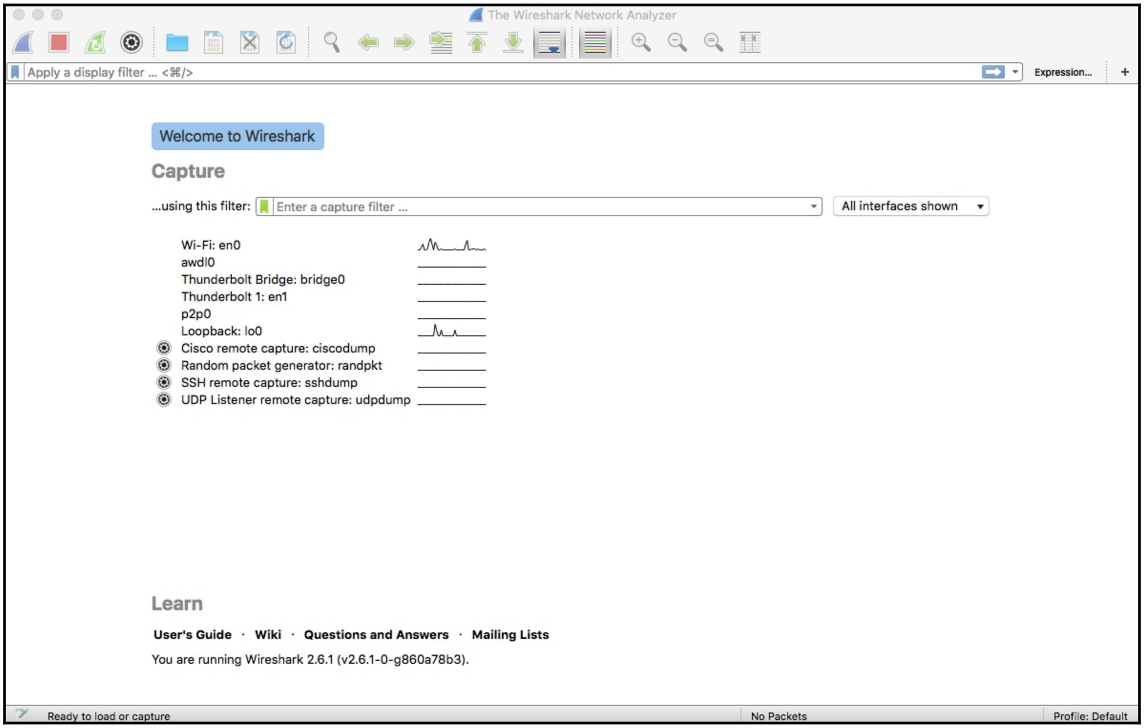
# Chapter 1: Installing Wireshark



The Wireshark Network Analyzer

Apply a display filter … <⌘/>

Expression… +

Welcome to Wireshark

Capture

...using this filter: Enter a capture filter … All interfaces shown

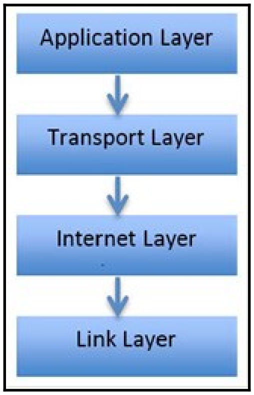
Wi-Fi: en0
awdl0
Thunderbolt Bridge: bridge0
Thunderbolt 1: en1
p2p0
Loopback: lo0
Cisco remote capture: ciscodump
Random packet generator: randpkt
SSH remote capture: sshdump
UDP Listener remote capture: udpdump

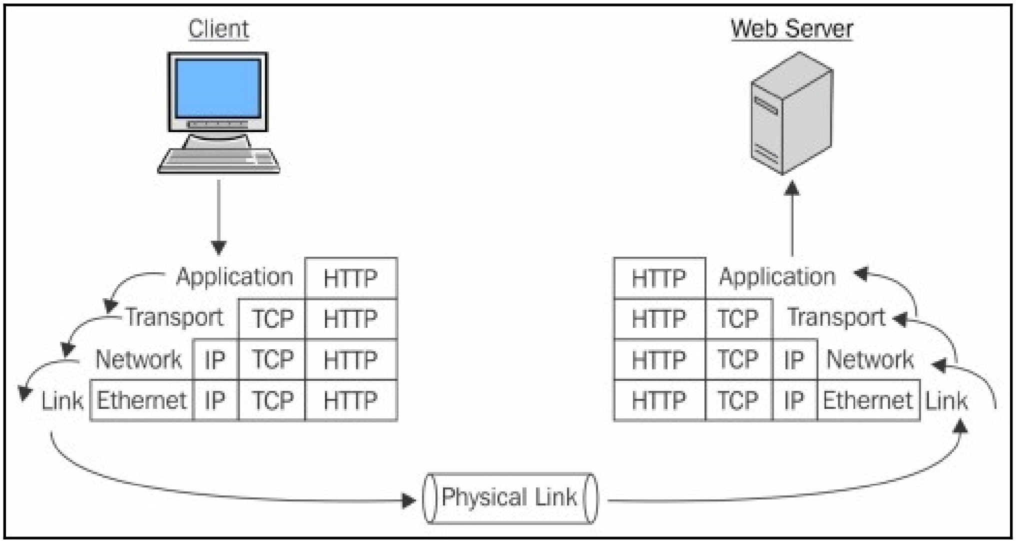
Learn

User's Guide · Wiki · Questions and Answers · Mailing Lists

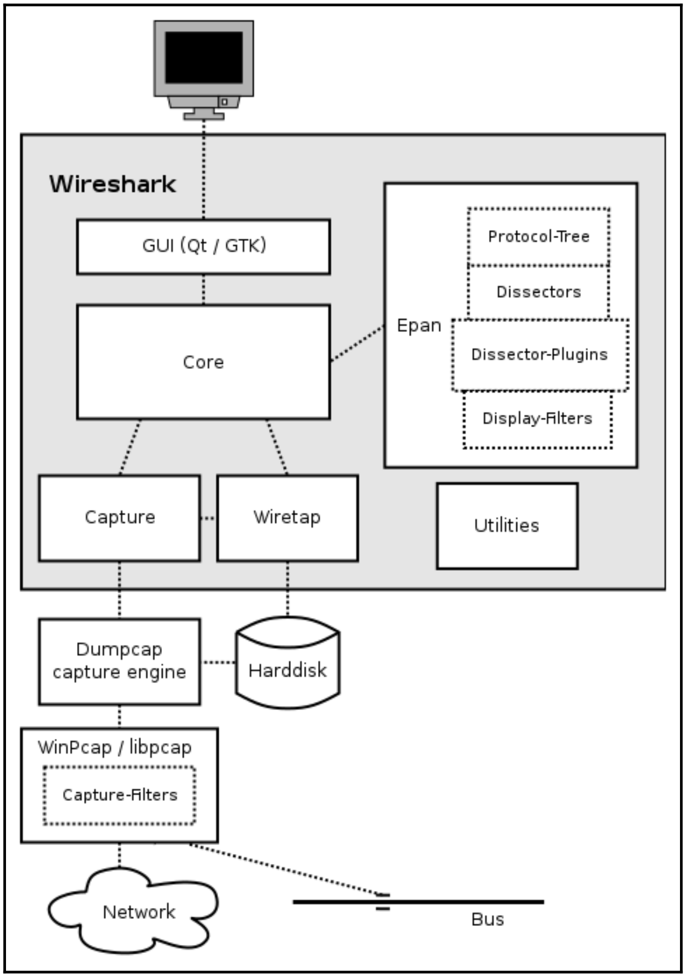
You are running Wireshark 2.6.1 (v2.6.1-0-g860a78b3).

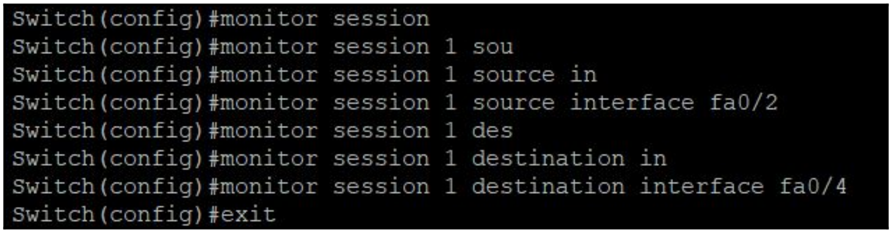
Ready to load or capture | No Packets | Profile: Default



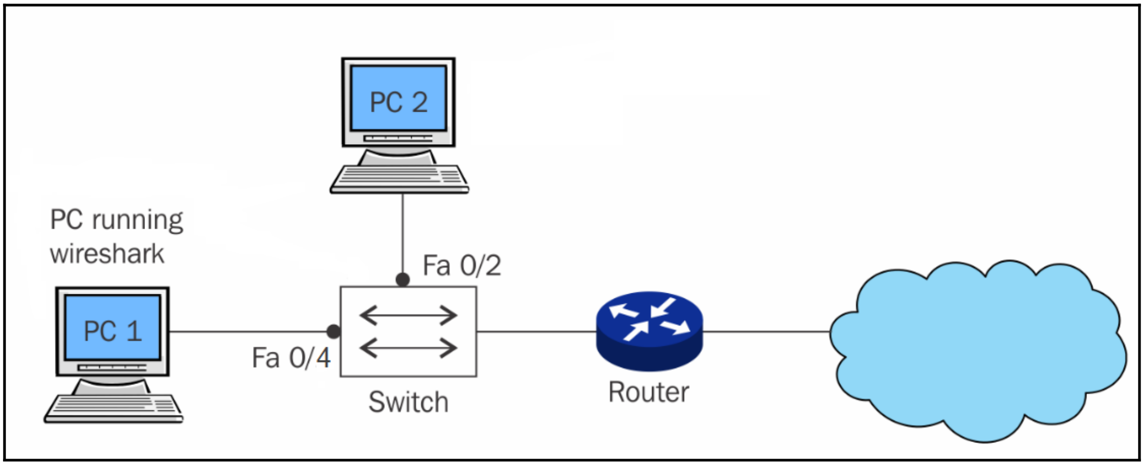

Client
Web Server
Application
HTTP
Transport
TCP
HTTP
Network
IP
TCP
HTTP
Link
Ethernet
IP
TCP
HTTP
HTTP
Application
HTTP
TCP
Transport
HTTP
TCP
IP
Network
HTTP
TCP
IP
Ethernet
Link
Physical Link

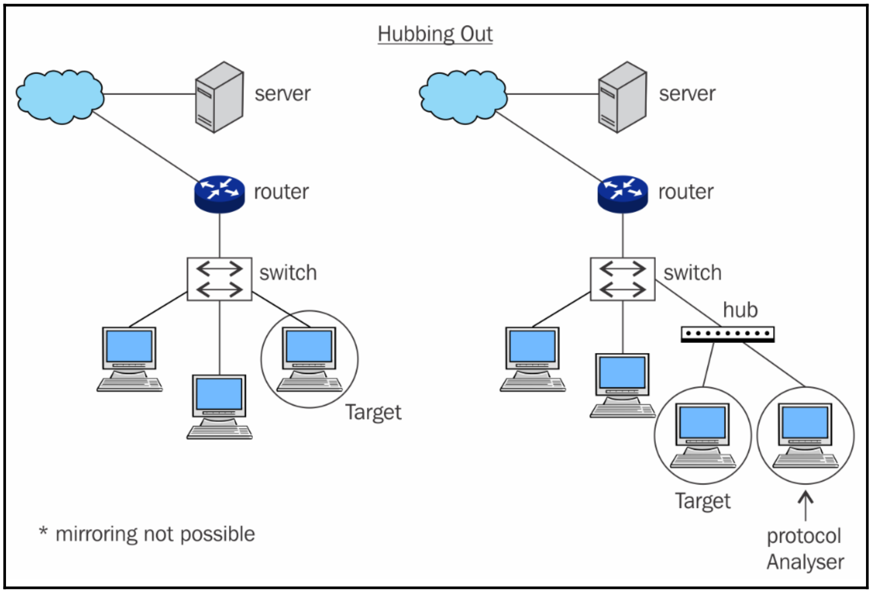
# Chapter 2:
# Introduction to Wireshark and Packet Analys is

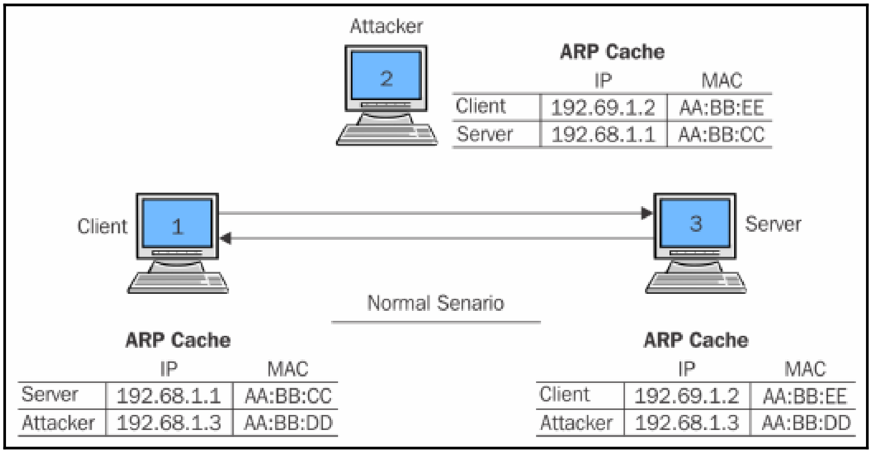




```
Switch(config)#monitor session
Switch(config)#monitor session 1 sou
Switch(config)#monitor session 1 source in
Switch(config)#monitor session 1 source interface fa0/2
Switch(config)#monitor session 1 des
Switch(config)#monitor session 1 destination in
Switch(config)#monitor session 1 destination interface fa0/4
Switch(config)#exit
```







**ARP Cache**

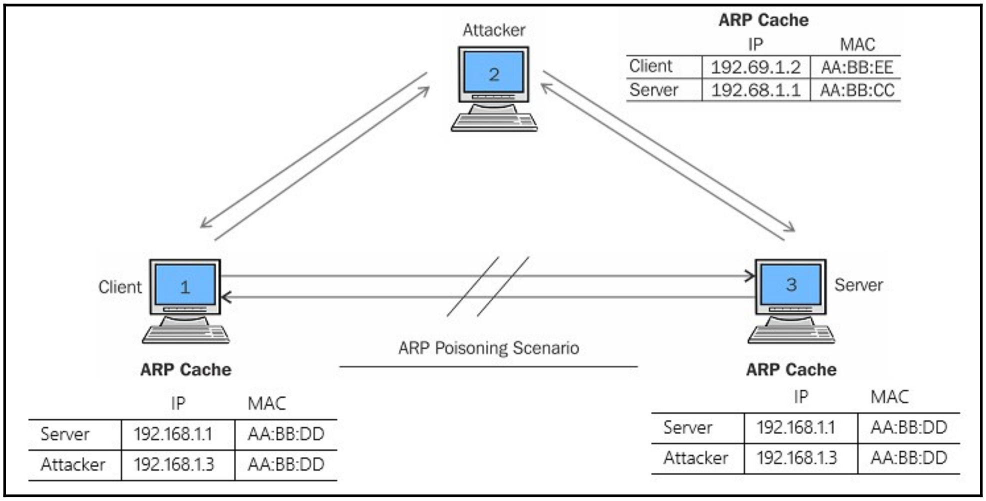
| | IP | MAC |
|---|---|---|
| Client | 192.69.1.2 | AA:BB:EE |
| Server | 192.68.1.1 | AA:BB:CC |

**ARP Cache**

| | IP | MAC |
|---|---|---|
| Server | 192.68.1.1 | AA:BB:CC |
| Attacker | 192.68.1.3 | AA:BB:DD |

**ARP Cache**

| | IP | MAC |
|---|---|---|
| Client | 192.69.1.2 | AA:BB:EE |
| Attacker | 192.68.1.3 | AA:BB:DD |



**ARP Cache**

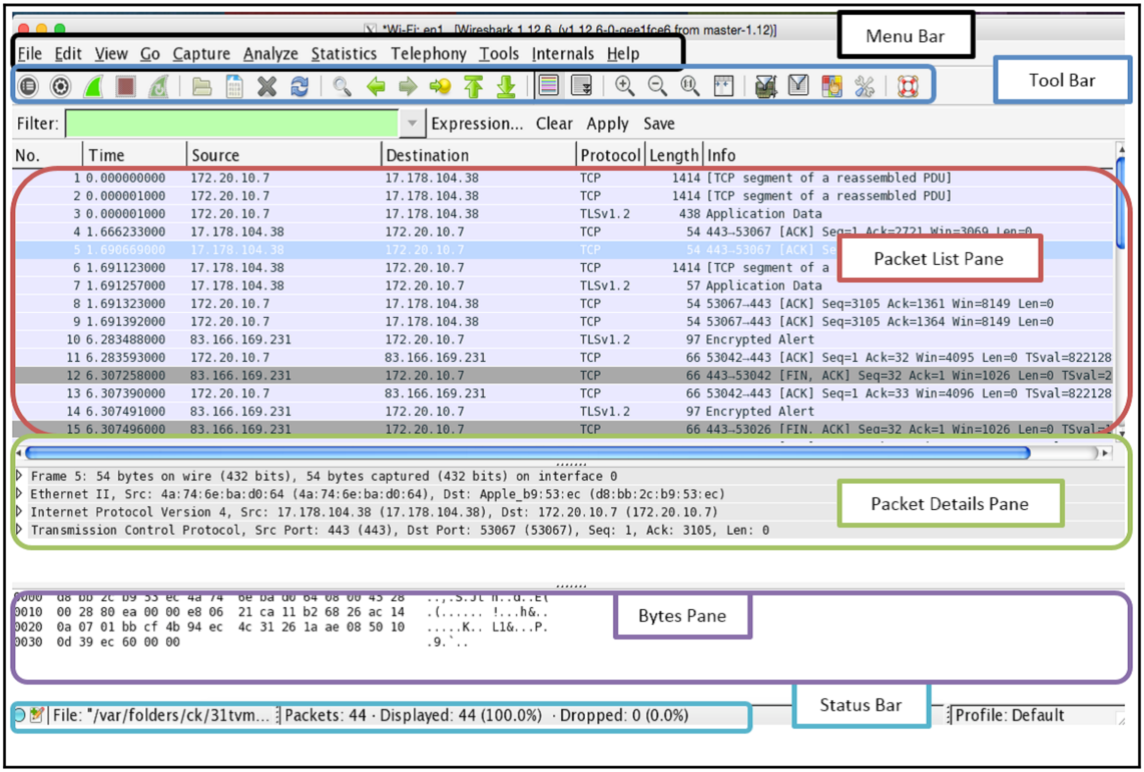
| | IP | MAC |
|---|---|---|
| Client | 192.69.1.2 | AA:BB:EE |
| Server | 192.68.1.1 | AA:BB:CC |

**ARP Cache**

| | IP | MAC |
|---|---|---|
| Server | 192.168.1.1 | AA:BB:DD |
| Attacker | 192.168.1.3 | AA:BB:DD |

**ARP Cache**

| | IP | MAC |
|---|---|---|
| Server | 192.168.1.1 | AA:BB:DD |
| Attacker | 192.168.1.3 | AA:BB:DD |

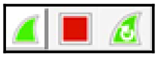

*Wi-Fi: en1 [Wireshark 1.12.6 (v1.12.6-0-gee1fce6 from master-1.12)]
Menu Bar
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Tool Bar
Filter:
Expression... Clear Apply Save
Packet List Pane
Packet Details Pane
Bytes Pane
Status Bar

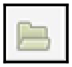
```
No.    Time          Source          Destination     Protocol Length Info
     1 0.000000000   172.20.10.7     17.178.104.38   TCP      1414 [TCP segment of a reassembled PDU]
     2 0.000001000   172.20.10.7     17.178.104.38   TCP      1414 [TCP segment of a reassembled PDU]
     3 0.000001000   172.20.10.7     17.178.104.38   TLSv1.2   438 Application Data
     4 1.666233000   17.178.104.38   172.20.10.7     TCP        54 443→53067 [ACK] Seq=1 Ack=2721 Win=3069 Len=0
     5 1.690669000   17.178.104.38   172.20.10.7     TCP        54 443→53067 [ACK] Se
     6 1.691123000   17.178.104.38   172.20.10.7     TCP      1414 [TCP segment of a
     7 1.691257000   17.178.104.38   172.20.10.7     TLSv1.2    57 Application Data
     8 1.691323000   172.20.10.7     17.178.104.38   TCP        54 53067→443 [ACK] Seq=3105 Ack=1361 Win=8149 Len=0
     9 1.691392000   172.20.10.7     17.178.104.38   TCP        54 53067→443 [ACK] Seq=3105 Ack=1364 Win=8149 Len=0
    10 6.283488000   83.166.169.231  172.20.10.7     TLSv1.2    97 Encrypted Alert
    11 6.283593000   172.20.10.7     83.166.169.231  TCP        66 53042→443 [ACK] Seq=1 Ack=32 Win=4095 Len=0 TSval=822128
    12 6.307258000   83.166.169.231  172.20.10.7     TCP        66 443→53042 [FIN, ACK] Seq=32 Ack=1 Win=1026 Len=0 TSval=2
    13 6.307390000   172.20.10.7     83.166.169.231  TCP        66 53042→443 [ACK] Seq=1 Ack=33 Win=4096 Len=0 TSval=822128
    14 6.307491000   83.166.169.231  172.20.10.7     TLSv1.2    97 Encrypted Alert
    15 6.307496000   83.166.169.231  172.20.10.7     TCP        66 443→53026 [FIN, ACK] Seq=32 Ack=1 Win=1026 Len=0 TSval=
```

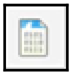
```
▷ Frame 5: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
▷ Ethernet II, Src: 4a:74:6e:ba:d0:64 (4a:74:6e:ba:d0:64), Dst: Apple_b9:53:ec (d8:bb:2c:b9:53:ec)
▷ Internet Protocol Version 4, Src: 17.178.104.38 (17.178.104.38), Dst: 172.20.10.7 (172.20.10.7)
▷ Transmission Control Protocol, Src Port: 443 (443), Dst Port: 53067 (53067), Seq: 1, Ack: 3105, Len: 0
```

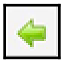
```
0000  d8 bb 2c b9 53 ec 4a 74  6e ba d0 64 08 00 45 28   ..,.S.Jt n..d..E(
0010  00 28 80 ea 00 00 e8 06  21 ca 11 b2 68 26 ac 14   .(...... !...h&..
0020  0a 07 01 bb cf 4b 94 ec  4c 31 26 1a ae 08 50 10   .....K.. L1&...P.
0030  0d 39 ec 60 00 00                                  .9.`..
```

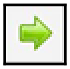
File: "/var/folders/ck/31tvm... Packets: 44 · Displayed: 44 (100.0%) · Dropped: 0 (0.0%) Profile: Default

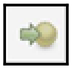


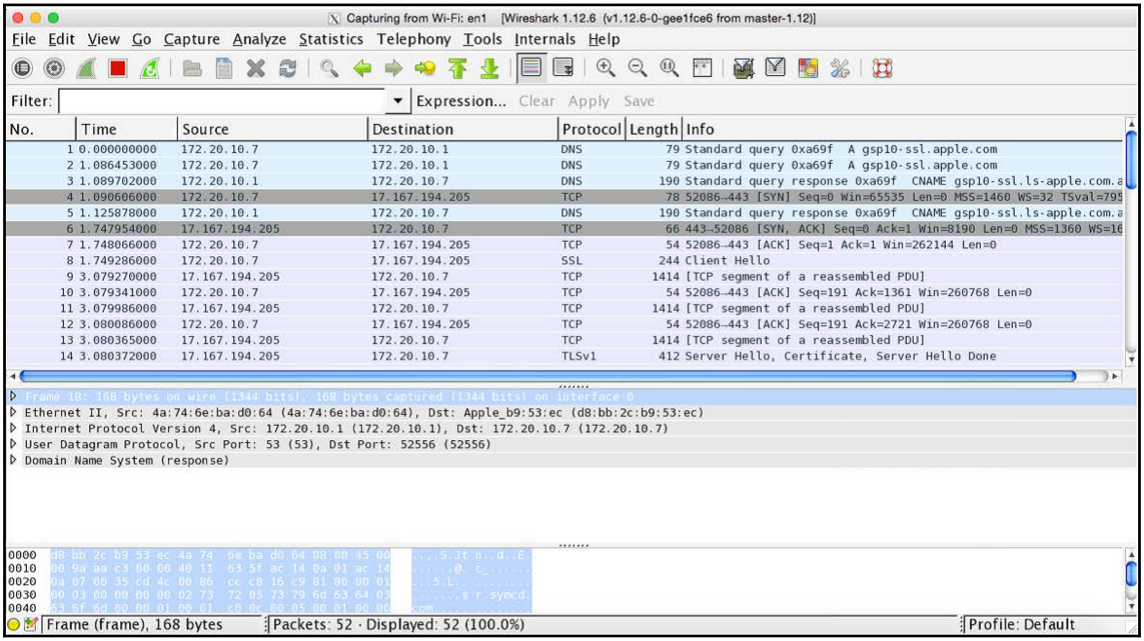










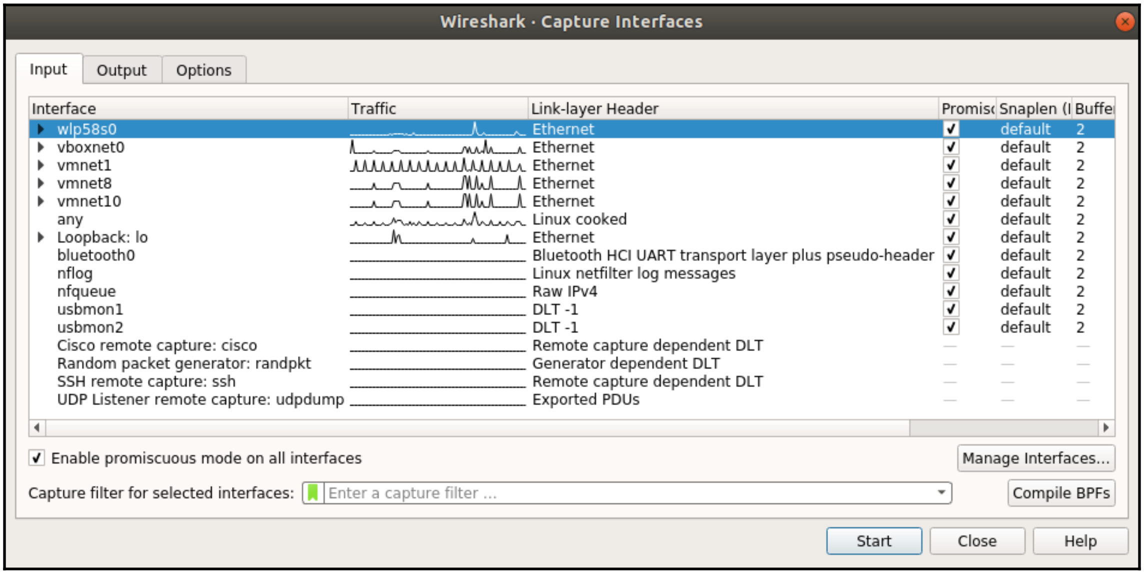


```
No.   Time         Source           Destination      Protocol Length Info
    1 0.000000000  172.20.10.7      172.20.10.1      DNS          79 Standard query 0xa69f  A gsp10-ssl.apple.com
    2 1.086453000  172.20.10.7      172.20.10.1      DNS          79 Standard query 0xa69f  A gsp10-ssl.apple.com
    3 1.089702000  172.20.10.1      172.20.10.7      DNS         190 Standard query response 0xa69f  CNAME gsp10-ssl.ls-apple.com.a
    4 1.090606000  172.20.10.7      17.167.194.205   TCP          78 52086→443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=795
    5 1.125878000  172.20.10.1      172.20.10.7      DNS         190 Standard query response 0xa69f  CNAME gsp10-ssl.ls-apple.com.a
    6 1.747954000  17.167.194.205   172.20.10.7      TCP          66 443→52086 [SYN, ACK] Seq=0 Ack=1 Win=8190 Len=0 MSS=1360 WS=16
    7 1.748066000  172.20.10.7      17.167.194.205   TCP          54 52086→443 [ACK] Seq=1 Ack=1 Win=262144 Len=0
    8 1.749286000  172.20.10.7      17.167.194.205   SSL         244 Client Hello
    9 3.079270000  17.167.194.205   172.20.10.7      TCP        1414 [TCP segment of a reassembled PDU]
   10 3.079341000  172.20.10.7      17.167.194.205   TCP          54 52086→443 [ACK] Seq=191 Ack=1361 Win=260768 Len=0
   11 3.079986000  17.167.194.205   172.20.10.7      TCP        1414 [TCP segment of a reassembled PDU]
   12 3.080086000  172.20.10.7      17.167.194.205   TCP          54 52086→443 [ACK] Seq=191 Ack=2721 Win=260768 Len=0
   13 3.080365000  17.167.194.205   172.20.10.7      TCP        1414 [TCP segment of a reassembled PDU]
   14 3.080372000  17.167.194.205   172.20.10.7      TLSv1       412 Server Hello, Certificate, Server Hello Done
```

```
▷ Frame 18: 168 bytes on wire (1344 bits), 168 bytes captured (1344 bits) on interface 0
▷ Ethernet II, Src: 4a:74:6e:ba:d0:64 (4a:74:6e:ba:d0:64), Dst: Apple_b9:53:ec (d8:bb:2c:b9:53:ec)
▷ Internet Protocol Version 4, Src: 172.20.10.1 (172.20.10.1), Dst: 172.20.10.7 (172.20.10.7)
▷ User Datagram Protocol, Src Port: 53 (53), Dst Port: 52556 (52556)
▷ Domain Name System (response)
```

```
0000  d8 bb 2c b9 53 ec 4a 74  6e ba d0 64 08 00 45 00   ....S.Jt n..d..E.
0010  00 9a aa c3 00 00 40 11  63 5f ac 14 0a 01 ac 14   ......@. c_......
0020  0a 07 00 35 cd 4c 00 86  cc c8 16 c9 81 80 00 01   ...5.L.. ........
0030  00 03 00 00 00 00 02 73  72 05 73 79 6d 63 64 03   .......s r.symcd.
0040  63 6f 6d 00 00 01 00 01  c0 0c 00 05 00 01 00 00   com..... ........
```

Frame (frame), 168 bytes | Packets: 52 · Displayed: 52 (100.0%) | Profile: Default

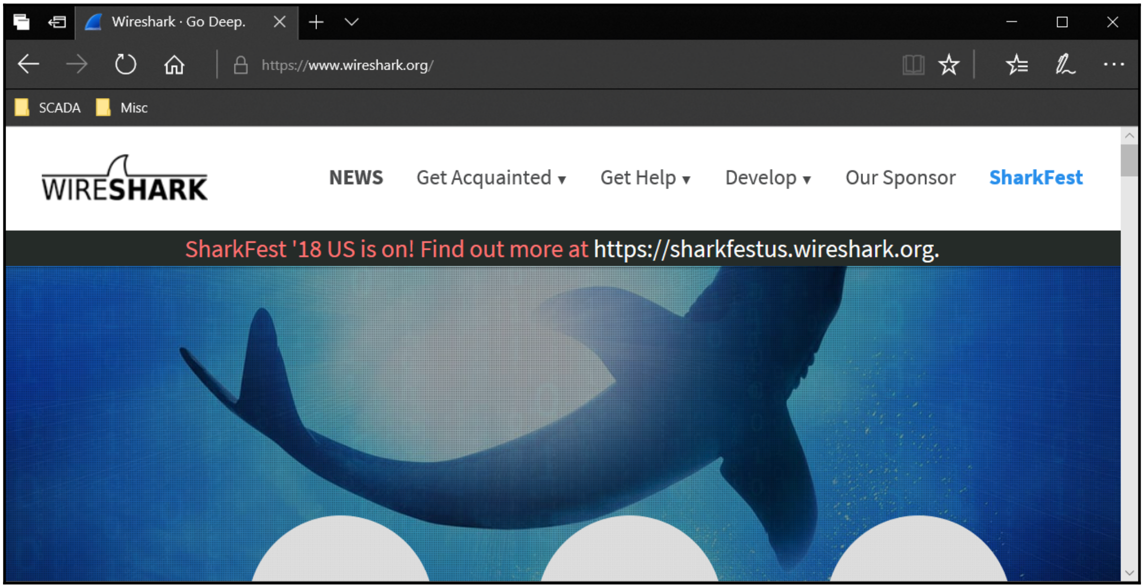


Wireshark · Capture Interfaces

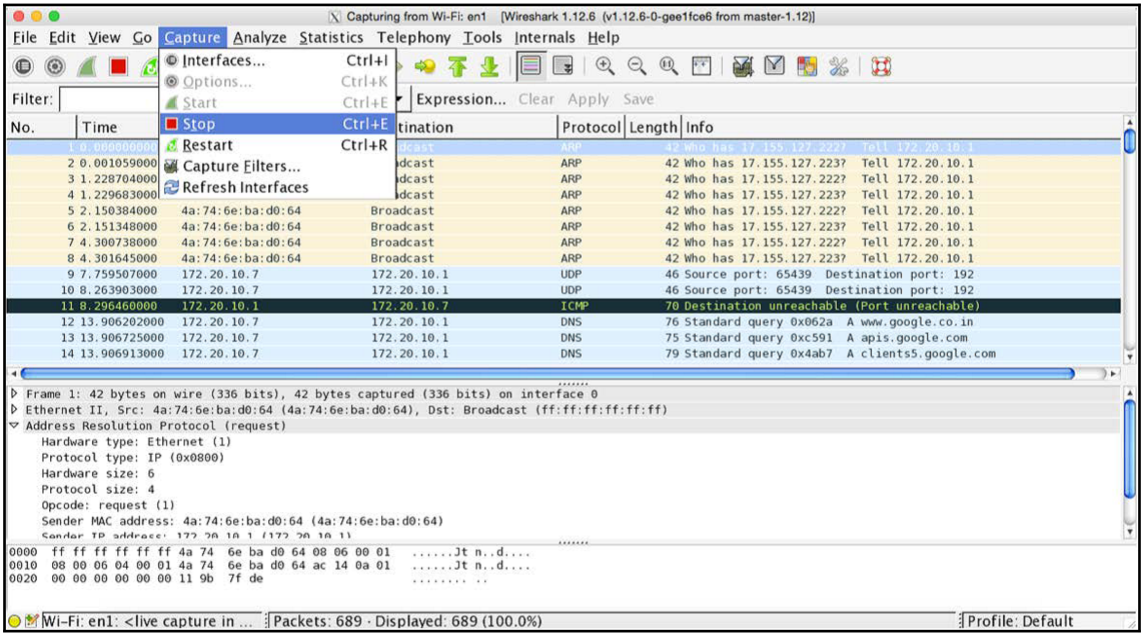
| Interface | Traffic | Link-layer Header | Promisc | Snaplen (I | Buffe |
|---|---|---|---|---|---|
| wlp58s0 | | Ethernet | ☑ | default | 2 |
| vboxnet0 | | Ethernet | ☑ | default | 2 |
| vmnet1 | | Ethernet | ☑ | default | 2 |
| vmnet8 | | Ethernet | ☑ | default | 2 |
| vmnet10 | | Ethernet | ☑ | default | 2 |
| any | | Linux cooked | ☑ | default | 2 |
| Loopback: lo | | Ethernet | ☑ | default | 2 |
| bluetooth0 | | Bluetooth HCI UART transport layer plus pseudo-header | ☑ | default | 2 |
| nflog | | Linux netfilter log messages | ☑ | default | 2 |
| nfqueue | | Raw IPv4 | ☑ | default | 2 |
| usbmon1 | | DLT -1 | ☑ | default | 2 |
| usbmon2 | | DLT -1 | ☑ | default | 2 |
| Cisco remote capture: cisco | | Remote capture dependent DLT | — | — | — |
| Random packet generator: randpkt | | Generator dependent DLT | — | — | — |
| SSH remote capture: ssh | | Remote capture dependent DLT | — | — | — |
| UDP Listener remote capture: udpdump | | Exported PDUs | — | — | — |

☑ Enable promiscuous mode on all interfaces

Capture filter for selected interfaces: Enter a capture filter …



SharkFest '18 US is on! Find out more at https://sharkfestus.wireshark.org.


Capturing from Wi-Fi: en1 [Wireshark 1.12.6 (v1.12.6-0-gee1fce6 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Interfaces... Ctrl+I
Options... Ctrl+K
Start Ctrl+E
Stop Ctrl+E
Restart Ctrl+R
Capture Filters...
Refresh Interfaces
Filter:
Expression... Clear Apply Save

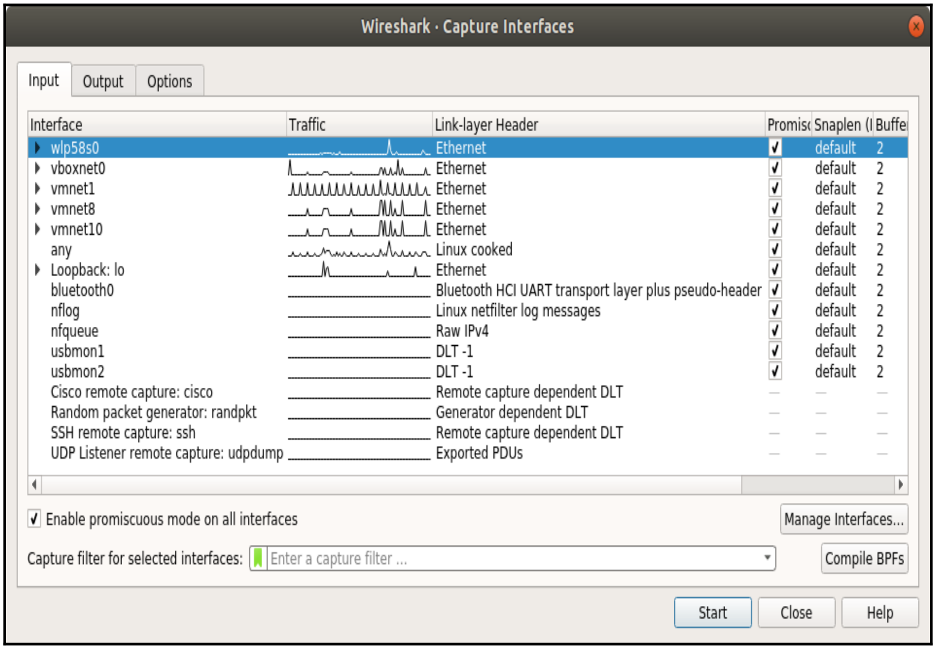
```
No.   Time          tination           Protocol Length Info
    1 0.000000000   dcast              ARP       42 Who has 17.155.127.222?  Tell 172.20.10.1
    2 0.001059000   dcast              ARP       42 Who has 17.155.127.223?  Tell 172.20.10.1
    3 1.228704000   dcast              ARP       42 Who has 17.155.127.222?  Tell 172.20.10.1
    4 1.229683000   dcast              ARP       42 Who has 17.155.127.223?  Tell 172.20.10.1
    5 2.150384000  4a:74:6e:ba:d0:64  Broadcast   ARP  42 Who has 17.155.127.222?  Tell 172.20.10.1
    6 2.151348000  4a:74:6e:ba:d0:64  Broadcast   ARP  42 Who has 17.155.127.223?  Tell 172.20.10.1
    7 4.300738000  4a:74:6e:ba:d0:64  Broadcast   ARP  42 Who has 17.155.127.222?  Tell 172.20.10.1
    8 4.301645000  4a:74:6e:ba:d0:64  Broadcast   ARP  42 Who has 17.155.127.223?  Tell 172.20.10.1
    9 7.759507000  172.20.10.7        172.20.10.1 UDP  46 Source port: 65439  Destination port: 192
   10 8.263903000  172.20.10.7        172.20.10.1 UDP  46 Source port: 65439  Destination port: 192
   11 8.296460000  172.20.10.1        172.20.10.7 ICMP 70 Destination unreachable (Port unreachable)
   12 13.906202000 172.20.10.7        172.20.10.1 DNS  76 Standard query 0x062a  A www.google.co.in
   13 13.906725000 172.20.10.7        172.20.10.1 DNS  75 Standard query 0xc591  A apis.google.com
   14 13.906913000 172.20.10.7        172.20.10.1 DNS  79 Standard query 0x4ab7  A clients5.google.com
```

```
▷ Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
▷ Ethernet II, Src: 4a:74:6e:ba:d0:64 (4a:74:6e:ba:d0:64), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▽ Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: 4a:74:6e:ba:d0:64 (4a:74:6e:ba:d0:64)
    Sender IP address: 172.20.10.1 (172.20.10.1)
```

```
0000  ff ff ff ff ff ff 4a 74  6e ba d0 64 08 06 00 01   ......Jt n..d....
0010  08 00 06 04 00 01 4a 74  6e ba d0 64 ac 14 0a 01   ......Jt n..d....
0020  00 00 00 00 00 00 11 9b  7f de                     ........ ..
```

Wi-Fi: en1: <live capture in ...
Packets: 689 · Displayed: 689 (100.0%)
Profile: Default

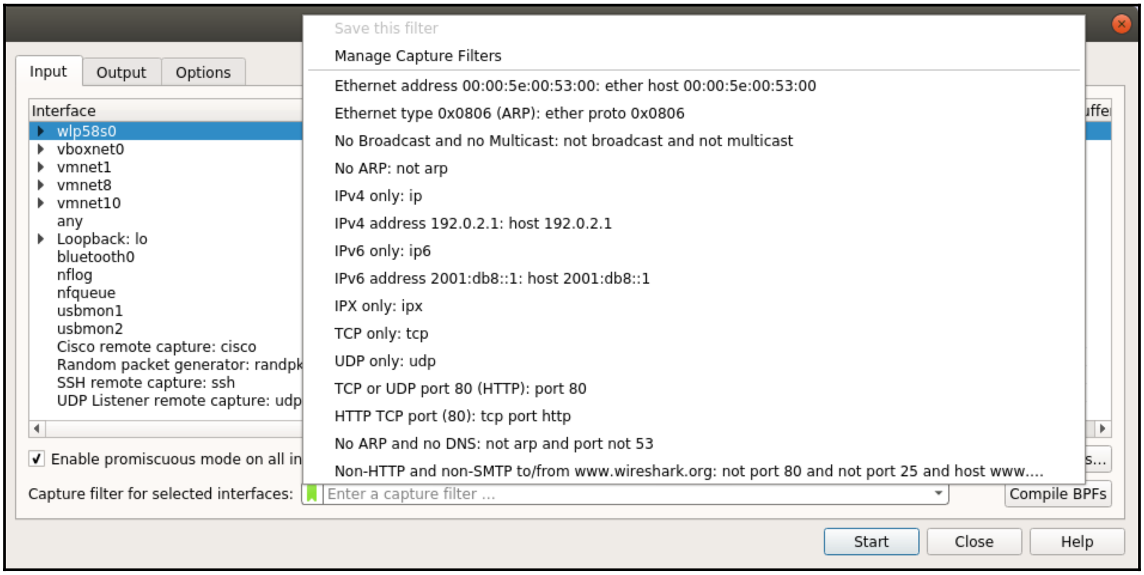
# Chapter 3: Filtering Our Way in Wireshark



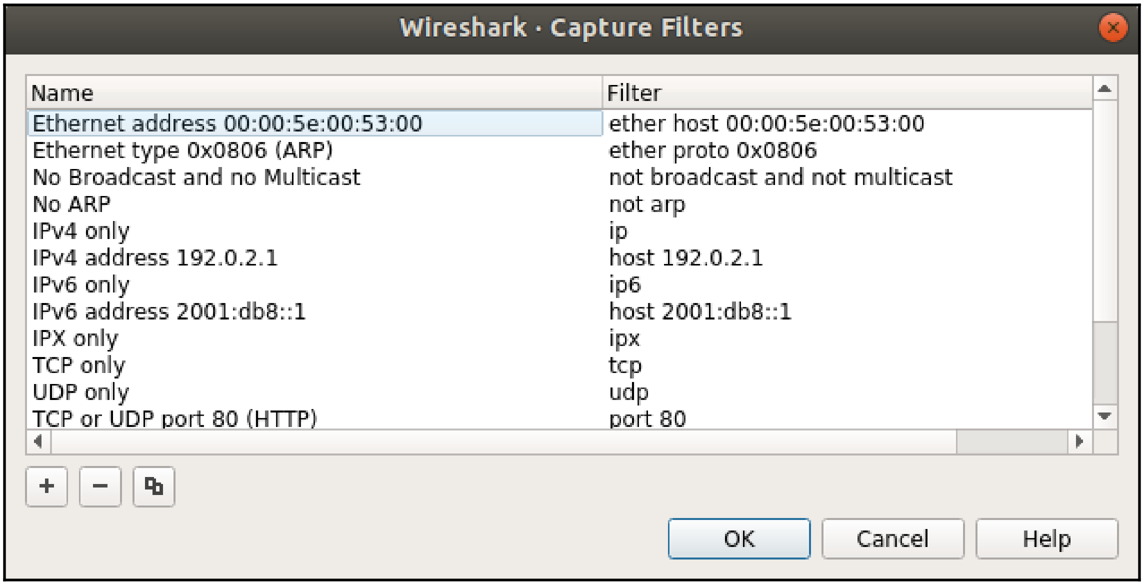
| Interface | Traffic | Link-layer Header | Promisc | Snaplen (I | Buffe |
|---|---|---|---|---|---|
| wlp58s0 | | Ethernet | ☑ | default | 2 |
| vboxnet0 | | Ethernet | ☑ | default | 2 |
| vmnet1 | | Ethernet | ☑ | default | 2 |
| vmnet8 | | Ethernet | ☑ | default | 2 |
| vmnet10 | | Ethernet | ☑ | default | 2 |
| any | | Linux cooked | ☑ | default | 2 |
| Loopback: lo | | Ethernet | ☑ | default | 2 |
| bluetooth0 | | Bluetooth HCI UART transport layer plus pseudo-header | ☑ | default | 2 |
| nflog | | Linux netfilter log messages | ☑ | default | 2 |
| nfqueue | | Raw IPv4 | ☑ | default | 2 |
| usbmon1 | | DLT -1 | ☑ | default | 2 |
| usbmon2 | | DLT -1 | ☑ | default | 2 |
| Cisco remote capture: cisco | | Remote capture dependent DLT | — | — | — |
| Random packet generator: randpkt | | Generator dependent DLT | — | — | — |
| SSH remote capture: ssh | | Remote capture dependent DLT | — | — | — |
| UDP Listener remote capture: udpdump | | Exported PDUs | — | — | — |

☑ Enable promiscuous mode on all interfaces

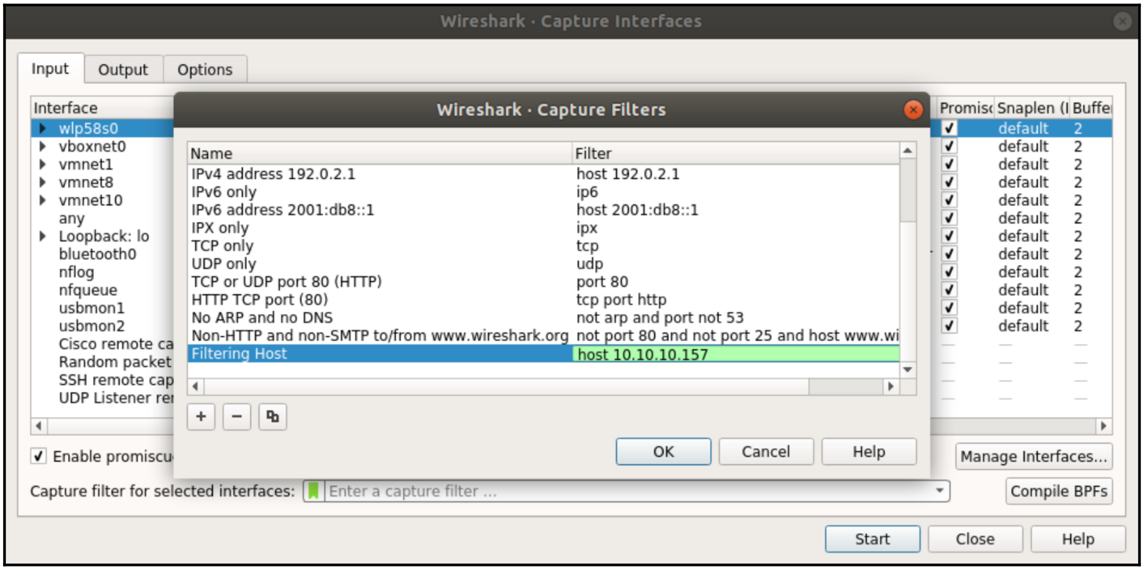
Capture filter for selected interfaces: Enter a capture filter ...


Input
Output
Options
Interface
wlp58s0
vboxnet0
vmnet1
vmnet8
vmnet10
any
Loopback: lo
bluetooth0
nflog
nfqueue
usbmon1
usbmon2
Cisco remote capture: cisco
Random packet generator: randpk
SSH remote capture: ssh
UDP Listener remote capture: udp
☑ Enable promiscuous mode on all in
Capture filter for selected interfaces: Enter a capture filter ...
Compile BPFs
Start
Close
Help

Save this filter
Manage Capture Filters
Ethernet address 00:00:5e:00:53:00: ether host 00:00:5e:00:53:00
Ethernet type 0x0806 (ARP): ether proto 0x0806
No Broadcast and no Multicast: not broadcast and not multicast
No ARP: not arp
IPv4 only: ip
IPv4 address 192.0.2.1: host 192.0.2.1
IPv6 only: ip6
IPv6 address 2001:db8::1: host 2001:db8::1
IPX only: ipx
TCP only: tcp
UDP only: udp
TCP or UDP port 80 (HTTP): port 80
HTTP TCP port (80): tcp port http
No ARP and no DNS: not arp and port not 53
Non-HTTP and non-SMTP to/from www.wireshark.org: not port 80 and not port 25 and host www....



| Name | Filter |
|---|---|
| Ethernet address 00:00:5e:00:53:00 | ether host 00:00:5e:00:53:00 |
| Ethernet type 0x0806 (ARP) | ether proto 0x0806 |
| No Broadcast and no Multicast | not broadcast and not multicast |
| No ARP | not arp |
| IPv4 only | ip |
| IPv4 address 192.0.2.1 | host 192.0.2.1 |
| IPv6 only | ip6 |
| IPv6 address 2001:db8::1 | host 2001:db8::1 |
| IPX only | ipx |
| TCP only | tcp |
| UDP only | udp |
| TCP or UDP port 80 (HTTP) | port 80 |

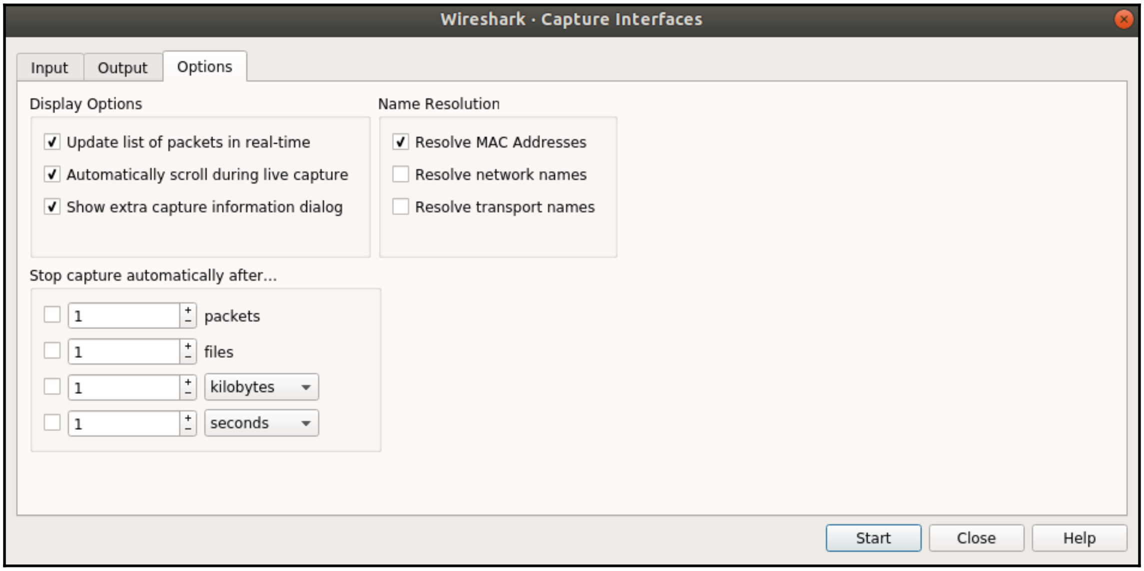

Wireshark · Capture Interfaces
Input
Output
Options
Wireshark · Capture Filters
+
−
OK
Cancel
Help
Manage Interfaces...
Compile BPFs
Enter a capture filter ...
Start
Close
Help

| Interface | Promisc | Snaplen (I | Buffer |
|---|---|---|---|
| wlp58s0 | ✓ | default | 2 |
| vboxnet0 | ✓ | default | 2 |
| vmnet1 | ✓ | default | 2 |
| vmnet8 | ✓ | default | 2 |
| vmnet10 | ✓ | default | 2 |
| any | ✓ | default | 2 |
| Loopback: lo | ✓ | default | 2 |
| bluetooth0 | ✓ | default | 2 |
| nflog | ✓ | default | 2 |
| nfqueue | ✓ | default | 2 |
| usbmon1 | ✓ | default | 2 |
| usbmon2 | ✓ | default | 2 |
| Cisco remote ca | — | — | — |
| Random packet | — | — | — |
| SSH remote cap | — | — | — |
| UDP Listener re | — | — | — |

| Name | Filter |
|---|---|
| IPv4 address 192.0.2.1 | host 192.0.2.1 |
| IPv6 only | ip6 |
| IPv6 address 2001:db8::1 | host 2001:db8::1 |
| IPX only | ipx |
| TCP only | tcp |
| UDP only | udp |
| TCP or UDP port 80 (HTTP) | port 80 |
| HTTP TCP port (80) | tcp port http |
| No ARP and no DNS | not arp and port not 53 |
| Non-HTTP and non-SMTP to/from www.wireshark.org | not port 80 and not port 25 and host www.wi |
| Filtering Host | host 10.10.10.157 |

☑ Enable promiscu

Capture filter for selected interfaces:



Wireshark · Capture Interfaces

Display Options

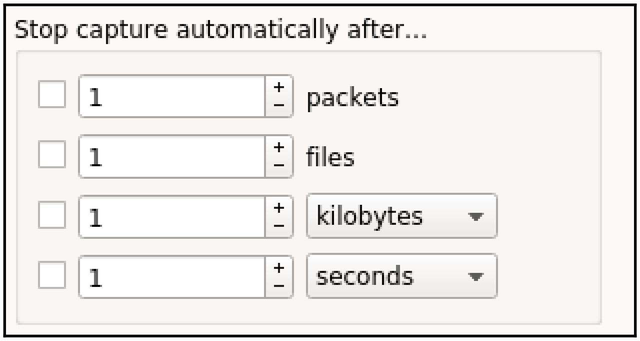
- ☑ Update list of packets in real-time
- ☑ Automatically scroll during live capture
- ☑ Show extra capture information dialog

Name Resolution

- ☑ Resolve MAC Addresses
- □ Resolve network names
- □ Resolve transport names

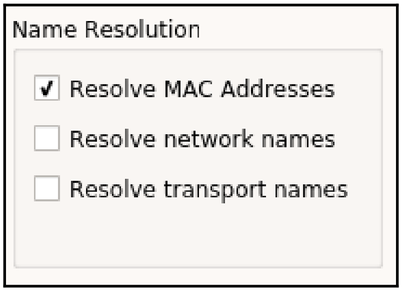
Stop capture automatically after...

- □ 1 packets
- □ 1 files
- □ 1 kilobytes
- □ 1 seconds



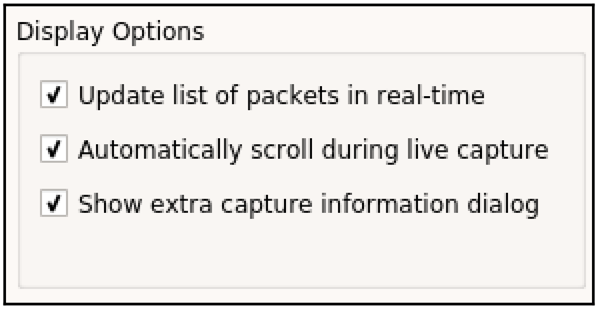
Stop capture automatically after...

- □ 1 packets
- □ 1 files
- □ 1 kilobytes
- □ 1 seconds



Name Resolution

- ☑ Resolve MAC Addresses
- □ Resolve network names
- □ Resolve transport names

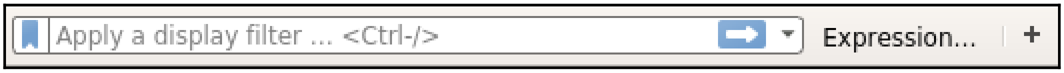


Display Options

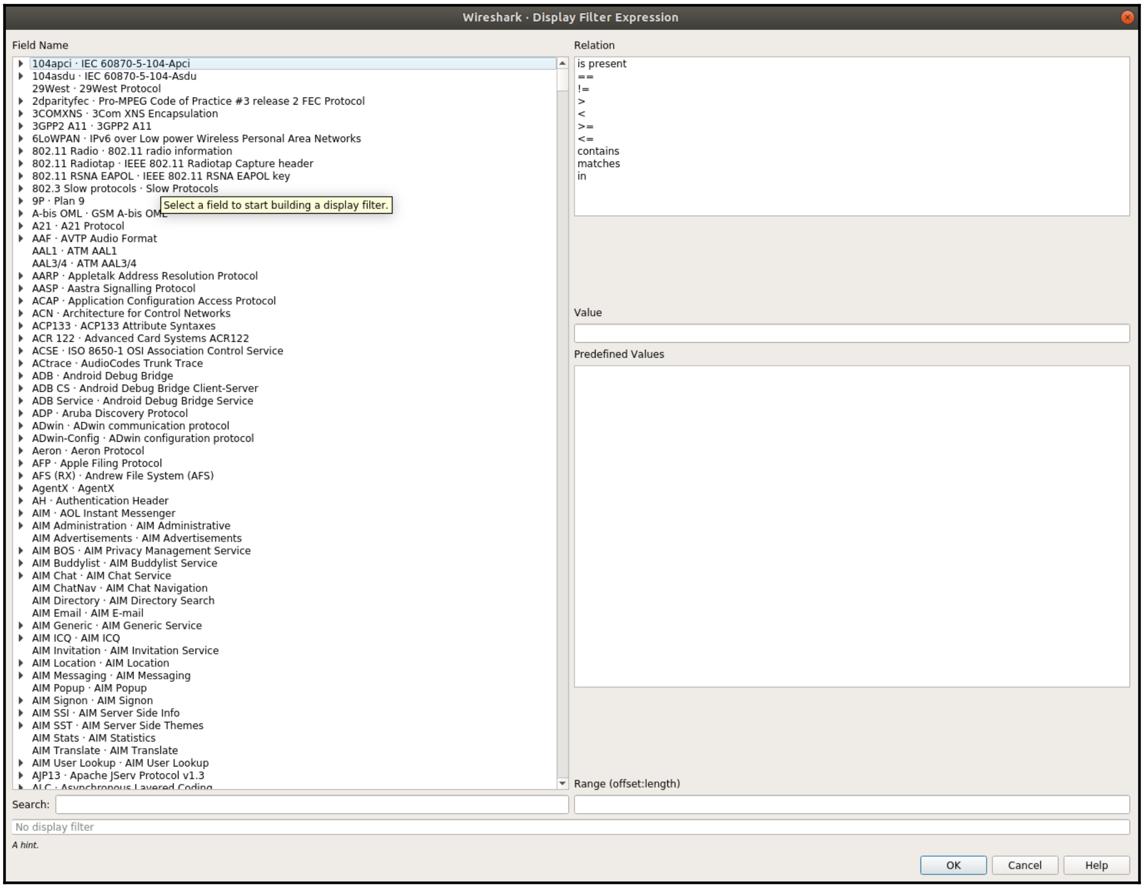
☑ Update list of packets in real-time

☑ Automatically scroll during live capture

☑ Show extra capture information dialog



Apply a display filter … <Ctrl-/>



Wireshark · Display Filter Expression

Field Name

104apci · IEC 60870-5-104-Apci
104asdu · IEC 60870-5-104-Asdu
29West · 29West Protocol
2dparityfec · Pro-MPEG Code of Practice #3 release 2 FEC Protocol
3COMXNS · 3Com XNS Encapsulation
3GPP2 A11 · 3GPP2 A11
6LoWPAN · IPv6 over Low power Wireless Personal Area Networks
802.11 Radio · 802.11 radio information
802.11 Radiotap · IEEE 802.11 Radiotap Capture header
802.11 RSNA EAPOL · IEEE 802.11 RSNA EAPOL key
802.3 Slow protocols · Slow Protocols
9P · Plan 9
A-bis OML · GSM A-bis OML
A21 · A21 Protocol
AAF · AVTP Audio Format
AAL1 · ATM AAL1
AAL3/4 · ATM AAL3/4
AARP · Appletalk Address Resolution Protocol
AASP · Aastra Signalling Protocol
ACAP · Application Configuration Access Protocol
ACN · Architecture for Control Networks
ACP133 · ACP133 Attribute Syntaxes
ACR 122 · Advanced Card Systems ACR122
ACSE · ISO 8650-1 OSI Association Control Service
ACtrace · AudioCodes Trunk Trace
ADB · Android Debug Bridge
ADB CS · Android Debug Bridge Client-Server
ADB Service · Android Debug Bridge Service
ADP · Aruba Discovery Protocol
ADwin · ADwin communication protocol
ADwin-Config · ADwin configuration protocol
Aeron · Aeron Protocol
AFP · Apple Filing Protocol
AFS (RX) · Andrew File System (AFS)
AgentX · AgentX
AH · Authentication Header
AIM · AOL Instant Messenger
AIM Administration · AIM Administrative
AIM Advertisements · AIM Advertisements
AIM BOS · AIM Privacy Management Service
AIM Buddylist · AIM Buddylist Service
AIM Chat · AIM Chat Service
AIM ChatNav · AIM Chat Navigation
AIM Directory · AIM Directory Search
AIM Email · AIM E-mail
AIM Generic · AIM Generic Service
AIM ICQ · AIM ICQ
AIM Invitation · AIM Invitation Service
AIM Location · AIM Location
AIM Messaging · AIM Messaging
AIM Popup · AIM Popup
AIM Signon · AIM Signon
AIM SSI · AIM Server Side Info
AIM SST · AIM Server Side Themes
AIM Stats · AIM Statistics
AIM Translate · AIM Translate
AIM User Lookup · AIM User Lookup
AJP13 · Apache JServ Protocol v1.3
ALC · Asynchronous Layered Coding

Select a field to start building a display filter.

Relation

is present
==
!=
>
<
>=
<=
contains
matches
in

Value

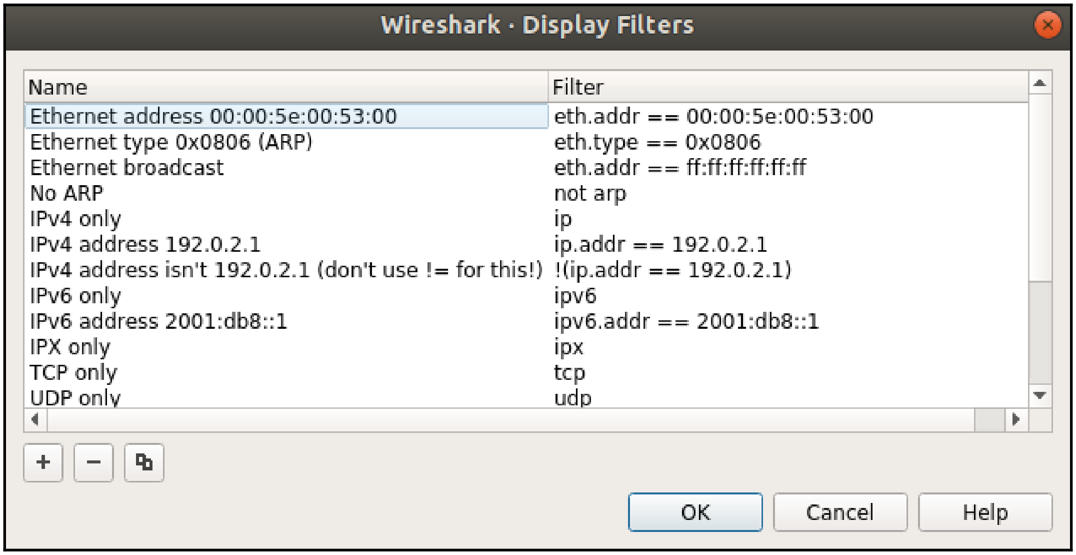
Predefined Values

Range (offset:length)

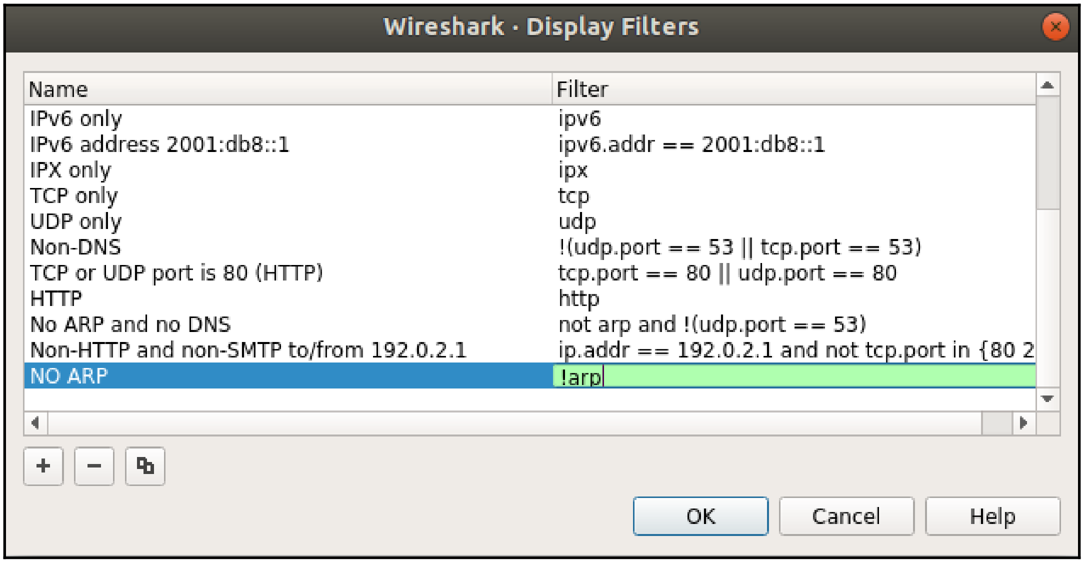
Search:

No display filter

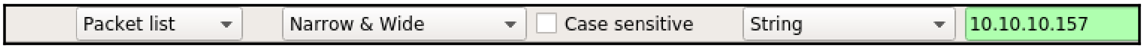
*A hint.*



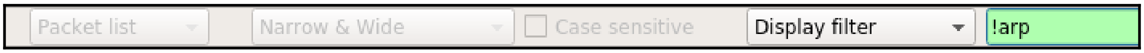
| Name | Filter |
|---|---|
| Ethernet address 00:00:5e:00:53:00 | eth.addr == 00:00:5e:00:53:00 |
| Ethernet type 0x0806 (ARP) | eth.type == 0x0806 |
| Ethernet broadcast | eth.addr == ff:ff:ff:ff:ff:ff |
| No ARP | not arp |
| IPv4 only | ip |
| IPv4 address 192.0.2.1 | ip.addr == 192.0.2.1 |
| IPv4 address isn't 192.0.2.1 (don't use != for this!) | !(ip.addr == 192.0.2.1) |
| IPv6 only | ipv6 |
| IPv6 address 2001:db8::1 | ipv6.addr == 2001:db8::1 |
| IPX only | ipx |
| TCP only | tcp |
| UDP only | udp |



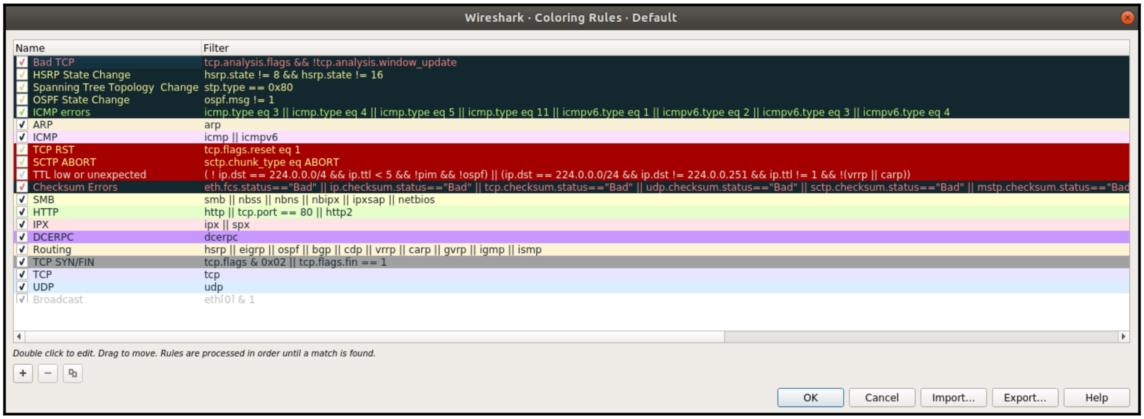
| Name | Filter |
|---|---|
| IPv6 only | ipv6 |
| IPv6 address 2001:db8::1 | ipv6.addr == 2001:db8::1 |
| IPX only | ipx |
| TCP only | tcp |
| UDP only | udp |
| Non-DNS | !(udp.port == 53 \|\| tcp.port == 53) |
| TCP or UDP port is 80 (HTTP) | tcp.port == 80 \|\| udp.port == 80 |
| HTTP | http |
| No ARP and no DNS | not arp and !(udp.port == 53) |
| Non-HTTP and non-SMTP to/from 192.0.2.1 | ip.addr == 192.0.2.1 and not tcp.port in {80 2 |
| NO ARP | !arp |



Packet list | Narrow & Wide | □ Case sensitive | String | 10.10.10.157



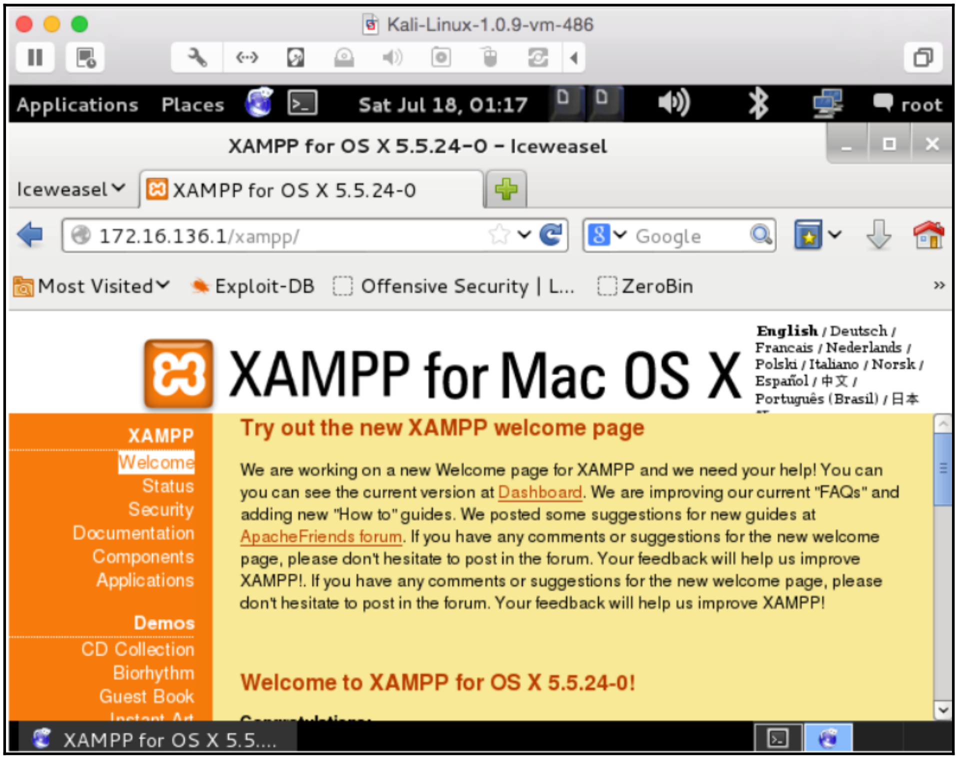
Packet list | Narrow & Wide | □ Case sensitive | Display filter | !arp



Wireshark · Coloring Rules · Default

<table>
<tr><th>Name</th><th>Filter</th></tr>
<tr><td>☑ Bad TCP</td><td>tcp.analysis.flags && !tcp.analysis.window_update</td></tr>
<tr><td>☑ HSRP State Change</td><td>hsrp.state != 8 && hsrp.state != 16</td></tr>
<tr><td>☑ Spanning Tree Topology  Change</td><td>stp.type == 0x80</td></tr>
<tr><td>☑ OSPF State Change</td><td>ospf.msg != 1</td></tr>
<tr><td>☑ ICMP errors</td><td>icmp.type eq 3 || icmp.type eq 4 || icmp.type eq 5 || icmp.type eq 11 || icmpv6.type eq 1 || icmpv6.type eq 2 || icmpv6.type eq 3 || icmpv6.type eq 4</td></tr>
<tr><td>☑ ARP</td><td>arp</td></tr>
<tr><td>☑ ICMP</td><td>icmp || icmpv6</td></tr>
<tr><td>☑ TCP RST</td><td>tcp.flags.reset eq 1</td></tr>
<tr><td>☑ SCTP ABORT</td><td>sctp.chunk_type eq ABORT</td></tr>
<tr><td>☑ TTL low or unexpected</td><td>( ! ip.dst == 224.0.0.0/4 && ip.ttl < 5 && !pim && !ospf) || (ip.dst == 224.0.0.0/24 && ip.dst != 224.0.0.251 && ip.ttl != 1 && !(vrrp || carp))</td></tr>
<tr><td>☑ Checksum Errors</td><td>eth.fcs.status=="Bad" || ip.checksum.status=="Bad" || tcp.checksum.status=="Bad" || udp.checksum.status=="Bad" || sctp.checksum.status=="Bad" || mstp.checksum.status=="Bad</td></tr>
<tr><td>☑ SMB</td><td>smb || nbss || nbns || nbipx || ipxsap || netbios</td></tr>
<tr><td>☑ HTTP</td><td>http || tcp.port == 80 || http2</td></tr>
<tr><td>☑ IPX</td><td>ipx || spx</td></tr>
<tr><td>☑ DCERPC</td><td>dcerpc</td></tr>
<tr><td>☑ Routing</td><td>hsrp || eigrp || ospf || bgp || cdp || vrrp || carp || gvrp || igmp || ismp</td></tr>
<tr><td>☑ TCP SYN/FIN</td><td>tcp.flags & 0x02 || tcp.flags.fin == 1</td></tr>
<tr><td>☑ TCP</td><td>tcp</td></tr>
<tr><td>☑ UDP</td><td>udp</td></tr>
<tr><td>☑ Broadcast</td><td>eth[0] & 1</td></tr>
</table>

*Double click to edit. Drag to move. Rules are processed in order until a match is found.*



XAMPP for Mac OS X

English / Deutsch / Francais / Nederlands / Polski / Italiano / Norsk / Español / 中文 / Português (Brasil) / 日本

XAMPP
Welcome
Status
Security
Documentation
Components
Applications

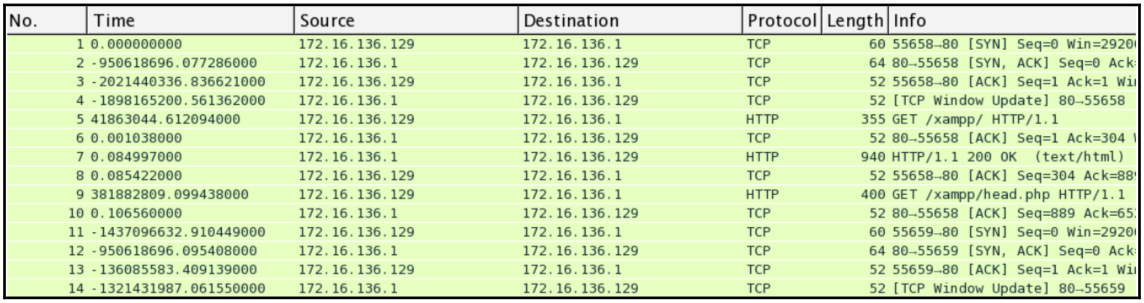
Demos
CD Collection
Biorhythm
Guest Book
Instant Art

Try out the new XAMPP welcome page

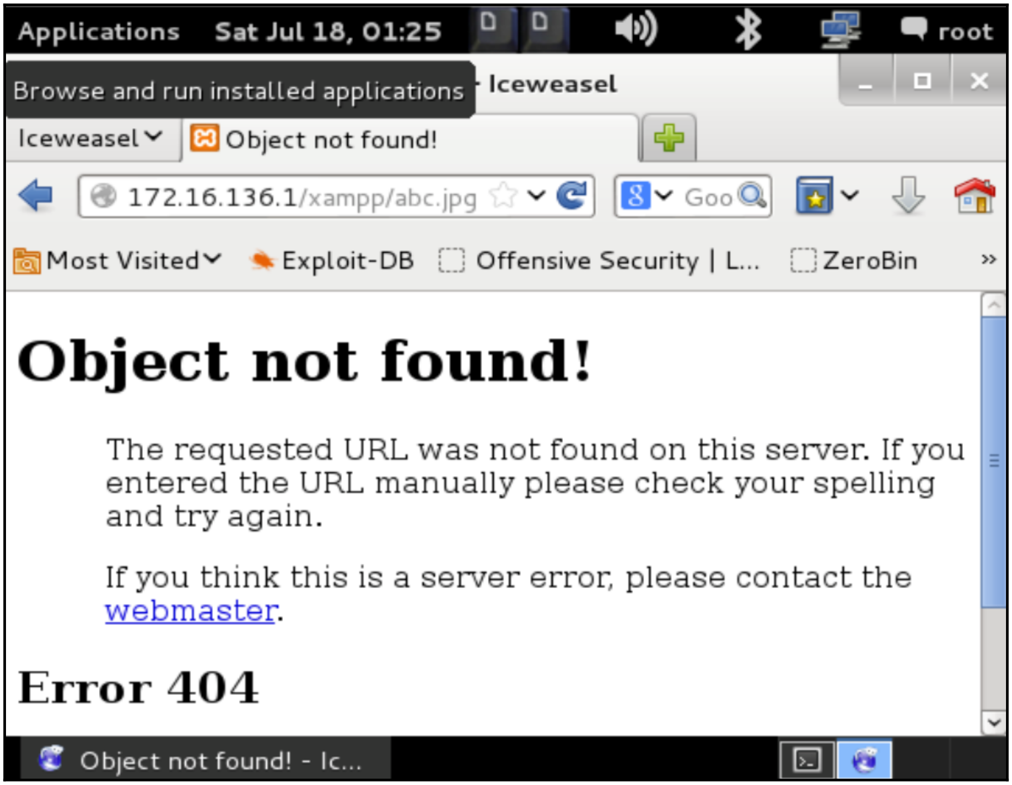
We are working on a new Welcome page for XAMPP and we need your help! You can you can see the current version at Dashboard. We are improving our current "FAQs" and adding new "How to" guides. We posted some suggestions for new guides at ApacheFriends forum. If you have any comments or suggestions for the new welcome page, please don't hesitate to post in the forum. Your feedback will help us improve XAMPP!. If you have any comments or suggestions for the new welcome page, please don't hesitate to post in the forum. Your feedback will help us improve XAMPP!

Welcome to XAMPP for OS X 5.5.24-0!

Congratulations:



| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 1 | 0.000000000 | 172.16.136.129 | 172.16.136.1 | TCP | 60 | 55658→80 [SYN] Seq=0 Win=2920 |
| 2 | -950618696.077286000 | 172.16.136.1 | 172.16.136.129 | TCP | 64 | 80→55658 [SYN, ACK] Seq=0 Ack |
| 3 | -2021440336.836621000 | 172.16.136.129 | 172.16.136.1 | TCP | 52 | 55658→80 [ACK] Seq=1 Ack=1 Wi |
| 4 | -1898165200.561362000 | 172.16.136.1 | 172.16.136.129 | TCP | 52 | [TCP Window Update] 80→55658 |
| 5 | 41863044.612094000 | 172.16.136.129 | 172.16.136.1 | HTTP | 355 | GET /xampp/ HTTP/1.1 |
| 6 | 0.001038000 | 172.16.136.1 | 172.16.136.129 | TCP | 52 | 80→55658 [ACK] Seq=1 Ack=304 |
| 7 | 0.084997000 | 172.16.136.1 | 172.16.136.129 | HTTP | 940 | HTTP/1.1 200 OK (text/html) |
| 8 | 0.085422000 | 172.16.136.129 | 172.16.136.1 | TCP | 52 | 55658→80 [ACK] Seq=304 Ack=88 |
| 9 | 381882809.099438000 | 172.16.136.129 | 172.16.136.1 | HTTP | 400 | GET /xampp/head.php HTTP/1.1 |
| 10 | 0.106560000 | 172.16.136.1 | 172.16.136.129 | TCP | 52 | 80→55658 [ACK] Seq=889 Ack=65 |
| 11 | -1437096632.910449000 | 172.16.136.129 | 172.16.136.1 | TCP | 60 | 55659→80 [SYN] Seq=0 Win=2920 |
| 12 | -950618696.095408000 | 172.16.136.1 | 172.16.136.129 | TCP | 64 | 80→55659 [SYN, ACK] Seq=0 Ack |
| 13 | -136085583.409139000 | 172.16.136.129 | 172.16.136.1 | TCP | 52 | 55659→80 [ACK] Seq=1 Ack=1 Wi |
| 14 | -1321431987.061550000 | 172.16.136.1 | 172.16.136.129 | TCP | 52 | [TCP Window Update] 80→55659 |



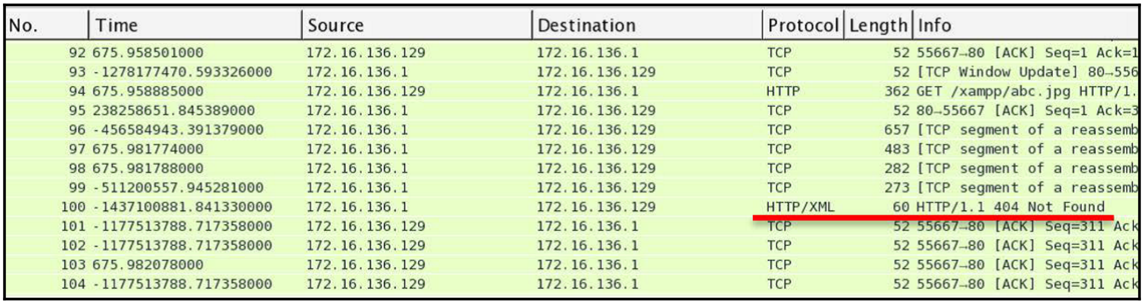
Applications
Sat Jul 18, 01:25
root
Browse and run installed applications
Iceweasel
Iceweasel
Object not found!
172.16.136.1/xampp/abc.jpg
Goo
Most Visited
Exploit-DB
Offensive Security | L...
ZeroBin
Object not found! - Ic...

Object not found!

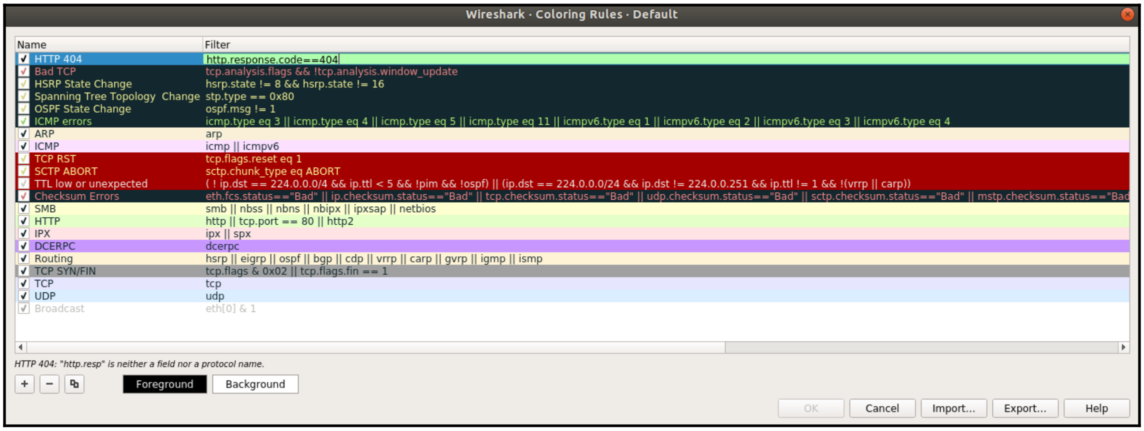
The requested URL was not found on this server. If you entered the URL manually please check your spelling and try again.

If you think this is a server error, please contact the webmaster.

Error 404



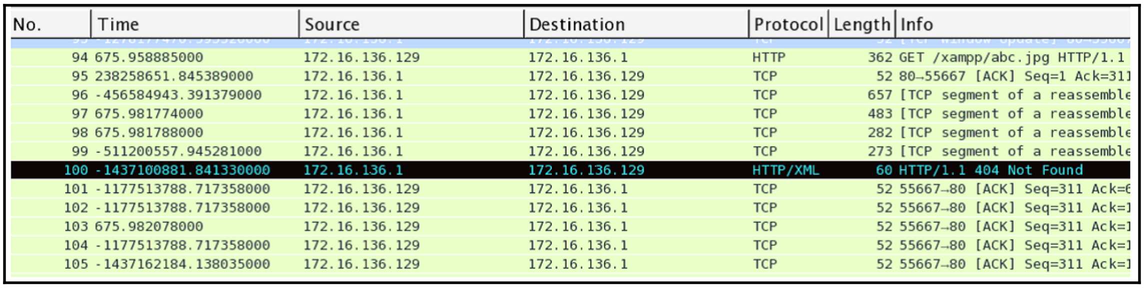
| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 92 | 675.958501000 | 172.16.136.129 | 172.16.136.1 | TCP | 52 | 55667→80 [ACK] Seq=1 Ack=1 |
| 93 | -1278177470.593326000 | 172.16.136.1 | 172.16.136.129 | TCP | 52 | [TCP Window Update] 80→556 |
| 94 | 675.958885000 | 172.16.136.129 | 172.16.136.1 | HTTP | 362 | GET /xampp/abc.jpg HTTP/1. |
| 95 | 238258651.845389000 | 172.16.136.1 | 172.16.136.129 | TCP | 52 | 80→55667 [ACK] Seq=1 Ack=3 |
| 96 | -456584943.391379000 | 172.16.136.1 | 172.16.136.129 | TCP | 657 | [TCP segment of a reassemb |
| 97 | 675.981774000 | 172.16.136.1 | 172.16.136.129 | TCP | 483 | [TCP segment of a reassemb |
| 98 | 675.981788000 | 172.16.136.1 | 172.16.136.129 | TCP | 282 | [TCP segment of a reassemb |
| 99 | -511200557.945281000 | 172.16.136.1 | 172.16.136.129 | TCP | 273 | [TCP segment of a reassemb |
| 100 | -1437100881.841330000 | 172.16.136.1 | 172.16.136.129 | HTTP/XML | 60 | HTTP/1.1 404 Not Found |
| 101 | -1177513788.717358000 | 172.16.136.129 | 172.16.136.1 | TCP | 52 | 55667→80 [ACK] Seq=311 Ack |
| 102 | -1177513788.717358000 | 172.16.136.129 | 172.16.136.1 | TCP | 52 | 55667→80 [ACK] Seq=311 Ack |
| 103 | 675.982078000 | 172.16.136.129 | 172.16.136.1 | TCP | 52 | 55667→80 [ACK] Seq=311 Ack |
| 104 | -1177513788.717358000 | 172.16.136.129 | 172.16.136.1 | TCP | 52 | 55667→80 [ACK] Seq=311 Ack |



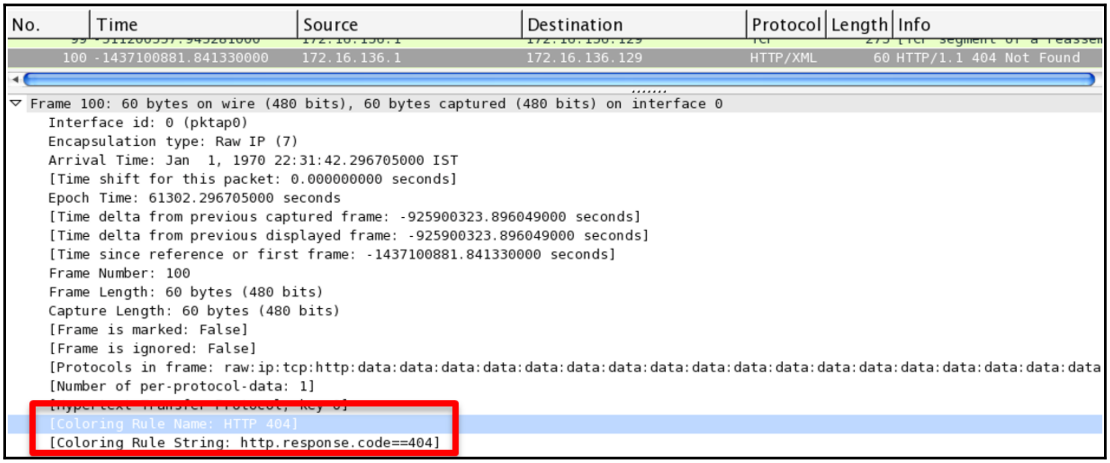
Wireshark · Coloring Rules · Default

| Name | Filter |
|---|---|
| ☑ HTTP 404 | http.response.code==404 |
| ☑ Bad TCP | tcp.analysis.flags && !tcp.analysis.window_update |
| ☑ HSRP State Change | hsrp.state != 8 && hsrp.state != 16 |
| ☑ Spanning Tree Topology  Change | stp.type == 0x80 |
| ☑ OSPF State Change | ospf.msg != 1 |
| ☑ ICMP errors | icmp.type eq 3 \|\| icmp.type eq 4 \|\| icmp.type eq 5 \|\| icmp.type eq 11 \|\| icmpv6.type eq 1 \|\| icmpv6.type eq 2 \|\| icmpv6.type eq 3 \|\| icmpv6.type eq 4 |
| ☑ ARP | arp |
| ☑ ICMP | icmp \|\| icmpv6 |
| ☑ TCP RST | tcp.flags.reset eq 1 |
| ☑ SCTP ABORT | sctp.chunk_type eq ABORT |
| ☑ TTL low or unexpected | ( ! ip.dst == 224.0.0.0/4 && ip.ttl < 5 && !pim && !ospf) \|\| (ip.dst == 224.0.0.0/24 && ip.dst != 224.0.0.251 && ip.ttl != 1 && !(vrrp \|\| carp)) |
| ☑ Checksum Errors | eth.fcs.status=="Bad" \|\| ip.checksum.status=="Bad" \|\| tcp.checksum.status=="Bad" \|\| udp.checksum.status=="Bad" \|\| sctp.checksum.status=="Bad" \|\| mstp.checksum.status=="Bad |
| ☑ SMB | smb \|\| nbss \|\| nbns \|\| nbipx \|\| ipxsap \|\| netbios |
| ☑ HTTP | http \|\| tcp.port == 80 \|\| http2 |
| ☑ IPX | ipx \|\| spx |
| ☑ DCERPC | dcerpc |
| ☑ Routing | hsrp \|\| eigrp \|\| ospf \|\| bgp \|\| cdp \|\| vrrp \|\| carp \|\| gvrp \|\| igmp \|\| ismp |
| ☑ TCP SYN/FIN | tcp.flags & 0x02 \|\| tcp.flags.fin == 1 |
| ☑ TCP | tcp |
| ☑ UDP | udp |
| ☑ Broadcast | eth[0] & 1 |

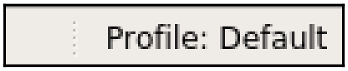
*HTTP 404: "http.resp" is neither a field nor a protocol name.*



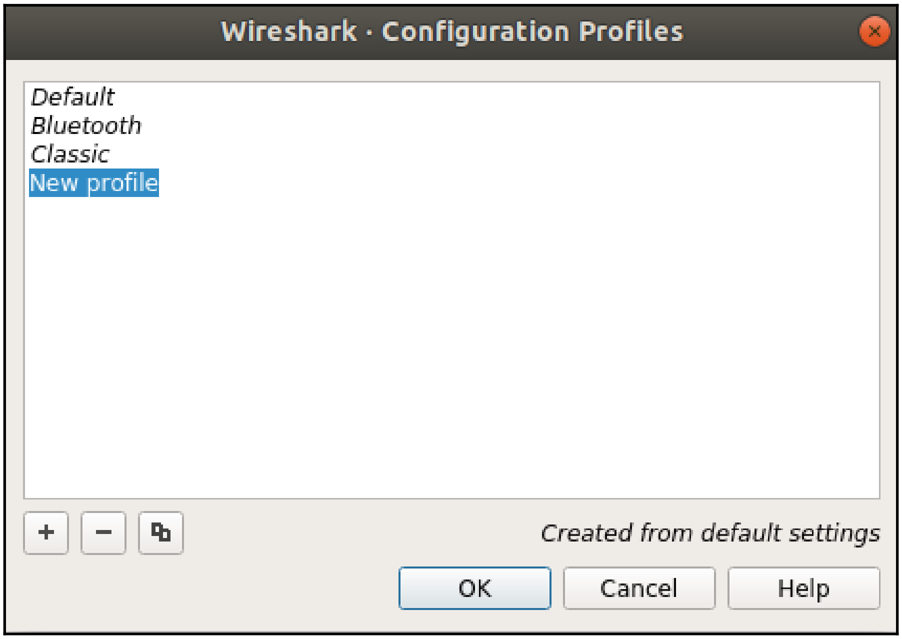
| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 94 | 675.958885000 | 172.16.136.129 | 172.16.136.1 | HTTP | 362 | GET /xampp/abc.jpg HTTP/1.1 |
| 95 | 238258651.845389000 | 172.16.136.1 | 172.16.136.129 | TCP | 52 | 80→55667 [ACK] Seq=1 Ack=311 |
| 96 | -456584943.391379000 | 172.16.136.1 | 172.16.136.129 | TCP | 657 | [TCP segment of a reassemble |
| 97 | 675.981774000 | 172.16.136.1 | 172.16.136.129 | TCP | 483 | [TCP segment of a reassemble |
| 98 | 675.981788000 | 172.16.136.1 | 172.16.136.129 | TCP | 282 | [TCP segment of a reassemble |
| 99 | -511200557.945281000 | 172.16.136.1 | 172.16.136.129 | TCP | 273 | [TCP segment of a reassemble |
| 100 | -1437100881.841330000 | 172.16.136.1 | 172.16.136.129 | HTTP/XML | 60 | HTTP/1.1 404 Not Found |
| 101 | -1177513788.717358000 | 172.16.136.129 | 172.16.136.1 | TCP | 52 | 55667→80 [ACK] Seq=311 Ack=6 |
| 102 | -1177513788.717358000 | 172.16.136.129 | 172.16.136.1 | TCP | 52 | 55667→80 [ACK] Seq=311 Ack=1 |
| 103 | 675.982078000 | 172.16.136.129 | 172.16.136.1 | TCP | 52 | 55667→80 [ACK] Seq=311 Ack=1 |
| 104 | -1177513788.717358000 | 172.16.136.129 | 172.16.136.1 | TCP | 52 | 55667→80 [ACK] Seq=311 Ack=1 |
| 105 | -1437162184.138035000 | 172.16.136.129 | 172.16.136.1 | TCP | 52 | 55667→80 [ACK] Seq=311 Ack=1 |



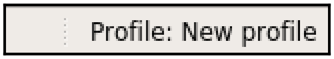
```
No.   Time                      Source            Destination        Protocol  Length Info
   99 -311200557.945281000      172.16.136.1      172.16.136.129     TCP          275 [TCP segment of a reassem
  100 -1437100881.841330000     172.16.136.1      172.16.136.129     HTTP/XML      60 HTTP/1.1 404 Not Found
▽ Frame 100: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
    Interface id: 0 (pktap0)
    Encapsulation type: Raw IP (7)
    Arrival Time: Jan  1, 1970 22:31:42.296705000 IST
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 61302.296705000 seconds
    [Time delta from previous captured frame: -925900323.896049000 seconds]
    [Time delta from previous displayed frame: -925900323.896049000 seconds]
    [Time since reference or first frame: -1437100881.841330000 seconds]
    Frame Number: 100
    Frame Length: 60 bytes (480 bits)
    Capture Length: 60 bytes (480 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: raw:ip:tcp:http:data:data:data:data:data:data:data:data:data:data:data:data:data:data:data:data:data:data
    [Number of per-protocol-data: 1]
    [Hypertext Transfer Protocol, key 0]
    [Coloring Rule Name: HTTP 404]
    [Coloring Rule String: http.response.code==404]
```



Profile: Default

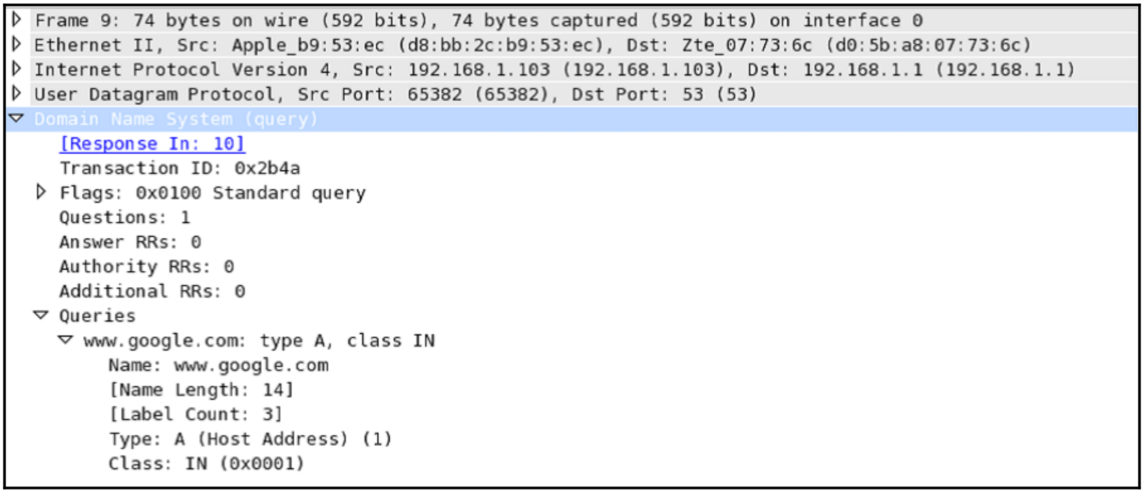


Created from default settings

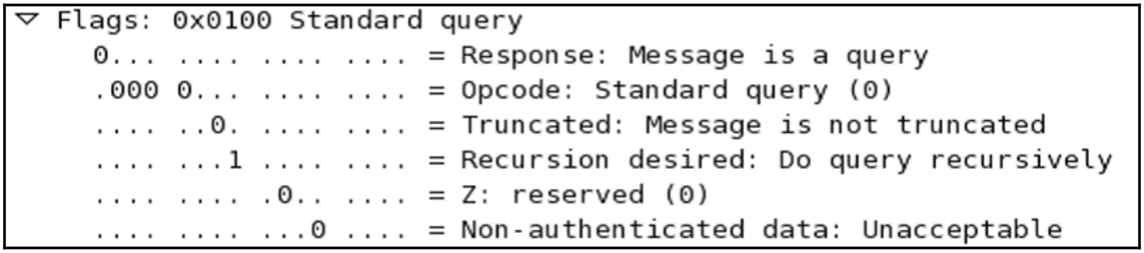


Profile: New profile

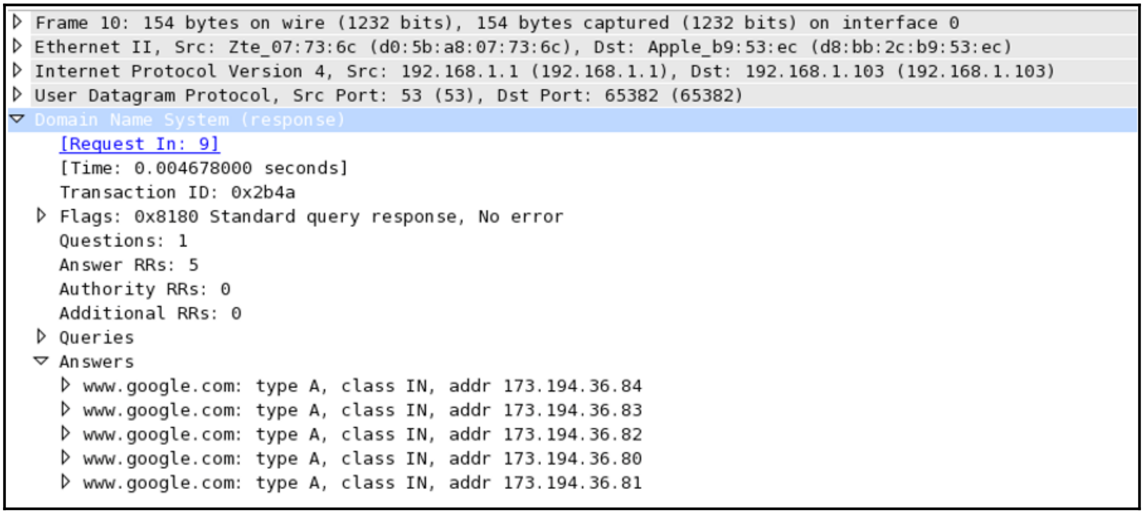
# Chapter 4:
# Analyzing Application  Layer Protocols



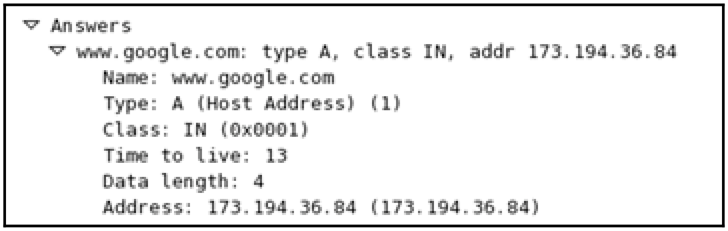
```
▷ Frame 9: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
▷ Ethernet II, Src: Apple_b9:53:ec (d8:bb:2c:b9:53:ec), Dst: Zte_07:73:6c (d0:5b:a8:07:73:6c)
▷ Internet Protocol Version 4, Src: 192.168.1.103 (192.168.1.103), Dst: 192.168.1.1 (192.168.1.1)
▷ User Datagram Protocol, Src Port: 65382 (65382), Dst Port: 53 (53)
▽ Domain Name System (query)
    [Response In: 10]
    Transaction ID: 0x2b4a
  ▷ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▽ Queries
    ▽ www.google.com: type A, class IN
        Name: www.google.com
        [Name Length: 14]
        [Label Count: 3]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
```



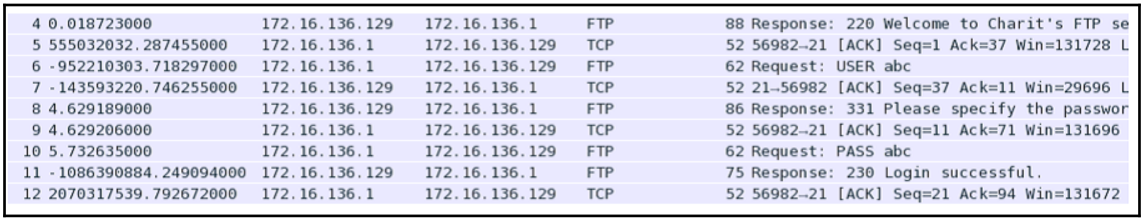
```
▽ Flags: 0x0100 Standard query
    0... .... .... .... = Response: Message is a query
    .000 0... .... .... = Opcode: Standard query (0)
    .... ..0. .... .... = Truncated: Message is not truncated
    .... ...1 .... .... = Recursion desired: Do query recursively
    .... .... .0.. .... = Z: reserved (0)
    .... .... ...0 .... = Non-authenticated data: Unacceptable
```



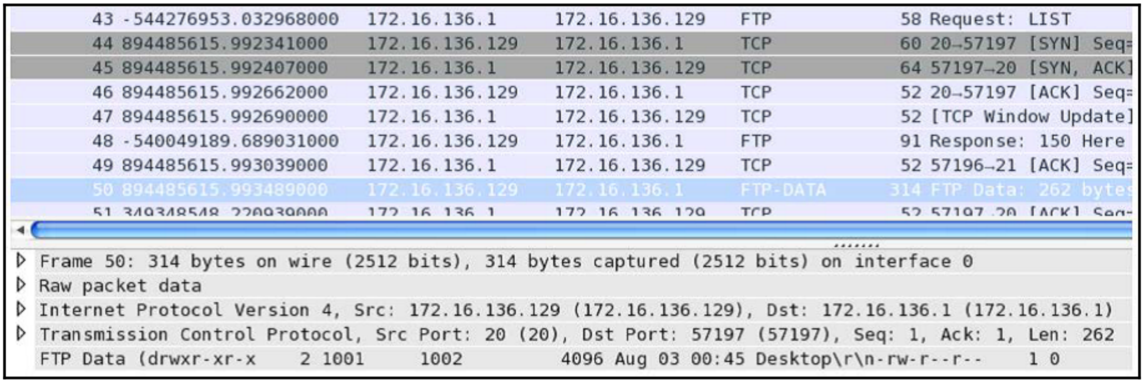
```
▷ Frame 10: 154 bytes on wire (1232 bits), 154 bytes captured (1232 bits) on interface 0
▷ Ethernet II, Src: Zte_07:73:6c (d0:5b:a8:07:73:6c), Dst: Apple_b9:53:ec (d8:bb:2c:b9:53:ec)
▷ Internet Protocol Version 4, Src: 192.168.1.1 (192.168.1.1), Dst: 192.168.1.103 (192.168.1.103)
▷ User Datagram Protocol, Src Port: 53 (53), Dst Port: 65382 (65382)
▽ Domain Name System (response)
    [Request In: 9]
    [Time: 0.004678000 seconds]
    Transaction ID: 0x2b4a
  ▷ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 5
    Authority RRs: 0
    Additional RRs: 0
  ▷ Queries
  ▽ Answers
    ▷ www.google.com: type A, class IN, addr 173.194.36.84
    ▷ www.google.com: type A, class IN, addr 173.194.36.83
    ▷ www.google.com: type A, class IN, addr 173.194.36.82
    ▷ www.google.com: type A, class IN, addr 173.194.36.80
    ▷ www.google.com: type A, class IN, addr 173.194.36.81
```



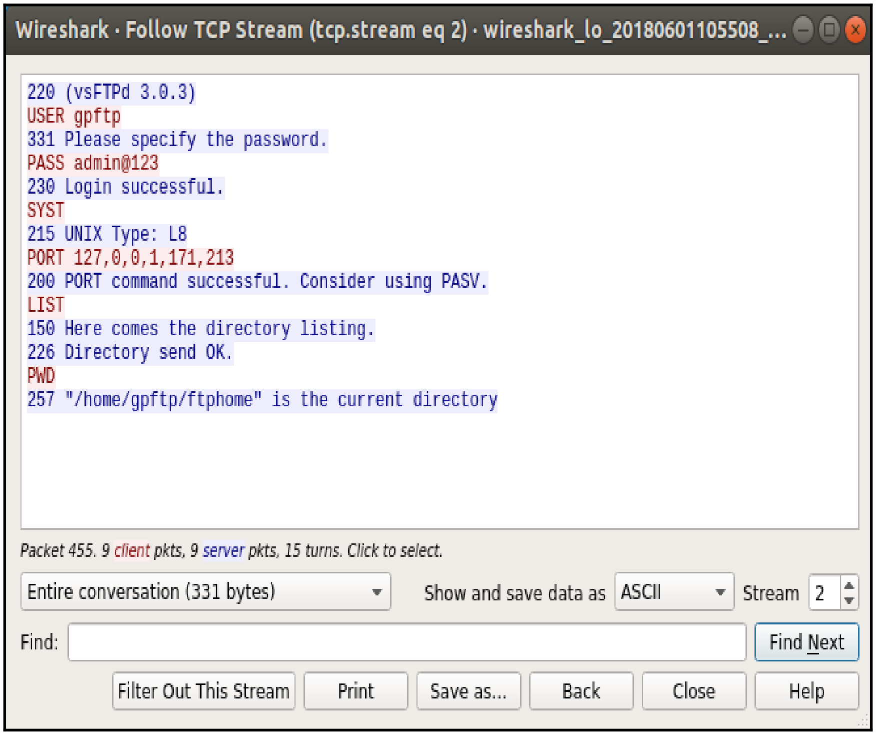
```
▽ Answers
  ▽ www.google.com: type A, class IN, addr 173.194.36.84
      Name: www.google.com
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 13
      Data length: 4
      Address: 173.194.36.84 (173.194.36.84)
```



```
 4 0.018723000             172.16.136.129   172.16.136.1     FTP          88 Response: 220 Welcome to Charit's FTP se
 5 555032032.287455000     172.16.136.1     172.16.136.129   TCP          52 56982→21 [ACK] Seq=1 Ack=37 Win=131728 L
 6 -952210303.718297000    172.16.136.1     172.16.136.129   FTP          62 Request: USER abc
 7 -143593220.746255000    172.16.136.129   172.16.136.1     TCP          52 21→56982 [ACK] Seq=37 Ack=11 Win=29696 L
 8 4.629189000             172.16.136.129   172.16.136.1     FTP          86 Response: 331 Please specify the passwor
 9 4.629206000             172.16.136.1     172.16.136.129   TCP          52 56982→21 [ACK] Seq=11 Ack=71 Win=131696
10 5.732635000             172.16.136.1     172.16.136.129   FTP          62 Request: PASS abc
11 -1086390884.249094000   172.16.136.129   172.16.136.1     FTP          75 Response: 230 Login successful.
12 2070317539.792672000    172.16.136.1     172.16.136.129   TCP          52 56982→21 [ACK] Seq=21 Ack=94 Win=131672
```



```
43 -544276953.032968000  172.16.136.1    172.16.136.129  FTP        58 Request: LIST
44 894485615.992341000   172.16.136.129  172.16.136.1    TCP        60 20→57197 [SYN] Seq=
45 894485615.992407000   172.16.136.1    172.16.136.129  TCP        64 57197→20 [SYN, ACK]
46 894485615.992662000   172.16.136.129  172.16.136.1    TCP        52 20→57197 [ACK] Seq=
47 894485615.992690000   172.16.136.1    172.16.136.129  TCP        52 [TCP Window Update]
48 -540049189.689031000  172.16.136.129  172.16.136.1    FTP        91 Response: 150 Here
49 894485615.993039000   172.16.136.1    172.16.136.129  TCP        52 57196→21 [ACK] Seq=
50 894485615.993489000   172.16.136.129  172.16.136.1    FTP-DATA  314 FTP Data: 262 bytes
51 349348548.220939000   172.16.136.1    172.16.136.129  TCP        52 57197→20 [ACK] Seq=

▷ Frame 50: 314 bytes on wire (2512 bits), 314 bytes captured (2512 bits) on interface 0
▷ Raw packet data
▷ Internet Protocol Version 4, Src: 172.16.136.129 (172.16.136.129), Dst: 172.16.136.1 (172.16.136.1)
▷ Transmission Control Protocol, Src Port: 20 (20), Dst Port: 57197 (57197), Seq: 1, Ack: 1, Len: 262
  FTP Data (drwxr-xr-x    2 1001     1002         4096 Aug 03 00:45 Desktop\r\n-rw-r--r--    1 0
```



Wireshark · Follow TCP Stream (tcp.stream eq 2) · wireshark_lo_20180601105508_...

```
220 (vsFTPd 3.0.3)
USER gpftp
331 Please specify the password.
PASS admin@123
230 Login successful.
SYST
215 UNIX Type: L8
PORT 127,0,0,1,171,213
200 PORT command successful. Consider using PASV.
LIST
150 Here comes the directory listing.
226 Directory send OK.
PWD
257 "/home/gpftp/ftphome" is the current directory
```

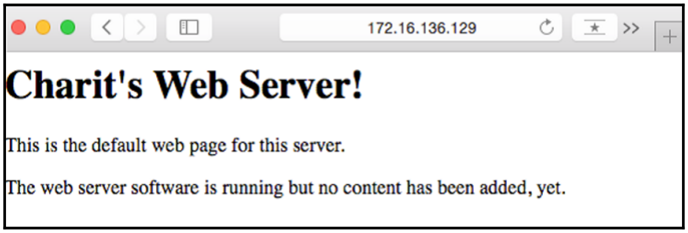
*Packet 455. 9 client pkts, 9 server pkts, 15 turns. Click to select.*

Entire conversation (331 bytes)

Show and save data as ASCII

Stream 2

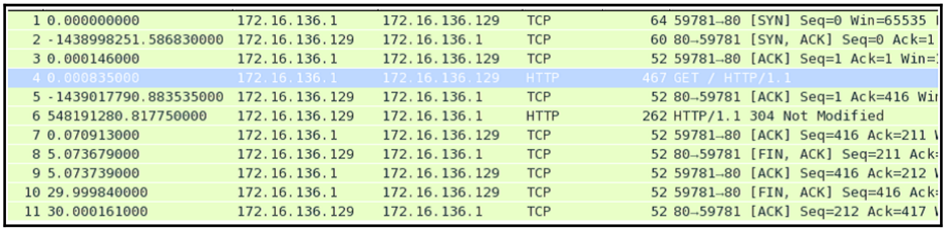
Find:



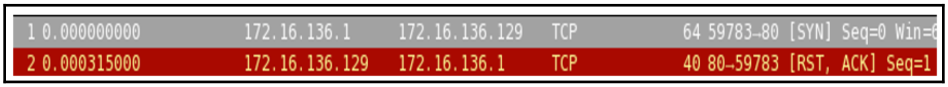
# Charit's Web Server!

This is the default web page for this server.

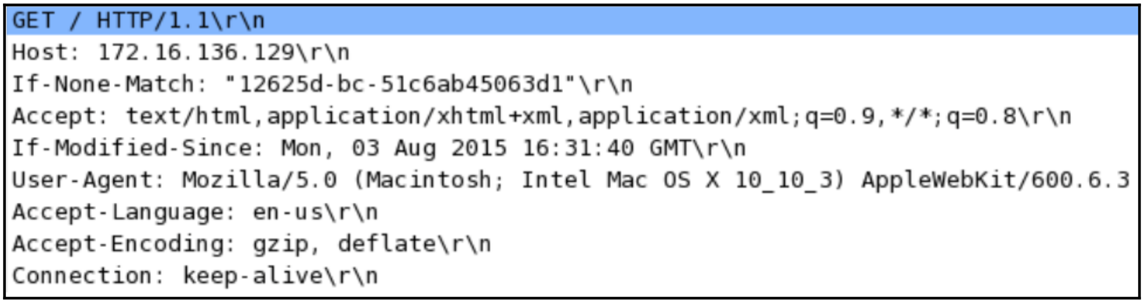
The web server software is running but no content has been added, yet.



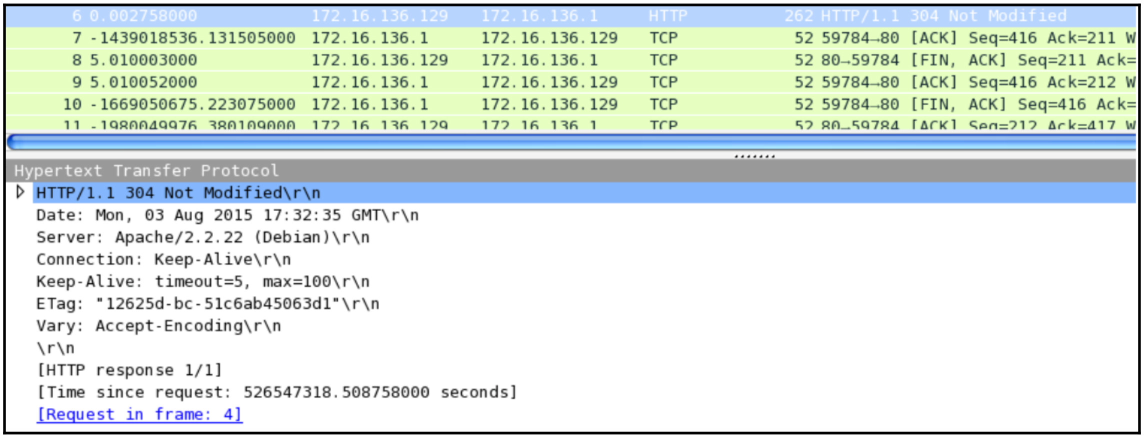
```
 1 0.000000000            172.16.136.1     172.16.136.129   TCP          64 59781→80 [SYN] Seq=0 Win=65535
 2 -1438998251.586830000  172.16.136.129   172.16.136.1     TCP          60 80→59781 [SYN, ACK] Seq=0 Ack=1
 3 0.000146000            172.16.136.1     172.16.136.129   TCP          52 59781→80 [ACK] Seq=1 Ack=1 Win=
 4 0.000835000            172.16.136.1     172.16.136.129   HTTP        467 GET / HTTP/1.1
 5 -1439017790.883535000  172.16.136.129   172.16.136.1     TCP          52 80→59781 [ACK] Seq=1 Ack=416 Wi
 6 548191280.817750000    172.16.136.129   172.16.136.1     HTTP        262 HTTP/1.1 304 Not Modified
 7 0.070913000            172.16.136.1     172.16.136.129   TCP          52 59781→80 [ACK] Seq=416 Ack=211
 8 5.073679000            172.16.136.129   172.16.136.1     TCP          52 80→59781 [FIN, ACK] Seq=211 Ack
 9 5.073739000            172.16.136.1     172.16.136.129   TCP          52 59781→80 [ACK] Seq=416 Ack=212
10 29.999840000           172.16.136.1     172.16.136.129   TCP          52 59781→80 [FIN, ACK] Seq=416 Ack
11 30.000161000           172.16.136.129   172.16.136.1     TCP          52 80→59781 [ACK] Seq=212 Ack=417
```



```
1 0.000000000         172.16.136.1     172.16.136.129   TCP         64 59783→80 [SYN] Seq=0 Win=
2 0.000315000         172.16.136.129   172.16.136.1     TCP         40 80→59783 [RST, ACK] Seq=1
```

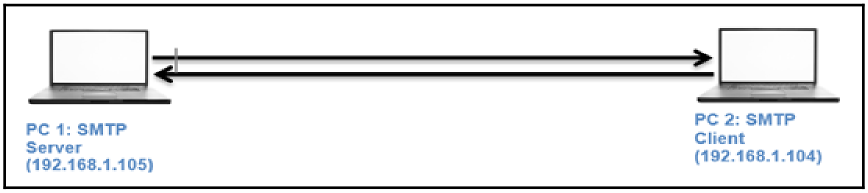


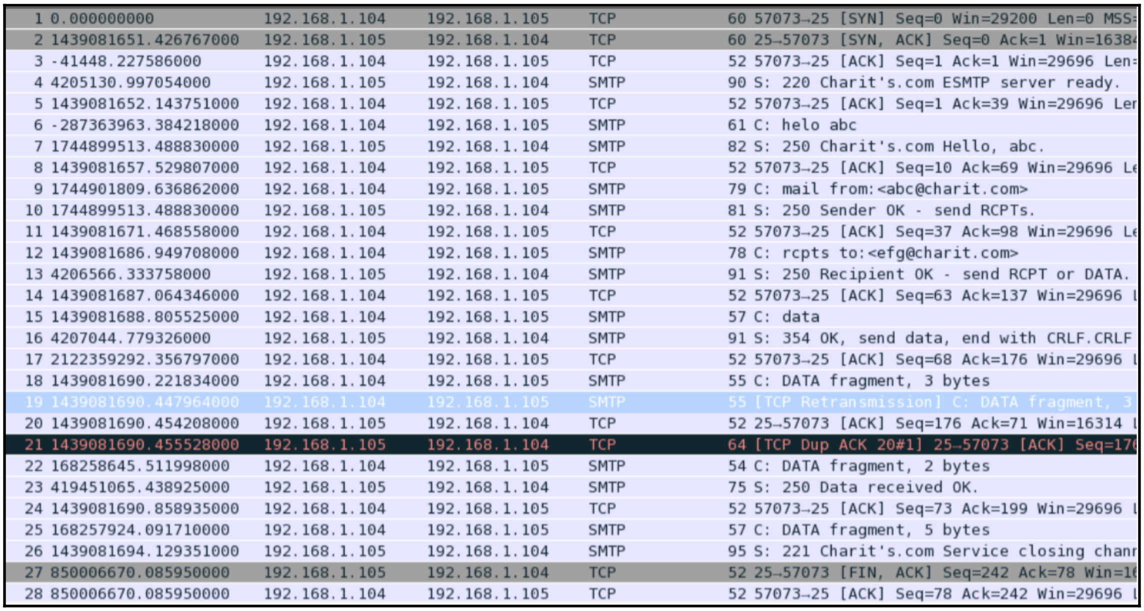
```
GET / HTTP/1.1\r\n
Host: 172.16.136.129\r\n
If-None-Match: "12625d-bc-51c6ab45063d1"\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
If-Modified-Since: Mon, 03 Aug 2015 16:31:40 GMT\r\n
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_3) AppleWebKit/600.6.3
Accept-Language: en-us\r\n
Accept-Encoding: gzip, deflate\r\n
Connection: keep-alive\r\n
```



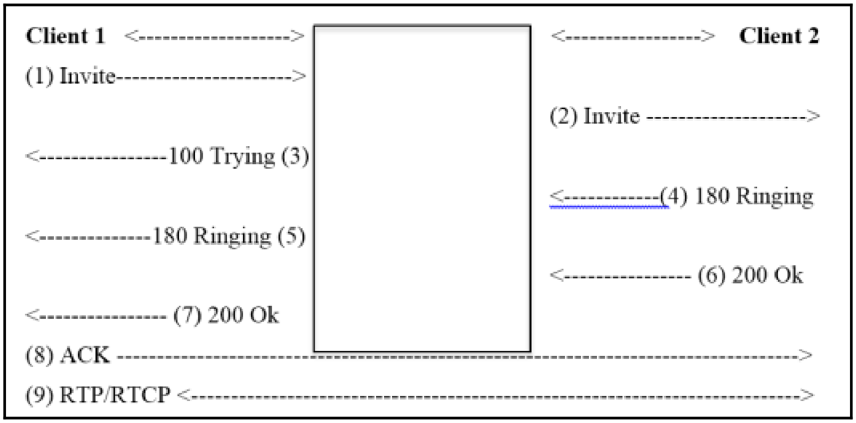
```
  6 0.002758000              172.16.136.129   172.16.136.1     HTTP        262 HTTP/1.1 304 Not Modified
  7 -1439018536.131505000    172.16.136.1     172.16.136.129   TCP          52 59784→80 [ACK] Seq=416 Ack=211 W
  8 5.010003000              172.16.136.129   172.16.136.1     TCP          52 80→59784 [FIN, ACK] Seq=211 Ack=
  9 5.010052000              172.16.136.1     172.16.136.129   TCP          52 59784→80 [ACK] Seq=416 Ack=212 W
 10 -1669050675.223075000    172.16.136.1     172.16.136.129   TCP          52 59784→80 [FIN, ACK] Seq=416 Ack=
 11 -1980049976.380109000    172.16.136.129   172.16.136.1     TCP          52 80→59784 [ACK] Seq=212 Ack=417 W
```

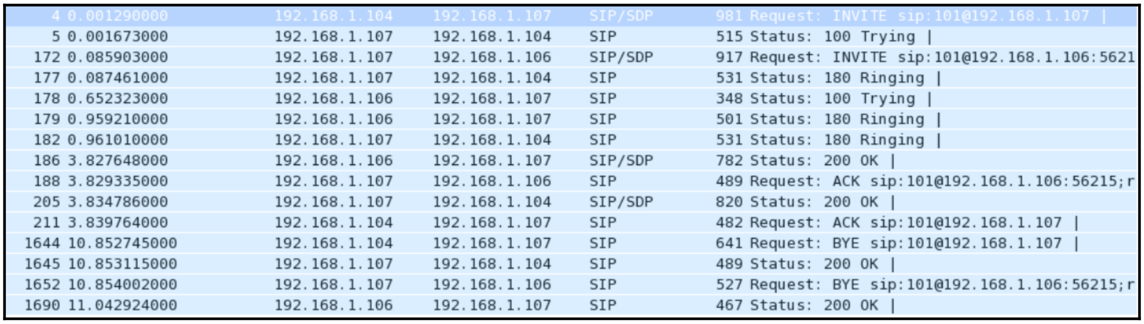
```
Hypertext Transfer Protocol
▷ HTTP/1.1 304 Not Modified\r\n
  Date: Mon, 03 Aug 2015 17:32:35 GMT\r\n
  Server: Apache/2.2.22 (Debian)\r\n
  Connection: Keep-Alive\r\n
  Keep-Alive: timeout=5, max=100\r\n
  ETag: "12625d-bc-51c6ab45063d1"\r\n
  Vary: Accept-Encoding\r\n
  \r\n
  [HTTP response 1/1]
  [Time since request: 526547318.508758000 seconds]
  [Request in frame: 4]
```


PC 1: SMTP Server (192.168.1.105)
PC 2: SMTP Client (192.168.1.104)

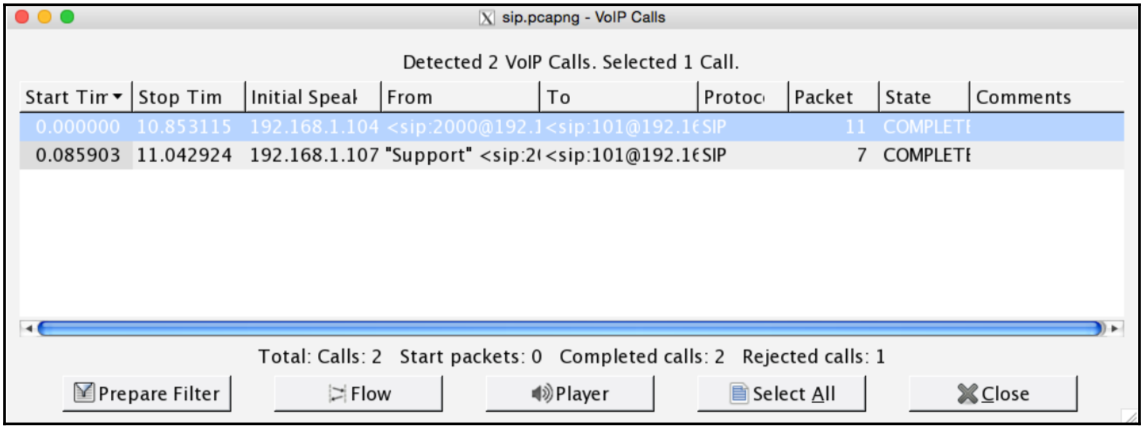


```
 1 0.000000000             192.168.1.104   192.168.1.105   TCP       60 57073→25 [SYN] Seq=0 Win=29200 Len=0 MSS=
 2 1439081651.426767000    192.168.1.105   192.168.1.104   TCP       60 25→57073 [SYN, ACK] Seq=0 Ack=1 Win=16384
 3 -41448.227586000        192.168.1.104   192.168.1.105   TCP       52 57073→25 [ACK] Seq=1 Ack=1 Win=29696 Len=
 4 4205130.997054000       192.168.1.105   192.168.1.104   SMTP      90 S: 220 Charit's.com ESMTP server ready.
 5 1439081652.143751000    192.168.1.104   192.168.1.105   TCP       52 57073→25 [ACK] Seq=1 Ack=39 Win=29696 Len
 6 -287363963.384218000    192.168.1.104   192.168.1.105   SMTP      61 C: helo abc
 7 1744899513.488830000    192.168.1.105   192.168.1.104   SMTP      82 S: 250 Charit's.com Hello, abc.
 8 1439081657.529807000    192.168.1.104   192.168.1.105   TCP       52 57073→25 [ACK] Seq=10 Ack=69 Win=29696 Le
 9 1744901809.636862000    192.168.1.104   192.168.1.105   SMTP      79 C: mail from:<abc@charit.com>
10 1744899513.488830000    192.168.1.105   192.168.1.104   SMTP      81 S: 250 Sender OK - send RCPTs.
11 1439081671.468558000    192.168.1.104   192.168.1.105   TCP       52 57073→25 [ACK] Seq=37 Ack=98 Win=29696 Le
12 1439081686.949708000    192.168.1.104   192.168.1.105   SMTP      78 C: rcpts to:<efg@charit.com>
13 4206566.333758000       192.168.1.105   192.168.1.104   SMTP      91 S: 250 Recipient OK - send RCPT or DATA.
14 1439081687.064346000    192.168.1.104   192.168.1.105   TCP       52 57073→25 [ACK] Seq=63 Ack=137 Win=29696 L
15 1439081688.805525000    192.168.1.104   192.168.1.105   SMTP      57 C: data
16 4207044.779326000       192.168.1.105   192.168.1.104   SMTP      91 S: 354 OK, send data, end with CRLF.CRLF
17 2122359292.356797000    192.168.1.104   192.168.1.105   TCP       52 57073→25 [ACK] Seq=68 Ack=176 Win=29696 L
18 1439081690.221834000    192.168.1.104   192.168.1.105   SMTP      55 C: DATA fragment, 3 bytes
19 1439081690.447964000    192.168.1.104   192.168.1.105   SMTP      55 [TCP Retransmission] C: DATA fragment, 3
20 1439081690.454208000    192.168.1.105   192.168.1.104   TCP       52 25→57073 [ACK] Seq=176 Ack=71 Win=16314 L
21 1439081690.455528000    192.168.1.105   192.168.1.104   TCP       64 [TCP Dup ACK 20#1] 25→57073 [ACK] Seq=176
22 168258645.511998000     192.168.1.104   192.168.1.105   SMTP      54 C: DATA fragment, 2 bytes
23 419451065.438925000     192.168.1.105   192.168.1.104   SMTP      75 S: 250 Data received OK.
24 1439081690.858935000    192.168.1.104   192.168.1.105   TCP       52 57073→25 [ACK] Seq=73 Ack=199 Win=29696 L
25 168257924.091710000     192.168.1.104   192.168.1.105   SMTP      57 C: DATA fragment, 5 bytes
26 1439081694.129351000    192.168.1.105   192.168.1.104   SMTP      95 S: 221 Charit's.com Service closing chann
27 850006670.085950000     192.168.1.105   192.168.1.104   TCP       52 25→57073 [FIN, ACK] Seq=242 Ack=78 Win=16
28 850006670.085950000     192.168.1.104   192.168.1.105   TCP       52 57073→25 [ACK] Seq=78 Ack=242 Win=29696 L
```





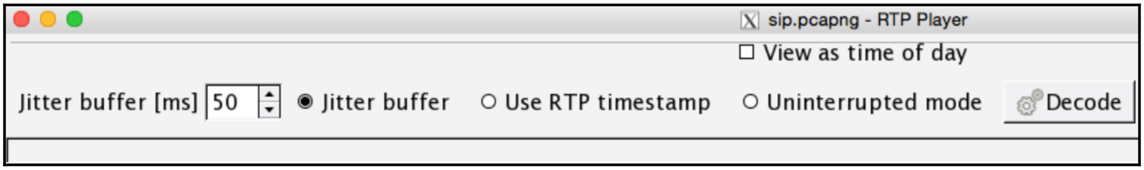
```
   4 0.001290000        192.168.1.104   192.168.1.107   SIP/SDP     981 Request: INVITE sip:101@192.168.1.107 |
   5 0.001673000        192.168.1.107   192.168.1.104   SIP         515 Status: 100 Trying |
 172 0.085903000        192.168.1.107   192.168.1.106   SIP/SDP     917 Request: INVITE sip:101@192.168.1.106:5621
 177 0.087461000        192.168.1.107   192.168.1.104   SIP         531 Status: 180 Ringing |
 178 0.652323000        192.168.1.106   192.168.1.107   SIP         348 Status: 100 Trying |
 179 0.959210000        192.168.1.106   192.168.1.107   SIP         501 Status: 180 Ringing |
 182 0.961010000        192.168.1.107   192.168.1.104   SIP         531 Status: 180 Ringing |
 186 3.827648000        192.168.1.106   192.168.1.107   SIP/SDP     782 Status: 200 OK |
 188 3.829335000        192.168.1.107   192.168.1.106   SIP         489 Request: ACK sip:101@192.168.1.106:56215;r
 205 3.834786000        192.168.1.107   192.168.1.104   SIP/SDP     820 Status: 200 OK |
 211 3.839764000        192.168.1.104   192.168.1.107   SIP         482 Request: ACK sip:101@192.168.1.107 |
1644 10.852745000       192.168.1.104   192.168.1.107   SIP         641 Request: BYE sip:101@192.168.1.107 |
1645 10.853115000       192.168.1.107   192.168.1.104   SIP         489 Status: 200 OK |
1652 10.854002000       192.168.1.107   192.168.1.106   SIP         527 Request: BYE sip:101@192.168.1.106:56215;r
1690 11.042924000       192.168.1.106   192.168.1.107   SIP         467 Status: 200 OK |
```



Detected 2 VoIP Calls. Selected 1 Call.

| Start Tim | Stop Tim | Initial Speal | From | To | Protoc | Packet | State | Comments |
|---|---|---|---|---|---|---|---|---|
| 0.000000 | 10.853115 | 192.168.1.104 | <sip:2000@192.1 | <sip:101@192.16 | SIP | 11 | COMPLETE | |
| 0.085903 | 11.042924 | 192.168.1.107 | "Support" <sip:2( | <sip:101@192.16 | SIP | 7 | COMPLETE | |

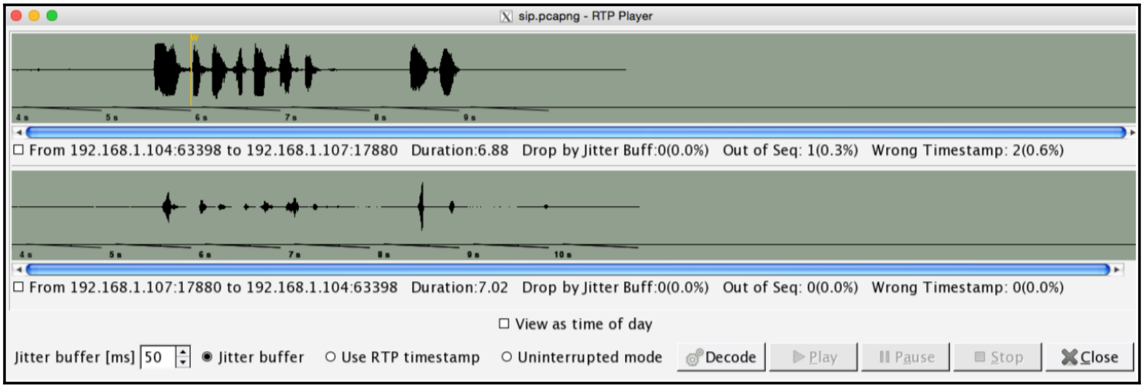
Total: Calls: 2 Start packets: 0 Completed calls: 2 Rejected calls: 1



sip.pcapng - RTP Player

☐ View as time of day

Jitter buffer [ms] 50 ● Jitter buffer ○ Use RTP timestamp ○ Uninterrupted mode

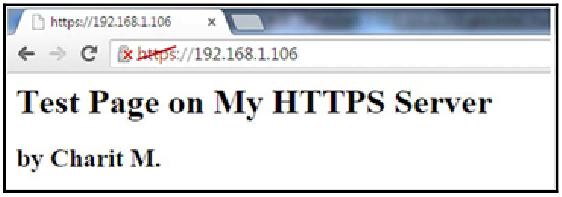


☐ From 192.168.1.104:63398 to 192.168.1.107:17880 Duration:6.88 Drop by Jitter Buff:0(0.0%) Out of Seq: 1(0.3%) Wrong Timestamp: 2(0.6%)

☐ From 192.168.1.107:17880 to 192.168.1.104:63398 Duration:7.02 Drop by Jitter Buff:0(0.0%) Out of Seq: 0(0.0%) Wrong Timestamp: 0(0.0%)

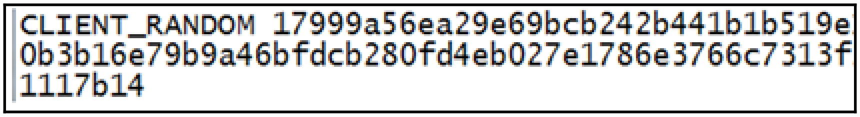
☐ View as time of day

Jitter buffer [ms] 50 ● Jitter buffer ○ Use RTP timestamp ○ Uninterrupted mode

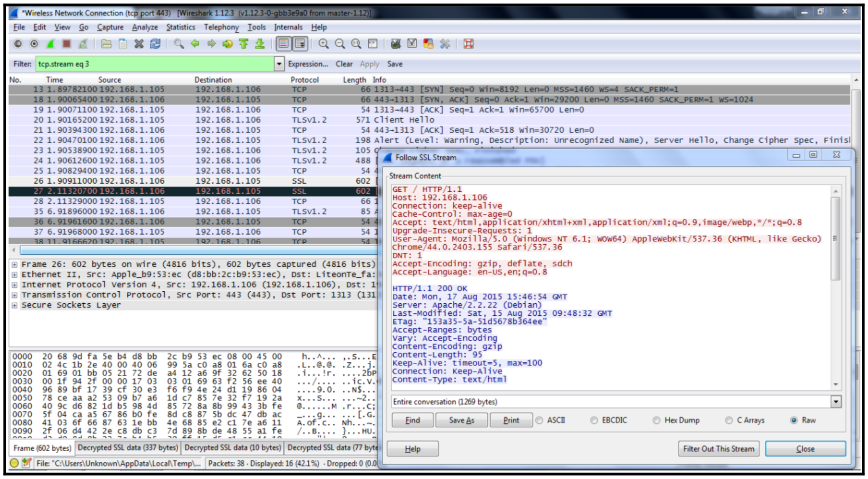


**Test Page on My HTTPS Server**

**by Charit M.**



```
CLIENT_RANDOM 17999a56ea29e69bcb242b441b1b519e
0b3b16e79b9a46bfdcb280fd4eb027e1786e3766c7313f
1117b14
```


*Wireless Network Connection (tcp port 443)   [Wireshark 1.12.3  (v1.12.3-0-gbb3e9a0 from master-1.12)]
File  Edit  View  Go  Capture  Analyze  Statistics  Telephony  Tools  Internals  Help
Expression...  Clear  Apply  Save

Filter: tcp.stream eq 3

```
No.   Time        Source          Destination     Protocol  Length Info
   13 1.89782100 192.168.1.105   192.168.1.106   TCP           66 1313→443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
   18 1.90065400 192.168.1.106   192.168.1.105   TCP           66 443→1313 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=1024
   19 1.90071100 192.168.1.105   192.168.1.106   TCP           54 1313→443 [ACK] Seq=1 Ack=1 Win=65700 Len=0
   20 1.90165200 192.168.1.105   192.168.1.106   TLSv1.2      571 Client Hello
   21 1.90394300 192.168.1.106   192.168.1.105   TCP           54 443→1313 [ACK] Seq=1 Ack=518 Win=30720 Len=0
   22 1.90470100 192.168.1.106   192.168.1.105   TLSv1.2      198 Alert (Level: Warning, Description: Unrecognized Name), Server Hello, Change Cipher Spec, Finisl
   23 1.90538900 192.168.1.105   192.168.1.106   TLSv1.2      105 C
   24 1.90612600 192.168.1.105   192.168.1.106   TLSv1.2      488 [
   25 1.90829400 192.168.1.106   192.168.1.105   TCP           54 4
   26 1.90911000 192.168.1.106   192.168.1.105   SSL          602 [
   27 2.11320700 192.168.1.106   192.168.1.105   SSL          602 [
   28 2.11329000 192.168.1.105   192.168.1.106   TCP           66 1
   35 6.91896000 192.168.1.106   192.168.1.105   TLSv1.2       85 A
   36 6.91961600 192.168.1.106   192.168.1.105   TCP           54 4
   37 6.91968000 192.168.1.105   192.168.1.106   TCP           54 1
   38 11.9166620 192.168.1.105   192.168.1.106   TCP           54 1
```

```
⊞ Frame 26: 602 bytes on wire (4816 bits), 602 bytes captured (4816 bits)
⊞ Ethernet II, Src: Apple_b9:53:ec (d8:bb:2c:b9:53:ec), Dst: LiteonTe_fa:
⊞ Internet Protocol Version 4, Src: 192.168.1.106 (192.168.1.106), Dst: 1
⊞ Transmission Control Protocol, Src Port: 443 (443), Dst Port: 1313 (131
⊞ Secure Sockets Layer
```

```
0000  20 68 9d fa 5e b4 d8 bb  2c b9 53 ec 08 00 45 00   h..^... ,.S...E
0010  02 4c 1b 2e 40 00 40 06  99 5a c0 a8 01 6a c0 a8  .L..@.@. .Z...j.
0020  01 69 01 bb 05 21 72 de  a4 12 a6 9f 32 62 50 18  .i...!r. ....2bP
0030  00 1f 94 2f 00 00 17 03  03 01 69 63 f2 56 ee 40  .../.... ..ic.V.
0040  96 89 bf 17 39 cf 30 e3  f6 f9 4e 24 d1 19 86 04  ....9.0. ..N$...
0050  78 ce aa a2 53 09 b7 a6  1d c7 85 7e 32 f7 19 2a  x...S... ...~2..
0060  40 9c d6 82 1d b5 98 4d  85 72 8a 8b 99 43 3b fe  @......M .r...C;
0070  5f 04 ca a5 67 86 b0 fe  8d c8 87 5b dc 47 db ac  _...g... ...[.G.
0080  41 03 6f 66 87 63 1e bb  4e 68 85 e2 c1 7e a6 11  A.of.c.. Nh...~.
0090  2f 06 d4 42 2e c8 db c3  7d 89 8b de 48 55 a1 fe  /..B.... }...HU.
```

Frame (602 bytes)
Decrypted SSL data (337 bytes)
Decrypted SSL data (10 bytes)
Decrypted SSL data (77 byte

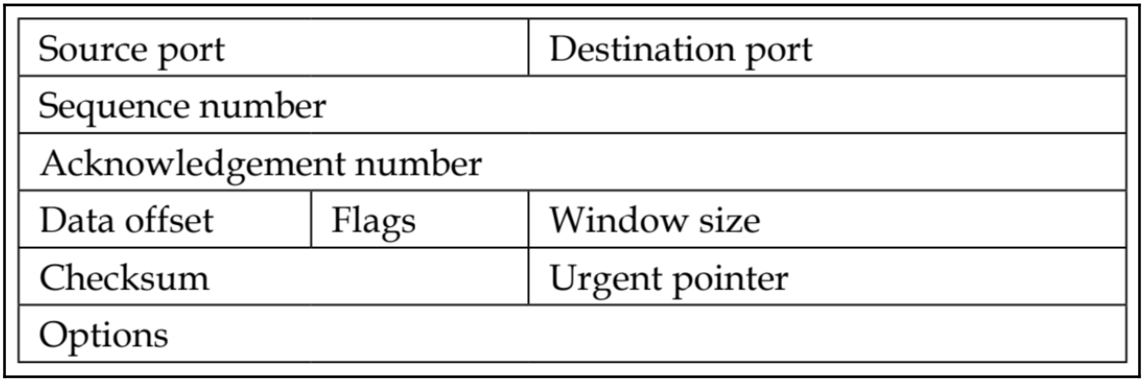
File: "C:\Users\Unknown\AppData\Local\Temp\...   Packets: 38 · Displayed: 16 (42.1%) · Dropped: 0 (0.0

```
GET / HTTP/1.1
Host: 192.168.1.106
Connection: keep-alive
Cache-Control: max-age=0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/44.0.2403.155 Safari/537.36
DNT: 1
Accept-Encoding: gzip, deflate, sdch
Accept-Language: en-US,en;q=0.8

HTTP/1.1 200 OK
Date: Mon, 17 Aug 2015 15:46:54 GMT
Server: Apache/2.2.22 (Debian)
Last-Modified: Sat, 15 Aug 2015 09:48:32 GMT
ETag: "153a35-5a-51d5678b364ee"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 95
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html
```

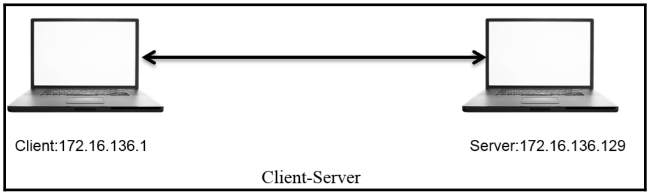
Entire conversation (1269 bytes)

○ ASCII  ○ EBCDIC  ○ Hex Dump  ○ C Arrays  ● Raw

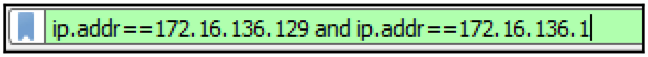
# Chapter 5:
# Analyzing the Transport Layer Protocols TCP/UDP



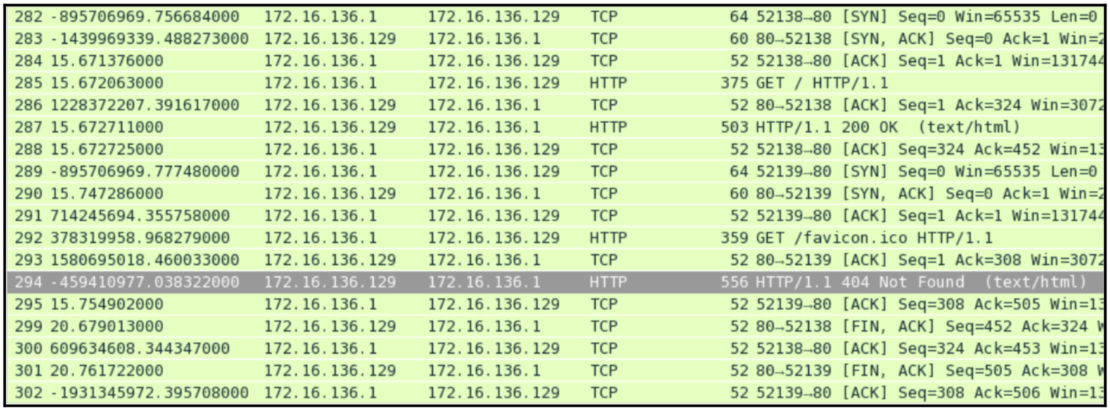
| | | |
|---|---|---|
| Source port | | Destination port |
| Sequence number | | |
| Acknowledgement number | | |
| Data offset | Flags | Window size |
| Checksum | | Urgent pointer |
| Options | | |



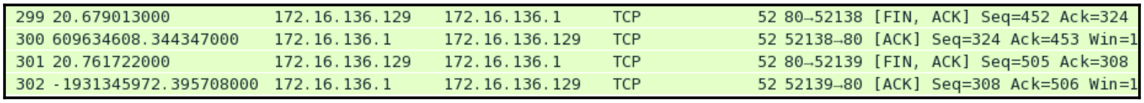
Client-Server



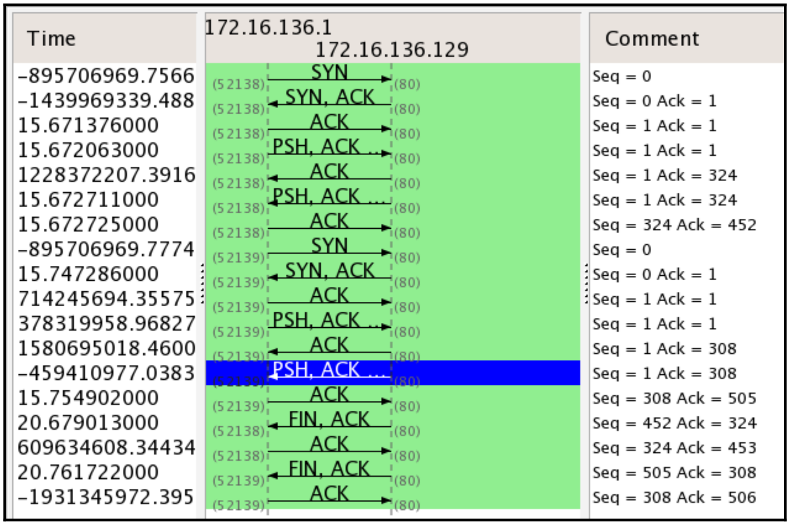
```
ip.addr==172.16.136.129 and ip.addr==172.16.136.1
```



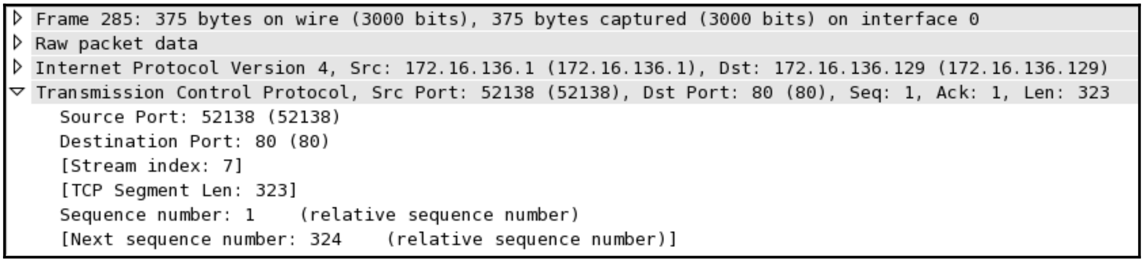
```
282 -895706969.756684000   172.16.136.1      172.16.136.129    TCP         64 52138→80 [SYN] Seq=0 Win=65535 Len=0
283 -1439969339.488273000  172.16.136.129    172.16.136.1      TCP         60 80→52138 [SYN, ACK] Seq=0 Ack=1 Win=2
284 15.671376000           172.16.136.1      172.16.136.129    TCP         52 52138→80 [ACK] Seq=1 Ack=1 Win=131744
285 15.672063000           172.16.136.1      172.16.136.129    HTTP       375 GET / HTTP/1.1
286 1228372207.391617000   172.16.136.129    172.16.136.1      TCP         52 80→52138 [ACK] Seq=1 Ack=324 Win=3072
287 15.672711000           172.16.136.129    172.16.136.1      HTTP       503 HTTP/1.1 200 OK  (text/html)
288 15.672725000           172.16.136.1      172.16.136.129    TCP         52 52138→80 [ACK] Seq=324 Ack=452 Win=13
289 -895706969.777480000   172.16.136.1      172.16.136.129    TCP         64 52139→80 [SYN] Seq=0 Win=65535 Len=0
290 15.747286000           172.16.136.129    172.16.136.1      TCP         60 80→52139 [SYN, ACK] Seq=0 Ack=1 Win=2
291 714245694.355758000    172.16.136.1      172.16.136.129    TCP         52 52139→80 [ACK] Seq=1 Ack=1 Win=131744
292 378319958.968279000    172.16.136.1      172.16.136.129    HTTP       359 GET /favicon.ico HTTP/1.1
293 1580695018.460033000   172.16.136.129    172.16.136.1      TCP         52 80→52139 [ACK] Seq=1 Ack=308 Win=3072
294 -459410977.038322000   172.16.136.129    172.16.136.1      HTTP       556 HTTP/1.1 404 Not Found  (text/html)
295 15.754902000           172.16.136.1      172.16.136.129    TCP         52 52139→80 [ACK] Seq=308 Ack=505 Win=13
299 20.679013000           172.16.136.129    172.16.136.1      TCP         52 80→52138 [FIN, ACK] Seq=452 Ack=324 W
300 609634608.344347000    172.16.136.1      172.16.136.129    TCP         52 52138→80 [ACK] Seq=324 Ack=453 Win=13
301 20.761722000           172.16.136.129    172.16.136.1      TCP         52 80→52139 [FIN, ACK] Seq=505 Ack=308 W
302 -1931345972.395708000  172.16.136.1      172.16.136.129    TCP         52 52139→80 [ACK] Seq=308 Ack=506 Win=13
```



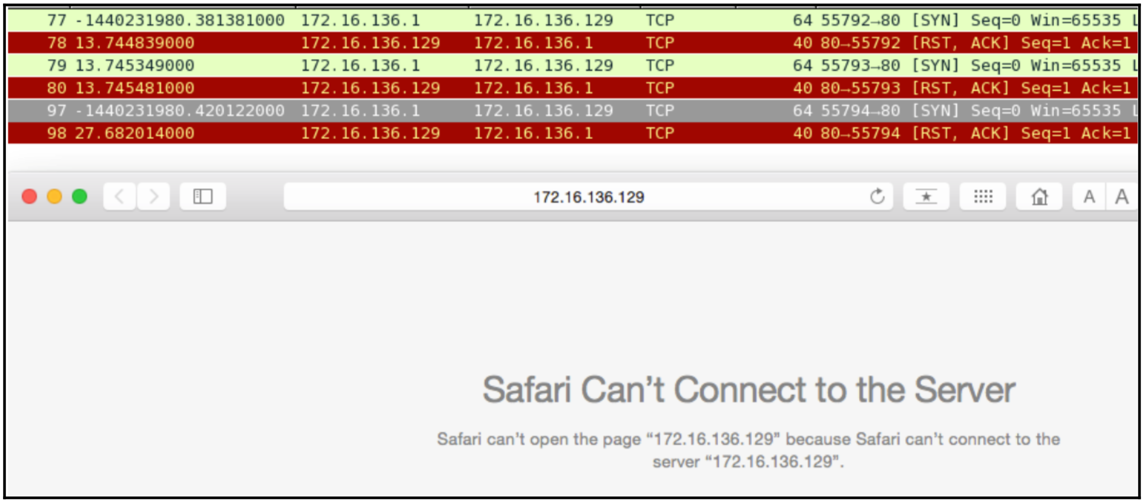
```
299 20.679013000          172.16.136.129    172.16.136.1      TCP          52 80→52138 [FIN, ACK] Seq=452 Ack=324
300 609634608.344347000   172.16.136.1      172.16.136.129    TCP          52 52138→80 [ACK] Seq=324 Ack=453 Win=1
301 20.761722000          172.16.136.129    172.16.136.1      TCP          52 80→52139 [FIN, ACK] Seq=505 Ack=308
302 -1931345972.395708000 172.16.136.1      172.16.136.129    TCP          52 52139→80 [ACK] Seq=308 Ack=506 Win=1
```



| Time | 172.16.136.1<br>172.16.136.129 | Comment |
|---|---|---|
| -895706969.7566 | (52138) SYN → (80) | Seq = 0 |
| -1439969339.488 | (52138) ← SYN, ACK (80) | Seq = 0 Ack = 1 |
| 15.671376000 | (52138) ACK → (80) | Seq = 1 Ack = 1 |
| 15.672063000 | (52138) PSH, ACK ... → (80) | Seq = 1 Ack = 1 |
| 1228372207.3916 | (52138) ← ACK (80) | Seq = 1 Ack = 324 |
| 15.672711000 | (52138) ← PSH, ACK ... (80) | Seq = 1 Ack = 324 |
| 15.672725000 | (52138) ACK → (80) | Seq = 324 Ack = 452 |
| -895706969.7774 | (52139) SYN → (80) | Seq = 0 |
| 15.747286000 | (52139) ← SYN, ACK (80) | Seq = 0 Ack = 1 |
| 714245694.35575 | (52139) ACK → (80) | Seq = 1 Ack = 1 |
| 378319958.96827 | (52139) PSH, ACK ... → (80) | Seq = 1 Ack = 1 |
| 1580695018.4600 | (52139) ← ACK (80) | Seq = 1 Ack = 308 |
| -459410977.0383 | (52139) ← PSH, ACK ... (80) | Seq = 1 Ack = 308 |
| 15.754902000 | (52139) ACK → (80) | Seq = 308 Ack = 505 |
| 20.679013000 | (52138) ← FIN, ACK (80) | Seq = 452 Ack = 324 |
| 609634608.34434 | (52138) ACK → (80) | Seq = 324 Ack = 453 |
| 20.761722000 | (52139) ← FIN, ACK (80) | Seq = 505 Ack = 308 |
| -1931345972.395 | (52139) ACK → (80) | Seq = 308 Ack = 506 |



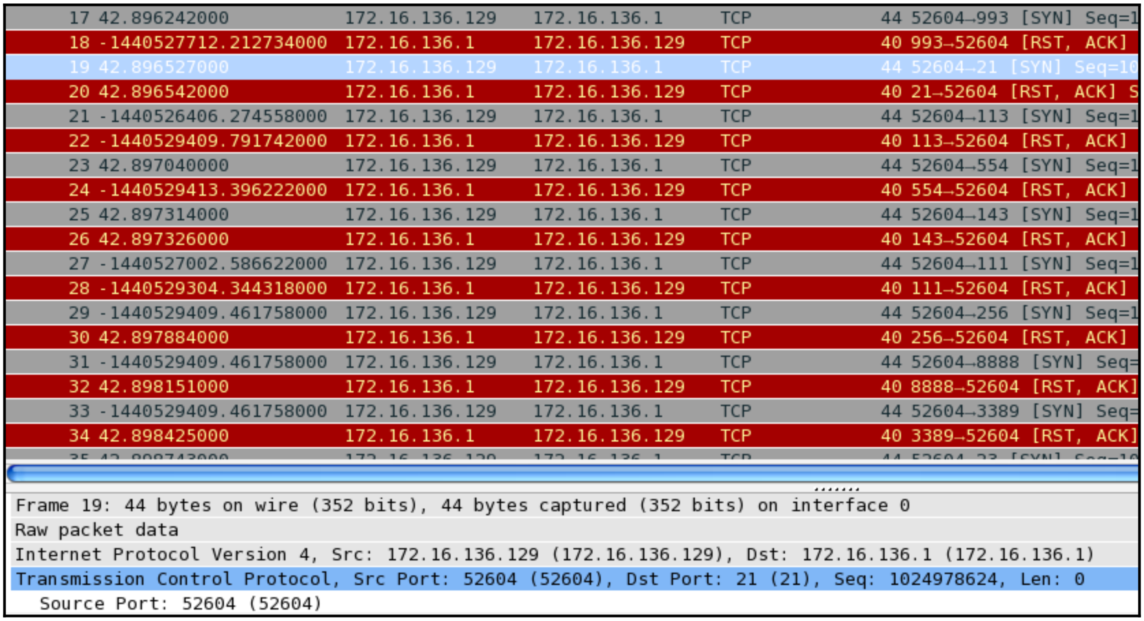
```
▷ Frame 285: 375 bytes on wire (3000 bits), 375 bytes captured (3000 bits) on interface 0
▷ Raw packet data
▷ Internet Protocol Version 4, Src: 172.16.136.1 (172.16.136.1), Dst: 172.16.136.129 (172.16.136.129)
▽ Transmission Control Protocol, Src Port: 52138 (52138), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 323
    Source Port: 52138 (52138)
    Destination Port: 80 (80)
    [Stream index: 7]
    [TCP Segment Len: 323]
    Sequence number: 1    (relative sequence number)
    [Next sequence number: 324    (relative sequence number)]
```



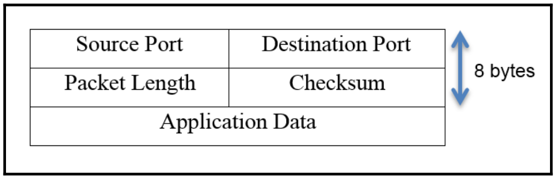
```
77 -1440231980.381381000 172.16.136.1     172.16.136.129   TCP        64 55792→80 [SYN] Seq=0 Win=65535 L
78 13.744839000          172.16.136.129   172.16.136.1     TCP        40 80→55792 [RST, ACK] Seq=1 Ack=1
79 13.745349000          172.16.136.1     172.16.136.129   TCP        64 55793→80 [SYN] Seq=0 Win=65535 L
80 13.745481000          172.16.136.129   172.16.136.1     TCP        40 80→55793 [RST, ACK] Seq=1 Ack=1
97 -1440231980.420122000 172.16.136.1     172.16.136.129   TCP        64 55794→80 [SYN] Seq=0 Win=65535 L
98 27.682014000          172.16.136.129   172.16.136.1     TCP        40 80→55794 [RST, ACK] Seq=1 Ack=1
```

Safari Can’t Connect to the Server

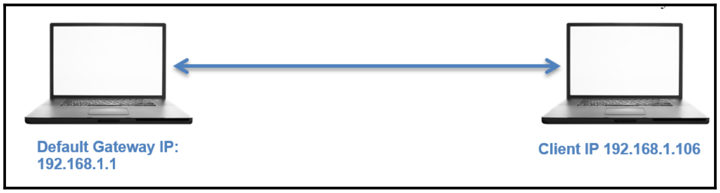
Safari can’t open the page “172.16.136.129” because Safari can’t connect to the server “172.16.136.129”.

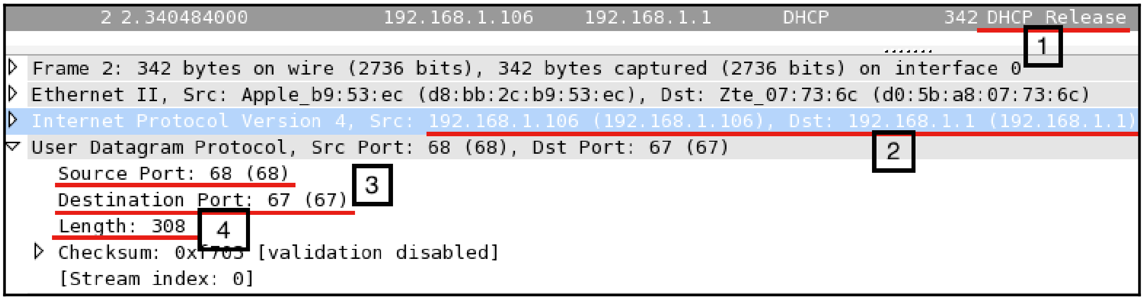


```
17 42.896242000          172.16.136.129   172.16.136.1     TCP        44 52604→993 [SYN] Seq=1
18 -1440527712.212734000 172.16.136.1     172.16.136.129   TCP        40 993→52604 [RST, ACK]
19 42.896527000          172.16.136.129   172.16.136.1     TCP        44 52604→21 [SYN] Seq=10
20 42.896542000          172.16.136.1     172.16.136.129   TCP        40 21→52604 [RST, ACK] S
21 -1440526406.274558000 172.16.136.129   172.16.136.1     TCP        44 52604→113 [SYN] Seq=1
22 -1440529409.791742000 172.16.136.1     172.16.136.129   TCP        40 113→52604 [RST, ACK]
23 42.897040000          172.16.136.129   172.16.136.1     TCP        44 52604→554 [SYN] Seq=1
24 -1440529413.396222000 172.16.136.1     172.16.136.129   TCP        40 554→52604 [RST, ACK]
25 42.897314000          172.16.136.129   172.16.136.1     TCP        44 52604→143 [SYN] Seq=1
26 42.897326000          172.16.136.1     172.16.136.129   TCP        40 143→52604 [RST, ACK]
27 -1440527002.586622000 172.16.136.129   172.16.136.1     TCP        44 52604→111 [SYN] Seq=1
28 -1440529304.344318000 172.16.136.1     172.16.136.129   TCP        40 111→52604 [RST, ACK]
29 -1440529409.461758000 172.16.136.129   172.16.136.1     TCP        44 52604→256 [SYN] Seq=1
30 42.897884000          172.16.136.1     172.16.136.129   TCP        40 256→52604 [RST, ACK]
31 -1440529409.461758000 172.16.136.129   172.16.136.1     TCP        44 52604→8888 [SYN] Seq=
32 42.898151000          172.16.136.1     172.16.136.129   TCP        40 8888→52604 [RST, ACK]
33 -1440529409.461758000 172.16.136.129   172.16.136.1     TCP        44 52604→3389 [SYN] Seq=
34 42.898425000          172.16.136.1     172.16.136.129   TCP        40 3389→52604 [RST, ACK]
35 42.898743000          172.16.136.129   172.16.136.1     TCP        44 52604→23 [SYN] Seq=10

Frame 19: 44 bytes on wire (352 bits), 44 bytes captured (352 bits) on interface 0
Raw packet data
Internet Protocol Version 4, Src: 172.16.136.129 (172.16.136.129), Dst: 172.16.136.1 (172.16.136.1)
Transmission Control Protocol, Src Port: 52604 (52604), Dst Port: 21 (21), Seq: 1024978624, Len: 0
  Source Port: 52604 (52604)
```

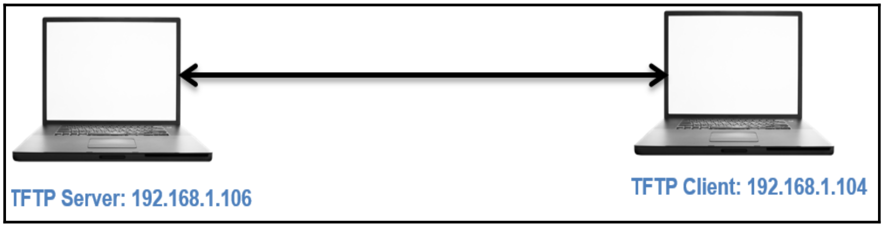


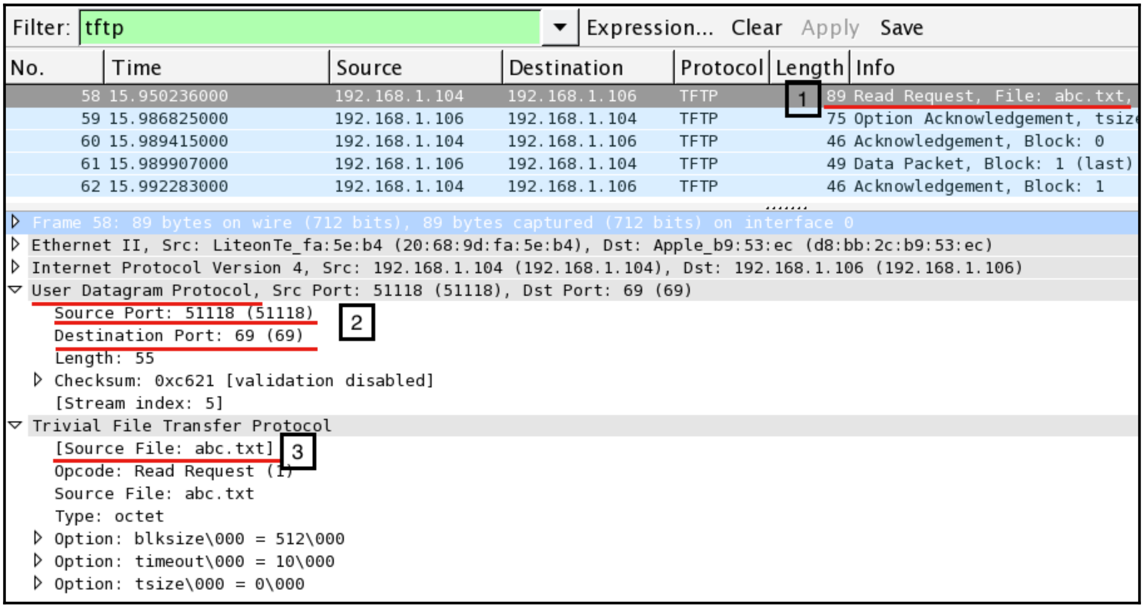
| | |
|---|---|
| Source Port | Destination Port |
| Packet Length | Checksum |
| Application Data | |





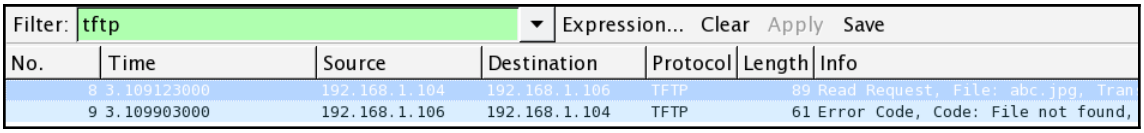
```
        2 2.340484000          192.168.1.106    192.168.1.1      DHCP          342 DHCP Release
▷ Frame 2: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
▷ Ethernet II, Src: Apple_b9:53:ec (d8:bb:2c:b9:53:ec), Dst: Zte_07:73:6c (d0:5b:a8:07:73:6c)
▷ Internet Protocol Version 4, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.1 (192.168.1.1)
▽ User Datagram Protocol, Src Port: 68 (68), Dst Port: 67 (67)
    Source Port: 68 (68)
    Destination Port: 67 (67)
    Length: 308
  ▷ Checksum: 0xf703 [validation disabled]
    [Stream index: 0]
```



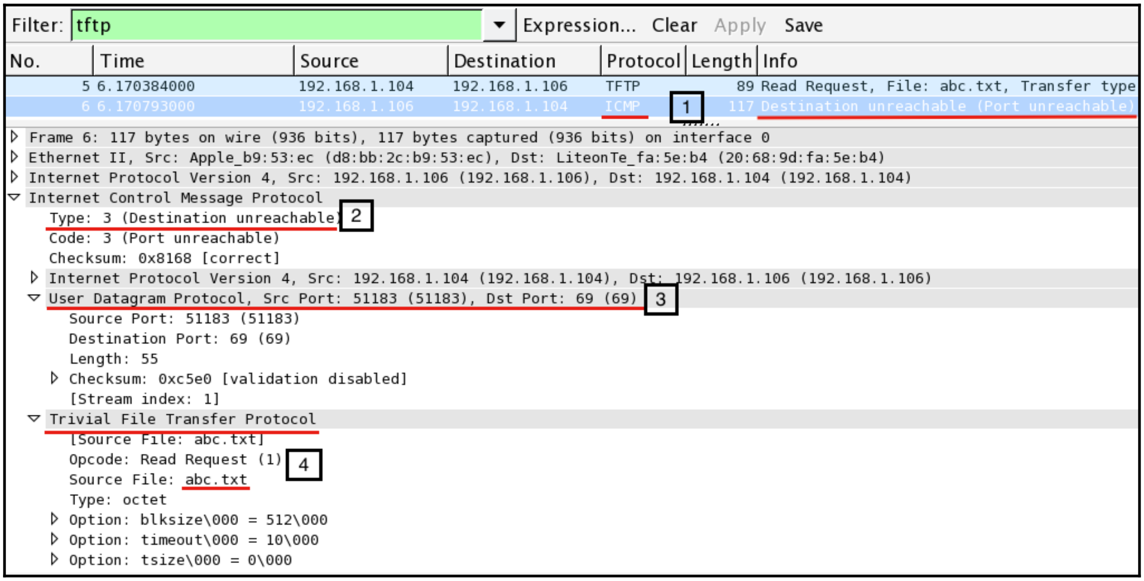


```
No.    Time             Source          Destination     Protocol Length Info
    58 15.950236000     192.168.1.104   192.168.1.106   TFTP         89 Read Request, File: abc.txt,
    59 15.986825000     192.168.1.106   192.168.1.104   TFTP         75 Option Acknowledgement, tsize
    60 15.989415000     192.168.1.104   192.168.1.106   TFTP         46 Acknowledgement, Block: 0
    61 15.989907000     192.168.1.106   192.168.1.104   TFTP         49 Data Packet, Block: 1 (last)
    62 15.992283000     192.168.1.104   192.168.1.106   TFTP         46 Acknowledgement, Block: 1
```

```
▷ Frame 58: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface 0
▷ Ethernet II, Src: LiteonTe_fa:5e:b4 (20:68:9d:fa:5e:b4), Dst: Apple_b9:53:ec (d8:bb:2c:b9:53:ec)
▷ Internet Protocol Version 4, Src: 192.168.1.104 (192.168.1.104), Dst: 192.168.1.106 (192.168.1.106)
▽ User Datagram Protocol, Src Port: 51118 (51118), Dst Port: 69 (69)
    Source Port: 51118 (51118)
    Destination Port: 69 (69)
    Length: 55
  ▷ Checksum: 0xc621 [validation disabled]
    [Stream index: 5]
▽ Trivial File Transfer Protocol
    [Source File: abc.txt]
    Opcode: Read Request (1)
    Source File: abc.txt
    Type: octet
  ▷ Option: blksize\000 = 512\000
  ▷ Option: timeout\000 = 10\000
  ▷ Option: tsize\000 = 0\000
```

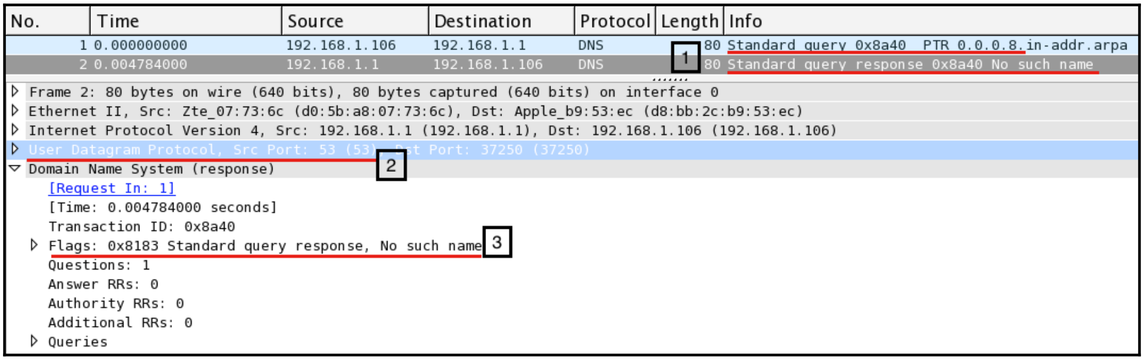


```
No.    Time            Source          Destination     Protocol Length Info
     8 3.109123000     192.168.1.104   192.168.1.106   TFTP         89 Read Request, File: abc.jpg, Tran
     9 3.109903000     192.168.1.106   192.168.1.104   TFTP         61 Error Code, Code: File not found,
```



```
No.    Time            Source          Destination     Protocol Length Info
     5 6.170384000     192.168.1.104   192.168.1.106   TFTP         89 Read Request, File: abc.txt, Transfer type
     6 6.170793000     192.168.1.106   192.168.1.104   ICMP        117 Destination unreachable (Port unreachable)
```

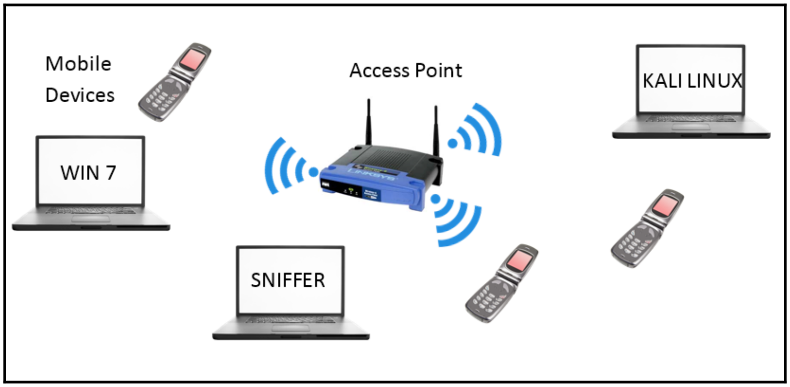
```
▷ Frame 6: 117 bytes on wire (936 bits), 117 bytes captured (936 bits) on interface 0
▷ Ethernet II, Src: Apple_b9:53:ec (d8:bb:2c:b9:53:ec), Dst: LiteonTe_fa:5e:b4 (20:68:9d:fa:5e:b4)
▷ Internet Protocol Version 4, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.104 (192.168.1.104)
▽ Internet Control Message Protocol
    Type: 3 (Destination unreachable)
    Code: 3 (Port unreachable)
    Checksum: 0x8168 [correct]
  ▷ Internet Protocol Version 4, Src: 192.168.1.104 (192.168.1.104), Dst: 192.168.1.106 (192.168.1.106)
  ▽ User Datagram Protocol, Src Port: 51183 (51183), Dst Port: 69 (69)
      Source Port: 51183 (51183)
      Destination Port: 69 (69)
      Length: 55
    ▷ Checksum: 0xc5e0 [validation disabled]
      [Stream index: 1]
  ▽ Trivial File Transfer Protocol
      [Source File: abc.txt]
      Opcode: Read Request (1)
      Source File: abc.txt
      Type: octet
    ▷ Option: blksize\000 = 512\000
    ▷ Option: timeout\000 = 10\000
    ▷ Option: tsize\000 = 0\000
```

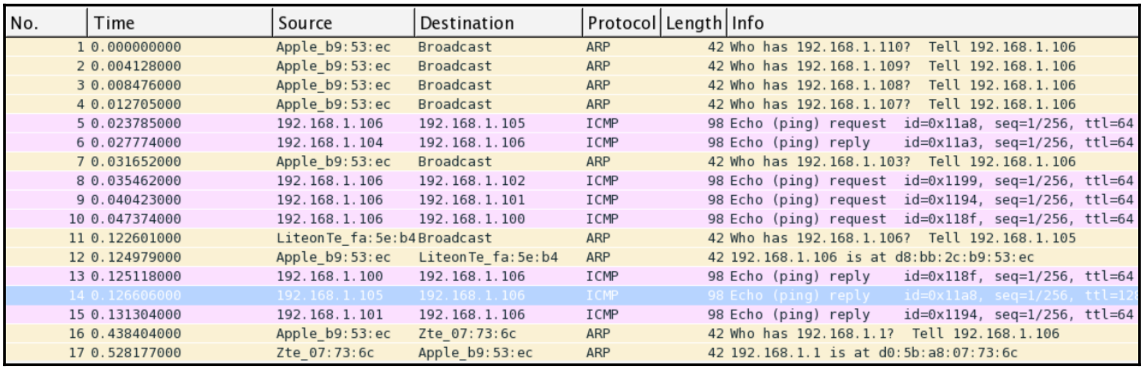


| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 1 | 0.000000000 | 192.168.1.106 | 192.168.1.1 | DNS | 80 | Standard query 0x8a40  PTR 0.0.0.8.in-addr.arpa |
| 2 | 0.004784000 | 192.168.1.1 | 192.168.1.106 | DNS | 80 | Standard query response 0x8a40 No such name |

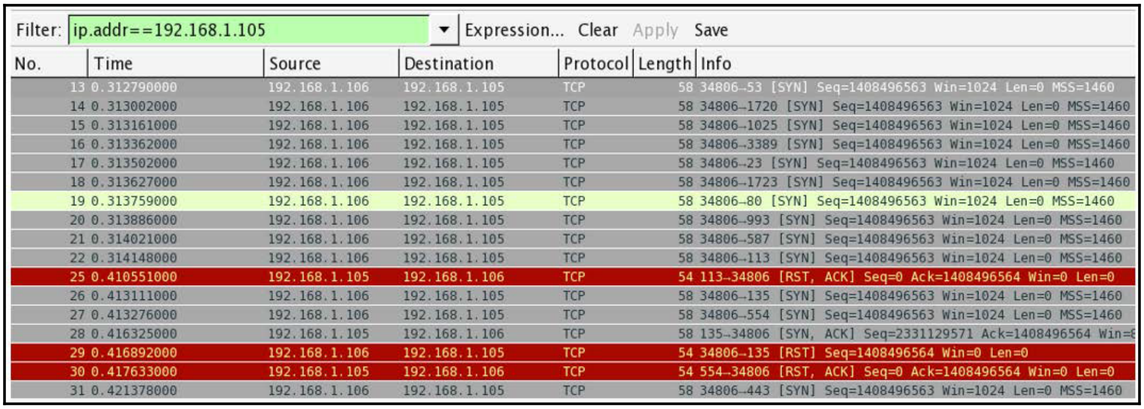
```
▷ Frame 2: 80 bytes on wire (640 bits), 80 bytes captured (640 bits) on interface 0
▷ Ethernet II, Src: Zte_07:73:6c (d0:5b:a8:07:73:6c), Dst: Apple_b9:53:ec (d8:bb:2c:b9:53:ec)
▷ Internet Protocol Version 4, Src: 192.168.1.1 (192.168.1.1), Dst: 192.168.1.106 (192.168.1.106)
▷ User Datagram Protocol, Src Port: 53 (53), Dst Port: 37250 (37250)
▽ Domain Name System (response)
    [Request In: 1]
    [Time: 0.004784000 seconds]
    Transaction ID: 0x8a40
  ▷ Flags: 0x8183 Standard query response, No such name
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▷ Queries
```

# Chapter 6: Network Security Packet Analysis



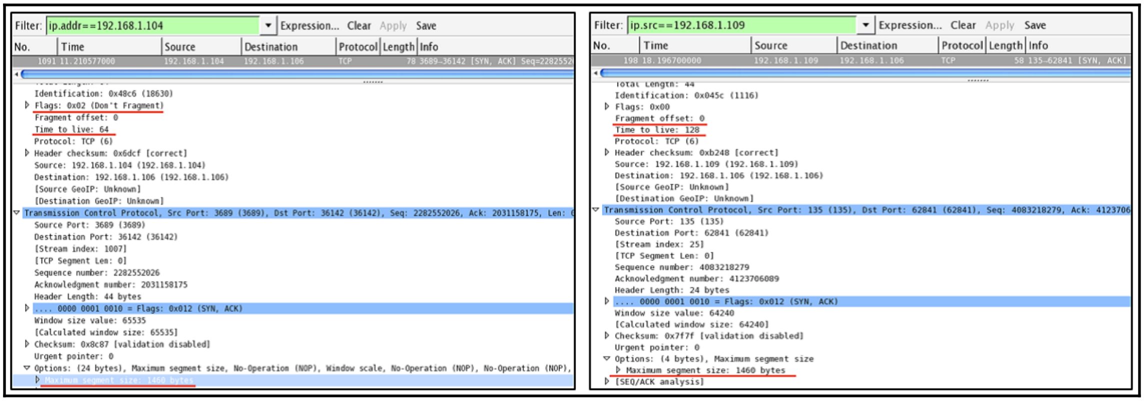


| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 1 | 0.000000000 | Apple_b9:53:ec | Broadcast | ARP | 42 | Who has 192.168.1.110? Tell 192.168.1.106 |
| 2 | 0.004128000 | Apple_b9:53:ec | Broadcast | ARP | 42 | Who has 192.168.1.109? Tell 192.168.1.106 |
| 3 | 0.008476000 | Apple_b9:53:ec | Broadcast | ARP | 42 | Who has 192.168.1.108? Tell 192.168.1.106 |
| 4 | 0.012705000 | Apple_b9:53:ec | Broadcast | ARP | 42 | Who has 192.168.1.107? Tell 192.168.1.106 |
| 5 | 0.023785000 | 192.168.1.106 | 192.168.1.105 | ICMP | 98 | Echo (ping) request id=0x11a8, seq=1/256, ttl=64 |
| 6 | 0.027774000 | 192.168.1.104 | 192.168.1.106 | ICMP | 98 | Echo (ping) reply id=0x11a3, seq=1/256, ttl=64 |
| 7 | 0.031652000 | Apple_b9:53:ec | Broadcast | ARP | 42 | Who has 192.168.1.103? Tell 192.168.1.106 |
| 8 | 0.035462000 | 192.168.1.106 | 192.168.1.102 | ICMP | 98 | Echo (ping) request id=0x1199, seq=1/256, ttl=64 |
| 9 | 0.040423000 | 192.168.1.106 | 192.168.1.101 | ICMP | 98 | Echo (ping) request id=0x1194, seq=1/256, ttl=64 |
| 10 | 0.047374000 | 192.168.1.106 | 192.168.1.100 | ICMP | 98 | Echo (ping) request id=0x118f, seq=1/256, ttl=64 |
| 11 | 0.122601000 | LiteonTe_fa:5e:b4 | Broadcast | ARP | 42 | Who has 192.168.1.106? Tell 192.168.1.105 |
| 12 | 0.124979000 | Apple_b9:53:ec | LiteonTe_fa:5e:b4 | ARP | 42 | 192.168.1.106 is at d8:bb:2c:b9:53:ec |
| 13 | 0.125118000 | 192.168.1.100 | 192.168.1.106 | ICMP | 98 | Echo (ping) reply id=0x118f, seq=1/256, ttl=64 |
| 14 | 0.126606000 | 192.168.1.105 | 192.168.1.106 | ICMP | 98 | Echo (ping) reply id=0x11a8, seq=1/256, ttl=12 |
| 15 | 0.131304000 | 192.168.1.101 | 192.168.1.106 | ICMP | 98 | Echo (ping) reply id=0x1194, seq=1/256, ttl=64 |
| 16 | 0.438404000 | Apple_b9:53:ec | Zte_07:73:6c | ARP | 42 | Who has 192.168.1.1? Tell 192.168.1.106 |
| 17 | 0.528177000 | Zte_07:73:6c | Apple_b9:53:ec | ARP | 42 | 192.168.1.1 is at d0:5b:a8:07:73:6c |



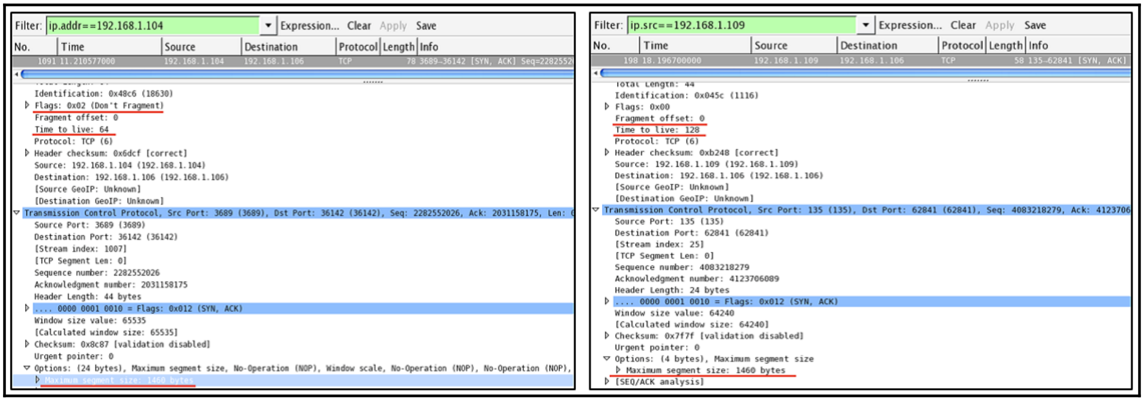
Filter: ip.addr==192.168.1.105 ▾ Expression... Clear Apply Save

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 13 | 0.312790000 | 192.168.1.106 | 192.168.1.105 | TCP | 58 | 34806→53 [SYN] Seq=1408496563 Win=1024 Len=0 MSS=1460 |
| 14 | 0.313002000 | 192.168.1.106 | 192.168.1.105 | TCP | 58 | 34806→1720 [SYN] Seq=1408496563 Win=1024 Len=0 MSS=1460 |
| 15 | 0.313161000 | 192.168.1.106 | 192.168.1.105 | TCP | 58 | 34806→1025 [SYN] Seq=1408496563 Win=1024 Len=0 MSS=1460 |
| 16 | 0.313362000 | 192.168.1.106 | 192.168.1.105 | TCP | 58 | 34806→3389 [SYN] Seq=1408496563 Win=1024 Len=0 MSS=1460 |
| 17 | 0.313502000 | 192.168.1.106 | 192.168.1.105 | TCP | 58 | 34806→23 [SYN] Seq=1408496563 Win=1024 Len=0 MSS=1460 |
| 18 | 0.313627000 | 192.168.1.106 | 192.168.1.105 | TCP | 58 | 34806→1723 [SYN] Seq=1408496563 Win=1024 Len=0 MSS=1460 |
| 19 | 0.313759000 | 192.168.1.106 | 192.168.1.105 | TCP | 58 | 34806→80 [SYN] Seq=1408496563 Win=1024 Len=0 MSS=1460 |
| 20 | 0.313886000 | 192.168.1.106 | 192.168.1.105 | TCP | 58 | 34806→993 [SYN] Seq=1408496563 Win=1024 Len=0 MSS=1460 |
| 21 | 0.314021000 | 192.168.1.106 | 192.168.1.105 | TCP | 58 | 34806→587 [SYN] Seq=1408496563 Win=1024 Len=0 MSS=1460 |
| 22 | 0.314148000 | 192.168.1.106 | 192.168.1.105 | TCP | 58 | 34806→113 [SYN] Seq=1408496563 Win=1024 Len=0 MSS=1460 |
| 25 | 0.410551000 | 192.168.1.105 | 192.168.1.106 | TCP | 54 | 113→34806 [RST, ACK] Seq=0 Ack=1408496564 Win=0 Len=0 |
| 26 | 0.413111000 | 192.168.1.106 | 192.168.1.105 | TCP | 58 | 34806→135 [SYN] Seq=1408496563 Win=1024 Len=0 MSS=1460 |
| 27 | 0.413276000 | 192.168.1.106 | 192.168.1.105 | TCP | 58 | 34806→554 [SYN] Seq=1408496563 Win=1024 Len=0 MSS=1460 |
| 28 | 0.416325000 | 192.168.1.105 | 192.168.1.106 | TCP | 58 | 135→34806 [SYN, ACK] Seq=2331129571 Ack=1408496564 Win= |
| 29 | 0.416892000 | 192.168.1.106 | 192.168.1.105 | TCP | 54 | 34806→135 [RST] Seq=1408496564 Win=0 Len=0 |
| 30 | 0.417633000 | 192.168.1.105 | 192.168.1.106 | TCP | 54 | 554→34806 [RST, ACK] Seq=0 Ack=1408496564 Win=0 Len=0 |
| 31 | 0.421378000 | 192.168.1.106 | 192.168.1.105 | TCP | 58 | 34806→443 [SYN] Seq=1408496563 Win=1024 Len=0 MSS=1460 |



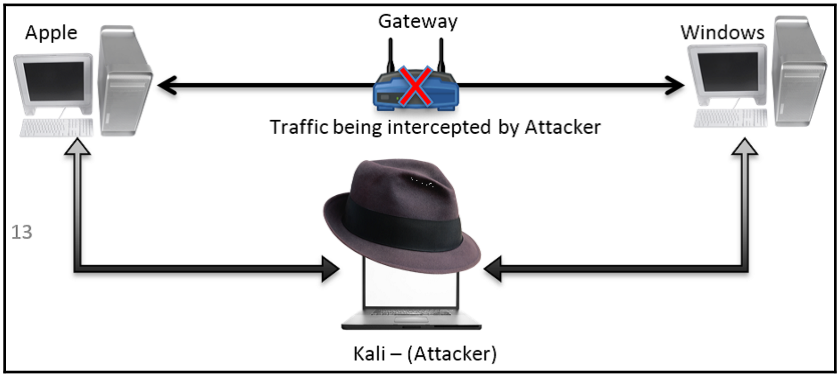
```
Filter: ip.addr==192.168.1.104          Expression...  Clear  Apply  Save
No.   Time          Source         Destination    Protocol Length Info
 1091 11.210577000  192.168.1.104  192.168.1.106  TCP          78 3689→36142 [SYN, ACK] Seq=2282552
    Identification: 0x48c6 (18630)
  ▷ Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (6)
  ▷ Header checksum: 0x6dcf [correct]
    Source: 192.168.1.104 (192.168.1.104)
    Destination: 192.168.1.106 (192.168.1.106)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
▽ Transmission Control Protocol, Src Port: 3689 (3689), Dst Port: 36142 (36142), Seq: 2282552026, Ack: 2031158175, Len: 
    Source Port: 3689 (3689)
    Destination Port: 36142 (36142)
    [Stream index: 1007]
    [TCP Segment Len: 0]
    Sequence number: 2282552026
    Acknowledgment number: 2031158175
    Header Length: 44 bytes
  ▷ .... 0000 0001 0010 = Flags: 0x012 (SYN, ACK)
    Window size value: 65535
    [Calculated window size: 65535]
  ▷ Checksum: 0x8c87 [validation disabled]
    Urgent pointer: 0
  ▽ Options: (24 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP),
    ▷ Maximum segment size: 1460 bytes
```

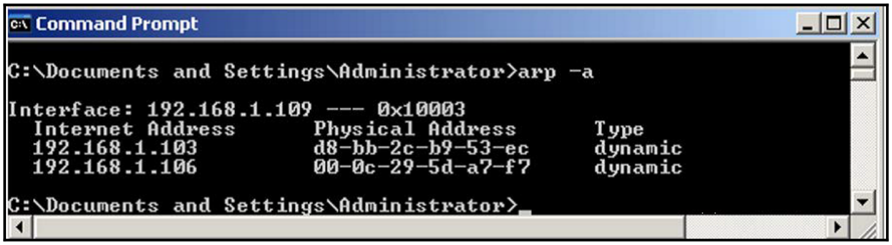
```
Filter: ip.src==192.168.1.109           Expression...  Clear  Apply  Save
No.   Time          Source         Destination    Protocol Length Info
  198 18.196700000  192.168.1.109  192.168.1.106  TCP          58 135→62841 [SYN, ACK]
    Total Length: 44
    Identification: 0x045c (1116)
  ▷ Flags: 0x00
    Fragment offset: 0
    Time to live: 128
    Protocol: TCP (6)
  ▷ Header checksum: 0xb248 [correct]
    Source: 192.168.1.109 (192.168.1.109)
    Destination: 192.168.1.106 (192.168.1.106)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
▽ Transmission Control Protocol, Src Port: 135 (135), Dst Port: 62841 (62841), Seq: 4083218279, Ack: 4123706
    Source Port: 135 (135)
    Destination Port: 62841 (62841)
    [Stream index: 25]
    [TCP Segment Len: 0]
    Sequence number: 4083218279
    Acknowledgment number: 4123706089
    Header Length: 24 bytes
  ▷ .... 0000 0001 0010 = Flags: 0x012 (SYN, ACK)
    Window size value: 64240
    [Calculated window size: 64240]
  ▷ Checksum: 0x7f7f [validation disabled]
    Urgent pointer: 0
  ▽ Options: (4 bytes), Maximum segment size
    ▷ Maximum segment size: 1460 bytes
  ▷ [SEQ/ACK analysis]
```



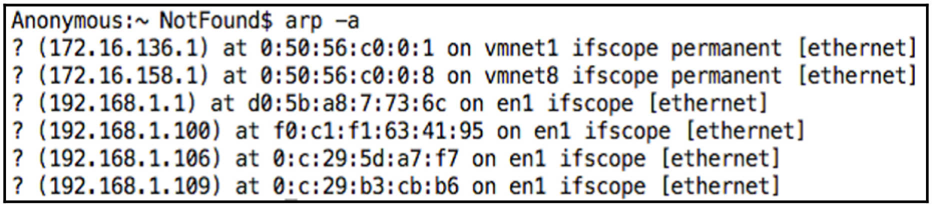
```
Filter: ip.addr==192.168.1.104          Expression...  Clear  Apply  Save
No.   Time          Source         Destination    Protocol Length Info
 1091 11.210577000  192.168.1.104  192.168.1.106  TCP          78 3689→36142 [SYN, ACK] Seq=2282552
    Identification: 0x48c6 (18630)
  ▷ Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (6)
  ▷ Header checksum: 0x6dcf [correct]
    Source: 192.168.1.104 (192.168.1.104)
    Destination: 192.168.1.106 (192.168.1.106)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
▽ Transmission Control Protocol, Src Port: 3689 (3689), Dst Port: 36142 (36142), Seq: 2282552026, Ack: 2031158175, Len: 
    Source Port: 3689 (3689)
    Destination Port: 36142 (36142)
    [Stream index: 1007]
    [TCP Segment Len: 0]
    Sequence number: 2282552026
    Acknowledgment number: 2031158175
    Header Length: 44 bytes
  ▷ .... 0000 0001 0010 = Flags: 0x012 (SYN, ACK)
    Window size value: 65535
    [Calculated window size: 65535]
  ▷ Checksum: 0x8c87 [validation disabled]
    Urgent pointer: 0
  ▽ Options: (24 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP),
    ▷ Maximum segment size: 1460 bytes
```

```
Filter: ip.src==192.168.1.109           Expression...  Clear  Apply  Save
No.   Time          Source         Destination    Protocol Length Info
  198 18.196700000  192.168.1.109  192.168.1.106  TCP          58 135→62841 [SYN, ACK]
    Total Length: 44
    Identification: 0x045c (1116)
  ▷ Flags: 0x00
    Fragment offset: 0
    Time to live: 128
    Protocol: TCP (6)
  ▷ Header checksum: 0xb248 [correct]
    Source: 192.168.1.109 (192.168.1.109)
    Destination: 192.168.1.106 (192.168.1.106)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
▽ Transmission Control Protocol, Src Port: 135 (135), Dst Port: 62841 (62841), Seq: 4083218279, Ack: 4123706
    Source Port: 135 (135)
    Destination Port: 62841 (62841)
    [Stream index: 25]
    [TCP Segment Len: 0]
    Sequence number: 4083218279
    Acknowledgment number: 4123706089
    Header Length: 24 bytes
  ▷ .... 0000 0001 0010 = Flags: 0x012 (SYN, ACK)
    Window size value: 64240
    [Calculated window size: 64240]
  ▷ Checksum: 0x7f7f [validation disabled]
    Urgent pointer: 0
  ▽ Options: (4 bytes), Maximum segment size
    ▷ Maximum segment size: 1460 bytes
  ▷ [SEQ/ACK analysis]
```

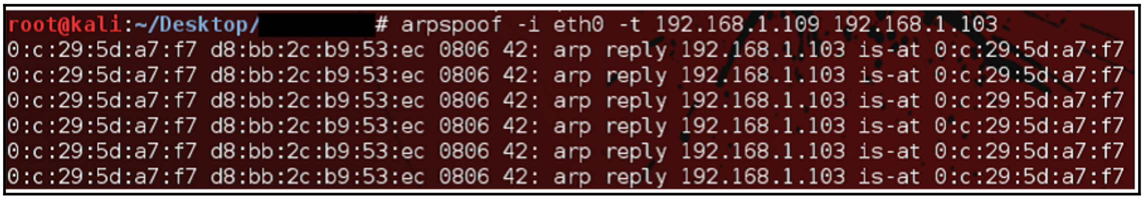




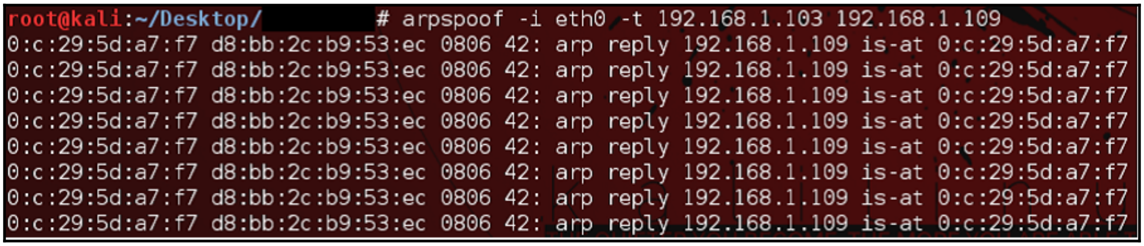
```
C:\Documents and Settings\Administrator>arp -a

Interface: 192.168.1.109 --- 0x10003
  Internet Address      Physical Address      Type
  192.168.1.103         d8-bb-2c-b9-53-ec     dynamic
  192.168.1.106         00-0c-29-5d-a7-f7     dynamic

C:\Documents and Settings\Administrator>_
```



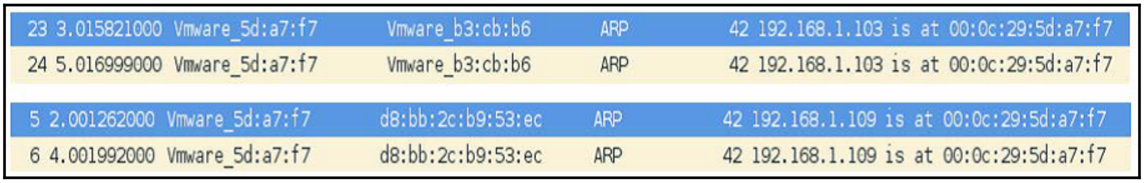
```
Anonymous:~ NotFound$ arp -a
? (172.16.136.1) at 0:50:56:c0:0:1 on vmnet1 ifscope permanent [ethernet]
? (172.16.158.1) at 0:50:56:c0:0:8 on vmnet8 ifscope permanent [ethernet]
? (192.168.1.1) at d0:5b:a8:7:73:6c on en1 ifscope [ethernet]
? (192.168.1.100) at f0:c1:f1:63:41:95 on en1 ifscope [ethernet]
? (192.168.1.106) at 0:c:29:5d:a7:f7 on en1 ifscope [ethernet]
? (192.168.1.109) at 0:c:29:b3:cb:b6 on en1 ifscope [ethernet]
```



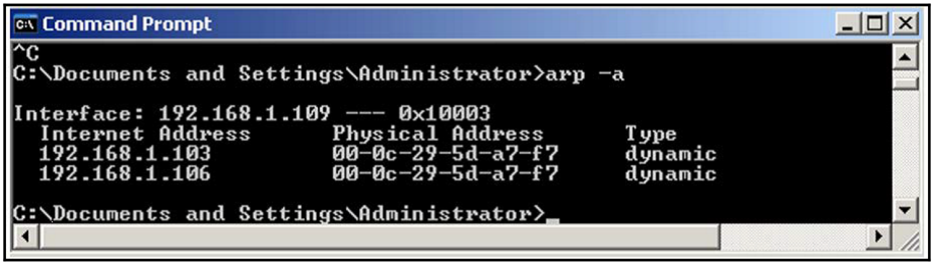
```
root@kali:~/Desktop/[redacted]# arpspoof -i eth0 -t 192.168.1.109 192.168.1.103
0:c:29:5d:a7:f7 d8:bb:2c:b9:53:ec 0806 42: arp reply 192.168.1.103 is-at 0:c:29:5d:a7:f7
0:c:29:5d:a7:f7 d8:bb:2c:b9:53:ec 0806 42: arp reply 192.168.1.103 is-at 0:c:29:5d:a7:f7
0:c:29:5d:a7:f7 d8:bb:2c:b9:53:ec 0806 42: arp reply 192.168.1.103 is-at 0:c:29:5d:a7:f7
0:c:29:5d:a7:f7 d8:bb:2c:b9:53:ec 0806 42: arp reply 192.168.1.103 is-at 0:c:29:5d:a7:f7
0:c:29:5d:a7:f7 d8:bb:2c:b9:53:ec 0806 42: arp reply 192.168.1.103 is-at 0:c:29:5d:a7:f7
0:c:29:5d:a7:f7 d8:bb:2c:b9:53:ec 0806 42: arp reply 192.168.1.103 is-at 0:c:29:5d:a7:f7
```



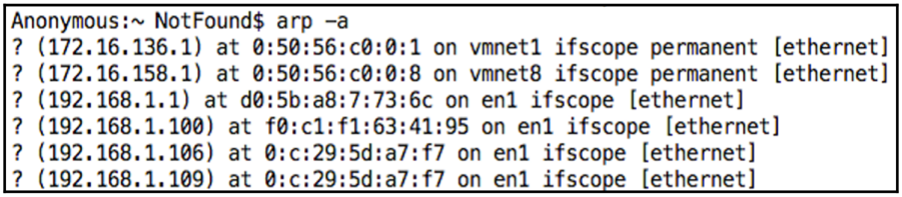
```
root@kali:~/Desktop/[redacted]# arpspoof -i eth0 -t 192.168.1.103 192.168.1.109
0:c:29:5d:a7:f7 d8:bb:2c:b9:53:ec 0806 42: arp reply 192.168.1.109 is-at 0:c:29:5d:a7:f7
0:c:29:5d:a7:f7 d8:bb:2c:b9:53:ec 0806 42: arp reply 192.168.1.109 is-at 0:c:29:5d:a7:f7
0:c:29:5d:a7:f7 d8:bb:2c:b9:53:ec 0806 42: arp reply 192.168.1.109 is-at 0:c:29:5d:a7:f7
0:c:29:5d:a7:f7 d8:bb:2c:b9:53:ec 0806 42: arp reply 192.168.1.109 is-at 0:c:29:5d:a7:f7
0:c:29:5d:a7:f7 d8:bb:2c:b9:53:ec 0806 42: arp reply 192.168.1.109 is-at 0:c:29:5d:a7:f7
0:c:29:5d:a7:f7 d8:bb:2c:b9:53:ec 0806 42: arp reply 192.168.1.109 is-at 0:c:29:5d:a7:f7
0:c:29:5d:a7:f7 d8:bb:2c:b9:53:ec 0806 42: arp reply 192.168.1.109 is-at 0:c:29:5d:a7:f7
0:c:29:5d:a7:f7 d8:bb:2c:b9:53:ec 0806 42: arp reply 192.168.1.109 is-at 0:c:29:5d:a7:f7
```



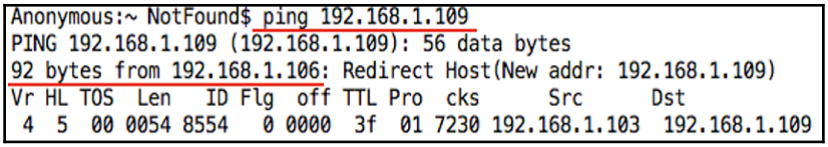
```
23 3.015821000 Vmware_5d:a7:f7    Vmware_b3:cb:b6    ARP    42 192.168.1.103 is at 00:0c:29:5d:a7:f7
24 5.016999000 Vmware_5d:a7:f7    Vmware_b3:cb:b6    ARP    42 192.168.1.103 is at 00:0c:29:5d:a7:f7

 5 2.001262000 Vmware_5d:a7:f7    d8:bb:2c:b9:53:ec  ARP    42 192.168.1.109 is at 00:0c:29:5d:a7:f7
 6 4.001992000 Vmware_5d:a7:f7    d8:bb:2c:b9:53:ec  ARP    42 192.168.1.109 is at 00:0c:29:5d:a7:f7
```



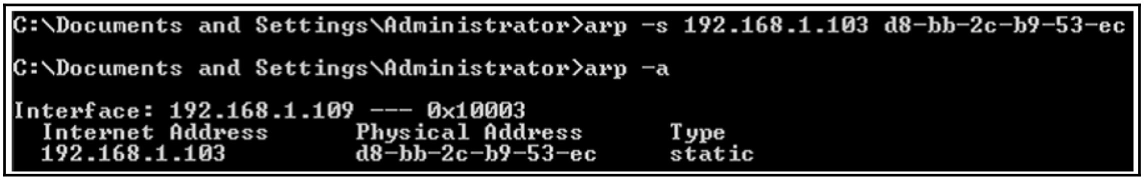
```
^C
C:\Documents and Settings\Administrator>arp -a

Interface: 192.168.1.109 --- 0x10003
  Internet Address      Physical Address      Type
  192.168.1.103         00-0c-29-5d-a7-f7     dynamic
  192.168.1.106         00-0c-29-5d-a7-f7     dynamic

C:\Documents and Settings\Administrator>_
```



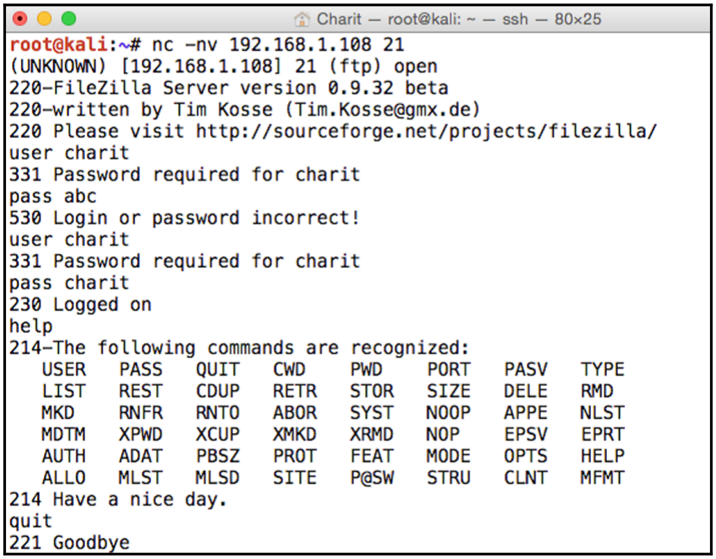
```
Anonymous:~ NotFound$ arp -a
? (172.16.136.1) at 0:50:56:c0:0:1 on vmnet1 ifscope permanent [ethernet]
? (172.16.158.1) at 0:50:56:c0:0:8 on vmnet8 ifscope permanent [ethernet]
? (192.168.1.1) at d0:5b:a8:7:73:6c on en1 ifscope [ethernet]
? (192.168.1.100) at f0:c1:f1:63:41:95 on en1 ifscope [ethernet]
? (192.168.1.106) at 0:c:29:5d:a7:f7 on en1 ifscope [ethernet]
? (192.168.1.109) at 0:c:29:5d:a7:f7 on en1 ifscope [ethernet]
```



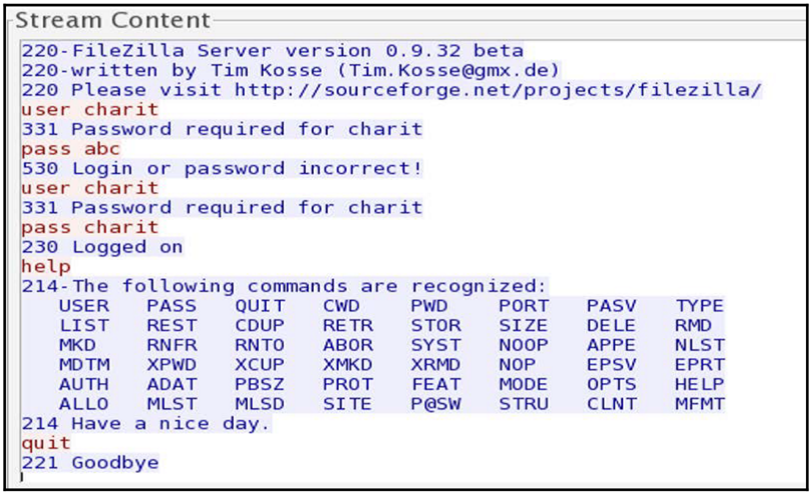
```
Anonymous:~ NotFound$ ping 192.168.1.109
PING 192.168.1.109 (192.168.1.109): 56 data bytes
92 bytes from 192.168.1.106: Redirect Host(New addr: 192.168.1.109)
Vr HL TOS  Len   ID Flg  off TTL Pro  cks      Src      Dst
 4  5  00 0054 8554   0 0000  3f  01 7230 192.168.1.103  192.168.1.109
```



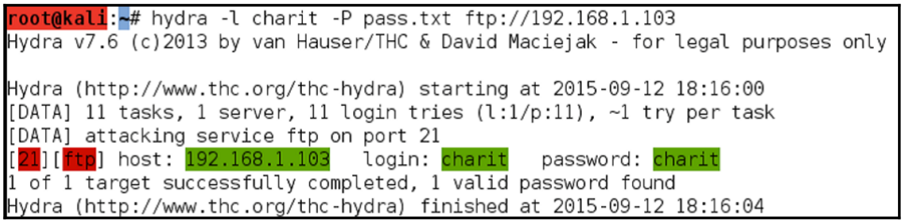
```
C:\Documents and Settings\Administrator>arp -s 192.168.1.103 d8-bb-2c-b9-53-ec

C:\Documents and Settings\Administrator>arp -a

Interface: 192.168.1.109 --- 0x10003
  Internet Address      Physical Address      Type
  192.168.1.103         d8-bb-2c-b9-53-ec     static
```



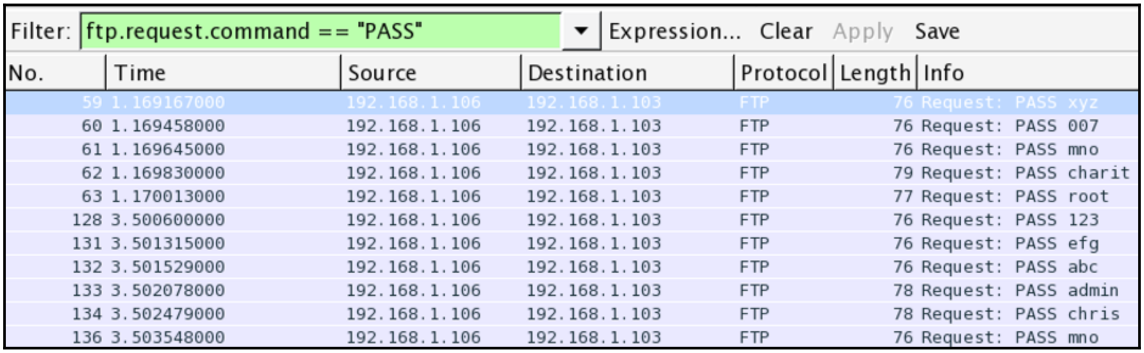
```
root@kali:~# nc -nv 192.168.1.108 21
(UNKNOWN) [192.168.1.108] 21 (ftp) open
220-FileZilla Server version 0.9.32 beta
220-written by Tim Kosse (Tim.Kosse@gmx.de)
220 Please visit http://sourceforge.net/projects/filezilla/
user charit
331 Password required for charit
pass abc
530 Login or password incorrect!
user charit
331 Password required for charit
pass charit
230 Logged on
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
214 Have a nice day.
quit
221 Goodbye
```



```
220-FileZilla Server version 0.9.32 beta
220-written by Tim Kosse (Tim.Kosse@gmx.de)
220 Please visit http://sourceforge.net/projects/filezilla/
user charit
331 Password required for charit
pass abc
530 Login or password incorrect!
user charit
331 Password required for charit
pass charit
230 Logged on
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
214 Have a nice day.
quit
221 Goodbye
```

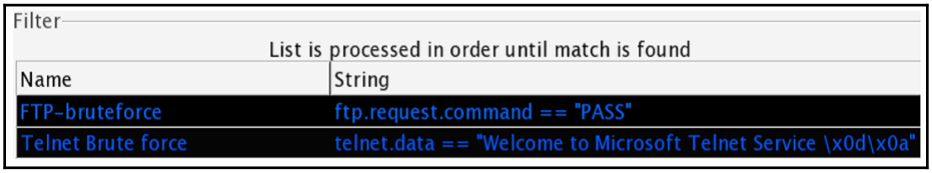


```
root@kali:~# hydra -l charit -P pass.txt ftp://192.168.1.103
Hydra v7.6 (c)2013 by van Hauser/THC & David Maciejak - for legal purposes only

Hydra (http://www.thc.org/thc-hydra) starting at 2015-09-12 18:16:00
[DATA] 11 tasks, 1 server, 11 login tries (l:1/p:11), ~1 try per task
[DATA] attacking service ftp on port 21
[21][ftp] host: 192.168.1.103   login: charit   password: charit
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2015-09-12 18:16:04
```



Filter: ftp.request.command == "PASS"

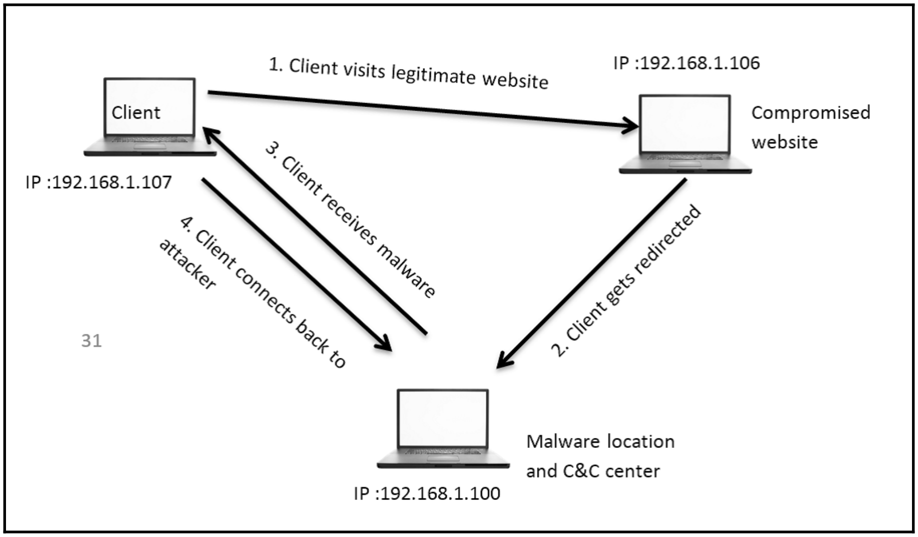
| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 59 | 1.169167000 | 192.168.1.106 | 192.168.1.103 | FTP | 76 | Request: PASS xyz |
| 60 | 1.169458000 | 192.168.1.106 | 192.168.1.103 | FTP | 76 | Request: PASS 007 |
| 61 | 1.169645000 | 192.168.1.106 | 192.168.1.103 | FTP | 76 | Request: PASS mno |
| 62 | 1.169830000 | 192.168.1.106 | 192.168.1.103 | FTP | 79 | Request: PASS charit |
| 63 | 1.170013000 | 192.168.1.106 | 192.168.1.103 | FTP | 77 | Request: PASS root |
| 128 | 3.500600000 | 192.168.1.106 | 192.168.1.103 | FTP | 76 | Request: PASS 123 |
| 131 | 3.501315000 | 192.168.1.106 | 192.168.1.103 | FTP | 76 | Request: PASS efg |
| 132 | 3.501529000 | 192.168.1.106 | 192.168.1.103 | FTP | 76 | Request: PASS abc |
| 133 | 3.502078000 | 192.168.1.106 | 192.168.1.103 | FTP | 78 | Request: PASS admin |
| 134 | 3.502479000 | 192.168.1.106 | 192.168.1.103 | FTP | 78 | Request: PASS chris |
| 136 | 3.503548000 | 192.168.1.106 | 192.168.1.103 | FTP | 76 | Request: PASS mno |



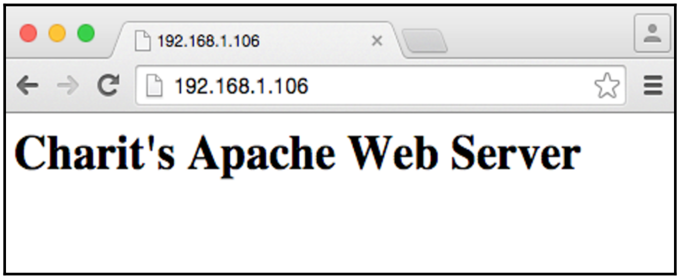
Filter

List is processed in order until match is found

| Name | String |
|---|---|
| FTP-bruteforce | ftp.request.command == "PASS" |
| Telnet Brute force | telnet.data == "Welcome to Microsoft Telnet Service \x0d\x0a" |



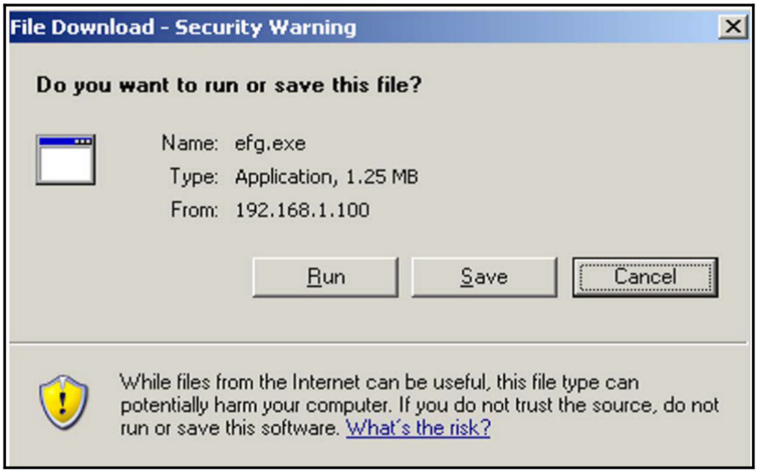
Client
IP :192.168.1.107
1. Client visits legitimate website
IP :192.168.1.106
Compromised website
2. Client gets redirected
3. Client receives malware
4. Client connects back to attacker
Malware location and C&C center
IP :192.168.1.100



192.168.1.106

192.168.1.106

Charit's Apache Web Server



File Download - Security Warning

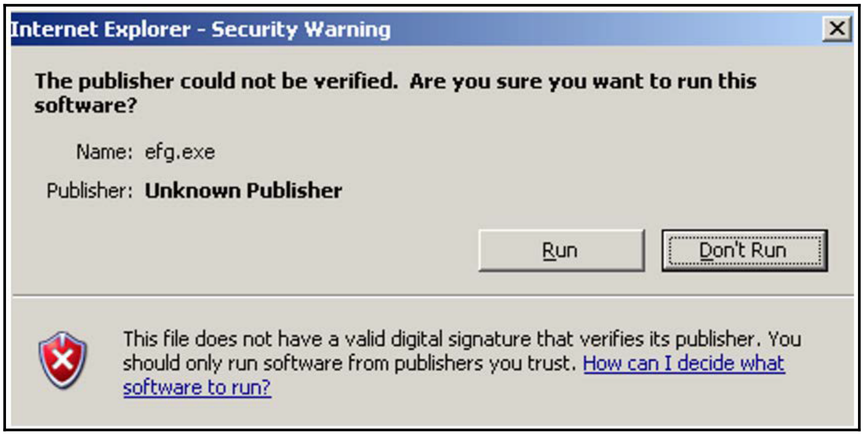
Do you want to run or save this file?

Name: efg.exe

Type: Application, 1.25 MB

From: 192.168.1.100

While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not run or save this software. What's the risk?



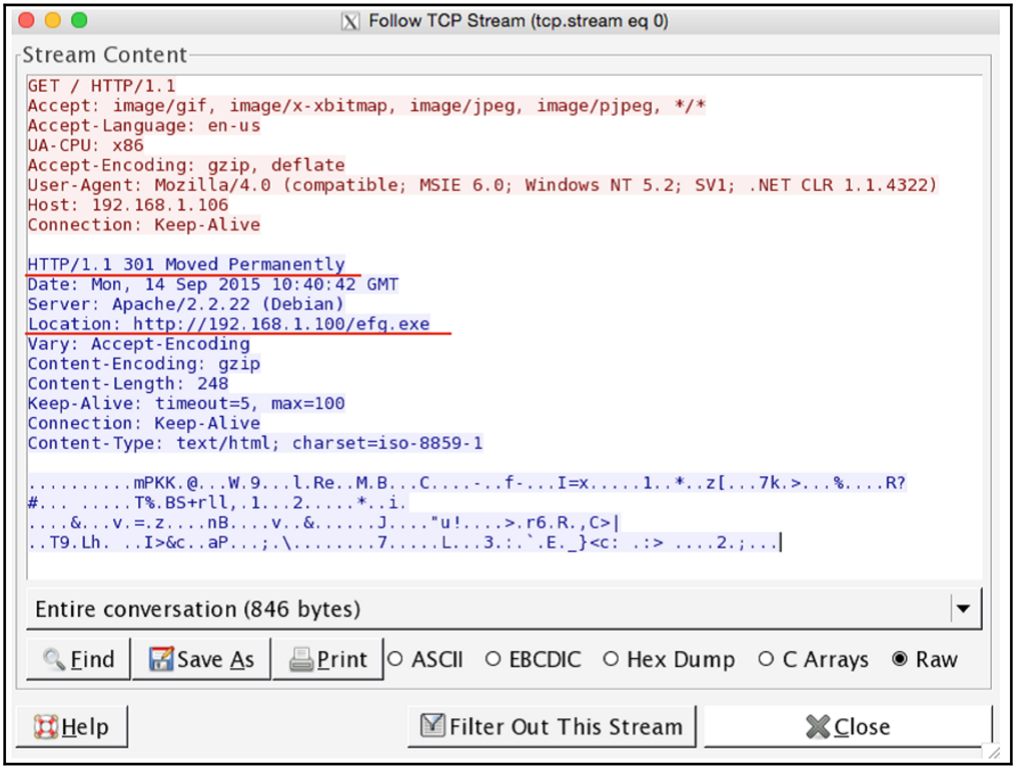
Internet Explorer - Security Warning

The publisher could not be verified. Are you sure you want to run this software?

Name: efg.exe

Publisher: **Unknown Publisher**

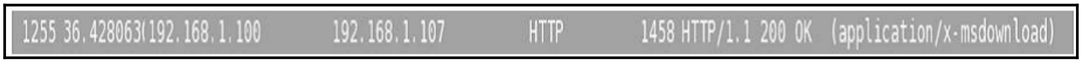
This file does not have a valid digital signature that verifies its publisher. You should only run software from publishers you trust. How can I decide what software to run?



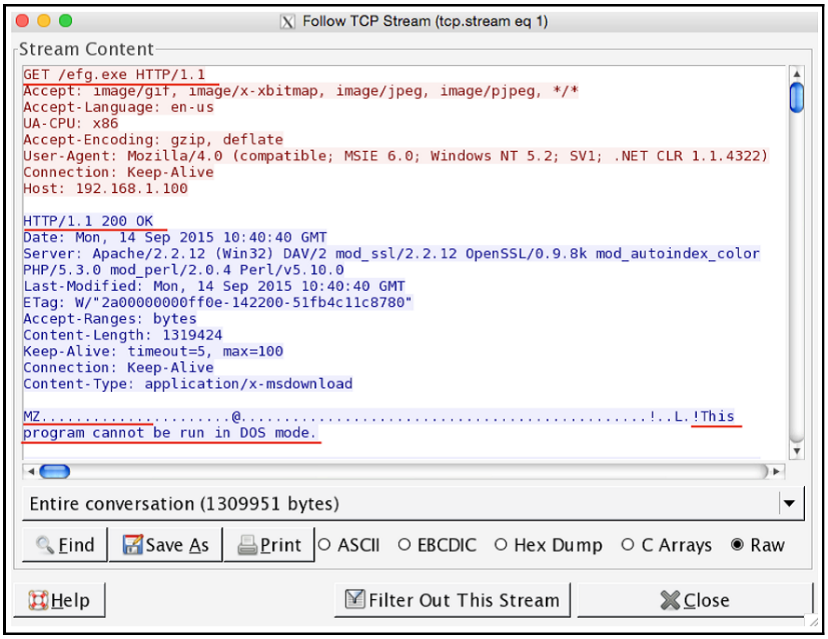
```
GET / HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, */*
Accept-Language: en-us
UA-CPU: x86
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; SV1; .NET CLR 1.1.4322)
Host: 192.168.1.106
Connection: Keep-Alive

HTTP/1.1 301 Moved Permanently
Date: Mon, 14 Sep 2015 10:40:42 GMT
Server: Apache/2.2.22 (Debian)
Location: http://192.168.1.100/efg.exe
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 248
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1

..........mPKK.@...W.9...l.Re..M.B...C....-..f-...I=x.....1..*..z[...7k.>...%....R?
#...  .....T%.BS+rll,.1...2.....*..i.
....&...v.=.z....nB....v..&......J...."u!....>.r6.R.,C>|
..T9.Lh.  ..I>&c..aP...;.\........7.....L...3.:.`.E._}<c:  .:>  ....2.;...
```

Entire conversation (846 bytes)

○ ASCII ○ EBCDIC ○ Hex Dump ○ C Arrays ● Raw

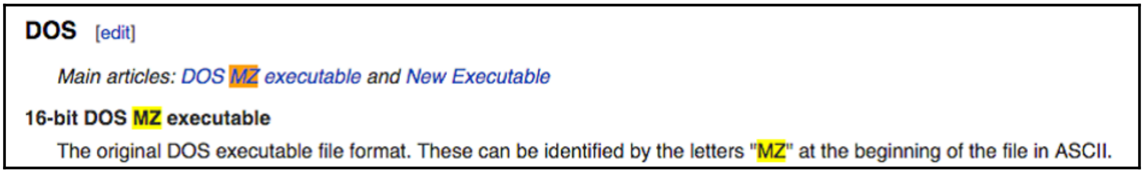


```
1255 36.428063(192.168.1.100        192.168.1.107        HTTP        1458 HTTP/1.1 200 OK  (application/x-msdownload)
```



```
GET /efg.exe HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, */*
Accept-Language: en-us
UA-CPU: x86
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; SV1; .NET CLR 1.1.4322)
Connection: Keep-Alive
Host: 192.168.1.100

HTTP/1.1 200 OK
Date: Mon, 14 Sep 2015 10:40:40 GMT
Server: Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color
PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0
Last-Modified: Mon, 14 Sep 2015 10:40:40 GMT
ETag: W/"2a00000000ff0e-142200-51fb4c11c8780"
Accept-Ranges: bytes
Content-Length: 1319424
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: application/x-msdownload

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

Entire conversation (1309951 bytes)

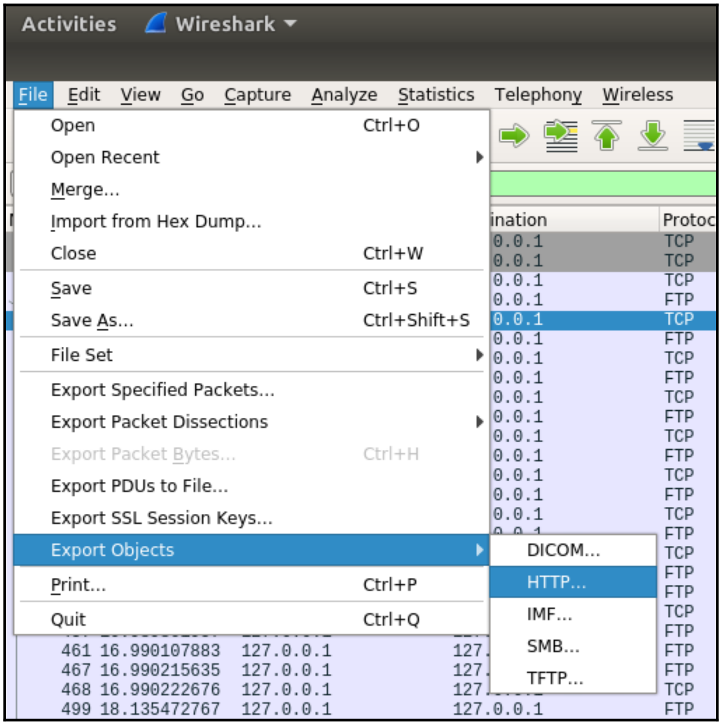


## DOS [edit]

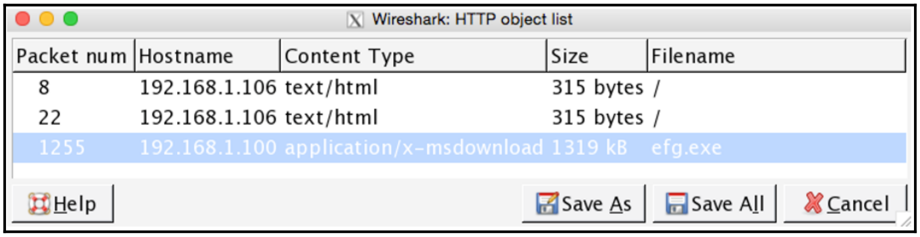
*Main articles: DOS MZ executable and New Executable*

### 16-bit DOS MZ executable

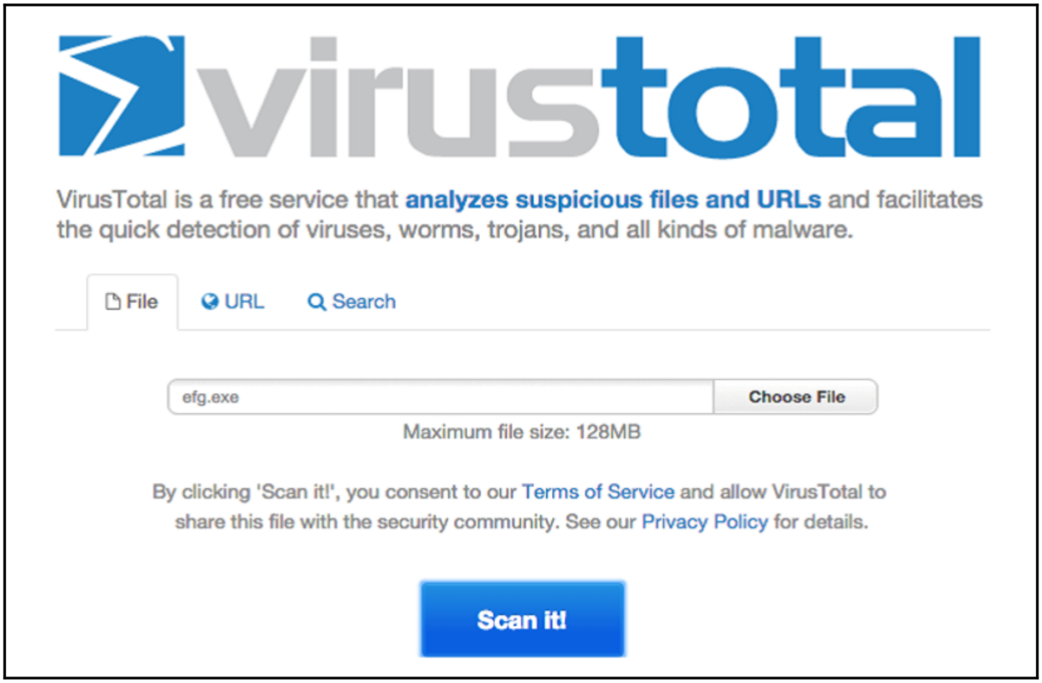
The original DOS executable file format. These can be identified by the letters "MZ" at the beginning of the file in ASCII.



```
461 16.990107883  127.0.0.1        127.
467 16.990215635  127.0.0.1        127.
468 16.990222676  127.0.0.1        127.
499 18.135472767  127.0.0.1        127.0.0.1        FTP
```


Wireshark: HTTP object list

| Packet num | Hostname | Content Type | Size | Filename |
|---|---|---|---|---|
| 8 | 192.168.1.106 | text/html | 315 bytes | / |
| 22 | 192.168.1.106 | text/html | 315 bytes | / |
| 1255 | 192.168.1.100 | application/x-msdownload | 1319 kB | efg.exe |

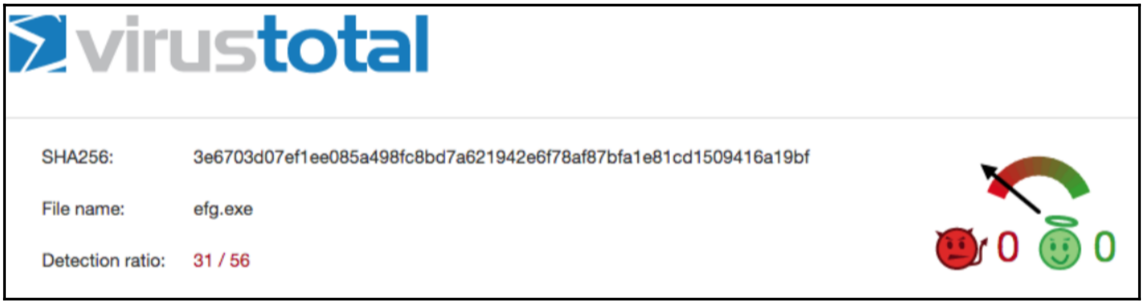


VirusTotal is a free service that **analyzes suspicious files and URLs** and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware.

efg.exe

Maximum file size: 128MB

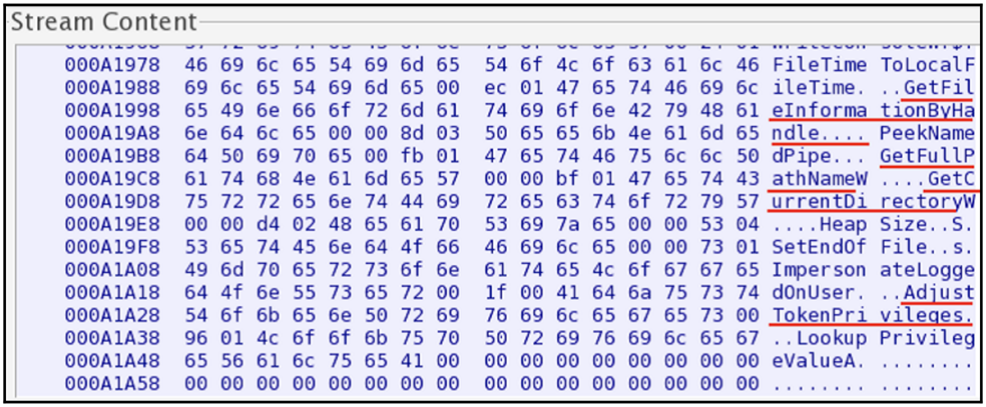
By clicking 'Scan it!', you consent to our Terms of Service and allow VirusTotal to share this file with the security community. See our Privacy Policy for details.



SHA256: 3e6703d07ef1ee085a498fc8bd7a621942e6f78af87bfa1e81cd1509416a19bf

File name: efg.exe

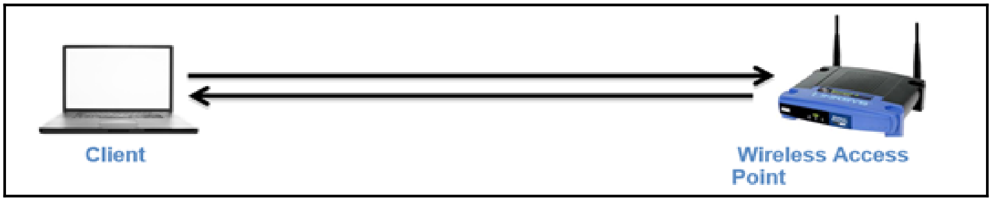
Detection ratio: 31 / 56

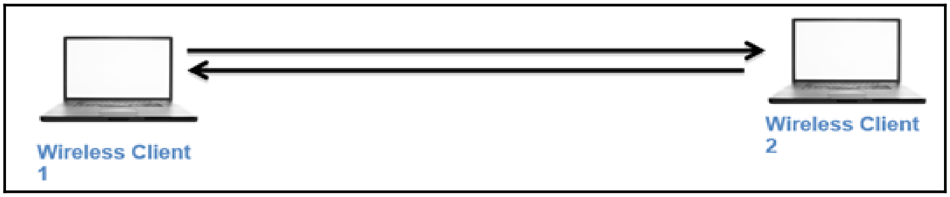


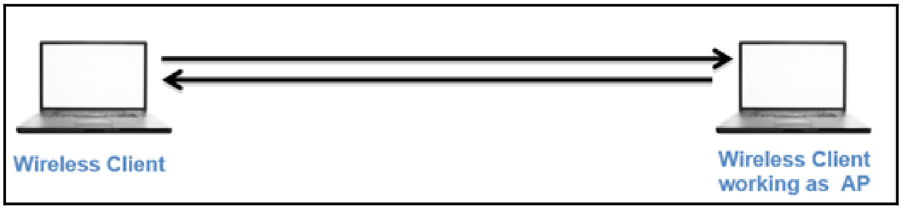
Stream Content

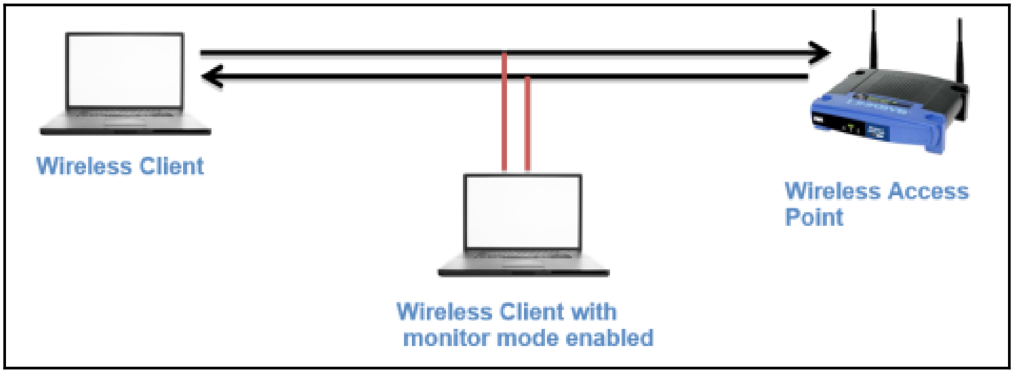
```
000A1978  46 69 6c 65 54 69 6d 65  54 6f 4c 6f 63 61 6c 46 FileTime ToLocalF
000A1988  69 6c 65 54 69 6d 65 00  ec 01 47 65 74 46 69 6c ileTime. ..GetFil
000A1998  65 49 6e 66 6f 72 6d 61  74 69 6f 6e 42 79 48 61 eInforma tionByHa
000A19A8  6e 64 6c 65 00 00 8d 03  50 65 65 6b 4e 61 6d 65 ndle.... PeekName
000A19B8  64 50 69 70 65 00 fb 01  47 65 74 46 75 6c 6c 50 dPipe... GetFullP
000A19C8  61 74 68 4e 61 6d 65 57  00 00 bf 01 47 65 74 43 athNameW ....GetC
000A19D8  75 72 72 65 6e 74 44 69  72 65 63 74 6f 72 79 57 urrentDi rectoryW
000A19E8  00 00 d4 02 48 65 61 70  53 69 7a 65 00 00 53 04 ....Heap Size..S.
000A19F8  53 65 74 45 6e 64 4f 66  46 69 6c 65 00 00 73 01 SetEndOf File..s.
000A1A08  49 6d 70 65 72 73 6f 6e  61 74 65 4c 6f 67 67 65 Imperson ateLogge
000A1A18  64 4f 6e 55 73 65 72 00  1f 00 41 64 6a 75 73 74 dOnUser. ..Adjust
000A1A28  54 6f 6b 65 6e 50 72 69  76 69 6c 65 67 65 73 00 TokenPri vileges.
000A1A38  96 01 4c 6f 6f 6b 75 70  50 72 69 76 69 6c 65 67 ..Lookup Privileg
000A1A48  65 56 61 6c 75 65 41 00  00 00 00 00 00 00 00 00 eValueA. ........
000A1A58  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00 ........ ........
```

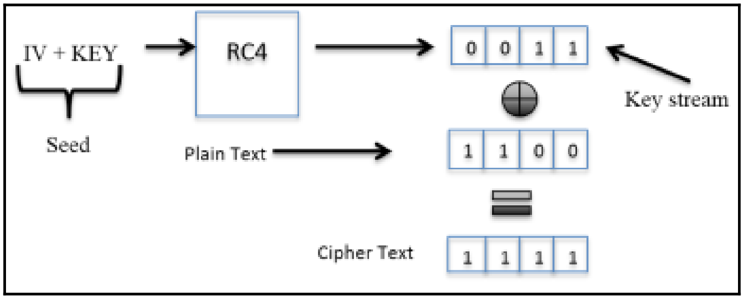
# Chapter 7: Analyzing Traffic in Thin Air

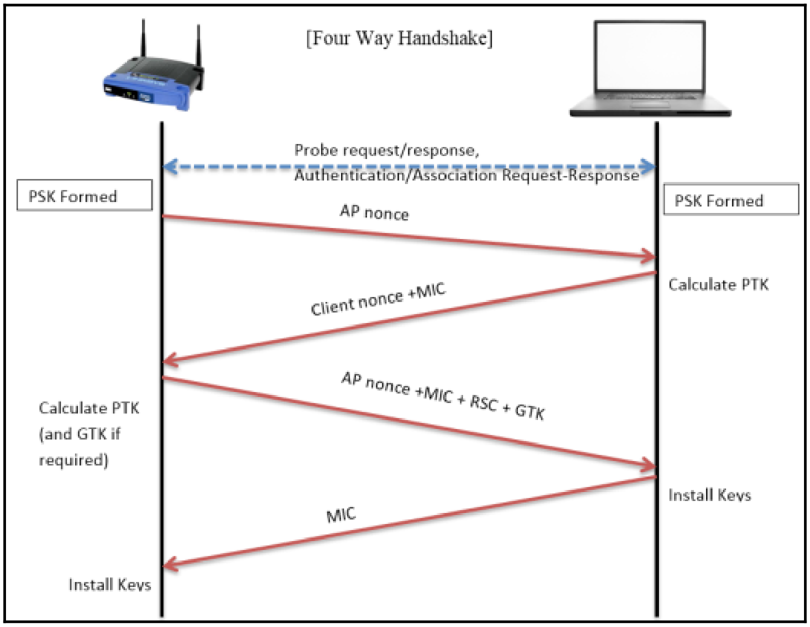


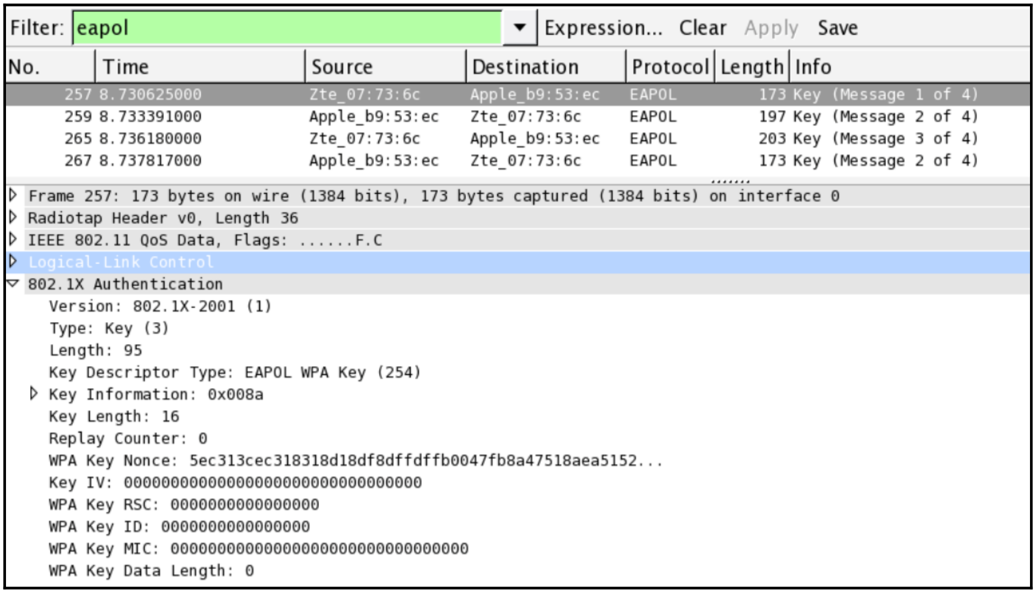







IV + KEY
Seed
RC4
0 0 1 1
Key stream
Plain Text
1 1 0 0
Cipher Text
1 1 1 1

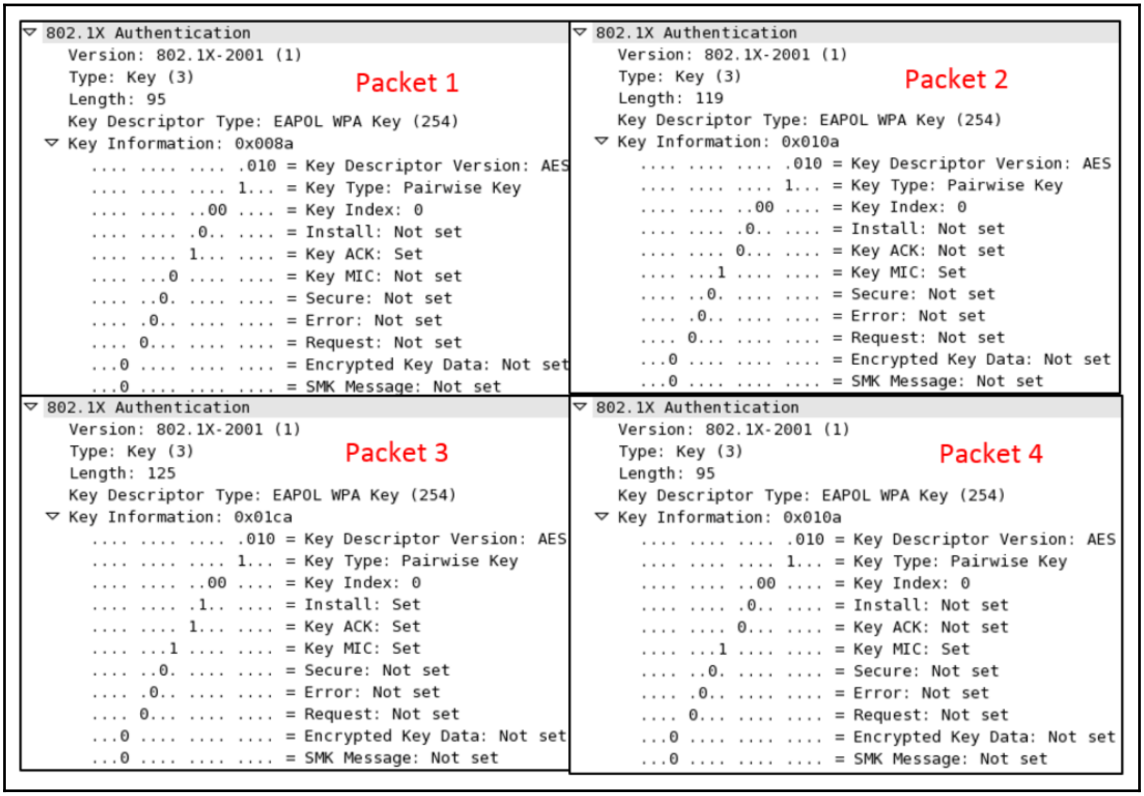

[Four Way Handshake]
Probe request/response,
Authentication/Association Request-Response
PSK Formed
PSK Formed
AP nonce
Calculate PTK
Client nonce +MIC
AP nonce +MIC + RSC + GTK
Calculate PTK
(and GTK if
required)
Install Keys
MIC
Install Keys



Filter: eapol

```
No.   Time          Source            Destination       Protocol Length Info
  257 8.730625000   Zte_07:73:6c      Apple_b9:53:ec    EAPOL       173 Key (Message 1 of 4)
  259 8.733391000   Apple_b9:53:ec    Zte_07:73:6c      EAPOL       197 Key (Message 2 of 4)
  265 8.736180000   Zte_07:73:6c      Apple_b9:53:ec    EAPOL       203 Key (Message 3 of 4)
  267 8.737817000   Apple_b9:53:ec    Zte_07:73:6c      EAPOL       173 Key (Message 2 of 4)
```

```
▷ Frame 257: 173 bytes on wire (1384 bits), 173 bytes captured (1384 bits) on interface 0
▷ Radiotap Header v0, Length 36
▷ IEEE 802.11 QoS Data, Flags: ......F.C
▷ Logical-Link Control
▽ 802.1X Authentication
    Version: 802.1X-2001 (1)
    Type: Key (3)
    Length: 95
    Key Descriptor Type: EAPOL WPA Key (254)
  ▷ Key Information: 0x008a
    Key Length: 16
    Replay Counter: 0
    WPA Key Nonce: 5ec313cec318318d18df8dffdffb0047fb8a47518aea5152...
    Key IV: 00000000000000000000000000000000
    WPA Key RSC: 0000000000000000
    WPA Key ID: 0000000000000000
    WPA Key MIC: 00000000000000000000000000000000
    WPA Key Data Length: 0
```



Packet 1

```
▽ 802.1X Authentication
    Version: 802.1X-2001 (1)
    Type: Key (3)
    Length: 95
    Key Descriptor Type: EAPOL WPA Key (254)
  ▽ Key Information: 0x008a
      .... .... .... .010 = Key Descriptor Version: AES
      .... .... .... 1... = Key Type: Pairwise Key
      .... .... ..00 .... = Key Index: 0
      .... .... .0.. .... = Install: Not set
      .... .... 1... .... = Key ACK: Set
      .... ...0 .... .... = Key MIC: Not set
      .... ..0. .... .... = Secure: Not set
      .... .0.. .... .... = Error: Not set
      .... 0... .... .... = Request: Not set
      ...0 .... .... .... = Encrypted Key Data: Not set
      ...0 .... .... .... = SMK Message: Not set
```

Packet 2

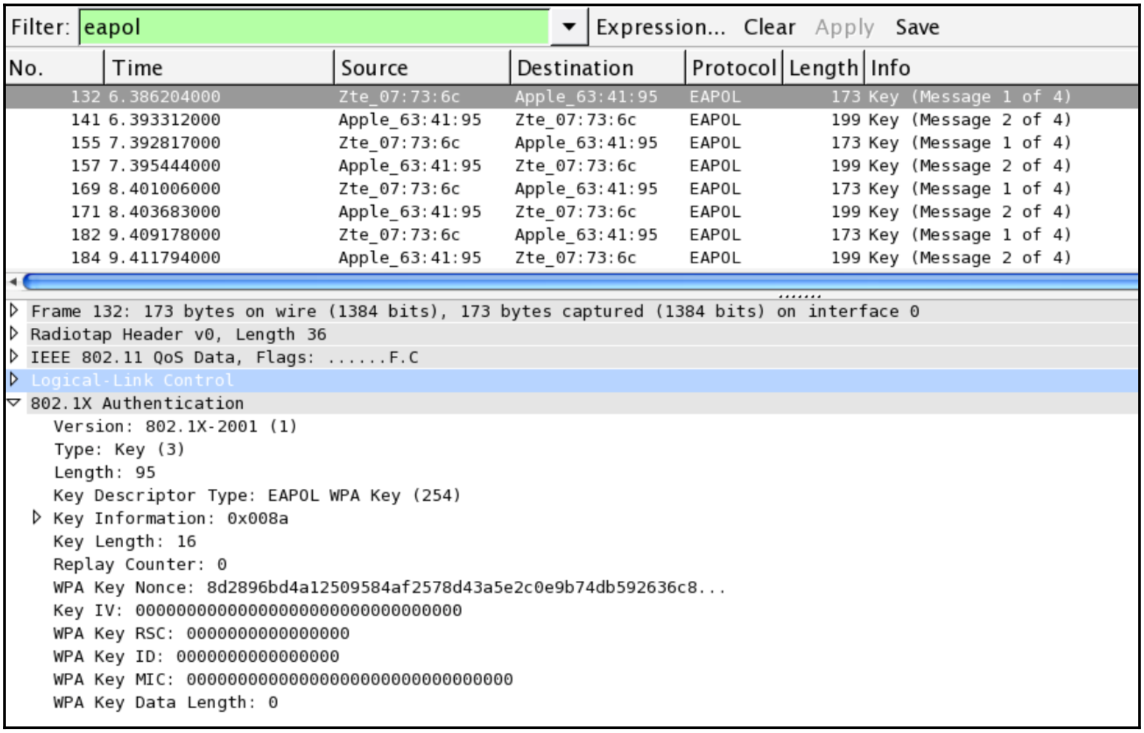
```
▽ 802.1X Authentication
    Version: 802.1X-2001 (1)
    Type: Key (3)
    Length: 119
    Key Descriptor Type: EAPOL WPA Key (254)
  ▽ Key Information: 0x010a
      .... .... .... .010 = Key Descriptor Version: AES
      .... .... .... 1... = Key Type: Pairwise Key
      .... .... ..00 .... = Key Index: 0
      .... .... .0.. .... = Install: Not set
      .... .... 0... .... = Key ACK: Not set
      .... ...1 .... .... = Key MIC: Set
      .... ..0. .... .... = Secure: Not set
      .... .0.. .... .... = Error: Not set
      .... 0... .... .... = Request: Not set
      ...0 .... .... .... = Encrypted Key Data: Not set
      ...0 .... .... .... = SMK Message: Not set
```

Packet 3

```
▽ 802.1X Authentication
    Version: 802.1X-2001 (1)
    Type: Key (3)
    Length: 125
    Key Descriptor Type: EAPOL WPA Key (254)
  ▽ Key Information: 0x01ca
      .... .... .... .010 = Key Descriptor Version: AES
      .... .... .... 1... = Key Type: Pairwise Key
      .... .... ..00 .... = Key Index: 0
      .... .... .1.. .... = Install: Set
      .... .... 1... .... = Key ACK: Set
      .... ...1 .... .... = Key MIC: Set
      .... ..0. .... .... = Secure: Not set
      .... .0.. .... .... = Error: Not set
      .... 0... .... .... = Request: Not set
      ...0 .... .... .... = Encrypted Key Data: Not set
      ...0 .... .... .... = SMK Message: Not set
```

Packet 4

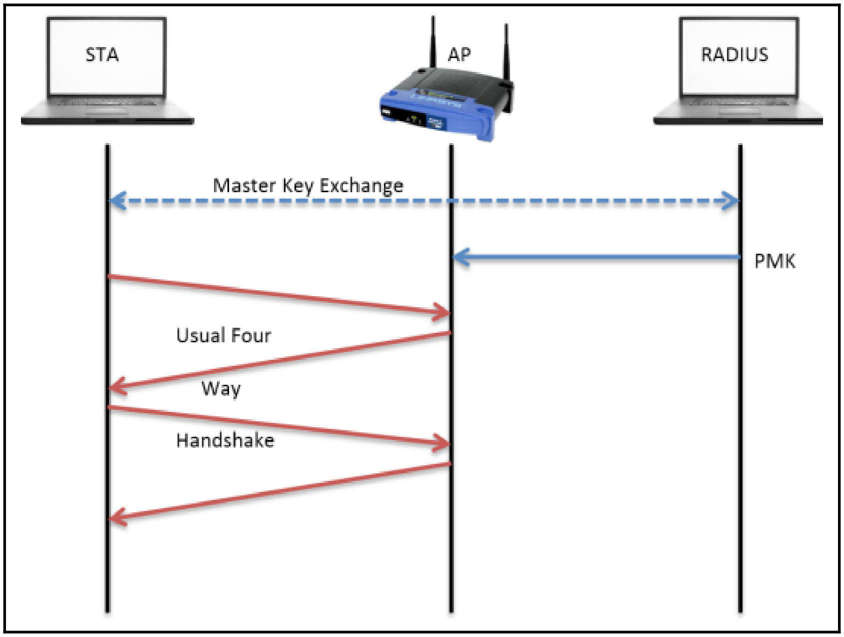
```
▽ 802.1X Authentication
    Version: 802.1X-2001 (1)
    Type: Key (3)
    Length: 95
    Key Descriptor Type: EAPOL WPA Key (254)
  ▽ Key Information: 0x010a
      .... .... .... .010 = Key Descriptor Version: AES
      .... .... .... 1... = Key Type: Pairwise Key
      .... .... ..00 .... = Key Index: 0
      .... .... .0.. .... = Install: Not set
      .... .... 0... .... = Key ACK: Not set
      .... ...1 .... .... = Key MIC: Set
      .... ..0. .... .... = Secure: Not set
      .... .0.. .... .... = Error: Not set
      .... 0... .... .... = Request: Not set
      ...0 .... .... .... = Encrypted Key Data: Not set
      ...0 .... .... .... = SMK Message: Not set
```

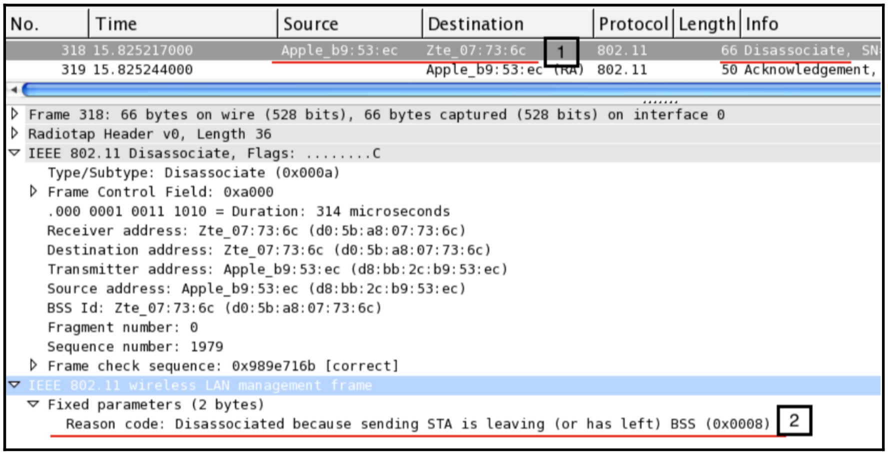


Filter: eapol

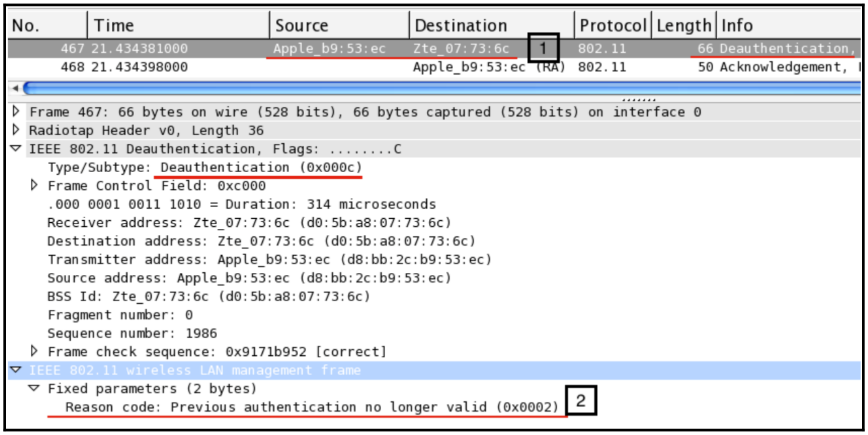
```
No.     Time          Source            Destination       Protocol Length Info
    132 6.386204000   Zte_07:73:6c      Apple_63:41:95    EAPOL       173 Key (Message 1 of 4)
    141 6.393312000   Apple_63:41:95    Zte_07:73:6c      EAPOL       199 Key (Message 2 of 4)
    155 7.392817000   Zte_07:73:6c      Apple_63:41:95    EAPOL       173 Key (Message 1 of 4)
    157 7.395444000   Apple_63:41:95    Zte_07:73:6c      EAPOL       199 Key (Message 2 of 4)
    169 8.401006000   Zte_07:73:6c      Apple_63:41:95    EAPOL       173 Key (Message 1 of 4)
    171 8.403683000   Apple_63:41:95    Zte_07:73:6c      EAPOL       199 Key (Message 2 of 4)
    182 9.409178000   Zte_07:73:6c      Apple_63:41:95    EAPOL       173 Key (Message 1 of 4)
    184 9.411794000   Apple_63:41:95    Zte_07:73:6c      EAPOL       199 Key (Message 2 of 4)
```

```
▷ Frame 132: 173 bytes on wire (1384 bits), 173 bytes captured (1384 bits) on interface 0
▷ Radiotap Header v0, Length 36
▷ IEEE 802.11 QoS Data, Flags: ......F.C
▷ Logical-Link Control
▽ 802.1X Authentication
    Version: 802.1X-2001 (1)
    Type: Key (3)
    Length: 95
    Key Descriptor Type: EAPOL WPA Key (254)
  ▷ Key Information: 0x008a
    Key Length: 16
    Replay Counter: 0
    WPA Key Nonce: 8d2896bd4a12509584af2578d43a5e2c0e9b74db592636c8...
    Key IV: 00000000000000000000000000000000
    WPA Key RSC: 0000000000000000
    WPA Key ID: 0000000000000000
    WPA Key MIC: 00000000000000000000000000000000
    WPA Key Data Length: 0
```



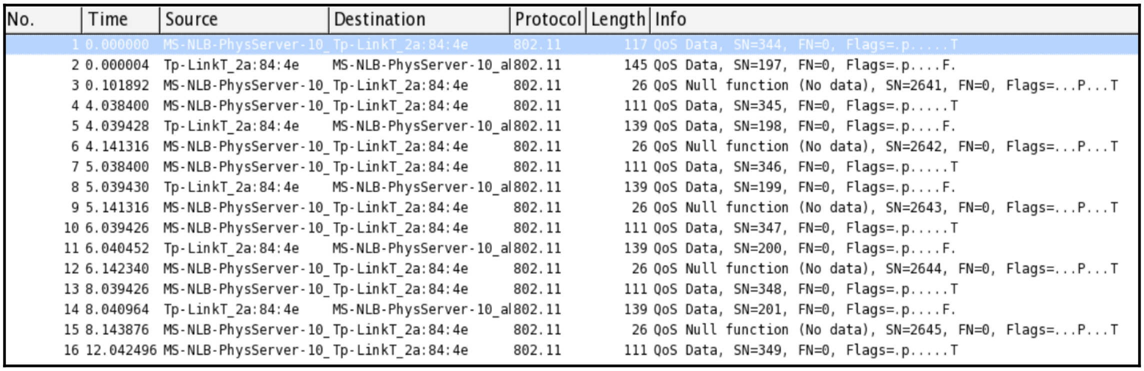


```
No.      Time            Source             Destination            Protocol  Length  Info
    318 15.825217000     Apple_b9:53:ec     Zte_07:73:6c           802.11        66 Disassociate, SN
    319 15.825244000                        Apple_b9:53:ec (RA)    802.11        50 Acknowledgement,

▷ Frame 318: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
▷ Radiotap Header v0, Length 36
▽ IEEE 802.11 Disassociate, Flags: ........C
    Type/Subtype: Disassociate (0x000a)
  ▷ Frame Control Field: 0xa000
    .000 0001 0011 1010 = Duration: 314 microseconds
    Receiver address: Zte_07:73:6c (d0:5b:a8:07:73:6c)
    Destination address: Zte_07:73:6c (d0:5b:a8:07:73:6c)
    Transmitter address: Apple_b9:53:ec (d8:bb:2c:b9:53:ec)
    Source address: Apple_b9:53:ec (d8:bb:2c:b9:53:ec)
    BSS Id: Zte_07:73:6c (d0:5b:a8:07:73:6c)
    Fragment number: 0
    Sequence number: 1979
  ▷ Frame check sequence: 0x989e716b [correct]
▽ IEEE 802.11 wireless LAN management frame
  ▽ Fixed parameters (2 bytes)
      Reason code: Disassociated because sending STA is leaving (or has left) BSS (0x0008)
```

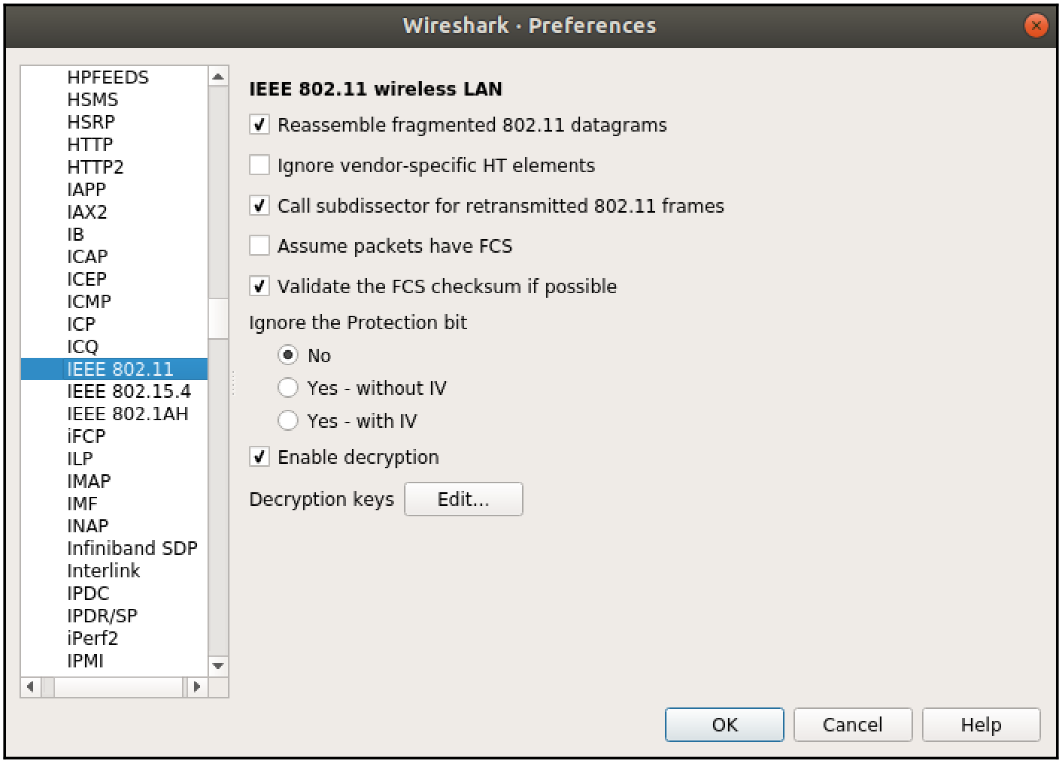


| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 467 | 21.434381000 | Apple_b9:53:ec | Zte_07:73:6c | 802.11 | 66 | Deauthentication, |
| 468 | 21.434398000 |  | Apple_b9:53:ec (RA) | 802.11 | 50 | Acknowledgement, |

```
▷ Frame 467: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
▷ Radiotap Header v0, Length 36
▽ IEEE 802.11 Deauthentication, Flags: ........C
    Type/Subtype: Deauthentication (0x000c)
  ▷ Frame Control Field: 0xc000
    .000 0001 0011 1010 = Duration: 314 microseconds
    Receiver address: Zte_07:73:6c (d0:5b:a8:07:73:6c)
    Destination address: Zte_07:73:6c (d0:5b:a8:07:73:6c)
    Transmitter address: Apple_b9:53:ec (d8:bb:2c:b9:53:ec)
    Source address: Apple_b9:53:ec (d8:bb:2c:b9:53:ec)
    BSS Id: Zte_07:73:6c (d0:5b:a8:07:73:6c)
    Fragment number: 0
    Sequence number: 1986
  ▷ Frame check sequence: 0x9171b952 [correct]
▽ IEEE 802.11 wireless LAN management frame
  ▽ Fixed parameters (2 bytes)
      Reason code: Previous authentication no longer valid (0x0002)
```



| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 1 | 0.000000 | MS-NLB-PhysServer-10_ | Tp-LinkT_2a:84:4e | 802.11 | 117 | QoS Data, SN=344, FN=0, Flags=.p.....T |
| 2 | 0.000004 | Tp-LinkT_2a:84:4e | MS-NLB-PhysServer-10_al | 802.11 | 145 | QoS Data, SN=197, FN=0, Flags=.p....F. |
| 3 | 0.101892 | MS-NLB-PhysServer-10_ | Tp-LinkT_2a:84:4e | 802.11 | 26 | QoS Null function (No data), SN=2641, FN=0, Flags=...P...T |
| 4 | 4.038400 | MS-NLB-PhysServer-10_ | Tp-LinkT_2a:84:4e | 802.11 | 111 | QoS Data, SN=345, FN=0, Flags=.p.....T |
| 5 | 4.039428 | Tp-LinkT_2a:84:4e | MS-NLB-PhysServer-10_al | 802.11 | 139 | QoS Data, SN=198, FN=0, Flags=.p....F. |
| 6 | 4.141316 | MS-NLB-PhysServer-10_ | Tp-LinkT_2a:84:4e | 802.11 | 26 | QoS Null function (No data), SN=2642, FN=0, Flags=...P...T |
| 7 | 5.038400 | MS-NLB-PhysServer-10_ | Tp-LinkT_2a:84:4e | 802.11 | 111 | QoS Data, SN=346, FN=0, Flags=.p.....T |
| 8 | 5.039430 | Tp-LinkT_2a:84:4e | MS-NLB-PhysServer-10_al | 802.11 | 139 | QoS Data, SN=199, FN=0, Flags=.p....F. |
| 9 | 5.141316 | MS-NLB-PhysServer-10_ | Tp-LinkT_2a:84:4e | 802.11 | 26 | QoS Null function (No data), SN=2643, FN=0, Flags=...P...T |
| 10 | 6.039426 | MS-NLB-PhysServer-10_ | Tp-LinkT_2a:84:4e | 802.11 | 111 | QoS Data, SN=347, FN=0, Flags=.p.....T |
| 11 | 6.040452 | Tp-LinkT_2a:84:4e | MS-NLB-PhysServer-10_al | 802.11 | 139 | QoS Data, SN=200, FN=0, Flags=.p....F. |
| 12 | 6.142340 | MS-NLB-PhysServer-10_ | Tp-LinkT_2a:84:4e | 802.11 | 26 | QoS Null function (No data), SN=2644, FN=0, Flags=...P...T |
| 13 | 8.039426 | MS-NLB-PhysServer-10_ | Tp-LinkT_2a:84:4e | 802.11 | 111 | QoS Data, SN=348, FN=0, Flags=.p.....T |
| 14 | 8.040964 | Tp-LinkT_2a:84:4e | MS-NLB-PhysServer-10_al | 802.11 | 139 | QoS Data, SN=201, FN=0, Flags=.p....F. |
| 15 | 8.143876 | MS-NLB-PhysServer-10_ | Tp-LinkT_2a:84:4e | 802.11 | 26 | QoS Null function (No data), SN=2645, FN=0, Flags=...P...T |
| 16 | 12.042496 | MS-NLB-PhysServer-10_ | Tp-LinkT_2a:84:4e | 802.11 | 111 | QoS Data, SN=349, FN=0, Flags=.p.....T |



**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

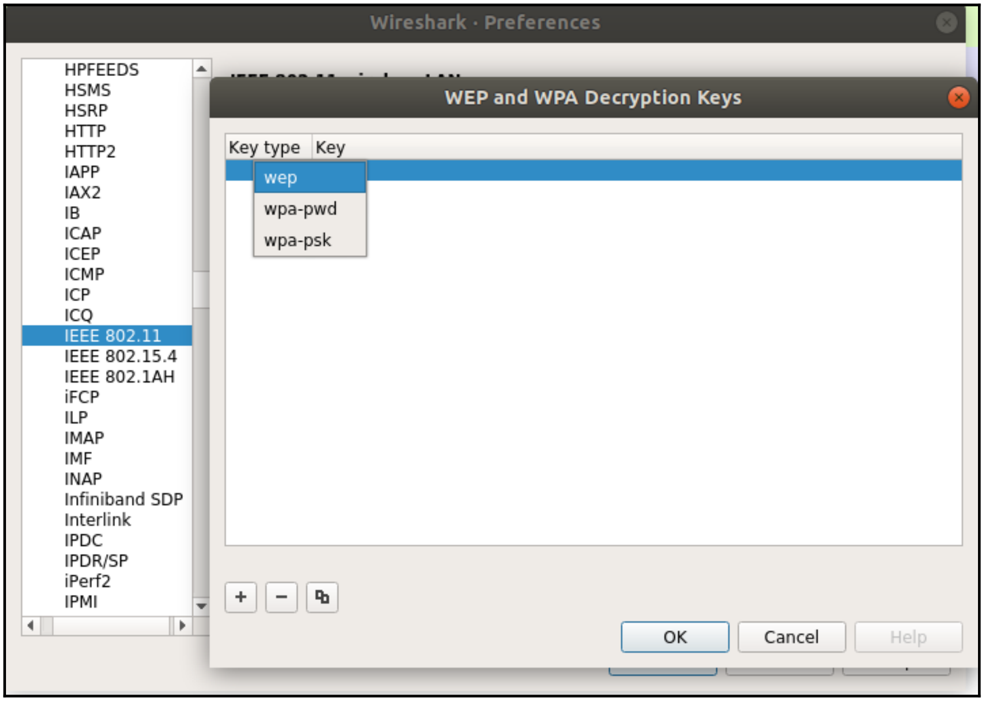
● No

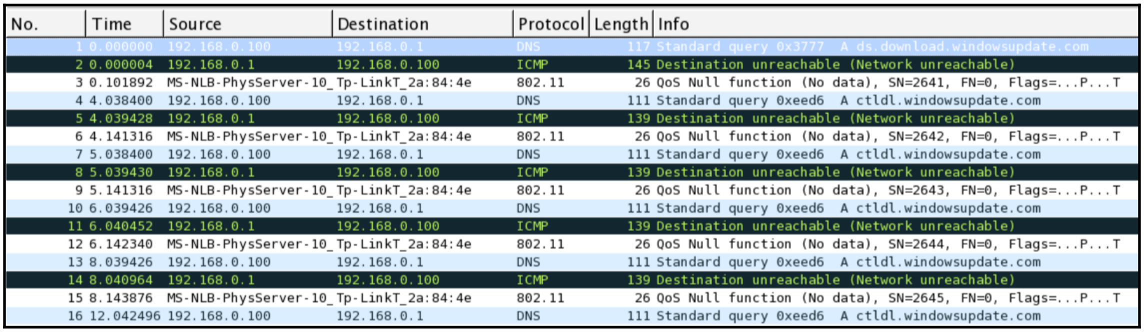
○ Yes - without IV

○ Yes - with IV

☑ Enable decryption

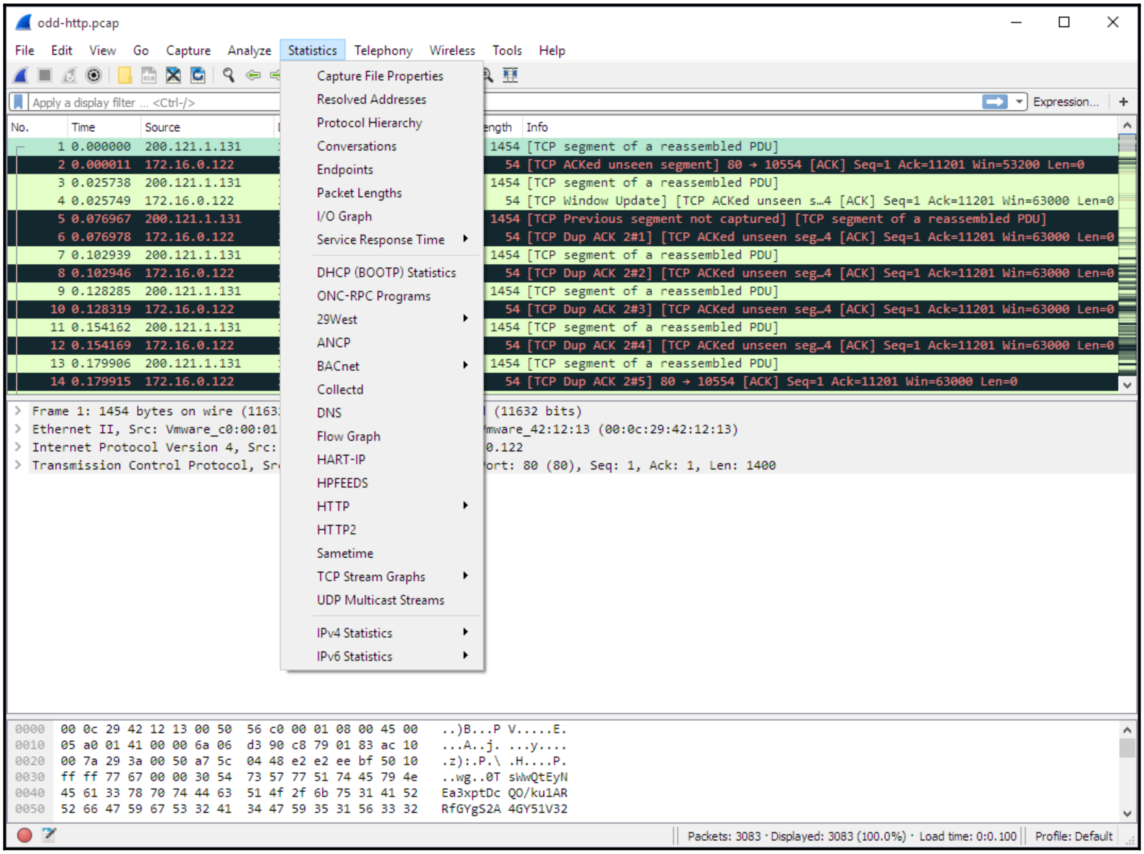
Decryption keys Edit...





| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 1 | 0.000000 | 192.168.0.100 | 192.168.0.1 | DNS | 117 | Standard query 0x3777  A ds.download.windowsupdate.com |
| 2 | 0.000004 | 192.168.0.1 | 192.168.0.100 | ICMP | 145 | Destination unreachable (Network unreachable) |
| 3 | 0.101892 | MS-NLB-PhysServer-10_ | Tp-LinkT_2a:84:4e | 802.11 | 26 | QoS Null function (No data), SN=2641, FN=0, Flags=...P...T |
| 4 | 4.038400 | 192.168.0.100 | 192.168.0.1 | DNS | 111 | Standard query 0xeed6  A ctldl.windowsupdate.com |
| 5 | 4.039428 | 192.168.0.1 | 192.168.0.100 | ICMP | 139 | Destination unreachable (Network unreachable) |
| 6 | 4.141316 | MS-NLB-PhysServer-10_ | Tp-LinkT_2a:84:4e | 802.11 | 26 | QoS Null function (No data), SN=2642, FN=0, Flags=...P...T |
| 7 | 5.038400 | 192.168.0.100 | 192.168.0.1 | DNS | 111 | Standard query 0xeed6  A ctldl.windowsupdate.com |
| 8 | 5.039430 | 192.168.0.1 | 192.168.0.100 | ICMP | 139 | Destination unreachable (Network unreachable) |
| 9 | 5.141316 | MS-NLB-PhysServer-10_ | Tp-LinkT_2a:84:4e | 802.11 | 26 | QoS Null function (No data), SN=2643, FN=0, Flags=...P...T |
| 10 | 6.039426 | 192.168.0.100 | 192.168.0.1 | DNS | 111 | Standard query 0xeed6  A ctldl.windowsupdate.com |
| 11 | 6.040452 | 192.168.0.1 | 192.168.0.100 | ICMP | 139 | Destination unreachable (Network unreachable) |
| 12 | 6.142340 | MS-NLB-PhysServer-10_ | Tp-LinkT_2a:84:4e | 802.11 | 26 | QoS Null function (No data), SN=2644, FN=0, Flags=...P...T |
| 13 | 8.039426 | 192.168.0.100 | 192.168.0.1 | DNS | 111 | Standard query 0xeed6  A ctldl.windowsupdate.com |
| 14 | 8.040964 | 192.168.0.1 | 192.168.0.100 | ICMP | 139 | Destination unreachable (Network unreachable) |
| 15 | 8.143876 | MS-NLB-PhysServer-10_ | Tp-LinkT_2a:84:4e | 802.11 | 26 | QoS Null function (No data), SN=2645, FN=0, Flags=...P...T |
| 16 | 12.042496 | 192.168.0.100 | 192.168.0.1 | DNS | 111 | Standard query 0xeed6  A ctldl.windowsupdate.com |

# Chapter 8:
# Mastering the Advanced Features of Wiresh ark

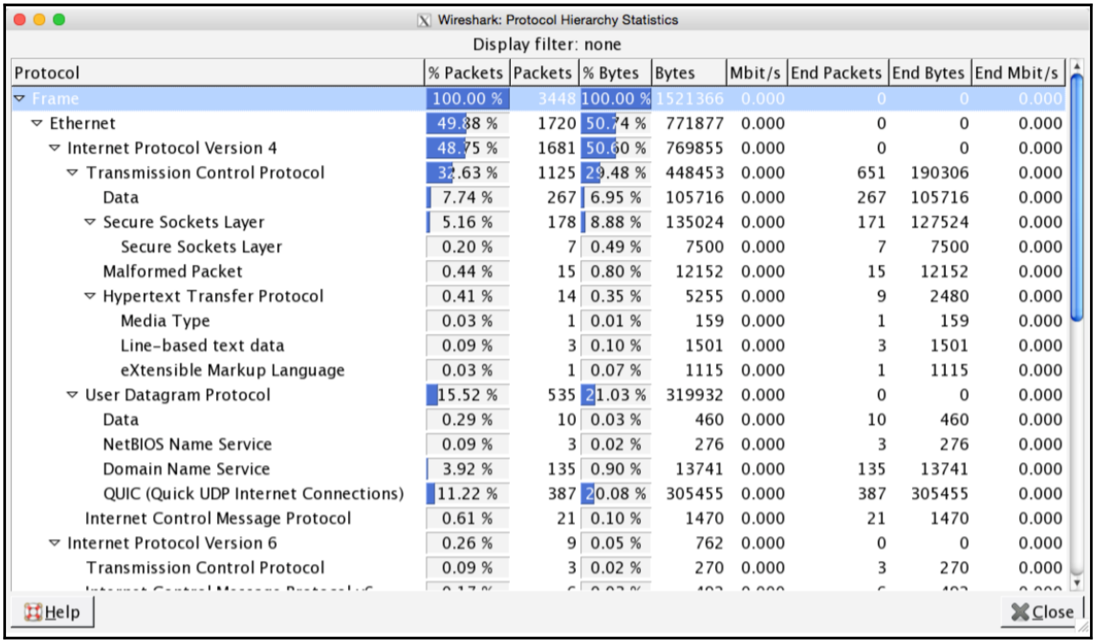


```
No.   Time       Source                ength  Info
    1 0.000000   200.121.1.131          1454 [TCP segment of a reassembled PDU]
    2 0.000011   172.16.0.122             54 [TCP ACKed unseen segment] 80 → 10554 [ACK] Seq=1 Ack=11201 Win=53200 Len=0
    3 0.025738   200.121.1.131          1454 [TCP segment of a reassembled PDU]
    4 0.025749   172.16.0.122             54 [TCP Window Update] [TCP ACKed unseen s…4 [ACK] Seq=1 Ack=11201 Win=63000 Len=0
    5 0.076967   200.121.1.131          1454 [TCP Previous segment not captured] [TCP segment of a reassembled PDU]
    6 0.076978   172.16.0.122             54 [TCP Dup ACK 2#1] [TCP ACKed unseen seg…4 [ACK] Seq=1 Ack=11201 Win=63000 Len=0
    7 0.102939   200.121.1.131          1454 [TCP segment of a reassembled PDU]
    8 0.102946   172.16.0.122             54 [TCP Dup ACK 2#2] [TCP ACKed unseen seg…4 [ACK] Seq=1 Ack=11201 Win=63000 Len=0
    9 0.128285   200.121.1.131          1454 [TCP segment of a reassembled PDU]
   10 0.128319   172.16.0.122             54 [TCP Dup ACK 2#3] [TCP ACKed unseen seg…4 [ACK] Seq=1 Ack=11201 Win=63000 Len=0
   11 0.154162   200.121.1.131          1454 [TCP segment of a reassembled PDU]
   12 0.154169   172.16.0.122             54 [TCP Dup ACK 2#4] [TCP ACKed unseen seg…4 [ACK] Seq=1 Ack=11201 Win=63000 Len=0
   13 0.179906   200.121.1.131          1454 [TCP segment of a reassembled PDU]
   14 0.179915   172.16.0.122             54 [TCP Dup ACK 2#5] 80 → 10554 [ACK] Seq=1 Ack=11201 Win=63000 Len=0
```

```
> Frame 1: 1454 bytes on wire (1163      (11632 bits)
> Ethernet II, Src: Vmware_c0:00:01     mware_42:12:13 (00:0c:29:42:12:13)
> Internet Protocol Version 4, Src:     0.122
> Transmission Control Protocol, Sr     ort: 80 (80), Seq: 1, Ack: 1, Len: 1400
```

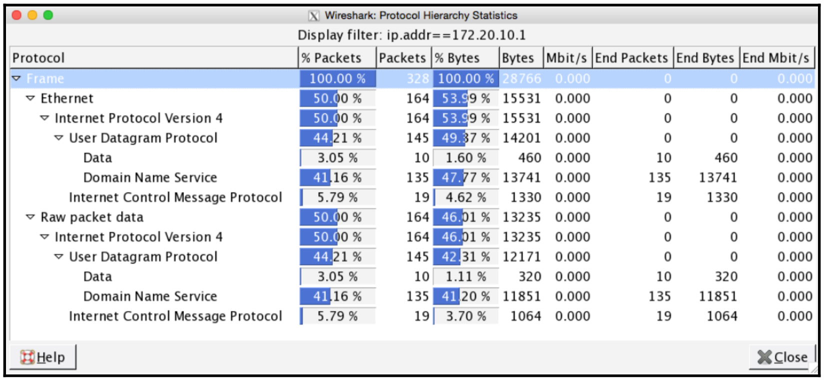
```
0000  00 0c 29 42 12 13 00 50  56 c0 00 01 08 00 45 00   ..)B...P V.....E.
0010  05 a0 01 41 00 00 6a 06  d3 90 c8 79 01 83 ac 10   ...A..j. ...y....
0020  00 7a 29 3a 00 50 a7 5c  04 48 e2 e2 ee bf 50 10   .z):.P.\ .H....P.
0030  ff ff 77 67 00 00 30 54  73 57 77 51 74 45 79 4e   ..wg..0T sWwQtEyN
0040  45 61 33 78 70 74 44 63  51 4f 2f 6b 75 31 41 52   Ea3xptDc QO/ku1AR
0050  52 66 47 59 67 53 32 41  34 47 59 35 31 56 33 32   RfGYgS2A 4GY51V32
```

Packets: 3083 · Displayed: 3083 (100.0%) · Load time: 0:0.100 | Profile: Default



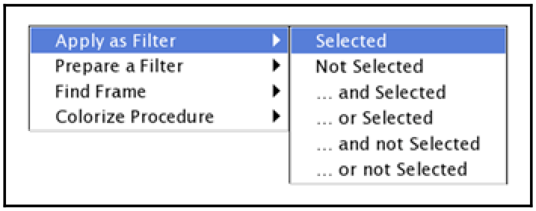
Display filter: none

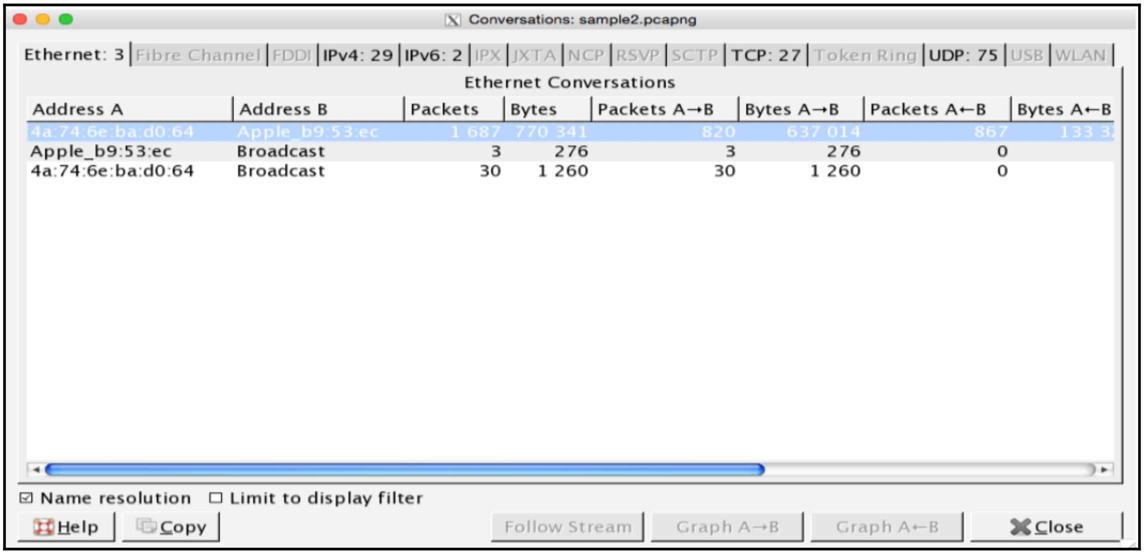
| Protocol | % Packets | Packets | % Bytes | Bytes | Mbit/s | End Packets | End Bytes | End Mbit/s |
|---|---|---|---|---|---|---|---|---|
| Frame | 100.00 % | 3448 | 100.00 % | 1521366 | 0.000 | 0 | 0 | 0.000 |
| Ethernet | 49.88 % | 1720 | 50.74 % | 771877 | 0.000 | 0 | 0 | 0.000 |
| Internet Protocol Version 4 | 48.75 % | 1681 | 50.60 % | 769855 | 0.000 | 0 | 0 | 0.000 |
| Transmission Control Protocol | 32.63 % | 1125 | 29.48 % | 448453 | 0.000 | 651 | 190306 | 0.000 |
| Data | 7.74 % | 267 | 6.95 % | 105716 | 0.000 | 267 | 105716 | 0.000 |
| Secure Sockets Layer | 5.16 % | 178 | 8.88 % | 135024 | 0.000 | 171 | 127524 | 0.000 |
| Secure Sockets Layer | 0.20 % | 7 | 0.49 % | 7500 | 0.000 | 7 | 7500 | 0.000 |
| Malformed Packet | 0.44 % | 15 | 0.80 % | 12152 | 0.000 | 15 | 12152 | 0.000 |
| Hypertext Transfer Protocol | 0.41 % | 14 | 0.35 % | 5255 | 0.000 | 9 | 2480 | 0.000 |
| Media Type | 0.03 % | 1 | 0.01 % | 159 | 0.000 | 1 | 159 | 0.000 |
| Line-based text data | 0.09 % | 3 | 0.10 % | 1501 | 0.000 | 3 | 1501 | 0.000 |
| eXtensible Markup Language | 0.03 % | 1 | 0.07 % | 1115 | 0.000 | 1 | 1115 | 0.000 |
| User Datagram Protocol | 15.52 % | 535 | 21.03 % | 319932 | 0.000 | 0 | 0 | 0.000 |
| Data | 0.29 % | 10 | 0.03 % | 460 | 0.000 | 10 | 460 | 0.000 |
| NetBIOS Name Service | 0.09 % | 3 | 0.02 % | 276 | 0.000 | 3 | 276 | 0.000 |
| Domain Name Service | 3.92 % | 135 | 0.90 % | 13741 | 0.000 | 135 | 13741 | 0.000 |
| QUIC (Quick UDP Internet Connections) | 11.22 % | 387 | 20.08 % | 305455 | 0.000 | 387 | 305455 | 0.000 |
| Internet Control Message Protocol | 0.61 % | 21 | 0.10 % | 1470 | 0.000 | 21 | 1470 | 0.000 |
| Internet Protocol Version 6 | 0.26 % | 9 | 0.05 % | 762 | 0.000 | 0 | 0 | 0.000 |
| Transmission Control Protocol | 0.09 % | 3 | 0.02 % | 270 | 0.000 | 3 | 270 | 0.000 |



Display filter: ip.addr==172.20.10.1

| Protocol | % Packets | Packets | % Bytes | Bytes | Mbit/s | End Packets | End Bytes | End Mbit/s |
|---|---|---|---|---|---|---|---|---|
| Frame | 100.00 % | 328 | 100.00 % | 28766 | 0.000 | 0 | 0 | 0.000 |
| Ethernet | 50.00 % | 164 | 53.99 % | 15531 | 0.000 | 0 | 0 | 0.000 |
| Internet Protocol Version 4 | 50.00 % | 164 | 53.99 % | 15531 | 0.000 | 0 | 0 | 0.000 |
| User Datagram Protocol | 44.21 % | 145 | 49.37 % | 14201 | 0.000 | 0 | 0 | 0.000 |
| Data | 3.05 % | 10 | 1.60 % | 460 | 0.000 | 10 | 460 | 0.000 |
| Domain Name Service | 41.16 % | 135 | 47.77 % | 13741 | 0.000 | 135 | 13741 | 0.000 |
| Internet Control Message Protocol | 5.79 % | 19 | 4.62 % | 1330 | 0.000 | 19 | 1330 | 0.000 |
| Raw packet data | 50.00 % | 164 | 46.01 % | 13235 | 0.000 | 0 | 0 | 0.000 |
| Internet Protocol Version 4 | 50.00 % | 164 | 46.01 % | 13235 | 0.000 | 0 | 0 | 0.000 |
| User Datagram Protocol | 44.21 % | 145 | 42.31 % | 12171 | 0.000 | 0 | 0 | 0.000 |
| Data | 3.05 % | 10 | 1.11 % | 320 | 0.000 | 10 | 320 | 0.000 |
| Domain Name Service | 41.16 % | 135 | 41.20 % | 11851 | 0.000 | 135 | 11851 | 0.000 |
| Internet Control Message Protocol | 5.79 % | 19 | 3.70 % | 1064 | 0.000 | 19 | 1064 | 0.000 |

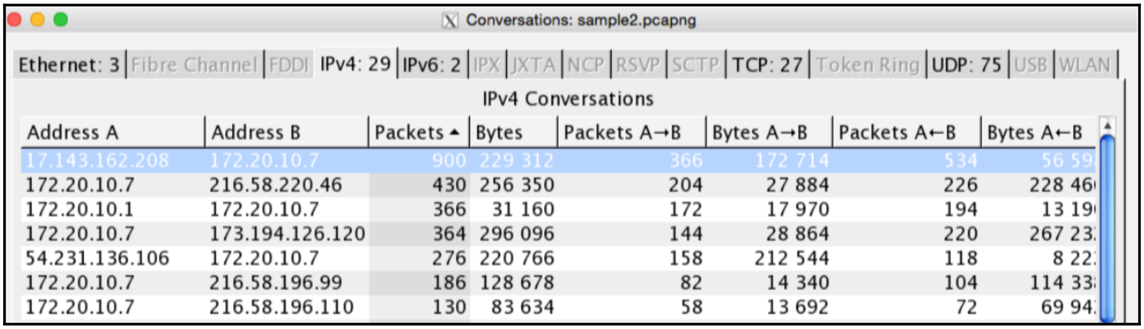




Ethernet Conversations

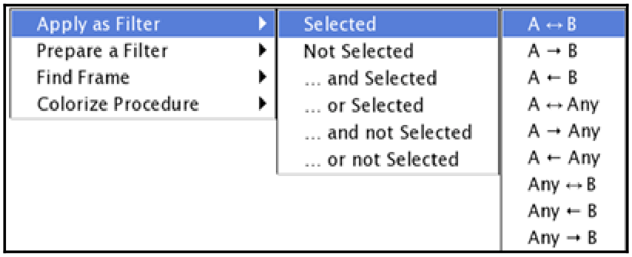
| Address A | Address B | Packets | Bytes | Packets A→B | Bytes A→B | Packets A←B | Bytes A←B |
|---|---|---|---|---|---|---|---|
| 4a:74:6e:ba:d0:64 | Apple_b9:53:ec | 1 687 | 770 341 | 820 | 637 014 | 867 | 133 3 |
| Apple_b9:53:ec | Broadcast | 3 | 276 | 3 | 276 | 0 | |
| 4a:74:6e:ba:d0:64 | Broadcast | 30 | 1 260 | 30 | 1 260 | 0 | |

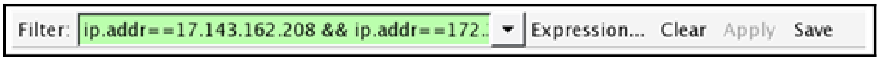
☑ Name resolution ☐ Limit to display filter

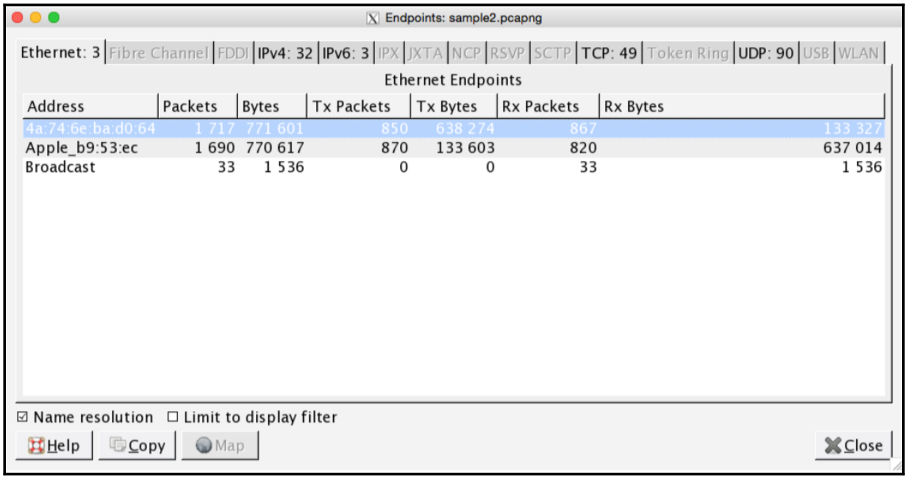


IPv4 Conversations

| Address A | Address B | Packets ▴ | Bytes | Packets A→B | Bytes A→B | Packets A←B | Bytes A←B |
|---|---|---|---|---|---|---|---|
| 17.143.162.208 | 172.20.10.7 | 900 | 229 312 | 366 | 172 714 | 534 | 56 59 |
| 172.20.10.7 | 216.58.220.46 | 430 | 256 350 | 204 | 27 884 | 226 | 228 46 |
| 172.20.10.1 | 172.20.10.7 | 366 | 31 160 | 172 | 17 970 | 194 | 13 19 |
| 172.20.10.7 | 173.194.126.120 | 364 | 296 096 | 144 | 28 864 | 220 | 267 23 |
| 54.231.136.106 | 172.20.10.7 | 276 | 220 766 | 158 | 212 544 | 118 | 8 22 |
| 172.20.10.7 | 216.58.196.99 | 186 | 128 678 | 82 | 14 340 | 104 | 114 33 |
| 172.20.10.7 | 216.58.196.110 | 130 | 83 634 | 58 | 13 692 | 72 | 69 94 |



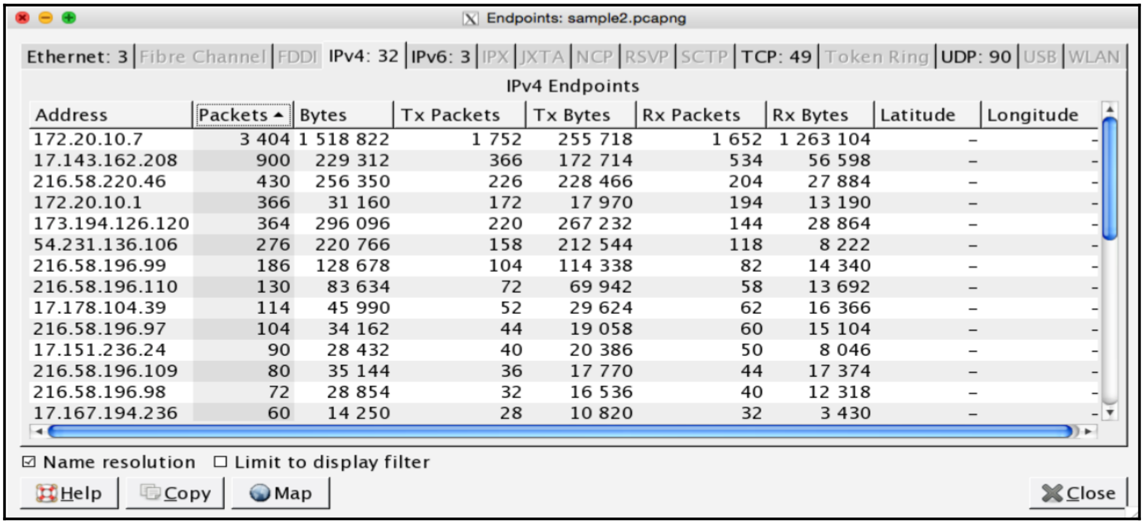

Filter: ip.addr==17.143.162.208 && ip.addr==172.


Endpoints: sample2.pcapng
Ethernet: 3 | Fibre Channel | FDDI | IPv4: 32 | IPv6: 3 | IPX | JXTA | NCP | RSVP | SCTP | TCP: 49 | Token Ring | UDP: 90 | USB | WLAN
Help
Copy
Map
Close

Ethernet Endpoints

| Address | Packets | Bytes | Tx Packets | Tx Bytes | Rx Packets | Rx Bytes |
|---|---|---|---|---|---|---|
| 4a:74:6e:ba:d0:64 | 1 717 | 771 601 | 850 | 638 274 | 867 | 133 327 |
| Apple_b9:53:ec | 1 690 | 770 617 | 870 | 133 603 | 820 | 637 014 |
| Broadcast | 33 | 1 536 | 0 | 0 | 33 | 1 536 |

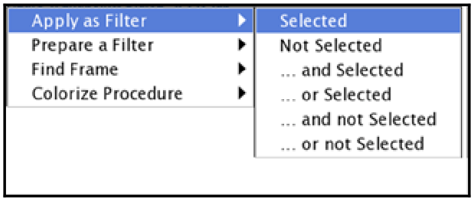
☑ Name resolution ☐ Limit to display filter

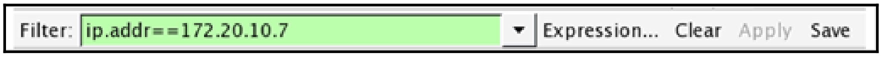

Endpoints: sample2.pcapng
Ethernet: 3 | Fibre Channel | FDDI | IPv4: 32 | IPv6: 3 | IPX | JXTA | NCP | RSVP | SCTP | TCP: 49 | Token Ring | UDP: 90 | USB | WLAN
Help
Copy
Map
Close

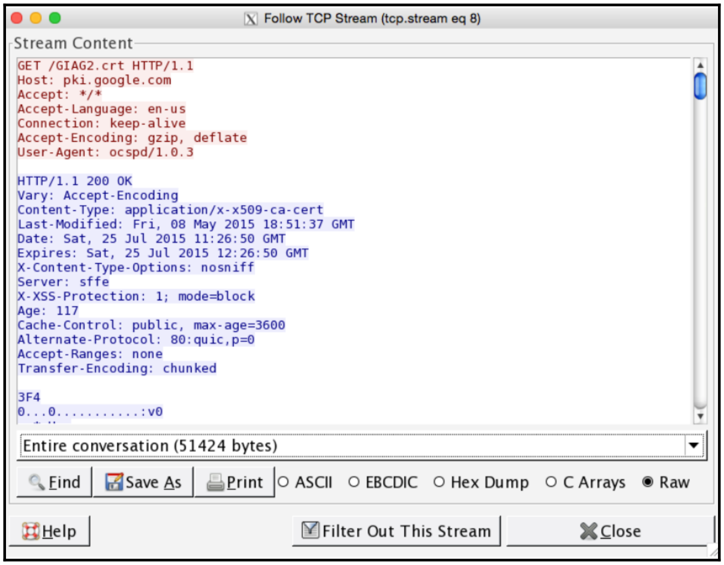
IPv4 Endpoints

| Address | Packets ▲ | Bytes | Tx Packets | Tx Bytes | Rx Packets | Rx Bytes | Latitude | Longitude |
|---|---|---|---|---|---|---|---|---|
| 172.20.10.7 | 3 404 | 1 518 822 | 1 752 | 255 718 | 1 652 | 1 263 104 | – | – |
| 17.143.162.208 | 900 | 229 312 | 366 | 172 714 | 534 | 56 598 | – | – |
| 216.58.220.46 | 430 | 256 350 | 226 | 228 466 | 204 | 27 884 | – | – |
| 172.20.10.1 | 366 | 31 160 | 172 | 17 970 | 194 | 13 190 | – | – |
| 173.194.126.120 | 364 | 296 096 | 220 | 267 232 | 144 | 28 864 | – | – |
| 54.231.136.106 | 276 | 220 766 | 158 | 212 544 | 118 | 8 222 | – | – |
| 216.58.196.99 | 186 | 128 678 | 104 | 114 338 | 82 | 14 340 | – | – |
| 216.58.196.110 | 130 | 83 634 | 72 | 69 942 | 58 | 13 692 | – | – |
| 17.178.104.39 | 114 | 45 990 | 52 | 29 624 | 62 | 16 366 | – | – |
| 216.58.196.97 | 104 | 34 162 | 44 | 19 058 | 60 | 15 104 | – | – |
| 17.151.236.24 | 90 | 28 432 | 40 | 20 386 | 50 | 8 046 | – | – |
| 216.58.196.109 | 80 | 35 144 | 36 | 17 770 | 44 | 17 374 | – | – |
| 216.58.196.98 | 72 | 28 854 | 32 | 16 536 | 40 | 12 318 | – | – |
| 17.167.194.236 | 60 | 14 250 | 28 | 10 820 | 32 | 3 430 | – | – |

☑ Name resolution ☐ Limit to display filter




Filter: ip.addr==172.20.10.7

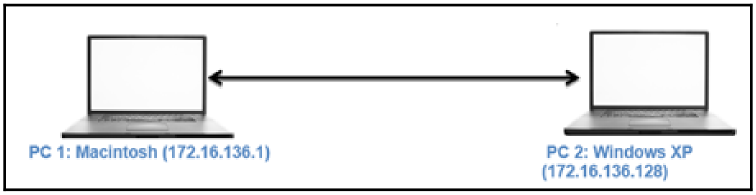


```
GET /GIAG2.crt HTTP/1.1
Host: pki.google.com
Accept: */*
Accept-Language: en-us
Connection: keep-alive
Accept-Encoding: gzip, deflate
User-Agent: ocspd/1.0.3

HTTP/1.1 200 OK
Vary: Accept-Encoding
Content-Type: application/x-x509-ca-cert
Last-Modified: Fri, 08 May 2015 18:51:37 GMT
Date: Sat, 25 Jul 2015 11:26:50 GMT
Expires: Sat, 25 Jul 2015 12:26:50 GMT
X-Content-Type-Options: nosniff
Server: sffe
X-XSS-Protection: 1; mode=block
Age: 117
Cache-Control: public, max-age=3600
Alternate-Protocol: 80:quic,p=0
Accept-Ranges: none
Transfer-Encoding: chunked

3F4
0...0...........:v0
```

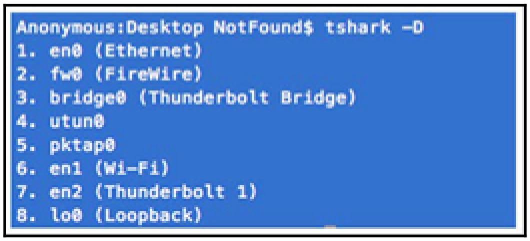
Entire conversation (51424 bytes)

○ ASCII ○ EBCDIC ○ Hex Dump ○ C Arrays ● Raw

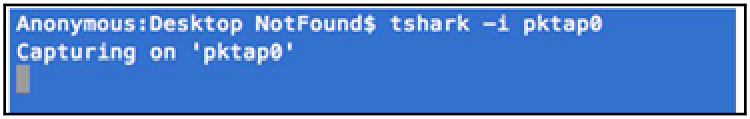
Find
Save As
Print
Help
Filter Out This Stream
Close



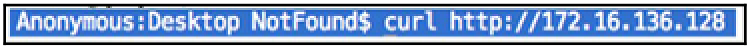
PC 1: Macintosh (172.16.136.1)
PC 2: Windows XP (172.16.136.128)



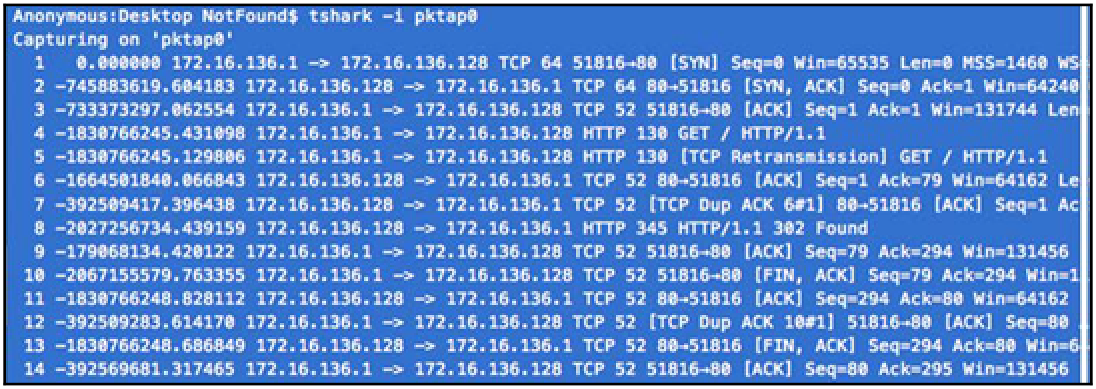
```
Anonymous:Desktop NotFound$ tshark -D
1. en0 (Ethernet)
2. fw0 (FireWire)
3. bridge0 (Thunderbolt Bridge)
4. utun0
5. pktap0
6. en1 (Wi-Fi)
7. en2 (Thunderbolt 1)
8. lo0 (Loopback)
```



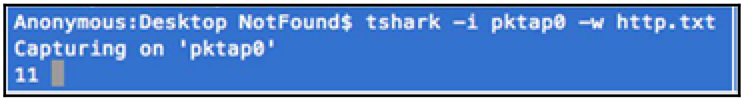
```
Anonymous:Desktop NotFound$ tshark -i pktap0
Capturing on 'pktap0'
```



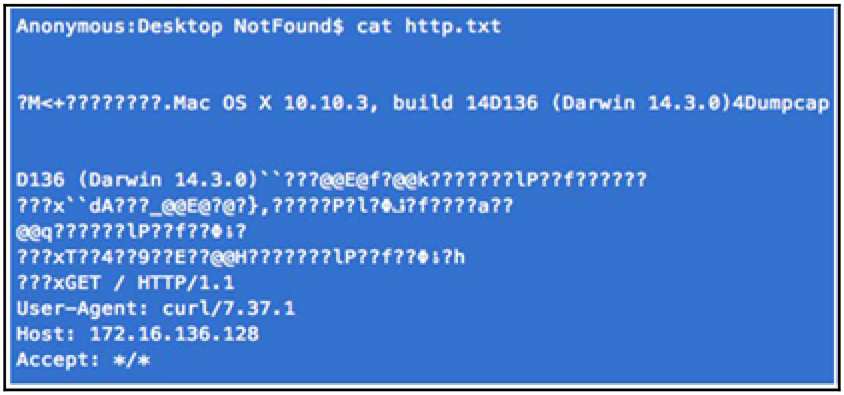
```
Anonymous:Desktop NotFound$ curl http://172.16.136.128
```



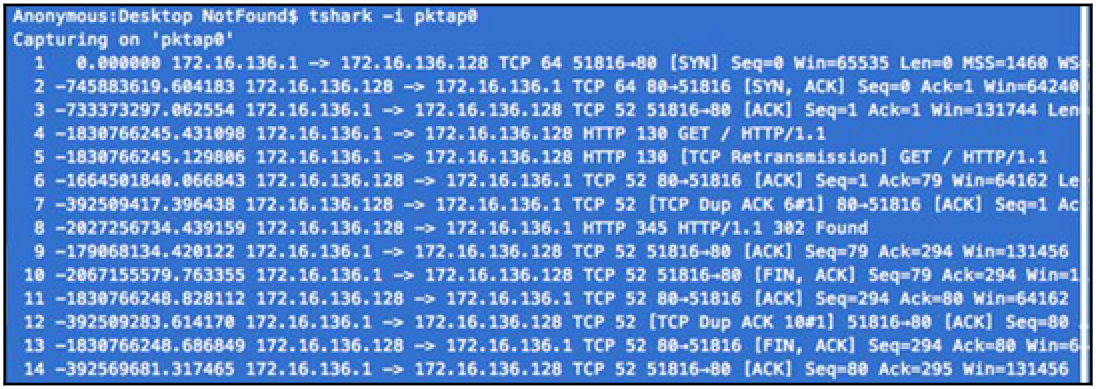
```
Anonymous:Desktop NotFound$ tshark -i pktap0
Capturing on 'pktap0'
  1   0.000000 172.16.136.1 -> 172.16.136.128 TCP 64 51816→80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS
  2 -745883619.604183 172.16.136.128 -> 172.16.136.1 TCP 64 80→51816 [SYN, ACK] Seq=0 Ack=1 Win=64240
  3 -733373297.062554 172.16.136.1 -> 172.16.136.128 TCP 52 51816→80 [ACK] Seq=1 Ack=1 Win=131744 Len
  4 -1830766245.431098 172.16.136.1 -> 172.16.136.128 HTTP 130 GET / HTTP/1.1
  5 -1830766245.129806 172.16.136.1 -> 172.16.136.128 HTTP 130 [TCP Retransmission] GET / HTTP/1.1
  6 -1664501840.066843 172.16.136.128 -> 172.16.136.1 TCP 52 80→51816 [ACK] Seq=1 Ack=79 Win=64162 Le
  7 -392509417.396438 172.16.136.128 -> 172.16.136.1 TCP 52 [TCP Dup ACK 6#1] 80→51816 [ACK] Seq=1 Ac
  8 -2027256734.439159 172.16.136.128 -> 172.16.136.1 HTTP 345 HTTP/1.1 302 Found
  9 -179068134.420122 172.16.136.1 -> 172.16.136.128 TCP 52 51816→80 [ACK] Seq=79 Ack=294 Win=131456
 10 -2067155579.763355 172.16.136.1 -> 172.16.136.128 TCP 52 51816→80 [FIN, ACK] Seq=79 Ack=294 Win=1
 11 -1830766248.828112 172.16.136.128 -> 172.16.136.1 TCP 52 80→51816 [ACK] Seq=294 Ack=80 Win=64162
 12 -392509283.614170 172.16.136.1 -> 172.16.136.128 TCP 52 [TCP Dup ACK 10#1] 51816→80 [ACK] Seq=80
 13 -1830766248.686849 172.16.136.128 -> 172.16.136.1 TCP 52 80→51816 [FIN, ACK] Seq=294 Ack=80 Win=6
 14 -392569681.317465 172.16.136.1 -> 172.16.136.128 TCP 52 51816→80 [ACK] Seq=80 Ack=295 Win=131456
```



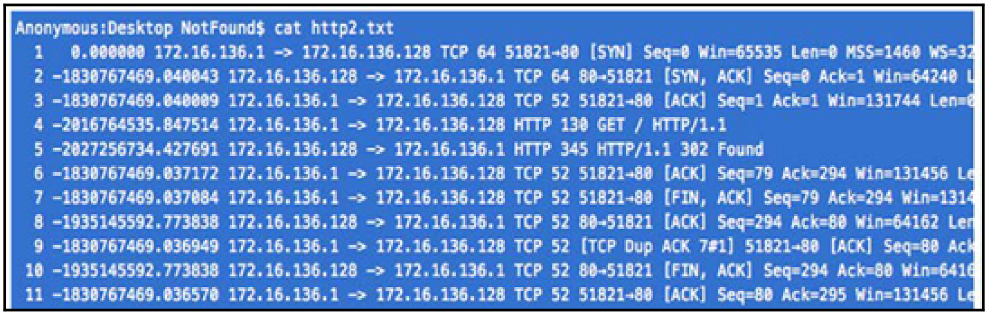
```
Anonymous:Desktop NotFound$ tshark -i pktap0 -w http.txt
Capturing on 'pktap0'
11
```



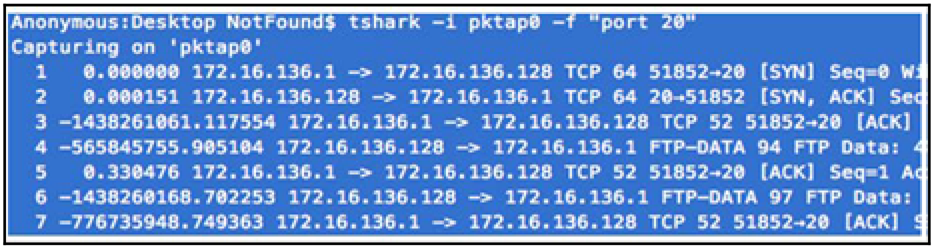
```
Anonymous:Desktop NotFound$ cat http.txt


?M<+????????.Mac OS X 10.10.3, build 14D136 (Darwin 14.3.0)4Dumpcap


D136 (Darwin 14.3.0)``???@@E@f?@@k???????lP??f??????
???x``dA???_@@E@?@?},?????P?l?●J?f????a??
@@q??????lP??f??●¡?
???xT??4??9??E??@@H???????lP??f??●¡?h
???xGET / HTTP/1.1
User-Agent: curl/7.37.1
Host: 172.16.136.128
Accept: */*
```



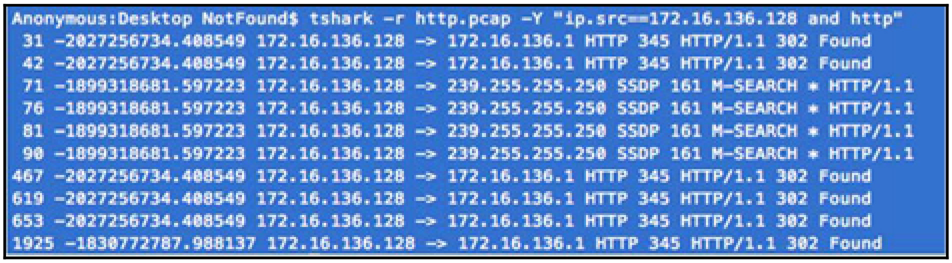
```
Anonymous:Desktop NotFound$ tshark -i pktap0
Capturing on 'pktap0'
  1   0.000000 172.16.136.1 -> 172.16.136.128 TCP 64 51816→80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS
  2 -745883619.604183 172.16.136.128 -> 172.16.136.1 TCP 64 80→51816 [SYN, ACK] Seq=0 Ack=1 Win=64240
  3 -733373297.062554 172.16.136.1 -> 172.16.136.128 TCP 52 51816→80 [ACK] Seq=1 Ack=1 Win=131744 Len
  4 -1830766245.431098 172.16.136.1 -> 172.16.136.128 HTTP 130 GET / HTTP/1.1
  5 -1830766245.129806 172.16.136.1 -> 172.16.136.128 HTTP 130 [TCP Retransmission] GET / HTTP/1.1
  6 -1664501840.066843 172.16.136.128 -> 172.16.136.1 TCP 52 80→51816 [ACK] Seq=1 Ack=79 Win=64162 Le
  7 -392509417.396438 172.16.136.128 -> 172.16.136.1 TCP 52 [TCP Dup ACK 6#1] 80→51816 [ACK] Seq=1 Ac
  8 -2027256734.439159 172.16.136.128 -> 172.16.136.1 HTTP 345 HTTP/1.1 302 Found
  9 -179068134.420122 172.16.136.1 -> 172.16.136.128 TCP 52 51816→80 [ACK] Seq=79 Ack=294 Win=131456
 10 -2067155579.763355 172.16.136.1 -> 172.16.136.128 TCP 52 51816→80 [FIN, ACK] Seq=79 Ack=294 Win=1
 11 -1830766248.828112 172.16.136.128 -> 172.16.136.1 TCP 52 80→51816 [ACK] Seq=294 Ack=80 Win=64162
 12 -392509283.614170 172.16.136.1 -> 172.16.136.128 TCP 52 [TCP Dup ACK 10#1] 51816→80 [ACK] Seq=80
 13 -1830766248.686849 172.16.136.128 -> 172.16.136.1 TCP 52 80→51816 [FIN, ACK] Seq=294 Ack=80 Win=6
 14 -392569681.317465 172.16.136.1 -> 172.16.136.128 TCP 52 51816→80 [ACK] Seq=80 Ack=295 Win=131456
```



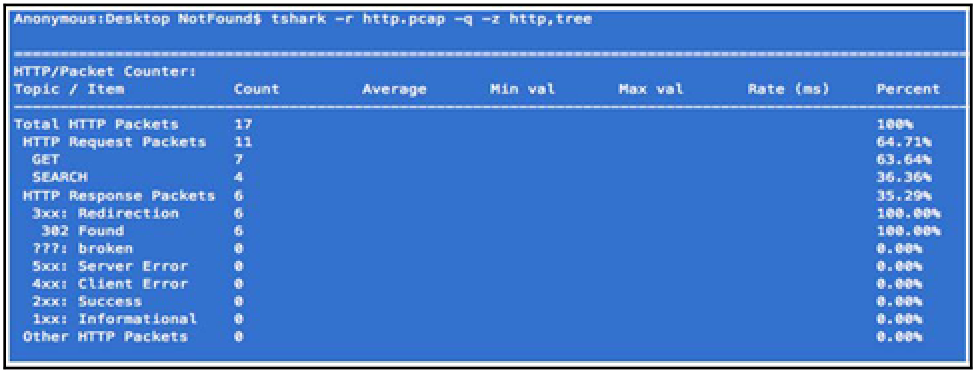
```
Anonymous:Desktop NotFound$ cat http2.txt
  1   0.000000 172.16.136.1 -> 172.16.136.128 TCP 64 51821→80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32
  2 -1830767469.040043 172.16.136.128 -> 172.16.136.1 TCP 64 80→51821 [SYN, ACK] Seq=0 Ack=1 Win=64240 L
  3 -1830767469.040009 172.16.136.1 -> 172.16.136.128 TCP 52 51821→80 [ACK] Seq=1 Ack=1 Win=131744 Len=0
  4 -2016764535.847514 172.16.136.1 -> 172.16.136.128 HTTP 130 GET / HTTP/1.1
  5 -2027256734.427691 172.16.136.128 -> 172.16.136.1 HTTP 345 HTTP/1.1 302 Found
  6 -1830767469.037172 172.16.136.1 -> 172.16.136.128 TCP 52 51821→80 [ACK] Seq=79 Ack=294 Win=131456 Le
  7 -1830767469.037084 172.16.136.1 -> 172.16.136.128 TCP 52 51821→80 [FIN, ACK] Seq=79 Ack=294 Win=1314
  8 -1935145592.773838 172.16.136.128 -> 172.16.136.1 TCP 52 80→51821 [ACK] Seq=294 Ack=80 Win=64162 Len
  9 -1830767469.036949 172.16.136.1 -> 172.16.136.128 TCP 52 [TCP Dup ACK 7#1] 51821→80 [ACK] Seq=80 Ack
 10 -1935145592.773838 172.16.136.128 -> 172.16.136.1 TCP 52 80→51821 [FIN, ACK] Seq=294 Ack=80 Win=6416
 11 -1830767469.036570 172.16.136.1 -> 172.16.136.128 TCP 52 51821→80 [ACK] Seq=80 Ack=295 Win=131456 Le
```



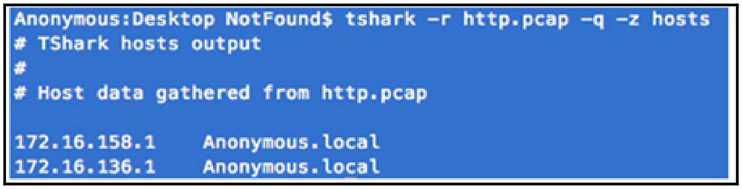
```
Anonymous:Desktop NotFound$ tshark -i pktap0 -f "port 20"
Capturing on 'pktap0'
  1   0.000000 172.16.136.1 -> 172.16.136.128 TCP 64 51852→20 [SYN] Seq=0 Wi
  2   0.000151 172.16.136.128 -> 172.16.136.1 TCP 64 20→51852 [SYN, ACK] Seq
  3 -1438261061.117554 172.16.136.1 -> 172.16.136.128 TCP 52 51852→20 [ACK]
  4 -565845755.905104 172.16.136.128 -> 172.16.136.1 FTP-DATA 94 FTP Data: 4
  5   0.330476 172.16.136.1 -> 172.16.136.128 TCP 52 51852→20 [ACK] Seq=1 Ac
  6 -1438260168.702253 172.16.136.128 -> 172.16.136.1 FTP-DATA 97 FTP Data:
  7 -776735948.749363 172.16.136.1 -> 172.16.136.128 TCP 52 51852→20 [ACK] S
```



```
Anonymous:Desktop NotFound$ tshark -r http.pcap -Y "ip.src==172.16.136.128 and http"
 31 -2027256734.408549 172.16.136.128 -> 172.16.136.1 HTTP 345 HTTP/1.1 302 Found
 42 -2027256734.408549 172.16.136.128 -> 172.16.136.1 HTTP 345 HTTP/1.1 302 Found
 71 -1899318681.597223 172.16.136.128 -> 239.255.255.250 SSDP 161 M-SEARCH * HTTP/1.1
 76 -1899318681.597223 172.16.136.128 -> 239.255.255.250 SSDP 161 M-SEARCH * HTTP/1.1
 81 -1899318681.597223 172.16.136.128 -> 239.255.255.250 SSDP 161 M-SEARCH * HTTP/1.1
 90 -1899318681.597223 172.16.136.128 -> 239.255.255.250 SSDP 161 M-SEARCH * HTTP/1.1
467 -2027256734.408549 172.16.136.128 -> 172.16.136.1 HTTP 345 HTTP/1.1 302 Found
619 -2027256734.408549 172.16.136.128 -> 172.16.136.1 HTTP 345 HTTP/1.1 302 Found
653 -2027256734.408549 172.16.136.128 -> 172.16.136.1 HTTP 345 HTTP/1.1 302 Found
1925 -1830772787.988137 172.16.136.128 -> 172.16.136.1 HTTP 345 HTTP/1.1 302 Found
```



```
Anonymous:Desktop NotFound$ tshark -r http.pcap -q -z http,tree

===================================================================================================
HTTP/Packet Counter:
Topic / Item            Count         Average       Min val       Max val       Rate (ms)     Percent
---------------------------------------------------------------------------------------------------
Total HTTP Packets      17                                                                    100%
 HTTP Request Packets   11                                                                    64.71%
  GET                   7                                                                     63.64%
  SEARCH                4                                                                     36.36%
 HTTP Response Packets  6                                                                     35.29%
  3xx: Redirection      6                                                                     100.00%
   302 Found            6                                                                     100.00%
  ???: broken           0                                                                     0.00%
  5xx: Server Error     0                                                                     0.00%
  4xx: Client Error     0                                                                     0.00%
  2xx: Success          0                                                                     0.00%
  1xx: Informational    0                                                                     0.00%
 Other HTTP Packets     0                                                                     0.00%
```



```
Anonymous:Desktop NotFound$ tshark -r http.pcap -q -z hosts
# TShark hosts output
#
# Host data gathered from http.pcap

172.16.158.1    Anonymous.local
172.16.136.1    Anonymous.local
```