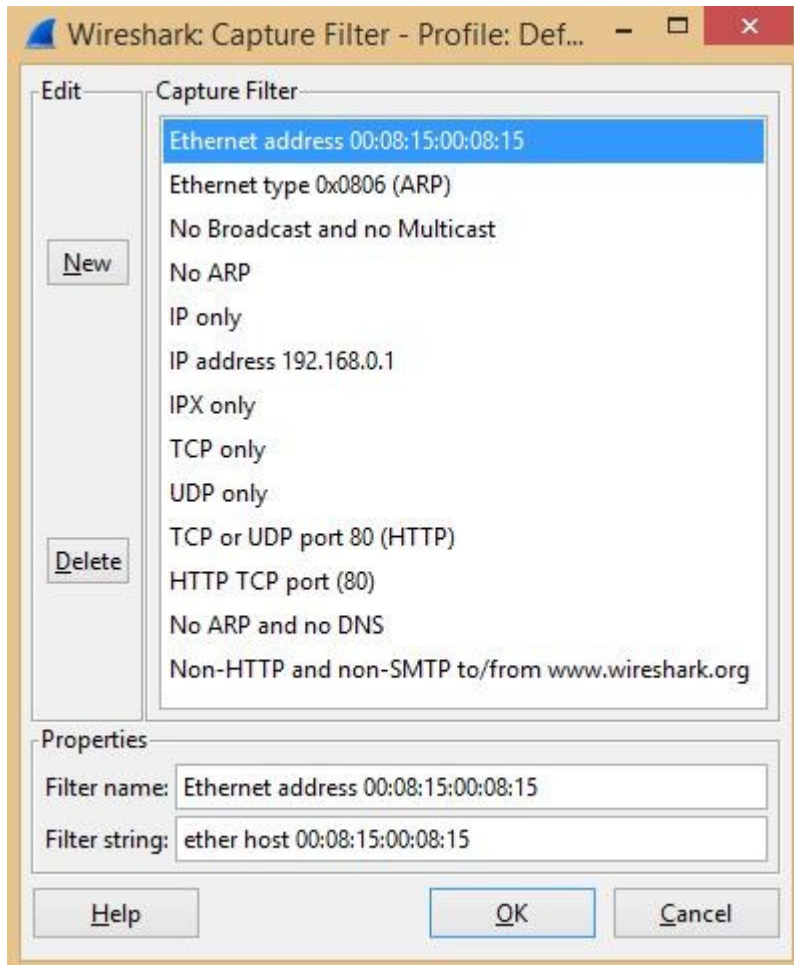
ip.addr != 192.168.1.1

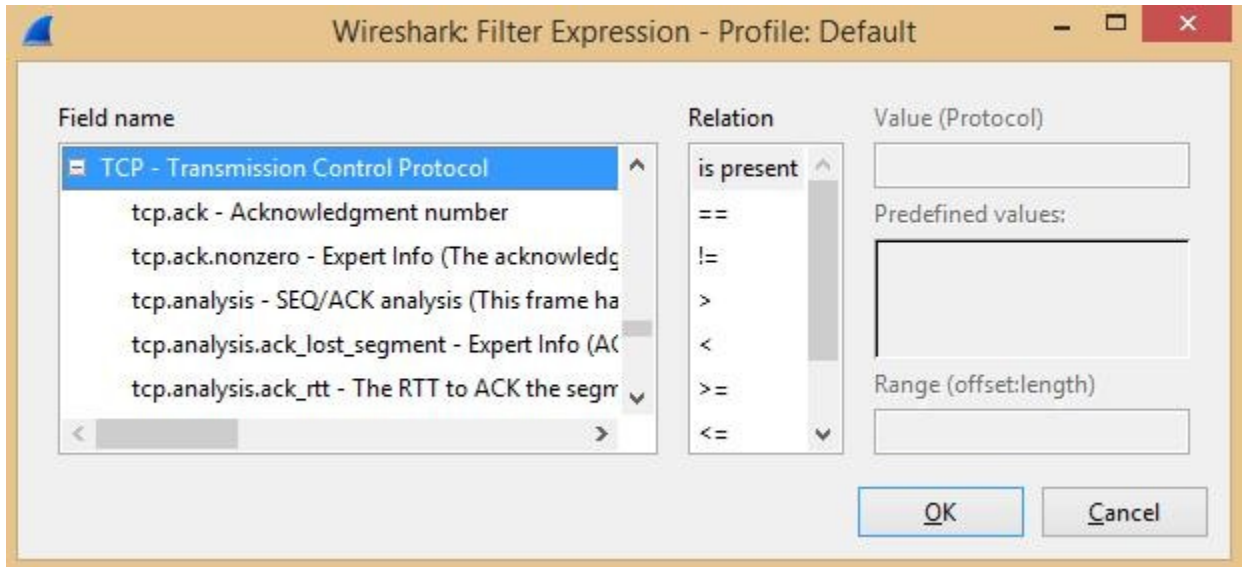


Chapter 2: Tweaking Wireshark

Filter: **arp** Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Time to live	Info
1	0.000000	Vmware_be:bf:94	Broadcast	ARP	42		who has 192.168.20.137? Tell 192.168.20.136
2	0.003036	Vmware_39:12:b2	Vmware_be:bf:94	ARP	60		192.168.20.137 is at 00:0c:29:39:12:b2
6	0.175932	Vmware_39:12:b2	Broadcast	ARP	60		who has 192.168.20.2? Tell 192.168.20.137
7	0.000271	Vmware_e9:a1:c8	Vmware_39:12:b2	ARP	60		192.168.20.2 is at 00:50:56:e9:a1:c8





10	0.015067	192.168.20.137	192.168.20.136	TELNET	66	Telnet Data ...
11	0.008564	192.168.20.136	192.168.20.137	TELNET	60	Telnet Data ...

Selected Packet

```

Frame 10: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
Ethernet II, Src: Vmware_39:12:b2 (00:0c:29:39:12:b2), Dst: Vmware_be:bf:94 (00:0c:29:be:bf:94)
Internet Protocol Version 4, Src: 192.168.20.137 (192.168.20.137), Dst: 192.168.20.136 (192.168.20.136)
Transmission Control Protocol, Src Port: 23 (23), Dst Port: 1485 (1485), Seq: 1, Ack: 1, Len: 12
Source Port: 23 (23)
Destination Port: 1485 (1485)
[Stream index: 0]
[TCP Segment Len: 12]
Sequence number: 1 (relative sequence number)
[Next sequence number: 13 (relative sequence number)]
Acknowledgment number: 1 (relative ack number)
Header length: 20 bytes
0000 00 0c 29 be bf 94 00 0c 29 39 12 b2 08 00 45 10 ..).....)9....E.
0010 00 34 5a ba 40 00 40 06 35 98 c0 a8 14 89 c0 a8 .4Z.@.@.5.....
0020 14 88 00 17 05 cd fe 8b 0e 53 81 7b c5 f5 50 18 ..].....S {...P.
0030 16 d0 5d 17 00 00 ff fd 18 ff fd 20 ff fd 23 ff .;]..... ..#.
0040 fd 27

```

Selected Field in the packet

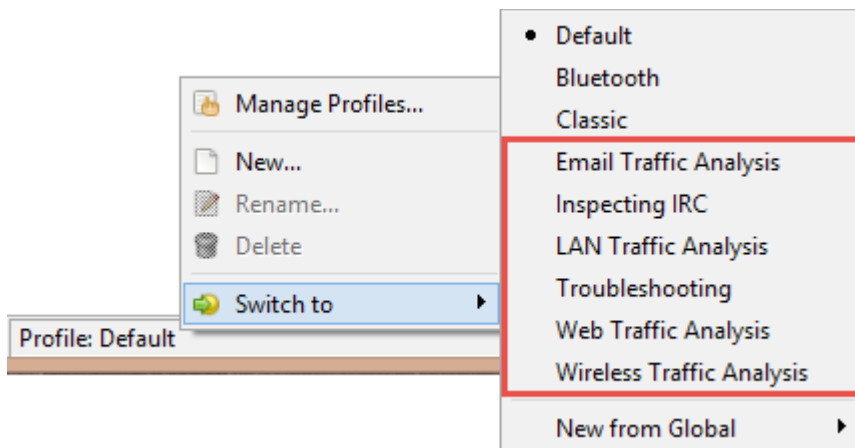
Respective Field-Name

Source Port (tcp.srcport), 2 bytes

Packets: 130 · Displayed: 130 (100.0%) · Load time: 0:00.024

Filter: tcp.srcport == 23

Expression...



Wireshark		
Authors		
Folders		
Plugins		
License		
Name	Folder	Typical Files
"File" dialogs	C:\Users\Piyush Verma\Documents\WNS Traces\	capture files
Temp	C:\Users\PIYUSH~1\AppData\Local\Temp	untitled capture files
Personal configuration	C:\Users\Piyush Verma\AppData\Roaming\Wireshark\	"dfilters", "preferences", "
Global configuration	C:\Program Files\Wireshark	"dfilters", "preferences", "
System	C:\Program Files\Wireshark	"ethers", "ipxnets"
Program	C:\Program Files\Wireshark	program files
Personal Plugins	C:\Users\Piyush Verma\AppData\Roaming\Wireshark\plugins	dissector plugins
Global Plugins	C:\Program Files\Wireshark\plugins\1.12.3	dissector plugins

Statistics

- Summary
 - Comments Summary
 - Show address resolution
 - Protocol Hierarchy
- Conversations
- Endpoints
 - Packet Lengths...
- IO Graph

- Conversation List ▶
- Endpoint List ▶
- Service Response Time ▶

- 29West ▶
- ANCP
- BACnet ▶
- Collectd...
- Compare...
- Flow Graph...
- HART-IP
- HTTP ▶
- ONC-RPC Programs
- Sametime ▶
- TCP StreamGraph ▶
- UDP Multicast Streams
- WLAN Traffic

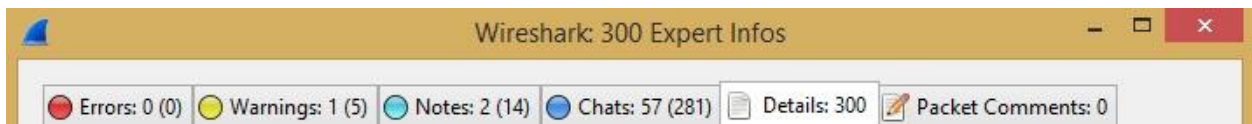
- IP Statistics ▶
- BOOTP-DHCP...

Protocol	% Packets	Packets	% Bytes	Bytes	Mbit/s	End	Packets	End	Bytes	End	Mbit/s
Frame	100.00 %	130	100.00 %	9700	0.003		0		0		0.000
Ethernet	100.00 %	130	100.00 %	9700	0.003		0		0		0.000
Address Resolution Protocol	3.08 %	4	2.29 %	222	0.000		4		222		0.000
Internet Protocol Version 4	96.92 %	126	97.71 %	9478	0.003		0		0		0.000
Transmission Control Protocol	95.38 %	124	95.56 %	9269	0.003		43		2428		0.001
Telnet	62.31 %	81	70.53 %	6841	0.002		81		6841		0.002
User Datagram Protocol	1.54 %	2	2.15 %	209	0.000		0		0		0.000
Domain Name Service	1.54 %	2	2.15 %	209	0.000		2		209		0.000

Ethernet: 1		Fibre Channel	FDDI	IPv4: 11	IPv6	IPX	JXTA	NCP	RSVP	SCTP	TCP: 47	Token Ring	UDP	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				
74.125.236.134	192.168.1.36	15	1 702	6	896	9	806	0.000000000	8.3824	855.12	769.23				
173.194.36.24	192.168.1.36	7	1 866	3	1 312	4	554	2.311967000	0.9999	10496.56	4432.23				
104.130.120.128	192.168.1.36	16	1 229	7	432	9	797	5.035609000	69.2034	49.94	92.13				
103.1.175.1	192.168.1.36	728	439 353	404	403 065	324	36 288	49.811886000	48.7821	66100.53	5951.04				
74.125.68.95	192.168.1.36	7	414	3	186	4	228	55.177722000	5.8228	255.55	313.25				
173.194.36.1	192.168.1.36	30	2 854	12	1 147	18	1 707	64.525158000	8.6327	1062.93	1581.89				
162.159.241.165	192.168.1.36	15	1 878	6	1 069	9	809	66.179249000	9.0287	947.20	716.82				
174.35.25.5	192.168.1.36	18	1 076	6	364	12	712	69.395466000	14.9738	194.47	380.40				
67.215.253.139	192.168.1.36	10	1 700	5	780	5	920	69.523729000	1.4166	4404.82	5195.42				
173.194.36.15	192.168.1.36	35	30 757	22	29 623	13	1 134	69.701714000	3.0205	78457.81	3003.45				
108.162.232.207	192.168.1.36	31	4 443	13	2 909	18	1 534	85.089718000	8.1839	2843.63	1499.53				

Ethernet: 2		Fibre Channel	FDDI	IPv4: 12	IPv6	IPX	JXTA	NCP	RSVP	SCTP	TCP: 58	Token Ring	UDP	USB	WLAN
IPv4 Endpoints															
Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City	Latitude	Longitude					
192.168.1.36	912	487 272	425	45 489	487	441 783	-	-	-	-					
74.125.236.134	15	1 702	6	896	9	806	United States	Mountain View, CA	37.419201	-122.057404					
173.194.36.24	7	1 866	3	1 312	4	554	United States	Mountain View, CA	37.419201	-122.057404					
104.130.120.128	16	1 229	7	432	9	797	United States	San Antonio, TX	29.488899	-98.398697					
103.1.175.1	728	439 353	404	403 065	324	36 288	Singapore	-	1.366700	103.800003					
74.125.68.95	7	414	3	186	4	228	United States	Mountain View, CA	37.419201	-122.057404					
173.194.36.1	30	2 854	12	1 147	18	1 707	United States	Mountain View, CA	37.419201	-122.057404					
162.159.241.165	15	1 878	6	1 069	9	809	United States	San Francisco, CA	37.769699	-122.393303					
174.35.25.5	18	1 076	6	364	12	712	United States	San Jose, CA	37.424999	-121.945999					
67.215.253.139	10	1 700	5	780	5	920	United States	Santa Ana, CA	33.763302	-117.794197					
173.194.36.15	35	30 757	22	29 623	13	1 134	United States	Mountain View, CA	37.419201	-122.057404					
108.162.232.207	31	4 443	13	2 909	18	1 534	United States	San Francisco, CA	37.769699	-122.393303					

Name resolution Limit to display filter



Expert - Expert Info

- _ws.expert.group - Group (Wireshark expert group)
- _ws.expert.message - Message (Wireshark expert information)
- _ws.expert.severity - Severity level (Wireshark expert severity level)




```
C:\>tshark -D
1. \Device\NPF_{A0A69947-9A6A-4B5F-87EE-900B6F7D307A} <UMware Network Adapter UM
net1>
2. \Device\NPF_{A0CC0E6D-5F3A-49EB-9AC7-9A8DBDFA5FDA} <Ethernet>
3. \Device\NPF_{A2BD2764-92CC-4DAB-A414-655ED62450C1} <Wi-Fi>
4. \Device\NPF_{8D64E150-0BD8-46F0-8454-5B9577DE25C9} <Local Area Connection>
```

```
C:\Users\Piyush Verma>tshark -r HTTP_traffic.pcap -qz io,phs
=====
Protocol Hierarchy Statistics
Filter:


eth                frames:721 bytes:598880
  ip                frames:721 bytes:598880
    tcp             frames:721 bytes:598880
      http          frames:86 bytes:56115
        data-text-lines
          tcp.segments frames:10 bytes:8063
            media     frames:6 bytes:3501
              tcp.segments frames:10 bytes:8649
                png    frames:9 bytes:7535
                  tcp.segments frames:22 bytes:16904
                    image-gif frames:21 bytes:16002
                      urlencoded-form frames:1 bytes:1390
                        urlencoded-form frames:1 bytes:733
=====
```







```
C:\Users\Piyush Verma>capinfos -tcsyizH HTTP_Traffic.pcap
File name: HTTP_Traffic.pcap
File type: Wireshark/tcpdump/... - pcap ← -t
Number of packets: 721 ← -c
File size: 610 kB ← -s -H
Data byte rate: 6465 bytes/s ← -y
Data bit rate: 51 kbps ← -i
Average packet size: 830.62 bytes ← -z
SHA1: 40d6829e50a407f0f993ad2a822a3259e8d31833
RIPEMD160: c912b71a9cbae82f9c5d3252d9e0fb7a9e28f1fc
MD5: 2a7d11176fc4802e9f84f8d3b1f84d48
```

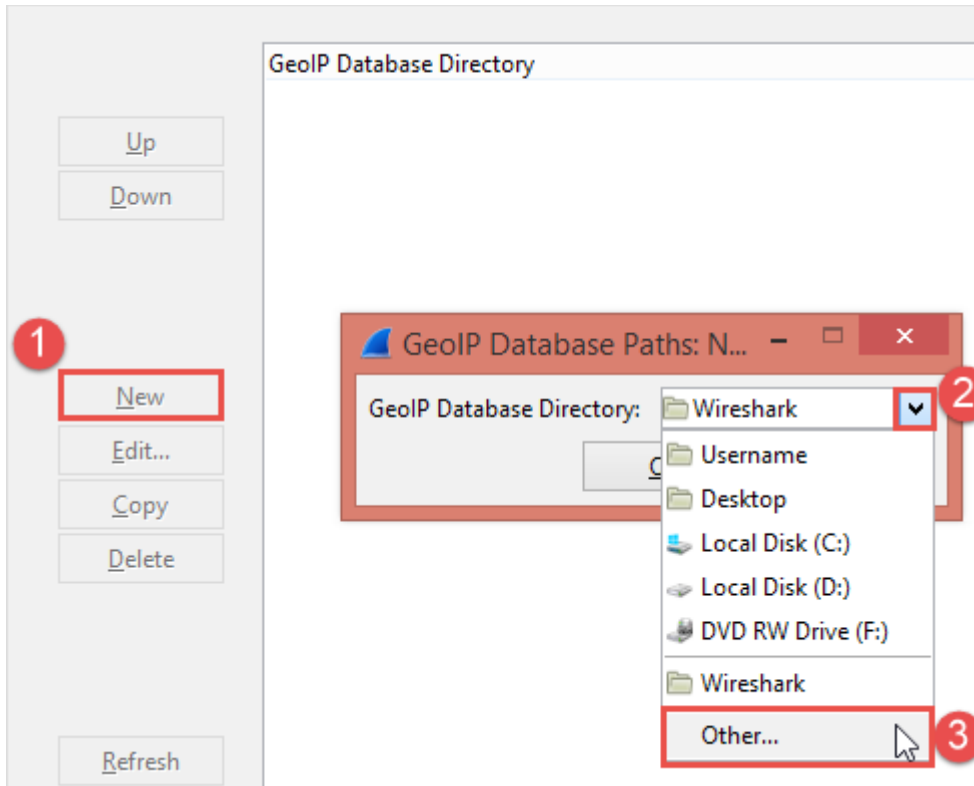
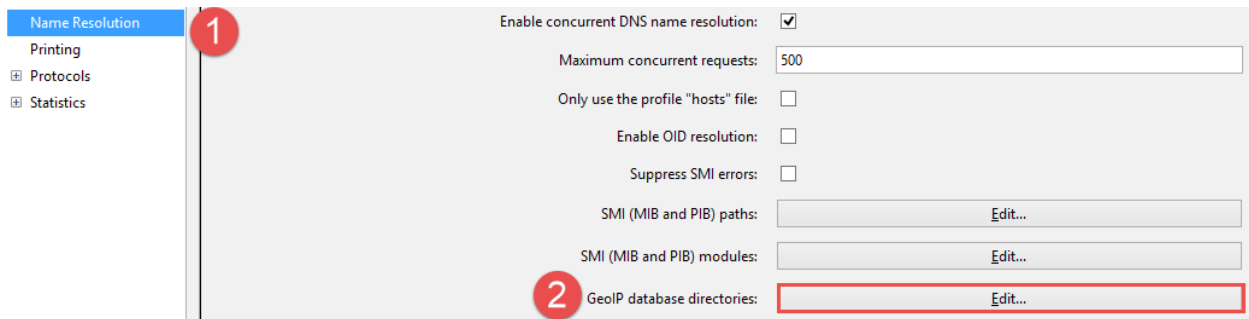
```
C:\Users\Piyush Verma>editcap -v -c 400 HTTP_Traffic.pcap HTTP.pcap
```

 HTTP_00000_20150210215026	2/12/2015 11:05 AM	Wireshark capture file	328 KB
 HTTP_00001_20150210215047	2/12/2015 11:05 AM	Wireshark capture file	282 KB
 HTTP_Traffic	2/10/2015 9:53 PM	Wireshark capture file	597 KB

```
C:\Users\Piyush Verma>mergcap HTTP_00000_20150210215026.pcap HTTP_00001_20150210215047.pcap -w HTTP_Merged.pcap
```

 HTTP_00000_20150210215026	2/12/2015 11:05 AM	Wireshark capture file	328 KB
 HTTP_00001_20150210215047	2/12/2015 11:05 AM	Wireshark capture file	282 KB
 HTTP_Merged	2/12/2015 10:24 PM	Wireshark capture file	609 KB

- Name
-  GeolIP.dat
 -  GeolIP.dat
 -  GeolPASNum.dat
 -  GeolPASNum.dat
 -  GeoLiteCity.dat
 -  GeoLiteCity.dat



Chapter 3: Analyzing Threats to LAN Security

5	0.001510000	192.168.20.129	192.168.20.200	TCP	49944-21 [ACK] Seq=1 Ack=28 win=29696 Li
6	3.285827000	192.168.20.129	192.168.20.200	FTP	Request: USER anonymous
7	3.286395000	192.168.20.200	192.168.20.129	FTP	Response: 331 Anonymous access allowed,
8	3.286570000	192.168.20.129	192.168.20.200	TCP	49944-21 [ACK] Seq=17 Ack=100 win=29696
9	5.610442000	192.168.20.129	192.168.20.200	FTP	Request: PASS anonymous
10	5.611472000	192.168.20.200	192.168.20.129	FTP	Response: 230 Anonymous user logged in.

Ethernet: 1 | Fibre Channel | FDDI | IPv4: 1 | IPv6 | IPX | JXTA | NCP | RSVP | SCTP | **TCP: 1** | Tok

TCP Conversations

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A→B	Bytes A→B
192.168.20.129	58914	192.168.20.137	23	157	12 866	95	

Name resolution Limit to display filter

Help Copy **Follow Stream** Graph A→B

metasploitable login: **mmssffaaddmminn**
 Password: **msfadmin**

TCP Ports: 80,3128,3132,5985,8080,8088,11371,1900,2869,2710

SSL/TLS Ports: 443

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A→B
192.168.20.129	57077	192.168.20.200	20	88	81 953	60
192.168.20.129	42114	192.168.20.200	21	28	2 202	17

Name resolution Limit to display filter

Help Copy **Follow Stream** Graph A→B

Entire conversation (77015 bytes)

192.168.20.129:57077 → 192.168.20.200:20 (77015 bytes)

192.168.20.200:20 → 192.168.20.129:57077 (0 bytes)

Stream Content

..... **JFIF** Exif..II*
 LCE-7.....

Errors: 1 (23597) Warnings: 0 (0) Notes: 0 (0) Chats: 0 (0) Details: 23597

Group Protocol Summary

Malformed TCP Malformed Packet (Exception occurred)

No.	Time	Source	Destination	Protocol	Time to live	Info
1650	0.964400	200.31.92.97	192.168.20.1	TCP	64	[Malformed Packet]
1651	0.964445	24.128.209.15	192.168.20.1	TCP	64	[Malformed Packet]
1652	0.964603	0.28.170.40	192.168.20.1	TCP	64	[Malformed Packet]
1653	0.964651	81.109.181.82	192.168.20.1	TCP	64	[Malformed Packet]
1654	0.964697	66.206.71.10	192.168.20.1	TCP	64	[Malformed Packet]
1655	0.970208	157.228.182.109	192.168.20.1	TCP	64	[Malformed Packet]
1656	0.970305	239.172.62.70	192.168.20.1	TCP	64	[Malformed Packet]
1657	0.970363	85.104.183.50	192.168.20.1	TCP	64	[Malformed Packet]
1658	0.970412	152.6.91.49	192.168.20.1	TCP	64	[Malformed Packet]
1659	0.970628	126.233.181.65	192.168.20.1	TCP	64	[Malformed Packet]
1660	0.970681	125.234.159.121	192.168.20.1	TCP	64	[Malformed Packet]
1661	0.970729	224.147.19.9	192.168.20.1	TCP	64	[Malformed Packet]
1662	0.970775	26.77.72.59	192.168.20.1	TCP	64	[Malformed Packet]

Frame 1650: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
 Ethernet II, Src: 79:0c:b6:43:6c:b3 (79:0c:b6:43:6c:b3), Dst: 92:94:32:04:f3:96 (92:94:32:04:f3:96)
 Destination: 92:94:32:04:f3:96 (92:94:32:04:f3:96)
 Source: 79:0c:b6:43:6c:b3 (79:0c:b6:43:6c:b3)
 [Expert Info (warn/Protocol): Source MAC must not be a group address: IEEE 802.3-2002, Section 3.2.3(b)]
 [Source MAC must not be a group address: IEEE 802.3-2002, Section 3.2.3(b)]
 [Severity level: warn]
 [Group: Protocol]

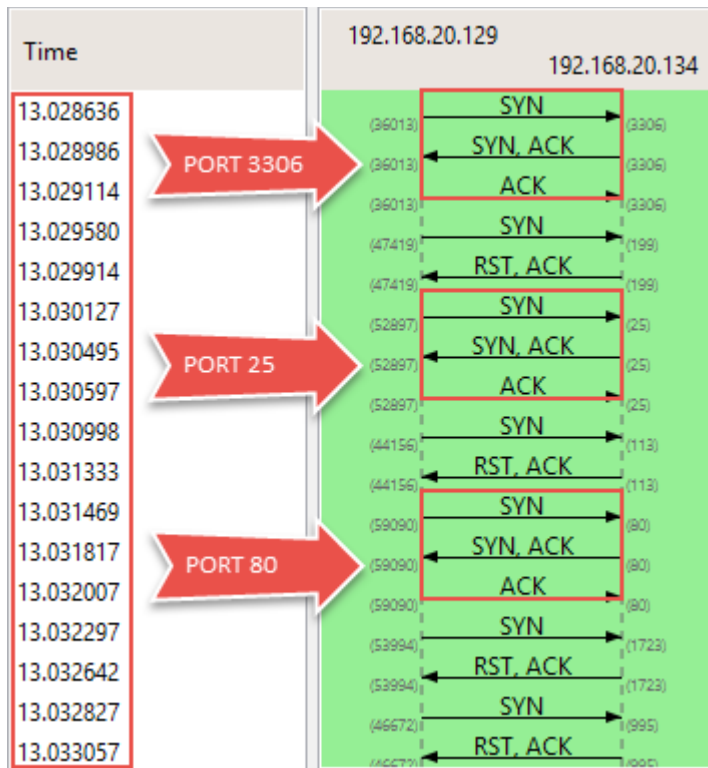
```

Interface: 192.168.20.132 --- 0xb
Internet Address      Physical Address      Type
192.168.20.1         00-0c-29-9b-1a-7a    dynamic
192.168.20.2         00-0c-29-9b-1a-7a    dynamic
192.168.20.128       00-0c-29-9b-1a-7a    dynamic
192.168.20.129       00-0c-29-9b-1a-7a    dynamic
192.168.20.135       00-0c-29-9b-1a-7a    dynamic
  
```

Errors: 0 (0) Warnings: 6 (420) Notes: 0 (0) Chats: 0 (0) Details: 420

Group	Protocol	Summary
Sequence	ARP/RARP	Duplicate IP address configured (192.168.20.135)
Sequence	ARP/RARP	Duplicate IP address configured (192.168.20.254)
Sequence	ARP/RARP	Duplicate IP address configured (192.168.20.132)
Sequence	ARP/RARP	Duplicate IP address configured (192.168.20.128)
Sequence	ARP/RARP	Duplicate IP address configured (192.168.20.2)
Sequence	ARP/RARP	Duplicate IP address configured (192.168.20.1)

No.	Time	Source	Destination	Protocol	Length	Info
200	*REF*	Vmware_e7:a7:32	Broadcast	ARP	42	who has 192.168.20.239? Tell 192.168.20.128
201	0.001763	Vmware_e7:a7:32	Broadcast	ARP	42	who has 192.168.20.211? Tell 192.168.20.128
202	0.003438	Vmware_e7:a7:32	Broadcast	ARP	42	who has 192.168.20.205? Tell 192.168.20.128
203	0.004951	Vmware_e7:a7:32	Broadcast	ARP	42	who has 192.168.20.197? Tell 192.168.20.128
204	0.007426	Vmware_e7:a7:32	Broadcast	ARP	42	who has 192.168.20.184? Tell 192.168.20.128
205	0.009151	Vmware_e7:a7:32	Broadcast	ARP	42	who has 192.168.20.243? Tell 192.168.20.128
206	0.010861	Vmware_e7:a7:32	Broadcast	ARP	42	who has 192.168.20.179? Tell 192.168.20.128
207	0.012412	Vmware_e7:a7:32	Broadcast	ARP	42	who has 192.168.20.163? Tell 192.168.20.128
208	0.014607	Vmware_e7:a7:32	Broadcast	ARP	42	who has 192.168.20.136? Tell 192.168.20.128
209	0.017888	Vmware_e7:a7:32	Broadcast	ARP	42	who has 192.168.20.123? Tell 192.168.20.128



Errors: 0 (0) Warnings: 1 (946) Notes: 0 (0) Chats: 1012 (1012) Details: 1958 Packet Comments: 0

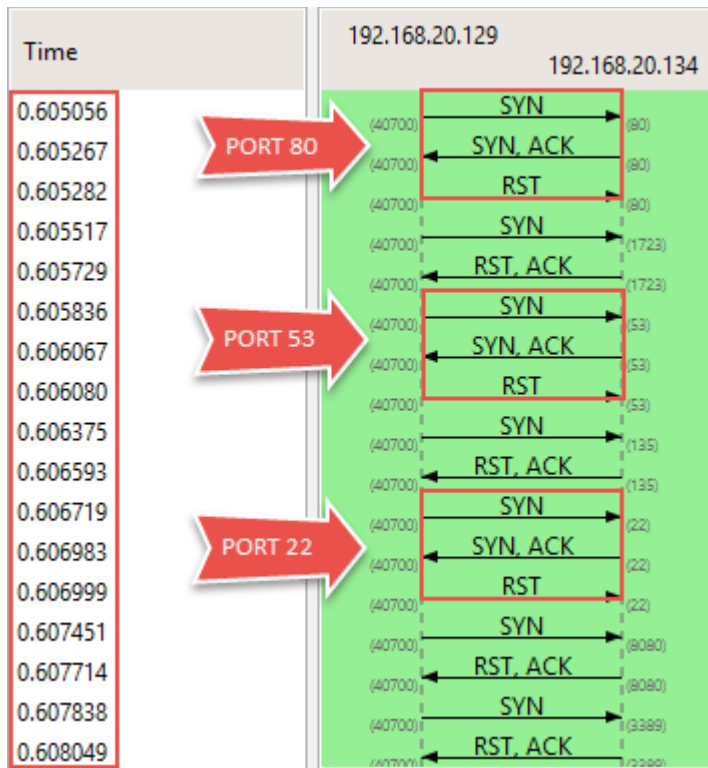
Group Protocol Summary Count

Sequence TCP Connection reset (RST) 946

Address A	Port A	Address B	Port B	Packets	Bytes
192.168.20.129	51610	192.168.20.134	53	4	280
192.168.20.129	38185	192.168.20.134	21	4	280
192.168.20.129	37020	192.168.20.134	3306	4	280
192.168.20.129	56592	192.168.20.134	23	4	280
192.168.20.129	60096	192.168.20.134	80	4	280
192.168.20.129	53907	192.168.20.134	25	4	280
192.168.20.129	43531	192.168.20.134	22	4	280
192.168.20.129	35940	192.168.20.134	139	4	280
192.168.20.129	51495	192.168.20.134	445	4	280
192.168.20.129	36845	192.168.20.134	8180	4	280
192.168.20.129	42382	192.168.20.134	8009	4	280
192.168.20.129	50915	192.168.20.134	5432	4	280
192.168.20.129	43550	192.168.20.134	143	2	134
192.168.20.129	54997	192.168.20.134	1723	2	134
192.168.20.129	48425	192.168.20.134	199	2	134
192.168.20.129	39179	192.168.20.134	256	2	134

Green arrow: Open Ports (points to Port 25)

Red arrow: Closed Ports (points to Port 143)



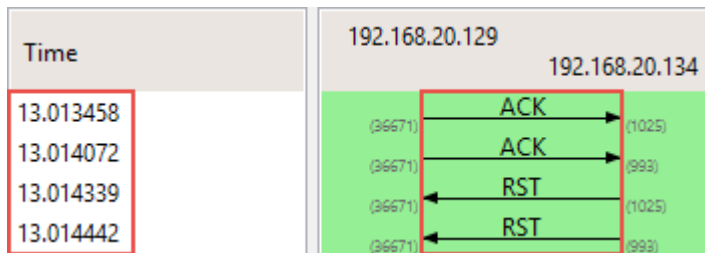
Errors: 0 (0) Warnings: 1 (905) Notes: 0 (0) Chats: 924 (924) Details: 1829 Packet Comments: 0

Group	Protocol	Summary	Count
Sequence	TCP	Connection reset (RST)	905

Address A	Port A	Address B	Port B	Packets	Bytes
192.168.20.129	63122	192.168.20.134	139	3	172
192.168.20.129	63122	192.168.20.134	445	3	172
192.168.20.129	63122	192.168.20.134	22	3	172
192.168.20.129	63122	192.168.20.134	53	3	172
192.168.20.129	63122	192.168.20.134	25	3	172
192.168.20.129	63122	192.168.20.134	3306	3	172
192.168.20.129	63122	192.168.20.134	23	3	172
192.168.20.129	63122	192.168.20.134	21	3	172
192.168.20.129	63122	192.168.20.134	80	3	172
192.168.20.129	63122	192.168.20.134	8180	3	172
192.168.20.129	63122	192.168.20.134	5432	3	172
192.168.20.129	63122	192.168.20.134	8009	3	172
192.168.20.129	63122	192.168.20.134	993	2	118
192.168.20.129	63122	192.168.20.134	1723	2	118
192.168.20.129	63122	192.168.20.134	554	2	118
192.168.20.129	63122	192.168.20.134	1720	2	118

Transmission Control Protocol, Src Port: 58221
 Source Port: 58221 (58221)
 Destination Port: 22 (22)
 [Stream index: 16]
 Header Length: 20 bytes
 0000 0000 0000 = Flags: 0x000 (<None>)

Indicates a packet with NO TCP flags (relative sequence num)



- ⊕ Form item: "GALX" = "iLLG0CpBk_Q"
- ⊕ Form item: "continue" = "http://mail.google.com/mail/"
- ⊕ Form item: "service" = "mail"
- ⊕ Form item: "rm" = "false"
- ⊕ Form item: "tmpl" = "default"
- ⊕ Form item: "scc" = "1"
- ⊕ Form item: "ss" = "1"
- ⊕ Form item: "osid" = "1"
- ⊕ Form item: "_utf8" = "☐☐☐"
- ⊕ Form item: "bgresponse" = "!FBdChXIXE5uStyNEA92AAJecXXI"
- ⊕ Form item: "pstMsg" = "1"
- ⊕ Form item: "dnConn" = ""
- ⊕ Form item: "checkConnection" = ""
- ⊕ Form item: "checkedDomains" = "youtube"
- ⊕ Form item: "Email" = "randomuser@gmail.com"
- ⊕ Form item: "Passwd" = "THE!R!SHC@FE"
- ⊕ Form item: "signIn" = "sign in"

[Full request URI: <http://login.yahoo.com/?src=ym&.int>]

[HTTP request 1/2]

[Response in frame: 8522]

[Next request in frame: 8525]

HTML Form URL Encoded: application/x-www-form-urlencoded

- ⊕ Form item: "countrycode" = "1"
- ⊕ Form item: "username" = "randomuser@yahoo.com"
- ⊕ Form item: "passwd" = "SUPER\$3CR3TP@\$w0rd"

- Case
- Cases
- New Case

Cases List

Name	External Reference	Type	Actions
------	--------------------	------	---------



- Case
- Cases
- Sessions
- Session
- Graphs
- Web
- Mail
- Voip
- Share
- Chat
- Shell
- Undecoded

Session Data

Case and Session name	FirstAnalysis -> Session1
Cap. Start Time	0000-00-00 00:00:00
Cap. End Time	0000-00-00 00:00:00
Status	EMPTY
Hosts	---

Pcap set

PCAP-over-IP TCP port: 30001.
 Add new pcap file.

Choose File No file chosen Upload PCAP Here

Upload

List of all pcap files.

HTTP

Post	0
Get	0
Video	0
Images	0

MMS

Number	0
Contents	0
Video	0
Images	0

Emails

Received	0
Sent	0
Unreaded	0/0

FTP - TFTP - HTTP file

Connections	0 - 0
Downloaded	0 - 0
Uploaded	0 - 0
HTTP	0

Web Mail

Total	0
Received	0
Sent	0



```

root@famstrang-vm:~# sysdig -w dump.scap
^Croot@famstrang-vm:~#
root@famstrang-vm:~#
root@famstrang-vm:~# sysdig -r dump.scap -c topprocs_net
Bytes          Process      PID
-----
20.24M        http        22729
8.84M         http        22728
1.22M         midori      16219
610.68KB     http        21462
5.45KB        sshd        22501
5.05KB        sshd        22537
2.53KB        sshd        22596
780B          avahi-daem  566
243B          sshd        22500
232B          sshd        22536
    
```

Write

Read the trace file and look for top processes

```
root@famstrang-vm:~# sysdig -cl
Category: CPU Usage
-----
spectrogram      Visualize OS latency in real time.
subsecoffset     Visualize subsecond offset execution time.
topcontainers_cpu Top containers by CPU usage
topprocs_cpu     Top processes by CPU usage

Category: Errors
-----
topcontainers_error Top containers by number of errors
topfiles_errors    Top files by number of errors
topprocs_errors    top processes by number of errors
```

```
C:\Pcap2xml-1.0\64-bit>Pcap2XML.exe Wireless_Sample.pcap -s Wireless_Sample.db
PCAP2XML
      ver 1.0 by Pentester Academy
      Info: http://PentesterAcademy.com/pcap2xml
      A tool to convert 802.11 trace files to XML and SQLite DB format
      Ver. 1.0 only supports WLAN MAC Header

[+] Opening file: Wireless_Sample.pcap (175.1 kB)
[+] Processing packet 1093... (100.00 %)
[+] Parsing completed
[+] Dumping into XML and/or SQLite
[+] Processing done!
[+] Run statistics:

Filename:           Wireless_Sample.pcap
Number of packets:  1093
Number of packets parsed: 1093
Data packets parsed: 286
Control packets parsed: 356
Management packets parsed: 451
SQLite out file:    Wireless_Sample.db
Total time taken:   0.484 sec
[-] No update available. This is the latest version
```

Database: Wireless_Sample File: C:\Pcap2xml-1.0\64-bit\Wireless_Sample.db

Wireless_Sample
 MACHeaders
 Packets

1 SELECT DISTINCT COALESCE(addr1, addr2, addr3, addr4) as Address FROM MACHeaders ;

Execute SQL Stop Query SQL Query

RecNo	Address
1	00:0C:41:82:B2:55
2	00:0D:93:82:36:3A
3	01:00:5E:00:00:01
4	01:00:5E:00:00:02
5	01:00:5E:00:00:FB
6	01:00:5E:7F:FF:FA
7	01:80:C2:00:00:00
8	05:48:79:D9:B2:75
9	09:00:07:FF:FF:FF

Result : Unique MAC Addresses

```

# ./sshflow.py SSH.pcap
| sshflow
loading analyzers
  general_stats
  nested_tunnels
  interactive_session
  jabber
  x11_tunneling
  scp
generating statistics from pcap file, please wait...
SSH handshake: 192.168.20.129:56467 -> 192.168.20.134:22
processed 390 packets, analysis follows...

--- analysis of conversation: 192.168.20.129:56467 -> 192.168.20.134:22 ---
General statistics
  Detected ciphersuite: aes128-ctr hmac-md5 zlib@openssh.com
  Smallest possible packet for ciphersuite: 48
  Packets sent by client: 111
  Packets sent by server: 136
  Average client packet length: 890
  Average server packet length: 1185
  Total bytes (of SSH data) sent by client: 7120
  Total bytes (of SSH data) sent by server: 15416
  Most common client packet size: [(48, 101), (64, 3), (144, 2), (32, 1), (16, 1)]
  Most common server packet size: [(48, 57), (64, 48), (80, 15), (112, 3), (1448, 3)]
  Average time between client packets: 0.618071027236
  Average time between server packets: 0.507311671527

-> Likely an interactive shell session
--- End of analysis ---

```



```

# ./sshflow.py SSH2.pcap
| sshflow
loading analyzers
  general_stats
  nested_tunnels
  interactive_session
  jabber
  x11_tunneling
  scp
generating statistics from pcap file, please wait...
SSH handshake: 192.168.10.129:39961 -> 192.168.10.133:22
processed 148 packets, analysis follows...

--- analysis of conversation: 192.168.10.129:39961 -> 192.168.10.133:22 ---
General statistics
  Detected ciphersuite: aes128-ctr hmac-md5 zlib@openssh.com
  Smallest possible packet for ciphersuite: 48
  Packets sent by client: 69
  Packets sent by server: 12
  Average client packet length: 7149
  Average server packet length: 275
  Total bytes (of SSH data) sent by client: 78640
  Total bytes (of SSH data) sent by server: 2200
  Most common client packet size: [(1448, 51), (64, 4), (504, 4), (32, 2), (144, 2)]
  Most common server packet size: [(48, 5), (32, 1), (64, 1), (80, 1), (128, 1)]
  Average time between client packets: 0.0535690151155
  Average time between server packets: 0.311237725345
-> Likely a file copy from client to server
--- End of analysis ---

```

```

GET /sqli-labs/Less-1/?id=1 HTTP/1.1\r\n
Host: 192.168.20.129\r\n
Accept: */*\r\n
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; windows NT 5.1; SV1; .NET CLR 2.0.50727) Havij\r\n
Connection: close\r\n

```

```

GET /sqli-labs/Less-1/?id=1 HTTP/1.1\r\n
Accept-Language: en-us,en;q=0.5\r\n
Accept-Encoding: gzip,deflate\r\n
Host: 127.0.0.1\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
User-Agent: sqlmap/1.0-dev-nongit-20150228 (http://sqlmap.org)\r\n

```

Wireshark: Protocol Hierarchy Statistics

Display filter: none

Protocol	% Packets	Packets	% Bytes
Frame	100.00 %	208428	100.00 %
IEEE 802.11 wireless LAN	100.00 %	208428	100.00 %
IEEE 802.11 wireless LAN management frame	0.10 %	213	0.14 %
Data	74.39 %	155051	95.07 %

Filter: wlan.wep.iv

802.11 Channel: Channel Offset: FCS Filter: All Fr

No.	Time	Source
5	13.203262	Cisco-Li_4c:bb:74
8	13.342526	Cisco-Li_4c:bb:74
9	15.214526	Cisco-Li_4c:bb:74
14	23.340478	Cisco-Li_4c:bb:74
16	23.342522	Cisco-Li_4c:bb:74
18	23.354302	Cisco-Li_4c:bb:74
28	37.516094	Cisco-Li_4c:bb:74
29	37.521214	Cisco-Li_4c:bb:74

<

F... Packets: 208428 · Displayed: 155051 (74.4%)

5 13.203262 Cisco-Li_4c:bb:74 Apple_3e:91:68

<

⊕ Frame 5: 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on 0

⊖ IEEE 802.11 Data, Flags: .p....F.

- Type/Subtype: Data (0x0020)
- ⊕ Frame Control Field: 0x0842
 - .000 0000 0011 0000 = Duration: 48 microseconds
 - Receiver address: Apple_3e:91:68 (e4:ce:8f:3e:91:68)
 - Destination address: Apple_3e:91:68 (e4:ce:8f:3e:91:68)
 - Transmitter address: Cisco-Li_4c:bb:76 (00:1a:70:4c:bb:76)
 - BSS Id: Cisco-Li_4c:bb:76 (00:1a:70:4c:bb:76)
 - Source address: Cisco-Li_4c:bb:74 (00:1a:70:4c:bb:74)
 - Fragment number: 0
 - Sequence number: 2688
- ⊖ WEP parameters
 - Initialization Vector: 0xa70468
 - Key Index: 0
 - WEP ICV: 0x0a624042 (not verified)

```

Aircrack-ng 1.2 rc2

[00:00:00] Tested 861 keys (got 50459 IVs)

KB   depth  byte(vote)
0    0/ 13   28(63744) A8(60928) 86(58880) C7(58880) 3D(58624)
1    0/ 1    57(76544) 0F(60928) 34(59392) 5B(58880) D4(57856)
2    1/ 2    1E(61952) A8(59648) 67(59136) 03(58624) 5F(58368)
3    0/ 1    B4(75264) 31(61184) 7F(60416) 66(58112) 83(57856)
4    9/ 4    F9(58368) 07(57856) EF(57856) FF(57856) 3B(57600)

KEY FOUND! [ 28:E6:6B:E9:D3:B6:20:95:DD:E9:2F:BE:37 ]
Decrypted correctly: 100%

```


802.11 Channel: [v] Channel Offset: [v] FCS Filter: All Frames [v] None [v] Wireless Settings... **Decryption Keys...**

Decryption Key Management

Decryption Keys

Add Decryption Key

Modify Selected Key

Type	Key
WEP	28e66be9d3b62095dde92fbe37

Buttons: New, Edit..., Delete, OK, Cancel, Apply, Cancel

Step 1: Click 'New'

Step 2: Select 'WEP' under the Type

Step 3: Add the key after removing the colons [:]

Step 4: Click 'OK'

Step 5: Click 'Apply'

192.168.0.122	49512	2.2.2.2	adobeserver-2	5	639	5
---------------	-------	---------	---------------	---	-----	---

Name resolution Limit to display filter

Buttons: Help, Copy, Follow Stream, Graph A-B

Follow TCP Stream (tcp.stream eq 2)

Stream Content

PK.. Signature for ZIP file

flag4.txtUT...

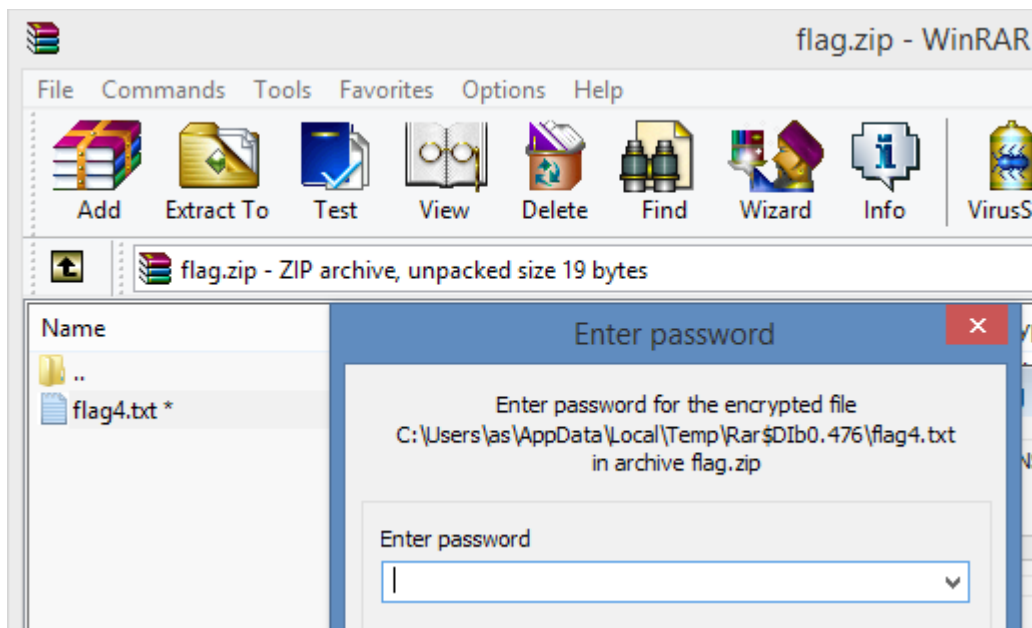
flag4.txtUT...

Entire conversation (215 bytes)

Buttons: Find, Save As, Print, ASCII, Hex Dump, C Arrays

Buttons: Help, Filter Out This Stream, Close

Click on this and Save as a ZIP file



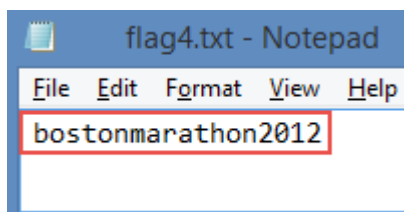
```

[-] Internet Message Format
    Received: from [192.168.0.122] ([2.2.2.1]) by c...
    Message-ID: <4F9DB1BE.9060902@carolinacon8.com>
    Date: Sun, 29 Apr 2012 17:25:18 -0400
    [+ From: metalman <metalman@carolinacon8.com>, 1 i...
    User-Agent: Mozilla/5.0 (windows; U; windows NT
    MIME-Version: 1.0
    [+ To: crashman@carolinacon8.com, metalman@carolin...
    Subject: yo...
    [+ Content-Type: text/plain; charset=ISO-8859-1; f...
    Content-Transfer-Encoding: 7bit
    Return-Path: <metalman@carolinacon8.c...
    [-] Line-based text data: text/plain
        cm,\r\n
        is this right?\r\n
        \r\n
        dGhlIHBhc3N3b3JkIGlzIGJvc3Rvbk1BMTk3Nwo=\r\n
  
```

Base-64 encoded string

```

:~# python
Python 2.7.3 (default, Mar 14 2014, 11:57:14)
[GCC 4.7.2] on linux2
Type "help", "copyright", "credits" or "licen
>>> import base64
>>> base64.b64decode("dGhlIHBhc3N3b3JkIGlzIGJvc3Rvbk1BMTk3Nwo=")
'the password is bostonMA1977\n'
  
```



No.	Time	Source	Destination	Protocol	Info
30225	*REF*	192.168.10.1	192.168.10.132	POP	C: PASS eeeevw
30226	0.000422	192.168.10.1	192.168.10.132	POP	C: PASS eeeevw
30264	0.074131	192.168.10.1	192.168.10.132	POP	C: PASS eeeevy
30312	0.199417	192.168.10.1	192.168.10.132	POP	C: PASS eeeevY
30322	0.249480	192.168.10.1	192.168.10.132	POP	C: PASS eeeevb
30325	0.262069	192.168.10.1	192.168.10.132	POP	C: PASS eeeevB
30326	0.262111	192.168.10.1	192.168.10.132	POP	C: PASS eeeevv
30330	0.277704	192.168.10.1	192.168.10.132	POP	C: PASS eeeevV
30331	0.277711	192.168.10.1	192.168.10.132	POP	C: PASS eeeevK
30332	0.277711	192.168.10.1	192.168.10.132	POP	C: PASS eeeevk
30345	0.327554	192.168.10.1	192.168.10.132	POP	C: PASS eeeevx
30346	0.327642	192.168.10.1	192.168.10.132	POP	C: PASS eeeevX

No.	Time	Source	Destination	Protocol	Info
25	*REF*	192.168.10.129	192.168.10.133	FTP	Request: USER admin
28	0.003557	192.168.10.129	192.168.10.133	FTP	Request: PASS anonymous
30	0.006026	192.168.10.129	192.168.10.133	FTP	Request: USER admin
32	0.009513	192.168.10.129	192.168.10.133	FTP	Request: PASS PACKT
34	0.021116	192.168.10.129	192.168.10.133	FTP	Request: USER admin
36	0.031096	192.168.10.129	192.168.10.133	FTP	Request: PASS packtpub
39	0.032572	192.168.10.129	192.168.10.133	FTP	Request: USER admin
48	0.048233	192.168.10.129	192.168.10.133	FTP	Request: USER admin
51	0.060492	192.168.10.129	192.168.10.133	FTP	Request: PASS ftppassword

No.	Time	Source	Destination	Protocol	Info
1576	10.316911	192.168.10.133	192.168.10.129	FTP	Response: 230 User msfadmin logged in



Chapter 4: Probing E-mail Communications

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.3	192.168.0.1	TCP	62	1077→25 [SYN] Seq=0 win=16384 Len=0 MS
2	0.000000	192.168.0.1	192.168.0.3	TCP	62	25→1077 [SYN, ACK] Seq=0 Ack=1 win=175
3	0.020029	192.168.0.3	192.168.0.1	TCP	60	1077→25 [ACK] Seq=1 Ack=1 win=17520 Len
4	0.020029	192.168.0.1	192.168.0.3	SMTP	158	S: 220 Server Microsoft ESMTP MAIL Ser
5	0.030043	192.168.0.3	192.168.0.1	SMTP	67	C: EHLO Client
6	0.190274	192.168.0.1	192.168.0.3	TCP	54	25→1077 [ACK] Seq=105 Ack=14 win=17507
7	0.420605	192.168.0.1	192.168.0.3	SMTP	290	S: 250 Server Hello [192.168.0.3] 25
8	0.430619	192.168.0.3	192.168.0.1	SMTP	66	C: AUTH LOGIN
9	0.430619	192.168.0.1	192.168.0.3	SMTP	72	S: 334 VXN1cm5hbWU6
10	0.430619	192.168.0.3	192.168.0.1	SMTP	64	C: User: QXVkaQ==
11	0.430619	192.168.0.1	192.168.0.3	SMTP	72	S: 334 UGFzc3dvcmQ6
12	0.430619	192.168.0.3	192.168.0.1	SMTP	64	C: Pass: MTIzNGFk
13	0.440634	192.168.0.1	192.168.0.3	SMTP	91	S: 235 2.7.0 Authentication successful

Ethernet: 5 Fibre Channel FDDI IPv4: 4 IPv6 IPX JXTA NCP RSVP SCTP **TCP: 2** Token Ring **UDP: 3** USB WLAN

TCP Conversations

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A-B	Bytes A-B	Packets A-B	Bytes A-B
192.168.56.102	1048	192.168.56.101	25	460	508 893	369	502 828	91	6 065
192.168.56.102	1047	192.168.56.101	25	16	1 327	8	541	8	786

Name resolution Limit to display filter


```

Content-Type: application/octet-stream;
.name="secret.rtf"
Content-Transfer-Encoding: quoted-printable
Content-Disposition: attachment;
.filename="secret.rtf"

{\rtf1\ansi\ansicpg1252\deff0\deflang2057{\fonttbl{\f0\fswiss\fcharset0 =
Arial;}}
{\*\generator Msftedit 5.41.21.2509;} \viewkind4\uc1\pard\f0\fs20 This is =
a secret proto type of the new car being launched by =
Securityoverride.\par
\par
{\object\objemb{\*\objclass Package}\objw1200\objh810{\*\objdata=20

```

Beginning of the RTF file

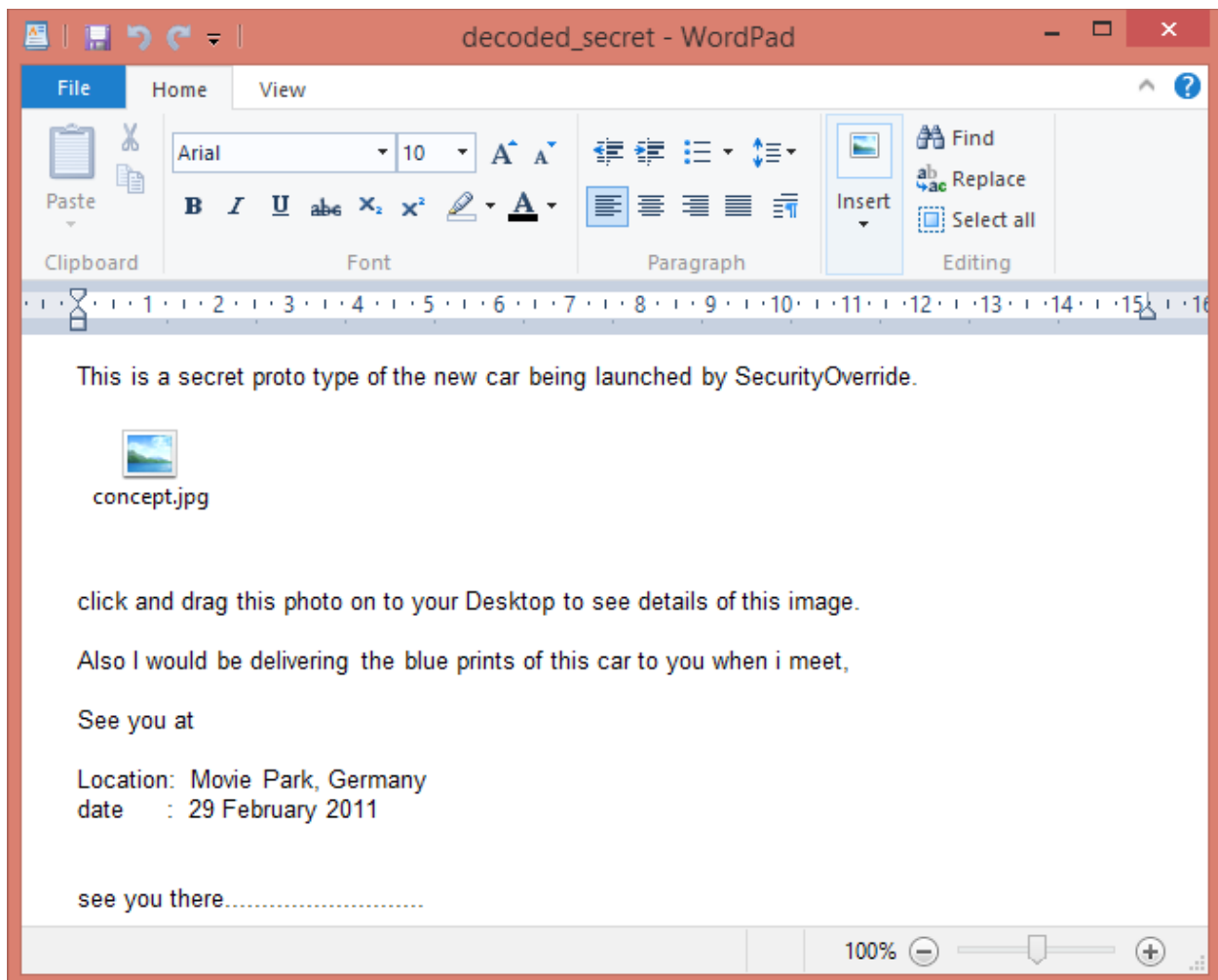
Stream Content

```

000005000000020101000000050000002e01
42e6a
706700210028001c000000fb021000070000
d0000
ef01662300000a0022008a0100000000ffff
000
}}} \par
\par
\par
click and drag this photo on to your
image.\par
\par
Also I would be delivering the blue
meet, \par
\par
See you at \par
\par
Location: Movie Park, Germany\par
date\tab : 29 February 2011\par

```

End of RTF File



```
famstrang@GHost:~$ nc -v 192.168.20.160 25
itsecgames.com [192.168.20.160] 25 (smtp) open
220 bee-box ESMTMP Postfix (Ubuntu)
VRFY root
252 2.0.0 root
VRFY piyush
550 5.1.1 <piyush>: Recipient address rejected: User unknown in local recipient table
VRFY bee
252 2.0.0 bee
```

Response for Valid User

Response for Invalid User

```
msf auxiliary(smtp_enum) > run

[*] 192.168.20.160:25 Banner: 220 bee-box ESMTMP Postfix (Ubuntu)
[+] 192.168.20.160:25 Users found: , avahi, avahi-autoipd, backup, bin, daemon,
ftp, games, gdm, gnats, haldaemon, hplip, irc, libuuid, list, lp, mail, man, mes
sagebus, news, nobody, postmaster, proxy, pulse, sshd, sync, sys, syslog, uucp,
www-data
```


Filter: smtp.req.command == "RCPT" Expression... Clear Apply Save

No.	Source	Destination	Protocol	Info
15	192.168.20.140	192.168.20.160	SMTP	C: RCPT TO: brZjrzFw@bee-box
21	192.168.20.140	192.168.20.160	SMTP	C: RCPT TO: @bee-box
27	192.168.20.140	192.168.20.160	SMTP	C: RCPT TO: 4dgifts@bee-box
33	192.168.20.140	192.168.20.160	SMTP	C: RCPT TO: EZsetup@bee-box
39	192.168.20.140	192.168.20.160	SMTP	C: RCPT TO: OutOfBox@bee-box
45	192.168.20.140	192.168.20.160	SMTP	C: RCPT TO: adm@bee-box
51	192.168.20.140	192.168.20.160	SMTP	C: RCPT TO: admin@bee-box
57	192.168.20.140	192.168.20.160	SMTP	C: RCPT TO: administrator@bee-box
63	192.168.20.140	192.168.20.160	SMTP	C: RCPT TO: anon@bee-box
69	192.168.20.140	192.168.20.160	SMTP	C: RCPT TO: auditor@bee-box
77	192.168.20.140	192.168.20.160	SMTP	C: RCPT TO: avahi@bee-box
86	192.168.20.140	192.168.20.160	SMTP	C: RCPT TO: avahi-autoipd@bee-box
95	192.168.20.140	192.168.20.160	SMTP	C: RCPT TO: backup@bee-box
104	192.168.20.140	192.168.20.160	SMTP	C: RCPT TO: bbs@bee-box

Filter: smtp.response.code == 554 Expression... Clear Apply Save

No.	Source	Destination	Protocol	Info
21	192.168.20.141	192.168.20.140	SMTP	S: 554 5.7.1 <relaytest@nmap.scanme.org>: Relay access denied
27	192.168.20.141	192.168.20.140	SMTP	S: 554 5.7.1 <relaytest@nmap.scanme.org>: Relay access denied
33	192.168.20.141	192.168.20.140	SMTP	S: 554 5.7.1 <relaytest@nmap.scanme.org>: Relay access denied
39	192.168.20.141	192.168.20.140	SMTP	S: 554 5.7.1 <relaytest@nmap.scanme.org>: Relay access denied
45	192.168.20.141	192.168.20.140	SMTP	S: 554 5.7.1 <relaytest%nmap.scanme.org@[192.168.20.141]>: Rel
51	192.168.20.141	192.168.20.140	SMTP	S: 554 5.7.1 <relaytest%nmap.scanme.org@metasploitable.localdo
57	192.168.20.141	192.168.20.140	SMTP	S: 554 5.7.1 <relaytest@nmap.scanme.org>: Relay access denied
63	192.168.20.141	192.168.20.140	SMTP	S: 554 5.7.1 <relaytest%nmap.scanme.org>: Relay access denied

Source	Destination	Protocol	Length	Info
192.1		SMTP	66	C: AUTH LOGIN 1
192.1		SMTP	72	S: 33
192.1		SMTP	64	C: US
192.1		SMTP	72	S: 334 UGFzc3dvcmQ6
192.1		SMTP	64	C: Pass: MTIZNGFk
192.1		SMTP	91	S: 235 2.7.0 Authentication
192.1		SMTP	94	C: MAIL FROM: <Audi@securi
192.1		SMTP	104	S: 250 2.1.0 Audi@security
192.1		SMTP	79	C: RCPT TO: <Gotya@i.suck>
192.1		SMTP	79	S: 250 2.1.5 Gotya@i.suck
192.1		SMTP	60	C: DATA
192.1		SMTP	100	S: 354 Start mail input; e
192.1		SMTP	1404	C: DATA fragment, 1350 byt
192.1		TCP	54	25→1077 [ACK] Seq=535 Ack=
192.1		IMF	60	from: "Audi" <Audi@securit
192.1		SMTP	131	S: 250 2.6.0 <000801cad7e
192.1		SMTP	60	C: QUIT
192.1		SMTP	109	S: 221 2.0.0 Server Servic

bytes on wire (528 bits), 6

- 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

Right-click any SMTP Frame

Simple Mail Transfer Protocol Preferences...

- Reassemble SMTP command and response lines spanning multiple TCP segments
- Reassemble SMTP DATA commands spanning multiple TCP segments
- Decrypt AUTH parameters

```
:~# python b64decoder.py QXVkaQ==  
Base64 decoded value = Audi  
:~# python b64decoder.py MTIzNGFk  
Base64 decoded value = 1234ad
```

```
:~# md5sum concept.jpg  
3796102e17ff50382cb48160b76a3946 concept.jpg
```

Chapter 5: Inspecting Malware Traffic

No.	Time	Source	SPort	Destination	DPort	Length	Protocol	HTTP Host	URI
2346	17.03	172.16.165.2	53	172.16.165.132	57758	289	DNS		

[Coloring Rule Name: Unusual # of DNS Answers]
[Coloring Rule string: dns.count.answers > 5]

Filter: Expression... Clear Apply Save HTTP Req Host via DHCP Host via DNS IRC - Join Command IRC - Requests

Protocol

- Frame
- Ethernet
 - Internet Protocol Version 4
 - Transmission Control Protocol
 - Hypertext Transfer Protocol
 - HyperText Transfer Protocol 2
 - Secure Sockets Layer
 - Data

Conversations: 2013-07-21-Blackhole-EK-traffic.pcap

Ethernet: 2 Fibre Chan IPv6 IPX

Infected Box

Address A	Port A	Address B	Port B
192.168.204.150	54616	91.186.20.51	80
192.168.204.150	54618	176.119.5.7	80
192.168.204.150	54619	176.119.5.7	80
192.168.204.150	54622	176.119.5.7	80
192.168.204.150	54624	176.119.5.7	80
192.168.204.150	54626	176.119.5.7	80
192.168.204.150	54627	91.228.53.137	443
192.168.204.150	54628	91.228.53.137	443
192.168.204.150	54631	173.224.210.244	443
192.168.204.150	54632	91.228.53.137	443
192.168.204.150	54633	173.224.210.244	443
192.168.204.150	54636	173.224.210.244	443
192.168.204.150	54638	173.224.210.244	443
192.168.204.150	54639	91.228.53.137	443
192.168.204.150	54640	91.228.53.199	443
192.168.204.150	54641	91.228.53.199	443

Filter: http.request

No.	Time	Source
4	0	192.168.204.150
13	0	192.168.204.150
24	1	192.168.204.150
99	3	192.168.204.150
112	3	192.168.204.150
119	8	192.168.204.150
175	9	192.168.204.150

How to detect the ZeroAccess botnet on your network and ...

scwoa.com/how-to-detect-the-zeroaccess-botnet-on-your-network-and-st...

Dec 11, 2013 - ZeroAccess (as of this writing) uses ports 16464, 16465, 16470, and / or 16471. The specific port depends on whether the version is 32-bit or ...

[PDF] The ZeroAccess Botnet – Mining and Fraud for Massive ...


cyber-peace.org/wp-content/uploads/.../Sophos_ZeroAccess_Botnet.pdf

by J Wyke - 2012 - Cited by 19 - Related articles

Sep 4, 2012 - Ports 16464 and 16465 are used by the 32-bit and 64-bit versions of one botnet; ports 16470 and 16471 are used by the. 64-bit and 32-bit ...

Malicious URL History	Hostname Usage History	Malicious Sample Download History	Normal Sample Download History	Malicious Sample Communication History	Normal Sample Communication History
0	0	0	0	27	2

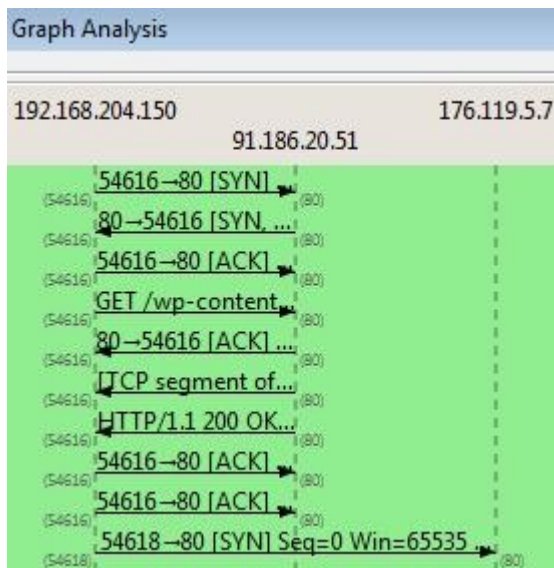
≡ Malicious sample history communicated with this IP

No.	SHA-256	Anti-virus	Scan Date 
27	2144D81A9EACBD6D90F72A547E4AE7547F6ED727711F6AE17F327E7665D546E1	35 / 47	2015-01-26 01:37:06
26	A8D136368FA08EE00266857CAB92FD7D2290B42611C1FA28DA47B5C926E45F81	46 / 53	2014-05-27 01:23:29
25	C3854C173EF08D75F5134691FEB78A75B054E170CE387085A0D28D4208BE705	14 / 46	2013-08-17 03:45:19
24	BEF57360968571756223311BC86C5CFEB3955F0044C1706F0A492E49C61F5369	8 / 46	2013-08-14 15:52:43

Host
 tonerkozpont.com
 raiwinners.org
 domenicossos.com
 domenicossos.com
 domenicossos.com
 domenicossos.com
 domenicossos.com
 domenicossos.com
 domenicossos.com

```
<html>
<head>
<meta http-equiv="Refresh" content="1;URL="http://raiwinners.org/sword/in.cgi?2">
</head>
<body>
```

HTTP/1.1 302 Found
 Date: Thu, 18 Jul 2013 20:45:33 GMT
 Server: nginx/0.7.67
 Location: <http://domenicossos.com/ngen/controlling/mydb.php>
 Connection: Keep-Alive



Packet num	Hostname	Content Type	Size	Filename
7	tonerkozpont.com	text/html	258 bytes	sftxtel.html
17	raiwinners.org	text/html	232 bytes	in.cgi?2
93	domenicossos.com	text/html	46 kB	mydb.php
106	domenicossos.com	application/octet-stream	4170 bytes	shrift.php
163	domenicossos.com	application/java-archive	31 kB	mydb.php?IMugUQWjIXMtBPs=kOYtJQ
665	domenicossos.com	application/x-msdownload	348 kB	mydb.php?Vf=53322f312h&be=2g522j3:
1017	domenicossos.com	application/x-msdownload	211 kB	mydb.php?Hf=53322f312h&ye=2g542d:
1212	domenicossos.com	application/x-msdownload	102 kB	mydb.php?ff=53322f312h&le=5552532f:

```

HTTP/1.1 200 OK
Date: Thu, 18 Jul 2013 20:45:40 GMT
ETag: "f472177c3d4f8d76cacb20c3a092a2cc"
Server: nginx/0.7.67
Connection: Keep-Alive
Content-Type: application/java-archive
X-Powered-By: PHP/5.3.23

```

```

HTTP/1.1 200 OK
Date: Thu, 18 Jul 2013 20:45:42 GMT
Pragma: public
Server: nginx/0.7.67
Expires: Thu, 18 Jul 2013 23:42:19 GMT
Connection: Keep-Alive
Content-Type: application/x-msdownload
X-Powered-By: PHP/5.3.23
Cache-Control: must-revalidate, post-check=0, pre-check=0
Cache-Control: private
Content-Length: 348160
Content-Disposition: attachment; filename="calc.exe"
Content-Transfer-Encoding: binary

```

File-signature for EXE

```

MZ.....@.....!..L.!This
program cannot be run in DOS mode.

```

```

Content-Length: 211968
Content-Disposition: attachment; filename="info.exe"
Content-Transfer-Encoding: binary

```

File-signature for EXE

```

MZ.....@.....!..L.!This
program cannot be run in DOS mode.

```

```

Content-Length: 102912
Content-Disposition: attachment; filename="readme.exe"
Content-Transfer-Encoding: binary




```

File-signature for EXE

```

MZ.....@.....!..L.!This
program cannot be run in DOS mode.

```

 calc	Application	340 KB
 info	Application	207 KB
 JavaArchive.jar	JAR File	31 KB
 readme	Application	101 KB



SHA256: 43565420246215bef3f02615166e38eaec4cde9d77c59f322c99421d1693649c

File name: readme.exe

Detection ratio: 36 / 49

Filter: irc Expression... Clear Apply

No.	Time	Source	SPort	Destination	DPort	Length	Protocol
46	19.02	147.32.84.165	1039	130.239.18.172	6667	101	IRC
47	19.06	130.239.18.172	6667	147.32.84.165	1039	118	IRC
58	19.22	130.239.18.172	6667	147.32.84.165	1039	159	IRC

42	18.98	147.32.80.9	53	147.32.84.165	1025	479	DNS	standard query response 0x3e54	CNAME chat.freenode.net
28627	795.26	147.32.80.9	53	147.32.84.165	1025	479	DNS	standard query response 0x3453	CNAME chat.freenode.net

Answers

- irc.freenode.net: type CNAME, class IN, cname chat.freenode.net
- chat.freenode.net: type A, class IN, addr 130.239.18.172
- chat.freenode.net: type A, class IN, addr 140.211.167.98
- chat.freenode.net: type A, class IN, addr 140.211.167.99
- chat.freenode.net: type A, class IN, addr 174.143.119.91
- chat.freenode.net: type A, class IN, addr 213.92.8.4
- chat.freenode.net: type A, class IN, addr 213.179.58.83
- chat.freenode.net: type A, class IN, addr 213.232.93.3
- chat.freenode.net: type A, class IN, addr 216.155.130.130
- chat.freenode.net: type A, class IN, addr 38.229.70.20
- chat.freenode.net: type A, class IN, addr 78.40.125.4
- chat.freenode.net: type A, class IN, addr 82.96.64.4
- chat.freenode.net: type A, class IN, addr 86.65.39.15
- chat.freenode.net: type A, class IN, addr 89.16.176.16
- chat.freenode.net: type A, class IN, addr 93.152.160.101
- chat.freenode.net: type A, class IN, addr 128.237.157.136

```
NICK Pepe889696
USER znuehjm 0 0 :Pepe889696
USERHOST Pepe889696
MODE Pepe889696 -x
JOIN #zarasa48
```



```

:pepe|2!~kvirc@cmpgw-27.felk.cvut.cz PRIVMSG #zarasa48 :.ddos.syn 147.32.96.69 1
:pepe|2!~kvirc@cmpgw-27.felk.cvut.cz PRIVMSG #zarasa48 :.ddos.syn 147.32.96.69 1 60
PRIVMSG #zarasa48 :[DDoS]: Done with flood (OKB/sec).
PRIVMSG #zarasa48 :[DDoS]: Flooding: (147.32.96.69:1) for 60 seconds.
:pepe|2!~kvirc@cmpgw-27.felk.cvut.cz PRIVMSG #zarasa48 :.tcpflood syn 147.32.96.69 1
1000
PRIVMSG #zarasa48 :[TCP]: Error sending packets to IP: 147.32.96.69. Packets sent:
0. Returned: <0>.
PRIVMSG #zarasa48 :[TCP]: Normal syn flooding: (147.32.96.69:1) for 1000 seconds.
:pepe|2!~kvirc@cmpgw-27.felk.cvut.cz PRIVMSG #zarasa48 :.tcpflood syn 147.32.96.69 1
100
PRIVMSG #zarasa48 :[TCP]: Error sending packets to IP: 147.32.96.69. Packets sent:
0. Returned: <0>.
PRIVMSG #zarasa48 :[TCP]: Normal syn flooding: (147.32.96.69:1) for 100 seconds.
:pepe|2!~kvirc@cmpgw-27.felk.cvut.cz PRIVMSG #zarasa48 :.tcpflood syn 147.32.96.69
22 100
PRIVMSG #zarasa48 :[TCP]: Error sending packets to IP: 147.32.96.69. Packets sent:
0. Returned: <0>.
PRIVMSG #zarasa48 :[TCP]: Normal syn flooding: (147.32.96.69:22) for 100 seconds.
:pepe|2!~kvirc@cmpgw-27.felk.cvut.cz PRIVMSG #zarasa48 :.dos.random 147.32.96.69 22
1000
:pepe|2!~kvirc@cmpgw-27.felk.cvut.cz PRIVMSG #zarasa48 :.ddos.random 147.32.96.69 22
1000
PRIVMSG #zarasa48 :[DDoS]: Done with flood (OKB/sec).
PRIVMSG #zarasa48 :[DDoS]: Flooding: (147.32.96.69:22) for 1000 seconds.
:pepe|2!~kvirc@cmpgw-27.felk.cvut.cz PRIVMSG #zarasa48 :.tcpflood ack 147.32.96.69
337 120 -r
PRIVMSG #zarasa48 :[TCP]: Error sending packets to IP: 147.32.96.69. Packets sent:
0. Returned: <0>.
PRIVMSG #zarasa48 :[TCP]: spoofed ack flooding: (147.32.96.69:337) for 120 seconds.
:pepe|2!~kvirc@cmpgw-27.felk.cvut.cz PRIVMSG #zarasa48 :.icmpflood 147.32.96.69 1800
PRIVMSG #zarasa48 :[ICMP]: Flooding: (147.32.96.69) for 1800 seconds.

```

Chapter 6: Network Performance Analysis

Show TCP summary in protocol tree:

Validate the TCP checksum if possible:

Allow subdissector to reassemble TCP streams:

Analyze TCP sequence numbers:

Relative sequence numbers:

Scaling factor to use when not available from capture:

Track number of bytes in flight:

Calculate conversation timestamps:

Try heuristic sub-dissectors first:

Ignore TCP Timestamps in summary:

Do not call subdissectors for error packets:

TCP Experimental Options with a Magic Number:

Filter: Expression... Clear Apply Save HTTP Errors DNS Errors FTP Errors WLAN Retries

No.	Time	TCP Delta	SEQ#	NEXTSEQ#	ACK#	WinSize	Source	Destination	Protocol
-----	------	-----------	------	----------	------	---------	--------	-------------	----------

Errors: 1 (2) Warnings: 5 (200) Notes: 163 (722) Chats: 19 (529) Details: 1453 Packet Comments: 0

Group	Protocol	Summary	Count
Sequence	TCP	This frame is a (suspected) fast retransmission	16
Sequence	TCP	This frame is a (suspected) retransmission	33

Filter: tcp.window_size_value ==0 Expression... Clear Apply Save HTTP Errors DNS Errors FTP Errors WLAN Retries

No.	Time	TCP Delta	Windows Size	Source	Destination	Protocol	Info
1323	12.962	8.104585000	0	192.168.10.132	68.232.44.114	TCP	5000-80 [RST, ACK] Seq=1 Ack=2 win=0 L
1324	12.963	7.943608000	0	192.168.10.132	54.169.22.250	TCP	4997-80 [RST, ACK] Seq=1 Ack=2 win=0 L

Filter: tcp.window_size_value ==0 Expression... Clear Apply Save HTTP Errors DNS Errors FTP Errors WLAN Retries

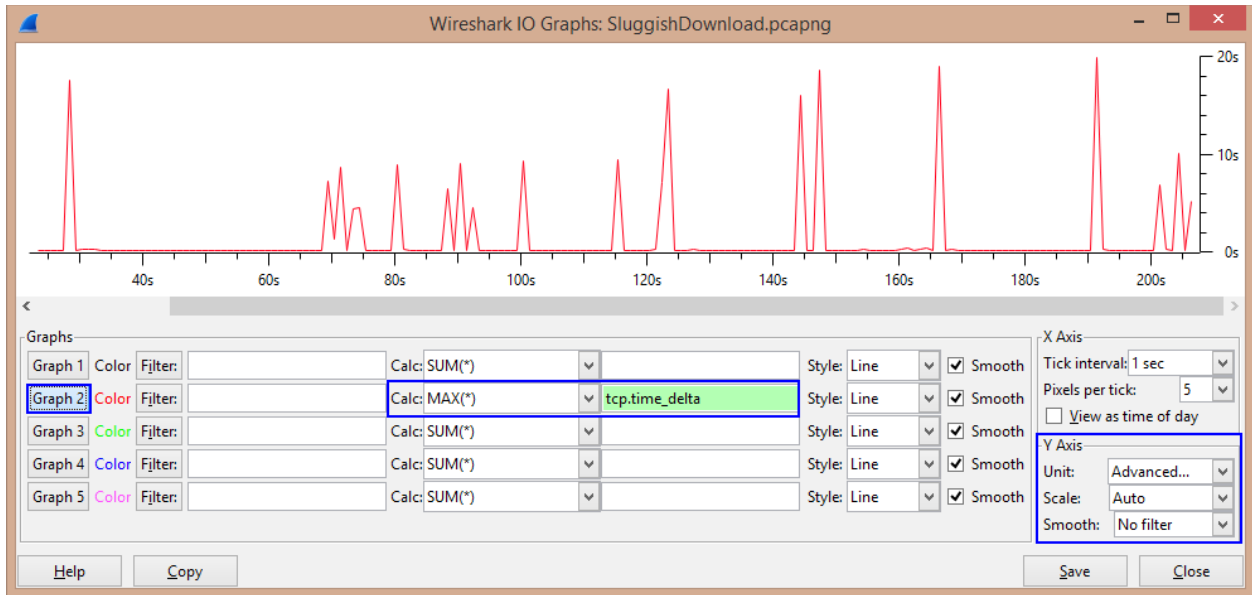
No.	Time	TCP Delta	Windows Size	Source	Destination	Protocol	Info
6482	57.315	0.000068000	0	192.168.0.4	54.187.150.105	TCP	[TCP Zerowindow] 51482-443 [ACK] Seq=373

UDP Conversations

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A-B	Bytes A-B
192.168.10.132	46816	182.58.215.46	17940	471	372 354	300	360 583
192.168.10.132	46816	116.203.219.84	31098	283	231 847	168	224 215
192.168.10.132	46816	2.51.48.167	26372	109	41 966	57	3 534

DNS	standard query	0xb445	A	version.vuze.com
DNS	standard query	0x10c7	SOA	piyush-40f60e5d.docomo.com
DNS	standard query	0x0001	ANY	tracker.istole.it
DNS	standard query	0x0001	ANY	12.rarbg.me
DNS	standard query	0x0002	ANY	tracker.istole.it
DNS	standard query	0xdc47	A	ipv4.tracker.harry.lu
DNS	standard query	0x2746	A	tracker.coppersurfer.tk
DNS	standard query	0x5e40	A	bttracker.crunchbanglinux.org
DNS	standard query	0x2943	A	tracker1.wasabii.com.tw
DNS	standard query	0xae4d	A	tracker.nwps.ws
DNS	standard query	0x6b4c	A	tracker.ccc.de

No.	Time	TCP Delta
278630	191.901	19.821587000
278309	191.754	19.689591000
278143	191.678	19.581039000
278151	191.682	19.575095000
278115	191.666	19.554924000
277988	191.625	19.534762000
277805	191.525	19.382842000
277185	191.244	19.136907000
276868	191.103	19.002715000
257247	166.221	18.860083000



Filter: `tcp.flags.syn==1 && tcp.flags.ack==0` Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Src Port	Dst Port	Info
1	0.000000	10.10.10.10	192.168.10.133	TCP	1563	80	cadabra-1m-http [SYN] Seq=0 win=512 Len=0
2	0.000873	10.10.10.10	192.168.10.133	TCP	1564	80	pay-per-view-http [SYN] Seq=0 win=512 Len=0
3	0.001093	10.10.10.10	192.168.10.133	TCP	1565	80	winddlb-http [SYN] Seq=0 win=512 Len=0
4	0.001283	10.10.10.10	192.168.10.133	TCP	1566	80	corelvideo-http [SYN] Seq=0 win=512 Len=0
5	0.001466	10.10.10.10	192.168.10.133	TCP	1567	80	jlicelmd-http [SYN] Seq=0 win=512 Len=0
6	0.001645	10.10.10.10	192.168.10.133	TCP	1568	80	tsspmap-http [SYN] Seq=0 win=512 Len=0
7	0.001822	10.10.10.10	192.168.10.133	TCP	1569	ets-http [SYN] Seq=0 win=512 Len=0	
8	0.002000	10.10.10.10	192.168.10.133	TCP	1570	80	orbixd-http [SYN] Seq=0 win=512 Len=0

Targeting the same Destination Port : 80