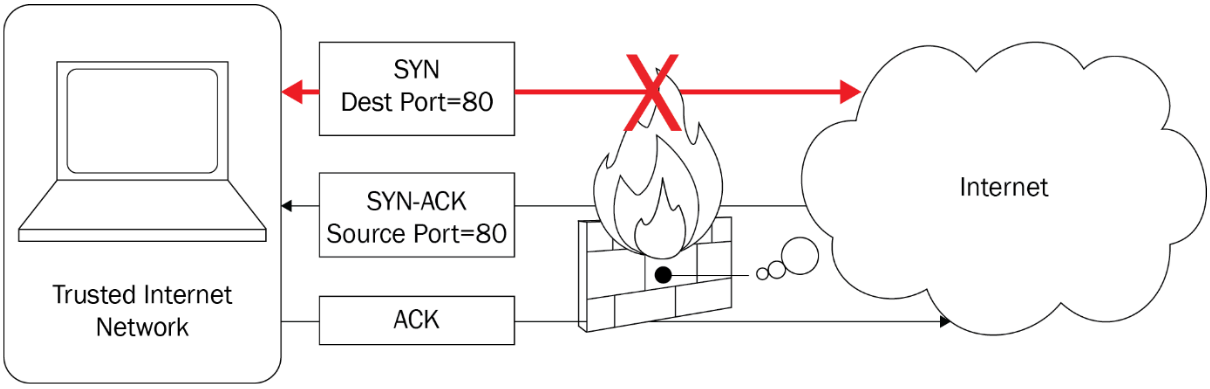
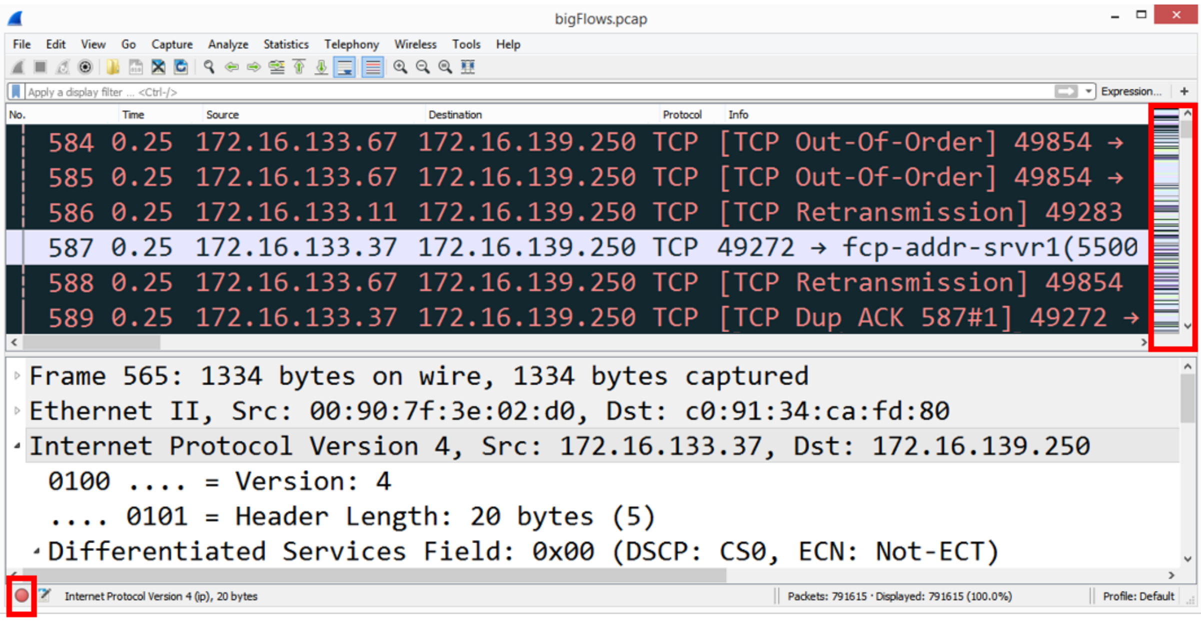
Chapter 1: Appreciating Traffic Analysis

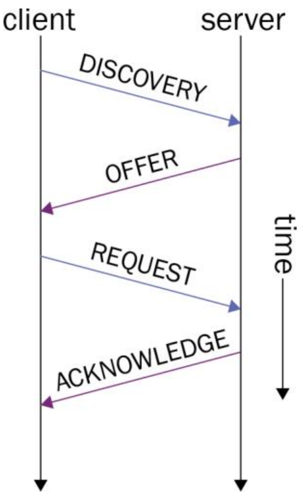


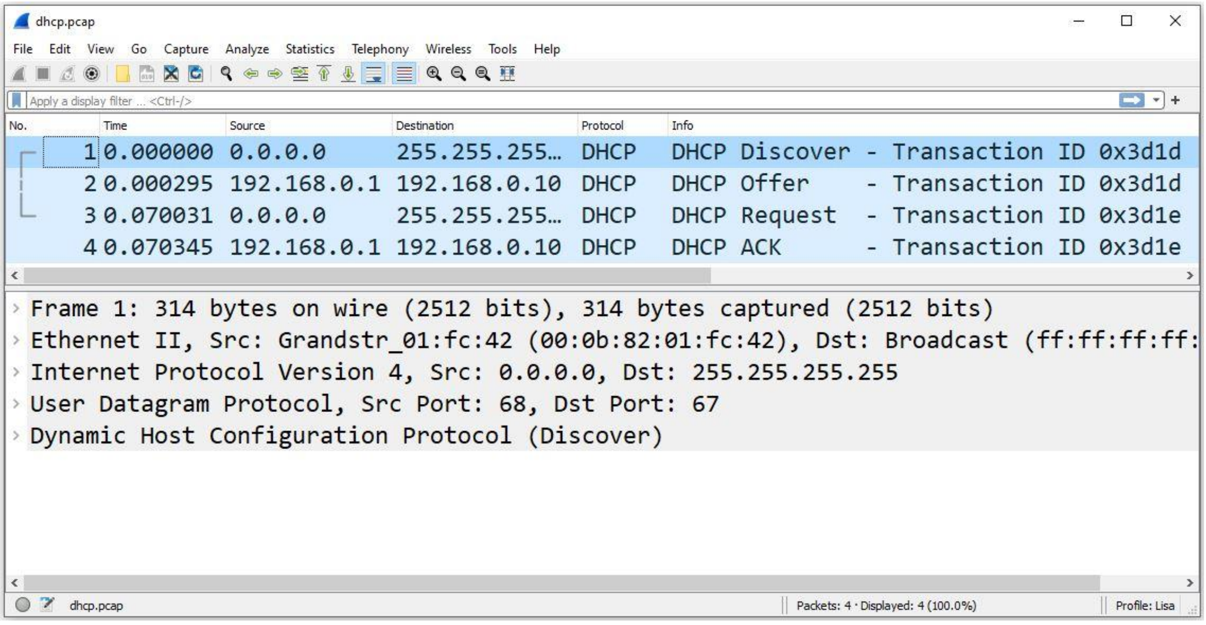

bigFlows.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Info

```
584 0.25 172.16.133.67 172.16.139.250 TCP [TCP Out-Of-Order] 49854 →
585 0.25 172.16.133.67 172.16.139.250 TCP [TCP Out-Of-Order] 49854 →
586 0.25 172.16.133.11 172.16.139.250 TCP [TCP Retransmission] 49283
587 0.25 172.16.133.37 172.16.139.250 TCP 49272 → fcp-addr-srvr1(5500
588 0.25 172.16.133.67 172.16.139.250 TCP [TCP Retransmission] 49854
589 0.25 172.16.133.37 172.16.139.250 TCP [TCP Dup ACK 587#1] 49272 →
```

```
Frame 565: 1334 bytes on wire, 1334 bytes captured
Ethernet II, Src: 00:90:7f:3e:02:d0, Dst: c0:91:34:ca:fd:80
Internet Protocol Version 4, Src: 172.16.133.37, Dst: 172.16.139.250
 0100 .... = Version: 4
 .... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
```

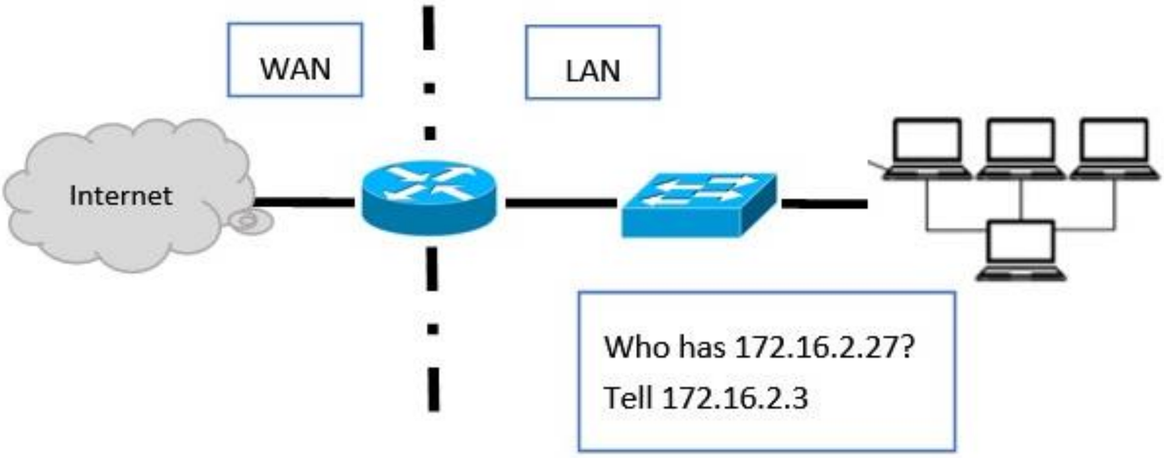
Internet Protocol Version 4 (ip), 20 bytes | Packets: 791615 · Displayed: 791615 (100.0%) | Profile: Default



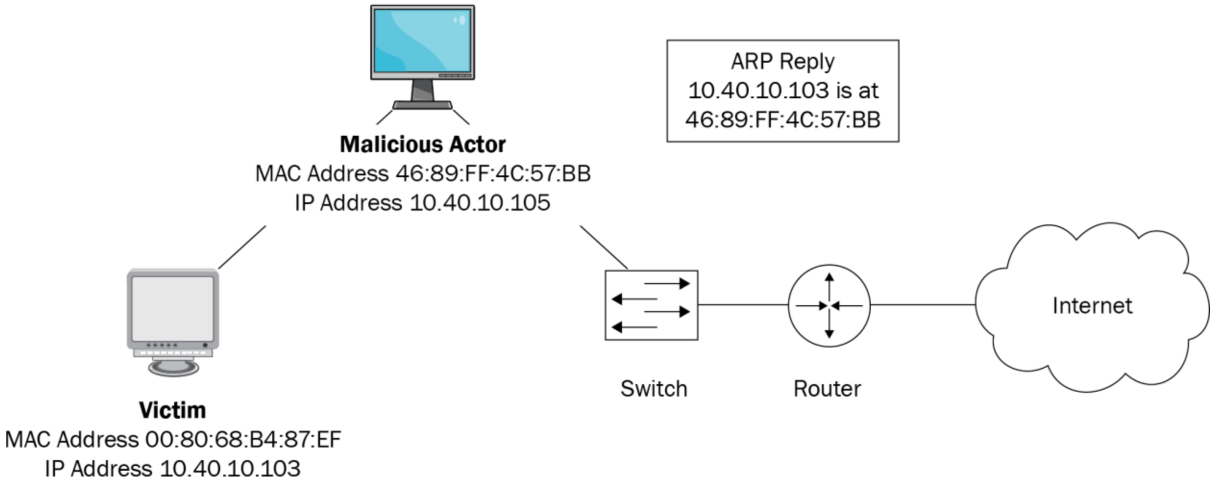

dhcp.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Packets: 4 · Displayed: 4 (100.0%)
Profile: Lisa

```
No. Time      Source      Destination    Protocol Info
  1 0.000000  0.0.0.0     255.255.255…   DHCP     DHCP Discover - Transaction ID 0x3d1d
  2 0.000295  192.168.0.1 192.168.0.10   DHCP     DHCP Offer    - Transaction ID 0x3d1d
  3 0.070031  0.0.0.0     255.255.255…   DHCP     DHCP Request  - Transaction ID 0x3d1e
  4 0.070345  192.168.0.1 192.168.0.10   DHCP     DHCP ACK      - Transaction ID 0x3d1e
```

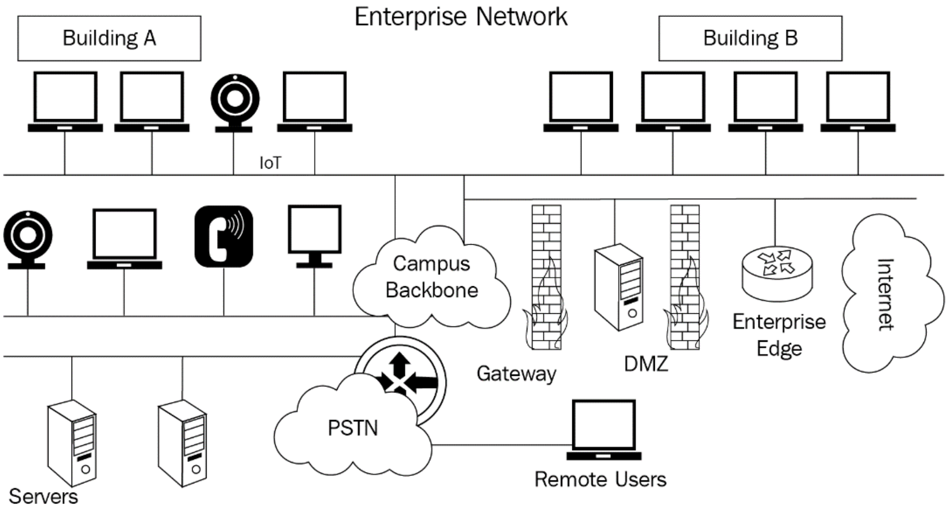
```
> Frame 1: 314 bytes on wire (2512 bits), 314 bytes captured (2512 bits)
> Ethernet II, Src: Grandstr_01:fc:42 (00:0b:82:01:fc:42), Dst: Broadcast (ff:ff:ff:ff:
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 68, Dst Port: 67
> Dynamic Host Configuration Protocol (Discover)
```

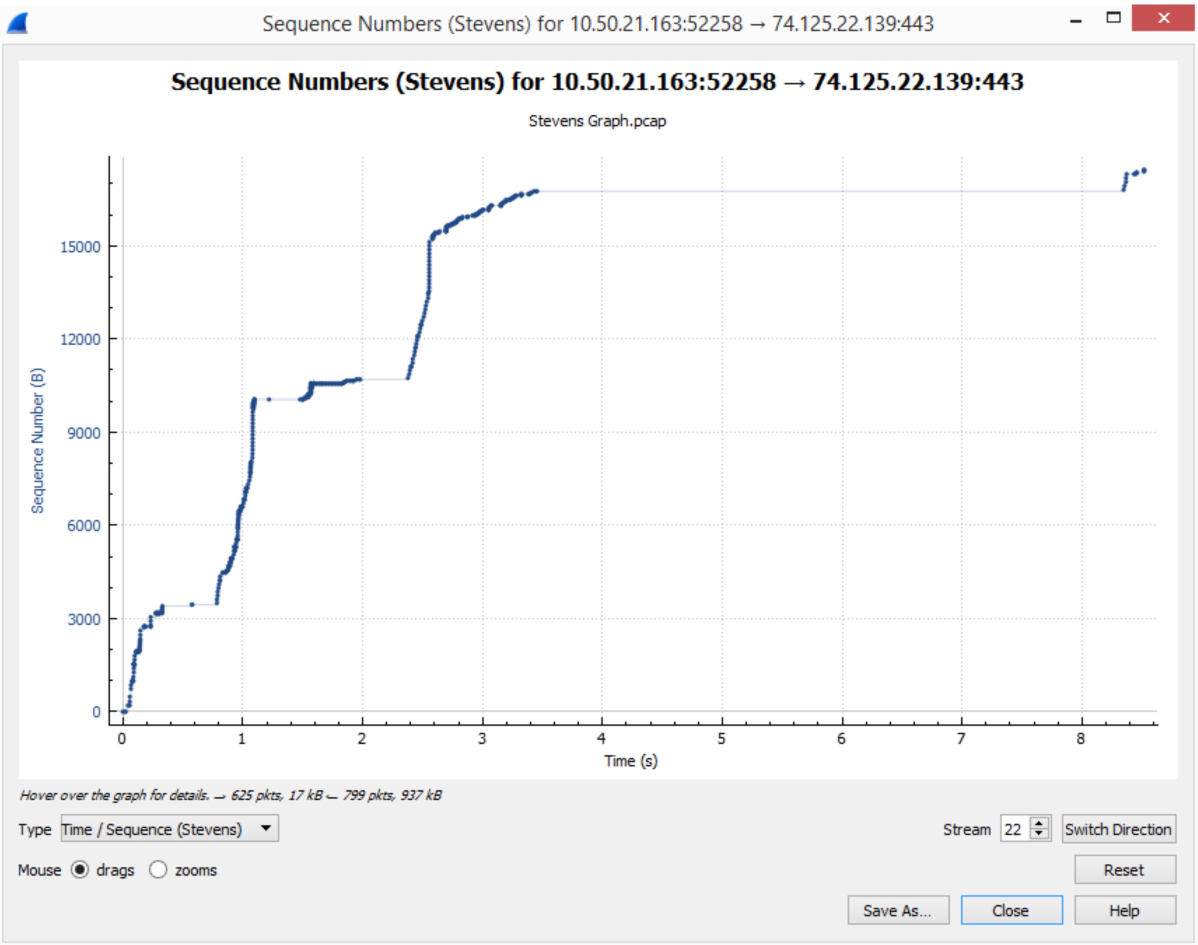


Who has 172.16.2.27?
Tell 172.16.2.3



ARP Reply
10.40.10.103 is at
46:89:FF:4C:57:BB




Sequence Numbers (Stevens) for 10.50.21.163:52258 → 74.125.22.139:443

Sequence Numbers (Stevens) for 10.50.21.163:52258 → 74.125.22.139:443

Stevens Graph.pcap

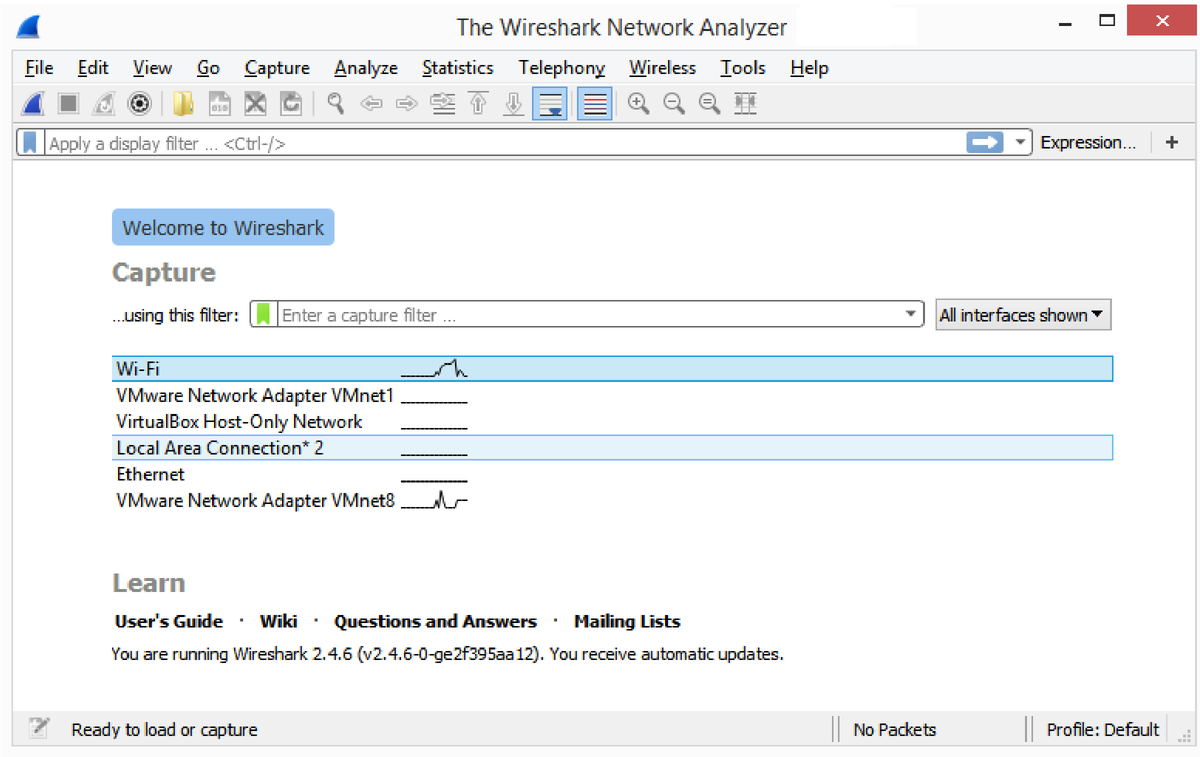
Hover over the graph for details. — 625 pkts, 17 kB — 799 pkts, 937 kB

Type: Time / Sequence (Stevens)

Stream: 22

Mouse ● drags ○ zooms

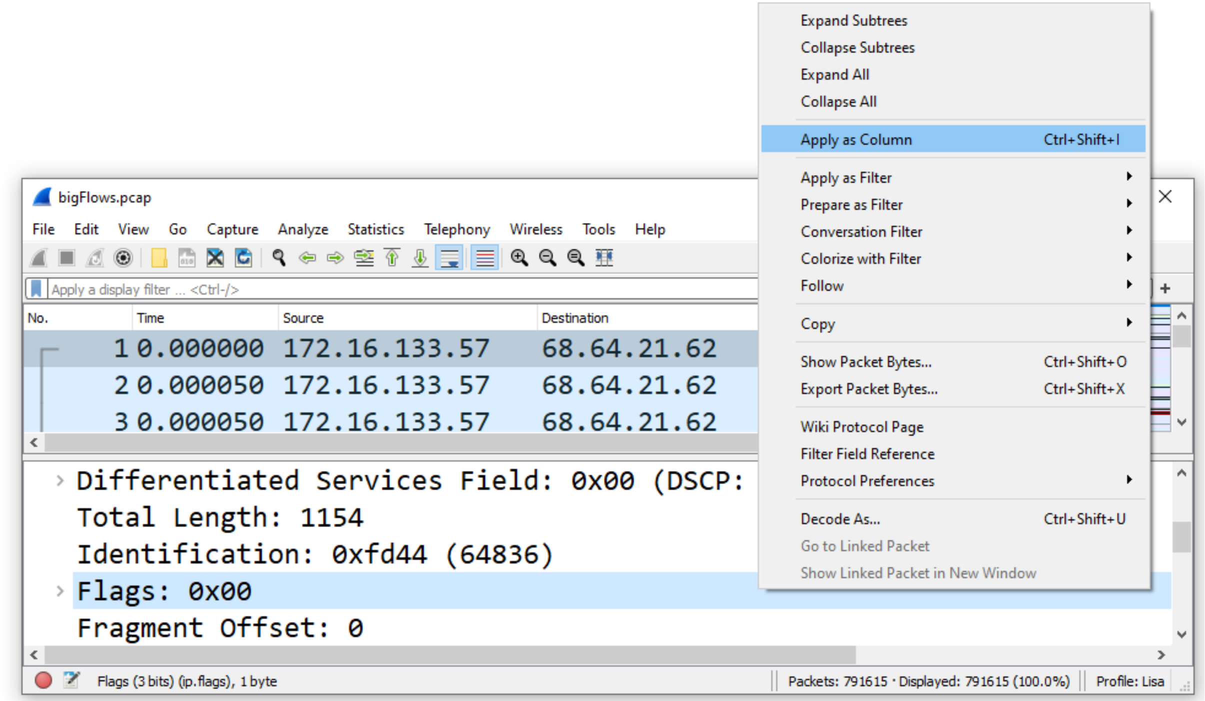
Chapter 2: Using Wireshark


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
+
Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...
All interfaces shown
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists

Wi-Fi
VMware Network Adapter VMnet1
VirtualBox Host-Only Network
Local Area Connection* 2
Ethernet
VMware Network Adapter VMnet8

You are running Wireshark 2.4.6 (v2.4.6-0-ge2f395aa12). You receive automatic updates.

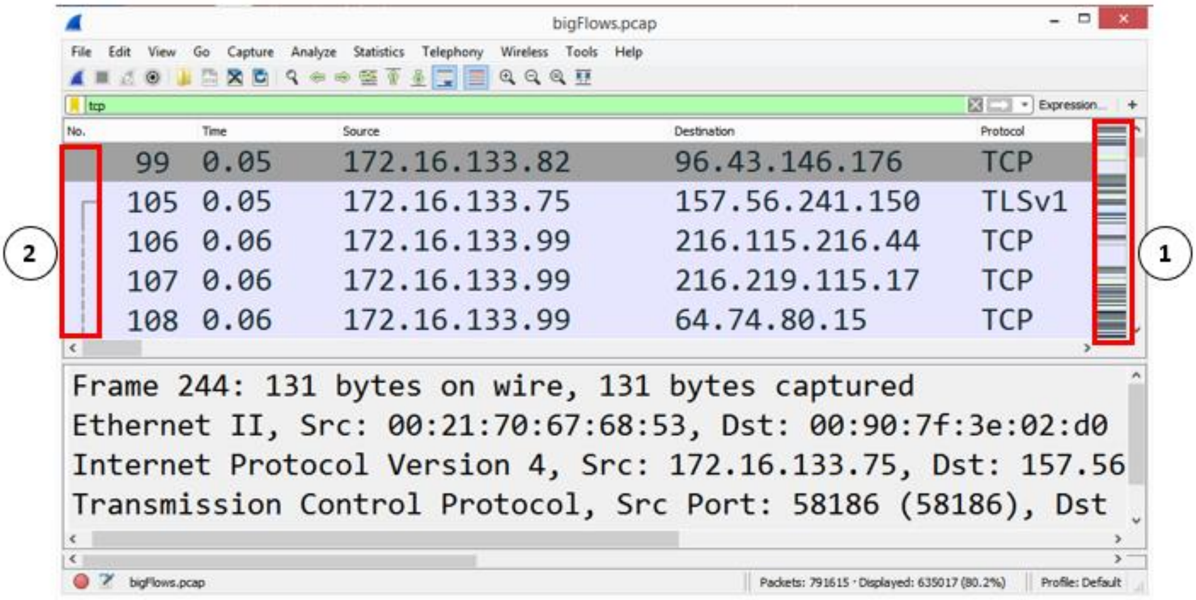
Ready to load or capture | No Packets | Profile: Default


Expand Subtrees
Collapse Subtrees
Expand All
Collapse All
Apply as Column Ctrl+Shift+I
Apply as Filter
Prepare as Filter
Conversation Filter
Colorize with Filter
Follow
Copy
Show Packet Bytes... Ctrl+Shift+O
Export Packet Bytes... Ctrl+Shift+X
Wiki Protocol Page
Filter Field Reference
Protocol Preferences
Decode As... Ctrl+Shift+U
Go to Linked Packet
Show Linked Packet in New Window
bigFlows.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  Time       Source          Destination
   1 0.000000  172.16.133.57   68.64.21.62
   2 0.000050  172.16.133.57   68.64.21.62
   3 0.000050  172.16.133.57   68.64.21.62
```

```
> Differentiated Services Field: 0x00 (DSCP:
  Total Length: 1154
  Identification: 0xfd44 (64836)
> Flags: 0x00
  Fragment Offset: 0
```

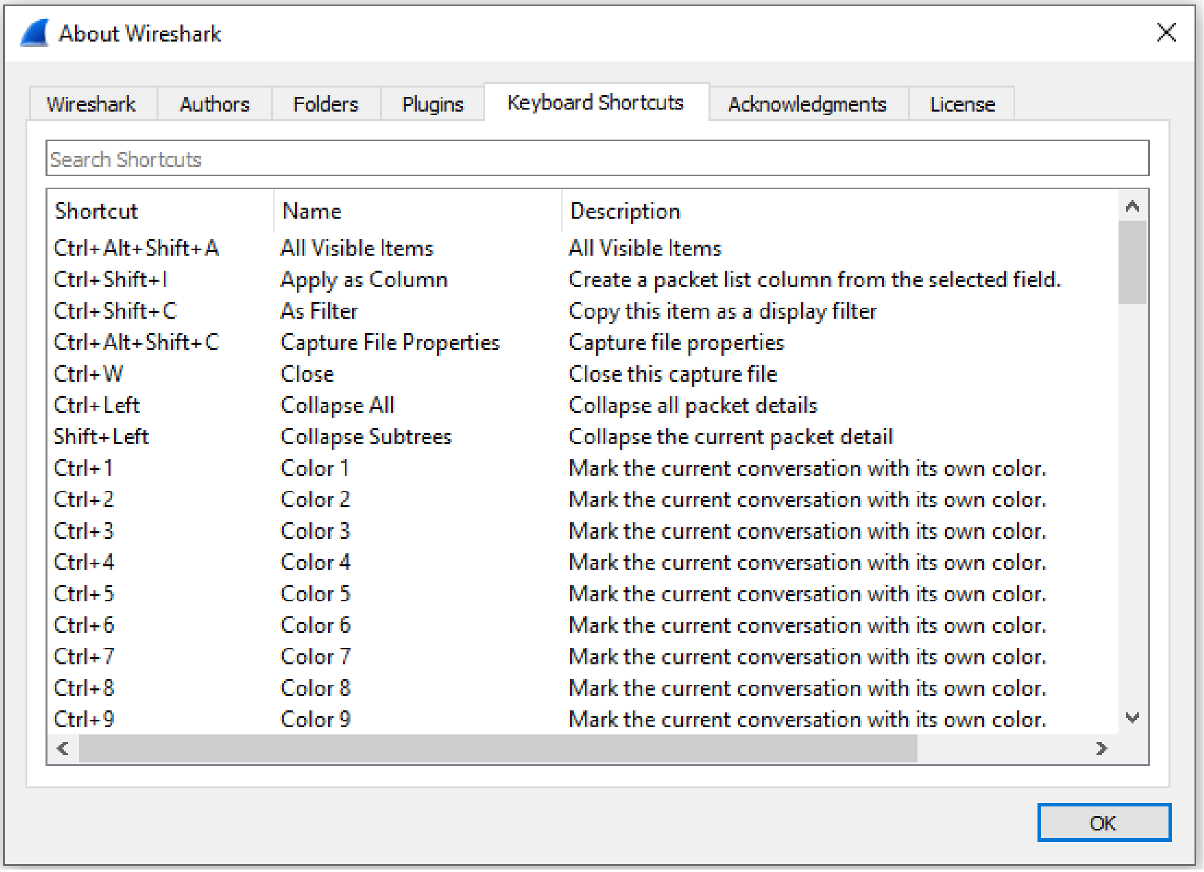
Flags (3 bits) (ip.flags), 1 byte | Packets: 791615 · Displayed: 791615 (100.0%) | Profile: Lisa


bigFlows.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp
Expression…
2
1

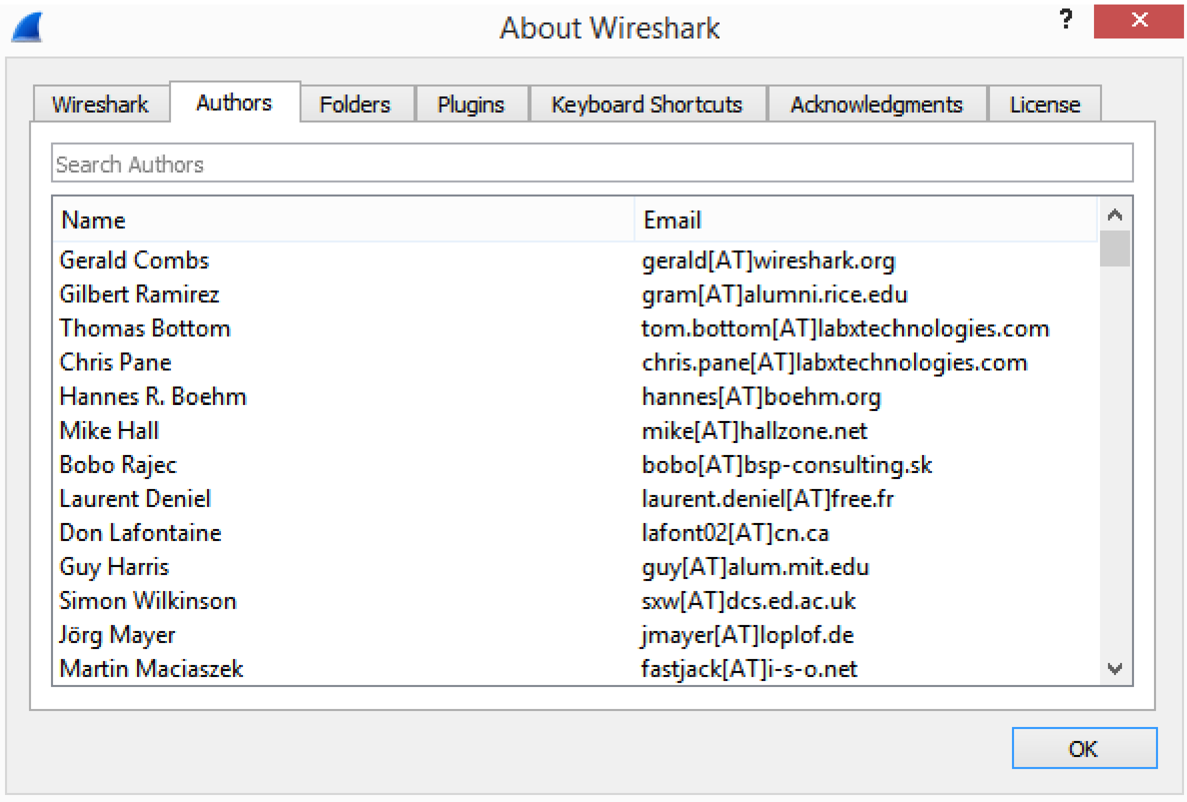
No.	Time	Source	Destination	Protocol
99	0.05	172.16.133.82	96.43.146.176	TCP
105	0.05	172.16.133.75	157.56.241.150	TLSv1
106	0.06	172.16.133.99	216.115.216.44	TCP
107	0.06	172.16.133.99	216.219.115.17	TCP
108	0.06	172.16.133.99	64.74.80.15	TCP

```
Frame 244: 131 bytes on wire, 131 bytes captured
Ethernet II, Src: 00:21:70:67:68:53, Dst: 00:90:7f:3e:02:d0
Internet Protocol Version 4, Src: 172.16.133.75, Dst: 157.56
Transmission Control Protocol, Src Port: 58186 (58186), Dst
```

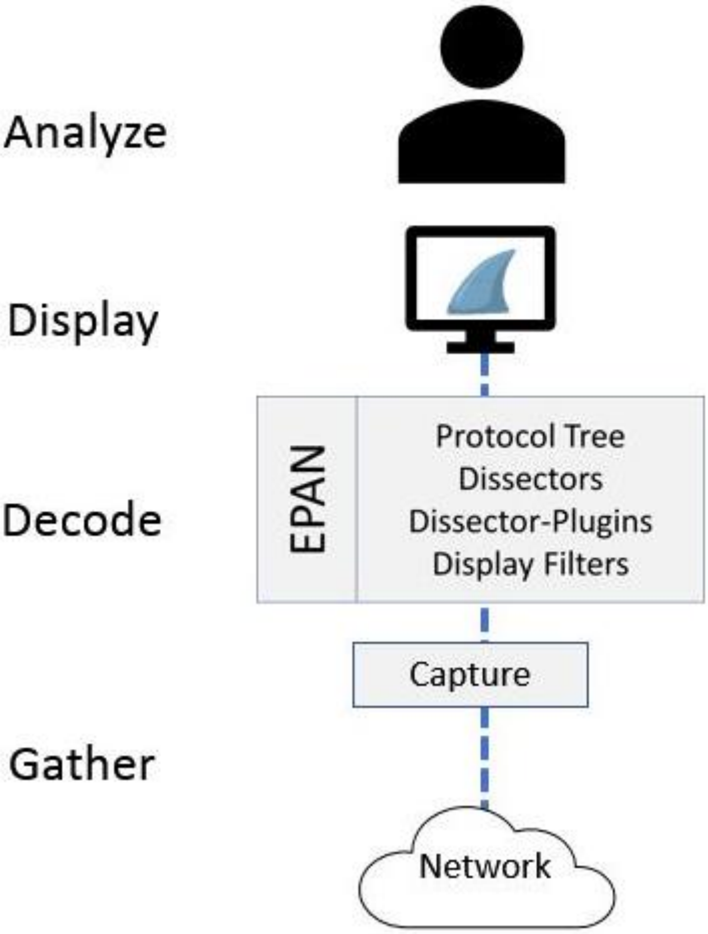
bigFlows.pcap | Packets: 791615 · Displayed: 635017 (80.2%) | Profile: Default

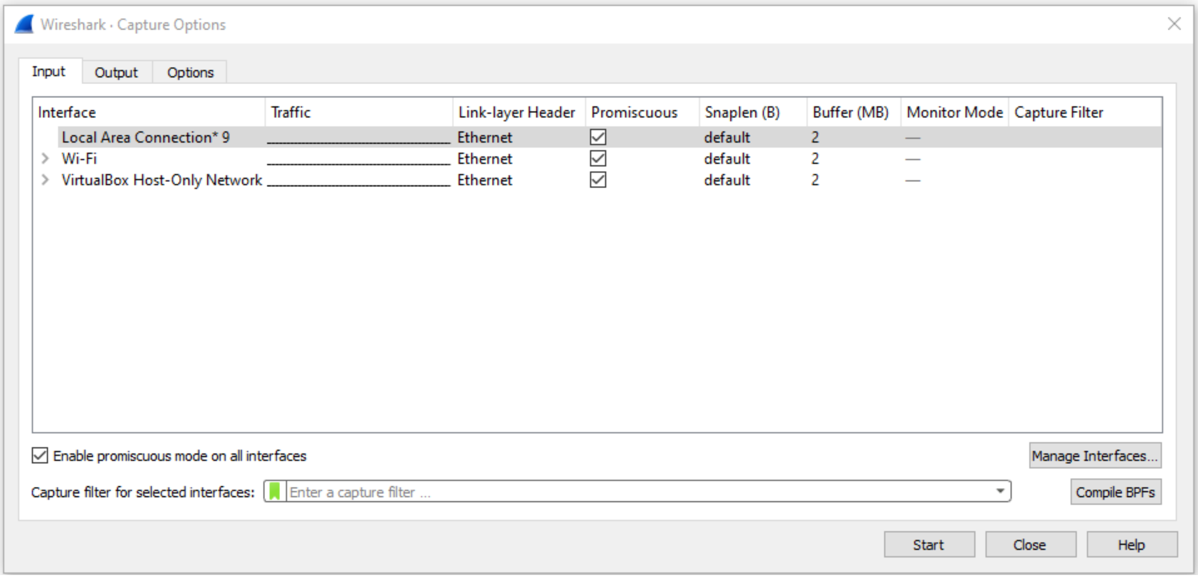


Shortcut	Name	Description
Ctrl+Alt+Shift+A	All Visible Items	All Visible Items
Ctrl+Shift+I	Apply as Column	Create a packet list column from the selected field.
Ctrl+Shift+C	As Filter	Copy this item as a display filter
Ctrl+Alt+Shift+C	Capture File Properties	Capture file properties
Ctrl+W	Close	Close this capture file
Ctrl+Left	Collapse All	Collapse all packet details
Shift+Left	Collapse Subtrees	Collapse the current packet detail
Ctrl+1	Color 1	Mark the current conversation with its own color.
Ctrl+2	Color 2	Mark the current conversation with its own color.
Ctrl+3	Color 3	Mark the current conversation with its own color.
Ctrl+4	Color 4	Mark the current conversation with its own color.
Ctrl+5	Color 5	Mark the current conversation with its own color.
Ctrl+6	Color 6	Mark the current conversation with its own color.
Ctrl+7	Color 7	Mark the current conversation with its own color.
Ctrl+8	Color 8	Mark the current conversation with its own color.
Ctrl+9	Color 9	Mark the current conversation with its own color.



Name	Email
Gerald Combs	gerald[AT]wireshark.org
Gilbert Ramirez	gram[AT]alumni.rice.edu
Thomas Bottom	tom.bottom[AT]labxtechnologies.com
Chris Pane	chris.pane[AT]labxtechnologies.com
Hannes R. Boehm	hannes[AT]boehm.org
Mike Hall	mike[AT]hallzone.net
Bobo Rajec	bobo[AT]bsp-consulting.sk
Laurent Deniel	laurent.deniel[AT]free.fr
Don Lafontaine	lafont02[AT]cn.ca
Guy Harris	guy[AT]alum.mit.edu
Simon Wilkinson	sxw[AT]dcs.ed.ac.uk
Jörg Mayer	jmayer[AT]loplof.de
Martin Maciaszek	fastjack[AT]i-s-o.net

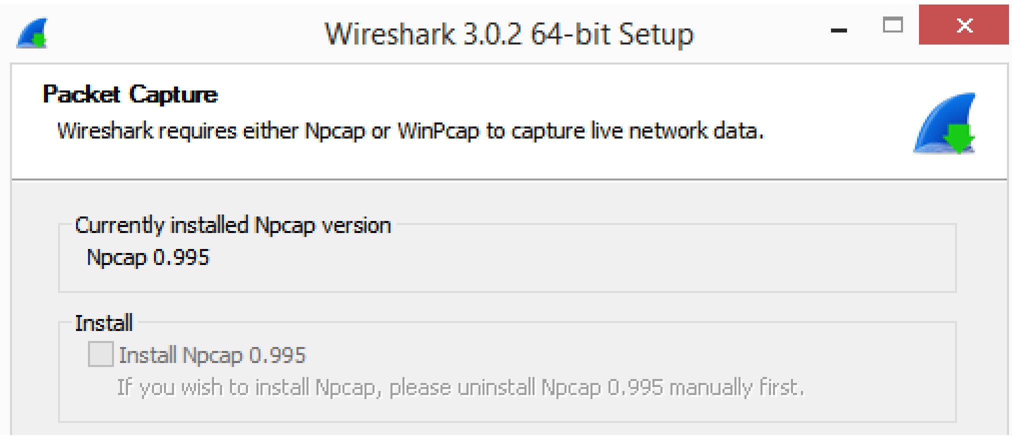




Interface	Traffic	Link-layer Header	Promiscuous	Snaplen (B)	Buffer (MB)	Monitor Mode	Capture Filter
Local Area Connection* 9		Ethernet	☑	default	2	—	
Wi-Fi		Ethernet	☑	default	2	—	
VirtualBox Host-Only Network		Ethernet	☑	default	2	—	

☑ Enable promiscuous mode on all interfaces

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



Wireshark 3.0.2 64-bit Setup

Packet Capture

Wireshark requires either Npcap or WinPcap to capture live network data.

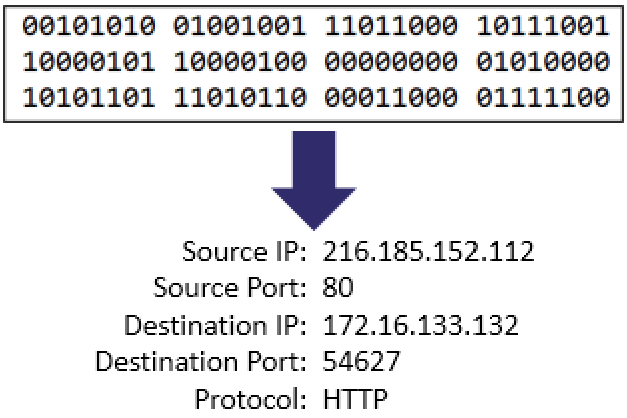
Currently installed Npcap version

Npcap 0.995

Install

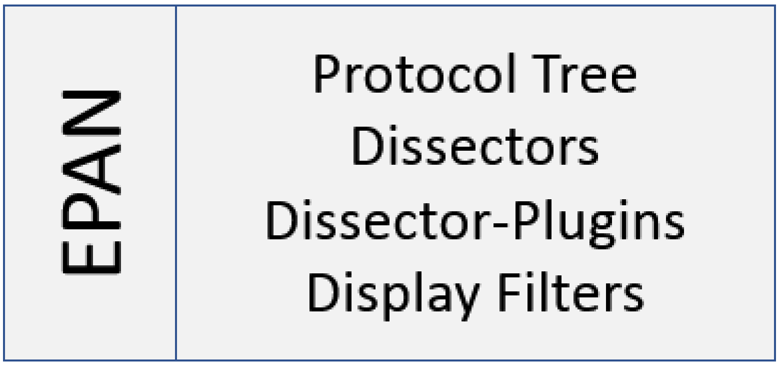
□ Install Npcap 0.995

If you wish to install Npcap, please uninstall Npcap 0.995 manually first.



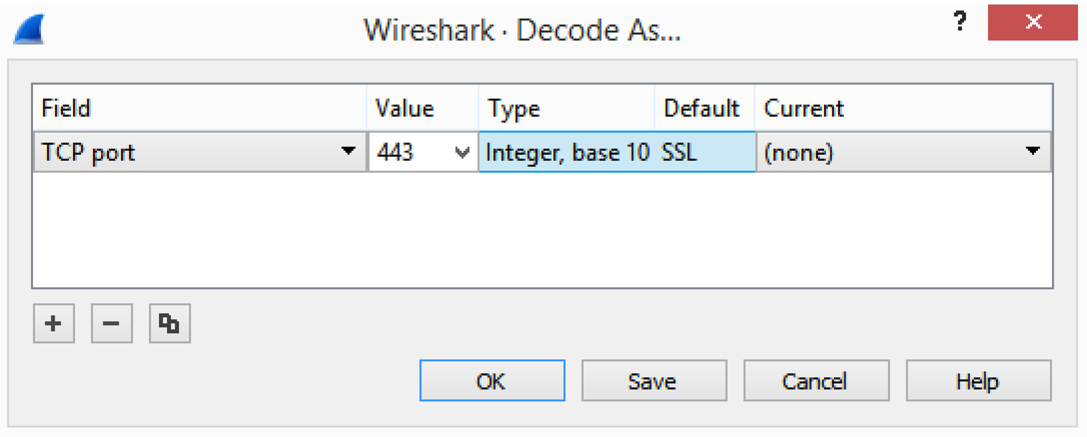
```
00101010 01001001 11011000 10111001
10000101 10000100 00000000 01010000
10101101 11010110 00011000 01111100
```

Source IP: 216.185.152.112
Source Port: 80
Destination IP: 172.16.133.132
Destination Port: 54627
Protocol: HTTP



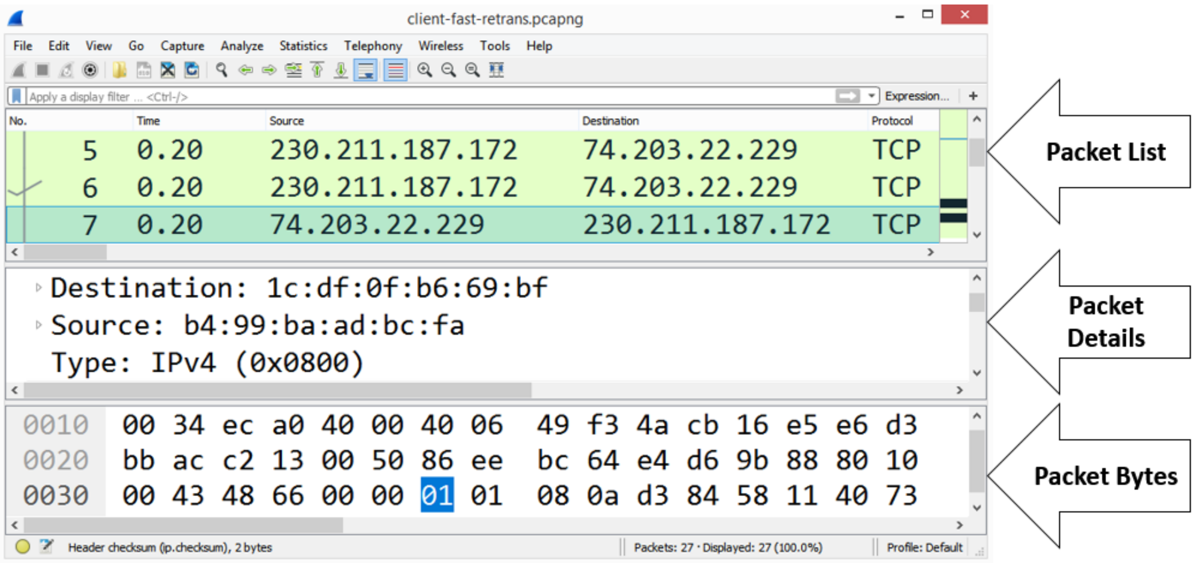
EPAN

Protocol Tree
Dissectors
Dissector-Plugins
Display Filters



Wireshark · Decode As…

Field	Value	Type	Default	Current
TCP port	443	Integer, base 10	SSL	(none)



client-fast-retrans.pcapng

```
No.  Time  Source           Destination      Protocol
  5  0.20  230.211.187.172  74.203.22.229    TCP
  6  0.20  230.211.187.172  74.203.22.229    TCP
  7  0.20  74.203.22.229    230.211.187.172  TCP
```

```
 Destination: 1c:df:0f:b6:69:bf
 Source: b4:99:ba:ad:bc:fa
 Type: IPv4 (0x0800)
```

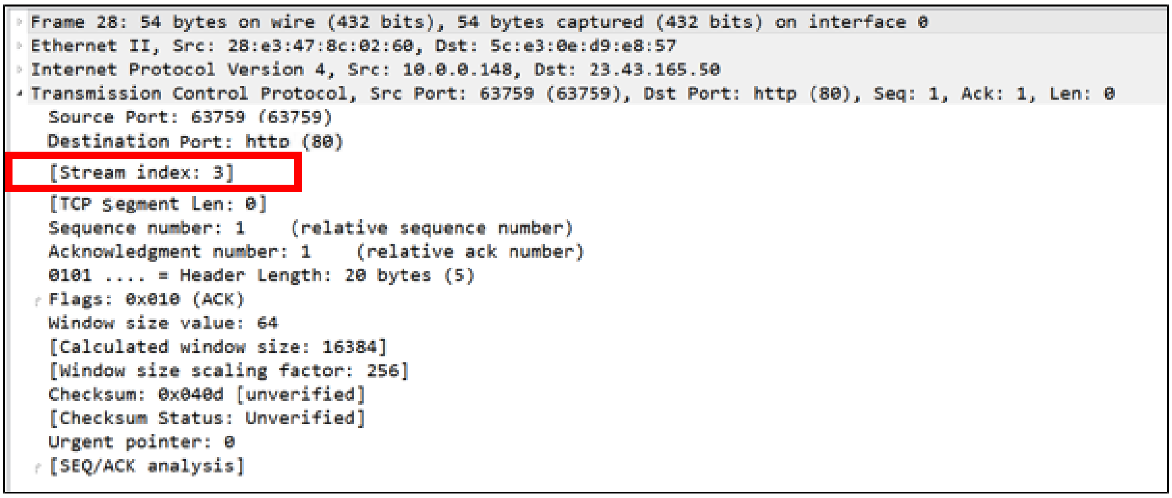
```
0010  00 34 ec a0 40 00 40 06  49 f3 4a cb 16 e5 e6 d3
0020  bb ac c2 13 00 50 86 ee  bc 64 e4 d6 9b 88 80 10
0030  00 43 48 66 00 00 01 01  08 0a d3 84 58 11 40 73
```

Header checksum (ip.checksum), 2 bytes | Packets: 27 · Displayed: 27 (100.0%) | Profile: Default

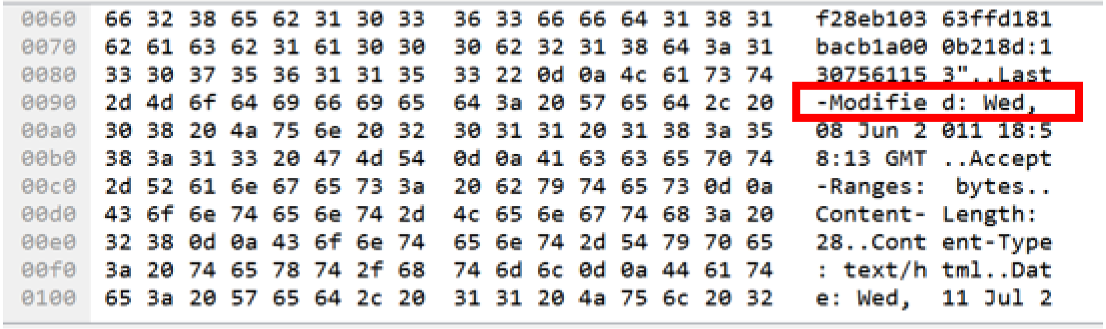
Packet List

Packet Details

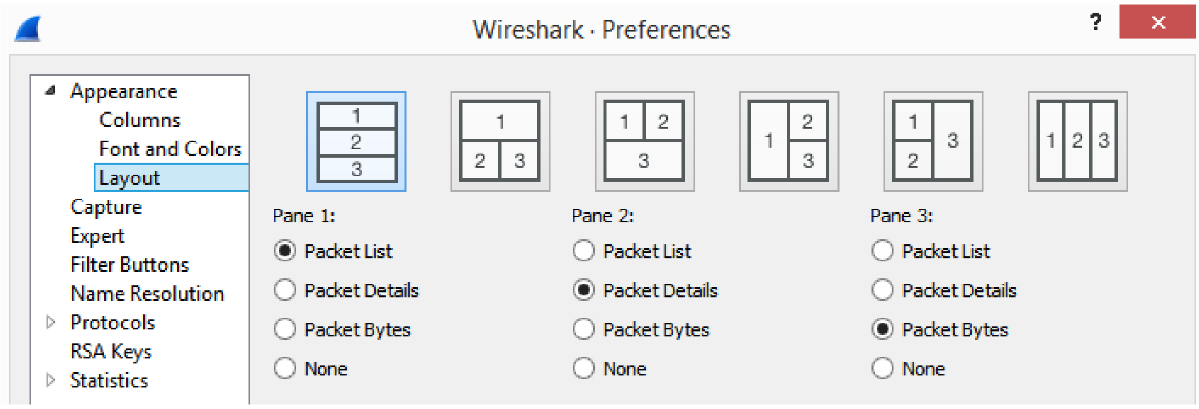
Packet Bytes



```
▸ Frame 28: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
▸ Ethernet II, Src: 28:e3:47:8c:02:60, Dst: 5c:e3:0e:d9:e8:57
▸ Internet Protocol Version 4, Src: 10.0.0.148, Dst: 23.43.165.50
▴ Transmission Control Protocol, Src Port: 63759 (63759), Dst Port: http (80), Seq: 1, Ack: 1, Len: 0
    Source Port: 63759 (63759)
    Destination Port: http (80)
    [Stream index: 3]
    [TCP Segment Len: 0]
    Sequence number: 1    (relative sequence number)
    Acknowledgment number: 1    (relative ack number)
    0101 .... = Header Length: 20 bytes (5)
  ▸ Flags: 0x010 (ACK)
    Window size value: 64
    [Calculated window size: 16384]
    [Window size scaling factor: 256]
    Checksum: 0x040d [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  ▸ [SEQ/ACK analysis]
```



```
0060  66 32 38 65 62 31 30 33  36 33 66 66 64 31 38 31   f28eb103 63ffd181
0070  62 61 63 62 31 61 30 30  30 62 32 31 38 64 3a 31   bacb1a00 0b218d:1
0080  33 30 37 35 36 31 31 35  33 22 0d 0a 4c 61 73 74   30756115 3"..Last
0090  2d 4d 6f 64 69 66 69 65  64 3a 20 57 65 64 2c 20   -Modifie d: Wed,
00a0  30 38 20 4a 75 6e 20 32  30 31 31 20 31 38 3a 35   08 Jun 2 011 18:5
00b0  38 3a 31 33 20 47 4d 54  0d 0a 41 63 63 65 70 74   8:13 GMT ..Accept
00c0  2d 52 61 6e 67 65 73 3a  20 62 79 74 65 73 0d 0a   -Ranges:  bytes..
00d0  43 6f 6e 74 65 6e 74 2d  4c 65 6e 67 74 68 3a 20   Content- Length:
00e0  32 38 0d 0a 43 6f 6e 74  65 6e 74 2d 54 79 70 65   28..Cont ent-Type
00f0  3a 20 74 65 78 74 2f 68  74 6d 6c 0d 0a 44 61 74   : text/h tml..Dat
0100  65 3a 20 57 65 64 2c 20  31 31 20 4a 75 6c 20 32   e: Wed,  11 Jul 2
```

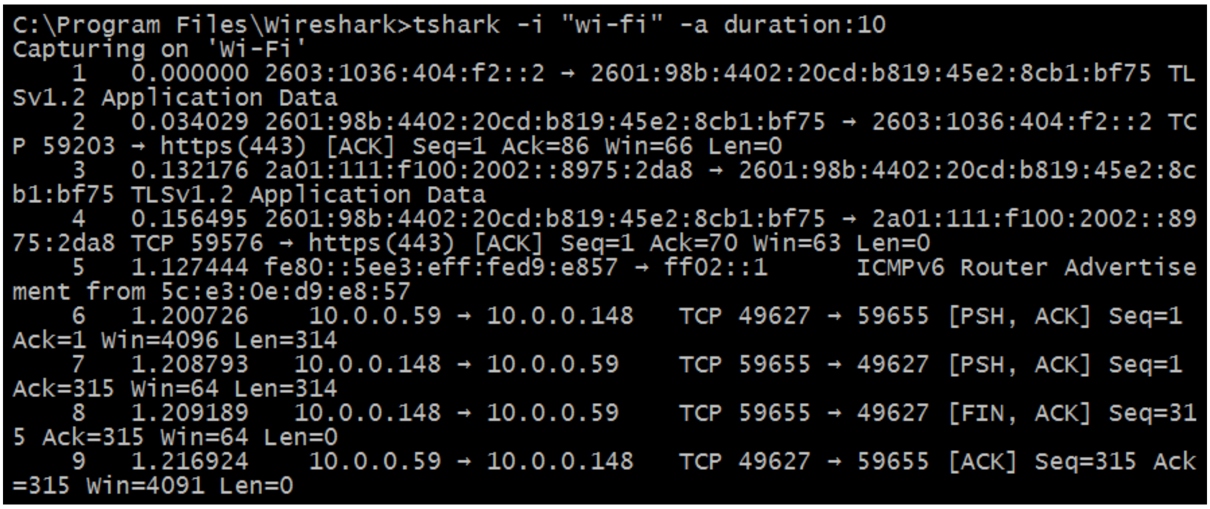


Wireshark · Preferences

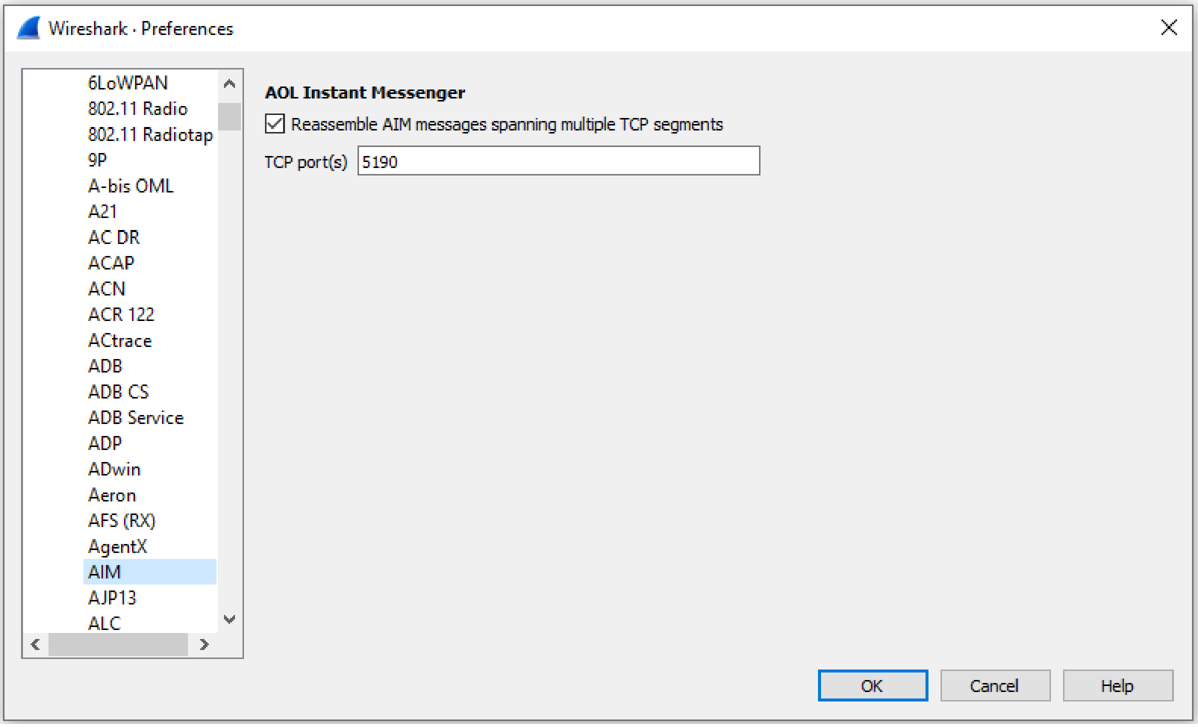
Pane 1:
● Packet List
○ Packet Details
○ Packet Bytes
○ None

Pane 2:
○ Packet List
● Packet Details
○ Packet Bytes
○ None

Pane 3:
○ Packet List
○ Packet Details
● Packet Bytes
○ None



```
C:\Program Files\Wireshark>tshark -i "wi-fi" -a duration:10
Capturing on 'Wi-Fi'
    1   0.000000 2603:1036:404:f2::2 → 2601:98b:4402:20cd:b819:45e2:8cb1:bf75 TL
Sv1.2 Application Data
    2   0.034029 2601:98b:4402:20cd:b819:45e2:8cb1:bf75 → 2603:1036:404:f2::2 TC
P 59203 → https(443) [ACK] Seq=1 Ack=86 Win=66 Len=0
    3   0.132176 2a01:111:f100:2002::8975:2da8 → 2601:98b:4402:20cd:b819:45e2:8c
b1:bf75 TLSv1.2 Application Data
    4   0.156495 2601:98b:4402:20cd:b819:45e2:8cb1:bf75 → 2a01:111:f100:2002::89
75:2da8 TCP 59576 → https(443) [ACK] Seq=1 Ack=70 Win=63 Len=0
    5   1.127444 fe80::5ee3:eff:fed9:e857 → ff02::1      ICMPv6 Router Advertise
ment from 5c:e3:0e:d9:e8:57
    6   1.200726    10.0.0.59 → 10.0.0.148   TCP 49627 → 59655 [PSH, ACK] Seq=1
Ack=1 Win=4096 Len=314
    7   1.208793   10.0.0.148 → 10.0.0.59    TCP 59655 → 49627 [PSH, ACK] Seq=1
Ack=315 Win=64 Len=314
    8   1.209189   10.0.0.148 → 10.0.0.59    TCP 59655 → 49627 [FIN, ACK] Seq=31
5 Ack=315 Win=64 Len=0
    9   1.216924    10.0.0.59 → 10.0.0.148   TCP 49627 → 59655 [ACK] Seq=315 Ack
=315 Win=4091 Len=0
```

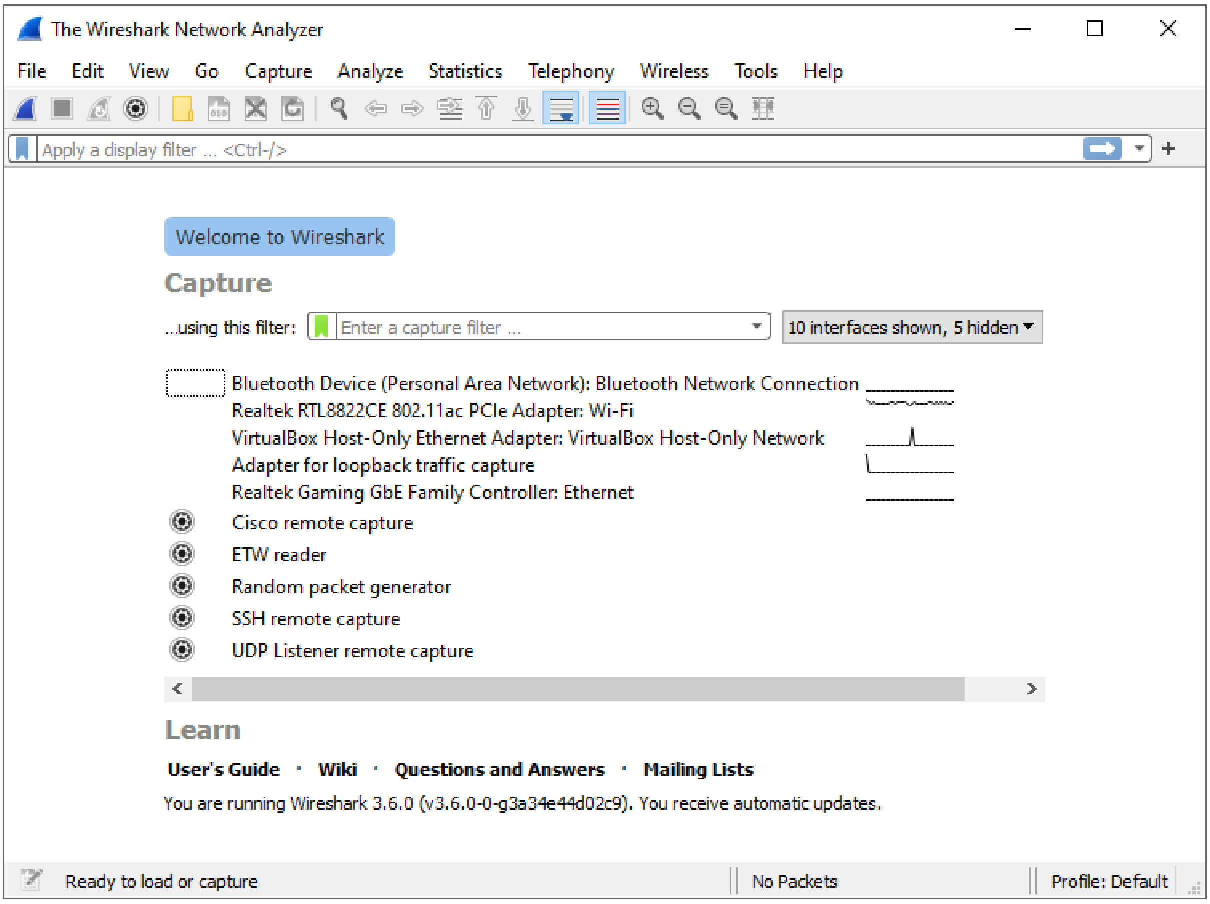


AOL Instant Messenger

☑ Reassemble AIM messages spanning multiple TCP segments

TCP port(s) 5190

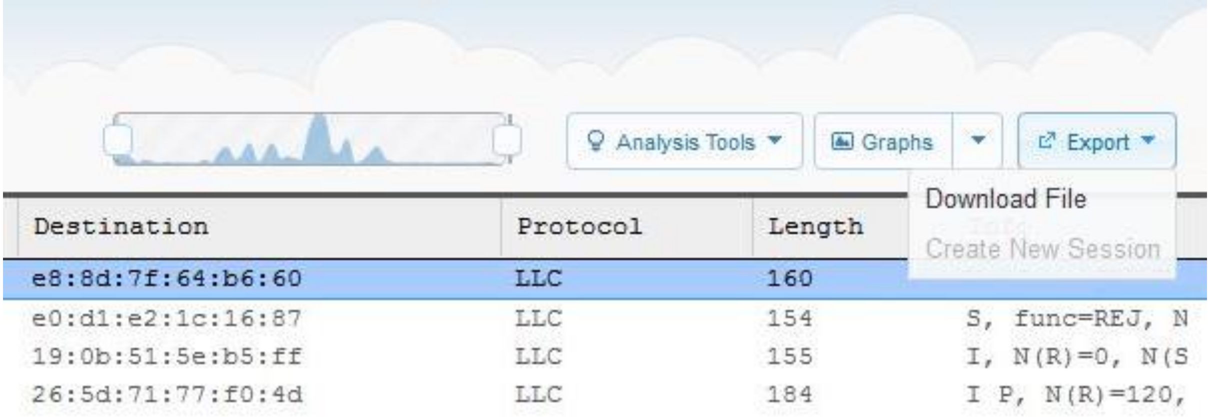
Chapter 3: Installing Wireshark


The Wireshark Network Analyzer
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Wireless
Tools
Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...
10 interfaces shown, 5 hidden
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists

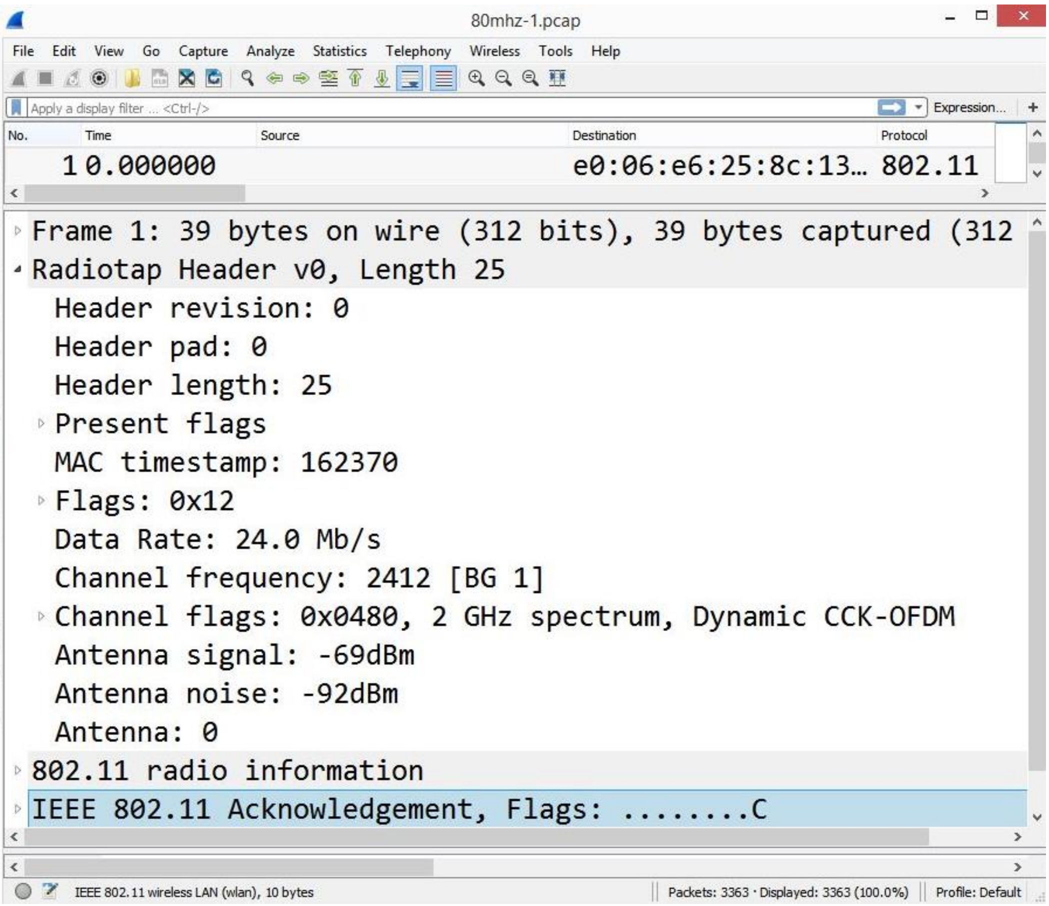
Bluetooth Device (Personal Area Network): Bluetooth Network Connection
Realtek RTL8822CE 802.11ac PCIe Adapter: Wi-Fi
VirtualBox Host-Only Ethernet Adapter: VirtualBox Host-Only Network
Adapter for loopback traffic capture
Realtek Gaming GbE Family Controller: Ethernet
Cisco remote capture
ETW reader
Random packet generator
SSH remote capture
UDP Listener remote capture

You are running Wireshark 3.6.0 (v3.6.0-0-g3a34e44d02c9). You receive automatic updates.

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



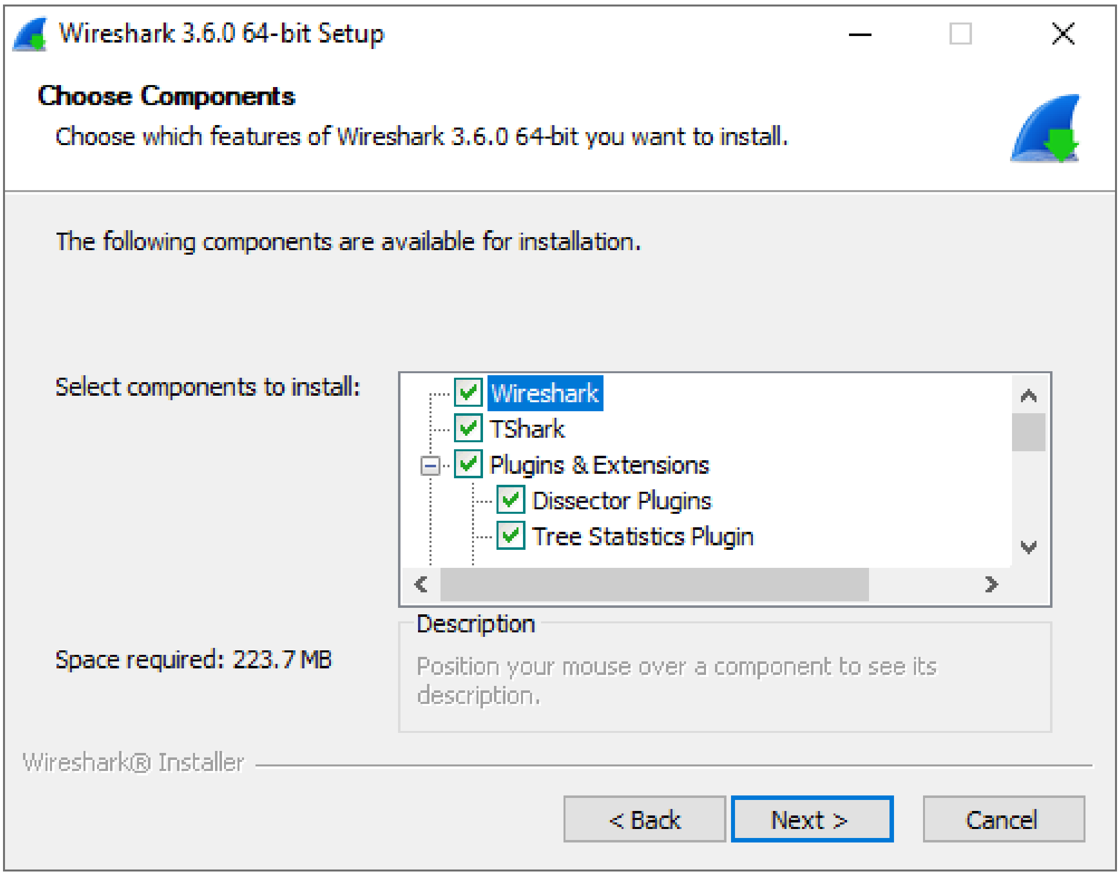
Destination	Protocol	Length	
e8:8d:7f:64:b6:60	LLC	160	
e0:d1:e2:1c:16:87	LLC	154	S, func=REJ, N
19:0b:51:5e:b5:ff	LLC	155	I, N(R)=0, N(S
26:5d:71:77:f0:4d	LLC	184	I P, N(R)=120,



```
No.   Time        Source    Destination            Protocol
   1 0.000000               e0:06:e6:25:8c:13…     802.11
```

```
▹ Frame 1: 39 bytes on wire (312 bits), 39 bytes captured (312
◂ Radiotap Header v0, Length 25
    Header revision: 0
    Header pad: 0
    Header length: 25
  ▹ Present flags
    MAC timestamp: 162370
  ▹ Flags: 0x12
    Data Rate: 24.0 Mb/s
    Channel frequency: 2412 [BG 1]
  ▹ Channel flags: 0x0480, 2 GHz spectrum, Dynamic CCK-OFDM
    Antenna signal: -69dBm
    Antenna noise: -92dBm
    Antenna: 0
▹ 802.11 radio information
▹ IEEE 802.11 Acknowledgement, Flags: ........C
```

```
IEEE 802.11 wireless LAN (wlan), 10 bytes    Packets: 3363 · Displayed: 3363 (100.0%)    Profile: Default
```


Wireshark 3.6.0 64-bit Setup

Choose Components

Choose which features of Wireshark 3.6.0 64-bit you want to install.

The following components are available for installation.

Select components to install:

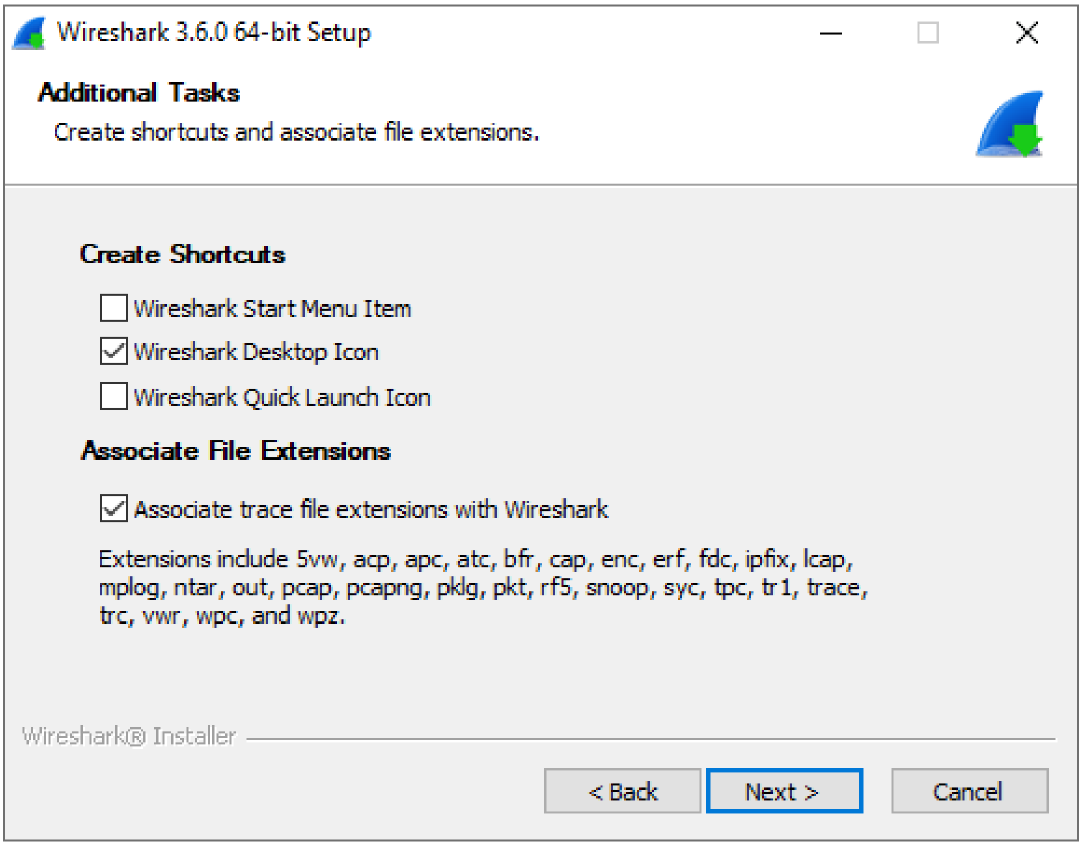
- ☑ Wireshark
- ☑ TShark
- ⊟ ☑ Plugins & Extensions
  - ☑ Dissector Plugins
  - ☑ Tree Statistics Plugin

Space required: 223.7 MB

Description

Position your mouse over a component to see its description.

Wireshark® Installer



Wireshark 3.6.0 64-bit Setup

Additional Tasks

Create shortcuts and associate file extensions.

Create Shortcuts

☐ Wireshark Start Menu Item

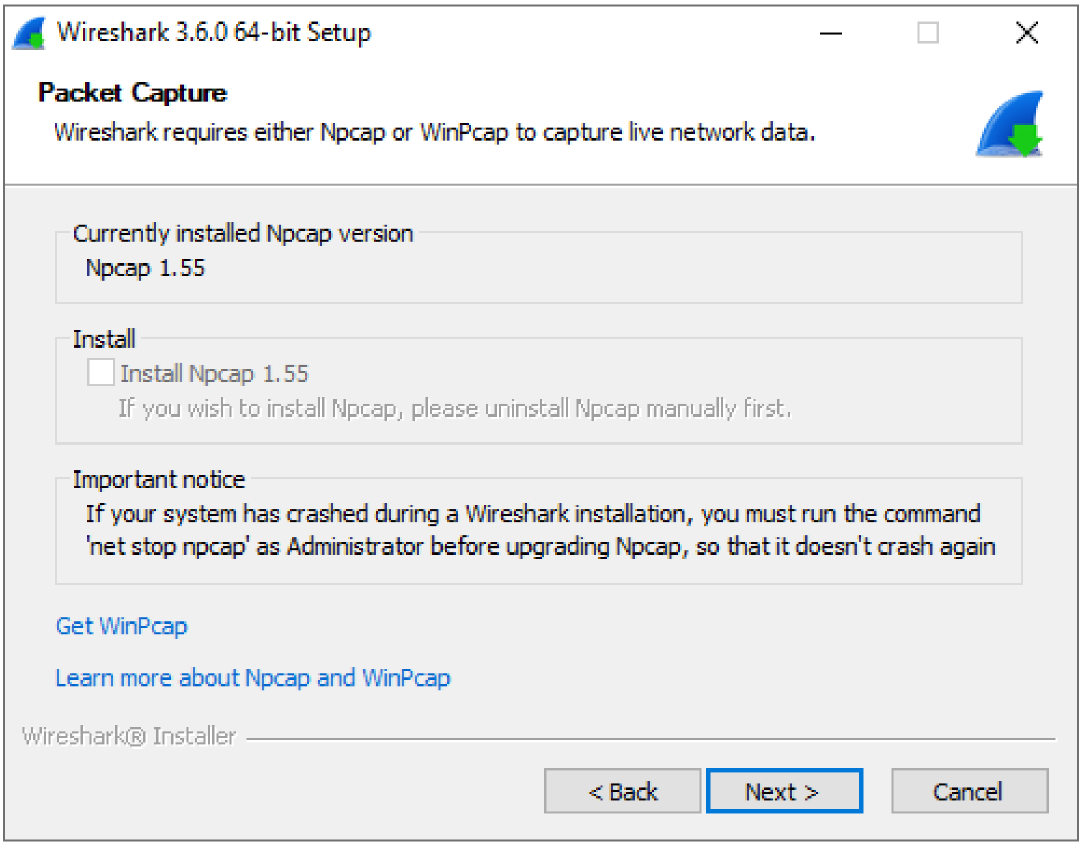
☑ Wireshark Desktop Icon

☐ Wireshark Quick Launch Icon

Associate File Extensions

☑ Associate trace file extensions with Wireshark

Extensions include 5vw, acp, apc, atc, bfr, cap, enc, erf, fdc, ipfix, lcap, mplog, ntar, out, pcap, pcapng, pklg, pkt, rf5, snoop, syc, tpc, tr1, trace, trc, vwr, wpc, and wpz.



Wireshark 3.6.0 64-bit Setup

Packet Capture

Wireshark requires either Npcap or WinPcap to capture live network data.

Currently installed Npcap version

Npcap 1.55

Install

☐ Install Npcap 1.55

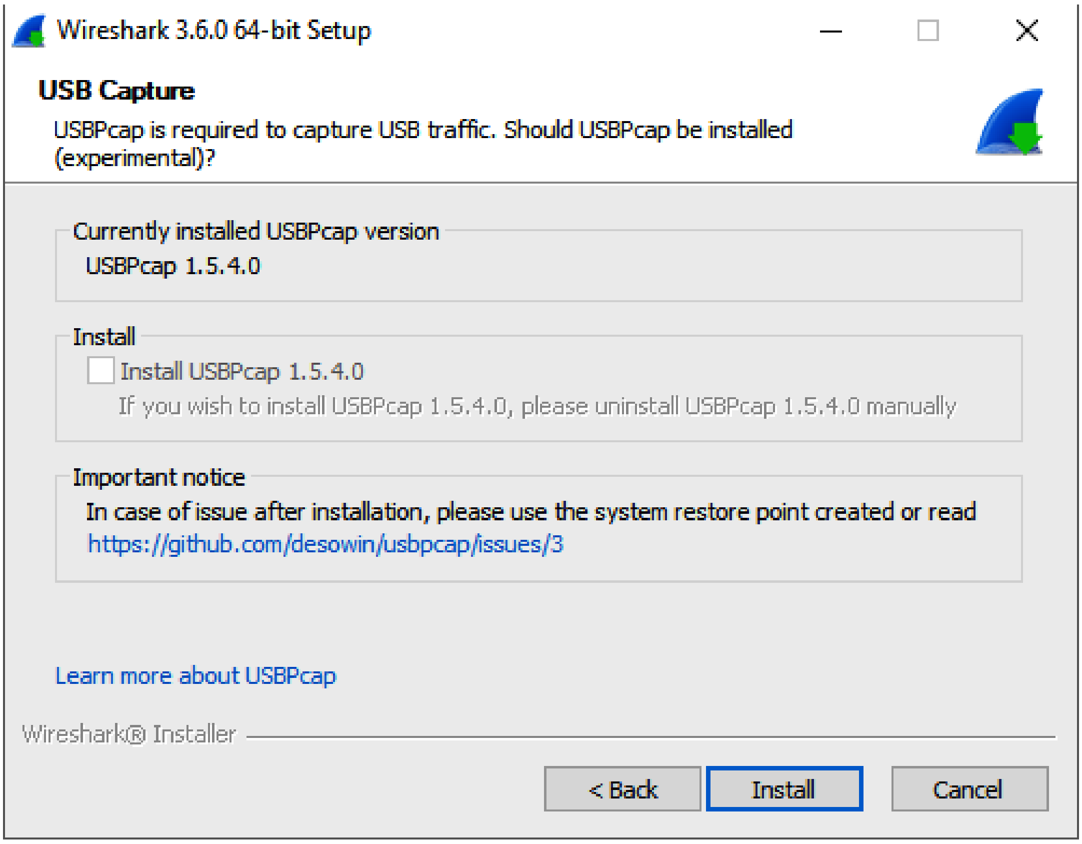
If you wish to install Npcap, please uninstall Npcap manually first.

Important notice

If your system has crashed during a Wireshark installation, you must run the command 'net stop npcap' as Administrator before upgrading Npcap, so that it doesn't crash again

Get WinPcap

Learn more about Npcap and WinPcap


Wireshark 3.6.0 64-bit Setup

USB Capture

USBPcap is required to capture USB traffic. Should USBPcap be installed (experimental)?

Currently installed USBPcap version

USBPcap 1.5.4.0

Install

□ Install USBPcap 1.5.4.0

If you wish to install USBPcap 1.5.4.0, please uninstall USBPcap 1.5.4.0 manually

Important notice

In case of issue after installation, please use the system restore point created or read https://github.com/desowin/usbpcap/issues/3

Learn more about USBPcap

Wireshark 3.6.0 Released

November 22, 2021

Wireshark 3.6.0 has been released. Installers for Windows, macOS 10.13 and later, and source code are now available.

What’s New

Many improvements have been made. See the “New and Updated Features” section below for more details. You might want to pay particular attention to the display filter syntax updates.

New and Updated Features

The following features are new (or have been significantly updated) since version 3.6.0rc3:

- The macOS Intel packages now ship with Qt 5.15.3 and require macOS 10.13 or later.

The following features are new (or have been significantly updated) since version 3.6.0rc2:

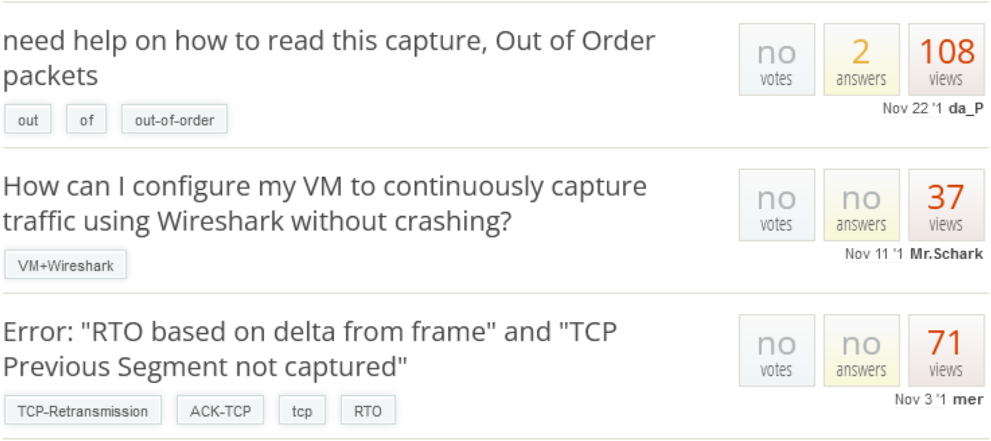
- Display filter set elements must now be comma-separated. See below for more details.

The following features are new (or have been significantly updated) since version 3.6.0rc1:

- The display filter expression “a != b” now has the same meaning as “!(a == b)”.

The following features are new (or have been significantly updated) since version 3.5.0:

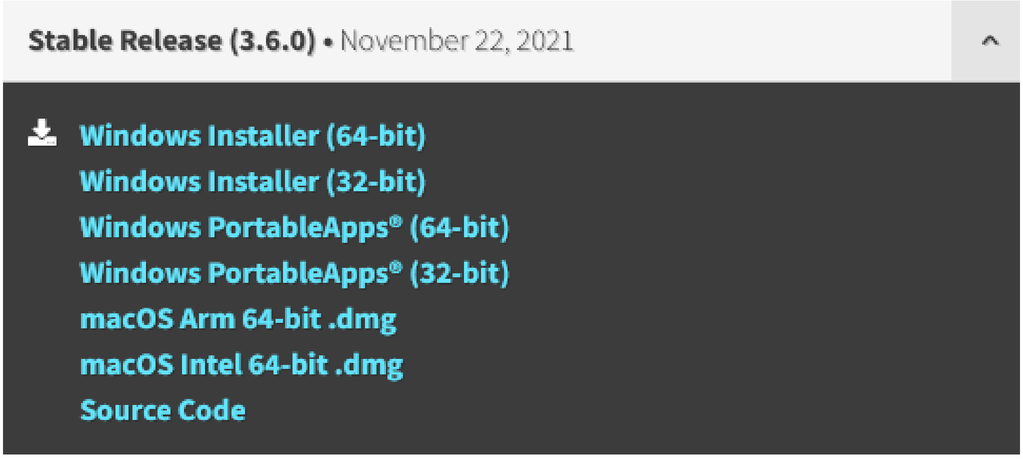
- Nothing of note.



need help on how to read this capture, Out of Order packets

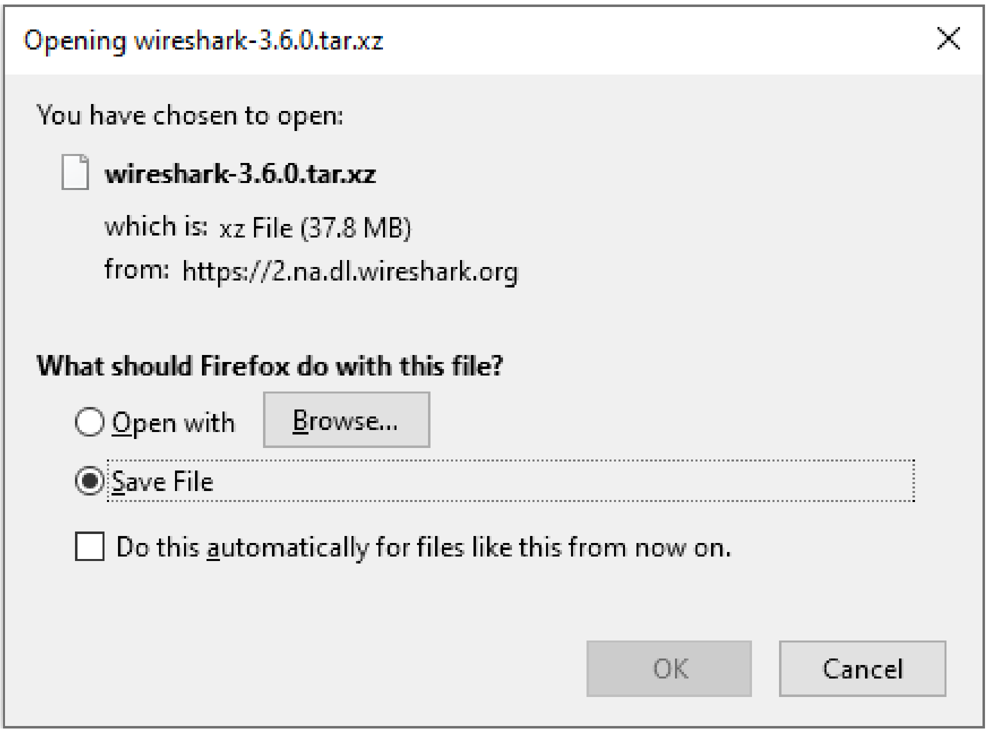
How can I configure my VM to continuously capture traffic using Wireshark without crashing?

Error: "RTO based on delta from frame" and "TCP Previous Segment not captured"



Stable Release (3.6.0) • November 22, 2021

- Windows Installer (64-bit)
- Windows Installer (32-bit)
- Windows PortableApps® (64-bit)
- Windows PortableApps® (32-bit)
- macOS Arm 64-bit .dmg
- macOS Intel 64-bit .dmg
- Source Code



Opening wireshark-3.6.0.tar.xz

You have chosen to open:

wireshark-3.6.0.tar.xz

which is: xz File (37.8 MB)

from: https://2.na.dl.wireshark.org

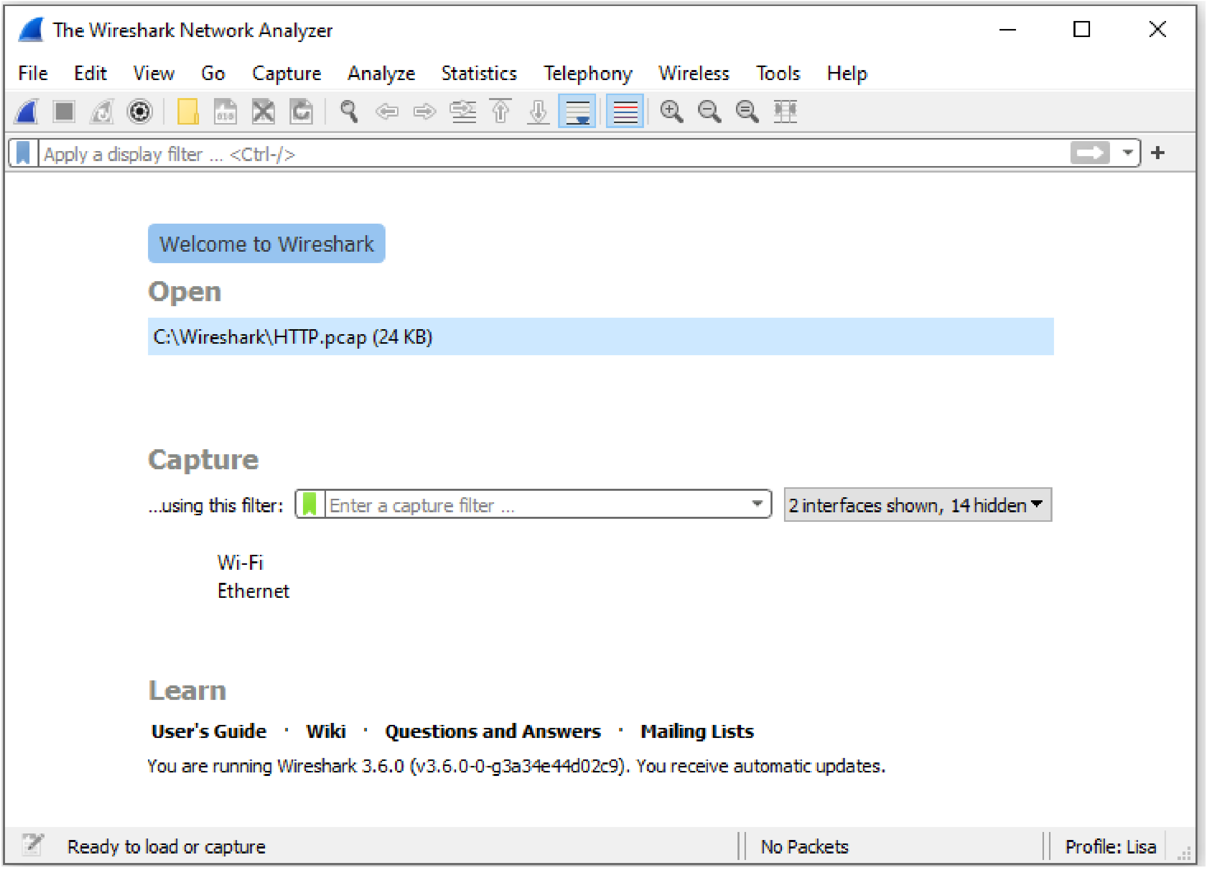
What should Firefox do with this file?

○ Open with Browse...

● Save File

□ Do this automatically for files like this from now on.

Chapter 4: Exploring the Wireshark Interface


The Wireshark Network Analyzer
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Wireless
Tools
Help
Apply a display filter … <Ctrl-/>
Welcome to Wireshark
Open
Capture
…using this filter:
Enter a capture filter …
2 interfaces shown, 14 hidden
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists

C:\Wireshark\HTTP.pcap (24 KB)

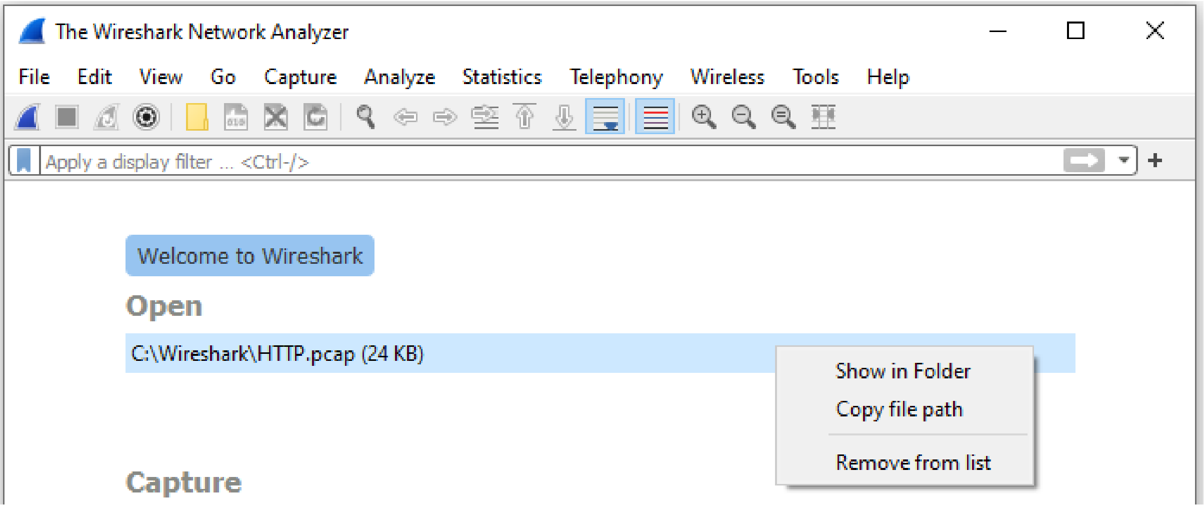
Wi-Fi
Ethernet

You are running Wireshark 3.6.0 (v3.6.0-0-g3a34e44d02c9). You receive automatic updates.

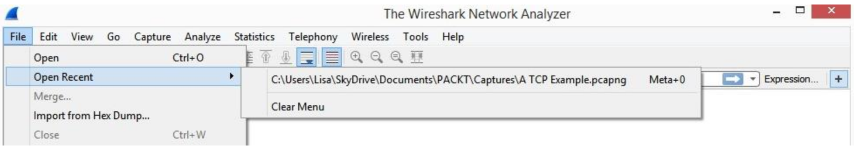
Ready to load or capture

No Packets

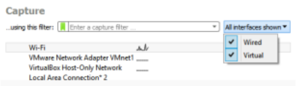
Profile: Lisa



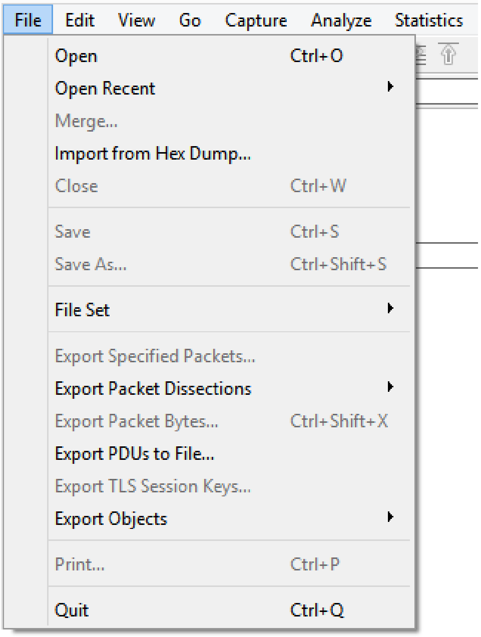
C:\Wireshark\HTTP.pcap (24 KB)

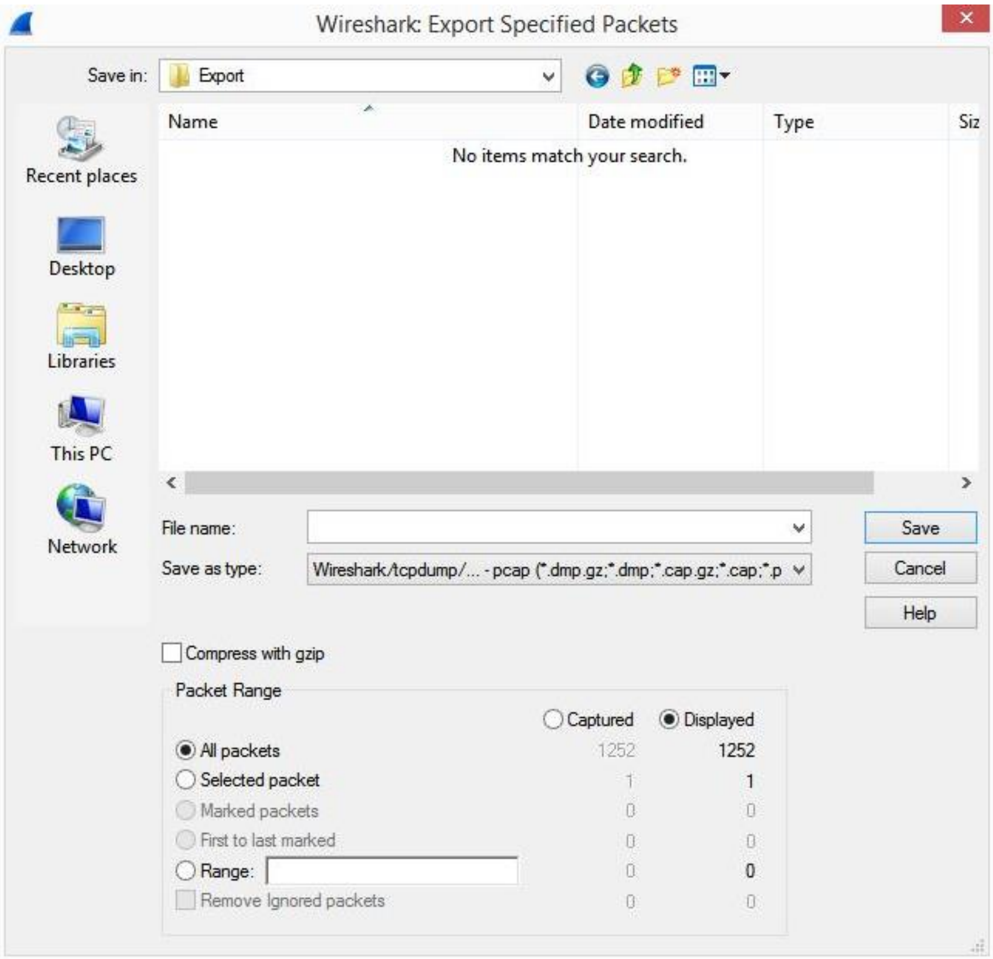


C:\Users\Lisa\SkyDrive\Documents\PACKT\Captures\A TCP Example.pcapng Meta+0



Wi-Fi
VMware Network Adapter VMnet1
VirtualBox Host-Only Network
Local Area Connection* 2





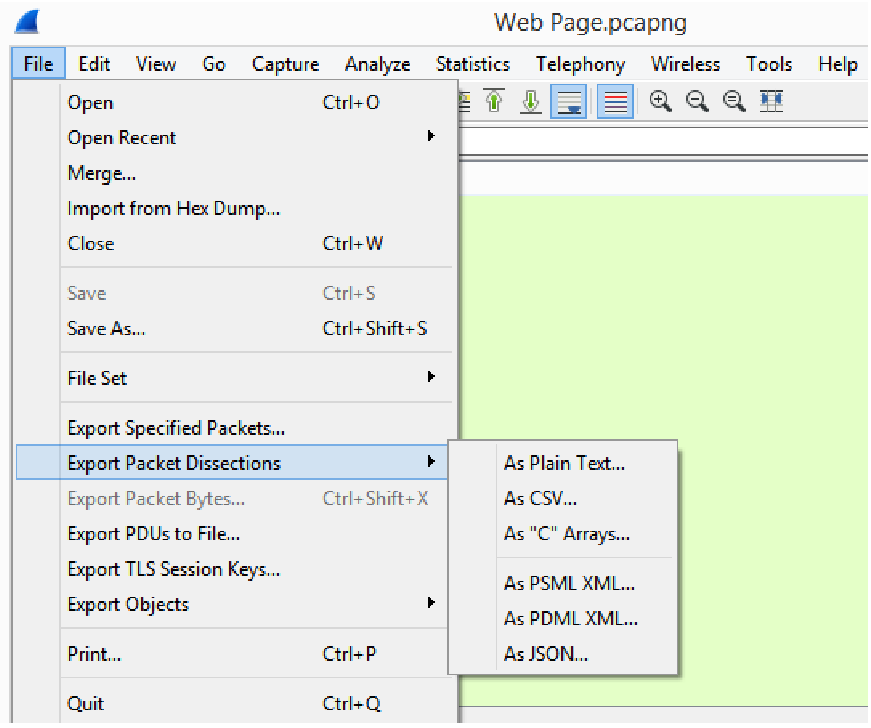
Save in: Export

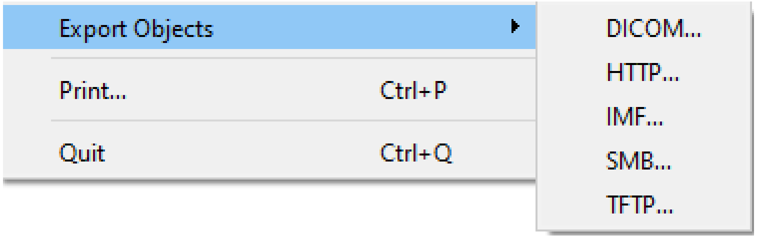
File name:

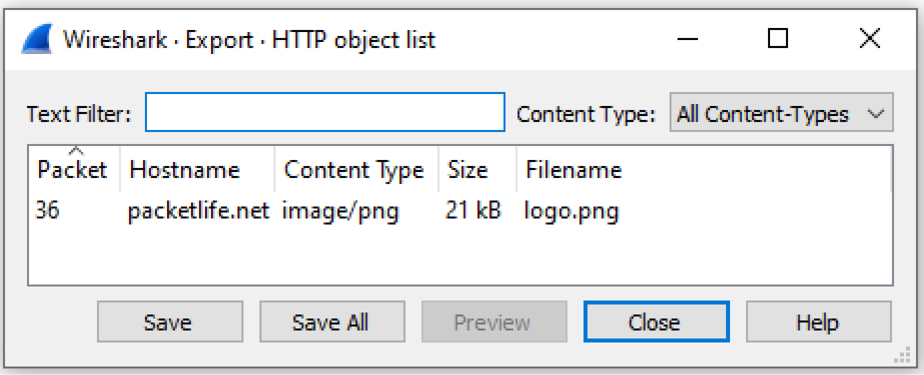
Save as type: Wireshark/tcpdump/... - pcap (*.dmp.gz;*.dmp;*.cap.gz;*.cap;*.p

□ Compress with gzip

	○ Captured	● Displayed
● All packets	1252	1252
○ Selected packet	1	1
○ Marked packets	0	0
○ First to last marked	0	0
○ Range:	0	0
□ Remove Ignored packets	0	0

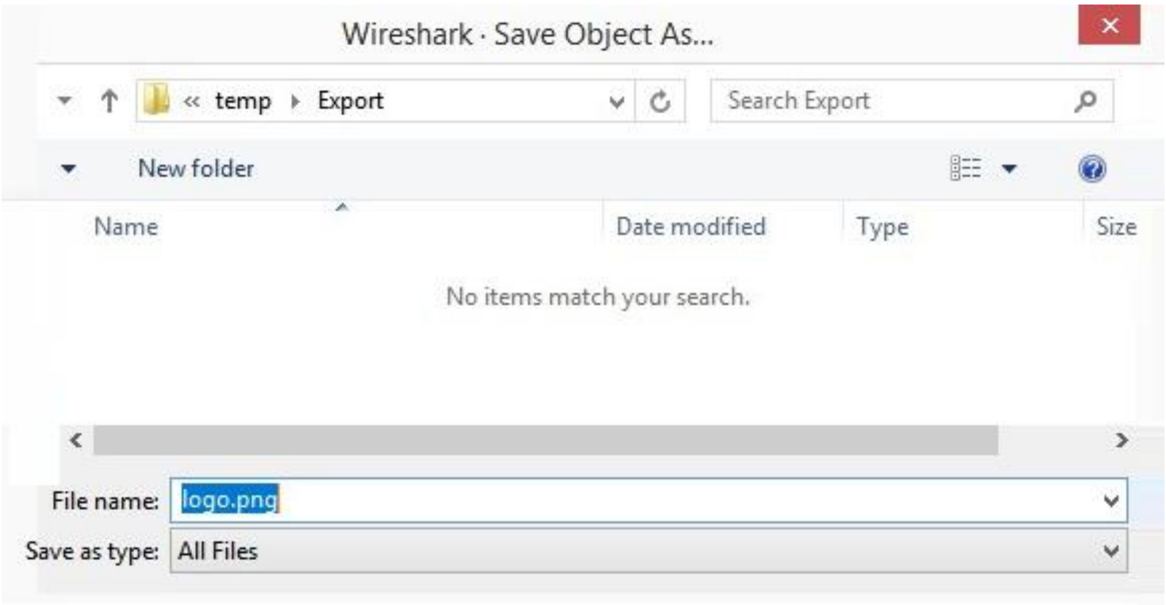





Wireshark · Export · HTTP object list

Text Filter: Content Type: All Content-Types

Packet	Hostname	Content Type	Size	Filename
36	packetlife.net	image/png	21 kB	logo.png



Wireshark · Save Object As...

« temp › Export

Search Export

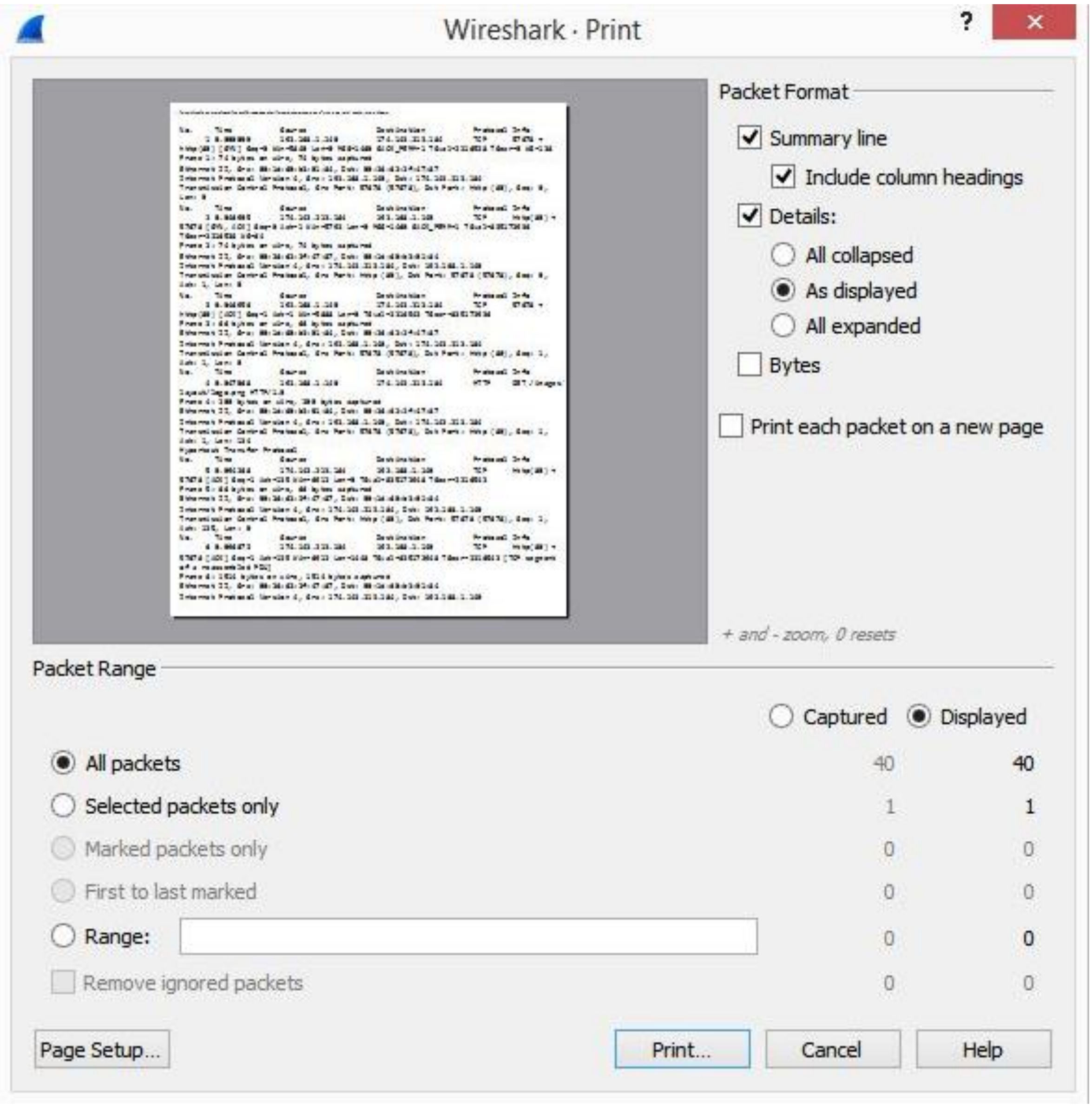
New folder

Name	Date modified	Type	Size

No items match your search.

File name: logo.png

Save as type: All Files



Wireshark · Print

Packet Format

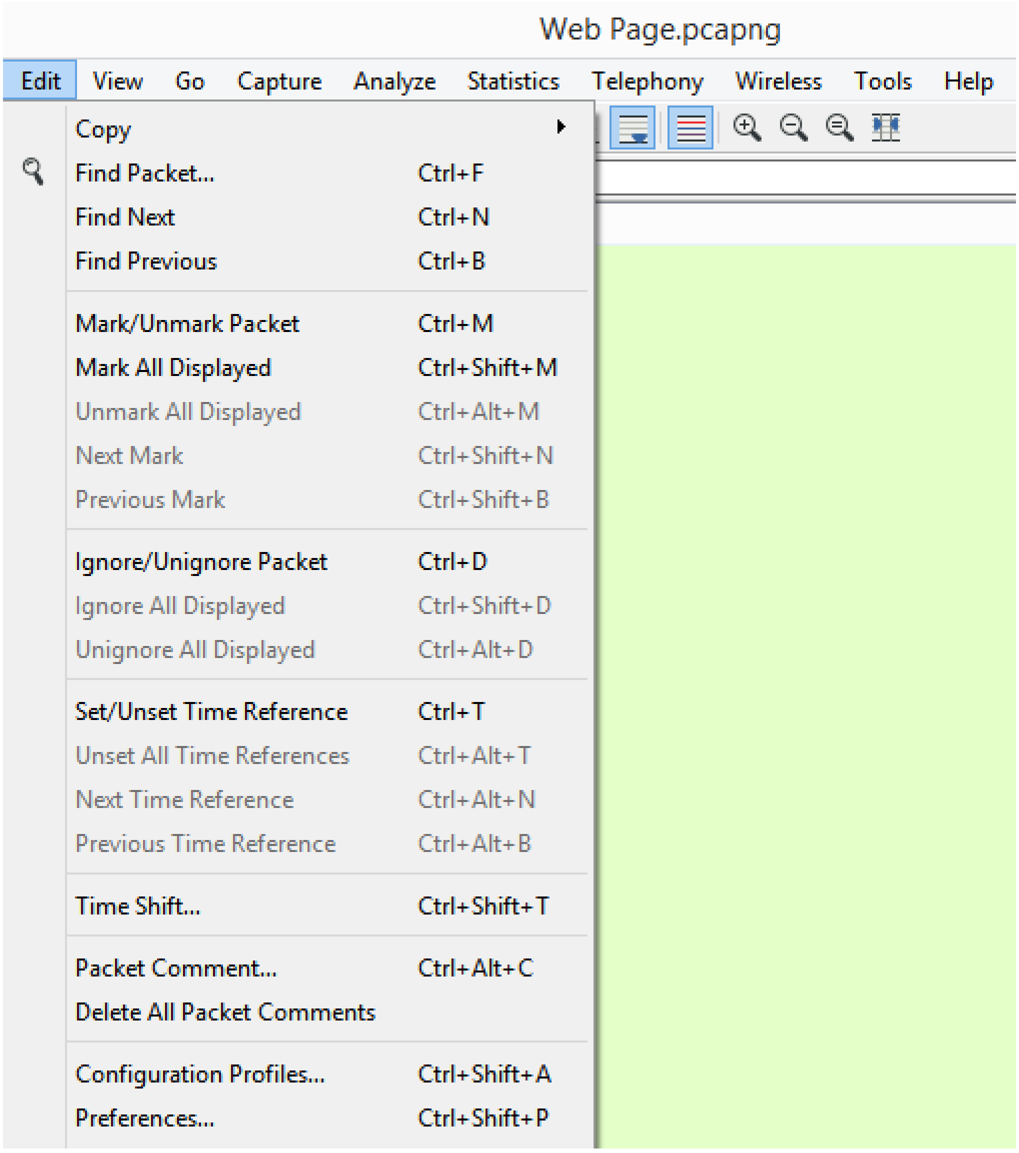
- ☑ Summary line
  - ☑ Include column headings
- ☑ Details:
  - ○ All collapsed
  - ● As displayed
  - ○ All expanded
- □ Bytes

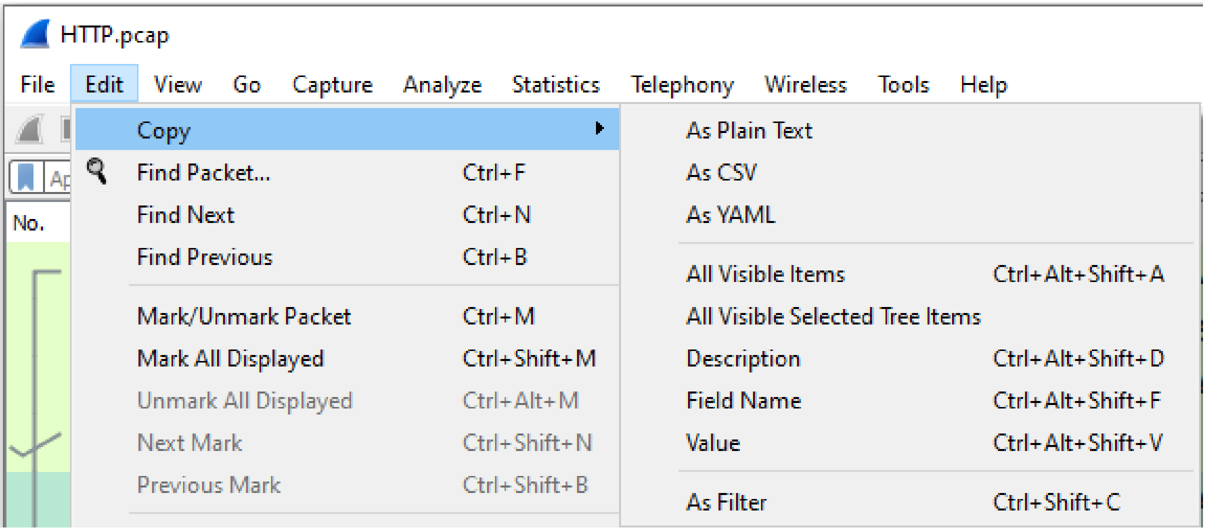
□ Print each packet on a new page

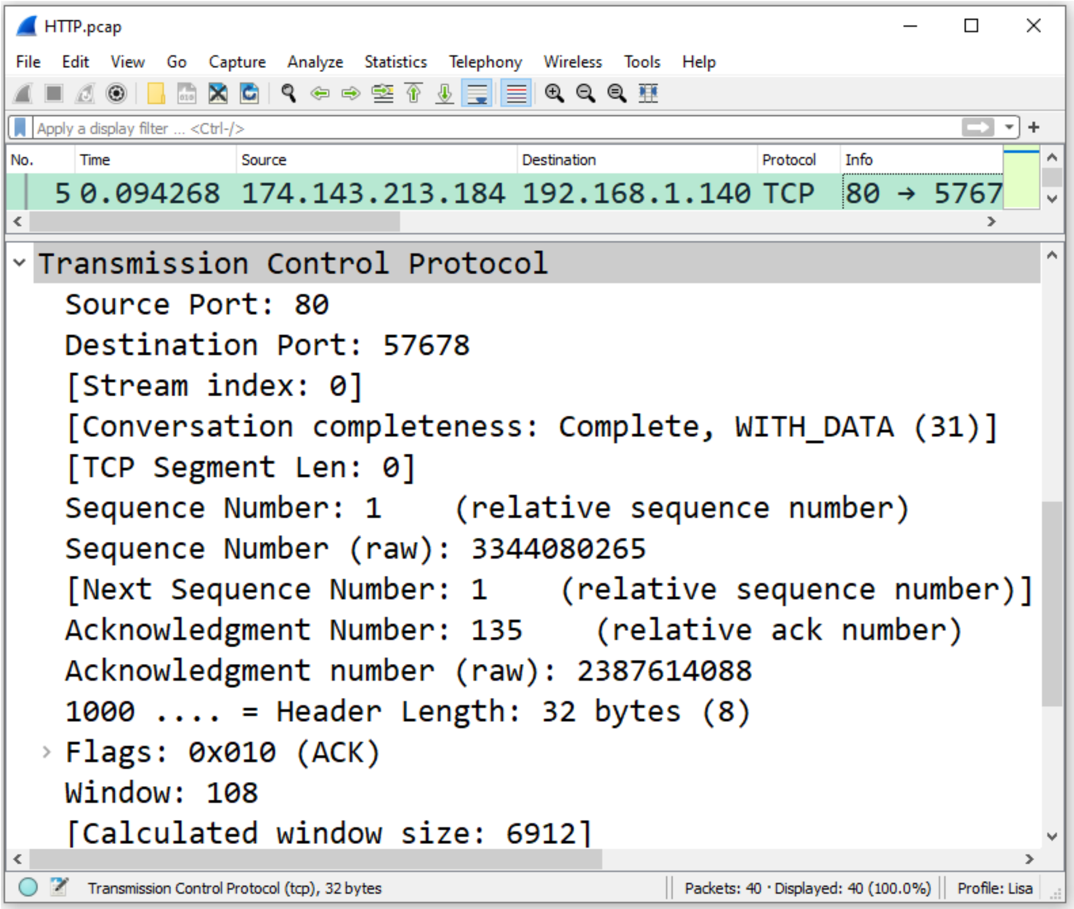
+ and - zoom, 0 resets

Packet Range

	○ Captured	● Displayed
● All packets	40	40
○ Selected packets only	1	1
○ Marked packets only	0	0
○ First to last marked	0	0
○ Range:	0	0
□ Remove ignored packets	0	0


Web Page.pcapng
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Wireless
Tools
Help
Copy
Find Packet... Ctrl+F
Find Next Ctrl+N
Find Previous Ctrl+B
Mark/Unmark Packet Ctrl+M
Mark All Displayed Ctrl+Shift+M
Unmark All Displayed Ctrl+Alt+M
Next Mark Ctrl+Shift+N
Previous Mark Ctrl+Shift+B
Ignore/Unignore Packet Ctrl+D
Ignore All Displayed Ctrl+Shift+D
Unignore All Displayed Ctrl+Alt+D
Set/Unset Time Reference Ctrl+T
Unset All Time References Ctrl+Alt+T
Next Time Reference Ctrl+Alt+N
Previous Time Reference Ctrl+Alt+B
Time Shift... Ctrl+Shift+T
Packet Comment... Ctrl+Alt+C
Delete All Packet Comments
Configuration Profiles... Ctrl+Shift+A
Preferences... Ctrl+Shift+P

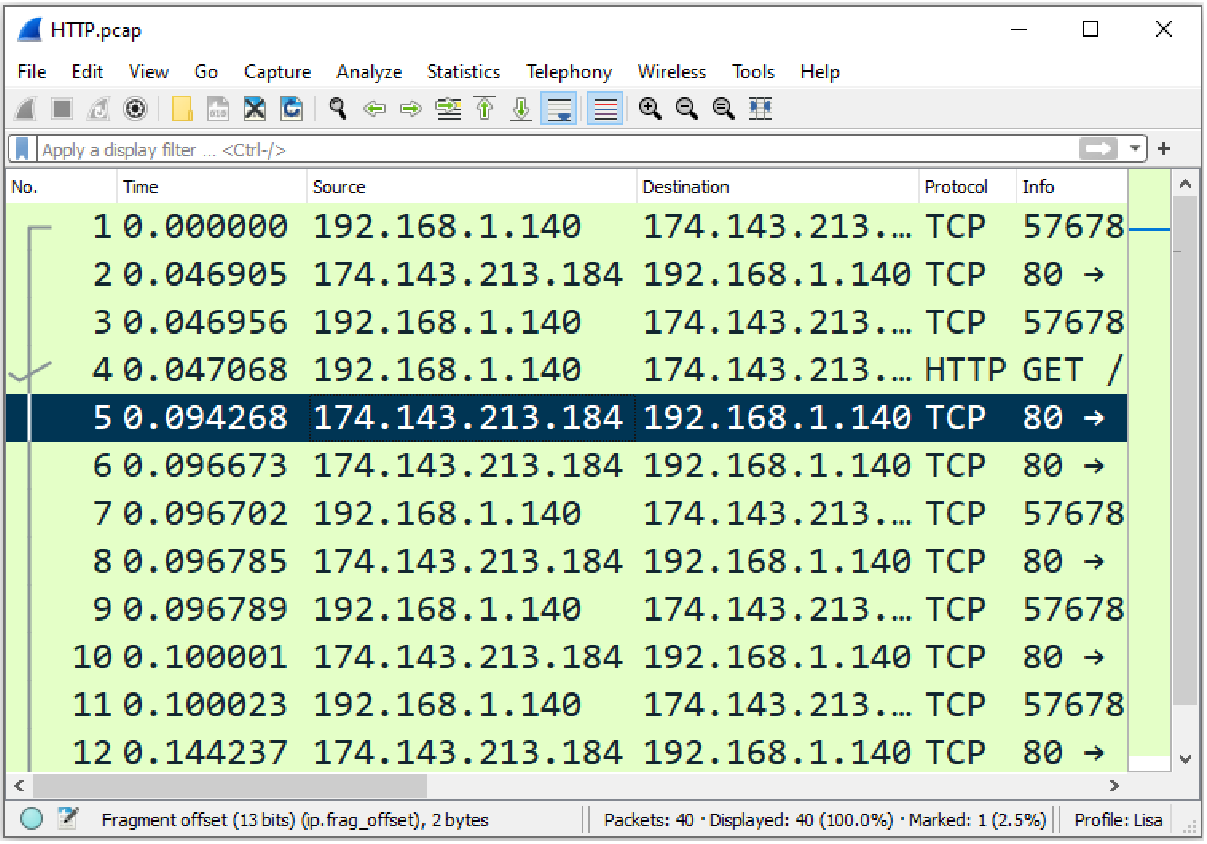

HTTP.pcap
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Wireless
Tools
Help
No.
Copy
Find Packet... Ctrl+F
Find Next Ctrl+N
Find Previous Ctrl+B
Mark/Unmark Packet Ctrl+M
Mark All Displayed Ctrl+Shift+M
Unmark All Displayed Ctrl+Alt+M
Next Mark Ctrl+Shift+N
Previous Mark Ctrl+Shift+B
As Plain Text
As CSV
As YAML
All Visible Items Ctrl+Alt+Shift+A
All Visible Selected Tree Items
Description Ctrl+Alt+Shift+D
Field Name Ctrl+Alt+Shift+F
Value Ctrl+Alt+Shift+V
As Filter Ctrl+Shift+C


HTTP.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  Time      Source           Destination    Protocol Info
   5 0.094268 174.143.213.184 192.168.1.140 TCP      80 → 5767
```

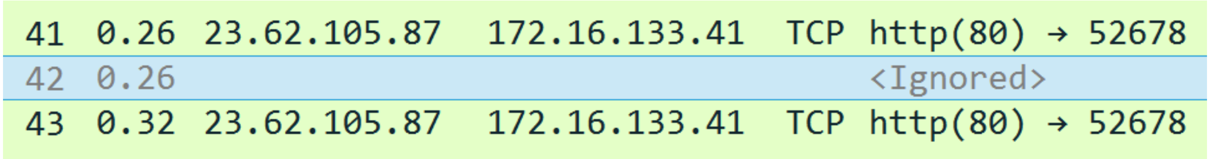
```
⌄ Transmission Control Protocol
    Source Port: 80
    Destination Port: 57678
    [Stream index: 0]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 0]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 3344080265
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 135    (relative ack number)
    Acknowledgment number (raw): 2387614088
    1000 .... = Header Length: 32 bytes (8)
  › Flags: 0x010 (ACK)
    Window: 108
    [Calculated window size: 6912]
```

```
Transmission Control Protocol (tcp), 32 bytes    Packets: 40 · Displayed: 40 (100.0%)    Profile: Lisa
```

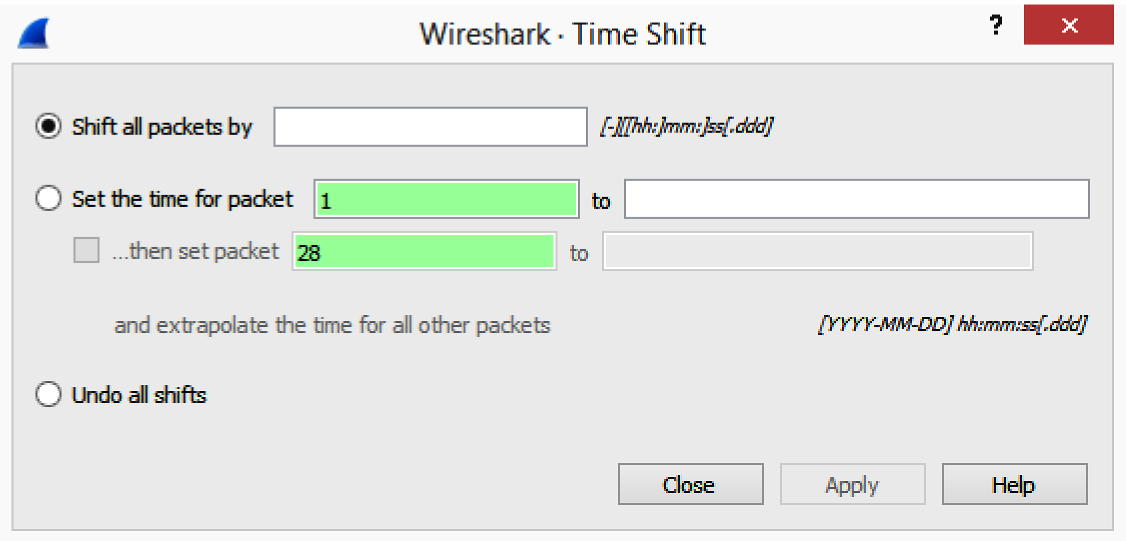

HTTP.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No. Time      Source           Destination       Protocol Info
  1 0.000000 192.168.1.140    174.143.213.... TCP      57678
  2 0.046905 174.143.213.184 192.168.1.140    TCP      80 →
  3 0.046956 192.168.1.140    174.143.213.... TCP      57678
  4 0.047068 192.168.1.140    174.143.213.... HTTP     GET /
  5 0.094268 174.143.213.184 192.168.1.140    TCP      80 →
  6 0.096673 174.143.213.184 192.168.1.140    TCP      80 →
  7 0.096702 192.168.1.140    174.143.213.... TCP      57678
  8 0.096785 174.143.213.184 192.168.1.140    TCP      80 →
  9 0.096789 192.168.1.140    174.143.213.... TCP      57678
 10 0.100001 174.143.213.184 192.168.1.140    TCP      80 →
 11 0.100023 192.168.1.140    174.143.213.... TCP      57678
 12 0.144237 174.143.213.184 192.168.1.140    TCP      80 →
```

```
Fragment offset (13 bits) (ip.frag_offset), 2 bytes    Packets: 40 · Displayed: 40 (100.0%) · Marked: 1 (2.5%)    Profile: Lisa
```



```
41  0.26  23.62.105.87   172.16.133.41  TCP  http(80) → 52678
42  0.26                                     <Ignored>
43  0.32  23.62.105.87   172.16.133.41  TCP  http(80) → 52678
```



Wireshark · Time Shift

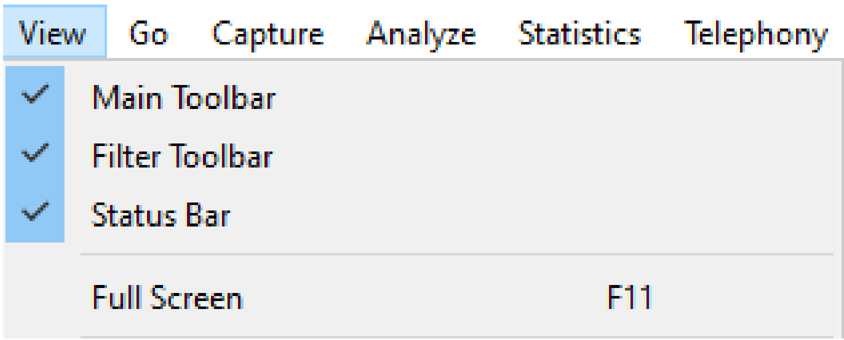
● Shift all packets by [-][[hh:]mm:]ss[.ddd]

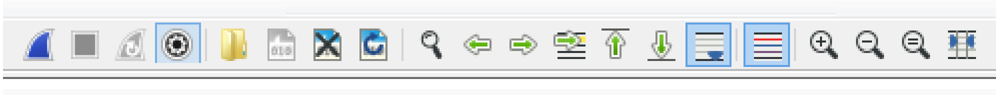
○ Set the time for packet 1 to

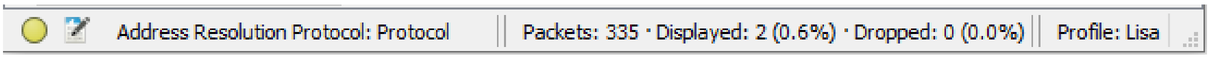
□ ...then set packet 28 to

and extrapolate the time for all other packets [YYYY-MM-DD] hh:mm:ss[.ddd]

○ Undo all shifts

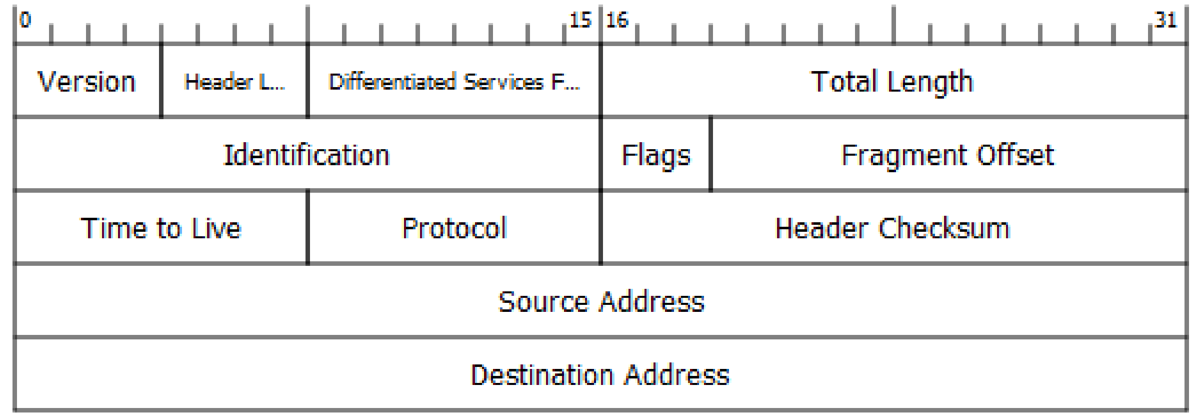




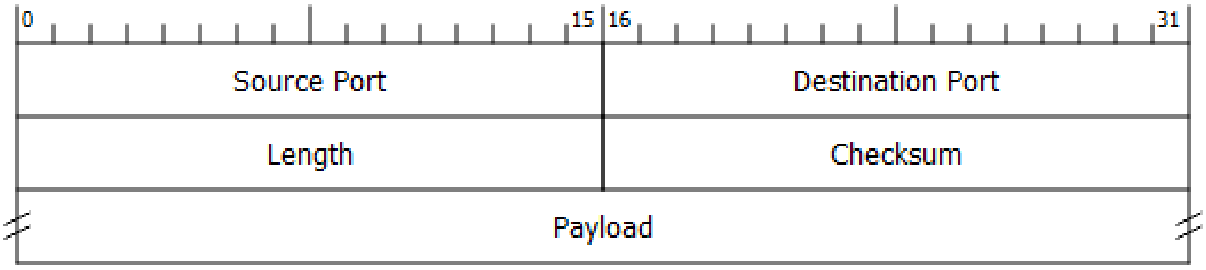


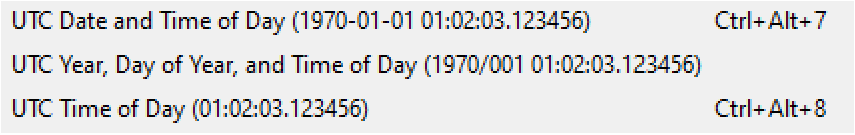
Address Resolution Protocol: Protocol || Packets: 335 · Displayed: 2 (0.6%) · Dropped: 0 (0.0%) || Profile: Lisa

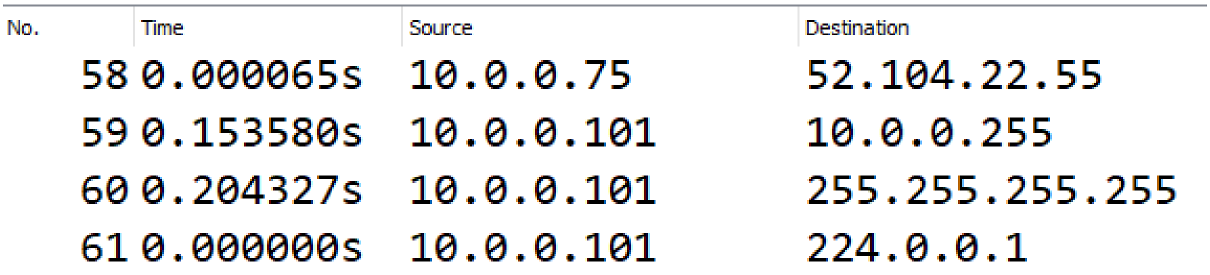
Internet Protocol Version 4



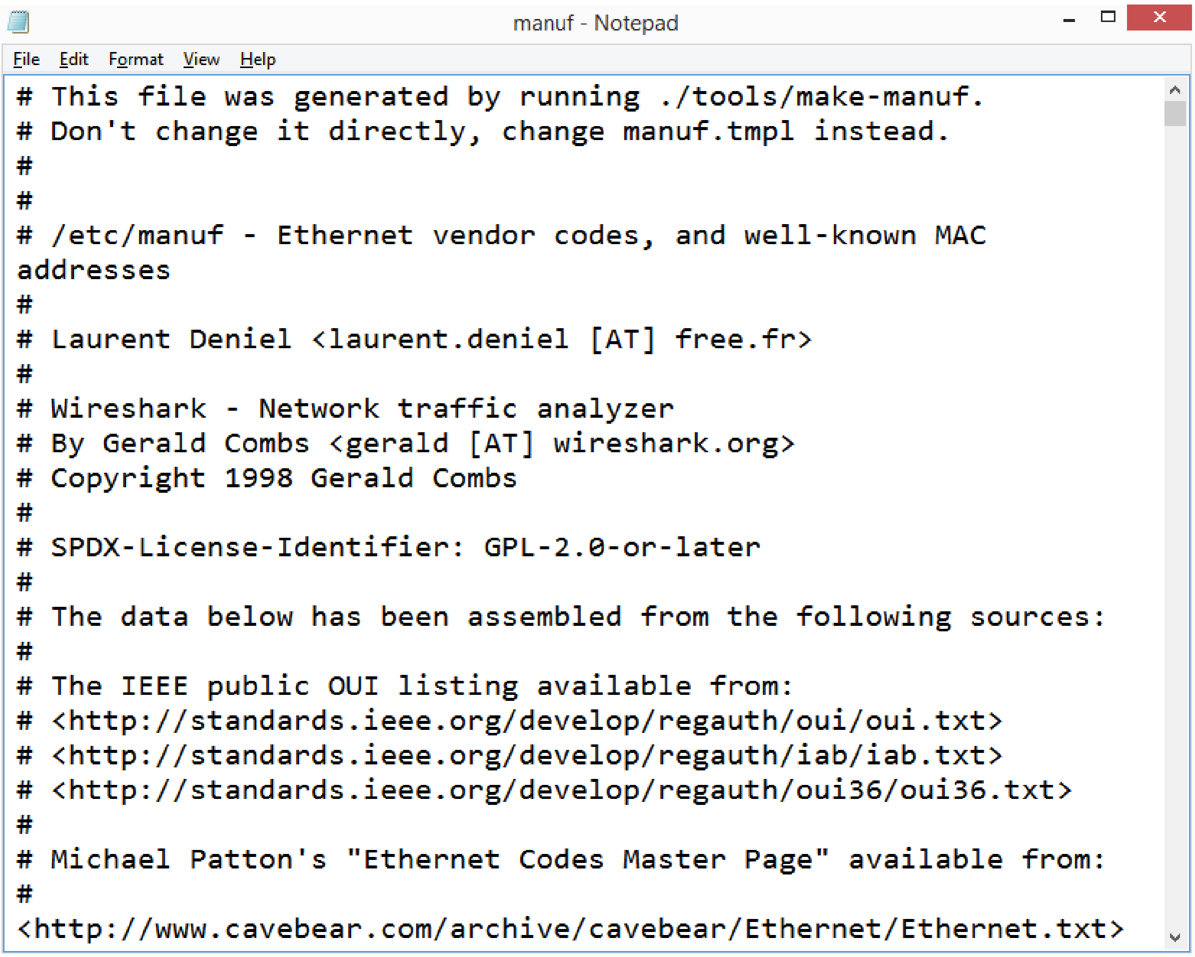
User Datagram Protocol



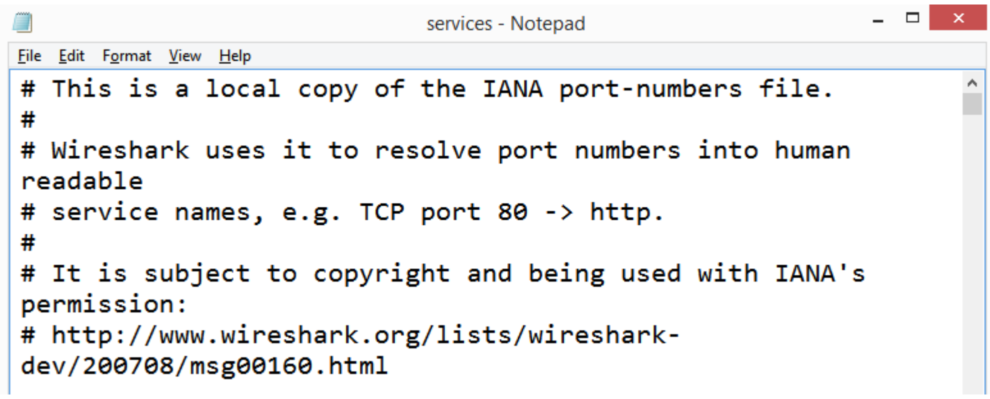

UTC Date and Time of Day (1970-01-01 01:02:03.123456) Ctrl+Alt+7
UTC Year, Day of Year, and Time of Day (1970/001 01:02:03.123456)
UTC Time of Day (01:02:03.123456) Ctrl+Alt+8



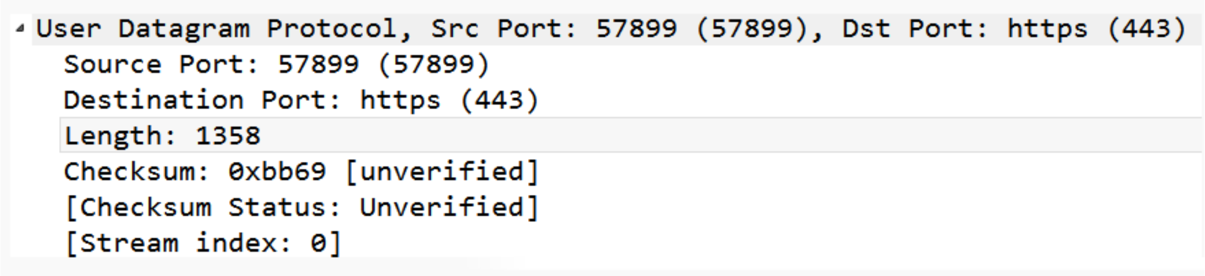
No.	Time	Source	Destination
58	0.000065s	10.0.0.75	52.104.22.55
59	0.153580s	10.0.0.101	10.0.0.255
60	0.204327s	10.0.0.101	255.255.255.255
61	0.000000s	10.0.0.101	224.0.0.1



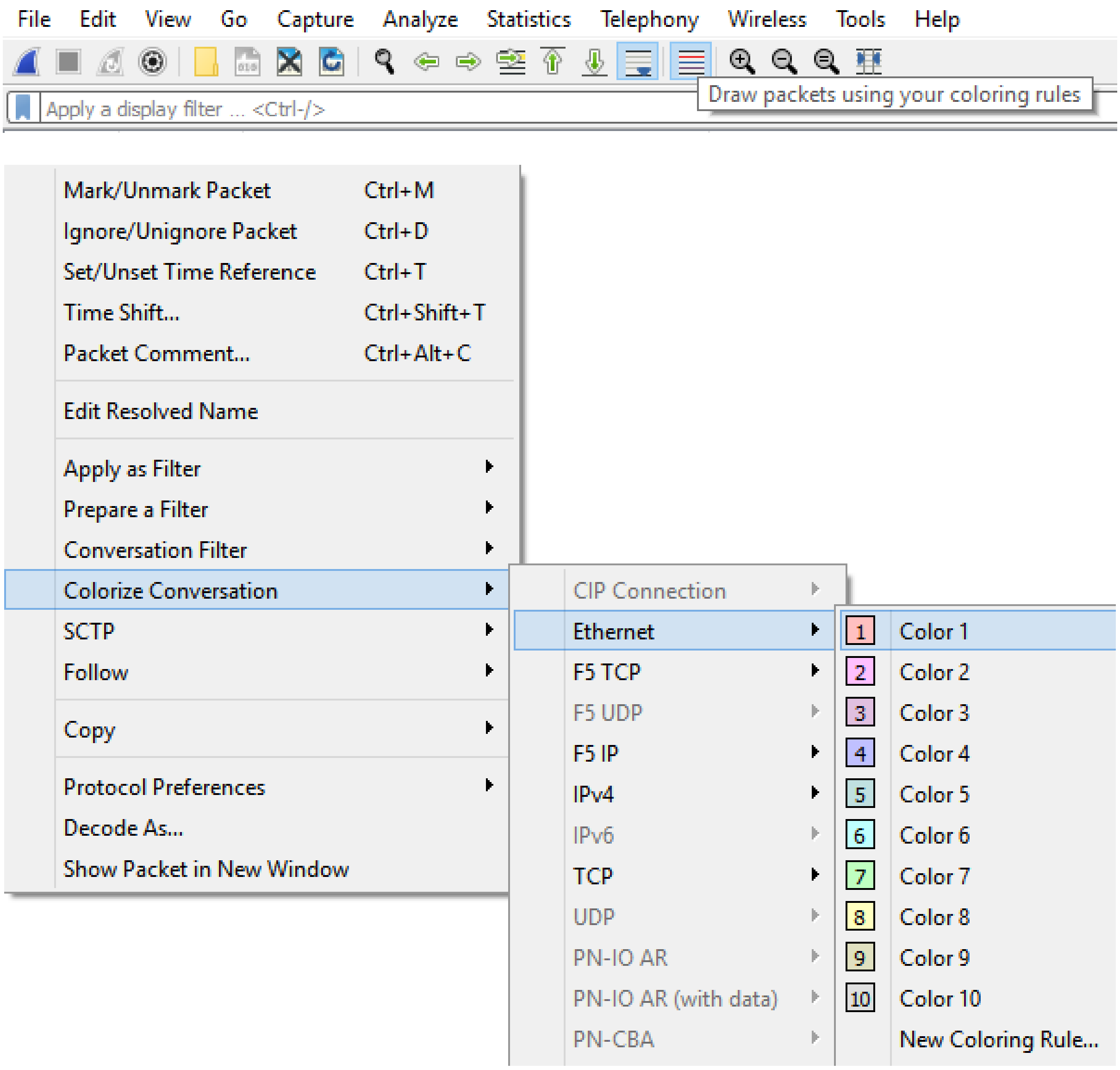
```
# This file was generated by running ./tools/make-manuf.
# Don't change it directly, change manuf.tmpl instead.
#
#
# /etc/manuf - Ethernet vendor codes, and well-known MAC
addresses
#
# Laurent Deniel <laurent.deniel [AT] free.fr>
#
# Wireshark - Network traffic analyzer
# By Gerald Combs <gerald [AT] wireshark.org>
# Copyright 1998 Gerald Combs
#
# SPDX-License-Identifier: GPL-2.0-or-later
#
# The data below has been assembled from the following sources:
#
# The IEEE public OUI listing available from:
# <http://standards.ieee.org/develop/regauth/oui/oui.txt>
# <http://standards.ieee.org/develop/regauth/iab/iab.txt>
# <http://standards.ieee.org/develop/regauth/oui36/oui36.txt>
#
# Michael Patton's "Ethernet Codes Master Page" available from:
#
<http://www.cavebear.com/archive/cavebear/Ethernet/Ethernet.txt>
```

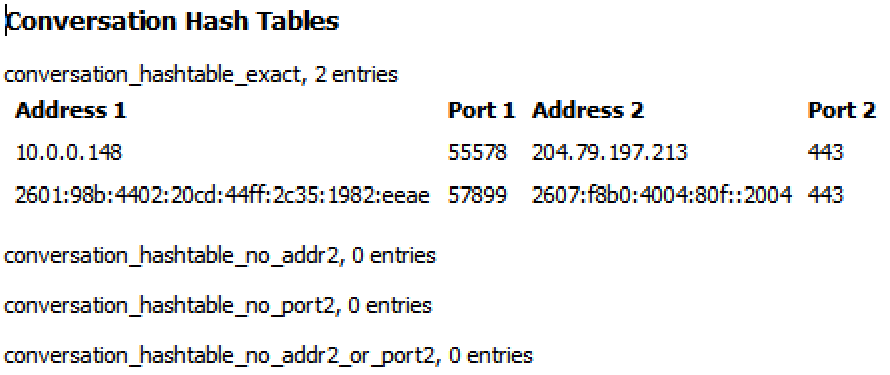


```
# This is a local copy of the IANA port-numbers file.
#
# Wireshark uses it to resolve port numbers into human
readable
# service names, e.g. TCP port 80 -> http.
#
# It is subject to copyright and being used with IANA's
permission:
# http://www.wireshark.org/lists/wireshark-
dev/200708/msg00160.html
```



```
◢ User Datagram Protocol, Src Port: 57899 (57899), Dst Port: https (443)
    Source Port: 57899 (57899)
    Destination Port: https (443)
    Length: 1358
    Checksum: 0xbb69 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
```





Conversation Hash Tables

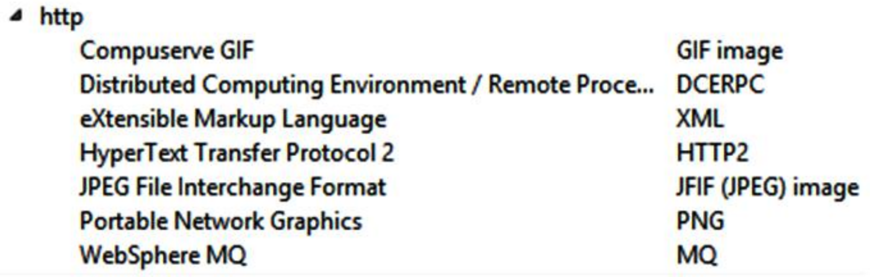
conversation_hashtable_exact, 2 entries

Address 1	Port 1	Address 2	Port 2
10.0.0.148	55578	204.79.197.213	443
2601:98b:4402:20cd:44ff:2c35:1982:eeae	57899	2607:f8b0:4004:80f::2004	443

conversation_hashtable_no_addr2, 0 entries

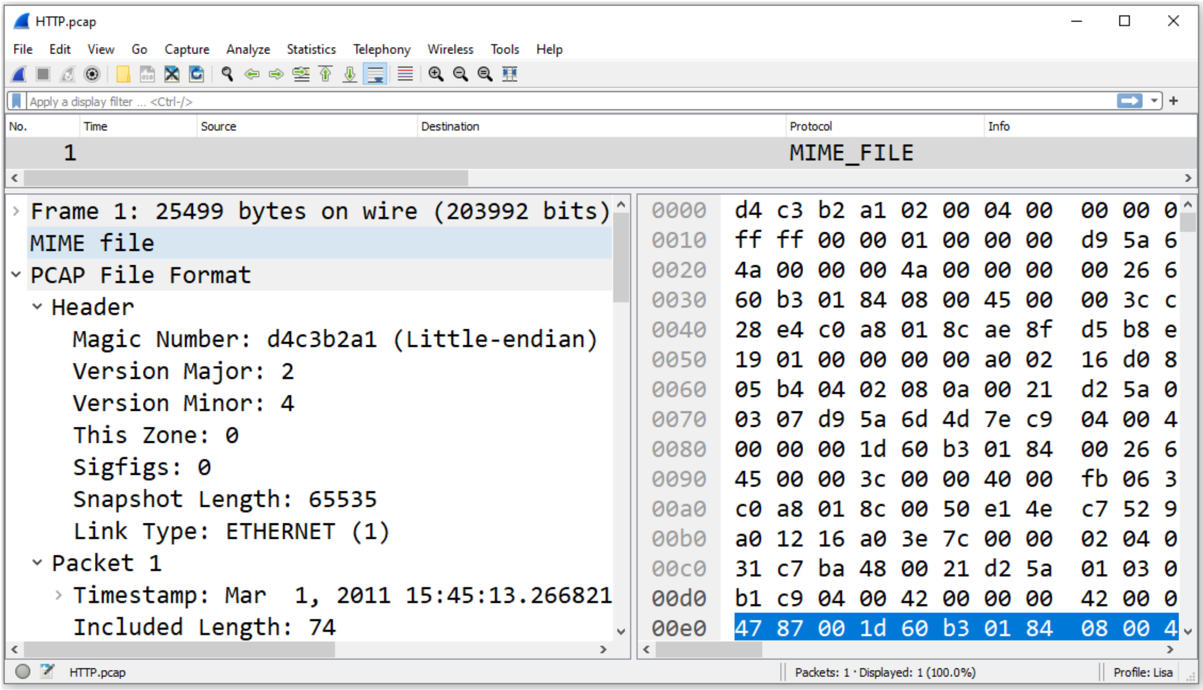
conversation_hashtable_no_port2, 0 entries

conversation_hashtable_no_addr2_or_port2, 0 entries



◢ http

Compuserve GIF	GIF image
Distributed Computing Environment / Remote Proce...	DCERPC
eXtensible Markup Language	XML
HyperText Transfer Protocol 2	HTTP2
JPEG File Interchange Format	JFIF (JPEG) image
Portable Network Graphics	PNG
WebSphere MQ	MQ

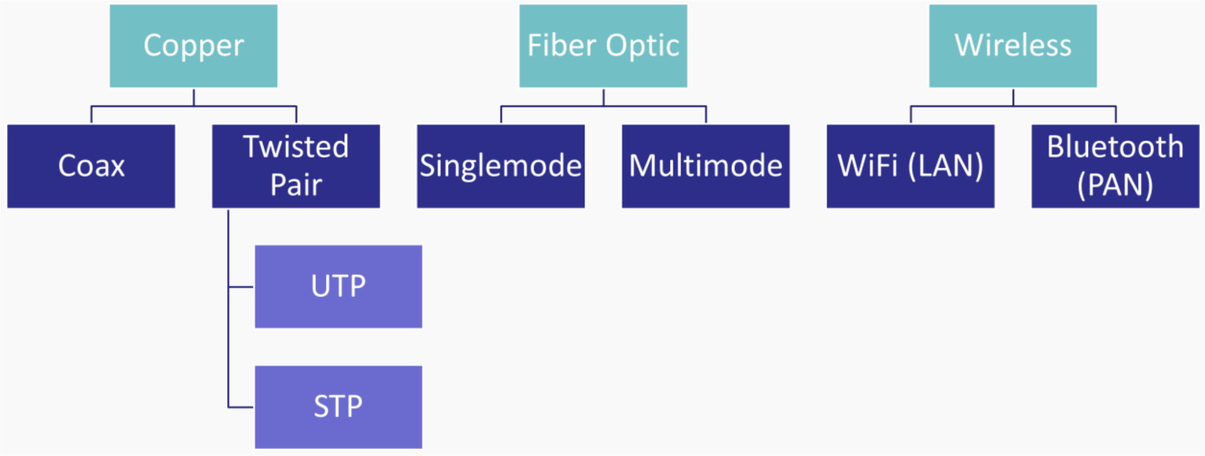


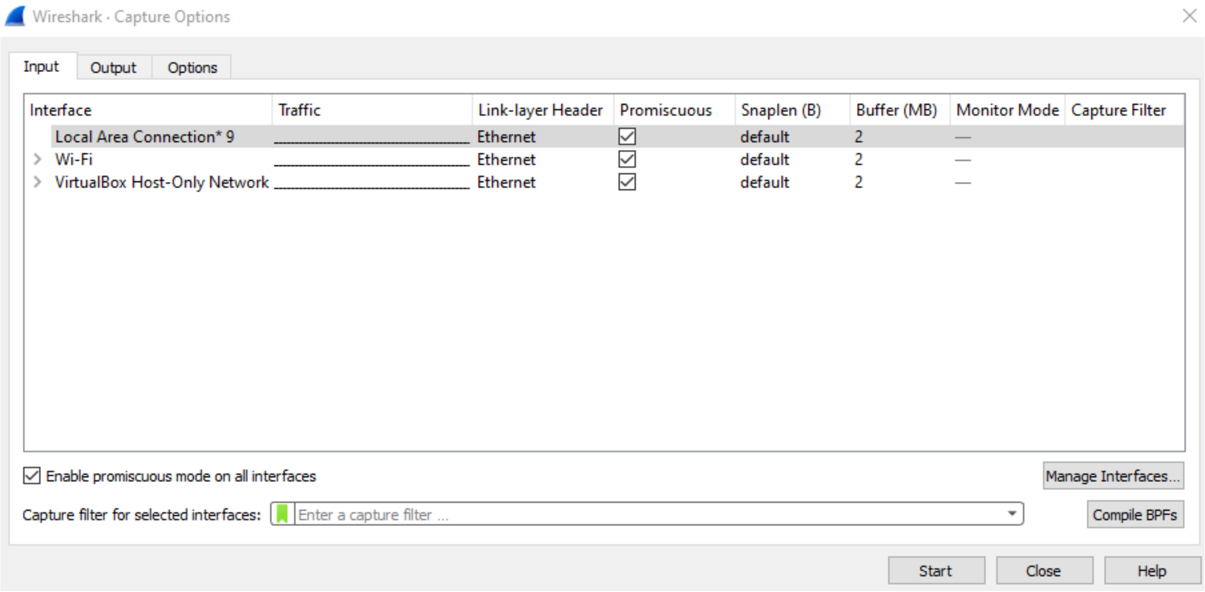
No.	Time	Source	Destination	Protocol	Info
1				MIME_FILE	

```
> Frame 1: 25499 bytes on wire (203992 bits)
  MIME file
v PCAP File Format
  v Header
      Magic Number: d4c3b2a1 (Little-endian)
      Version Major: 2
      Version Minor: 4
      This Zone: 0
      Sigfigs: 0
      Snapshot Length: 65535
      Link Type: ETHERNET (1)
  v Packet 1
    > Timestamp: Mar  1, 2011 15:45:13.266821
      Included Length: 74
```

```
0000  d4 c3 b2 a1 02 00 04 00  00 00 0
0010  ff ff 00 00 01 00 00 00  d9 5a 6
0020  4a 00 00 00 4a 00 00 00  00 26 6
0030  60 b3 01 84 08 00 45 00  00 3c c
0040  28 e4 c0 a8 01 8c ae 8f  d5 b8 e
0050  19 01 00 00 00 00 a0 02  16 d0 8
0060  05 b4 04 02 08 0a 00 21  d2 5a 0
0070  03 07 d9 5a 6d 4d 7e c9  04 00 4
0080  00 00 00 1d 60 b3 01 84  00 26 6
0090  45 00 00 3c 00 00 40 00  fb 06 3
00a0  c0 a8 01 8c 00 50 e1 4e  c7 52 9
00b0  a0 12 16 a0 3e 7c 00 00  02 04 0
00c0  31 c7 ba 48 00 21 d2 5a  01 03 0
00d0  b1 c9 04 00 42 00 00 00  42 00 0
00e0  47 87 00 1d 60 b3 01 84  08 00 4
```

Chapter 5: Tapping into the Data Stream

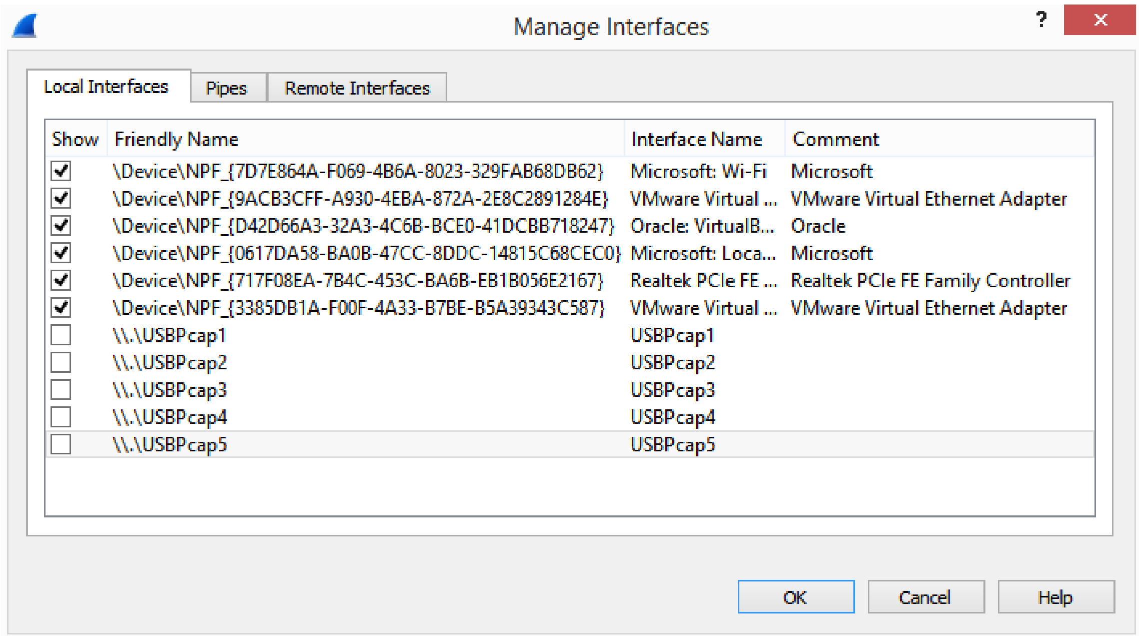




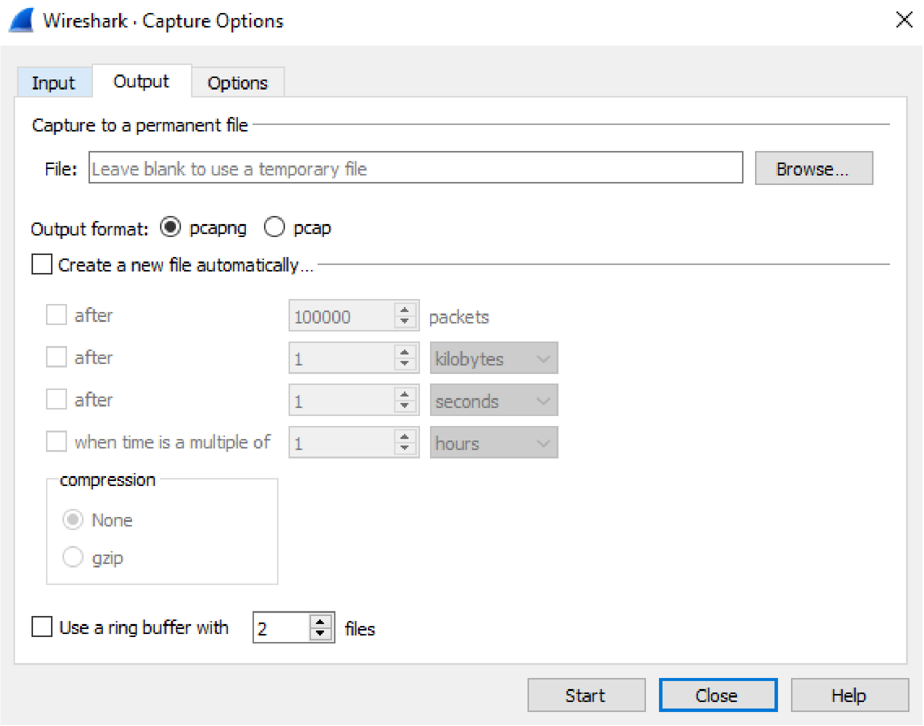
Interface	Traffic	Link-layer Header	Promiscuous	Snaplen (B)	Buffer (MB)	Monitor Mode	Capture Filter
Local Area Connection* 9		Ethernet	☑	default	2	—	
› Wi-Fi		Ethernet	☑	default	2	—	
› VirtualBox Host-Only Network		Ethernet	☑	default	2	—	

☑ Enable promiscuous mode on all interfaces

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



Show	Friendly Name	Interface Name	Comment
☑	\Device\NPF_{7D7E864A-F069-4B6A-8023-329FAB68DB62}	Microsoft: Wi-Fi	Microsoft
☑	\Device\NPF_{9ACB3CFF-A930-4EBA-872A-2E8C2891284E}	VMware Virtual ...	VMware Virtual Ethernet Adapter
☑	\Device\NPF_{D42D66A3-32A3-4C6B-BCE0-41DCBB718247}	Oracle: VirtualB...	Oracle
☑	\Device\NPF_{0617DA58-BA0B-47CC-8DDC-14815C68CEC0}	Microsoft: Loca...	Microsoft
☑	\Device\NPF_{717F08EA-7B4C-453C-BA6B-EB1B056E2167}	Realtek PCIe FE ...	Realtek PCIe FE Family Controller
☑	\Device\NPF_{3385DB1A-F00F-4A33-B7BE-B5A39343C587}	VMware Virtual ...	VMware Virtual Ethernet Adapter
☐	\\.\USBPcap1	USBPcap1	
☐	\\.\USBPcap2	USBPcap2	
☐	\\.\USBPcap3	USBPcap3	
☐	\\.\USBPcap4	USBPcap4	
☐	\\.\USBPcap5	USBPcap5	



Capture to a permanent file

File: Leave blank to use a temporary file

Output format: ● pcapng ○ pcap

□ Create a new file automatically...

□ after 100000 packets

□ after 1 kilobytes

□ after 1 seconds

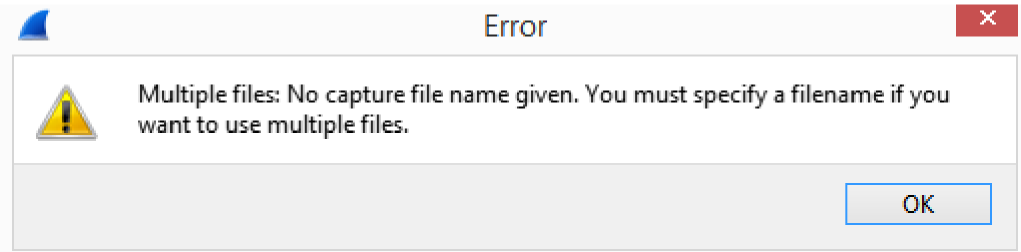
□ when time is a multiple of 1 hours

compression

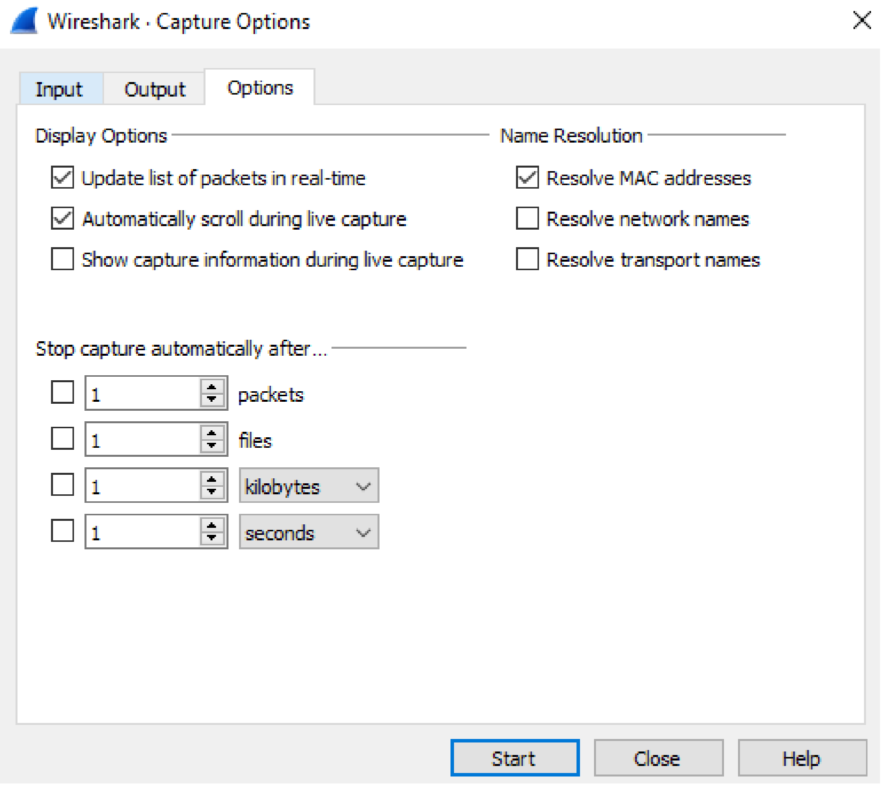
● None

○ gzip

□ Use a ring buffer with 2 files



Multiple files: No capture file name given. You must specify a filename if you want to use multiple files.



Display Options

☑ Update list of packets in real-time

☑ Automatically scroll during live capture

□ Show capture information during live capture

Name Resolution

☑ Resolve MAC addresses

□ Resolve network names

□ Resolve transport names

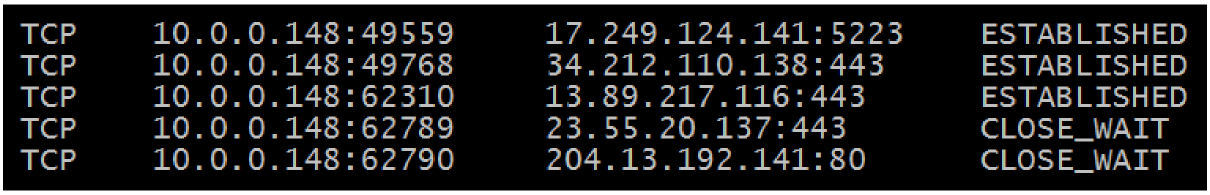
Stop capture automatically after...

□ 1 packets

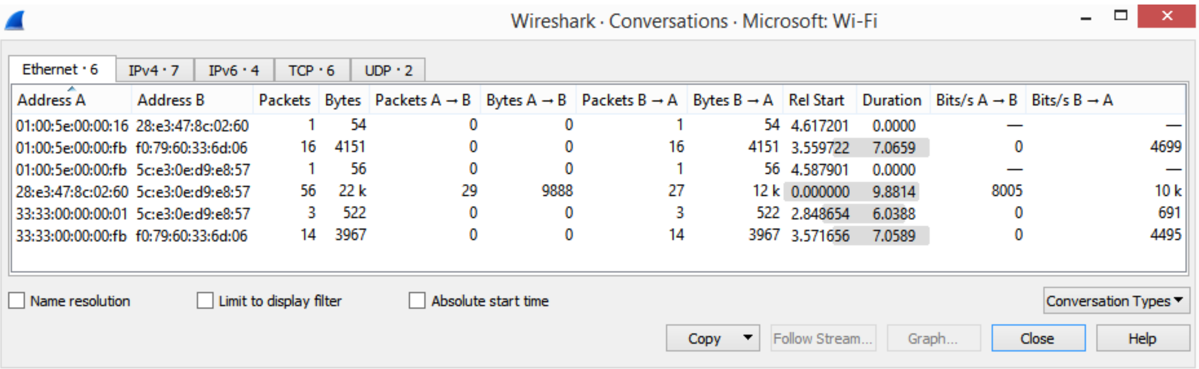
□ 1 files

□ 1 kilobytes

□ 1 seconds



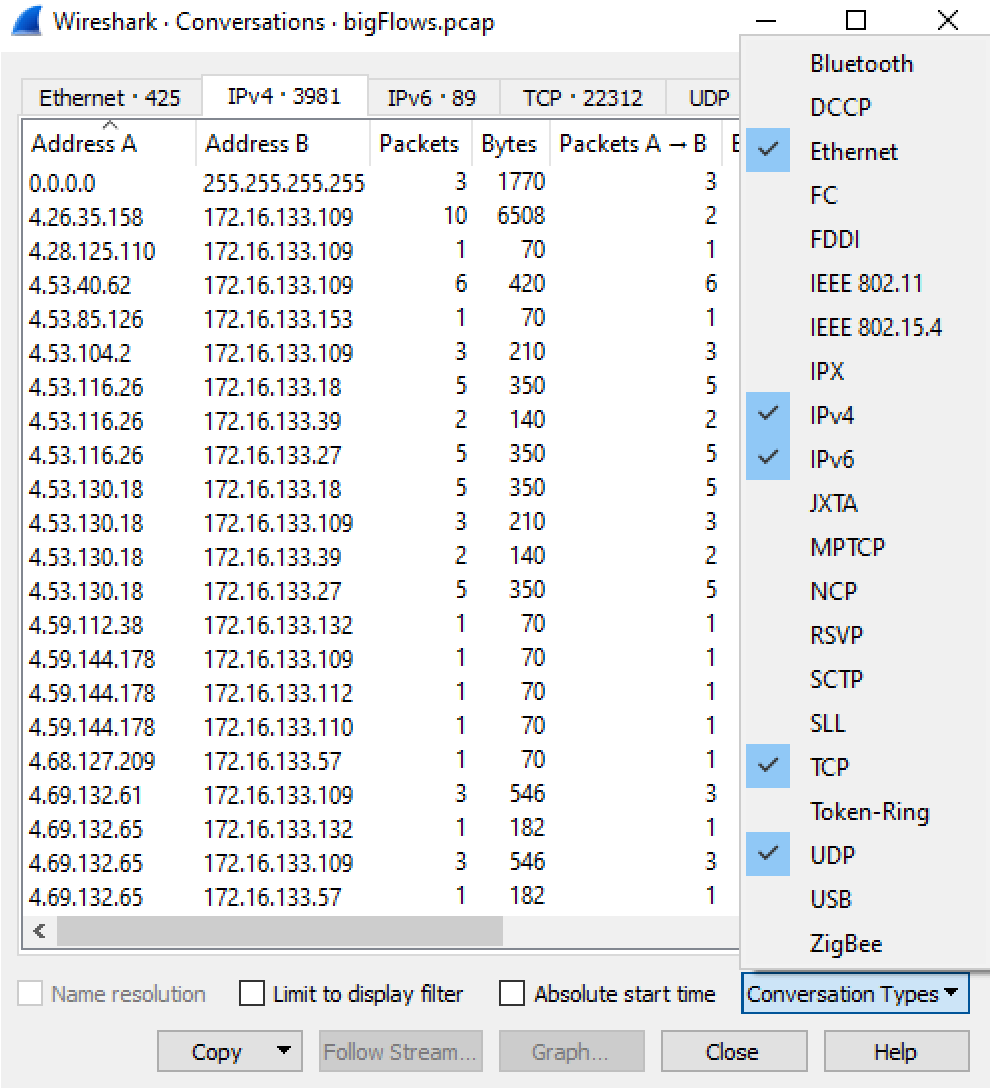
```
TCP    10.0.0.148:49559     17.249.124.141:5223    ESTABLISHED
TCP    10.0.0.148:49768     34.212.110.138:443     ESTABLISHED
TCP    10.0.0.148:62310     13.89.217.116:443      ESTABLISHED
TCP    10.0.0.148:62789     23.55.20.137:443       CLOSE_WAIT
TCP    10.0.0.148:62790     204.13.192.141:80      CLOSE_WAIT
```



Wireshark · Conversations · Microsoft: Wi-Fi

Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
01:00:5e:00:00:16	28:e3:47:8c:02:60	1	54	0	0	1	54	4.617201	0.0000	—	—
01:00:5e:00:00:fb	f0:79:60:33:6d:06	16	4151	0	0	16	4151	3.559722	7.0659	0	4699
01:00:5e:00:00:fb	5c:e3:0e:d9:e8:57	1	56	0	0	1	56	4.587901	0.0000	—	—
28:e3:47:8c:02:60	5c:e3:0e:d9:e8:57	56	22 k	29	9888	27	12 k	0.000000	9.8814	8005	10 k
33:33:00:00:00:01	5c:e3:0e:d9:e8:57	3	522	0	0	3	522	2.848654	6.0388	0	691
33:33:00:00:00:fb	f0:79:60:33:6d:06	14	3967	0	0	14	3967	3.571656	7.0589	0	4495

☐ Name resolution ☐ Limit to display filter ☐ Absolute start time

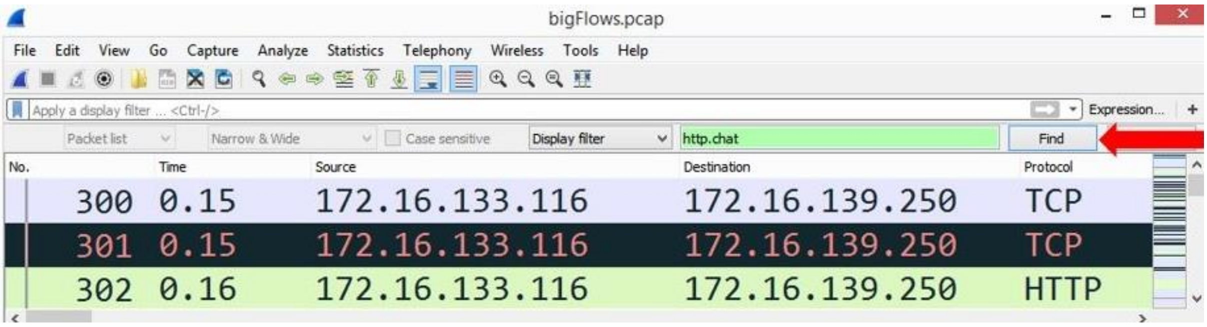


Wireshark · Conversations · bigFlows.pcap

Address A	Address B	Packets	Bytes	Packets A → B
0.0.0.0	255.255.255.255	3	1770	3
4.26.35.158	172.16.133.109	10	6508	2
4.28.125.110	172.16.133.109	1	70	1
4.53.40.62	172.16.133.109	6	420	6
4.53.85.126	172.16.133.153	1	70	1
4.53.104.2	172.16.133.109	3	210	3
4.53.116.26	172.16.133.18	5	350	5
4.53.116.26	172.16.133.39	2	140	2
4.53.116.26	172.16.133.27	5	350	5
4.53.130.18	172.16.133.18	5	350	5
4.53.130.18	172.16.133.109	3	210	3
4.53.130.18	172.16.133.39	2	140	2
4.53.130.18	172.16.133.27	5	350	5
4.59.112.38	172.16.133.132	1	70	1
4.59.144.178	172.16.133.109	1	70	1
4.59.144.178	172.16.133.112	1	70	1
4.59.144.178	172.16.133.110	1	70	1
4.68.127.209	172.16.133.57	1	70	1
4.69.132.61	172.16.133.109	3	546	3
4.69.132.65	172.16.133.132	1	182	1
4.69.132.65	172.16.133.109	3	546	3
4.69.132.65	172.16.133.57	1	182	1

Bluetooth
DCCP
✓ Ethernet
FC
FDDI
IEEE 802.11
IEEE 802.15.4
IPX
✓ IPv4
✓ IPv6
JXTA
MPTCP
NCP
RSVP
SCTP
SLL
✓ TCP
Token-Ring
✓ UDP
USB
ZigBee

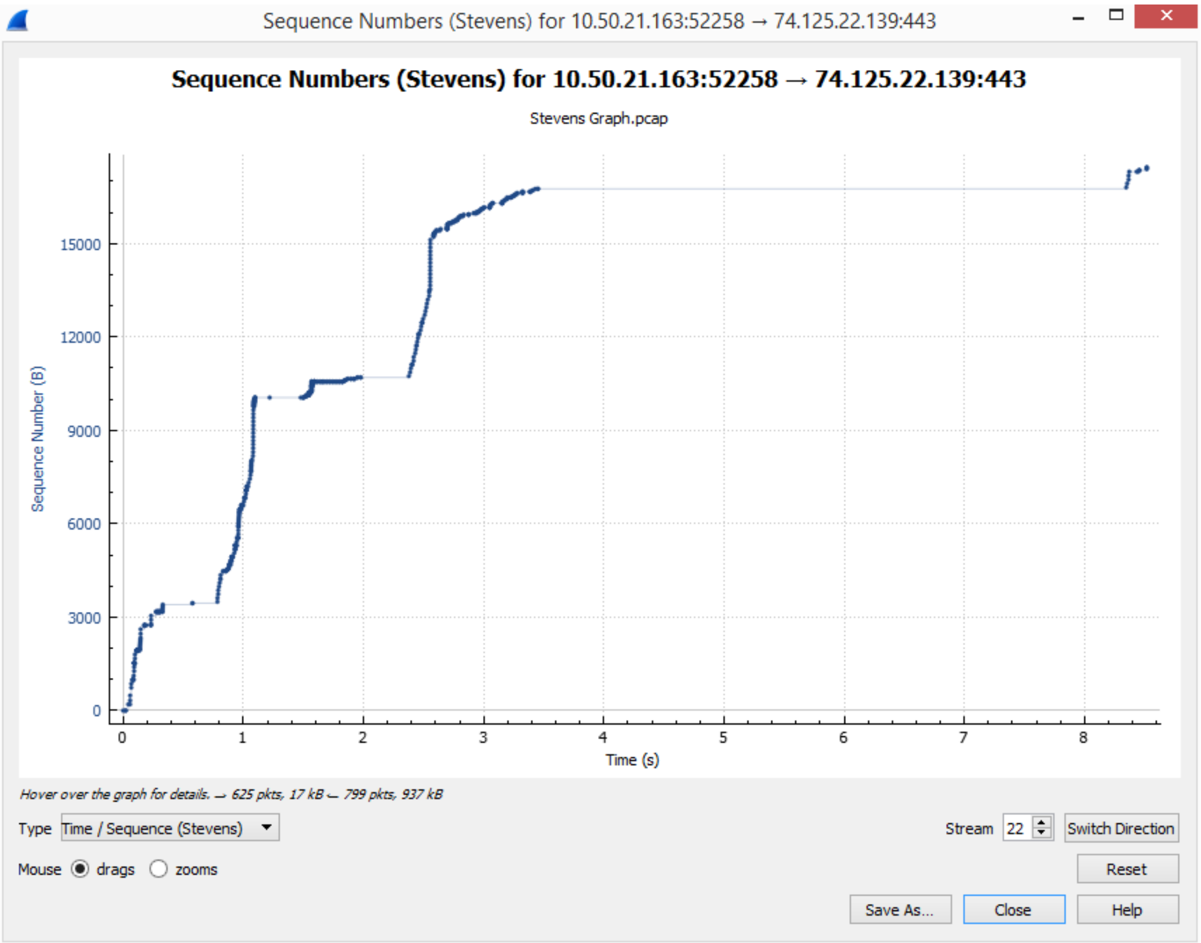
☐ Name resolution ☐ Limit to display filter ☐ Absolute start time



bigFlows.pcap

□ Case sensitive   Display filter   http.chat

No.	Time	Source	Destination	Protocol
300	0.15	172.16.133.116	172.16.139.250	TCP
301	0.15	172.16.133.116	172.16.139.250	TCP
302	0.16	172.16.133.116	172.16.139.250	HTTP



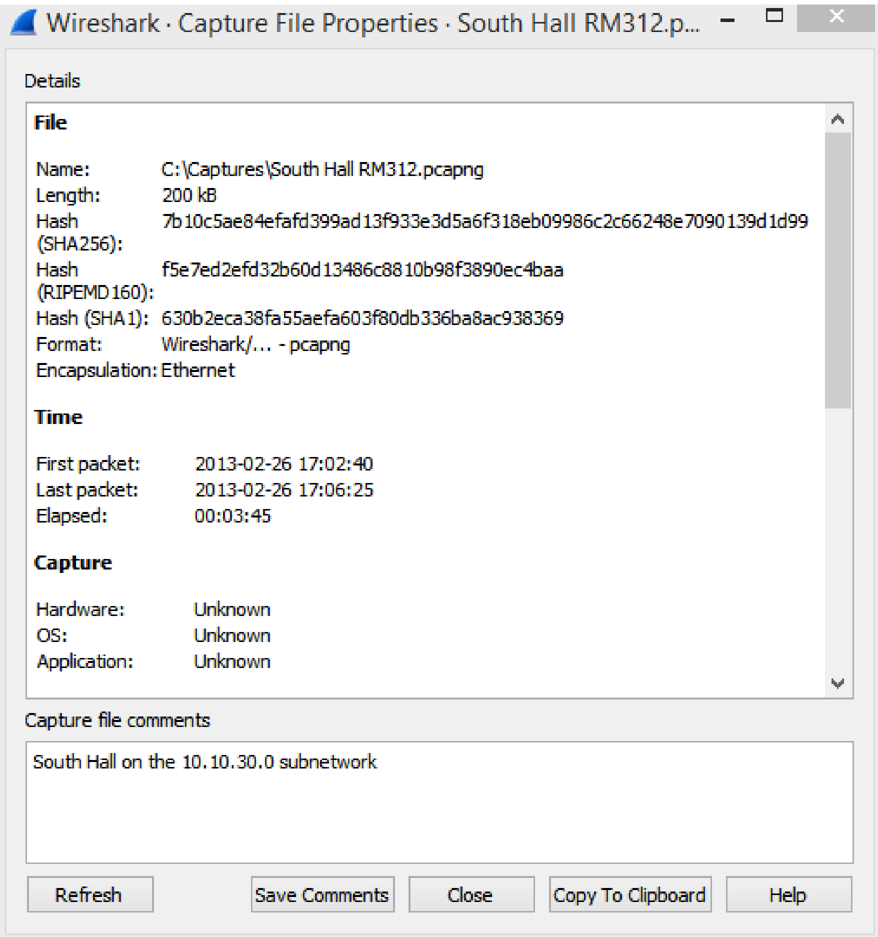
Sequence Numbers (Stevens) for 10.50.21.163:52258 → 74.125.22.139:443

Hover over the graph for details. → 625 pkts, 17 kB ← 799 pkts, 937 kB

Type Time / Sequence (Stevens)

Stream 22

Mouse ● drags ○ zooms



Details

File

Name: C:\Captures\South Hall RM312.pcapng
Length: 200 kB
Hash (SHA256): 7b10c5ae84efafd399ad13f933e3d5a6f318eb09986c2c66248e7090139d1d99
Hash (RIPEMD160): f5e7ed2efd32b60d13486c8810b98f3890ec4baa
Hash (SHA1): 630b2eca38fa55aefa603f80db336ba8ac938369
Format: Wireshark/... - pcapng
Encapsulation: Ethernet

Time

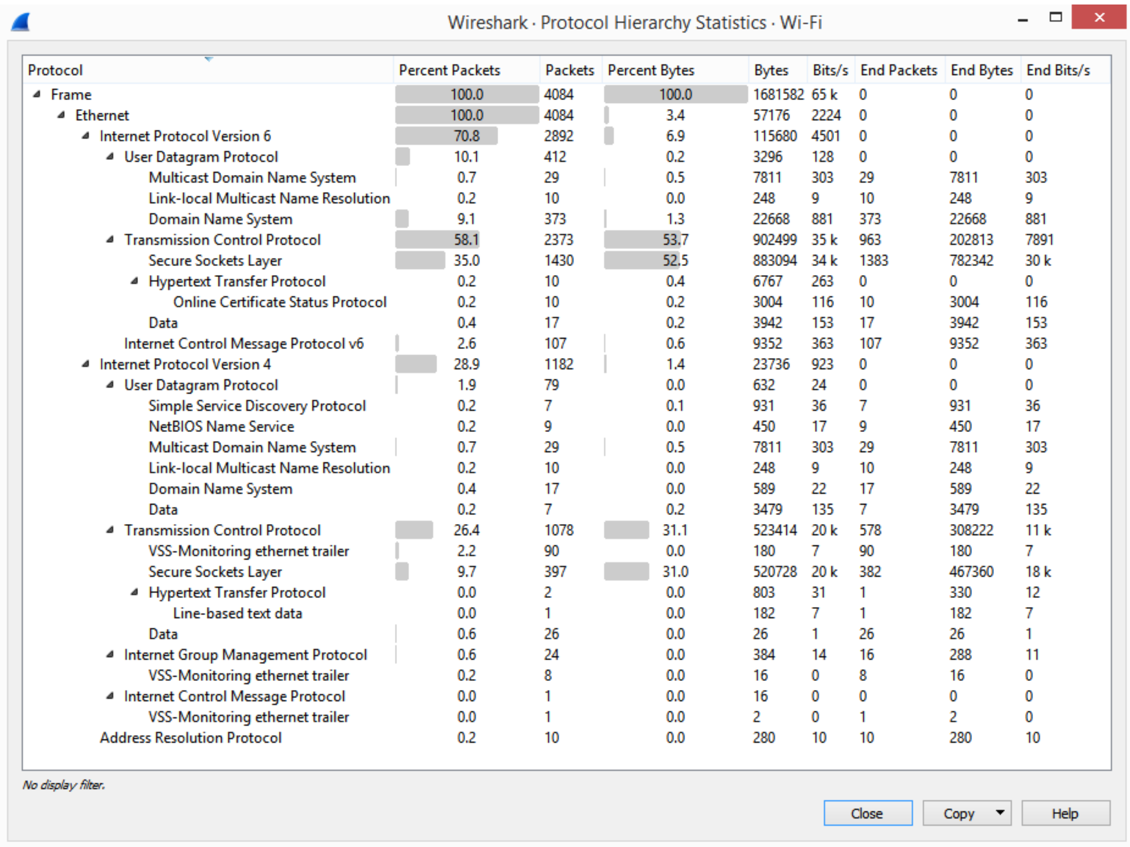
First packet: 2013-02-26 17:02:40
Last packet: 2013-02-26 17:06:25
Elapsed: 00:03:45

Capture

Hardware: Unknown
OS: Unknown
Application: Unknown

Capture file comments

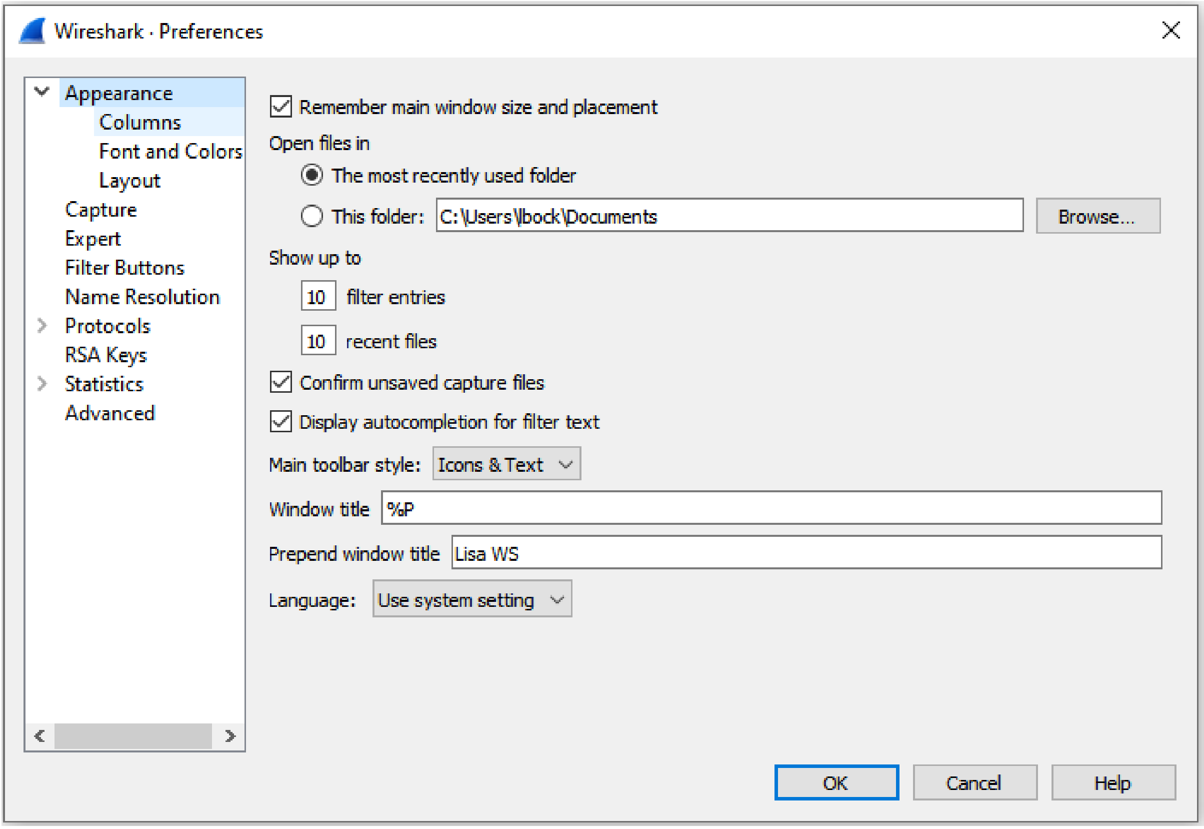
South Hall on the 10.10.30.0 subnetwork



Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	4084	100.0	1681582	65 k	0	0	0
Ethernet	100.0	4084	3.4	57176	2224	0	0	0
Internet Protocol Version 6	70.8	2892	6.9	115680	4501	0	0	0
User Datagram Protocol	10.1	412	0.2	3296	128	0	0	0
Multicast Domain Name System	0.7	29	0.5	7811	303	29	7811	303
Link-local Multicast Name Resolution	0.2	10	0.0	248	9	10	248	9
Domain Name System	9.1	373	1.3	22668	881	373	22668	881
Transmission Control Protocol	58.1	2373	53.7	902499	35 k	963	202813	7891
Secure Sockets Layer	35.0	1430	52.5	883094	34 k	1383	782342	30 k
Hypertext Transfer Protocol	0.2	10	0.4	6767	263	0	0	0
Online Certificate Status Protocol	0.2	10	0.2	3004	116	10	3004	116
Data	0.4	17	0.2	3942	153	17	3942	153
Internet Control Message Protocol v6	2.6	107	0.6	9352	363	107	9352	363
Internet Protocol Version 4	28.9	1182	1.4	23736	923	0	0	0
User Datagram Protocol	1.9	79	0.0	632	24	0	0	0
Simple Service Discovery Protocol	0.2	7	0.1	931	36	7	931	36
NetBIOS Name Service	0.2	9	0.0	450	17	9	450	17
Multicast Domain Name System	0.7	29	0.5	7811	303	29	7811	303
Link-local Multicast Name Resolution	0.2	10	0.0	248	9	10	248	9
Domain Name System	0.4	17	0.0	589	22	17	589	22
Data	0.2	7	0.2	3479	135	7	3479	135
Transmission Control Protocol	26.4	1078	31.1	523414	20 k	578	308222	11 k
VSS-Monitoring ethernet trailer	2.2	90	0.0	180	7	90	180	7
Secure Sockets Layer	9.7	397	31.0	520728	20 k	382	467360	18 k
Hypertext Transfer Protocol	0.0	2	0.0	803	31	1	330	12
Line-based text data	0.0	1	0.0	182	7	1	182	7
Data	0.6	26	0.0	26	1	26	26	1
Internet Group Management Protocol	0.6	24	0.0	384	14	16	288	11
VSS-Monitoring ethernet trailer	0.2	8	0.0	16	0	8	16	0
Internet Control Message Protocol	0.0	1	0.0	16	0	0	0	0
VSS-Monitoring ethernet trailer	0.0	1	0.0	2	0	1	2	0
Address Resolution Protocol	0.2	10	0.0	280	10	10	280	10

No display filter.

Chapter 6: Personalizing the Interface



Wireshark · Preferences

☑ Remember main window size and placement

Open files in

● The most recently used folder

○ This folder: C:\Users\lbock\Documents Browse...

Show up to

10 filter entries

10 recent files

☑ Confirm unsaved capture files

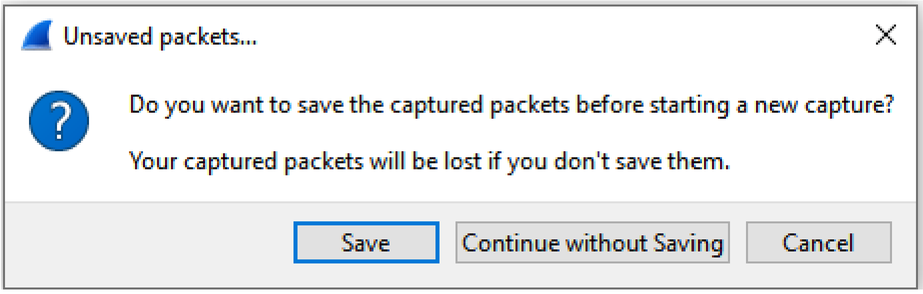
☑ Display autocompletion for filter text

Main toolbar style: Icons & Text

Window title: %P

Prepend window title: Lisa WS

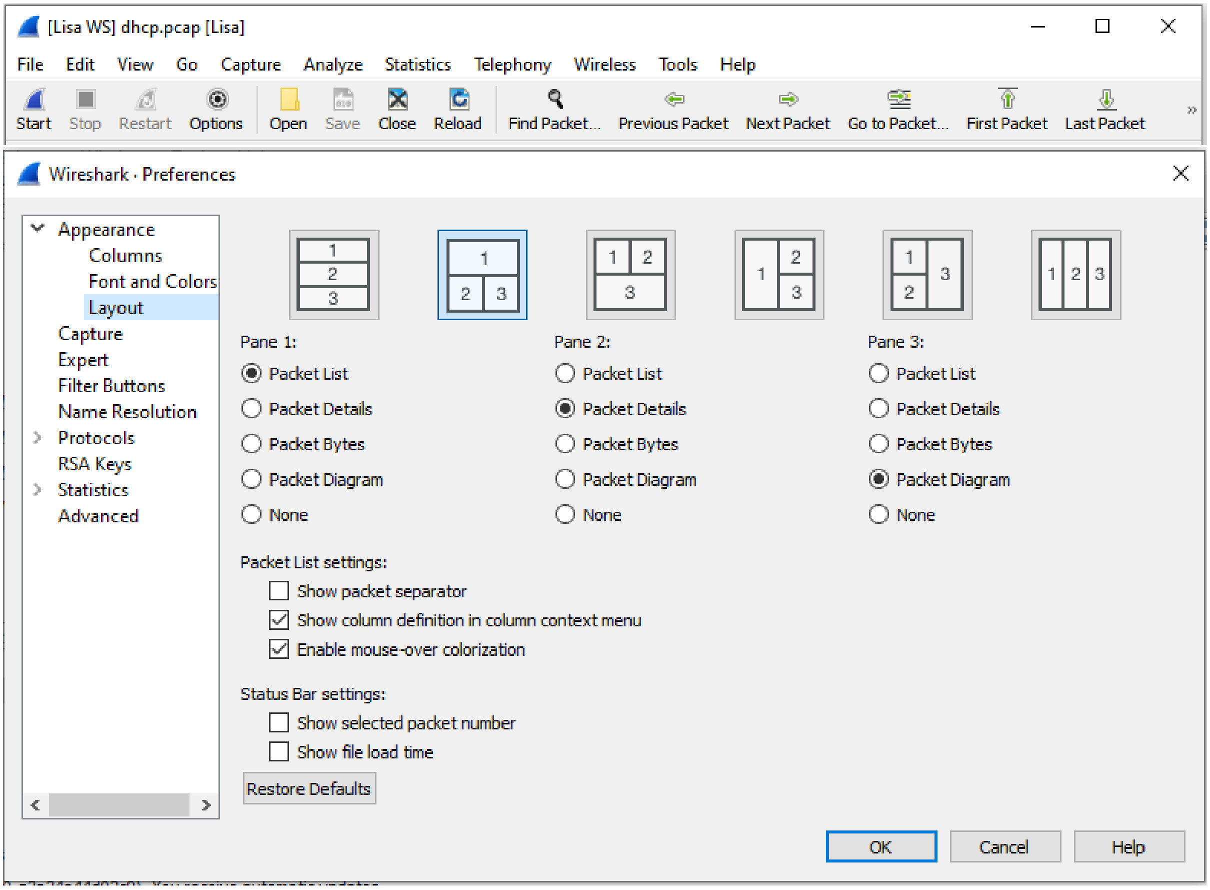
Language: Use system setting



Unsaved packets...

Do you want to save the captured packets before starting a new capture?

Your captured packets will be lost if you don't save them.


[Lisa WS] dhcp.pcap [Lisa]
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Start Stop Restart Options Open Save Close Reload Find Packet… Previous Packet Next Packet Go to Packet… First Packet Last Packet
Wireshark · Preferences
Appearance
Columns
Font and Colors
Layout
Capture
Expert
Filter Buttons
Name Resolution
Protocols
RSA Keys
Statistics
Advanced
1 2 3
Restore Defaults
OK
Cancel
Help

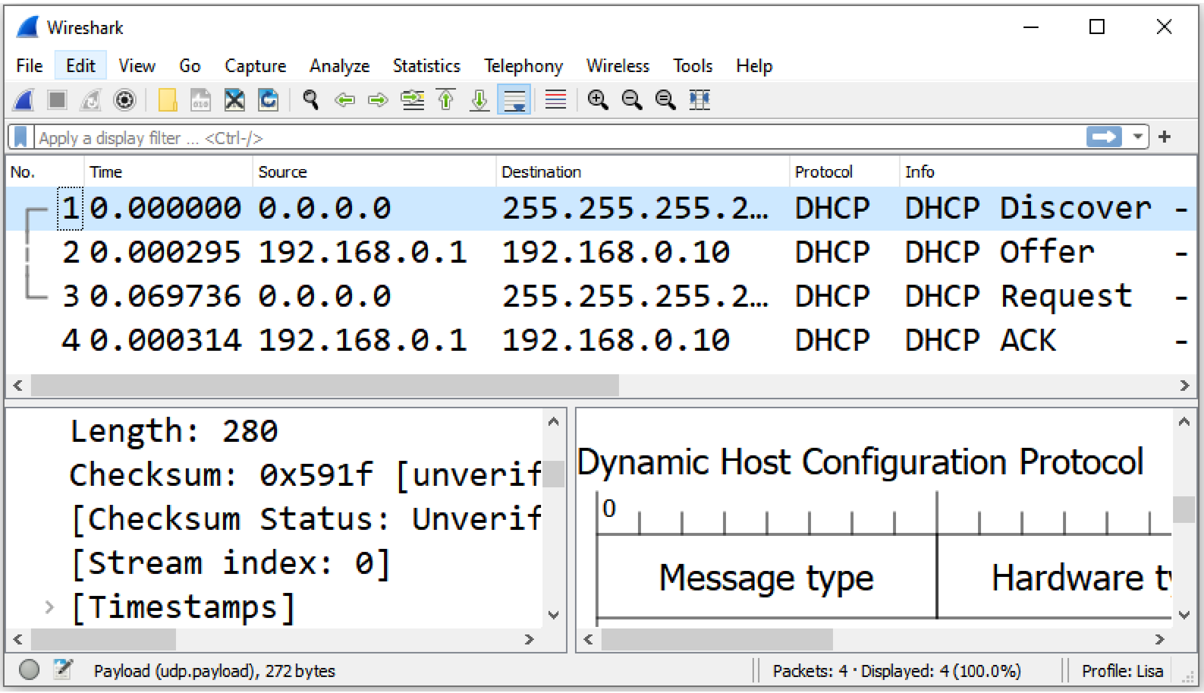
Pane 1:
- ● Packet List
- ○ Packet Details
- ○ Packet Bytes
- ○ Packet Diagram
- ○ None

Pane 2:
- ○ Packet List
- ● Packet Details
- ○ Packet Bytes
- ○ Packet Diagram
- ○ None

Pane 3:
- ○ Packet List
- ○ Packet Details
- ○ Packet Bytes
- ● Packet Diagram
- ○ None

Packet List settings:
- □ Show packet separator
- ☑ Show column definition in column context menu
- ☑ Enable mouse-over colorization

Status Bar settings:
- □ Show selected packet number
- □ Show file load time

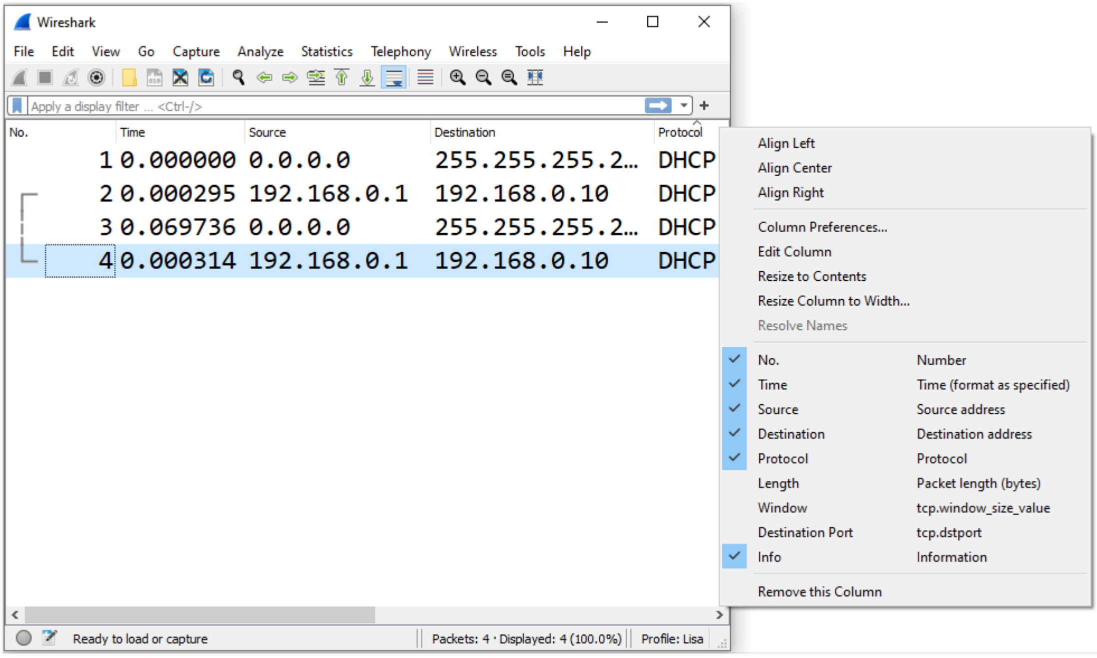

Wireshark
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

No.	Time	Source	Destination	Protocol	Info
1	0.000000	0.0.0.0	255.255.255.2…	DHCP	DHCP Discover -
2	0.000295	192.168.0.1	192.168.0.10	DHCP	DHCP Offer -
3	0.069736	0.0.0.0	255.255.255.2…	DHCP	DHCP Request -
4	0.000314	192.168.0.1	192.168.0.10	DHCP	DHCP ACK -

```
Length: 280
Checksum: 0x591f [unverif
[Checksum Status: Unverif
[Stream index: 0]
› [Timestamps]
```

Dynamic Host Configuration Protocol
0
Message type
Hardware t

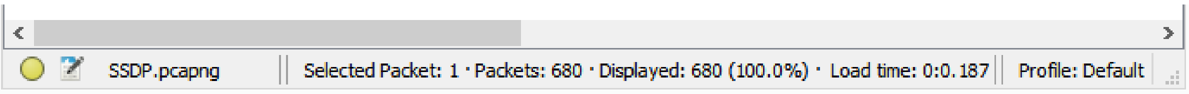
Payload (udp.payload), 272 bytes
Packets: 4 · Displayed: 4 (100.0%)
Profile: Lisa


Wireshark
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Align Left
Align Center
Align Right
Column Preferences...
Edit Column
Resize to Contents
Resize Column to Width...
Resolve Names
Remove this Column

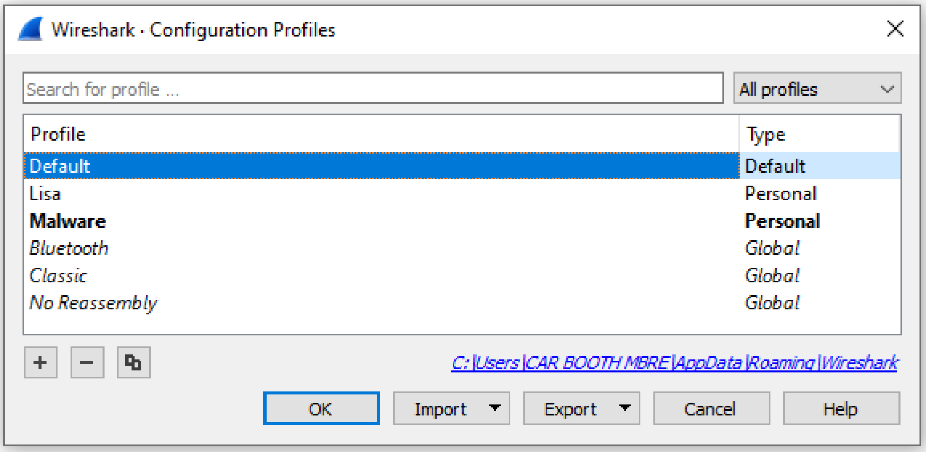
```
No.  Time      Source      Destination     Protocol
   1 0.000000 0.0.0.0     255.255.255.2… DHCP
   2 0.000295 192.168.0.1 192.168.0.10   DHCP
   3 0.069736 0.0.0.0     255.255.255.2… DHCP
   4 0.000314 192.168.0.1 192.168.0.10   DHCP
```

✓	No.	Number
✓	Time	Time (format as specified)
✓	Source	Source address
✓	Destination	Destination address
✓	Protocol	Protocol
	Length	Packet length (bytes)
	Window	tcp.window_size_value
	Destination Port	tcp.dstport
✓	Info	Information

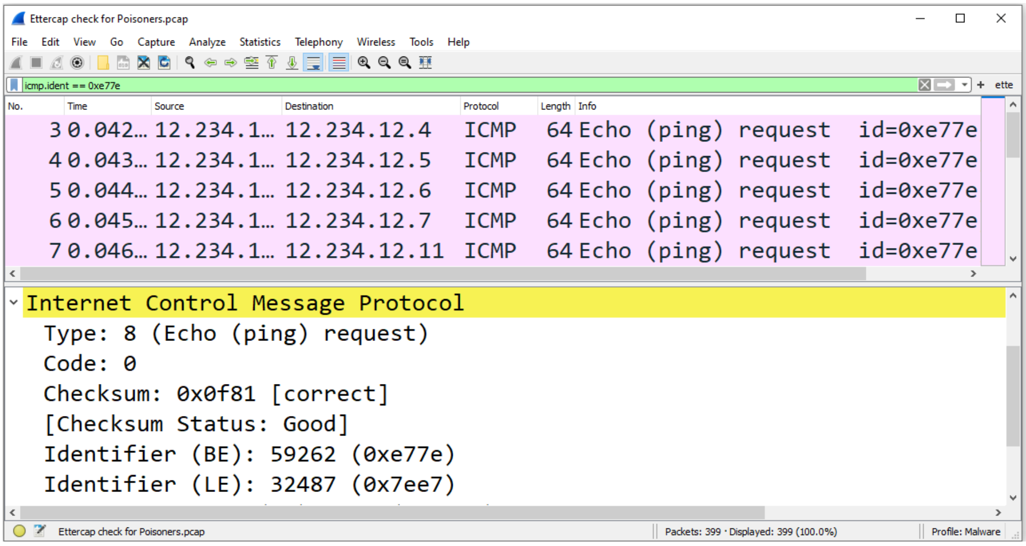
Ready to load or capture | Packets: 4 · Displayed: 4 (100.0%) | Profile: Lisa



SSDP.pcapng | Selected Packet: 1 · Packets: 680 · Displayed: 680 (100.0%) · Load time: 0:0.187 | Profile: Default


Wireshark · Configuration Profiles
Search for profile ...
All profiles
C:\Users\CAR BOOTH MBRE\AppData\Roaming\Wireshark
OK
Import
Export
Cancel
Help

Profile	Type
Default	Default
Lisa	Personal
Malware	**Personal**
Bluetooth	*Global*
Classic	*Global*
No Reassembly	*Global*

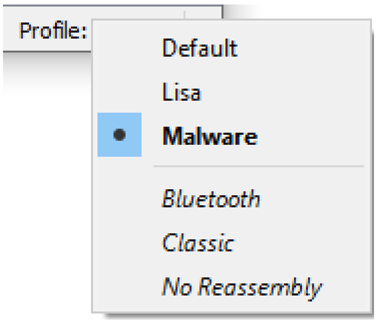

Ettercap check for Poisoners.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ette

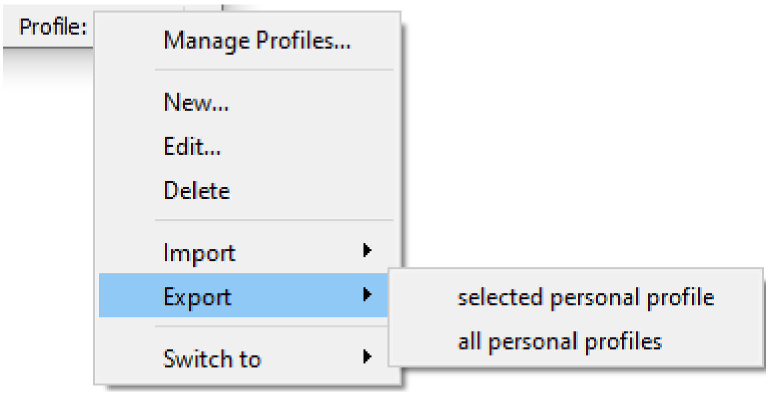
icmp.ident == 0xe77e

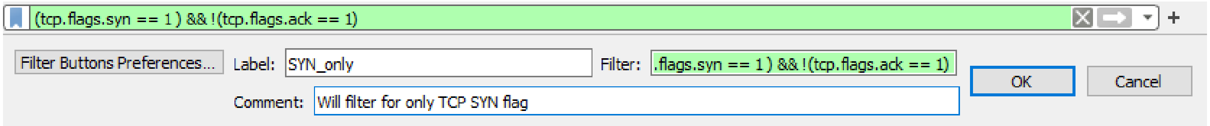
```
No. Time     Source      Destination   Protocol Length Info
  3 0.042… 12.234.1… 12.234.12.4  ICMP  64 Echo (ping) request  id=0xe77e
  4 0.043… 12.234.1… 12.234.12.5  ICMP  64 Echo (ping) request  id=0xe77e
  5 0.044… 12.234.1… 12.234.12.6  ICMP  64 Echo (ping) request  id=0xe77e
  6 0.045… 12.234.1… 12.234.12.7  ICMP  64 Echo (ping) request  id=0xe77e
  7 0.046… 12.234.1… 12.234.12.11 ICMP  64 Echo (ping) request  id=0xe77e
```

```
Internet Control Message Protocol
  Type: 8 (Echo (ping) request)
  Code: 0
  Checksum: 0x0f81 [correct]
  [Checksum Status: Good]
  Identifier (BE): 59262 (0xe77e)
  Identifier (LE): 32487 (0x7ee7)
```

Ettercap check for Poisoners.pcap | Packets: 399 · Displayed: 399 (100.0%) | Profile: Malware





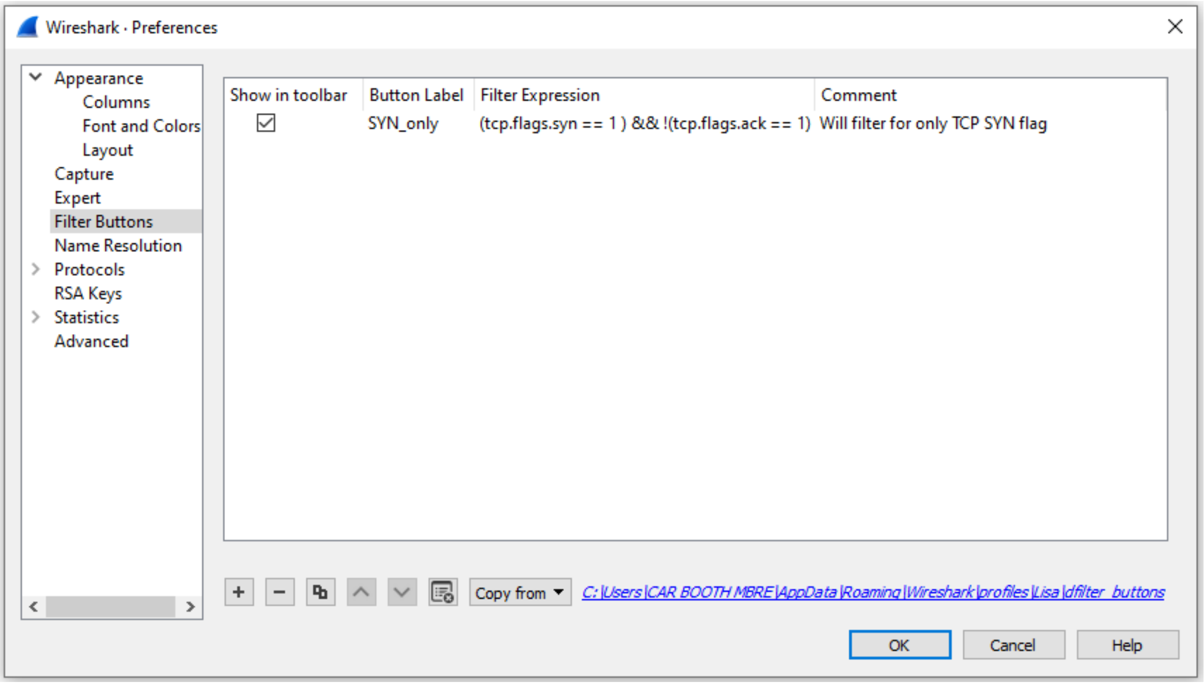


(tcp.flags.syn == 1) && !(tcp.flags.ack == 1)

Label: SYN_only

Filter: .flags.syn == 1) && !(tcp.flags.ack == 1)

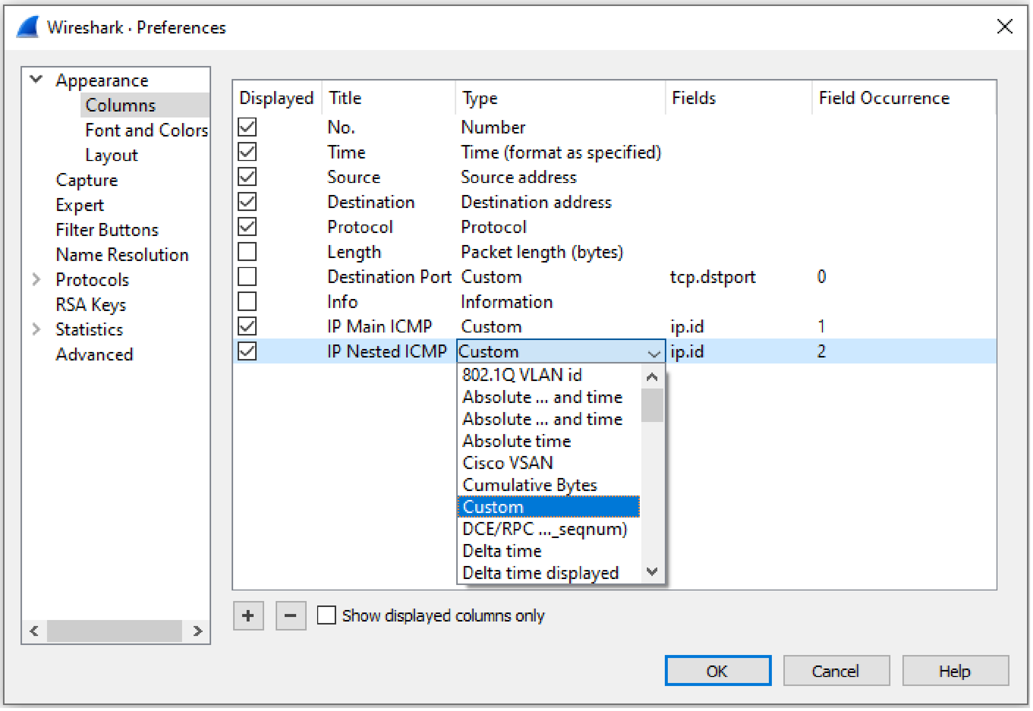
Comment: Will filter for only TCP SYN flag



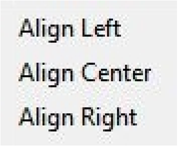
Wireshark · Preferences

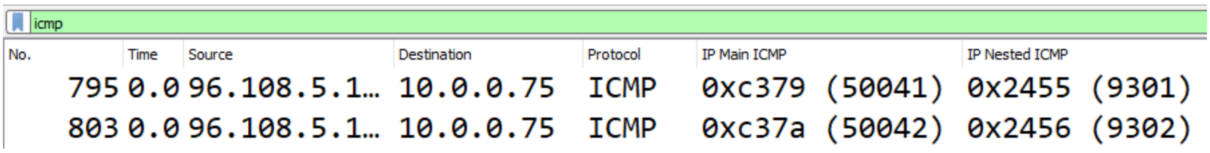
Show in toolbar	Button Label	Filter Expression	Comment
☑	SYN_only	(tcp.flags.syn == 1) && !(tcp.flags.ack == 1)	Will filter for only TCP SYN flag

C:\Users\CAR BOOTH MBRE\AppData\Roaming\Wireshark\profiles\Lisa\dfilter_buttons

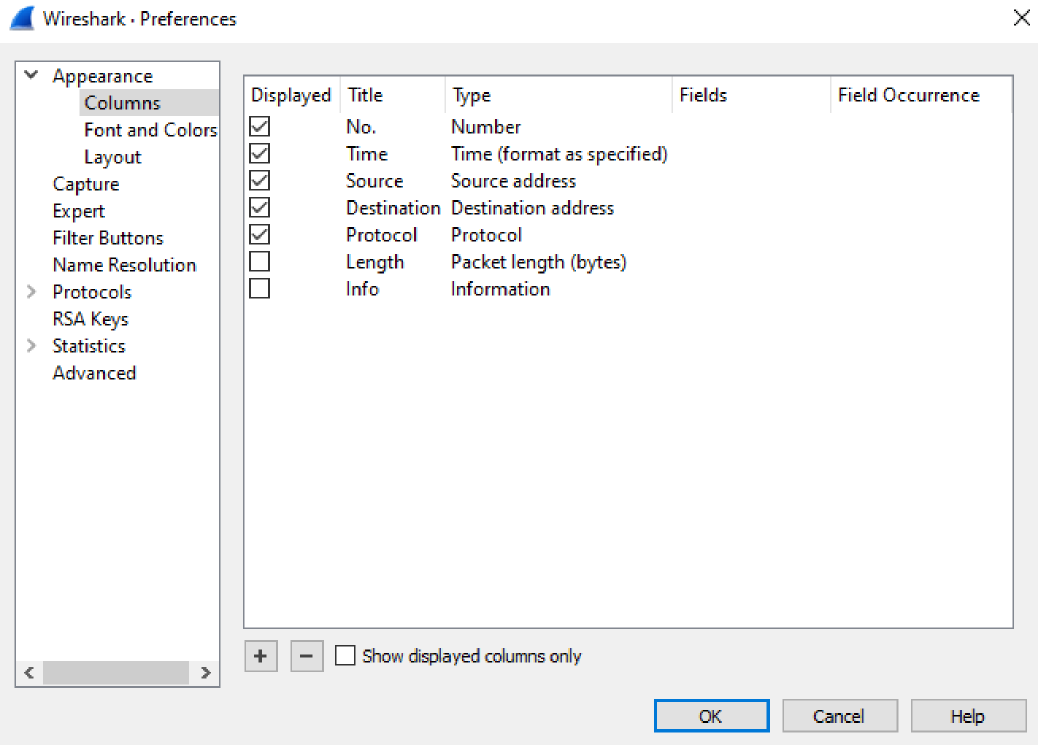


Displayed	Title	Type	Fields	Field Occurrence
☑	No.	Number		
☑	Time	Time (format as specified)		
☑	Source	Source address		
☑	Destination	Destination address		
☑	Protocol	Protocol		
☐	Length	Packet length (bytes)		
☐	Destination Port	Custom	tcp.dstport	0
☐	Info	Information		
☑	IP Main ICMP	Custom	ip.id	1
☑	IP Nested ICMP	Custom	ip.id	2

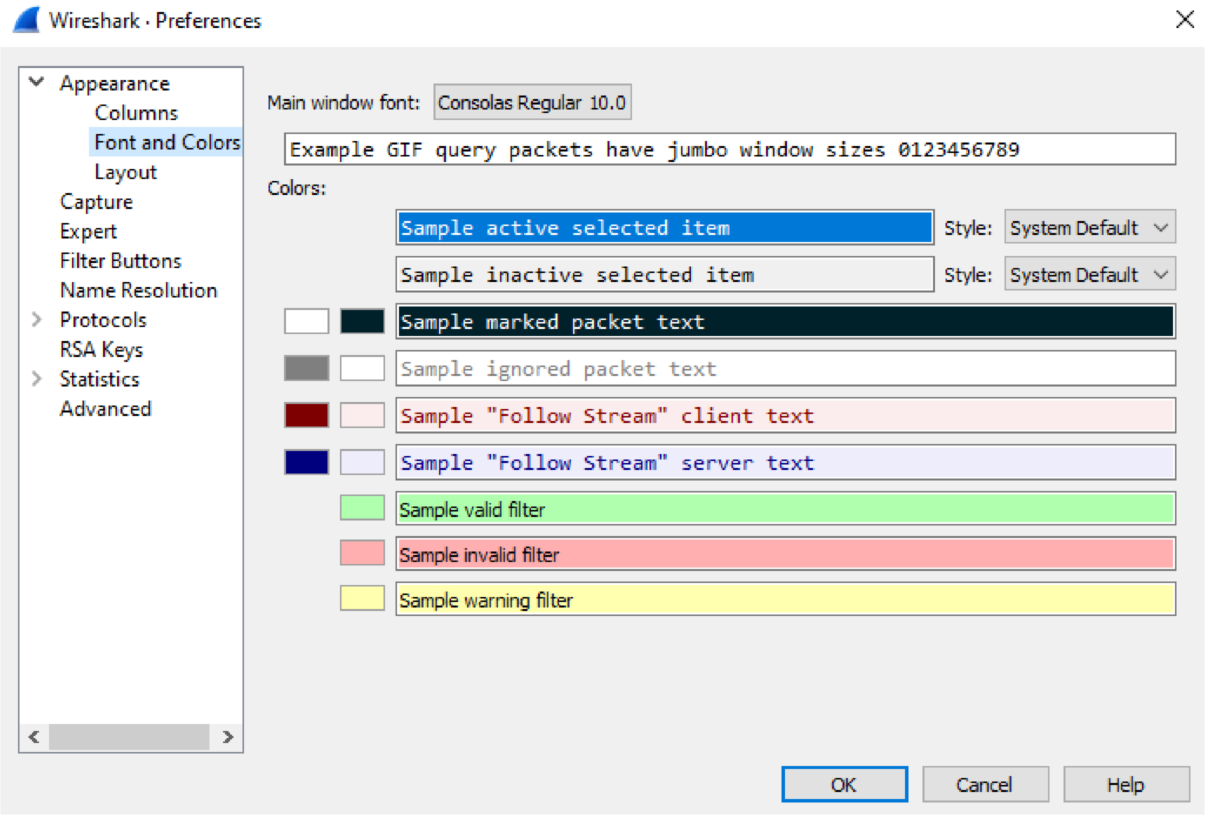




```
No.   Time  Source      Destination  Protocol  IP Main ICMP     IP Nested ICMP
  795 0.0 96.108.5.1…  10.0.0.75    ICMP      0xc379 (50041)   0x2455 (9301)
  803 0.0 96.108.5.1…  10.0.0.75    ICMP      0xc37a (50042)   0x2456 (9302)
```



Displayed	Title	Type	Fields	Field Occurrence
☑	No.	Number		
☑	Time	Time (format as specified)		
☑	Source	Source address		
☑	Destination	Destination address		
☑	Protocol	Protocol		
☐	Length	Packet length (bytes)		
☐	Info	Information		



Main window font: Consolas Regular 10.0

```
Example GIF query packets have jumbo window sizes 0123456789
```

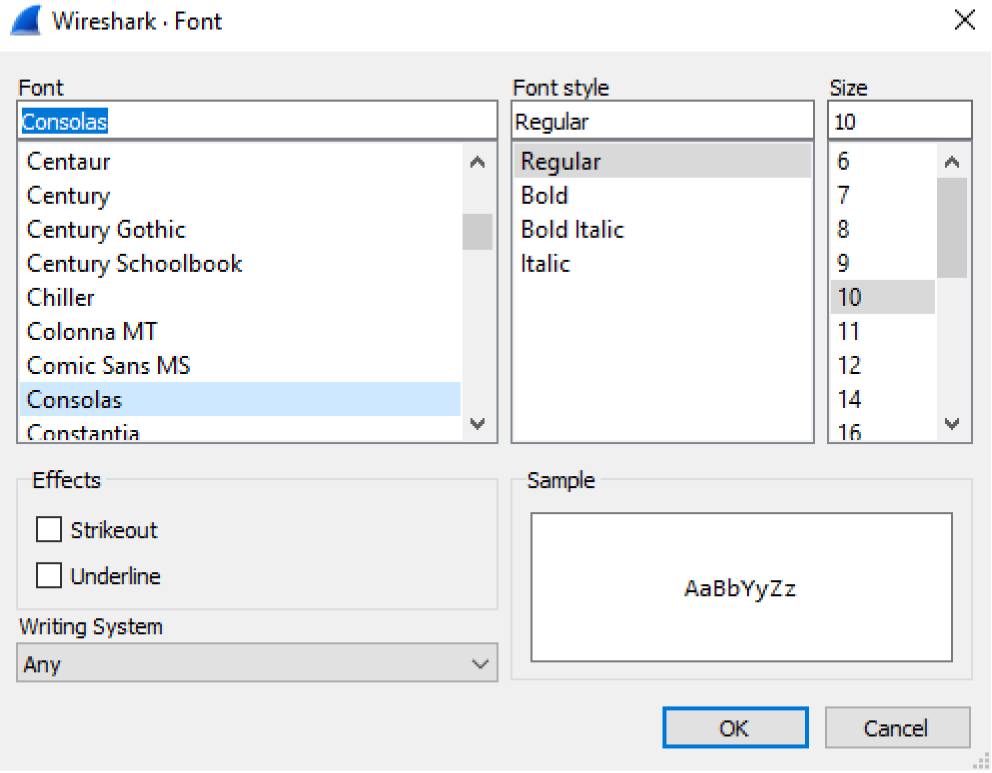
Colors:

```
Sample active selected item              Style: System Default
Sample inactive selected item            Style: System Default
Sample marked packet text
Sample ignored packet text
Sample "Follow Stream" client text
Sample "Follow Stream" server text
```

Sample valid filter

Sample invalid filter

Sample warning filter



Font: Consolas

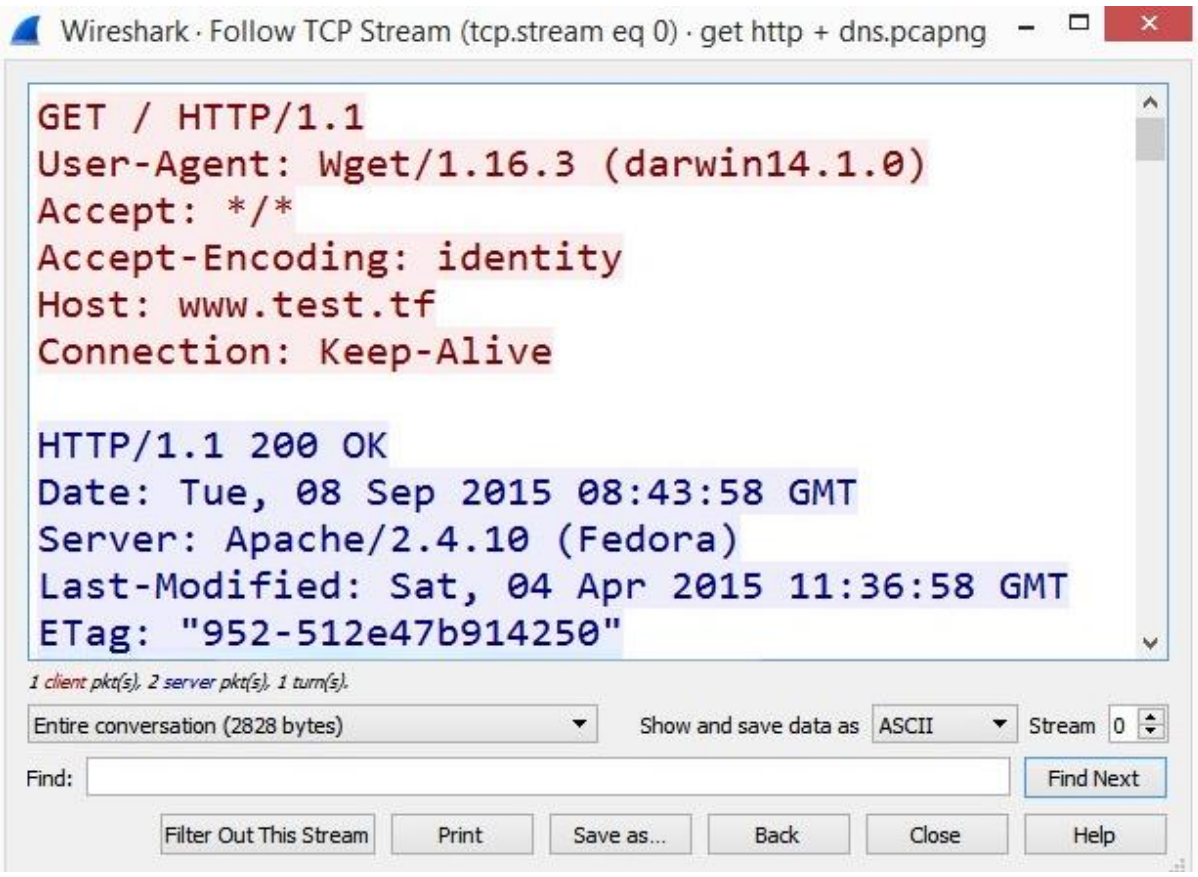
Font style: Regular

Size: 10

□ Strikeout

□ Underline

Writing System: Any

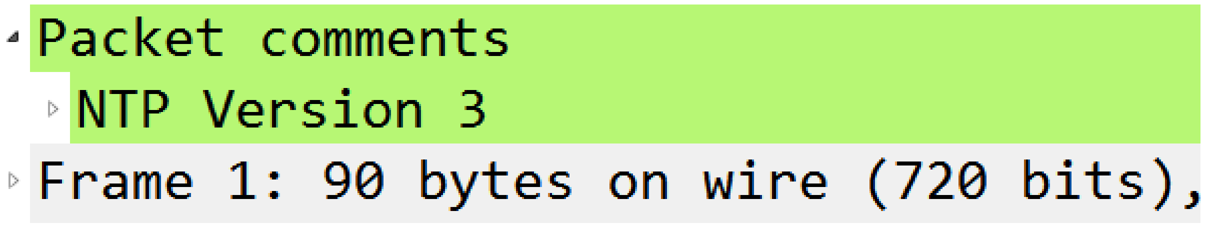

Wireshark · Follow TCP Stream (tcp.stream eq 0) · get http + dns.pcapng
Find Next
Filter Out This Stream
Print
Save as…
Back
Close
Help

```
GET / HTTP/1.1
User-Agent: Wget/1.16.3 (darwin14.1.0)
Accept: */*
Accept-Encoding: identity
Host: www.test.tf
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Tue, 08 Sep 2015 08:43:58 GMT
Server: Apache/2.4.10 (Fedora)
Last-Modified: Sat, 04 Apr 2015 11:36:58 GMT
ETag: "952-512e47b914250"
```

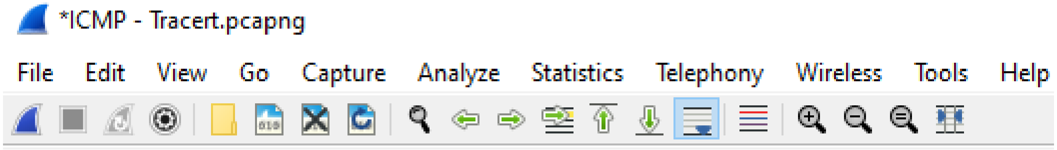
1 client pkt(s), 2 server pkt(s), 1 turn(s).

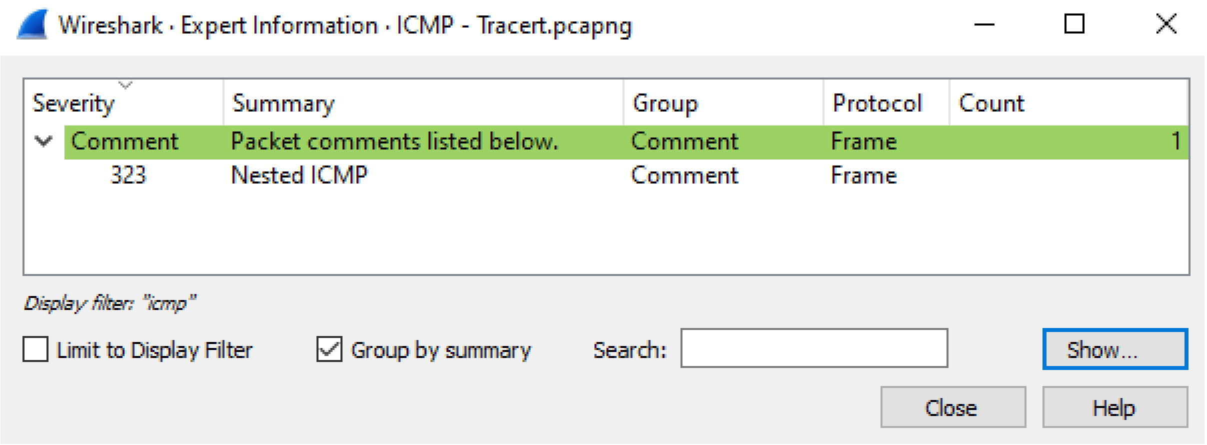
Entire conversation (2828 bytes) Show and save data as ASCII Stream 0

Find:



```
Packet comments
  NTP Version 3
Frame 1: 90 bytes on wire (720 bits),
```



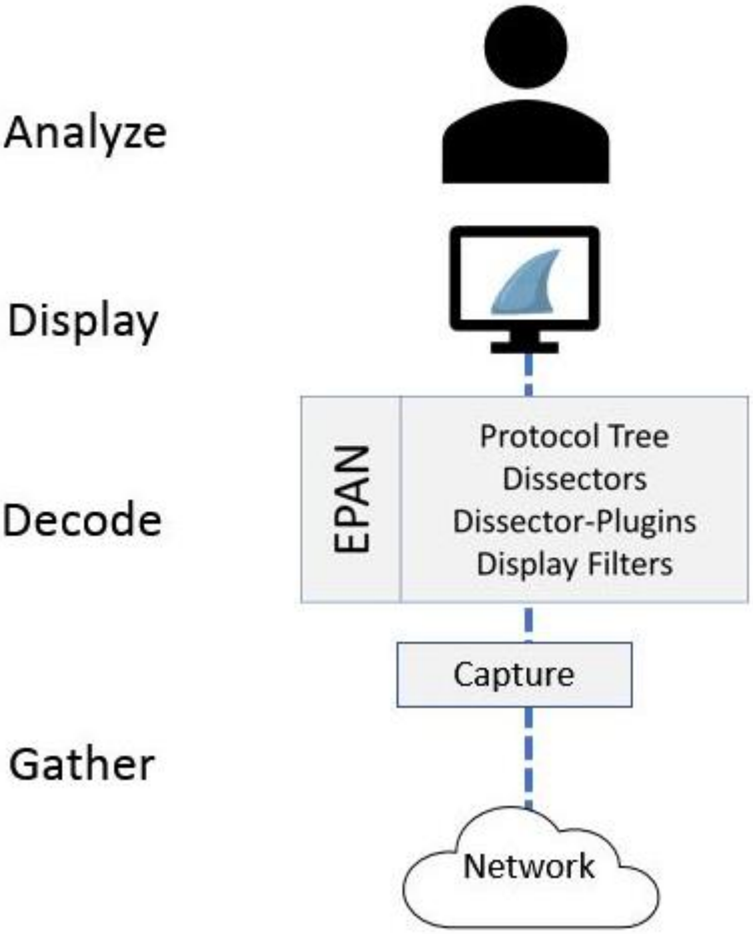


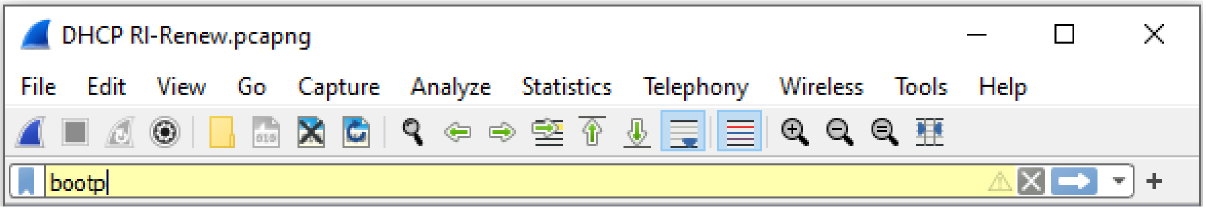
Severity	Summary	Group	Protocol	Count
Comment	Packet comments listed below.	Comment	Frame	1
323	Nested ICMP	Comment	Frame	

Display filter: "icmp"

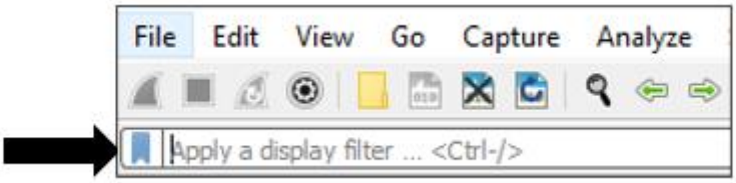
☐ Limit to Display Filter ☑ Group by summary Search:

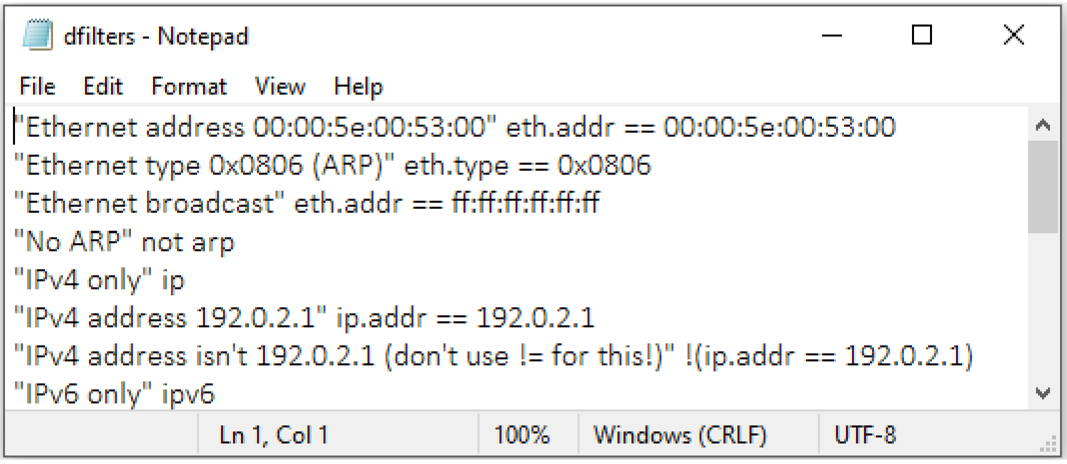
Chapter 7: Using Display and Capture Filters



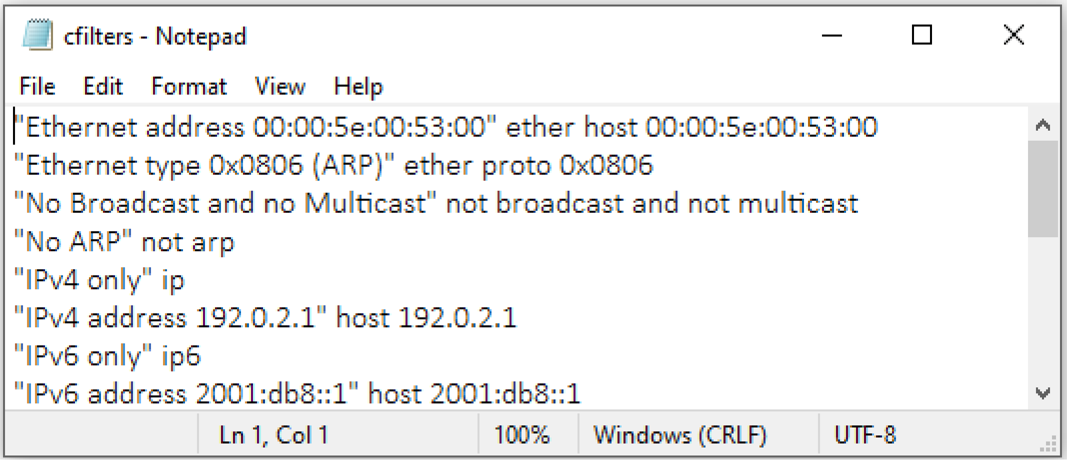


bootp

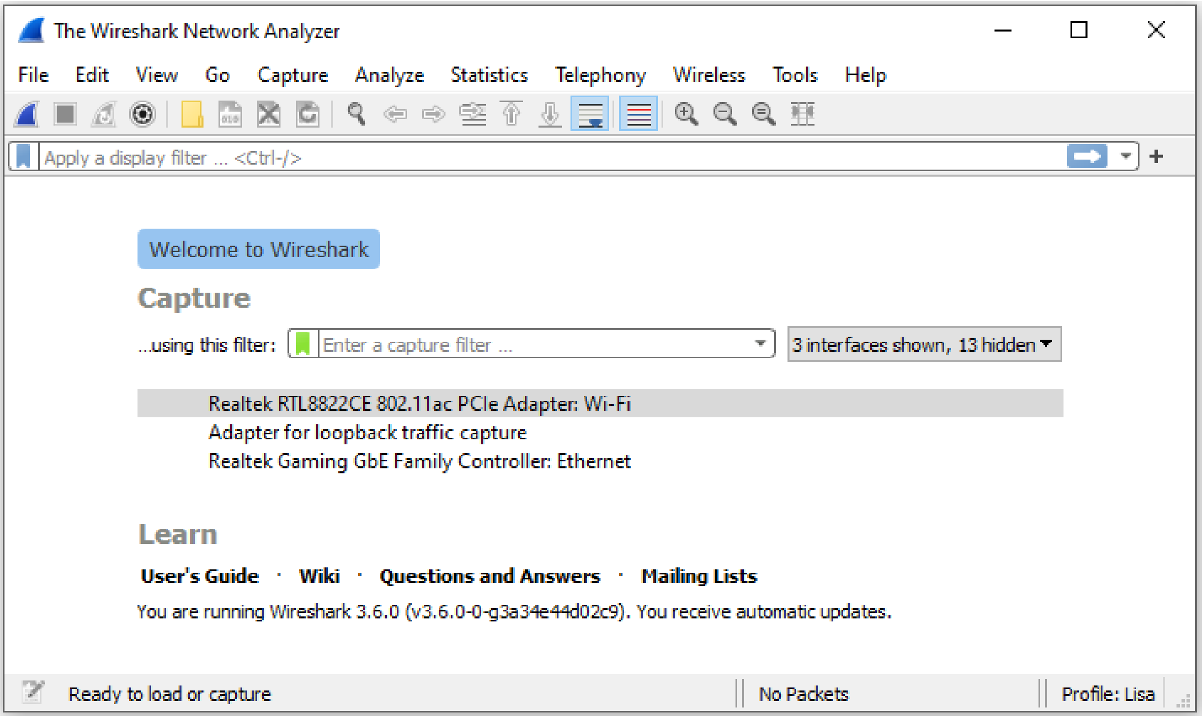




```
"Ethernet address 00:00:5e:00:53:00" eth.addr == 00:00:5e:00:53:00
"Ethernet type 0x0806 (ARP)" eth.type == 0x0806
"Ethernet broadcast" eth.addr == ff:ff:ff:ff:ff:ff
"No ARP" not arp
"IPv4 only" ip
"IPv4 address 192.0.2.1" ip.addr == 192.0.2.1
"IPv4 address isn't 192.0.2.1 (don't use != for this!)" !(ip.addr == 192.0.2.1)
"IPv6 only" ipv6
```

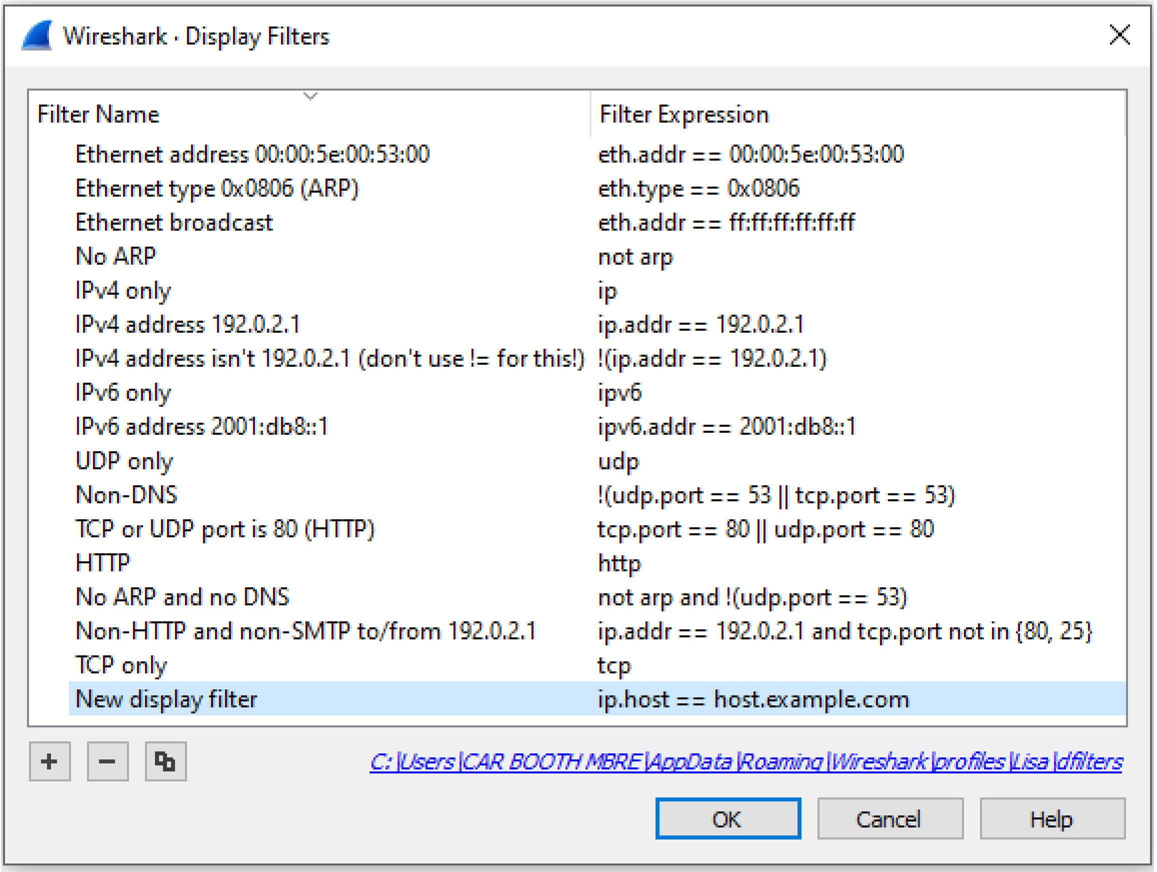


```
"Ethernet address 00:00:5e:00:53:00" ether host 00:00:5e:00:53:00
"Ethernet type 0x0806 (ARP)" ether proto 0x0806
"No Broadcast and no Multicast" not broadcast and not multicast
"No ARP" not arp
"IPv4 only" ip
"IPv4 address 192.0.2.1" host 192.0.2.1
"IPv6 only" ip6
"IPv6 address 2001:db8::1" host 2001:db8::1
```

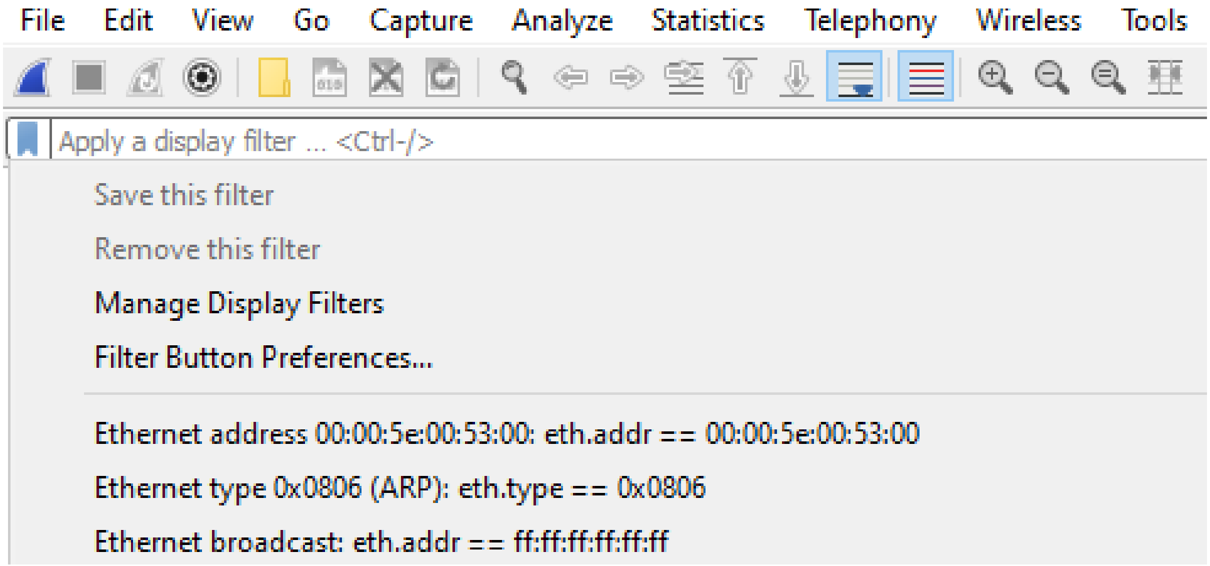

The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...
3 interfaces shown, 13 hidden
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
Ready to load or capture
No Packets
Profile: Lisa

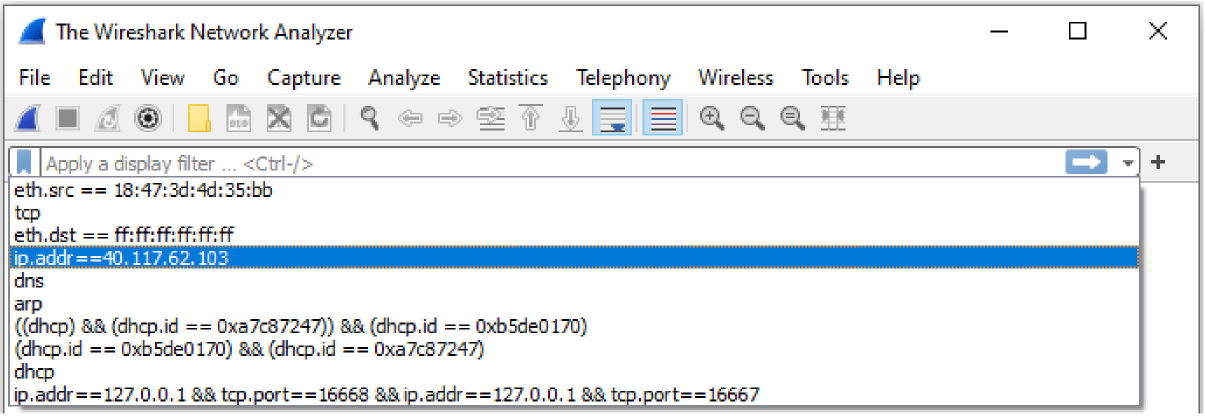
Realtek RTL8822CE 802.11ac PCIe Adapter: Wi-Fi
Adapter for loopback traffic capture
Realtek Gaming GbE Family Controller: Ethernet

You are running Wireshark 3.6.0 (v3.6.0-0-g3a34e44d02c9). You receive automatic updates.

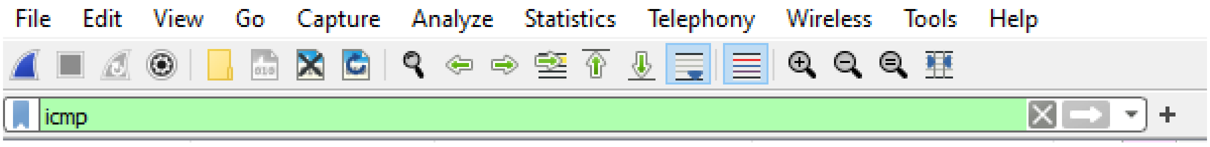

Wireshark · Display Filters
+
−
C:\Users\CAR BOOTH MBRE\AppData\Roaming\Wireshark\profiles\Lisa\dfilters
OK
Cancel
Help

Filter Name	Filter Expression
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
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 tcp.port not in {80, 25}
TCP only	tcp
New display filter	ip.host == host.example.com

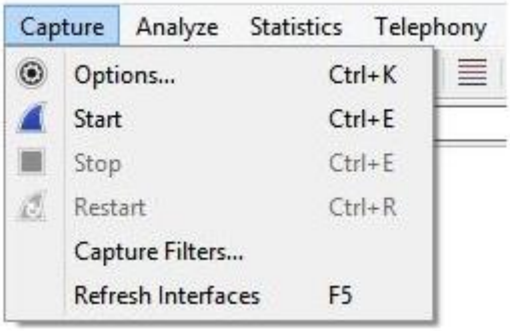

File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Wireless
Tools
Apply a display filter ... <Ctrl-/>
Save this filter
Remove this filter
Manage Display Filters
Filter Button Preferences...
Ethernet address 00:00:5e:00:53:00: eth.addr == 00:00:5e:00:53:00
Ethernet type 0x0806 (ARP): eth.type == 0x0806
Ethernet broadcast: eth.addr == ff:ff:ff:ff:ff:ff

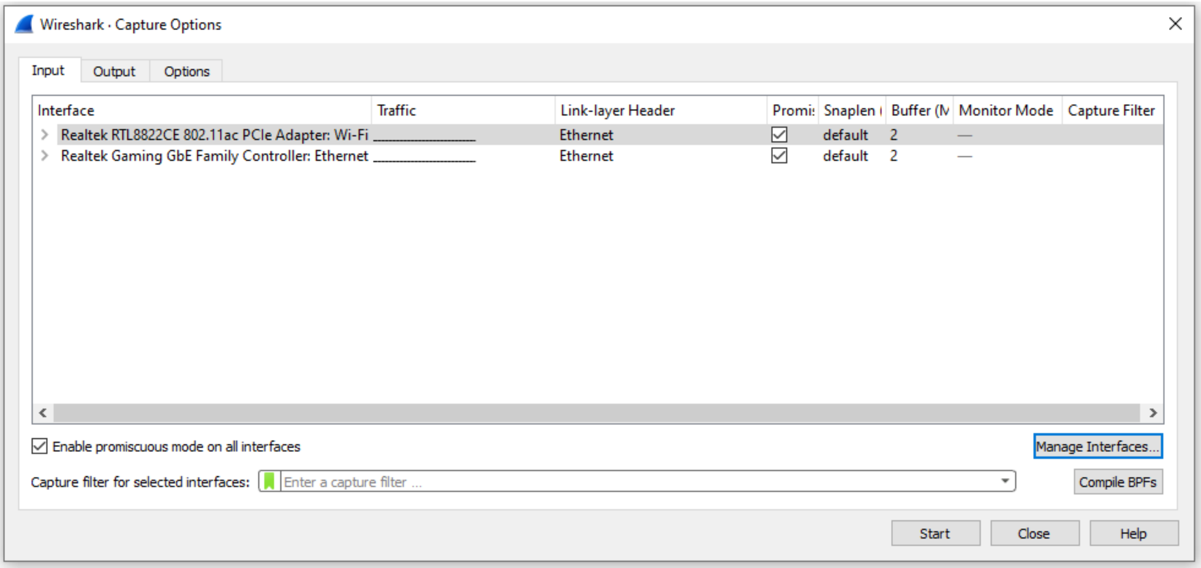

The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
eth.src == 18:47:3d:4d:35:bb
tcp
eth.dst == ff:ff:ff:ff:ff:ff
ip.addr==40.117.62.103
dns
arp
((dhcp) && (dhcp.id == 0xa7c87247)) && (dhcp.id == 0xb5de0170)
(dhcp.id == 0xb5de0170) && (dhcp.id == 0xa7c87247)
dhcp
ip.addr==127.0.0.1 && tcp.port==16668 && ip.addr==127.0.0.1 && tcp.port==16667
```


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
icmp
```

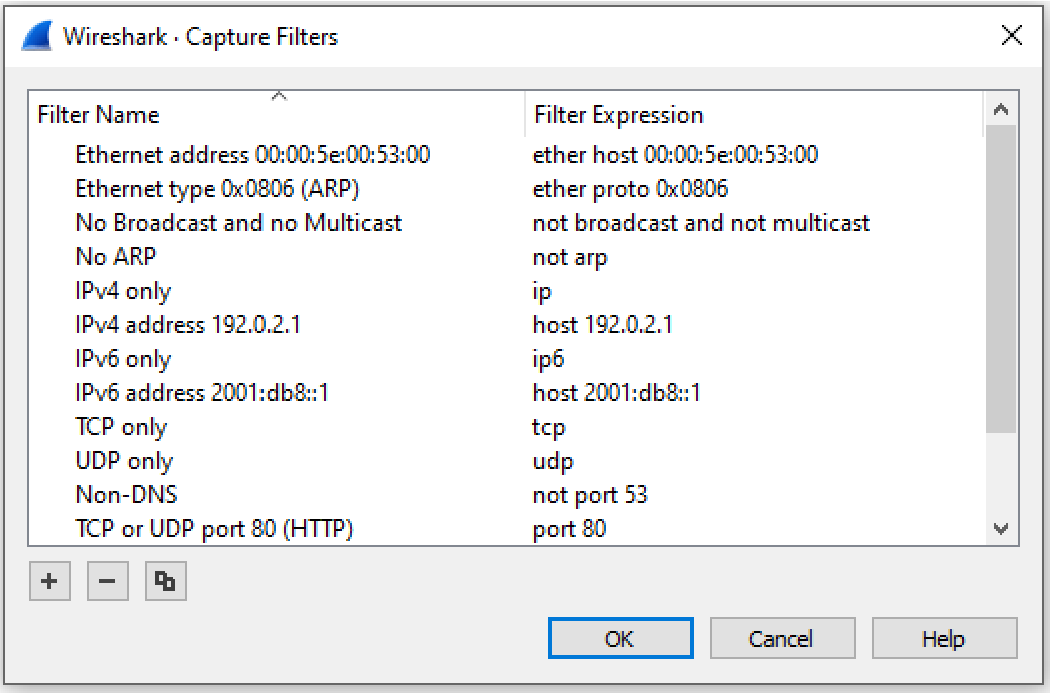




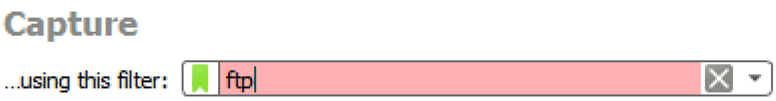
Interface	Traffic	Link-layer Header	Promi:	Snaplen (	Buffer (M	Monitor Mode	Capture Filter
› Realtek RTL8822CE 802.11ac PCIe Adapter: Wi-Fi		Ethernet	☑	default	2	—	
› Realtek Gaming GbE Family Controller: Ethernet		Ethernet	☑	default	2	—	

☑ Enable promiscuous mode on all interfaces

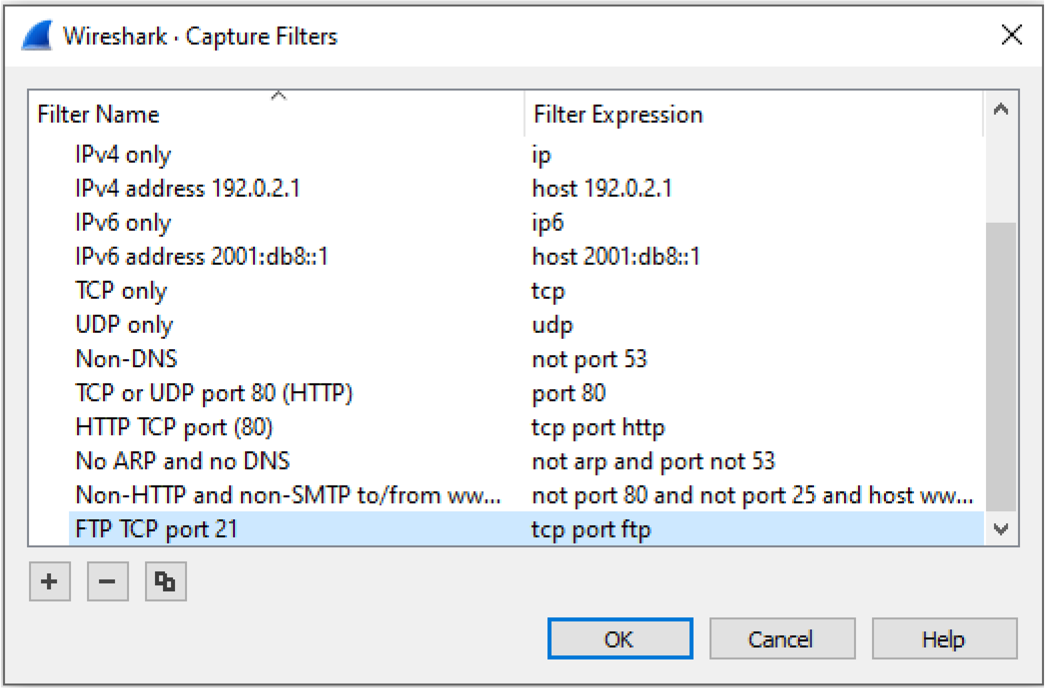
Capture filter for selected interfaces: Enter a capture filter ...



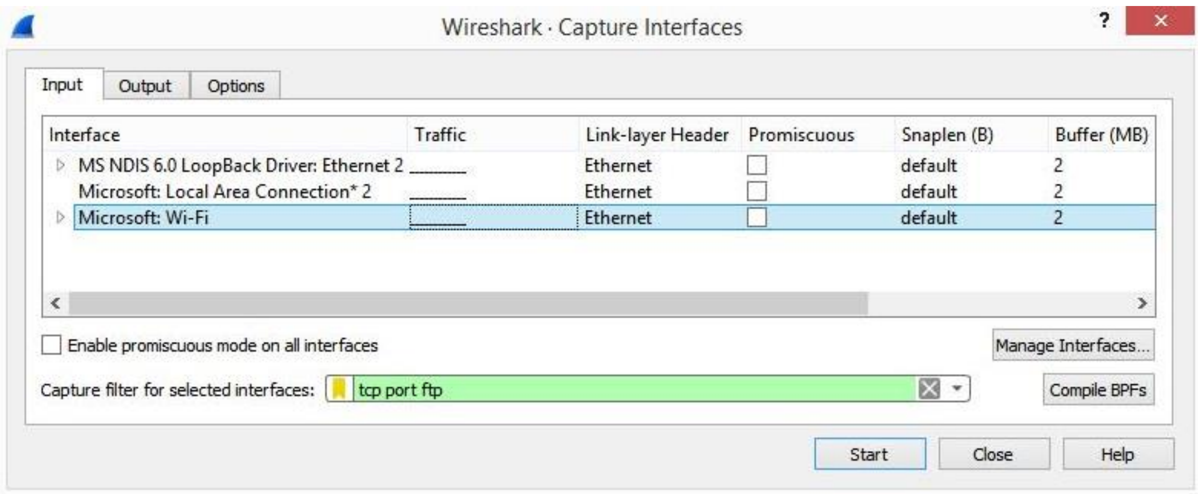
Filter Name	Filter Expression
Ethernet address 00:00:5e:00:53:00	ether host 00:00:5e:00:53:00
Ethernet type 0x0806 (ARP)	ether proto 0x0806
No Broadcast and no Multicast	not broadcast and not multicast
No ARP	not arp
IPv4 only	ip
IPv4 address 192.0.2.1	host 192.0.2.1
IPv6 only	ip6
IPv6 address 2001:db8::1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



...using this filter: ftp



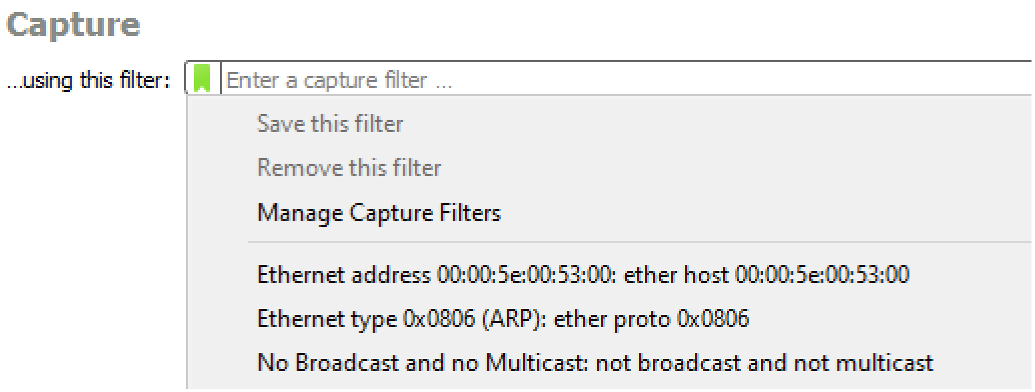
Filter Name	Filter Expression
IPv4 only	ip
IPv4 address 192.0.2.1	host 192.0.2.1
IPv6 only	ip6
IPv6 address 2001:db8::1	host 2001:db8::1
TCP only	tcp
UDP only	udp
Non-DNS	not port 53
TCP or UDP port 80 (HTTP)	port 80
HTTP TCP port (80)	tcp port http
No ARP and no DNS	not arp and port not 53
Non-HTTP and non-SMTP to/from ww...	not port 80 and not port 25 and host ww...
FTP TCP port 21	tcp port ftp



Interface	Traffic	Link-layer Header	Promiscuous	Snaplen (B)	Buffer (MB)
▷ MS NDIS 6.0 LoopBack Driver: Ethernet 2		Ethernet	□	default	2
Microsoft: Local Area Connection* 2		Ethernet	□	default	2
▷ Microsoft: Wi-Fi		Ethernet	□	default	2

□ Enable promiscuous mode on all interfaces

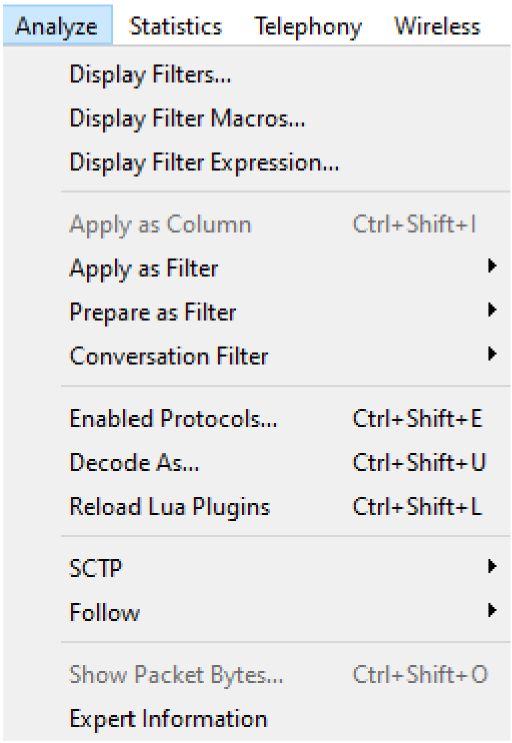
Capture filter for selected interfaces: tcp port ftp

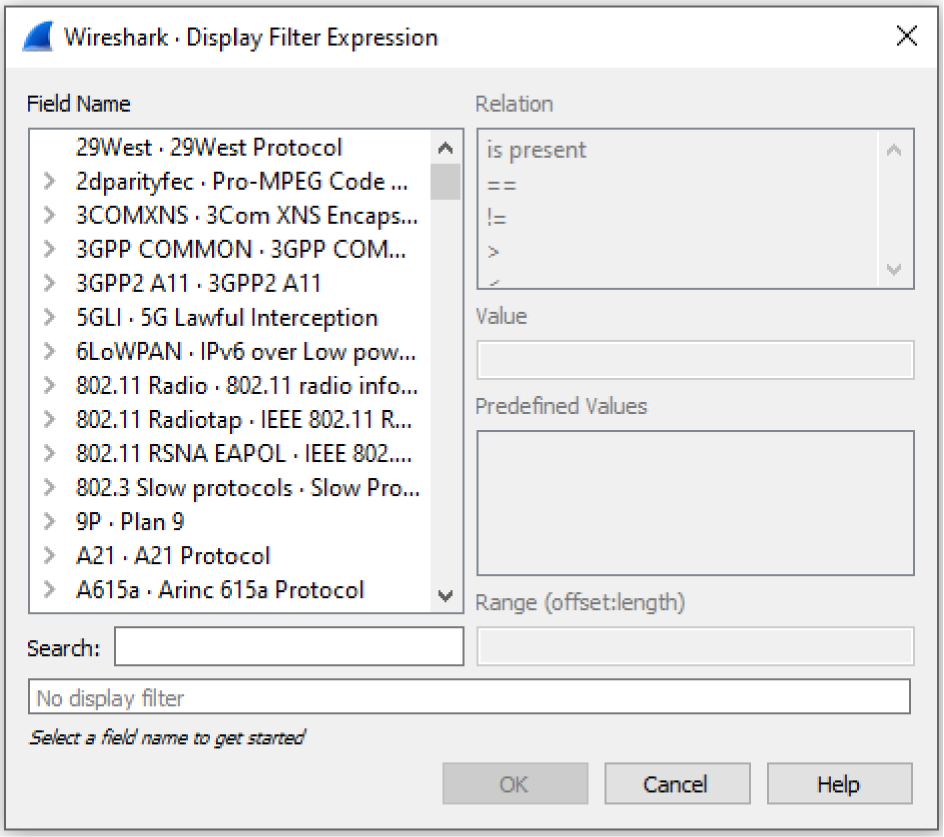


Ethernet address 00:00:5e:00:53:00: ether host 00:00:5e:00:53:00

Ethernet type 0x0806 (ARP): ether proto 0x0806

No Broadcast and no Multicast: not broadcast and not multicast

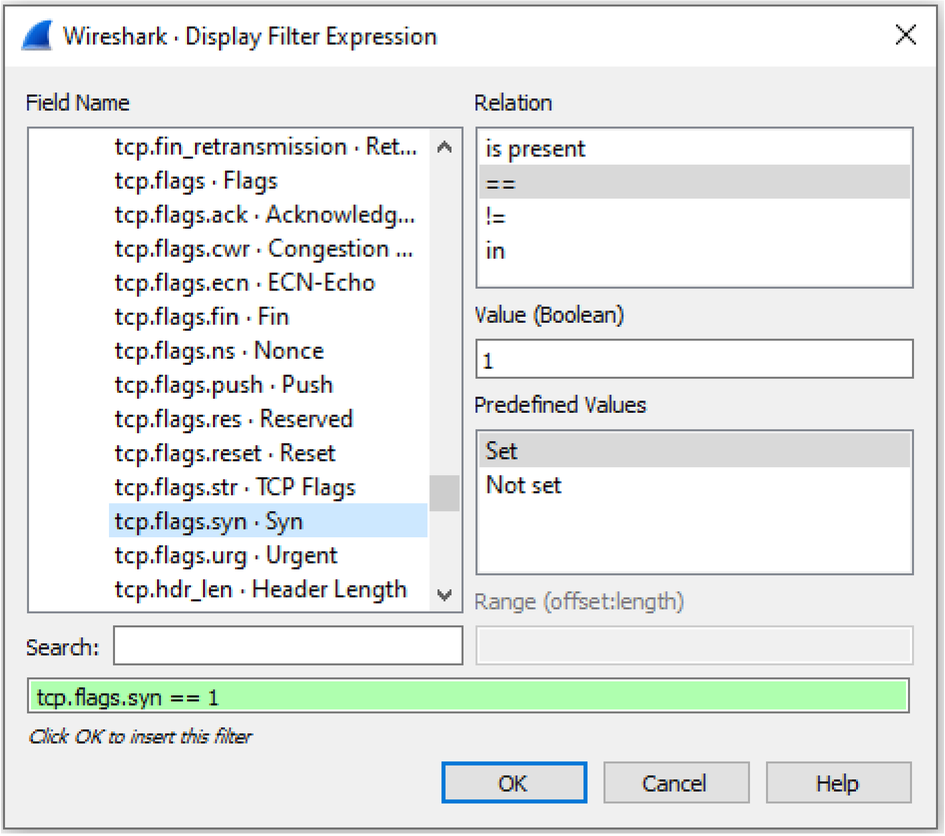

Analyze
Statistics
Telephony
Wireless
Display Filters...
Display Filter Macros...
Display Filter Expression...
Apply as Column Ctrl+Shift+I
Apply as Filter ▸
Prepare as Filter ▸
Conversation Filter ▸
Enabled Protocols... Ctrl+Shift+E
Decode As... Ctrl+Shift+U
Reload Lua Plugins Ctrl+Shift+L
SCTP ▸
Follow ▸
Show Packet Bytes... Ctrl+Shift+O
Expert Information



Wireshark · Display Filter Expression
Field Name
29West · 29West Protocol
2dparityfec · Pro-MPEG Code ...
3COMXNS · 3Com XNS Encaps...
3GPP COMMON · 3GPP COM...
3GPP2 A11 · 3GPP2 A11
5GLI · 5G Lawful Interception
6LoWPAN · IPv6 over Low pow...
802.11 Radio · 802.11 radio info...
802.11 Radiotap · IEEE 802.11 R...
802.11 RSNA EAPOL · IEEE 802....
802.3 Slow protocols · Slow Pro...
9P · Plan 9
A21 · A21 Protocol
A615a · Arinc 615a Protocol
Relation
is present
==
!=
>
Value
Predefined Values
Range (offset:length)
Search:
OK
Cancel
Help

No display filter

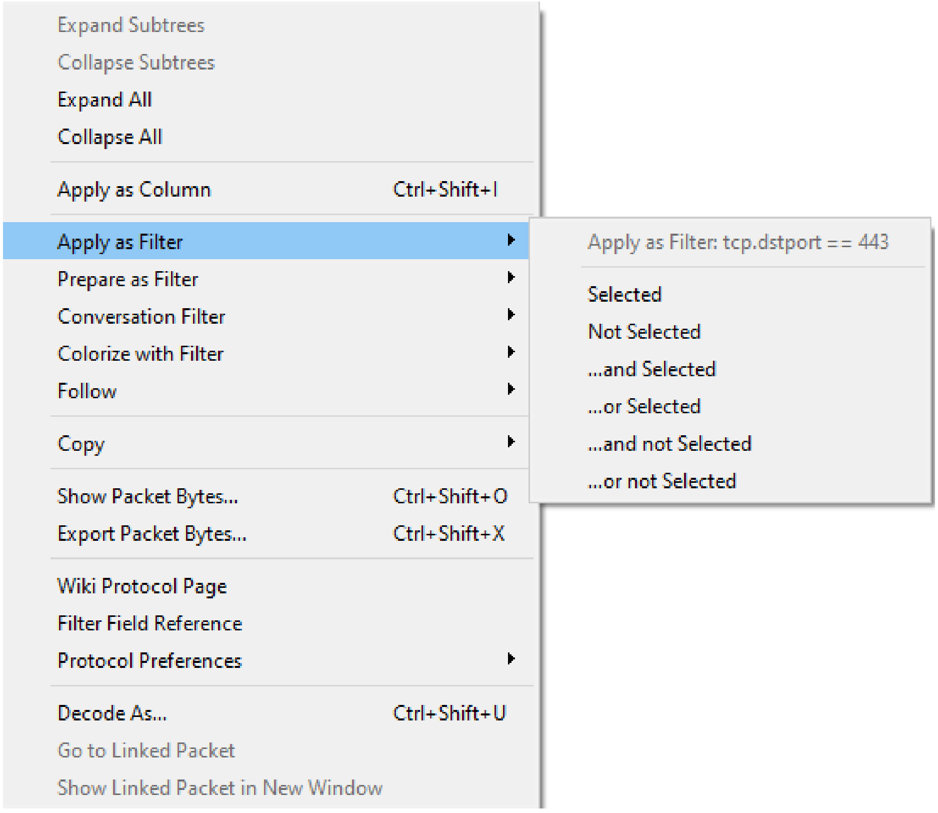
Select a field name to get started

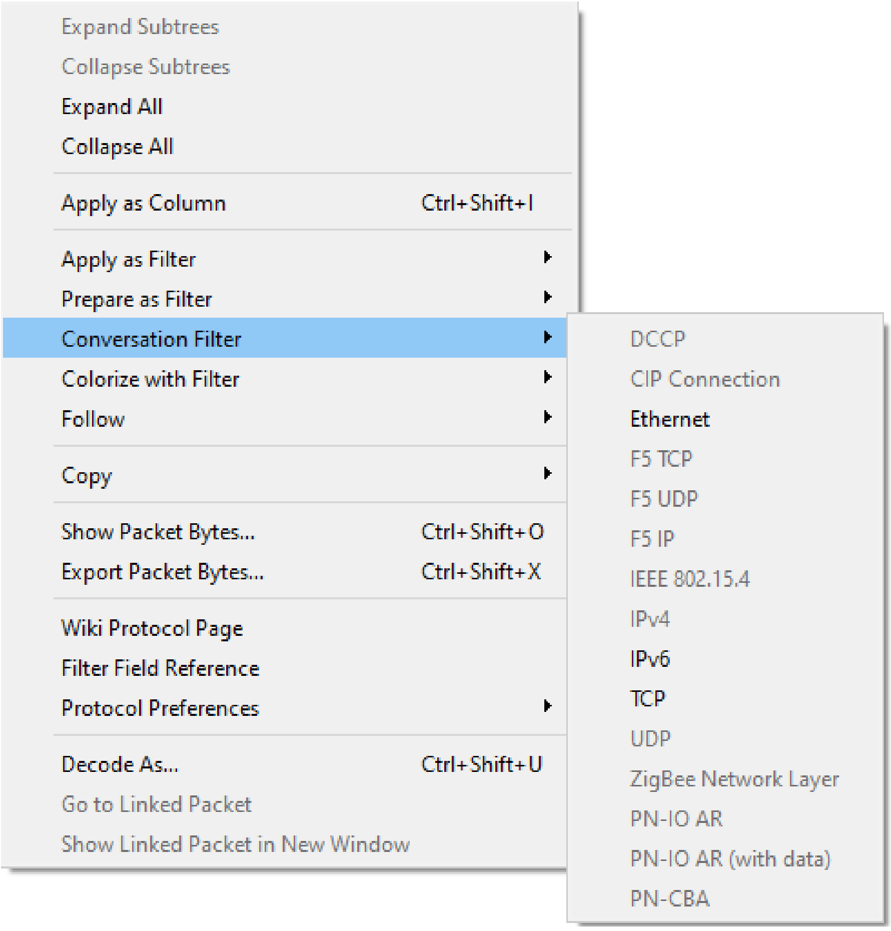


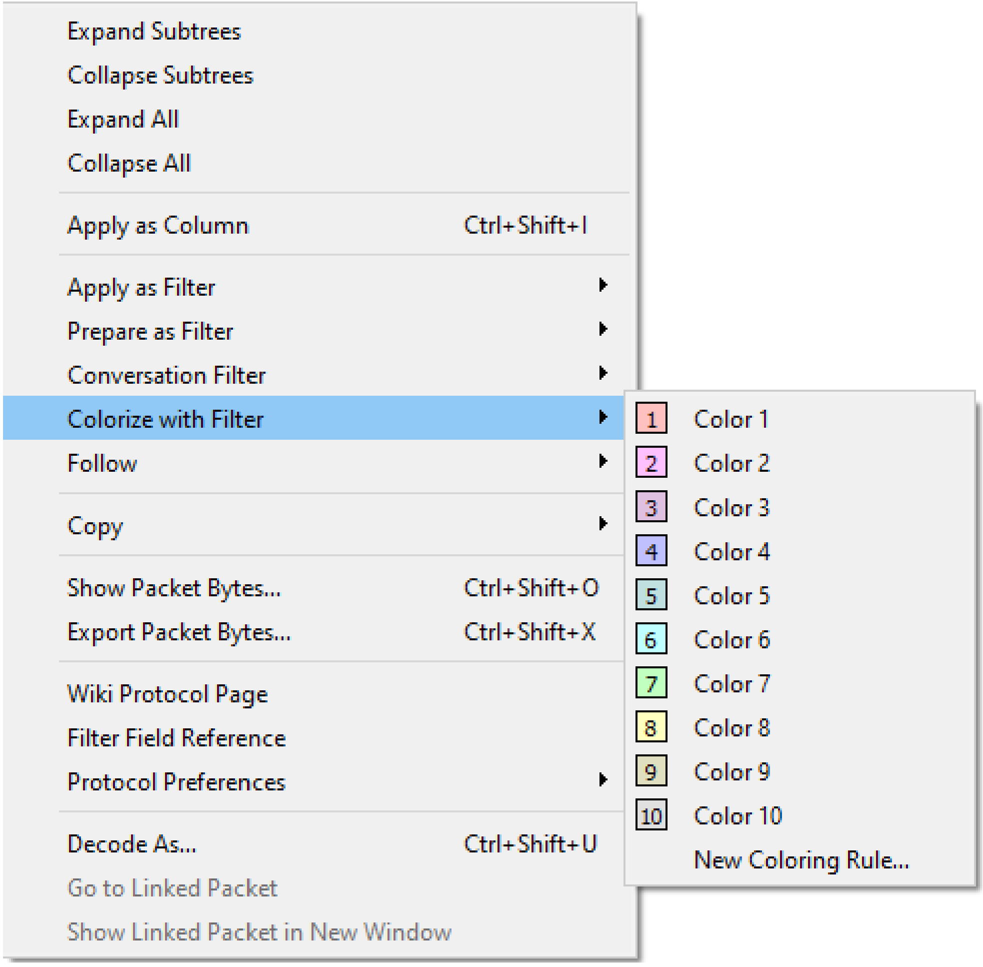
Value (Boolean): 1

tcp.flags.syn == 1

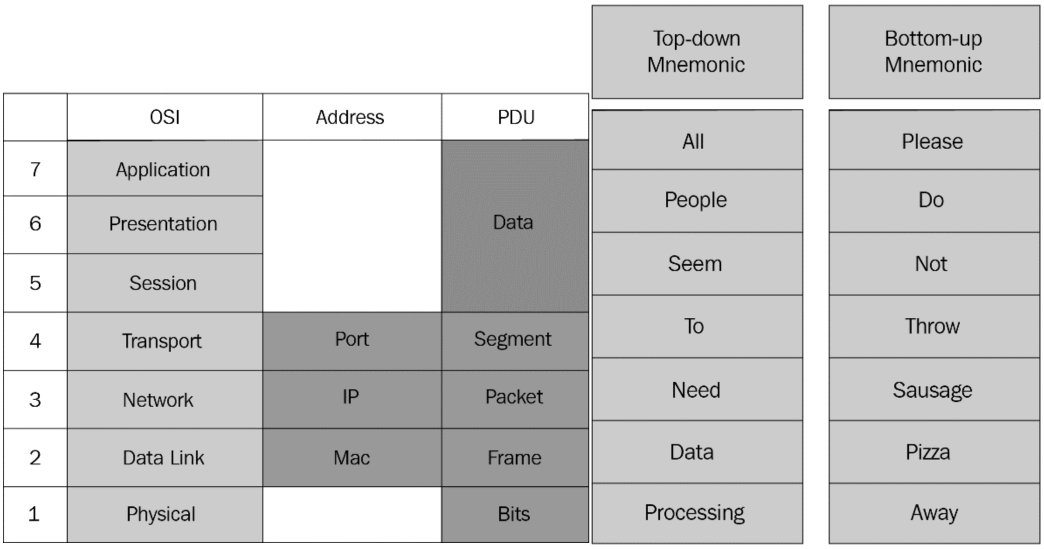
Click OK to insert this filter


Expand Subtrees
Collapse Subtrees
Expand All
Collapse All
Apply as Column Ctrl+Shift+I
Apply as Filter
Prepare as Filter
Conversation Filter
Colorize with Filter
Follow
Copy
Show Packet Bytes... Ctrl+Shift+O
Export Packet Bytes... Ctrl+Shift+X
Wiki Protocol Page
Filter Field Reference
Protocol Preferences
Decode As... Ctrl+Shift+U
Go to Linked Packet
Show Linked Packet in New Window
Apply as Filter: tcp.dstport == 443
Selected
Not Selected
...and Selected
...or Selected
...and not Selected
...or not Selected

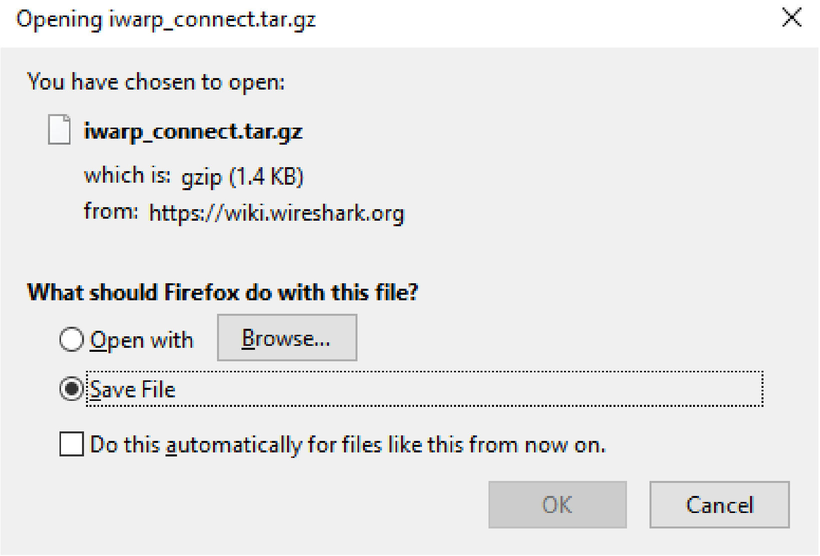

Expand Subtrees
Collapse Subtrees
Expand All
Collapse All
Apply as Column Ctrl+Shift+I
Apply as Filter
Prepare as Filter
Conversation Filter
Colorize with Filter
Follow
Copy
Show Packet Bytes... Ctrl+Shift+O
Export Packet Bytes... Ctrl+Shift+X
Wiki Protocol Page
Filter Field Reference
Protocol Preferences
Decode As... Ctrl+Shift+U
Go to Linked Packet
Show Linked Packet in New Window
DCCP
CIP Connection
Ethernet
F5 TCP
F5 UDP
F5 IP
IEEE 802.15.4
IPv4
IPv6
TCP
UDP
ZigBee Network Layer
PN-IO AR
PN-IO AR (with data)
PN-CBA


Expand Subtrees
Collapse Subtrees
Expand All
Collapse All
Apply as Column Ctrl+Shift+I
Apply as Filter
Prepare as Filter
Conversation Filter
Colorize with Filter
Follow
Copy
Show Packet Bytes... Ctrl+Shift+O
Export Packet Bytes... Ctrl+Shift+X
Wiki Protocol Page
Filter Field Reference
Protocol Preferences
Decode As... Ctrl+Shift+U
Go to Linked Packet
Show Linked Packet in New Window
1 Color 1
2 Color 2
3 Color 3
4 Color 4
5 Color 5
6 Color 6
7 Color 7
8 Color 8
9 Color 9
10 Color 10
New Coloring Rule...

Chapter 8: Outlining the OSI Model



	OSI	Address	PDU	Top-down Mnemonic	Bottom-up Mnemonic
7	Application		Data	All	Please
6	Presentation			People	Do
5	Session			Seem	Not
4	Transport	Port	Segment	To	Throw
3	Network	IP	Packet	Need	Sausage
2	Data Link	Mac	Frame	Data	Pizza
1	Physical		Bits	Processing	Away



Opening iwarp_connect.tar.gz

You have chosen to open:

iwarp_connect.tar.gz

which is: gzip (1.4 KB)

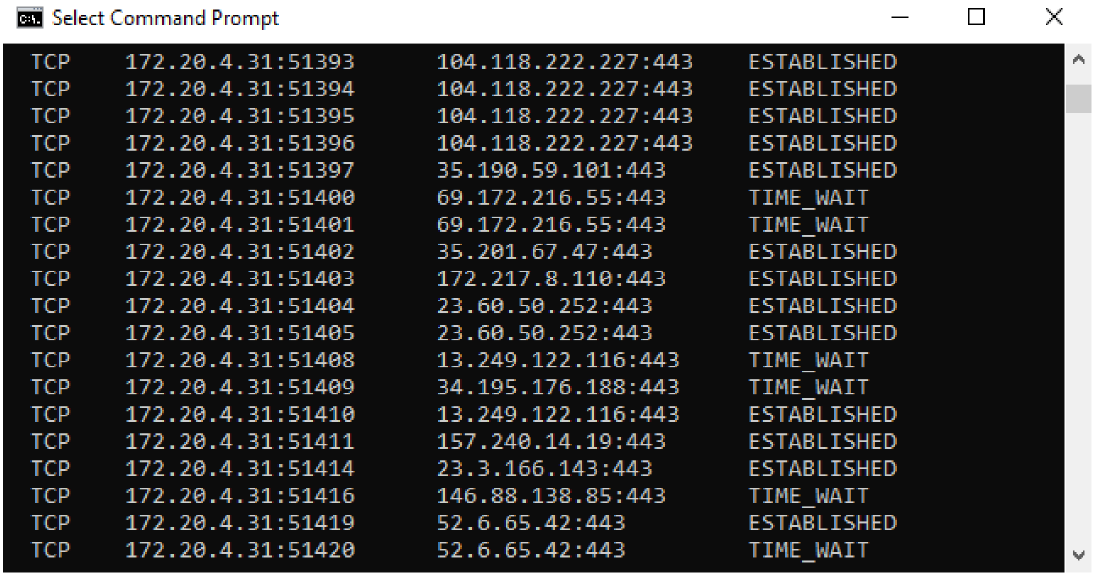
from: https://wiki.wireshark.org

What should Firefox do with this file?

○ Open with [Browse...]

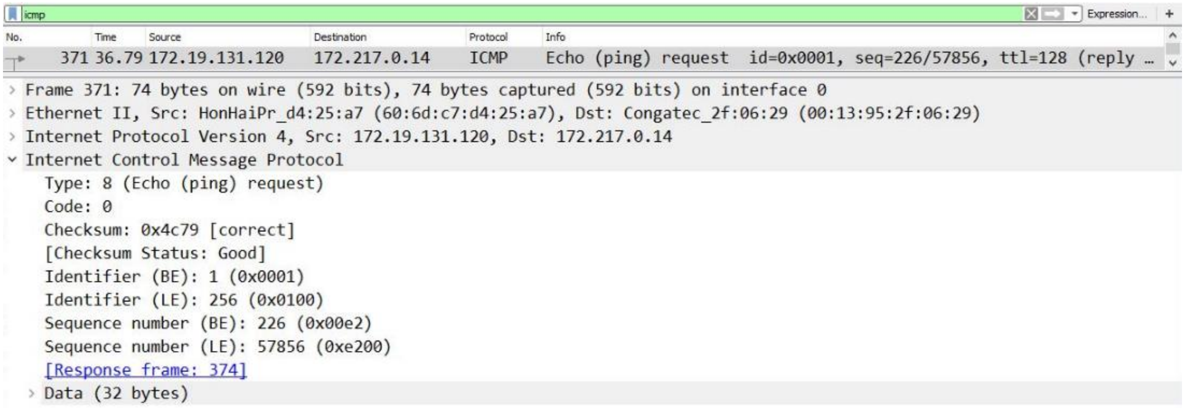
● Save File

□ Do this automatically for files like this from now on.

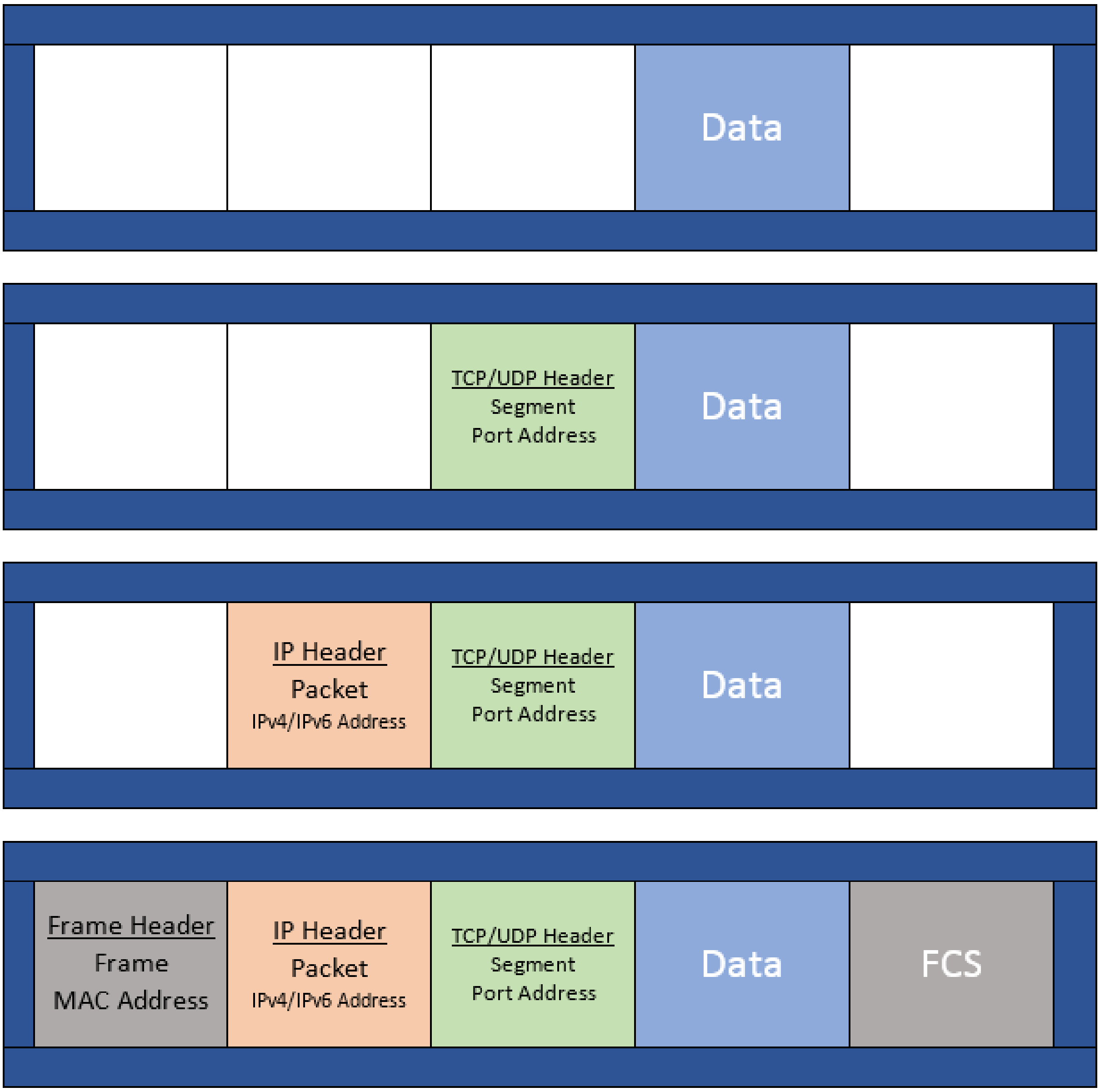


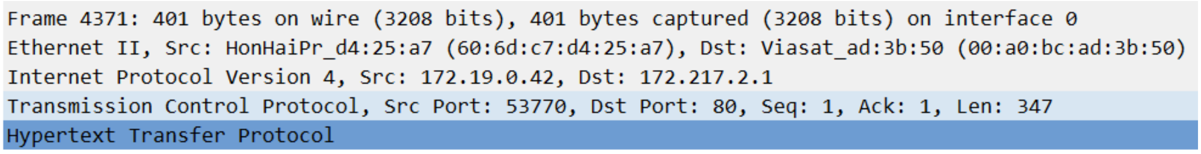
Select Command Prompt

```
TCP    172.20.4.31:51393      104.118.222.227:443    ESTABLISHED
TCP    172.20.4.31:51394      104.118.222.227:443    ESTABLISHED
TCP    172.20.4.31:51395      104.118.222.227:443    ESTABLISHED
TCP    172.20.4.31:51396      104.118.222.227:443    ESTABLISHED
TCP    172.20.4.31:51397      35.190.59.101:443      ESTABLISHED
TCP    172.20.4.31:51400      69.172.216.55:443      TIME_WAIT
TCP    172.20.4.31:51401      69.172.216.55:443      TIME_WAIT
TCP    172.20.4.31:51402      35.201.67.47:443       ESTABLISHED
TCP    172.20.4.31:51403      172.217.8.110:443      ESTABLISHED
TCP    172.20.4.31:51404      23.60.50.252:443       ESTABLISHED
TCP    172.20.4.31:51405      23.60.50.252:443       ESTABLISHED
TCP    172.20.4.31:51408      13.249.122.116:443     TIME_WAIT
TCP    172.20.4.31:51409      34.195.176.188:443     TIME_WAIT
TCP    172.20.4.31:51410      13.249.122.116:443     ESTABLISHED
TCP    172.20.4.31:51411      157.240.14.19:443      ESTABLISHED
TCP    172.20.4.31:51414      23.3.166.143:443       ESTABLISHED
TCP    172.20.4.31:51416      146.88.138.85:443      TIME_WAIT
TCP    172.20.4.31:51419      52.6.65.42:443         ESTABLISHED
TCP    172.20.4.31:51420      52.6.65.42:443         TIME_WAIT
```

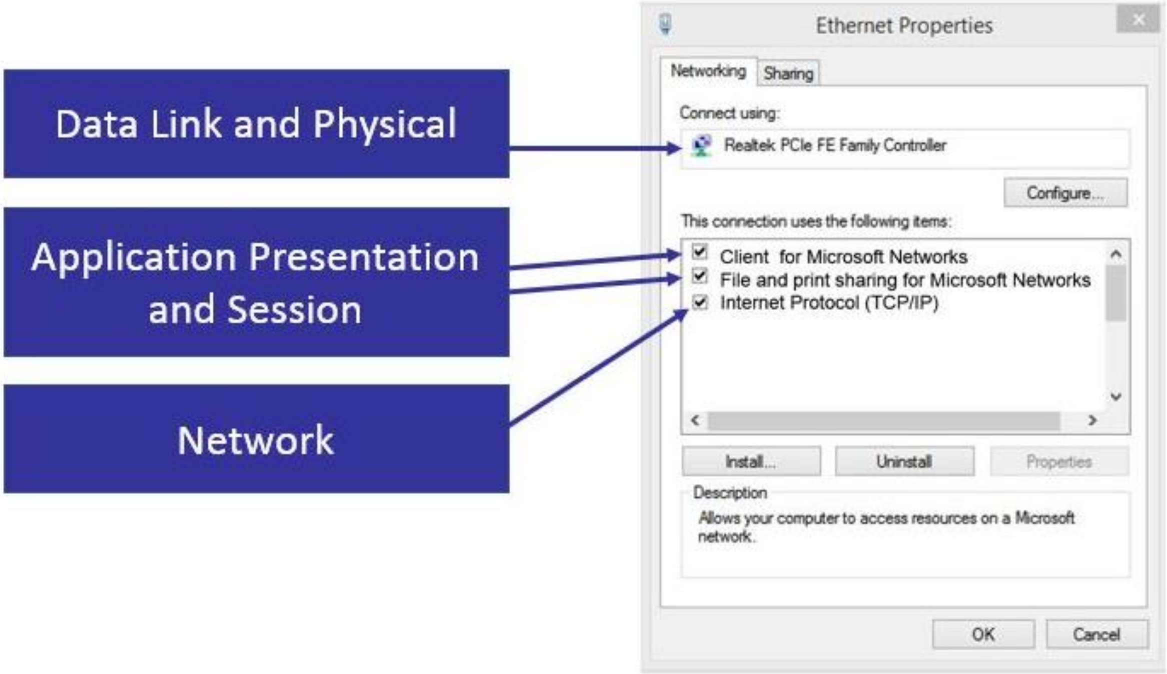


```
No.  Time   Source          Destination   Protocol  Info
 371 36.79  172.19.131.120  172.217.0.14  ICMP      Echo (ping) request  id=0x0001, seq=226/57856, ttl=128 (reply …
> Frame 371: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
> Ethernet II, Src: HonHaiPr_d4:25:a7 (60:6d:c7:d4:25:a7), Dst: Congatec_2f:06:29 (00:13:95:2f:06:29)
> Internet Protocol Version 4, Src: 172.19.131.120, Dst: 172.217.0.14
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4c79 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 226 (0x00e2)
    Sequence number (LE): 57856 (0xe200)
    [Response frame: 374]
  > Data (32 bytes)
```





```
Frame 4371: 401 bytes on wire (3208 bits), 401 bytes captured (3208 bits) on interface 0
Ethernet II, Src: HonHaiPr_d4:25:a7 (60:6d:c7:d4:25:a7), Dst: Viasat_ad:3b:50 (00:a0:bc:ad:3b:50)
Internet Protocol Version 4, Src: 172.19.0.42, Dst: 172.217.2.1
Transmission Control Protocol, Src Port: 53770, Dst Port: 80, Seq: 1, Ack: 1, Len: 347
Hypertext Transfer Protocol
```



Data Link and Physical

Application Presentation and Session

Network

Ethernet Properties

Connect using:

Realtek PCIe FE Family Controller

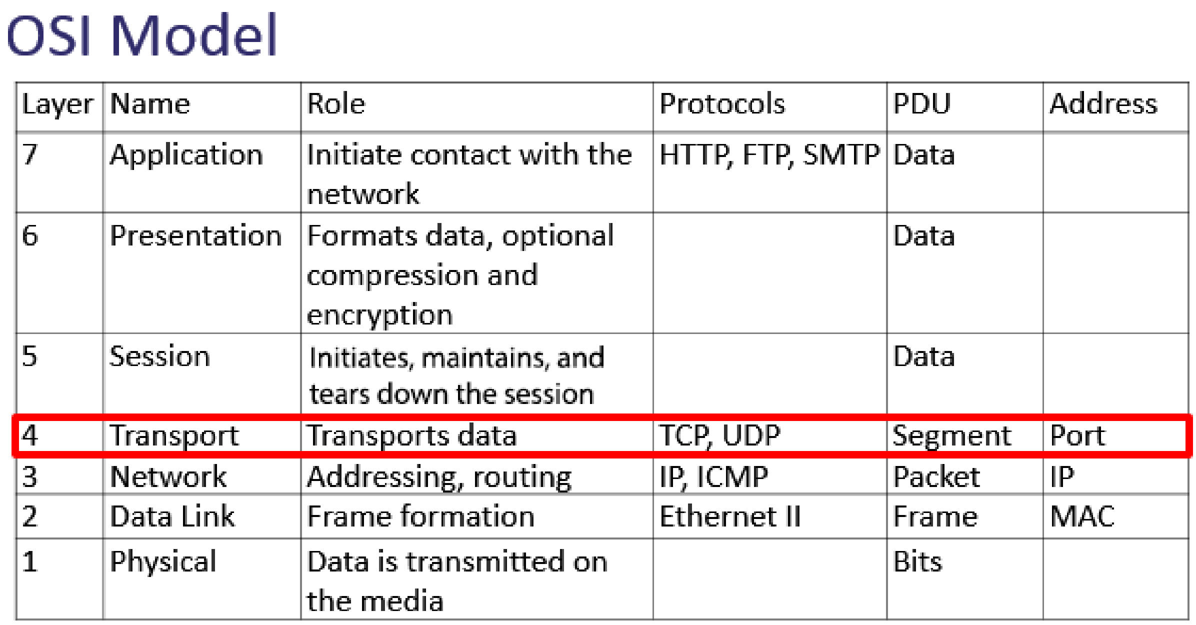
This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ File and print sharing for Microsoft Networks
- ☑ Internet Protocol (TCP/IP)

Description

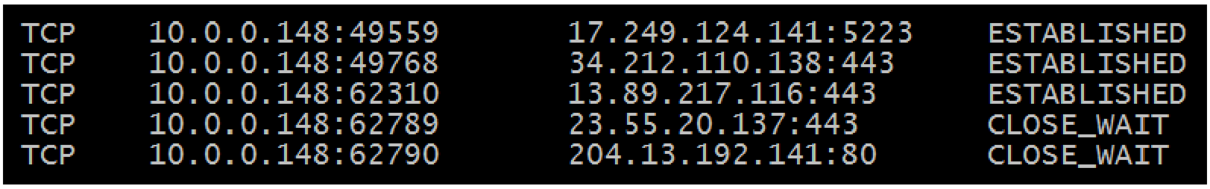
Allows your computer to access resources on a Microsoft network.

Chapter 9: Decoding TCP and UDP

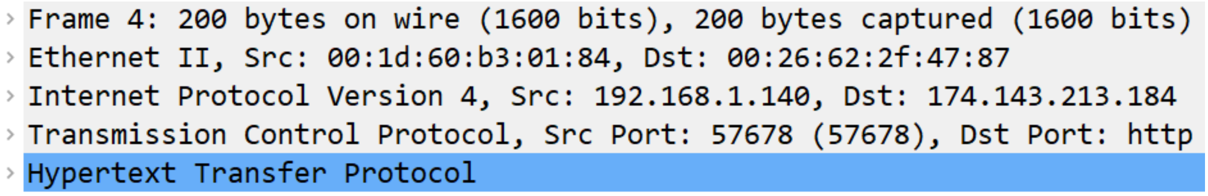


OSI Model

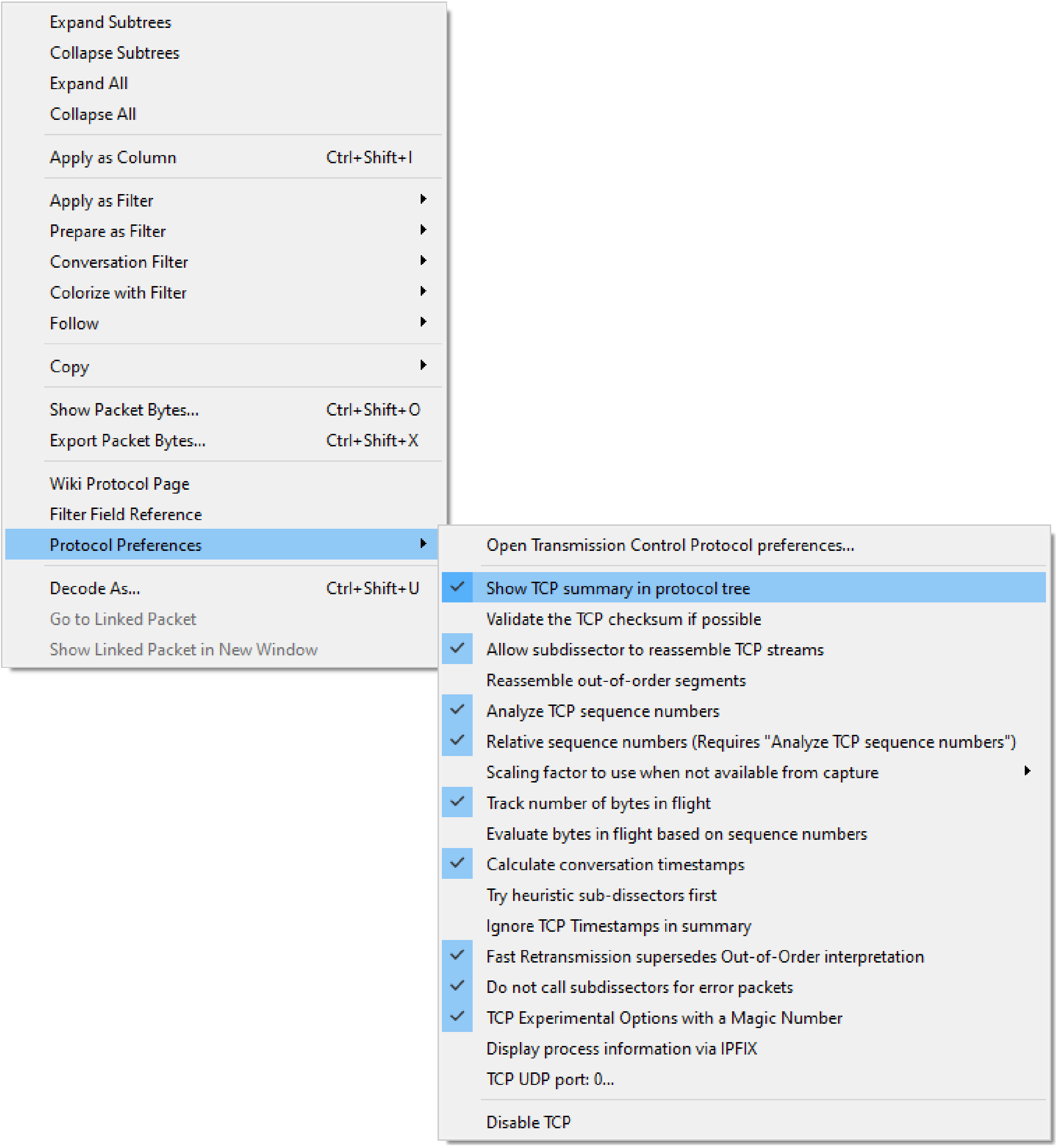
Layer	Name	Role	Protocols	PDU	Address
7	Application	Initiate contact with the network	HTTP, FTP, SMTP	Data	
6	Presentation	Formats data, optional compression and encryption		Data	
5	Session	Initiates, maintains, and tears down the session		Data	
4	Transport	Transports data	TCP, UDP	Segment	Port
3	Network	Addressing, routing	IP, ICMP	Packet	IP
2	Data Link	Frame formation	Ethernet II	Frame	MAC
1	Physical	Data is transmitted on the media		Bits	



```
TCP    10.0.0.148:49559       17.249.124.141:5223    ESTABLISHED
TCP    10.0.0.148:49768       34.212.110.138:443     ESTABLISHED
TCP    10.0.0.148:62310       13.89.217.116:443      ESTABLISHED
TCP    10.0.0.148:62789       23.55.20.137:443       CLOSE_WAIT
TCP    10.0.0.148:62790       204.13.192.141:80      CLOSE_WAIT
```

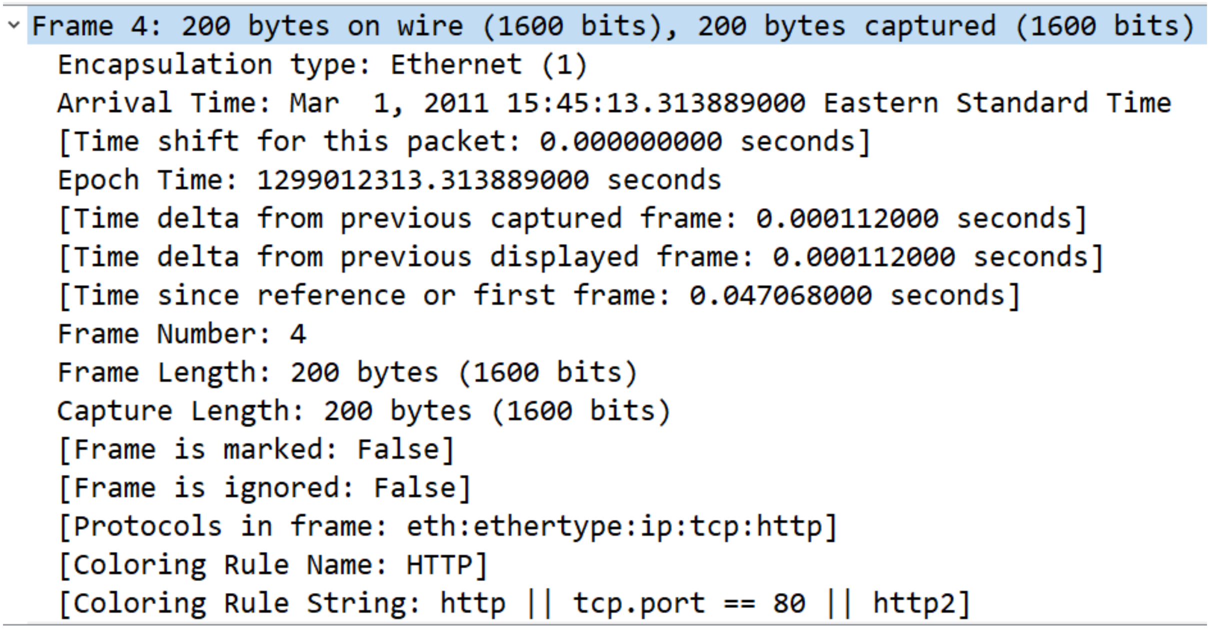


```
› Frame 4: 200 bytes on wire (1600 bits), 200 bytes captured (1600 bits)
› Ethernet II, Src: 00:1d:60:b3:01:84, Dst: 00:26:62:2f:47:87
› Internet Protocol Version 4, Src: 192.168.1.140, Dst: 174.143.213.184
› Transmission Control Protocol, Src Port: 57678 (57678), Dst Port: http
› Hypertext Transfer Protocol
```

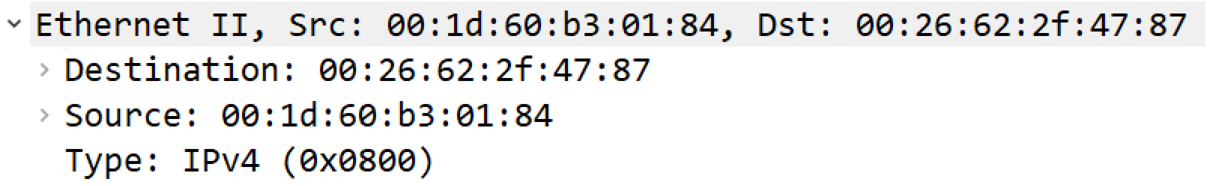


Expand Subtrees
Collapse Subtrees
Expand All
Collapse All
Apply as Column Ctrl+Shift+I
Apply as Filter ▸
Prepare as Filter ▸
Conversation Filter ▸
Colorize with Filter ▸
Follow ▸
Copy ▸
Show Packet Bytes... Ctrl+Shift+O
Export Packet Bytes... Ctrl+Shift+X
Wiki Protocol Page
Filter Field Reference
Protocol Preferences ▸
Decode As... Ctrl+Shift+U
Go to Linked Packet
Show Linked Packet in New Window

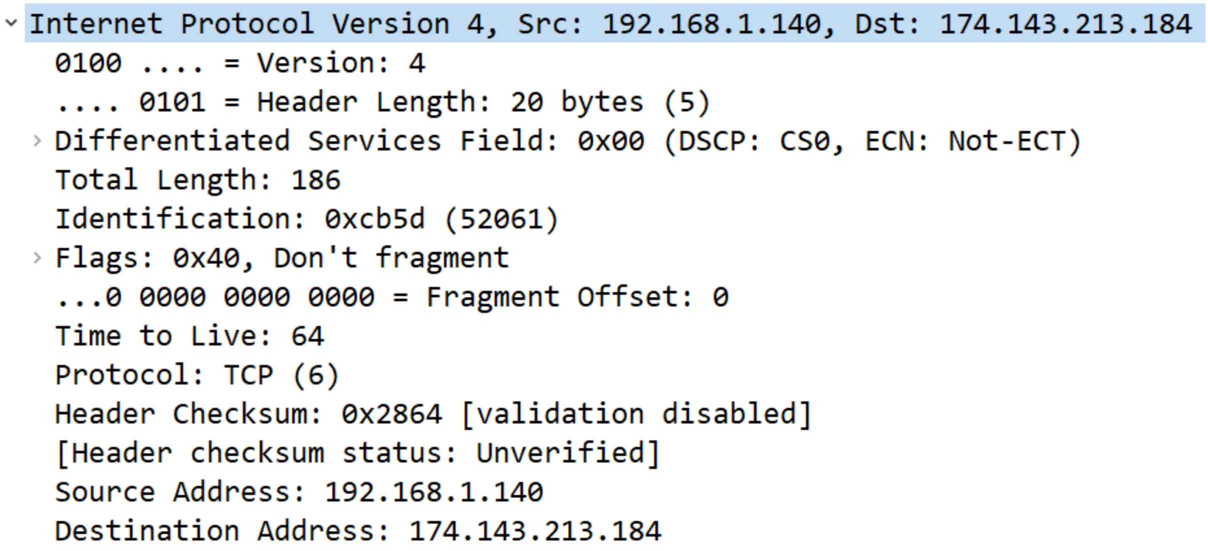
Open Transmission Control Protocol preferences...
✓ Show TCP summary in protocol tree
Validate the TCP checksum if possible
✓ Allow subdissector to reassemble TCP streams
Reassemble out-of-order segments
✓ Analyze TCP sequence numbers
✓ Relative sequence numbers (Requires "Analyze TCP sequence numbers")
Scaling factor to use when not available from capture ▸
✓ Track number of bytes in flight
Evaluate bytes in flight based on sequence numbers
✓ Calculate conversation timestamps
Try heuristic sub-dissectors first
Ignore TCP Timestamps in summary
✓ Fast Retransmission supersedes Out-of-Order interpretation
✓ Do not call subdissectors for error packets
✓ TCP Experimental Options with a Magic Number
Display process information via IPFIX
TCP UDP port: 0...
Disable TCP



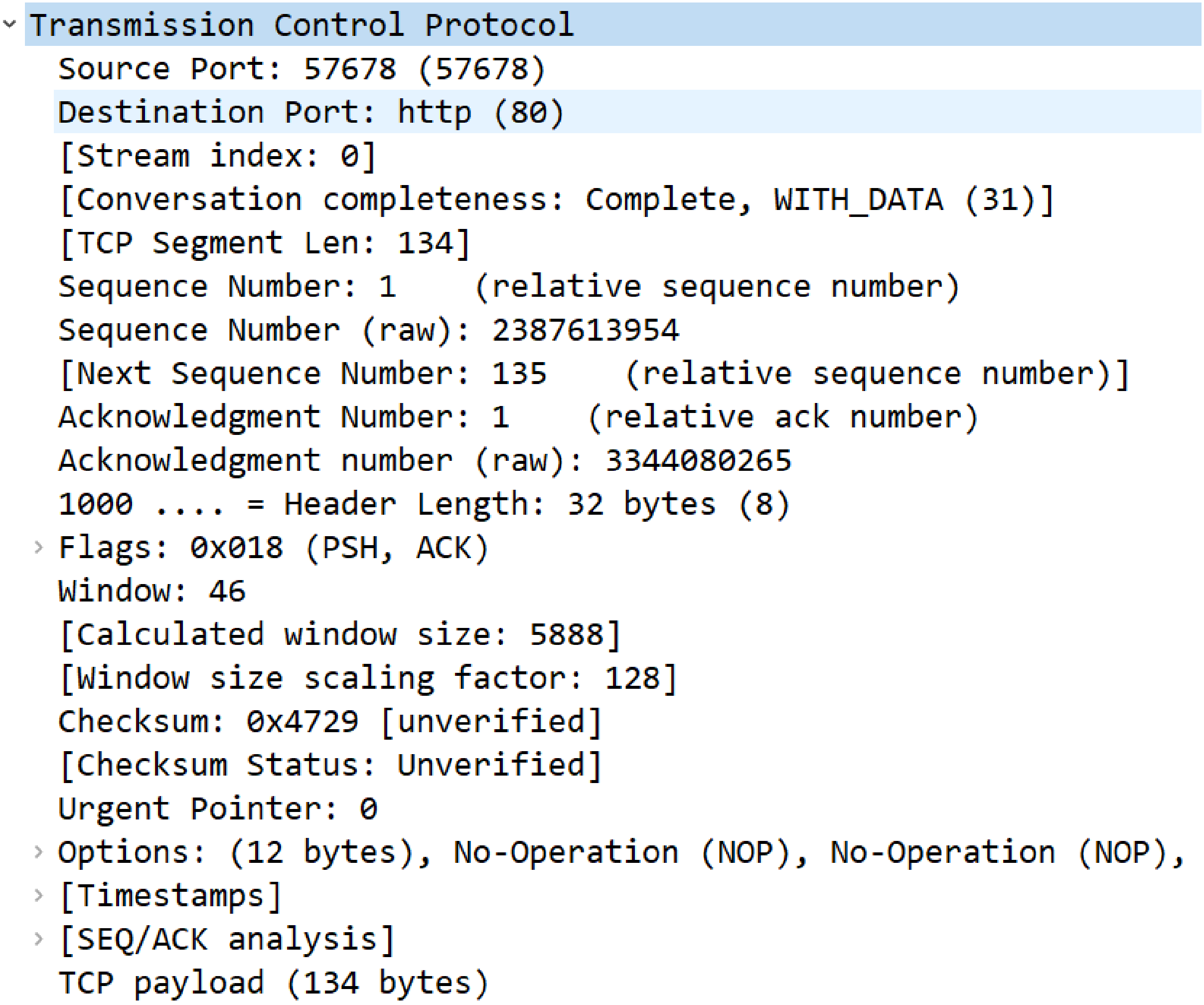
```
˅ Frame 4: 200 bytes on wire (1600 bits), 200 bytes captured (1600 bits)
    Encapsulation type: Ethernet (1)
    Arrival Time: Mar  1, 2011 15:45:13.313889000 Eastern Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1299012313.313889000 seconds
    [Time delta from previous captured frame: 0.000112000 seconds]
    [Time delta from previous displayed frame: 0.000112000 seconds]
    [Time since reference or first frame: 0.047068000 seconds]
    Frame Number: 4
    Frame Length: 200 bytes (1600 bits)
    Capture Length: 200 bytes (1600 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
```



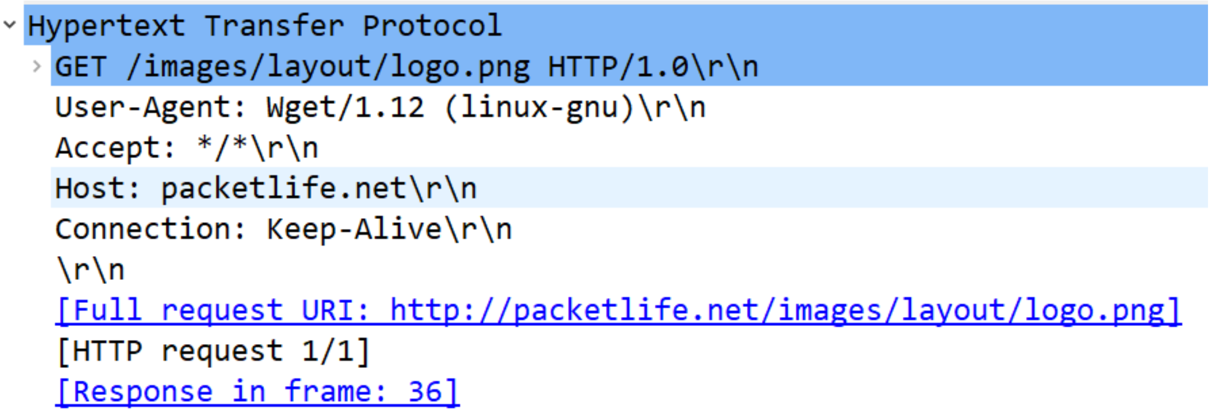
```
⌄ Ethernet II, Src: 00:1d:60:b3:01:84, Dst: 00:26:62:2f:47:87
  › Destination: 00:26:62:2f:47:87
  › Source: 00:1d:60:b3:01:84
    Type: IPv4 (0x0800)
```



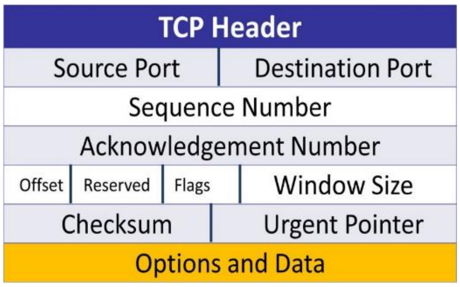
```
⌄ Internet Protocol Version 4, Src: 192.168.1.140, Dst: 174.143.213.184
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  › Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 186
    Identification: 0xcb5d (52061)
  › Flags: 0x40, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0x2864 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.140
    Destination Address: 174.143.213.184
```



```
⌄ Transmission Control Protocol
    Source Port: 57678 (57678)
    Destination Port: http (80)
    [Stream index: 0]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 134]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 2387613954
    [Next Sequence Number: 135    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 3344080265
    1000 .... = Header Length: 32 bytes (8)
  › Flags: 0x018 (PSH, ACK)
    Window: 46
    [Calculated window size: 5888]
    [Window size scaling factor: 128]
    Checksum: 0x4729 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  › Options: (12 bytes), No-Operation (NOP), No-Operation (NOP),
  › [Timestamps]
  › [SEQ/ACK analysis]
    TCP payload (134 bytes)
```



```
⌄ Hypertext Transfer Protocol
  › GET /images/layout/logo.png HTTP/1.0\r\n
    User-Agent: Wget/1.12 (linux-gnu)\r\n
    Accept: */*\r\n
    Host: packetlife.net\r\n
    Connection: Keep-Alive\r\n
    \r\n
    [Full request URI: http://packetlife.net/images/layout/logo.png]
    [HTTP request 1/1]
    [Response in frame: 36]
```



TCP Header

Source Port | Destination Port

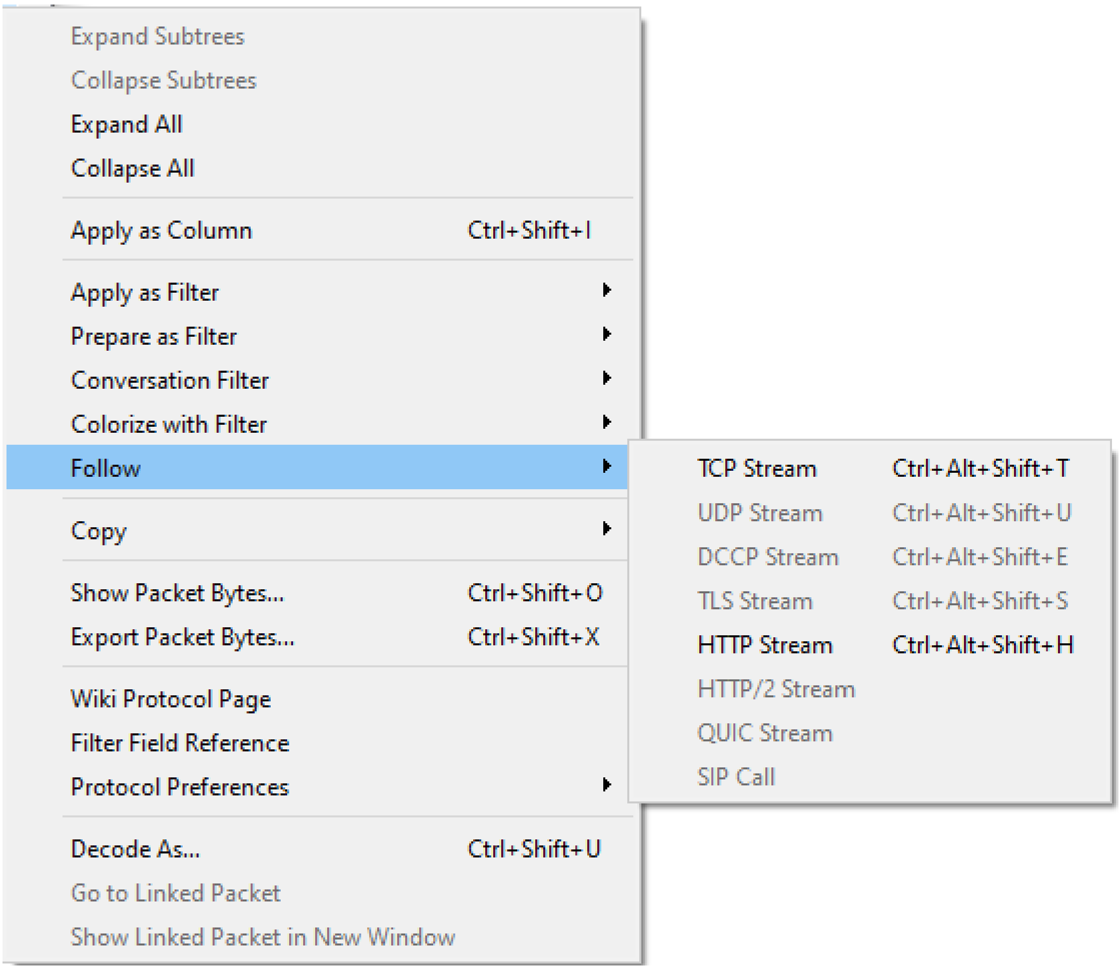
Sequence Number

Acknowledgement Number

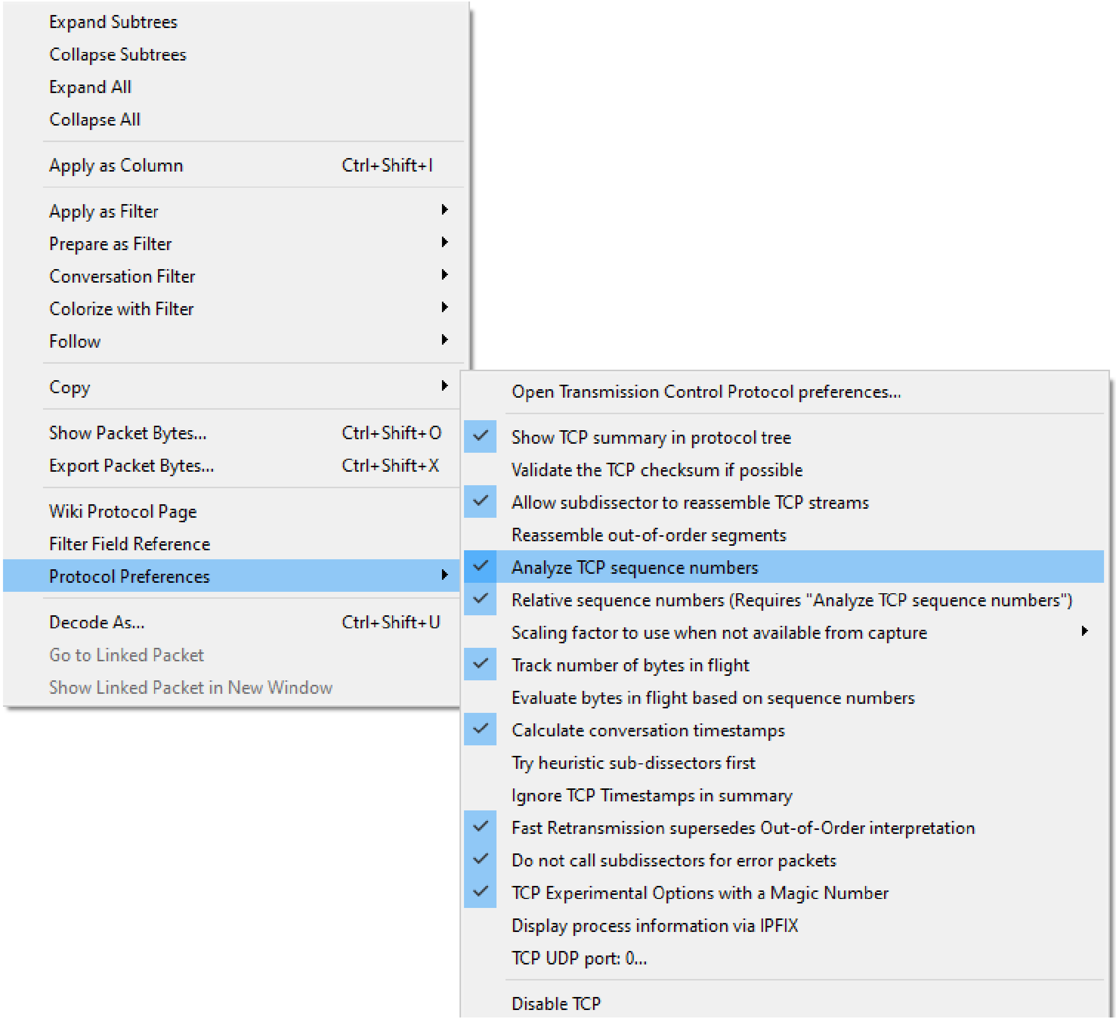
Offset | Reserved | Flags | Window Size

Checksum | Urgent Pointer

Options and Data


Expand Subtrees
Collapse Subtrees
Expand All
Collapse All
Apply as Column Ctrl+Shift+I
Apply as Filter
Prepare as Filter
Conversation Filter
Colorize with Filter
Follow
Copy
Show Packet Bytes... Ctrl+Shift+O
Export Packet Bytes... Ctrl+Shift+X
Wiki Protocol Page
Filter Field Reference
Protocol Preferences
Decode As... Ctrl+Shift+U
Go to Linked Packet
Show Linked Packet in New Window
TCP Stream Ctrl+Alt+Shift+T
UDP Stream Ctrl+Alt+Shift+U
DCCP Stream Ctrl+Alt+Shift+E
TLS Stream Ctrl+Alt+Shift+S
HTTP Stream Ctrl+Alt+Shift+H
HTTP/2 Stream
QUIC Stream
SIP Call

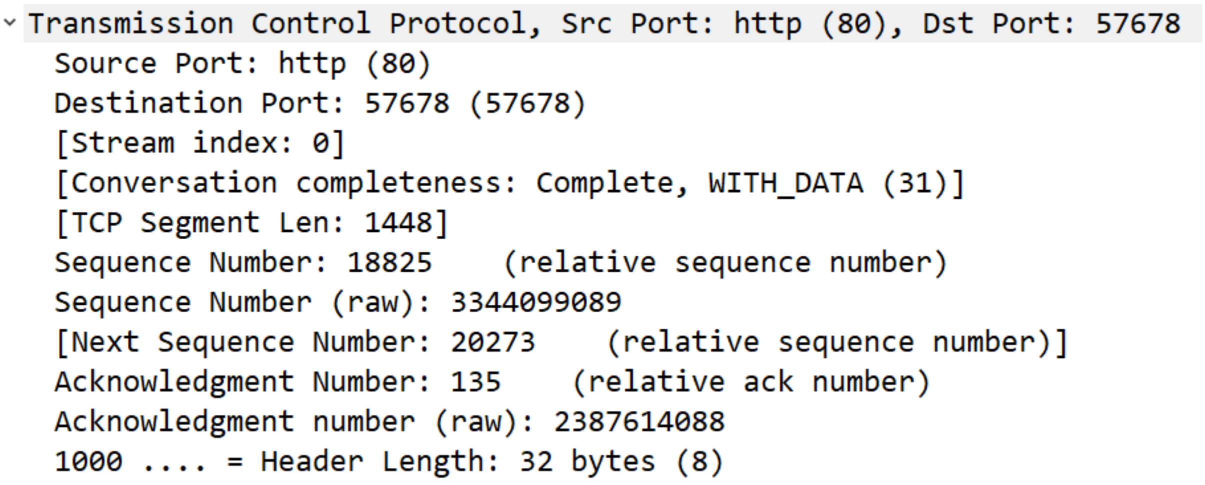
```
Client        <SYN><SEQ=100> -->          Server

Client   <-- <SEQ=300><ACK=101><SYN,ACK>  Server

Client      <SEQ=101><ACK=301><ACK>-->    Server
```



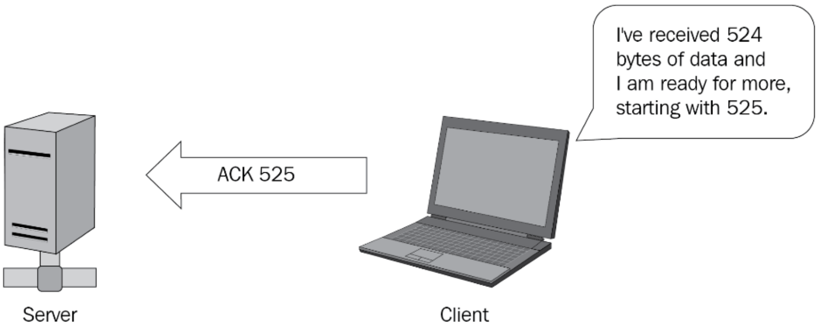
Open Transmission Control Protocol preferences...

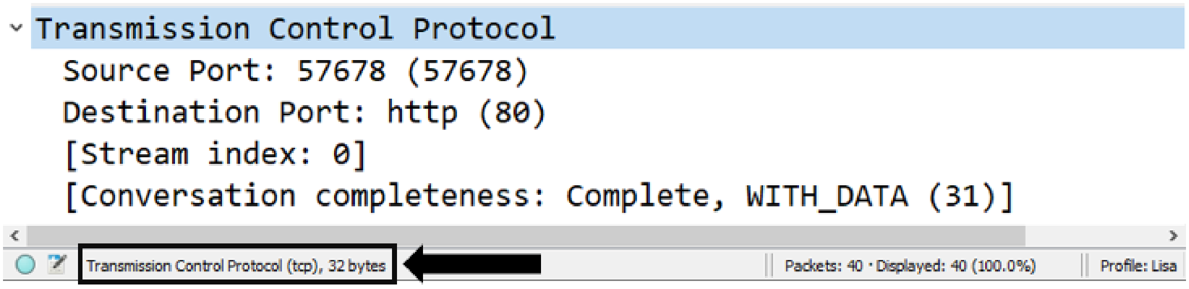
✓ Show TCP summary in protocol tree
Validate the TCP checksum if possible
✓ Allow subdissector to reassemble TCP streams
Reassemble out-of-order segments
✓ Analyze TCP sequence numbers
✓ Relative sequence numbers (Requires "Analyze TCP sequence numbers")
Scaling factor to use when not available from capture
✓ Track number of bytes in flight
Evaluate bytes in flight based on sequence numbers
✓ Calculate conversation timestamps
Try heuristic sub-dissectors first
Ignore TCP Timestamps in summary
✓ Fast Retransmission supersedes Out-of-Order interpretation
✓ Do not call subdissectors for error packets
✓ TCP Experimental Options with a Magic Number
Display process information via IPFIX
TCP UDP port: 0...

Disable TCP



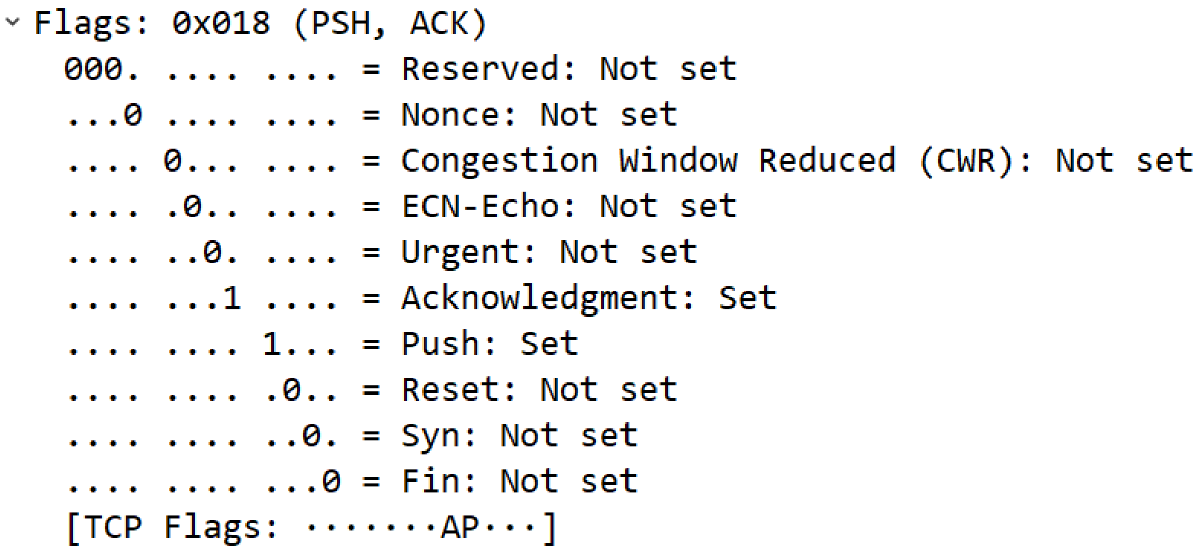
```
˅ Transmission Control Protocol, Src Port: http (80), Dst Port: 57678
    Source Port: http (80)
    Destination Port: 57678 (57678)
    [Stream index: 0]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 1448]
    Sequence Number: 18825    (relative sequence number)
    Sequence Number (raw): 3344099089
    [Next Sequence Number: 20273    (relative sequence number)]
    Acknowledgment Number: 135    (relative ack number)
    Acknowledgment number (raw): 2387614088
    1000 .... = Header Length: 32 bytes (8)
```


I've received 524 bytes of data and I am ready for more, starting with 525.
ACK 525
Server
Client

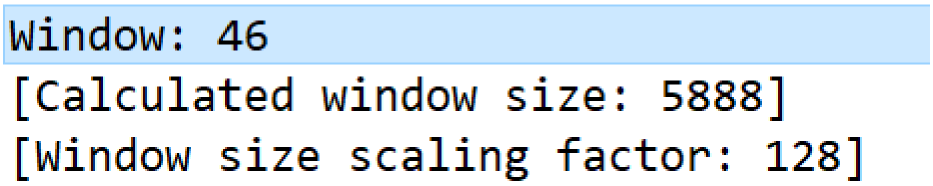


```
⌄ Transmission Control Protocol
    Source Port: 57678 (57678)
    Destination Port: http (80)
    [Stream index: 0]
    [Conversation completeness: Complete, WITH_DATA (31)]
```

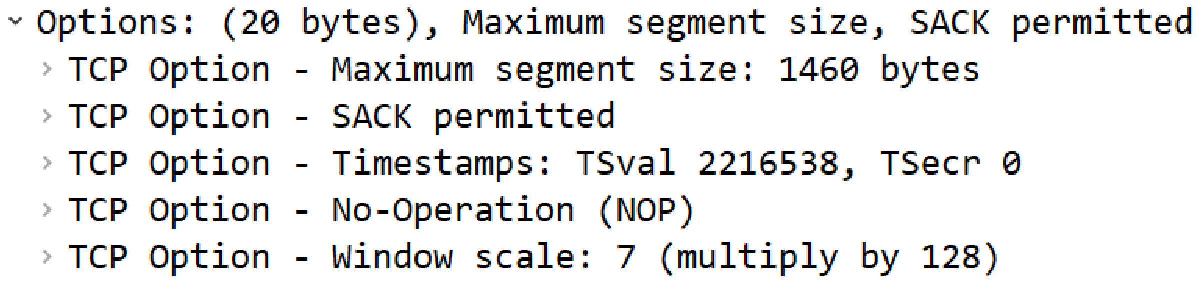
```
Transmission Control Protocol (tcp), 32 bytes    Packets: 40 · Displayed: 40 (100.0%)    Profile: Lisa
```



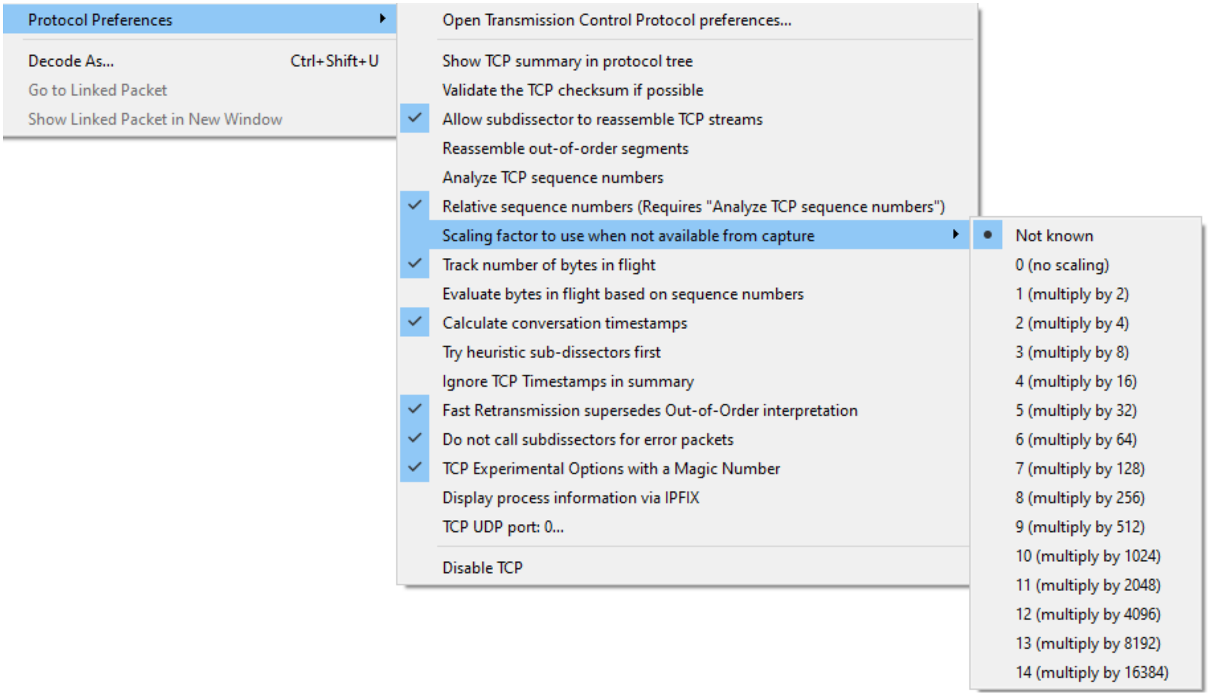
```
⌄ Flags: 0x018 (PSH, ACK)
    000. .... .... = Reserved: Not set
    ...0 .... .... = Nonce: Not set
    .... 0... .... = Congestion Window Reduced (CWR): Not set
    .... .0.. .... = ECN-Echo: Not set
    .... ..0. .... = Urgent: Not set
    .... ...1 .... = Acknowledgment: Set
    .... .... 1... = Push: Set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
    [TCP Flags: ·······AP···]
```



```
Window: 46
[Calculated window size: 5888]
[Window size scaling factor: 128]
```

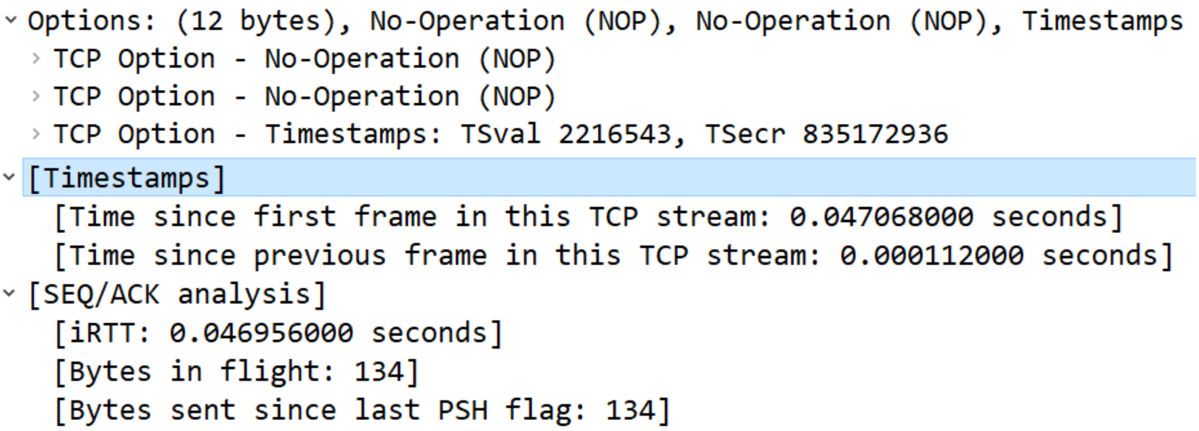


```
⌄ Options: (20 bytes), Maximum segment size, SACK permitted
  › TCP Option - Maximum segment size: 1460 bytes
  › TCP Option - SACK permitted
  › TCP Option - Timestamps: TSval 2216538, TSecr 0
  › TCP Option - No-Operation (NOP)
  › TCP Option - Window scale: 7 (multiply by 128)
```

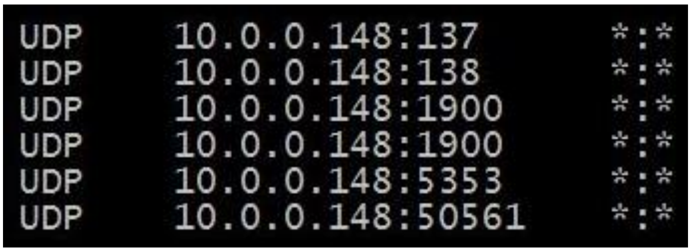


Open Transmission Control Protocol preferences...
Show TCP summary in protocol tree
Validate the TCP checksum if possible
✓ Allow subdissector to reassemble TCP streams
Reassemble out-of-order segments
Analyze TCP sequence numbers
✓ Relative sequence numbers (Requires "Analyze TCP sequence numbers")
Scaling factor to use when not available from capture
✓ Track number of bytes in flight
Evaluate bytes in flight based on sequence numbers
✓ Calculate conversation timestamps
Try heuristic sub-dissectors first
Ignore TCP Timestamps in summary
✓ Fast Retransmission supersedes Out-of-Order interpretation
✓ Do not call subdissectors for error packets
✓ TCP Experimental Options with a Magic Number
Display process information via IPFIX
TCP UDP port: 0...
Disable TCP

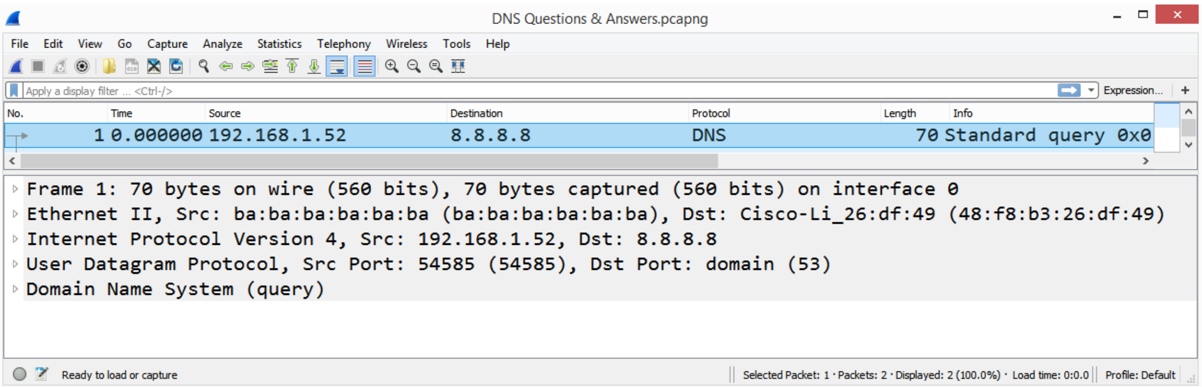
● Not known
0 (no scaling)
1 (multiply by 2)
2 (multiply by 4)
3 (multiply by 8)
4 (multiply by 16)
5 (multiply by 32)
6 (multiply by 64)
7 (multiply by 128)
8 (multiply by 256)
9 (multiply by 512)
10 (multiply by 1024)
11 (multiply by 2048)
12 (multiply by 4096)
13 (multiply by 8192)
14 (multiply by 16384)



```
Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  TCP Option - No-Operation (NOP)
  TCP Option - No-Operation (NOP)
  TCP Option - Timestamps: TSval 2216543, TSecr 835172936
[Timestamps]
  [Time since first frame in this TCP stream: 0.047068000 seconds]
  [Time since previous frame in this TCP stream: 0.000112000 seconds]
[SEQ/ACK analysis]
  [iRTT: 0.046956000 seconds]
  [Bytes in flight: 134]
  [Bytes sent since last PSH flag: 134]
```



```
UDP    10.0.0.148:137      *:*
UDP    10.0.0.148:138      *:*
UDP    10.0.0.148:1900     *:*
UDP    10.0.0.148:1900     *:*
UDP    10.0.0.148:5353     *:*
UDP    10.0.0.148:50561    *:*
```

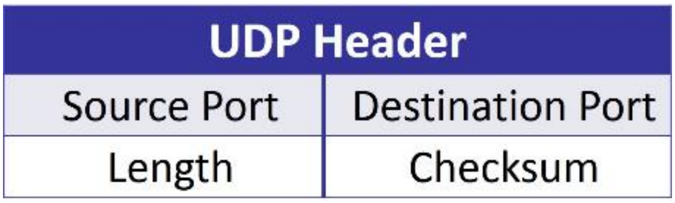


DNS Questions & Answers.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...

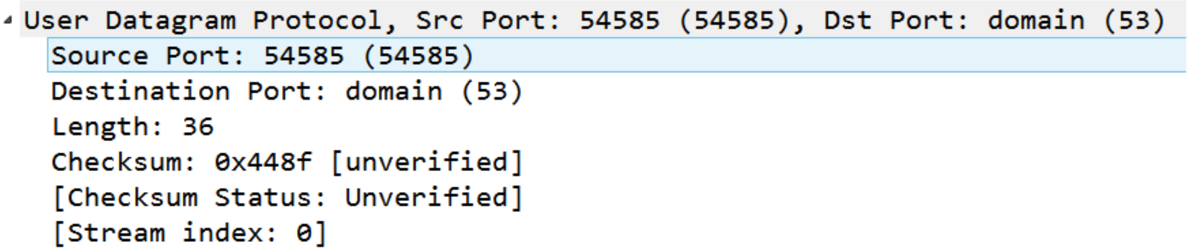
```
No.  Time      Source         Destination  Protocol  Length  Info
   1 0.000000  192.168.1.52   8.8.8.8      DNS           70  Standard query 0x0
```

```
Frame 1: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
Ethernet II, Src: ba:ba:ba:ba:ba:ba (ba:ba:ba:ba:ba:ba), Dst: Cisco-Li_26:df:49 (48:f8:b3:26:df:49)
Internet Protocol Version 4, Src: 192.168.1.52, Dst: 8.8.8.8
User Datagram Protocol, Src Port: 54585 (54585), Dst Port: domain (53)
Domain Name System (query)
```

Ready to load or capture
Selected Packet: 1 · Packets: 2 · Displayed: 2 (100.0%) · Load time: 0:0.0
Profile: Default

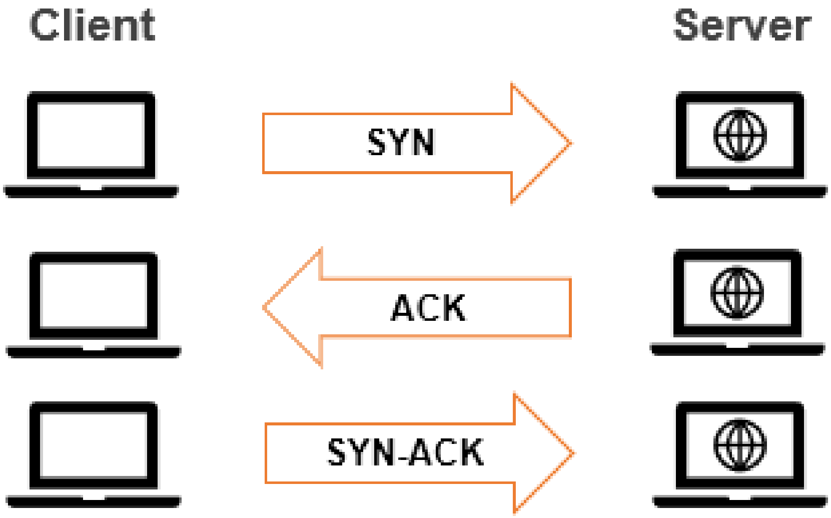


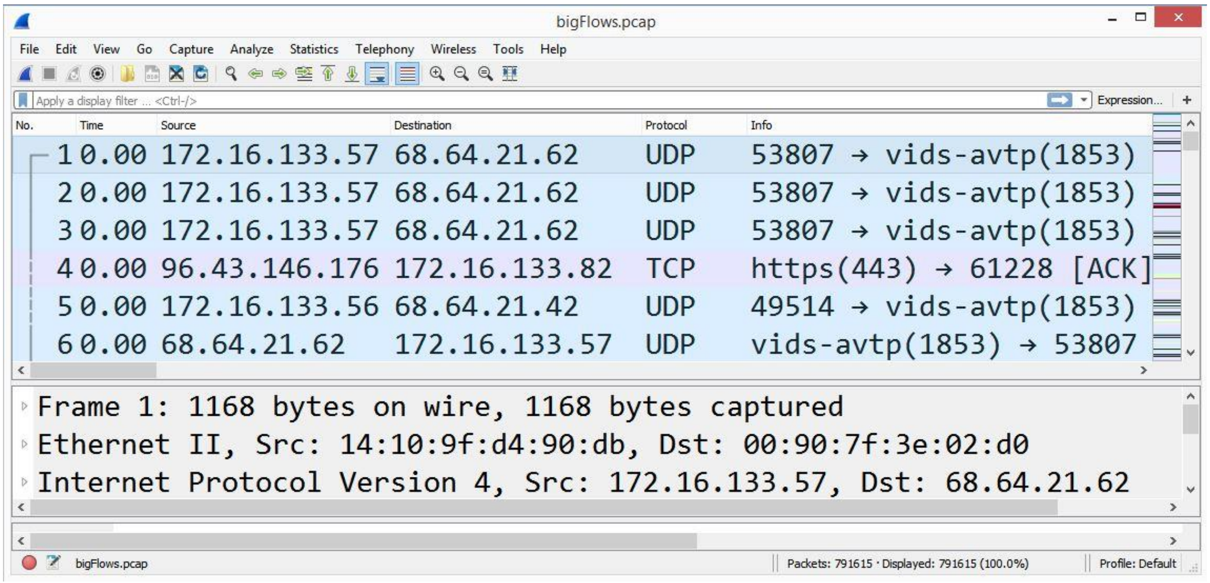
UDP Header	
Source Port	Destination Port
Length	Checksum



```
◢ User Datagram Protocol, Src Port: 54585 (54585), Dst Port: domain (53)
    Source Port: 54585 (54585)
    Destination Port: domain (53)
    Length: 36
    Checksum: 0x448f [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
```

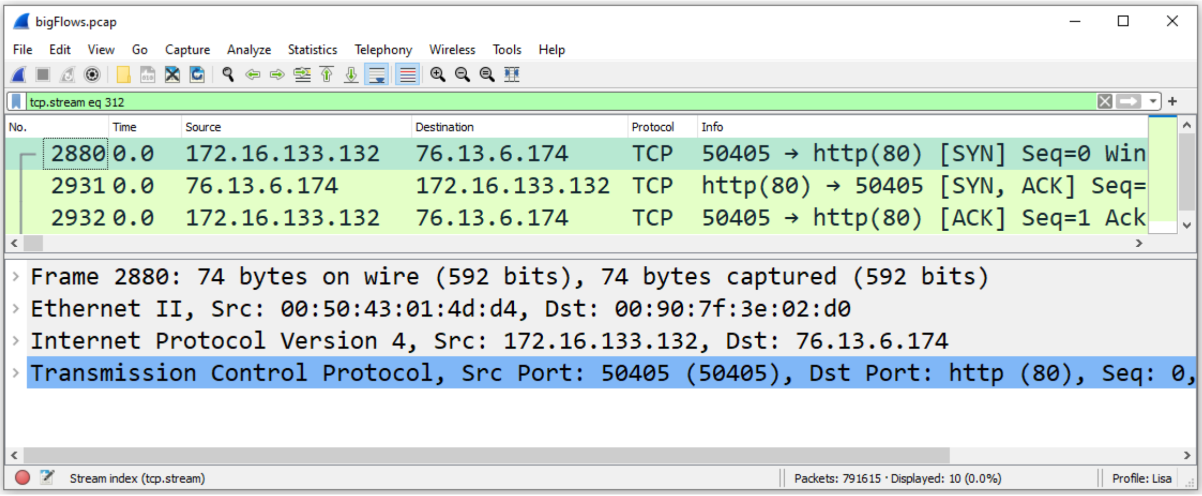
Chapter 10: Managing TCP Connections




bigFlows.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...

```
No. Time Source          Destination      Protocol Info
1   0.00 172.16.133.57   68.64.21.62      UDP      53807 → vids-avtp(1853)
2   0.00 172.16.133.57   68.64.21.62      UDP      53807 → vids-avtp(1853)
3   0.00 172.16.133.57   68.64.21.62      UDP      53807 → vids-avtp(1853)
4   0.00 96.43.146.176   172.16.133.82    TCP      https(443) → 61228 [ACK]
5   0.00 172.16.133.56   68.64.21.42      UDP      49514 → vids-avtp(1853)
6   0.00 68.64.21.62     172.16.133.57    UDP      vids-avtp(1853) → 53807

Frame 1: 1168 bytes on wire, 1168 bytes captured
Ethernet II, Src: 14:10:9f:d4:90:db, Dst: 00:90:7f:3e:02:d0
Internet Protocol Version 4, Src: 172.16.133.57, Dst: 68.64.21.62
```

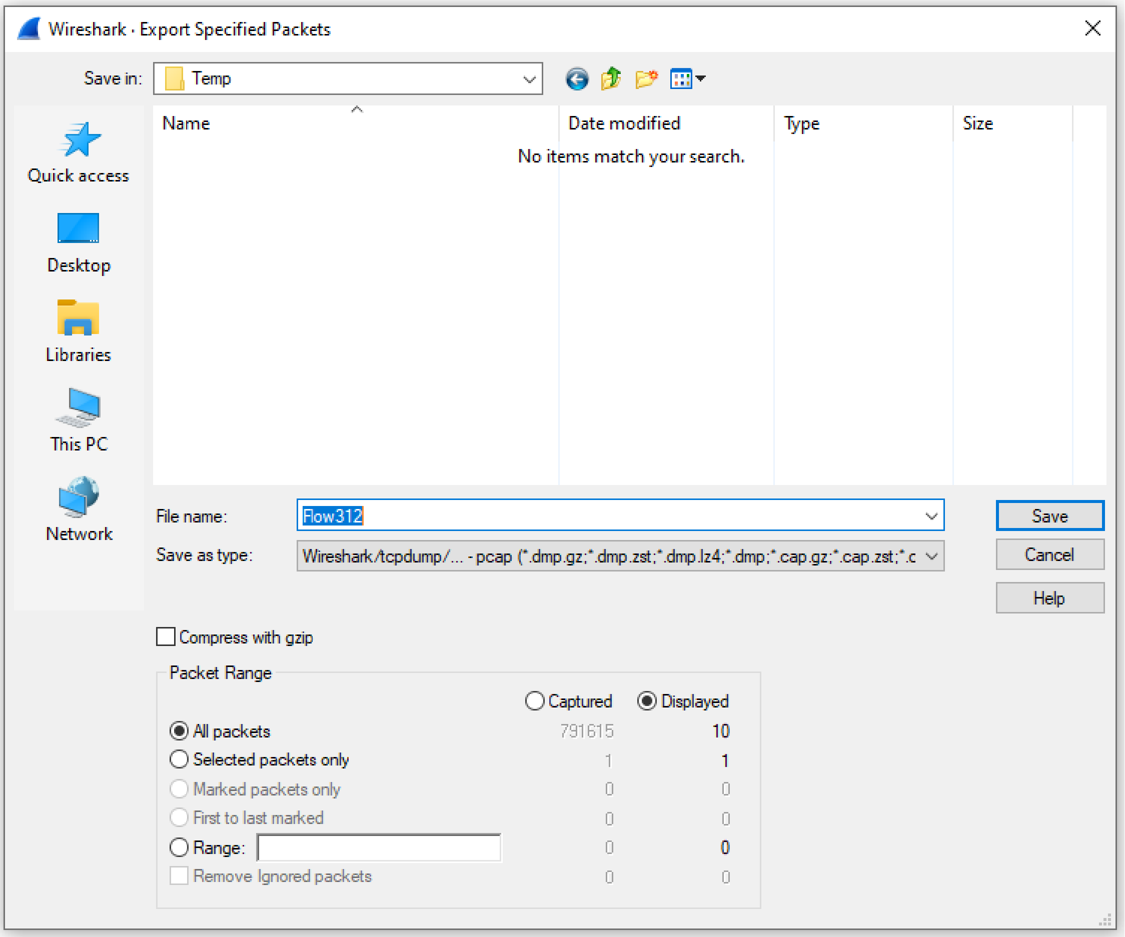
bigFlows.pcap | Packets: 791615 · Displayed: 791615 (100.0%) | Profile: Default


bigFlows.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.stream eq 312

```
No.  Time Source          Destination     Protocol Info
2880 0.0  172.16.133.132  76.13.6.174     TCP      50405 → http(80) [SYN] Seq=0 Win
2931 0.0  76.13.6.174     172.16.133.132  TCP      http(80) → 50405 [SYN, ACK] Seq=
2932 0.0  172.16.133.132  76.13.6.174     TCP      50405 → http(80) [ACK] Seq=1 Ack

Frame 2880: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
Ethernet II, Src: 00:50:43:01:4d:d4, Dst: 00:90:7f:3e:02:d0
Internet Protocol Version 4, Src: 172.16.133.132, Dst: 76.13.6.174
Transmission Control Protocol, Src Port: 50405 (50405), Dst Port: http (80), Seq: 0,
```

Stream index (tcp.stream) | Packets: 791615 · Displayed: 10 (0.0%) | Profile: Lisa



Save in: Temp

No items match your search.

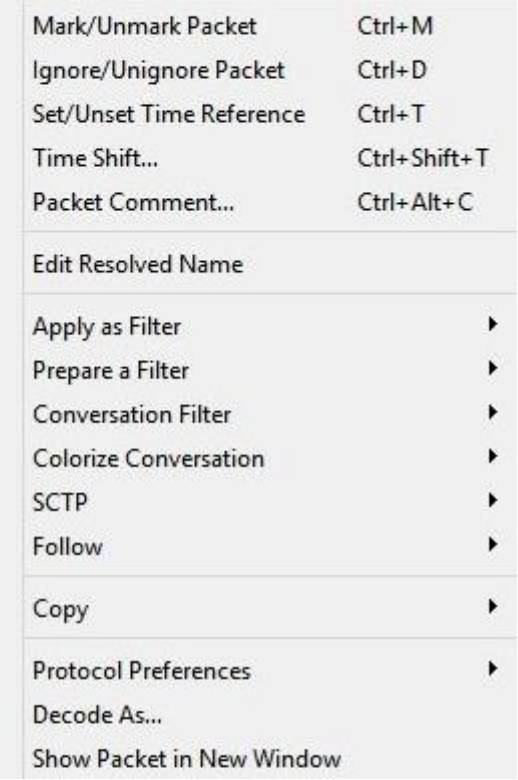
File name: Flow312

Save as type: Wireshark/tcpdump/... - pcap (*.dmp.gz;*.dmp.zst;*.dmp.lz4;*.dmp;*.cap.gz;*.cap.zst;*.c

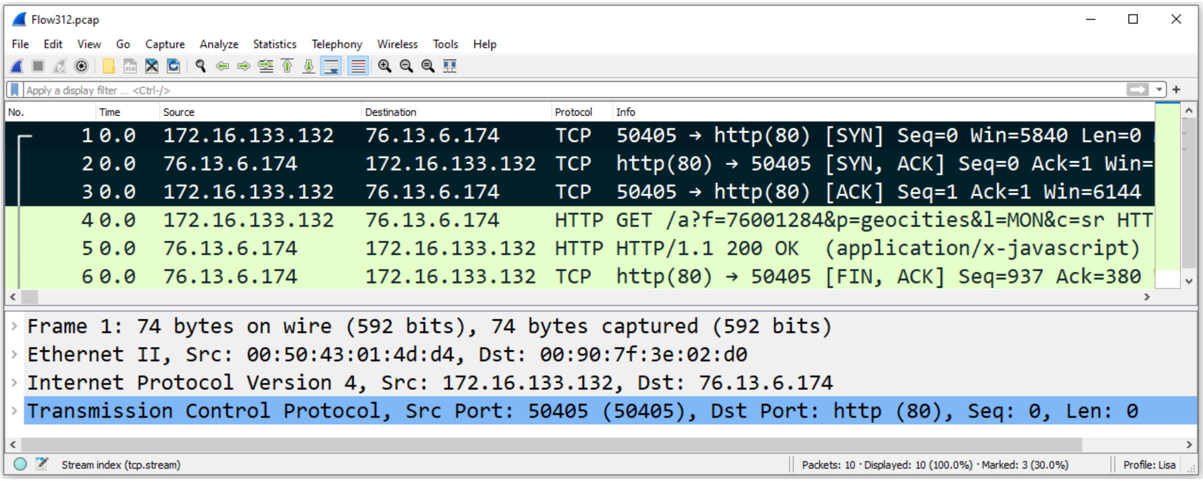
□ Compress with gzip

Packet Range

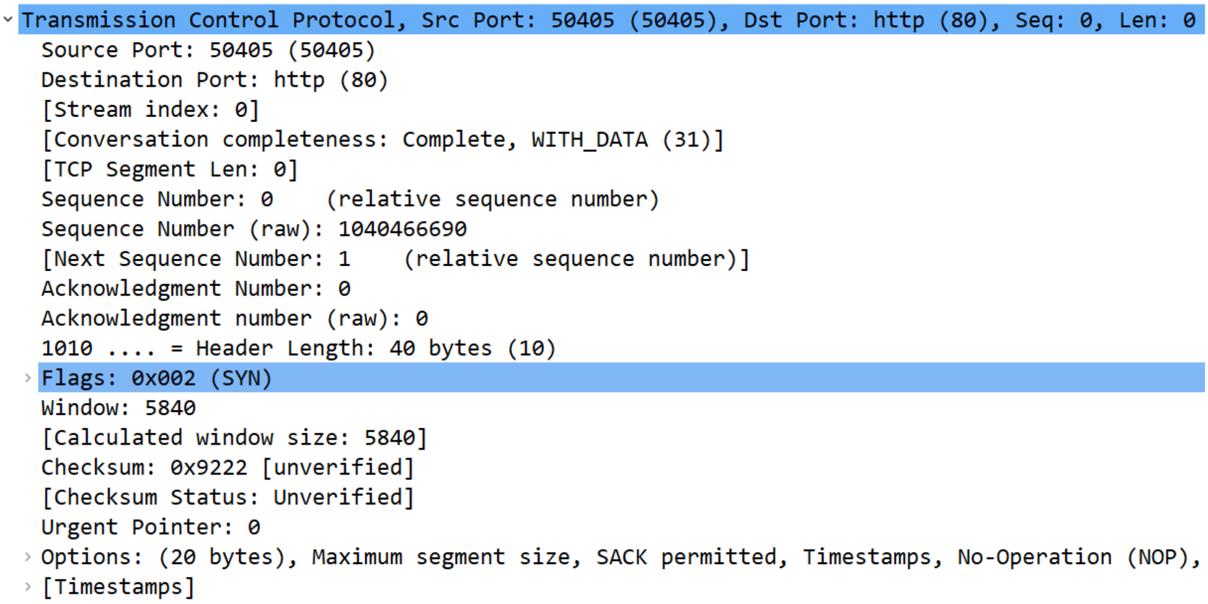
	○ Captured	● Displayed
● All packets	791615	10
○ Selected packets only	1	1
○ Marked packets only	0	0
○ First to last marked	0	0
○ Range:	0	0
□ Remove Ignored packets	0	0



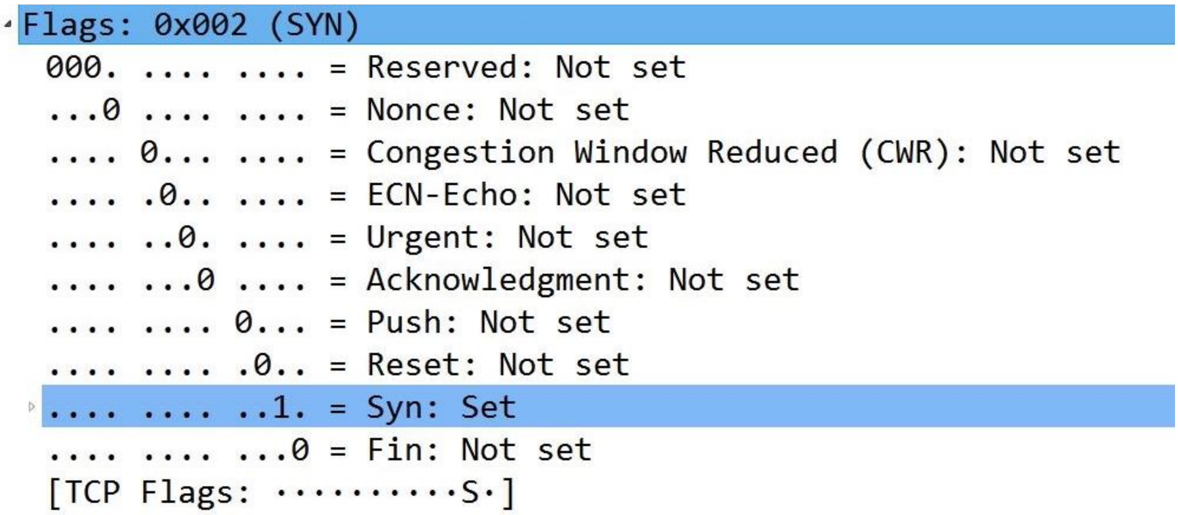
Mark/Unmark Packet Ctrl+M
Ignore/Unignore Packet Ctrl+D
Set/Unset Time Reference Ctrl+T
Time Shift... Ctrl+Shift+T
Packet Comment... Ctrl+Alt+C
Edit Resolved Name
Apply as Filter ▸
Prepare a Filter ▸
Conversation Filter ▸
Colorize Conversation ▸
SCTP ▸
Follow ▸
Copy ▸
Protocol Preferences ▸
Decode As...
Show Packet in New Window


Flow312.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

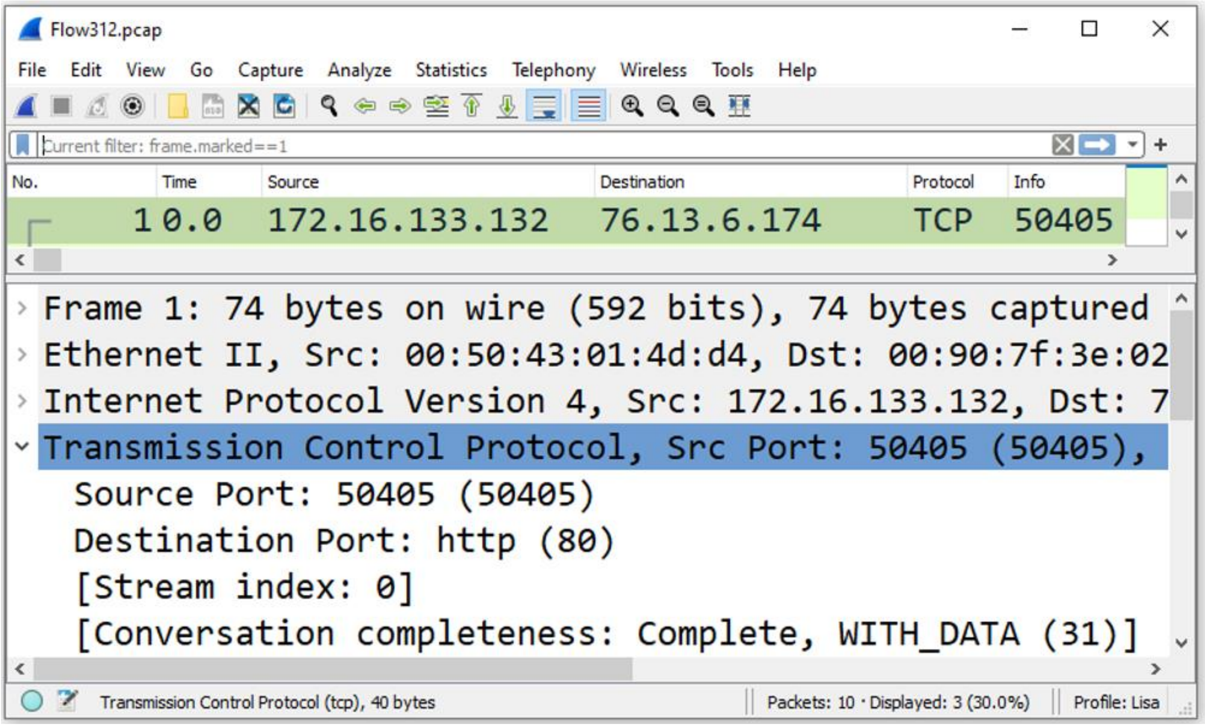
```
No.  Time  Source          Destination     Protocol Info
  1  0.0   172.16.133.132  76.13.6.174     TCP      50405 → http(80) [SYN] Seq=0 Win=5840 Len=0
  2  0.0   76.13.6.174     172.16.133.132  TCP      http(80) → 50405 [SYN, ACK] Seq=0 Ack=1 Win=
  3  0.0   172.16.133.132  76.13.6.174     TCP      50405 → http(80) [ACK] Seq=1 Ack=1 Win=6144
  4  0.0   172.16.133.132  76.13.6.174     HTTP     GET /a?f=76001284&p=geocities&l=MON&c=sr HTT
  5  0.0   76.13.6.174     172.16.133.132  HTTP     HTTP/1.1 200 OK  (application/x-javascript)
  6  0.0   76.13.6.174     172.16.133.132  TCP      http(80) → 50405 [FIN, ACK] Seq=937 Ack=380

> Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
> Ethernet II, Src: 00:50:43:01:4d:d4, Dst: 00:90:7f:3e:02:d0
> Internet Protocol Version 4, Src: 172.16.133.132, Dst: 76.13.6.174
> Transmission Control Protocol, Src Port: 50405 (50405), Dst Port: http (80), Seq: 0, Len: 0

Stream index (tcp.stream)    Packets: 10 · Displayed: 10 (100.0%) · Marked: 3 (30.0%)    Profile: Lisa
```



```
v Transmission Control Protocol, Src Port: 50405 (50405), Dst Port: http (80), Seq: 0, Len: 0
    Source Port: 50405 (50405)
    Destination Port: http (80)
    [Stream index: 0]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 1040466690
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 0
    Acknowledgment number (raw): 0
    1010 .... = Header Length: 40 bytes (10)
  > Flags: 0x002 (SYN)
    Window: 5840
    [Calculated window size: 5840]
    Checksum: 0x9222 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > Options: (20 bytes), Maximum segment size, SACK permitted, Timestamps, No-Operation (NOP),
  > [Timestamps]
```



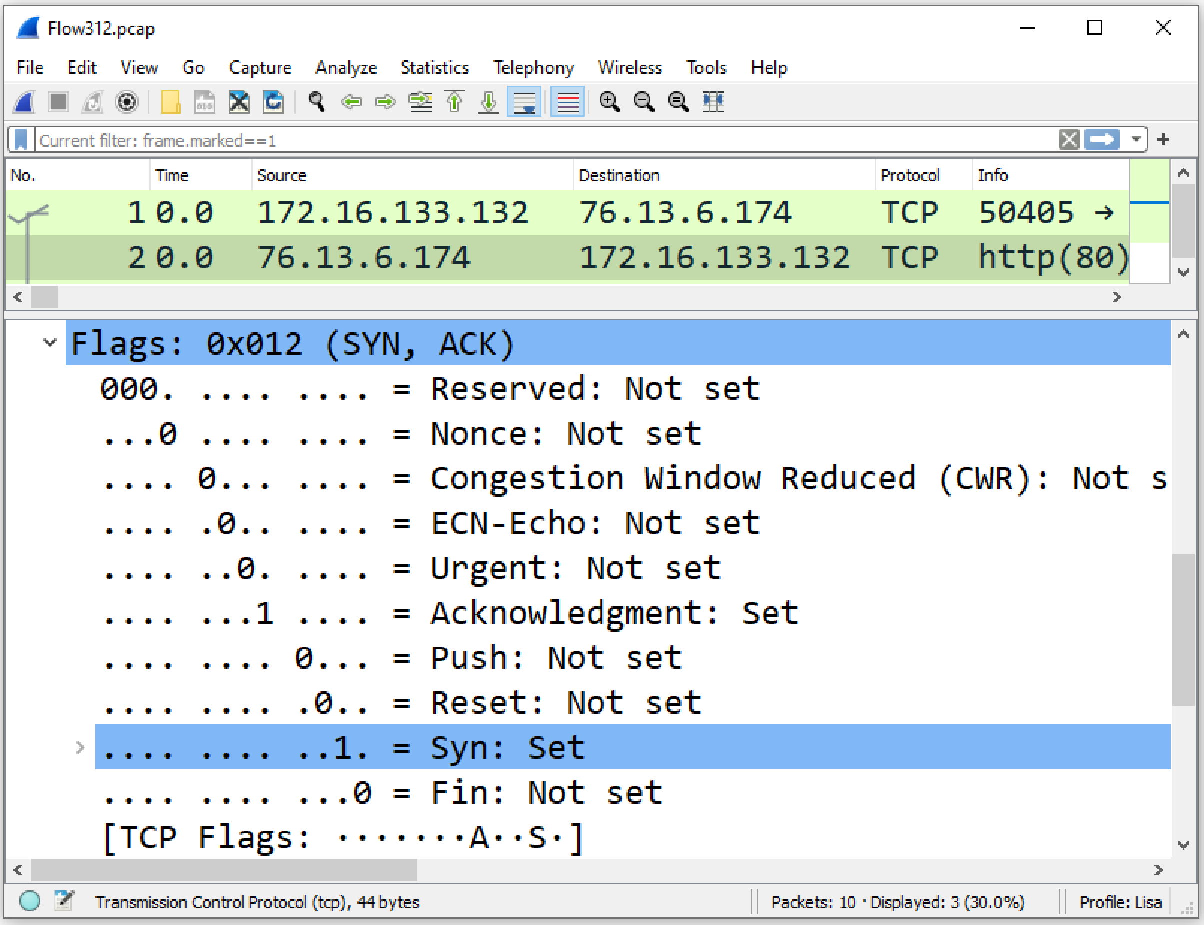
```
Flags: 0x002 (SYN)
  000. .... .... = Reserved: Not set
  ...0 .... .... = Nonce: Not set
  .... 0... .... = Congestion Window Reduced (CWR): Not set
  .... .0.. .... = ECN-Echo: Not set
  .... ..0. .... = Urgent: Not set
  .... ...0 .... = Acknowledgment: Not set
  .... .... 0... = Push: Not set
  .... .... .0.. = Reset: Not set
  .... .... ..1. = Syn: Set
  .... .... ...0 = Fin: Not set
  [TCP Flags: ··········S·]
```


Flow312.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Current filter: frame.marked==1

```
No.        Time   Source              Destination       Protocol  Info
       1   0.0    172.16.133.132      76.13.6.174       TCP       50405

> Frame 1: 74 bytes on wire (592 bits), 74 bytes captured
> Ethernet II, Src: 00:50:43:01:4d:d4, Dst: 00:90:7f:3e:02
> Internet Protocol Version 4, Src: 172.16.133.132, Dst: 7
v Transmission Control Protocol, Src Port: 50405 (50405),
    Source Port: 50405 (50405)
    Destination Port: http (80)
    [Stream index: 0]
    [Conversation completeness: Complete, WITH_DATA (31)]
```

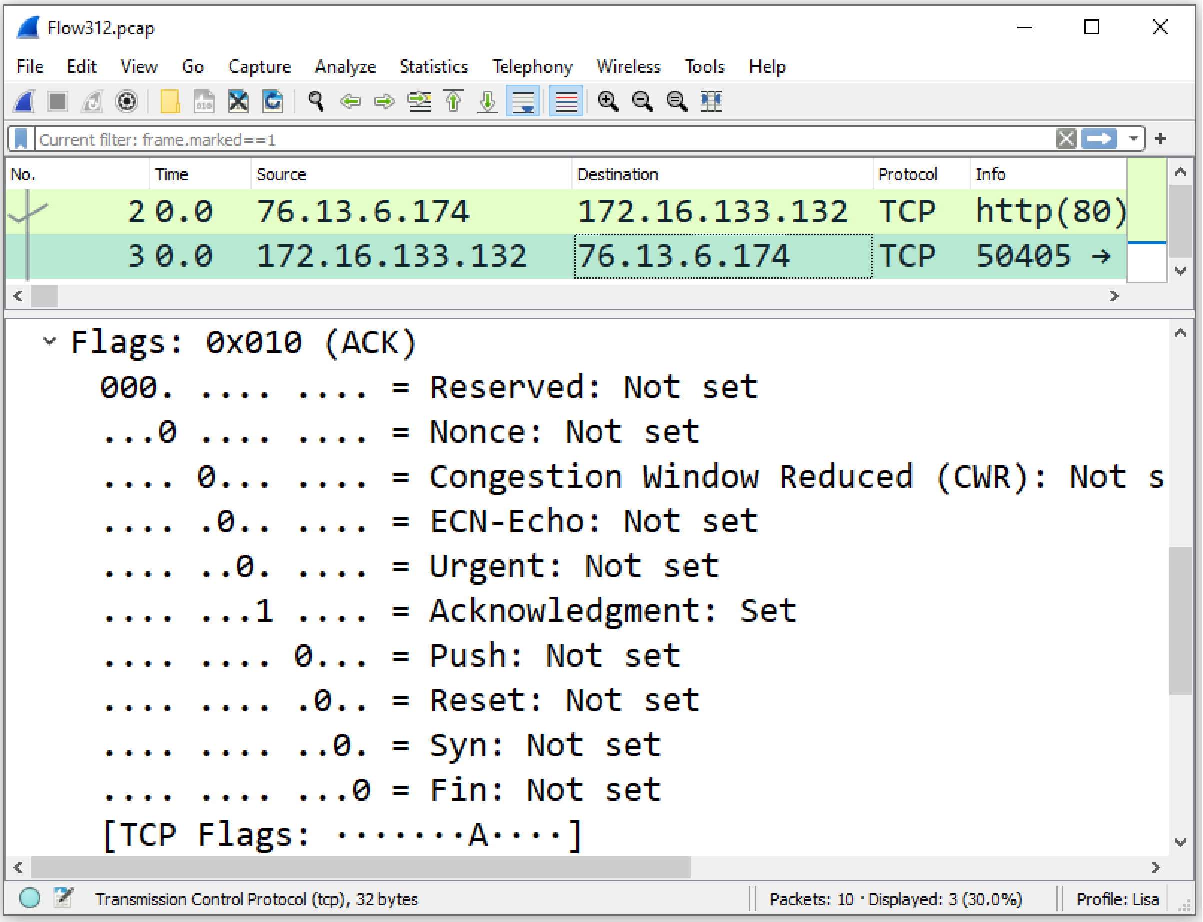
Transmission Control Protocol (tcp), 40 bytes | Packets: 10 · Displayed: 3 (30.0%) | Profile: Lisa


Flow312.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Current filter: frame.marked==1

```
No.        Time   Source              Destination       Protocol  Info
       1   0.0    172.16.133.132      76.13.6.174       TCP       50405 →
       2   0.0    76.13.6.174         172.16.133.132    TCP       http(80)

  v Flags: 0x012 (SYN, ACK)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Nonce: Not set
      .... 0... .... = Congestion Window Reduced (CWR): Not s
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...1 .... = Acknowledgment: Set
      .... .... 0... = Push: Not set
      .... .... .0.. = Reset: Not set
    > .... .... ..1. = Syn: Set
      .... .... ...0 = Fin: Not set
      [TCP Flags: ·······A··S·]
```

Transmission Control Protocol (tcp), 44 bytes | Packets: 10 · Displayed: 3 (30.0%) | Profile: Lisa

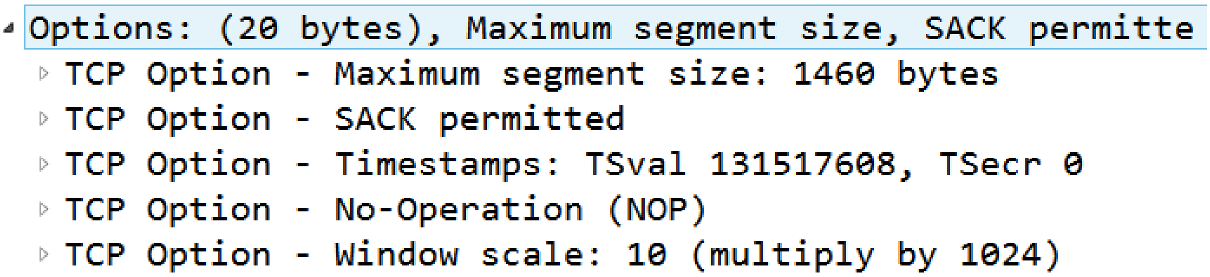

Flow312.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Current filter: frame.marked==1

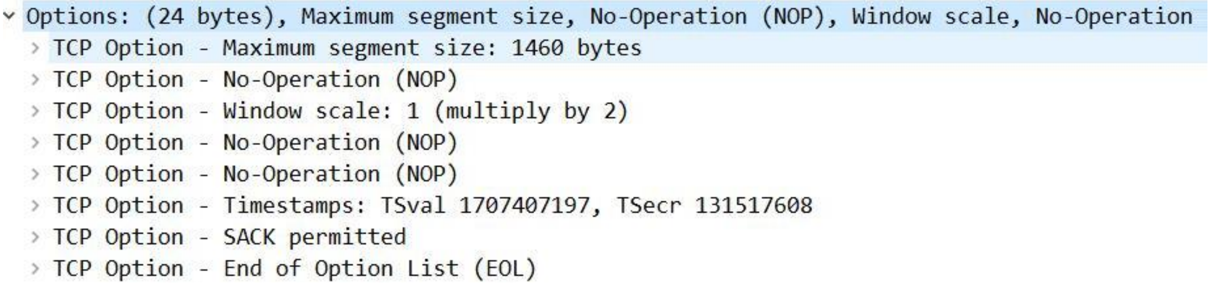
```
No.   Time   Source           Destination      Protocol  Info
   2  0.0    76.13.6.174      172.16.133.132   TCP       http(80)
   3  0.0    172.16.133.132   76.13.6.174      TCP       50405 →
```

```
⌄ Flags: 0x010 (ACK)
    000. .... .... = Reserved: Not set
    ...0 .... .... = Nonce: Not set
    .... 0... .... = Congestion Window Reduced (CWR): Not s
    .... .0.. .... = ECN-Echo: Not set
    .... ..0. .... = Urgent: Not set
    .... ...1 .... = Acknowledgment: Set
    .... .... 0... = Push: Not set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
    [TCP Flags: ·······A····]
```

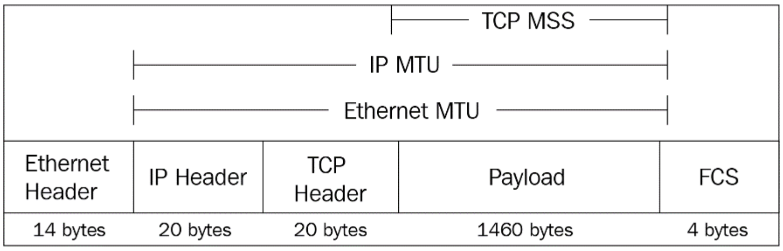
Transmission Control Protocol (tcp), 32 bytes | Packets: 10 · Displayed: 3 (30.0%) | Profile: Lisa

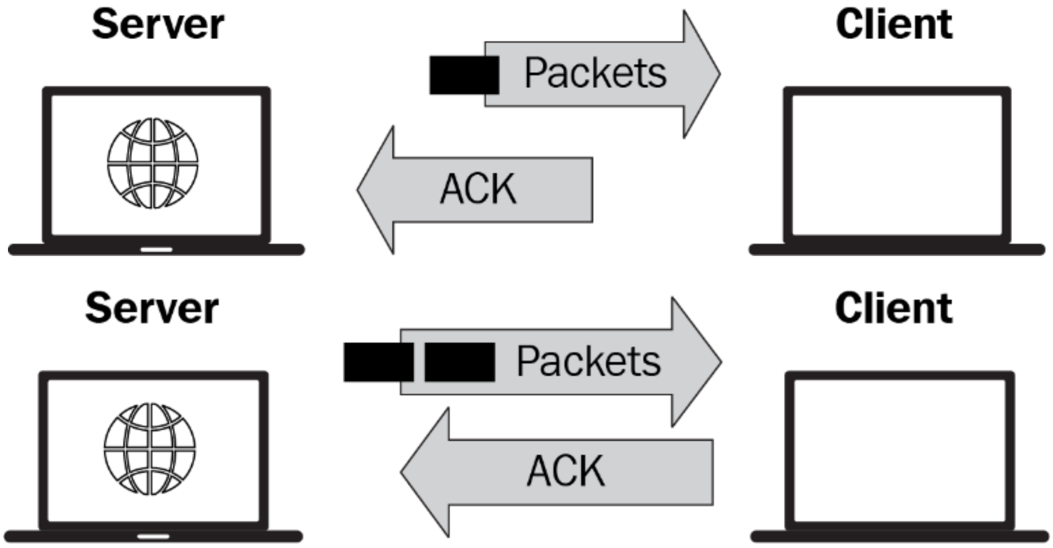


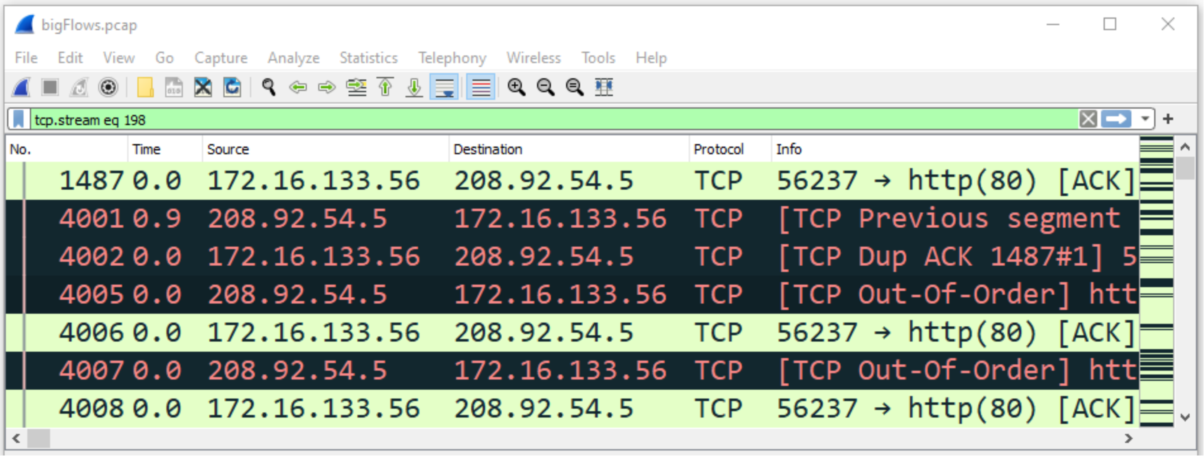
```
◢ Options: (20 bytes), Maximum segment size, SACK permitte
   ▷ TCP Option - Maximum segment size: 1460 bytes
   ▷ TCP Option - SACK permitted
   ▷ TCP Option - Timestamps: TSval 131517608, TSecr 0
   ▷ TCP Option - No-Operation (NOP)
   ▷ TCP Option - Window scale: 10 (multiply by 1024)
```



```
⌄ Options: (24 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation
   › TCP Option - Maximum segment size: 1460 bytes
   › TCP Option - No-Operation (NOP)
   › TCP Option - Window scale: 1 (multiply by 2)
   › TCP Option - No-Operation (NOP)
   › TCP Option - No-Operation (NOP)
   › TCP Option - Timestamps: TSval 1707407197, TSecr 131517608
   › TCP Option - SACK permitted
   › TCP Option - End of Option List (EOL)
```

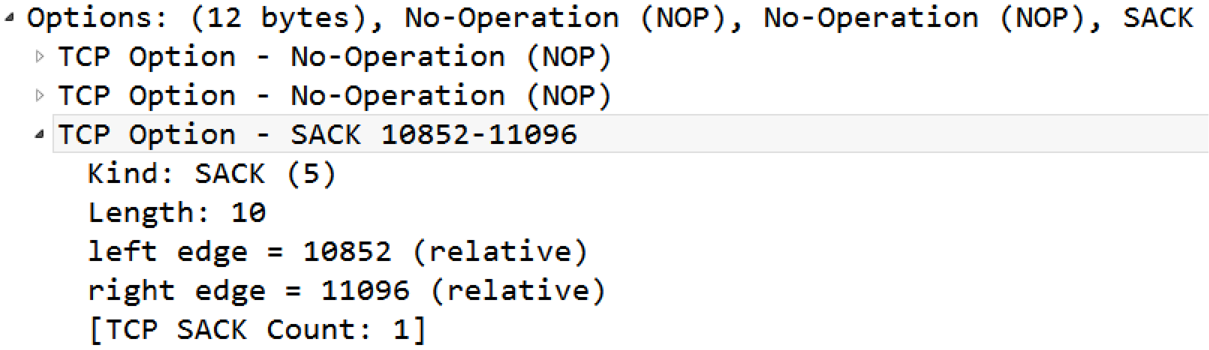




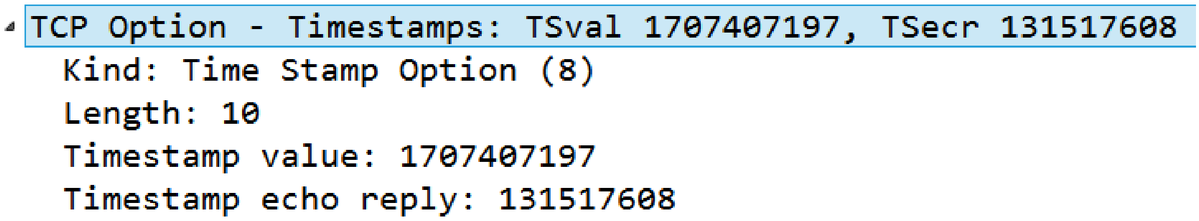

bigFlows.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.stream eq 198

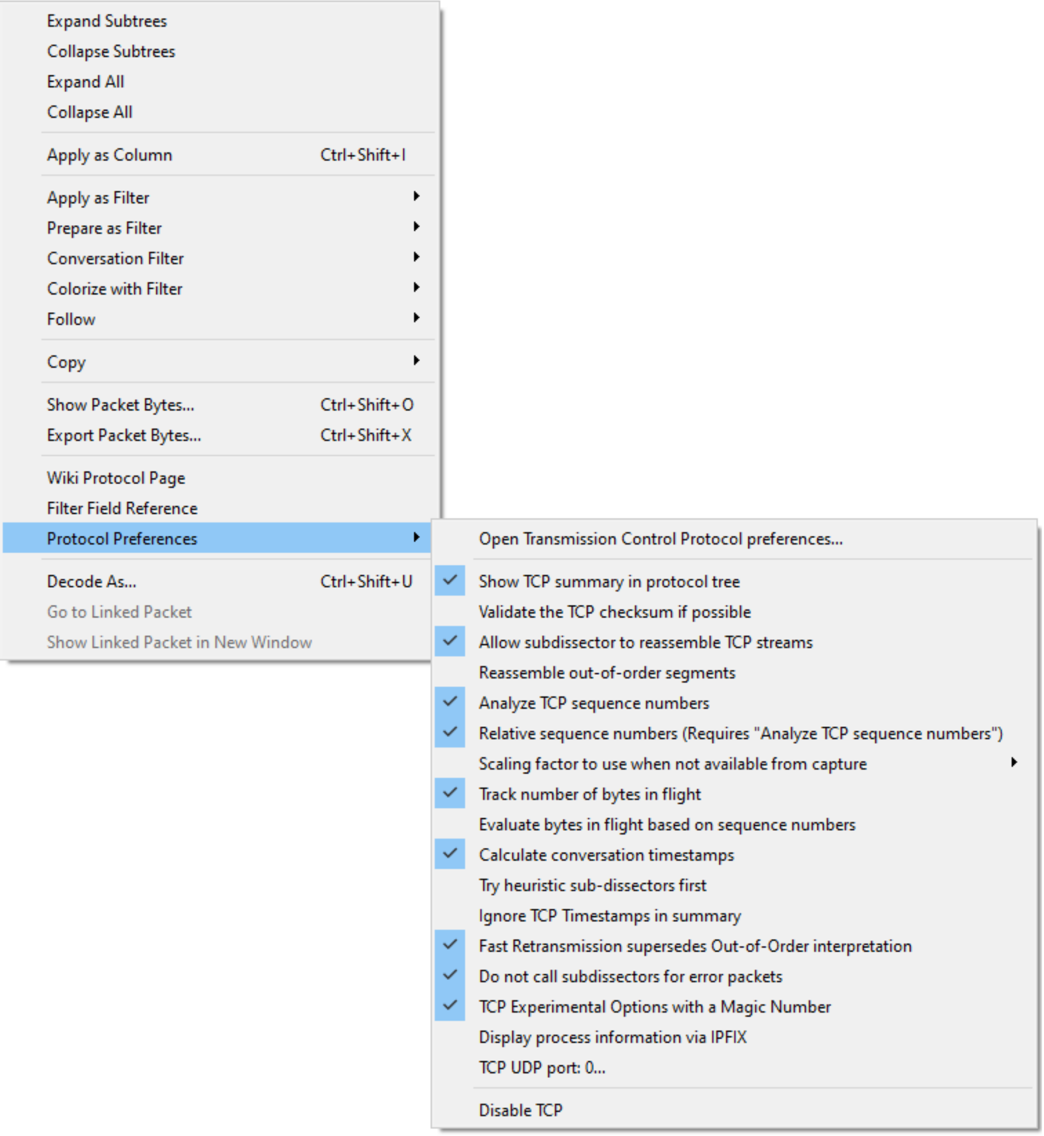
```
No.   Time Source          Destination     Protocol Info
1487 0.0  172.16.133.56   208.92.54.5     TCP      56237 → http(80) [ACK]
4001 0.9  208.92.54.5     172.16.133.56   TCP      [TCP Previous segment
4002 0.0  172.16.133.56   208.92.54.5     TCP      [TCP Dup ACK 1487#1] 5
4005 0.0  208.92.54.5     172.16.133.56   TCP      [TCP Out-Of-Order] htt
4006 0.0  172.16.133.56   208.92.54.5     TCP      56237 → http(80) [ACK]
4007 0.0  208.92.54.5     172.16.133.56   TCP      [TCP Out-Of-Order] htt
4008 0.0  172.16.133.56   208.92.54.5     TCP      56237 → http(80) [ACK]
```

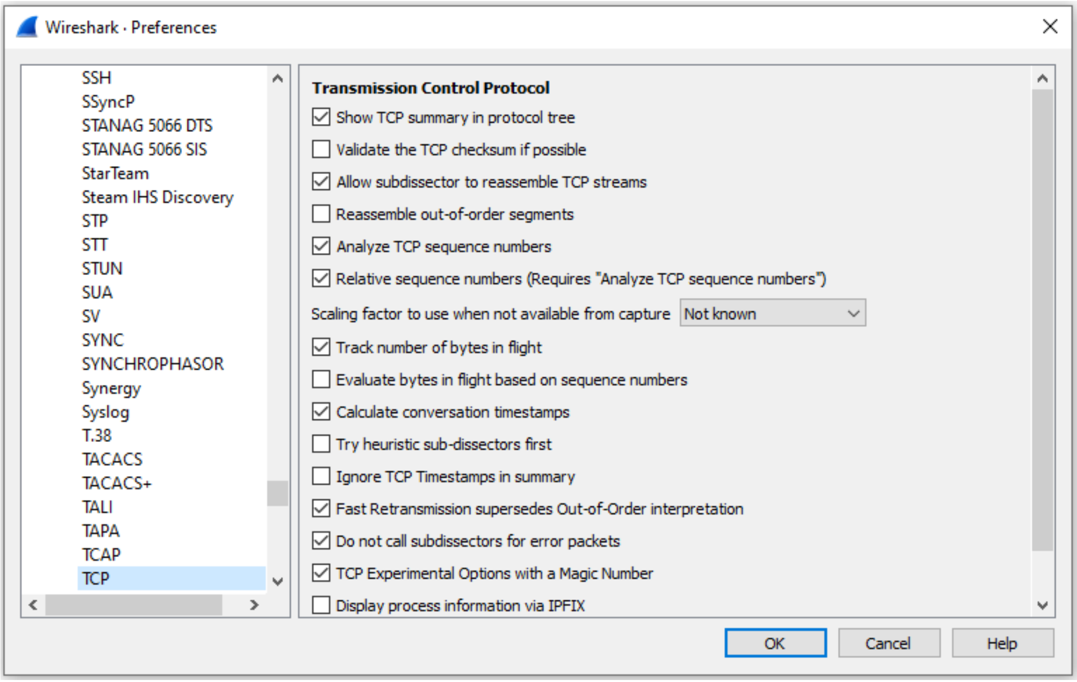


```
◢ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), SACK
   ▷ TCP Option - No-Operation (NOP)
   ▷ TCP Option - No-Operation (NOP)
   ◢ TCP Option - SACK 10852-11096
       Kind: SACK (5)
       Length: 10
       left edge = 10852 (relative)
       right edge = 11096 (relative)
       [TCP SACK Count: 1]
```



```
◢ TCP Option - Timestamps: TSval 1707407197, TSecr 131517608
     Kind: Time Stamp Option (8)
     Length: 10
     Timestamp value: 1707407197
     Timestamp echo reply: 131517608
```


Expand Subtrees
Collapse Subtrees
Expand All
Collapse All
Apply as Column Ctrl+Shift+I
Apply as Filter
Prepare as Filter
Conversation Filter
Colorize with Filter
Follow
Copy
Show Packet Bytes... Ctrl+Shift+O
Export Packet Bytes... Ctrl+Shift+X
Wiki Protocol Page
Filter Field Reference
Protocol Preferences
Decode As... Ctrl+Shift+U
Go to Linked Packet
Show Linked Packet in New Window
Open Transmission Control Protocol preferences...
✓ Show TCP summary in protocol tree
Validate the TCP checksum if possible
✓ Allow subdissector to reassemble TCP streams
Reassemble out-of-order segments
✓ Analyze TCP sequence numbers
✓ Relative sequence numbers (Requires "Analyze TCP sequence numbers")
Scaling factor to use when not available from capture
✓ Track number of bytes in flight
Evaluate bytes in flight based on sequence numbers
✓ Calculate conversation timestamps
Try heuristic sub-dissectors first
Ignore TCP Timestamps in summary
✓ Fast Retransmission supersedes Out-of-Order interpretation
✓ Do not call subdissectors for error packets
✓ TCP Experimental Options with a Magic Number
Display process information via IPFIX
TCP UDP port: 0...
Disable TCP



Transmission Control Protocol

☑ Show TCP summary in protocol tree

□ Validate the TCP checksum if possible

☑ Allow subdissector to reassemble TCP streams

□ Reassemble out-of-order segments

☑ Analyze TCP sequence numbers

☑ Relative sequence numbers (Requires "Analyze TCP sequence numbers")

Scaling factor to use when not available from capture: Not known

☑ Track number of bytes in flight

□ Evaluate bytes in flight based on sequence numbers

☑ Calculate conversation timestamps

□ Try heuristic sub-dissectors first

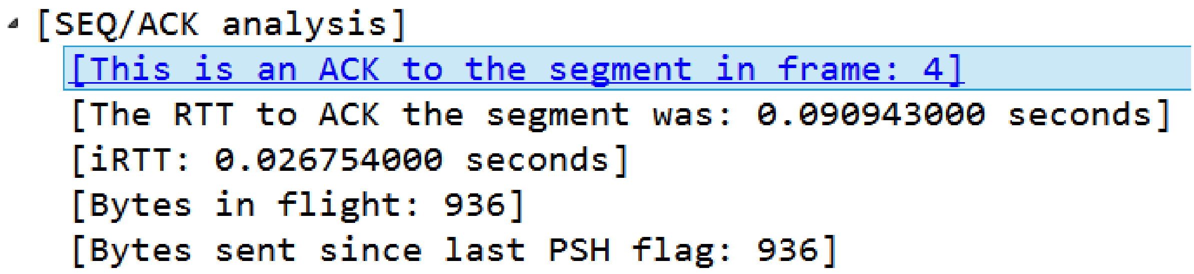
□ Ignore TCP Timestamps in summary

☑ Fast Retransmission supersedes Out-of-Order interpretation

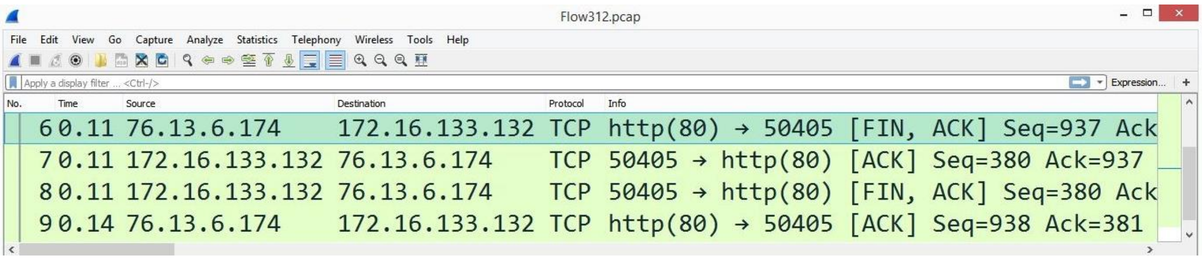
☑ Do not call subdissectors for error packets

☑ TCP Experimental Options with a Magic Number

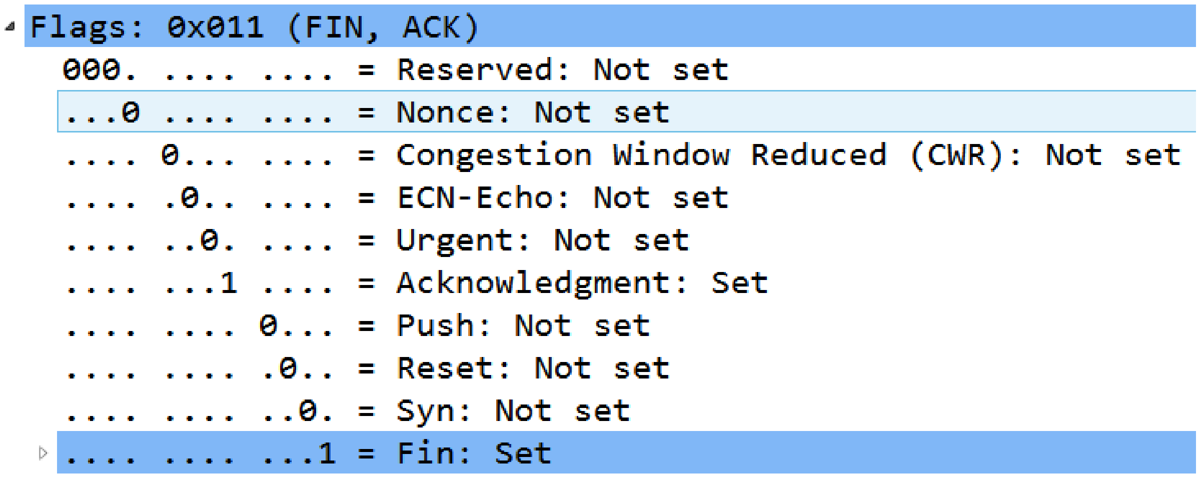
□ Display process information via IPFIX



```
◢ [SEQ/ACK analysis]
    [This is an ACK to the segment in frame: 4]
    [The RTT to ACK the segment was: 0.090943000 seconds]
    [iRTT: 0.026754000 seconds]
    [Bytes in flight: 936]
    [Bytes sent since last PSH flag: 936]
```

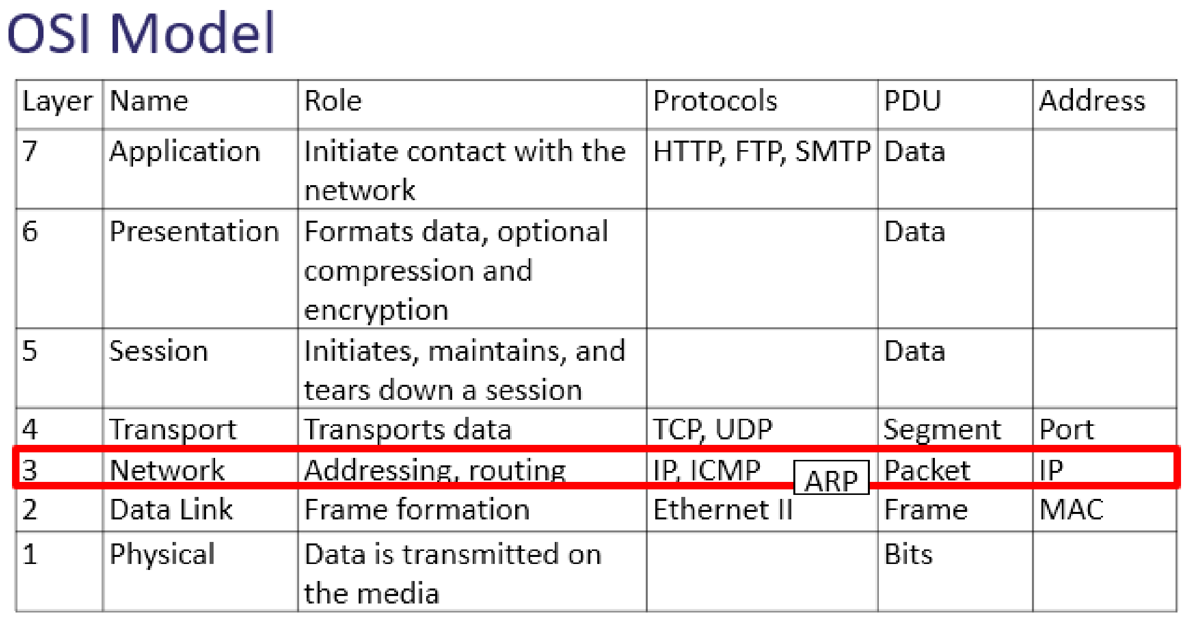

Flow312.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
+

```
No. Time Source         Destination    Protocol Info
6   0.11 76.13.6.174    172.16.133.132 TCP http(80) → 50405 [FIN, ACK] Seq=937 Ack
7   0.11 172.16.133.132 76.13.6.174    TCP 50405 → http(80) [ACK] Seq=380 Ack=937
8   0.11 172.16.133.132 76.13.6.174    TCP 50405 → http(80) [FIN, ACK] Seq=380 Ack
9   0.14 76.13.6.174    172.16.133.132 TCP http(80) → 50405 [ACK] Seq=938 Ack=381
```



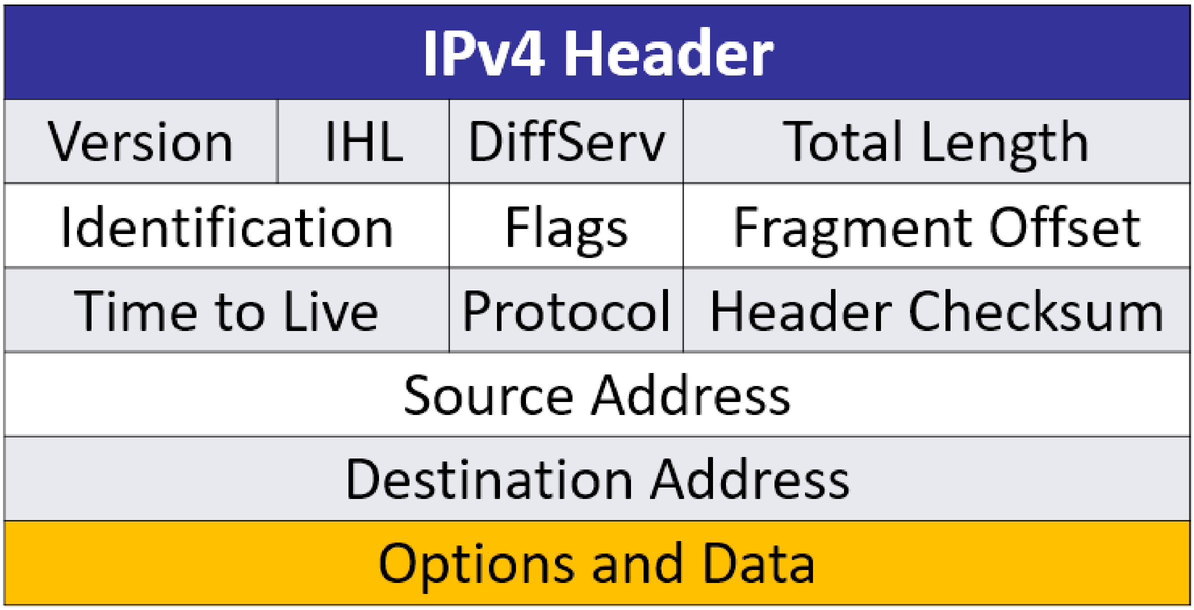
```
◢ Flags: 0x011 (FIN, ACK)
    000. .... .... = Reserved: Not set
    ...0 .... .... = Nonce: Not set
    .... 0... .... = Congestion Window Reduced (CWR): Not set
    .... .0.. .... = ECN-Echo: Not set
    .... ..0. .... = Urgent: Not set
    .... ...1 .... = Acknowledgment: Set
    .... .... 0... = Push: Not set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
  ▷ .... .... ...1 = Fin: Set
```

Chapter 11: Analyzing IPv4 and IPv6

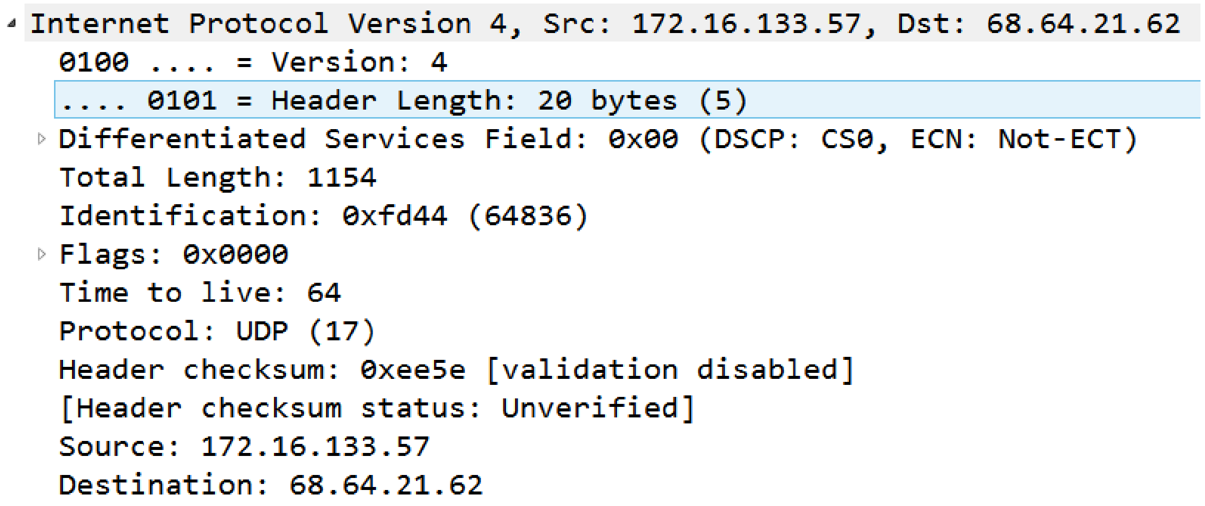


OSI Model

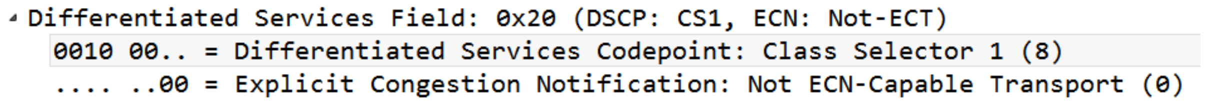
Layer	Name	Role	Protocols	PDU	Address
7	Application	Initiate contact with the network	HTTP, FTP, SMTP	Data	
6	Presentation	Formats data, optional compression and encryption		Data	
5	Session	Initiates, maintains, and tears down a session		Data	
4	Transport	Transports data	TCP, UDP	Segment	Port
3	Network	Addressing, routing	IP, ICMP ARP	Packet	IP
2	Data Link	Frame formation	Ethernet II	Frame	MAC
1	Physical	Data is transmitted on the media		Bits	



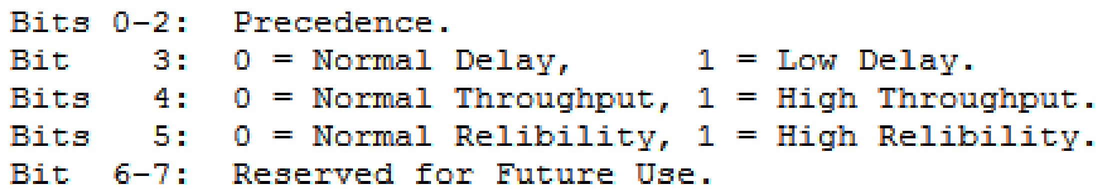
<table>
<tr><th colspan="4">IPv4 Header</th></tr>
<tr><td>Version</td><td>IHL</td><td>DiffServ</td><td>Total Length</td></tr>
<tr><td colspan="2">Identification</td><td>Flags</td><td>Fragment Offset</td></tr>
<tr><td colspan="2">Time to Live</td><td>Protocol</td><td>Header Checksum</td></tr>
<tr><td colspan="4">Source Address</td></tr>
<tr><td colspan="4">Destination Address</td></tr>
<tr><td colspan="4">Options and Data</td></tr>
</table>



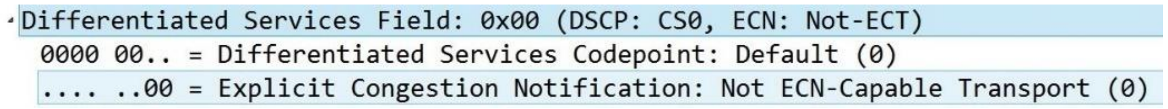
```
◢ Internet Protocol Version 4, Src: 172.16.133.57, Dst: 68.64.21.62
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▷ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1154
    Identification: 0xfd44 (64836)
  ▷ Flags: 0x0000
    Time to live: 64
    Protocol: UDP (17)
    Header checksum: 0xee5e [validation disabled]
    [Header checksum status: Unverified]
    Source: 172.16.133.57
    Destination: 68.64.21.62
```



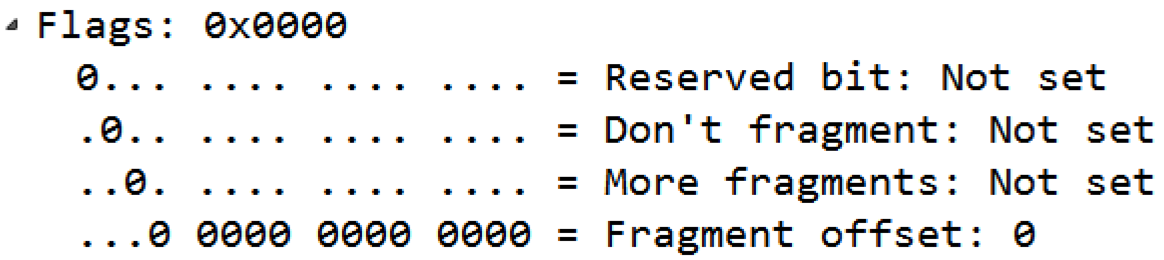
```
◢ Differentiated Services Field: 0x20 (DSCP: CS1, ECN: Not-ECT)
    0010 00.. = Differentiated Services Codepoint: Class Selector 1 (8)
    .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
```



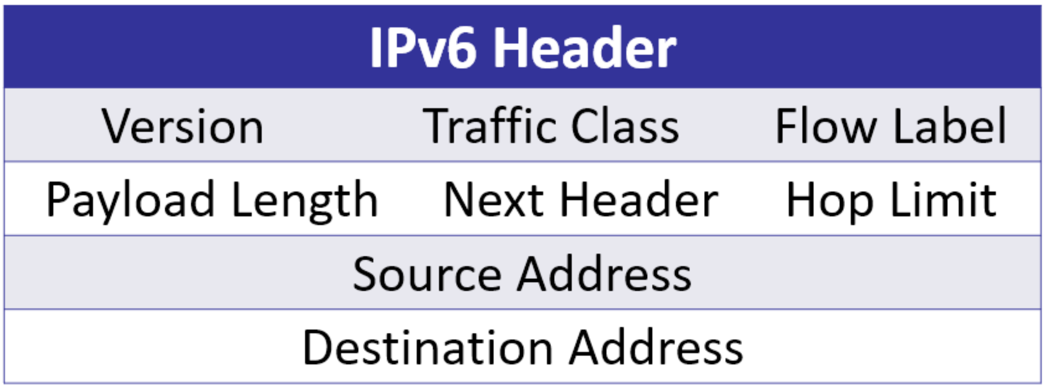
```
Bits 0-2:  Precedence.
Bit    3:  0 = Normal Delay,       1 = Low Delay.
Bits   4:  0 = Normal Throughput,  1 = High Throughput.
Bits   5:  0 = Normal Relibility,  1 = High Relibility.
Bit  6-7:  Reserved for Future Use.
```



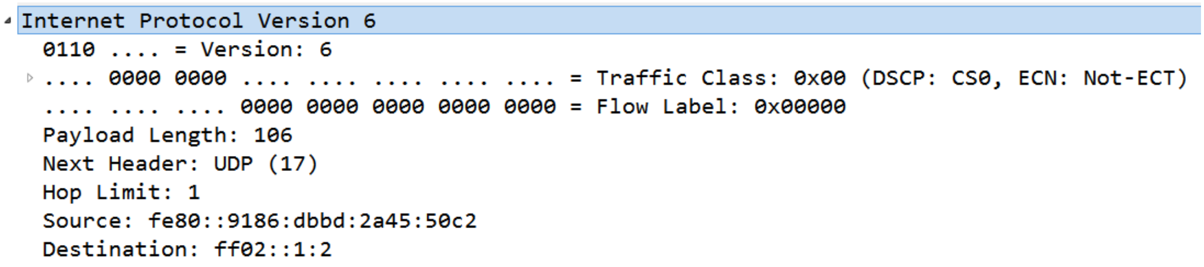
```
◢ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    0000 00.. = Differentiated Services Codepoint: Default (0)
    .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
```



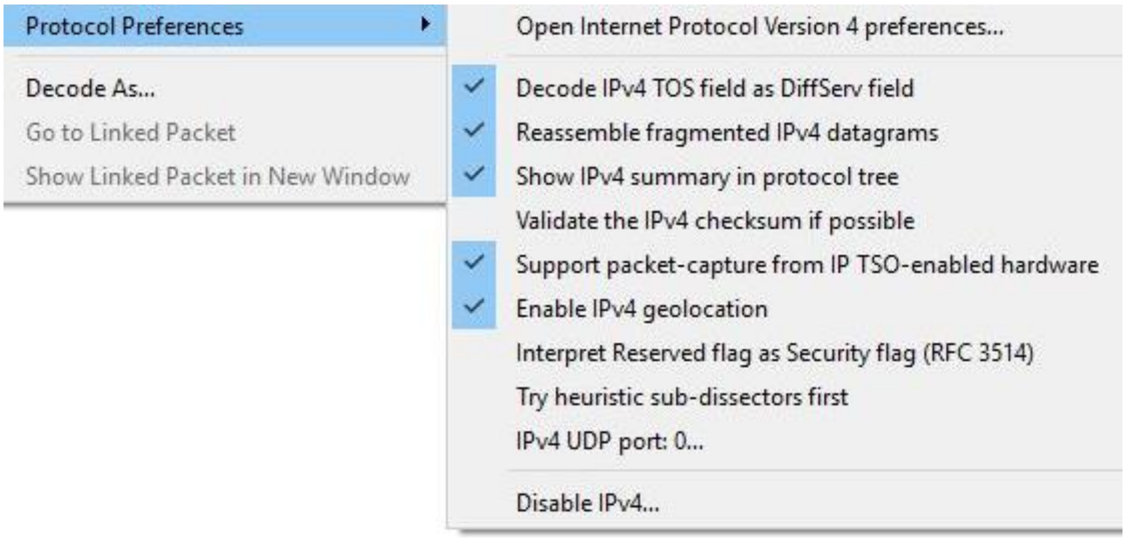
```
◢ Flags: 0x0000
    0... .... .... .... = Reserved bit: Not set
    .0.. .... .... .... = Don't fragment: Not set
    ..0. .... .... .... = More fragments: Not set
    ...0 0000 0000 0000 = Fragment offset: 0
```

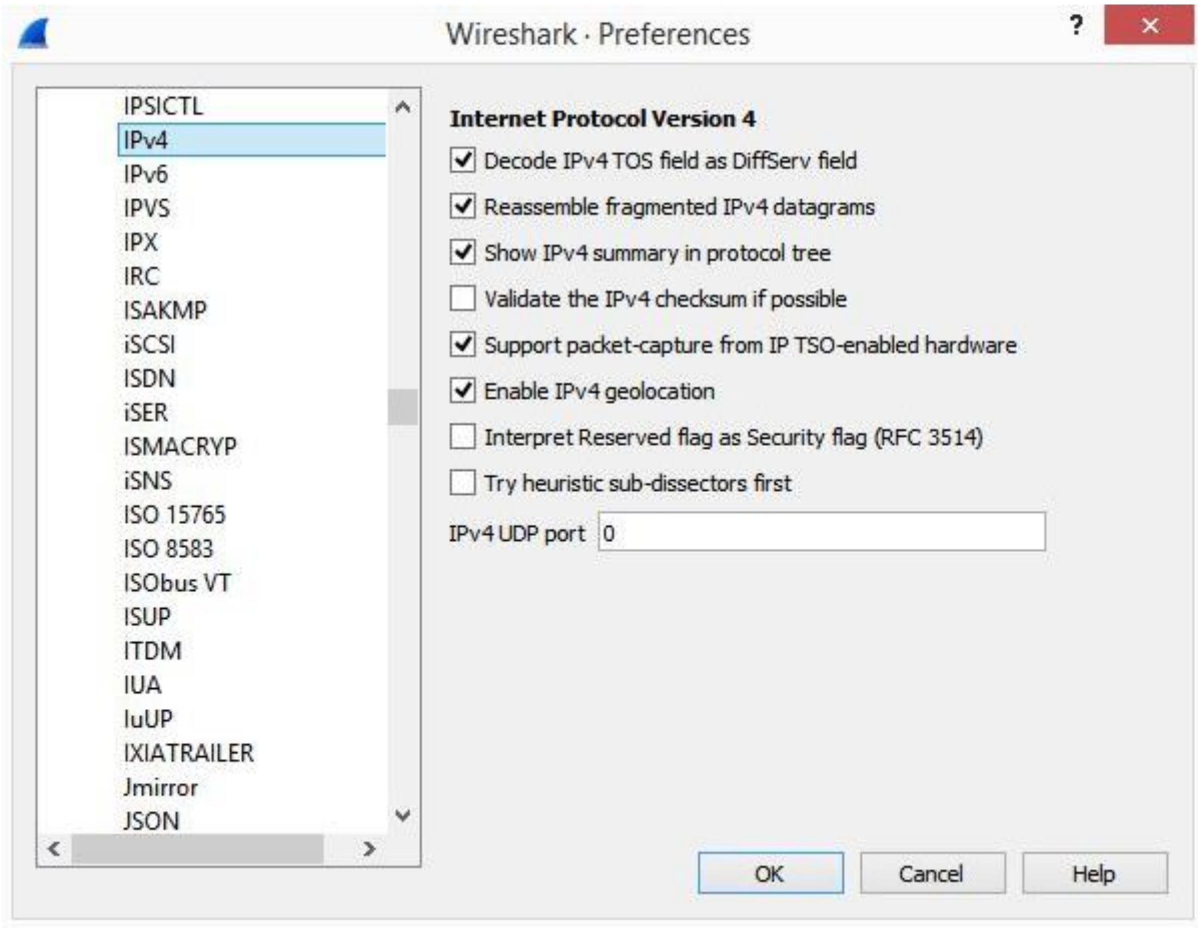


IPv6 Header		
Version	Traffic Class	Flow Label
Payload Length	Next Header	Hop Limit
Source Address		
Destination Address		



```
◂ Internet Protocol Version 6
    0110 .... = Version: 6
  ▹ .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... .... .... 0000 0000 0000 0000 0000 = Flow Label: 0x00000
    Payload Length: 106
    Next Header: UDP (17)
    Hop Limit: 1
    Source: fe80::9186:dbbd:2a45:50c2
    Destination: ff02::1:2
```


Protocol Preferences ▸
Decode As...
Go to Linked Packet
Show Linked Packet in New Window
Open Internet Protocol Version 4 preferences...
✓ Decode IPv4 TOS field as DiffServ field
✓ Reassemble fragmented IPv4 datagrams
✓ Show IPv4 summary in protocol tree
Validate the IPv4 checksum if possible
✓ Support packet-capture from IP TSO-enabled hardware
✓ Enable IPv4 geolocation
Interpret Reserved flag as Security flag (RFC 3514)
Try heuristic sub-dissectors first
IPv4 UDP port: 0...
Disable IPv4...



Internet Protocol Version 4

☑ Decode IPv4 TOS field as DiffServ field

☑ Reassemble fragmented IPv4 datagrams

☑ Show IPv4 summary in protocol tree

☐ Validate the IPv4 checksum if possible

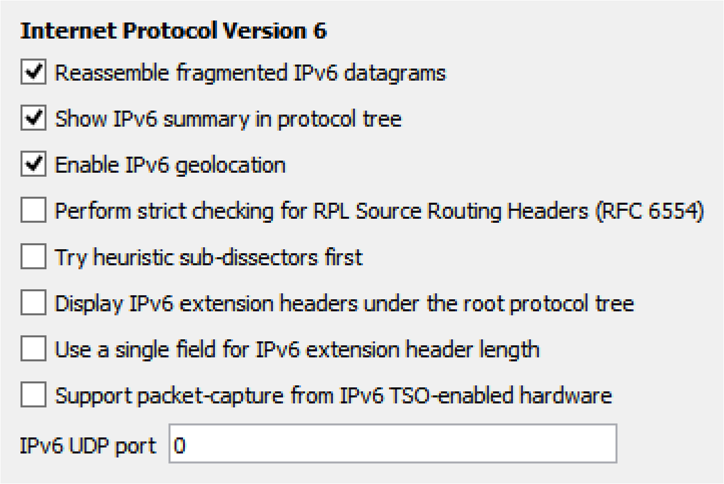
☑ Support packet-capture from IP TSO-enabled hardware

☑ Enable IPv4 geolocation

☐ Interpret Reserved flag as Security flag (RFC 3514)

☐ Try heuristic sub-dissectors first

IPv4 UDP port 0



Internet Protocol Version 6

☑ Reassemble fragmented IPv6 datagrams

☑ Show IPv6 summary in protocol tree

☑ Enable IPv6 geolocation

□ Perform strict checking for RPL Source Routing Headers (RFC 6554)

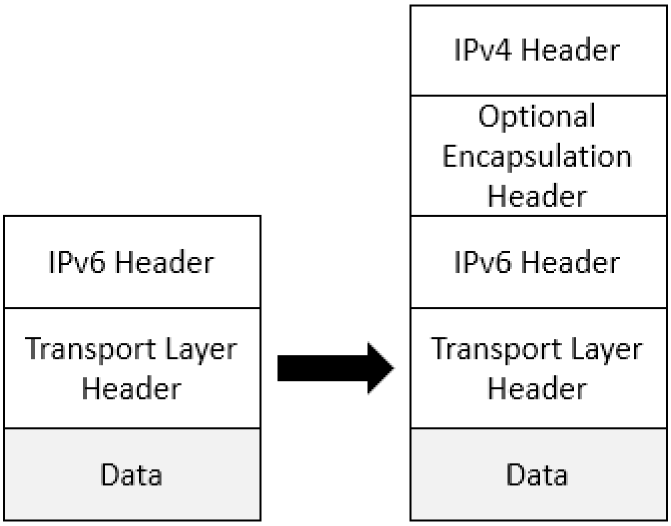
□ Try heuristic sub-dissectors first

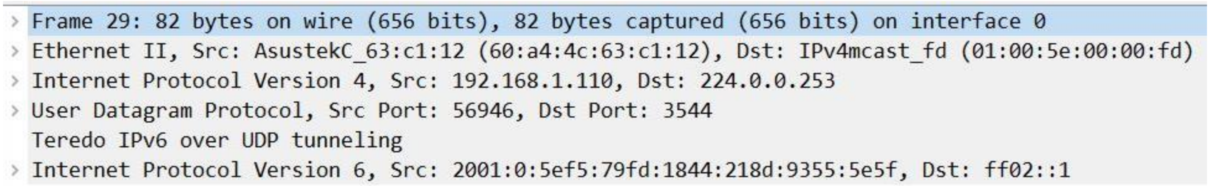
□ Display IPv6 extension headers under the root protocol tree

□ Use a single field for IPv6 extension header length

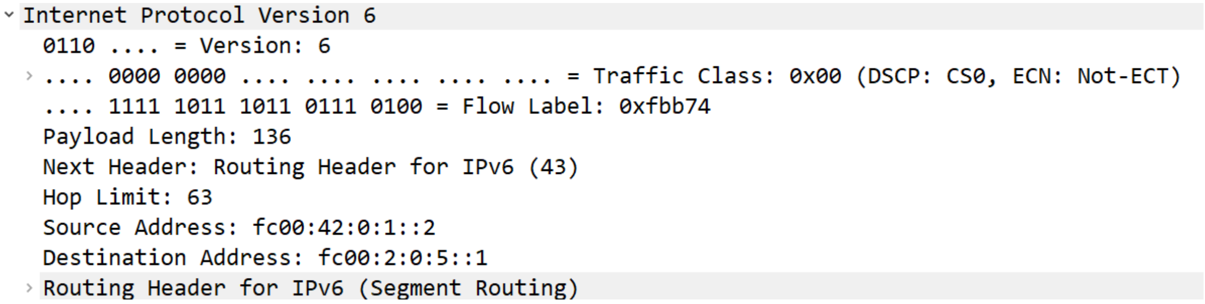
□ Support packet-capture from IPv6 TSO-enabled hardware

IPv6 UDP port: 0



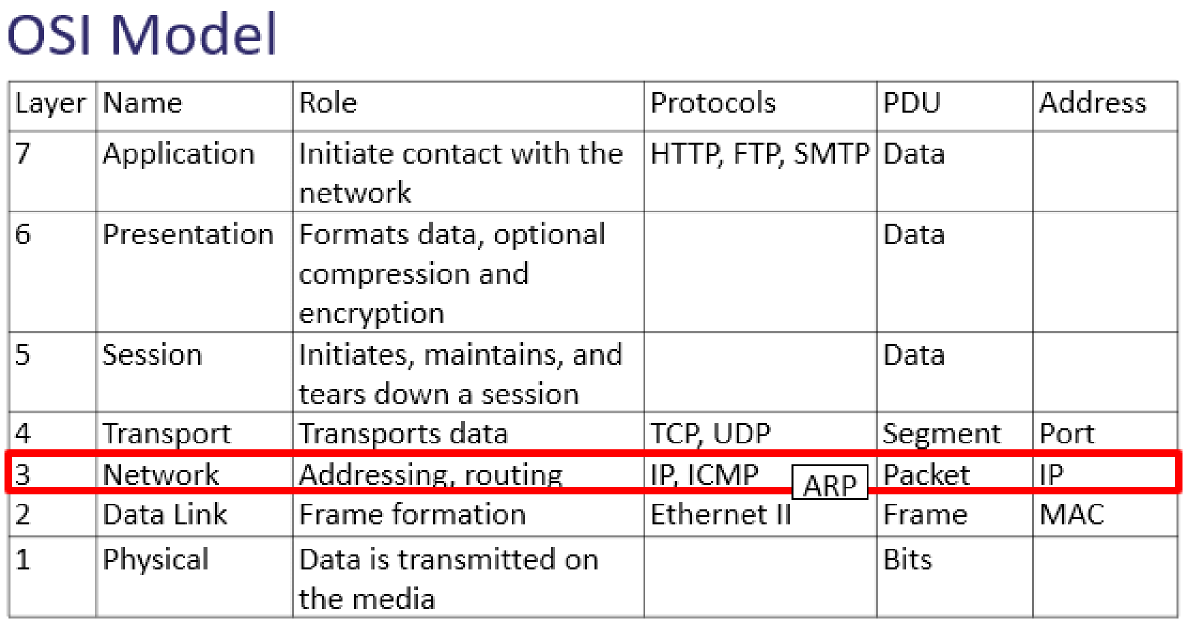


```
› Frame 29: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface 0
› Ethernet II, Src: AsustekC_63:c1:12 (60:a4:4c:63:c1:12), Dst: IPv4mcast_fd (01:00:5e:00:00:fd)
› Internet Protocol Version 4, Src: 192.168.1.110, Dst: 224.0.0.253
› User Datagram Protocol, Src Port: 56946, Dst Port: 3544
  Teredo IPv6 over UDP tunneling
› Internet Protocol Version 6, Src: 2001:0:5ef5:79fd:1844:218d:9355:5e5f, Dst: ff02::1
```



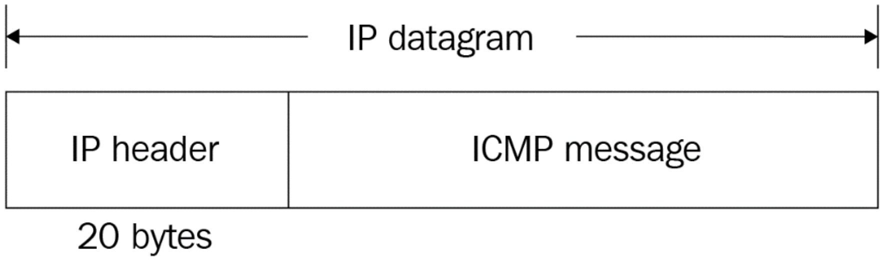
```
⌄ Internet Protocol Version 6
    0110 .... = Version: 6
  › .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... 1111 1011 1011 0111 0100 = Flow Label: 0xfbb74
    Payload Length: 136
    Next Header: Routing Header for IPv6 (43)
    Hop Limit: 63
    Source Address: fc00:42:0:1::2
    Destination Address: fc00:2:0:5::1
  › Routing Header for IPv6 (Segment Routing)
```

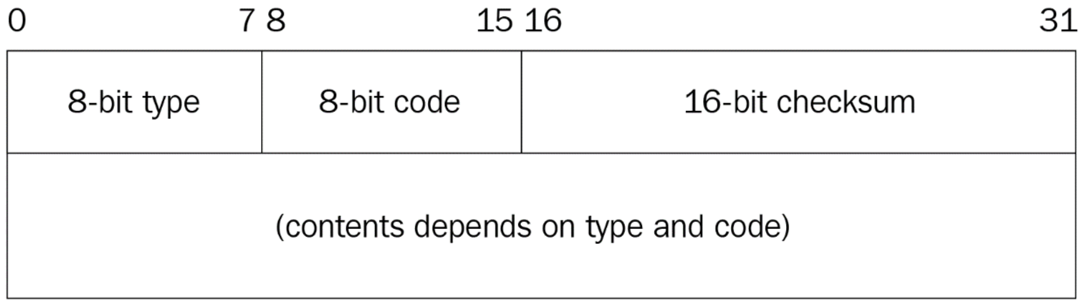
Chapter 12: Discovering ICMP

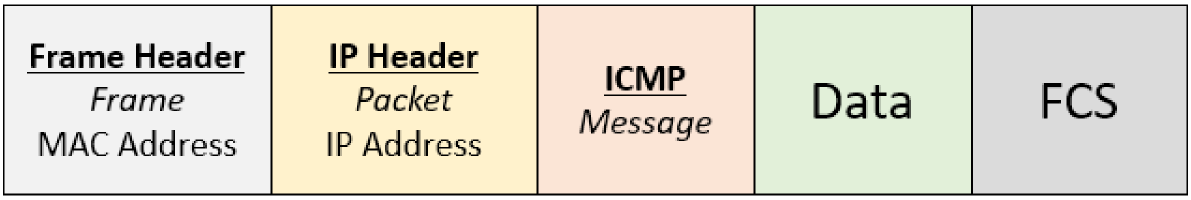


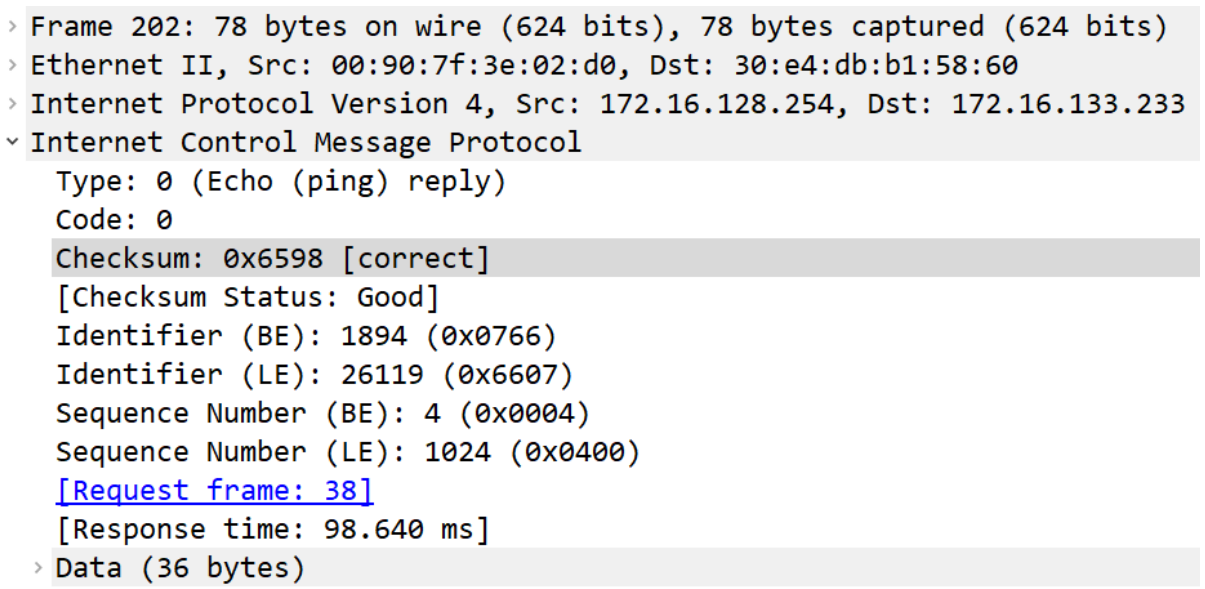
OSI Model

Layer	Name	Role	Protocols	PDU	Address
7	Application	Initiate contact with the network	HTTP, FTP, SMTP	Data	
6	Presentation	Formats data, optional compression and encryption		Data	
5	Session	Initiates, maintains, and tears down a session		Data	
4	Transport	Transports data	TCP, UDP	Segment	Port
3	Network	Addressing, routing	IP, ICMP ARP	Packet	IP
2	Data Link	Frame formation	Ethernet II	Frame	MAC
1	Physical	Data is transmitted on the media		Bits	

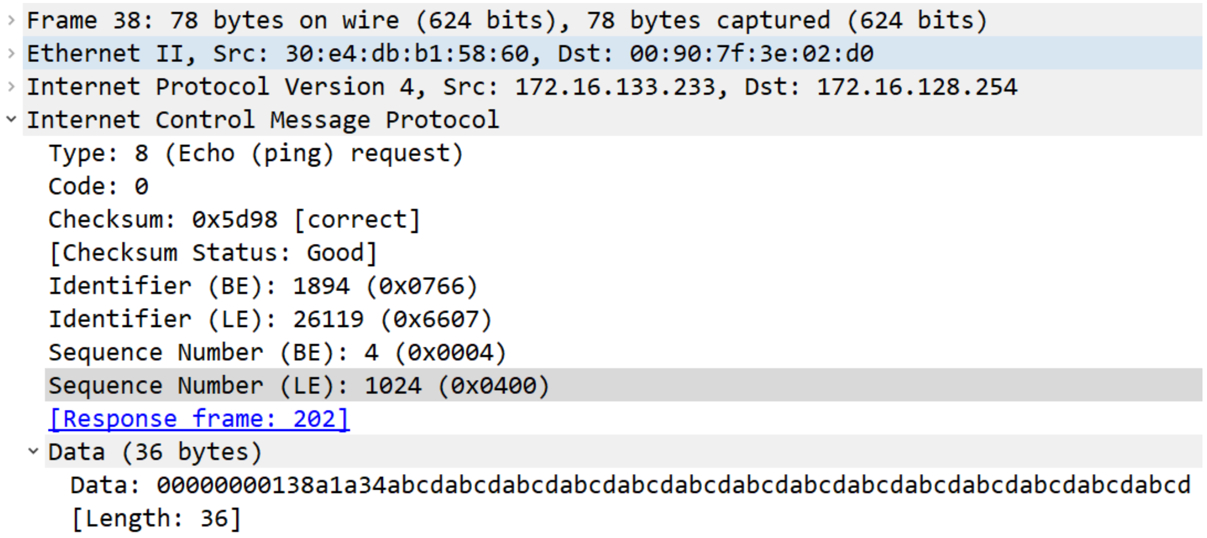




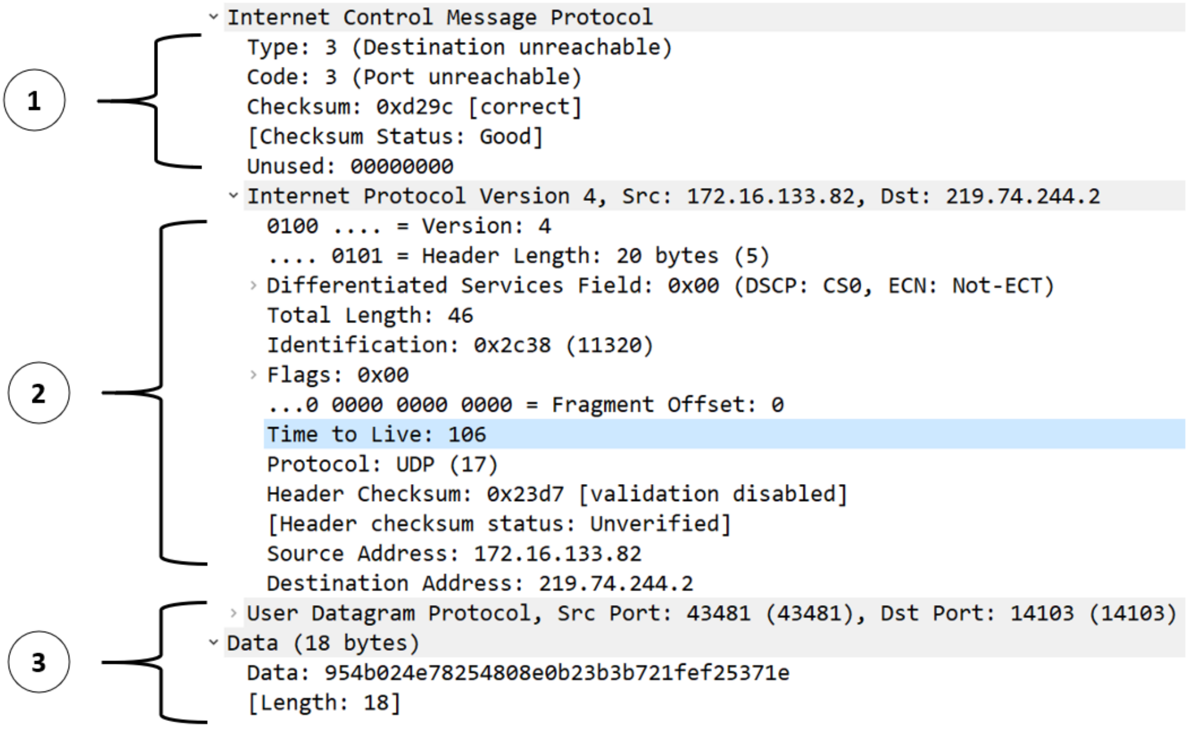




```
› Frame 202: 78 bytes on wire (624 bits), 78 bytes captured (624 bits)
› Ethernet II, Src: 00:90:7f:3e:02:d0, Dst: 30:e4:db:b1:58:60
› Internet Protocol Version 4, Src: 172.16.128.254, Dst: 172.16.133.233
⌄ Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x6598 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1894 (0x0766)
    Identifier (LE): 26119 (0x6607)
    Sequence Number (BE): 4 (0x0004)
    Sequence Number (LE): 1024 (0x0400)
    [Request frame: 38]
    [Response time: 98.640 ms]
  › Data (36 bytes)
```

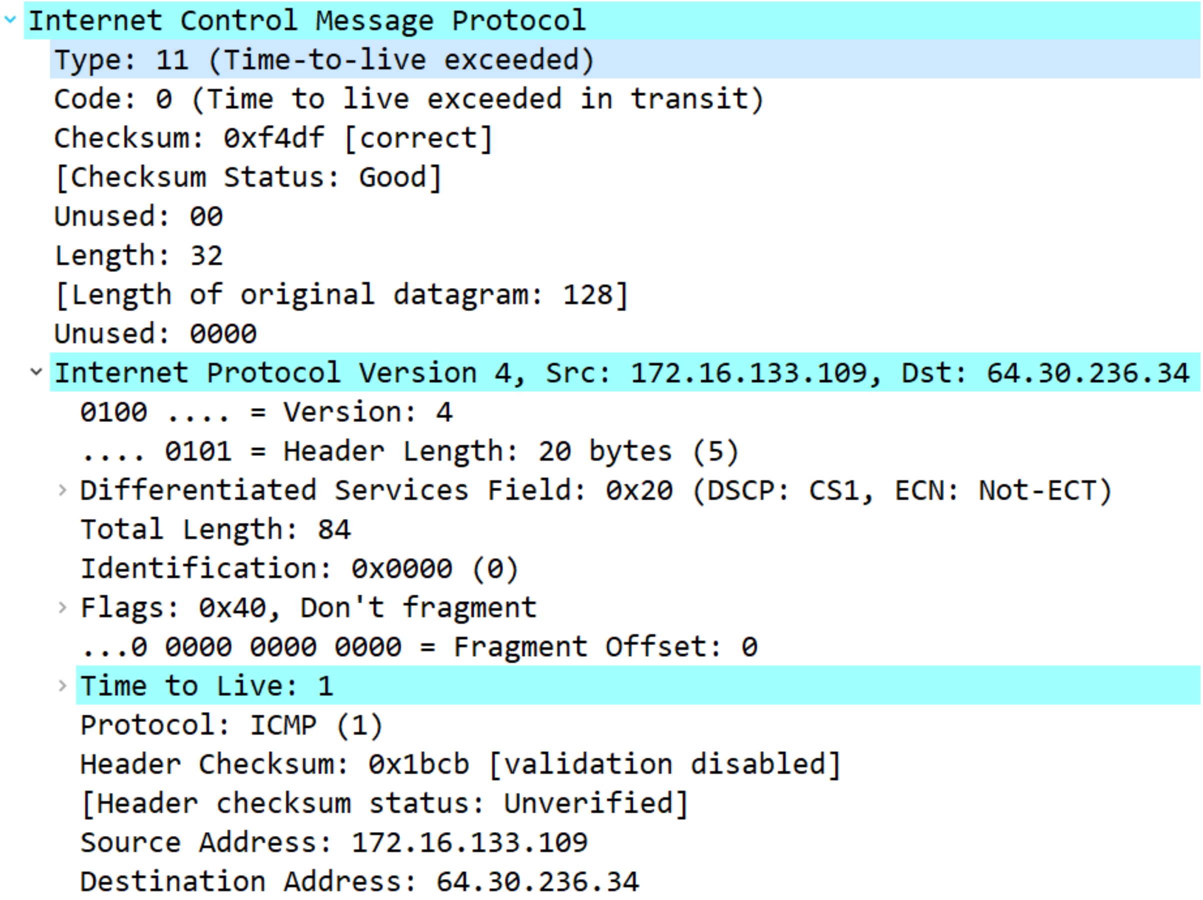


```
› Frame 38: 78 bytes on wire (624 bits), 78 bytes captured (624 bits)
› Ethernet II, Src: 30:e4:db:b1:58:60, Dst: 00:90:7f:3e:02:d0
› Internet Protocol Version 4, Src: 172.16.133.233, Dst: 172.16.128.254
⌄ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x5d98 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1894 (0x0766)
    Identifier (LE): 26119 (0x6607)
    Sequence Number (BE): 4 (0x0004)
    Sequence Number (LE): 1024 (0x0400)
    [Response frame: 202]
  ⌄ Data (36 bytes)
      Data: 00000000138a1a34abcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcd
      [Length: 36]
```

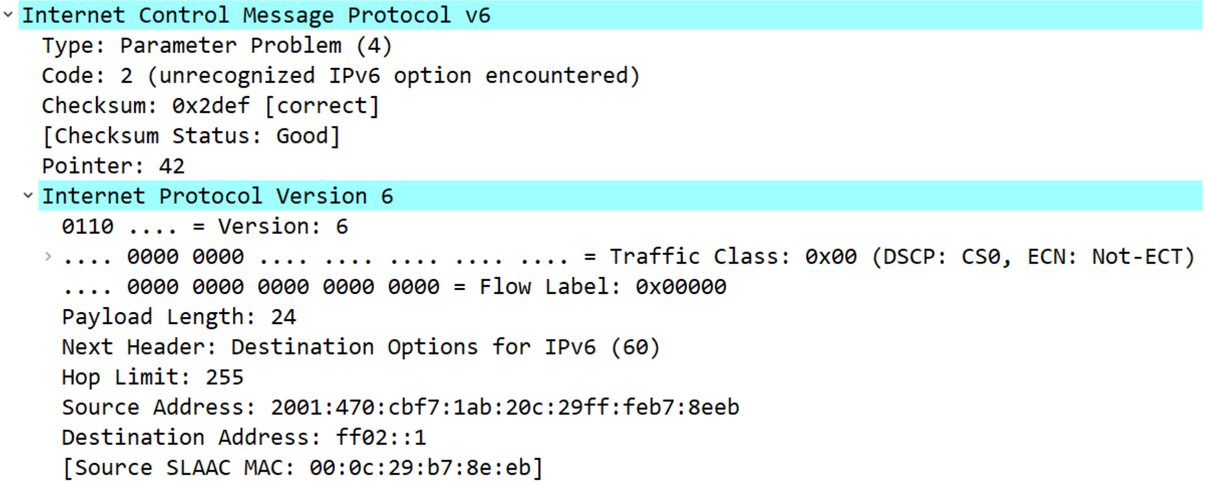


```
⌄ Internet Control Message Protocol
    Type: 3 (Destination unreachable)
    Code: 3 (Port unreachable)
    Checksum: 0xd29c [correct]
    [Checksum Status: Good]
    Unused: 00000000
  ⌄ Internet Protocol Version 4, Src: 172.16.133.82, Dst: 219.74.244.2
      0100 .... = Version: 4
      .... 0101 = Header Length: 20 bytes (5)
    › Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      Total Length: 46
      Identification: 0x2c38 (11320)
    › Flags: 0x00
      ...0 0000 0000 0000 = Fragment Offset: 0
      Time to Live: 106
      Protocol: UDP (17)
      Header Checksum: 0x23d7 [validation disabled]
      [Header checksum status: Unverified]
      Source Address: 172.16.133.82
      Destination Address: 219.74.244.2
  › User Datagram Protocol, Src Port: 43481 (43481), Dst Port: 14103 (14103)
⌄ Data (18 bytes)
    Data: 954b024e78254808e0b23b3b721fef25371e
    [Length: 18]
```

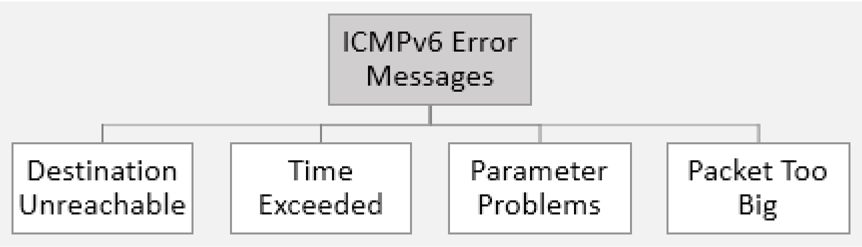
ICMP Messages				
Error Reporting			Queries	
Type	*Message*		Type	*Message*
3	Destination unreachable		8/0	Echo Request/Reply
11	Time exceeded		9	Router Advertisement
5	Parameter problem			

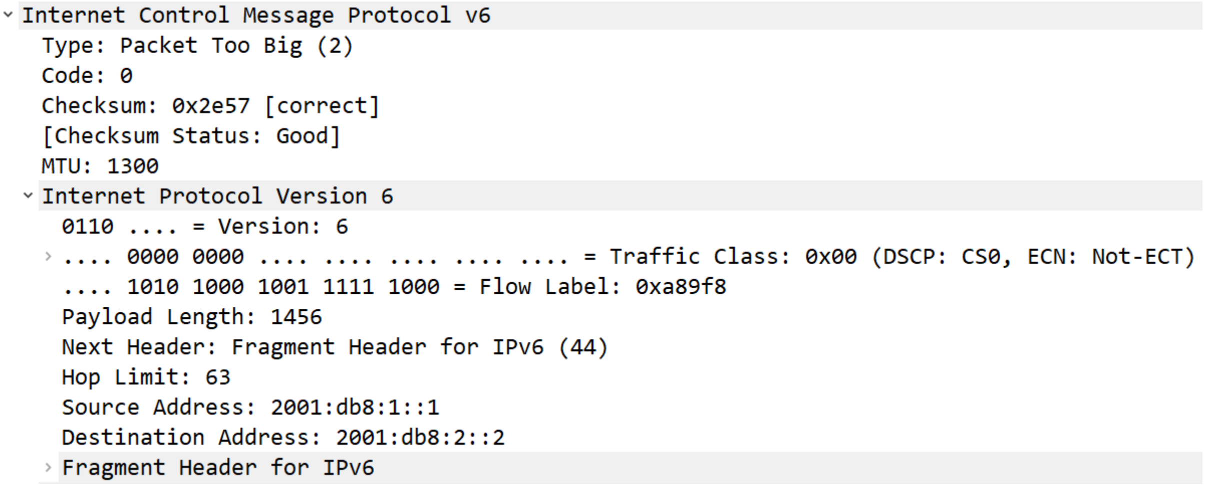


```
Internet Control Message Protocol
  Type: 11 (Time-to-live exceeded)
  Code: 0 (Time to live exceeded in transit)
  Checksum: 0xf4df [correct]
  [Checksum Status: Good]
  Unused: 00
  Length: 32
  [Length of original datagram: 128]
  Unused: 0000
  Internet Protocol Version 4, Src: 172.16.133.109, Dst: 64.30.236.34
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x20 (DSCP: CS1, ECN: Not-ECT)
    Total Length: 84
    Identification: 0x0000 (0)
    Flags: 0x40, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 1
    Protocol: ICMP (1)
    Header Checksum: 0x1bcb [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 172.16.133.109
    Destination Address: 64.30.236.34
```

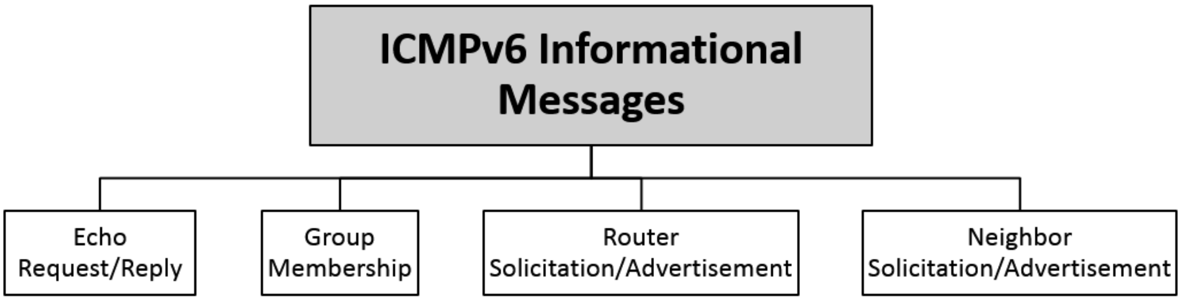


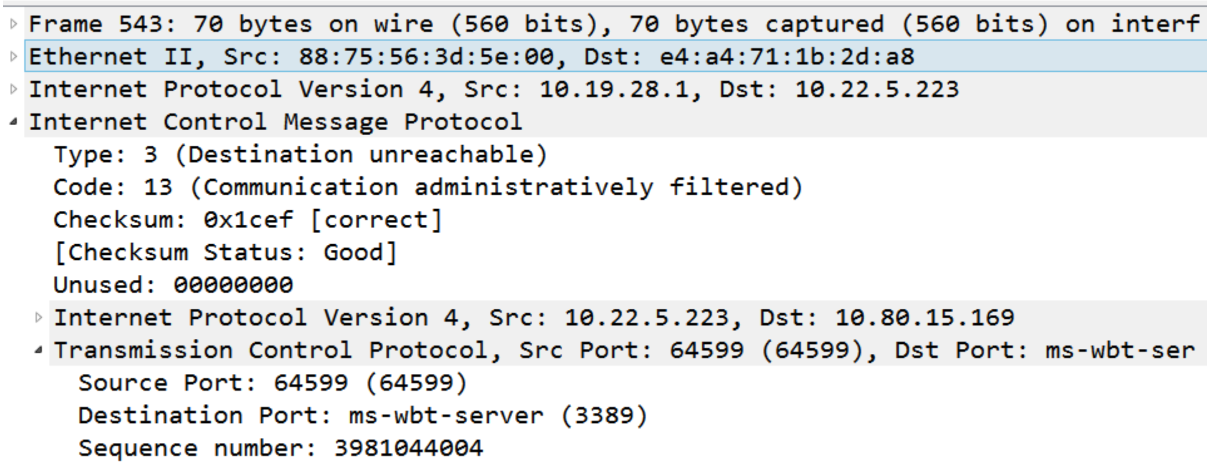
```
Internet Control Message Protocol v6
  Type: Parameter Problem (4)
  Code: 2 (unrecognized IPv6 option encountered)
  Checksum: 0x2def [correct]
  [Checksum Status: Good]
  Pointer: 42
  Internet Protocol Version 6
    0110 .... = Version: 6
    .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... 0000 0000 0000 0000 0000 = Flow Label: 0x00000
    Payload Length: 24
    Next Header: Destination Options for IPv6 (60)
    Hop Limit: 255
    Source Address: 2001:470:cbf7:1ab:20c:29ff:feb7:8eeb
    Destination Address: ff02::1
    [Source SLAAC MAC: 00:0c:29:b7:8e:eb]
```



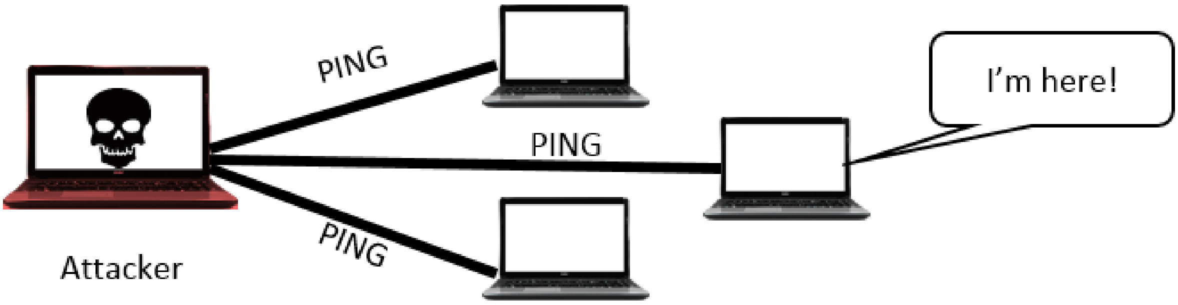


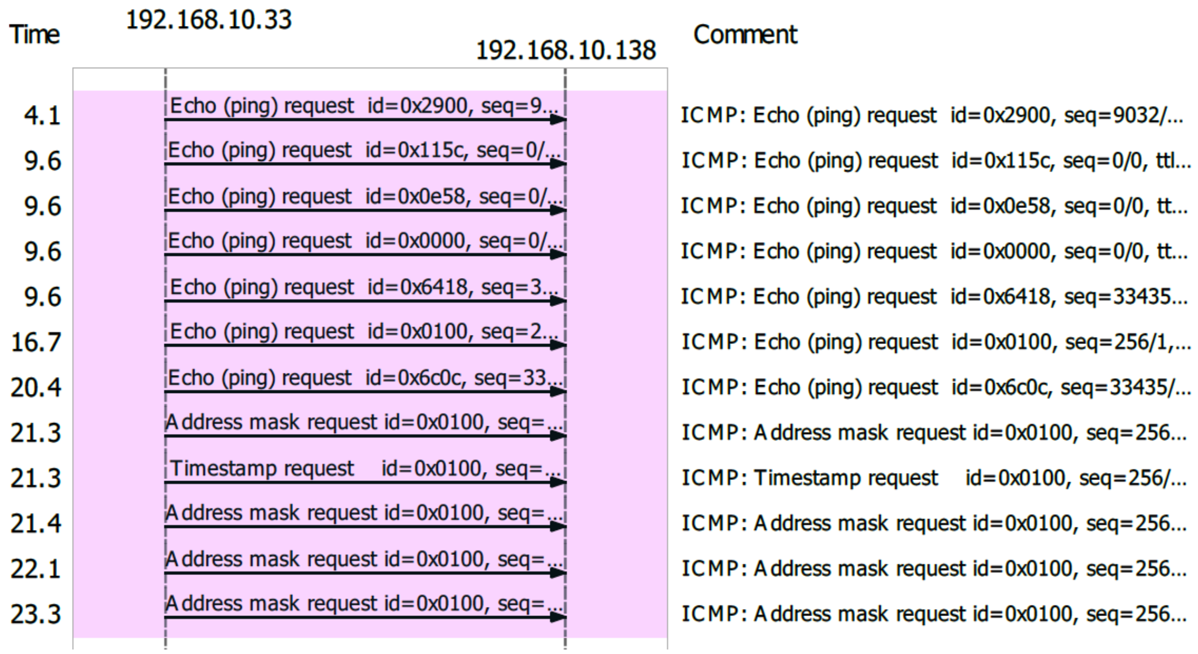
```
Internet Control Message Protocol v6
  Type: Packet Too Big (2)
  Code: 0
  Checksum: 0x2e57 [correct]
  [Checksum Status: Good]
  MTU: 1300
  Internet Protocol Version 6
    0110 .... = Version: 6
    .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... 1010 1000 1001 1111 1000 = Flow Label: 0xa89f8
    Payload Length: 1456
    Next Header: Fragment Header for IPv6 (44)
    Hop Limit: 63
    Source Address: 2001:db8:1::1
    Destination Address: 2001:db8:2::2
    Fragment Header for IPv6
```


ICMPv6 Informational Messages
Echo Request/Reply
Group Membership
Router Solicitation/Advertisement
Neighbor Solicitation/Advertisement

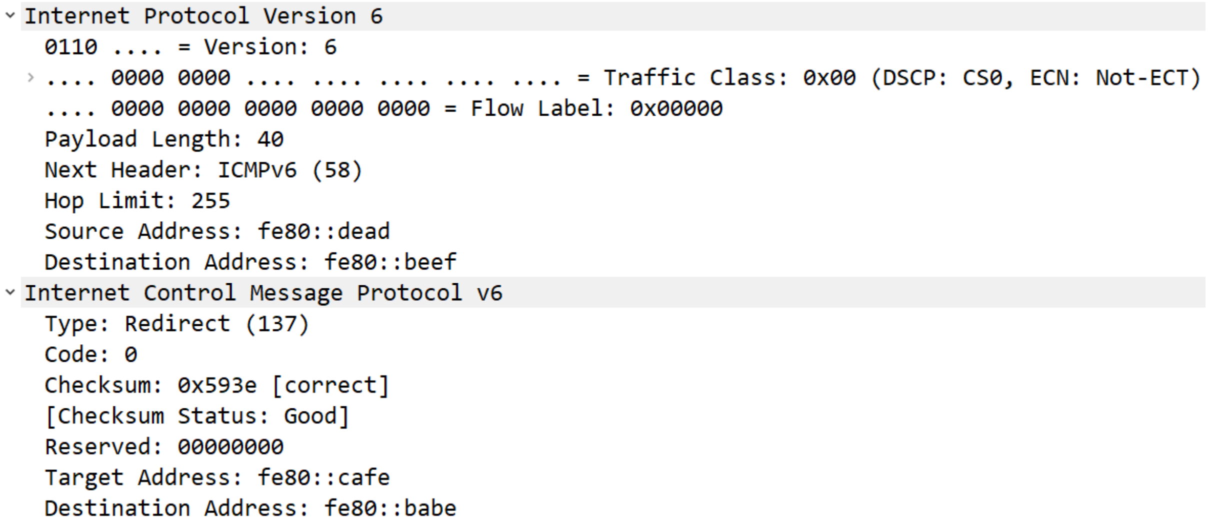


```
Frame 543: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interf
Ethernet II, Src: 88:75:56:3d:5e:00, Dst: e4:a4:71:1b:2d:a8
Internet Protocol Version 4, Src: 10.19.28.1, Dst: 10.22.5.223
Internet Control Message Protocol
  Type: 3 (Destination unreachable)
  Code: 13 (Communication administratively filtered)
  Checksum: 0x1cef [correct]
  [Checksum Status: Good]
  Unused: 00000000
  Internet Protocol Version 4, Src: 10.22.5.223, Dst: 10.80.15.169
  Transmission Control Protocol, Src Port: 64599 (64599), Dst Port: ms-wbt-ser
    Source Port: 64599 (64599)
    Destination Port: ms-wbt-server (3389)
    Sequence number: 3981044004
```

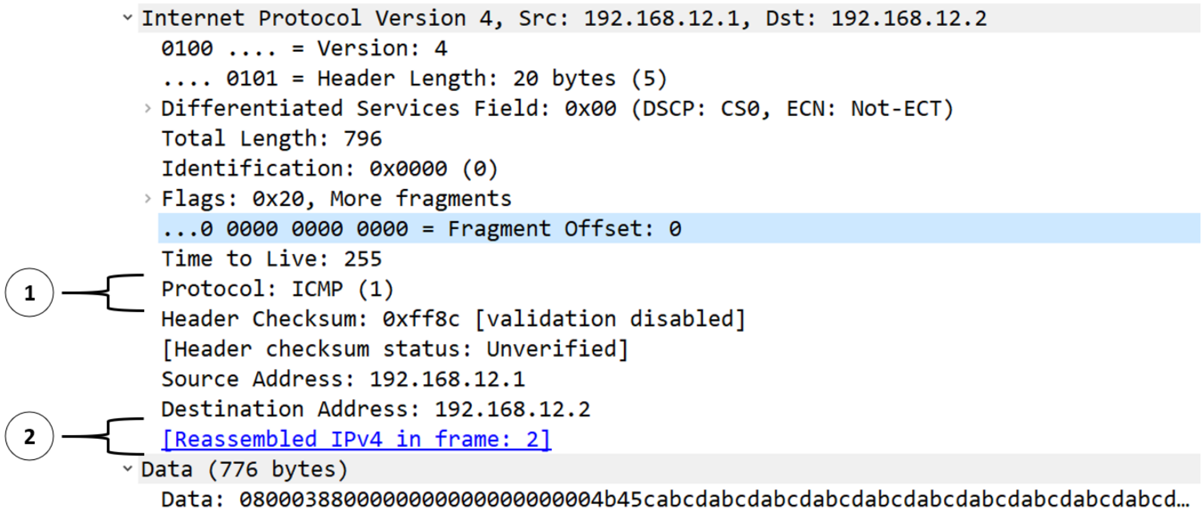




```
Time     192.168.10.33                                192.168.10.138    Comment

4.1      Echo (ping) request  id=0x2900, seq=9...                     ICMP: Echo (ping) request  id=0x2900, seq=9032/...
9.6      Echo (ping) request  id=0x115c, seq=0/...                    ICMP: Echo (ping) request  id=0x115c, seq=0/0, ttl...
9.6      Echo (ping) request  id=0x0e58, seq=0/...                    ICMP: Echo (ping) request  id=0x0e58, seq=0/0, tt...
9.6      Echo (ping) request  id=0x0000, seq=0/...                    ICMP: Echo (ping) request  id=0x0000, seq=0/0, tt...
9.6      Echo (ping) request  id=0x6418, seq=3...                     ICMP: Echo (ping) request  id=0x6418, seq=33435...
16.7     Echo (ping) request  id=0x0100, seq=2...                     ICMP: Echo (ping) request  id=0x0100, seq=256/1,...
20.4     Echo (ping) request  id=0x6c0c, seq=33...                    ICMP: Echo (ping) request  id=0x6c0c, seq=33435/...
21.3     Address mask request id=0x0100, seq=...                      ICMP: Address mask request id=0x0100, seq=256...
21.3     Timestamp request    id=0x0100, seq=...                      ICMP: Timestamp request    id=0x0100, seq=256/...
21.4     Address mask request id=0x0100, seq=...                      ICMP: Address mask request id=0x0100, seq=256...
22.1     Address mask request id=0x0100, seq=...                      ICMP: Address mask request id=0x0100, seq=256...
23.3     Address mask request id=0x0100, seq=...                      ICMP: Address mask request id=0x0100, seq=256...
```

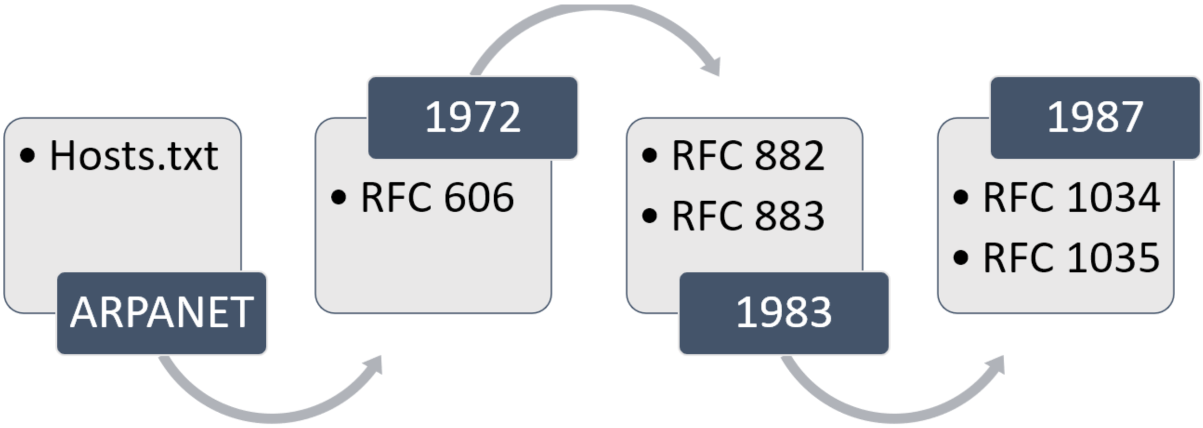


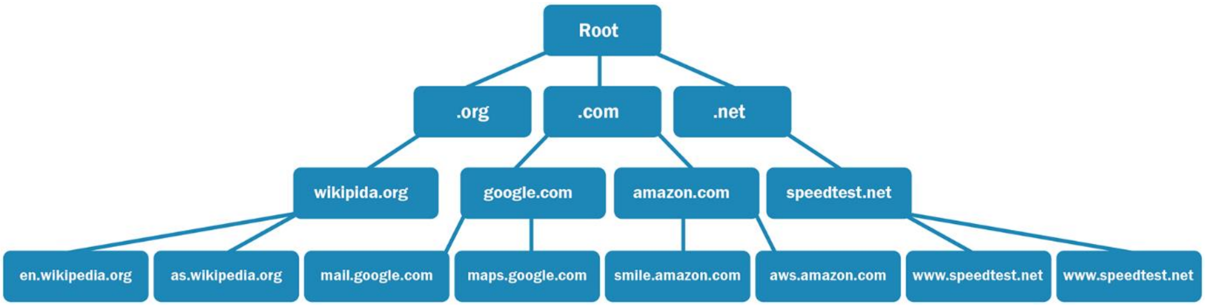
```
⌄ Internet Protocol Version 6
    0110 .... = Version: 6
  › .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... 0000 0000 0000 0000 0000 = Flow Label: 0x00000
    Payload Length: 40
    Next Header: ICMPv6 (58)
    Hop Limit: 255
    Source Address: fe80::dead
    Destination Address: fe80::beef
⌄ Internet Control Message Protocol v6
    Type: Redirect (137)
    Code: 0
    Checksum: 0x593e [correct]
    [Checksum Status: Good]
    Reserved: 00000000
    Target Address: fe80::cafe
    Destination Address: fe80::babe
```

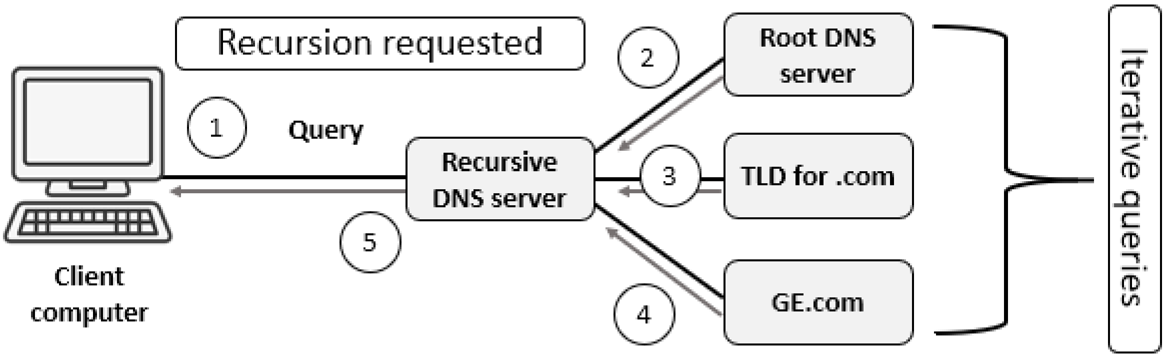


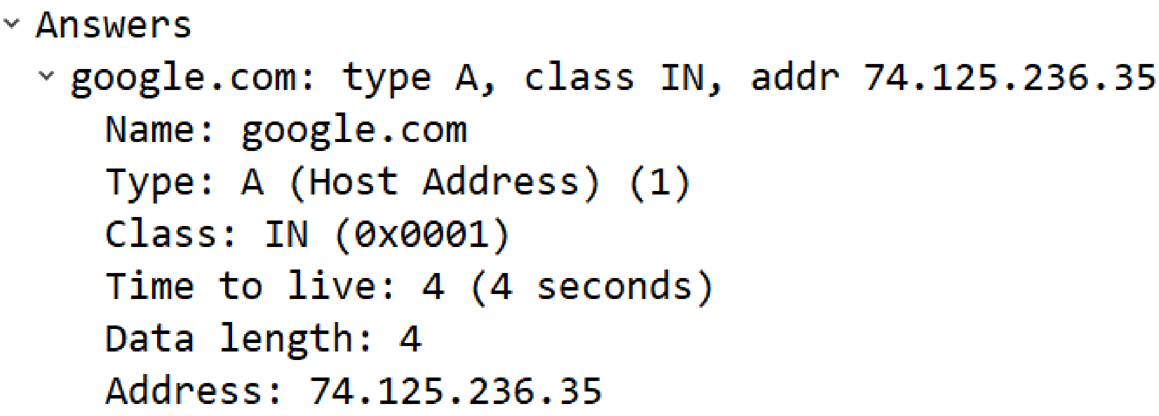
```
⌄ Internet Protocol Version 4, Src: 192.168.12.1, Dst: 192.168.12.2
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  › Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 796
    Identification: 0x0000 (0)
  › Flags: 0x20, More fragments
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 255
    Protocol: ICMP (1)
    Header Checksum: 0xff8c [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.12.1
    Destination Address: 192.168.12.2
    [Reassembled IPv4 in frame: 2]
⌄ Data (776 bytes)
    Data: 0800038800000000000000000004b45cabcdabcdabcdabcdabcdabcdabcdabcdabcd...
```

Chapter 13: Diving into DNS

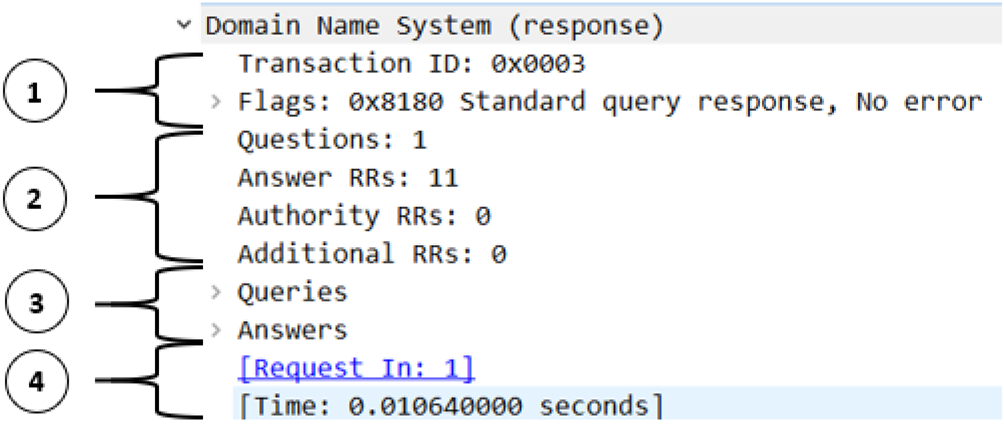




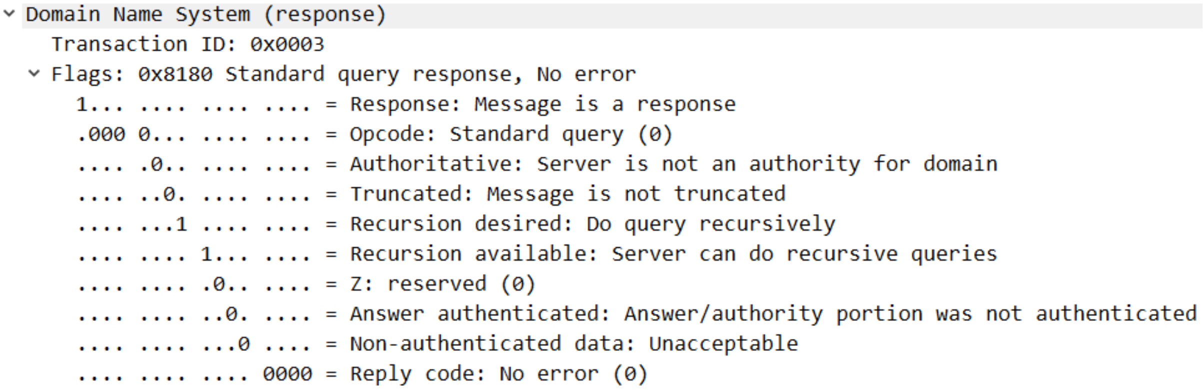




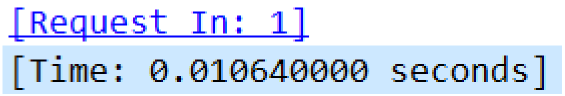
```
⌄ Answers
  ⌄ google.com: type A, class IN, addr 74.125.236.35
      Name: google.com
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 4 (4 seconds)
      Data length: 4
      Address: 74.125.236.35
```



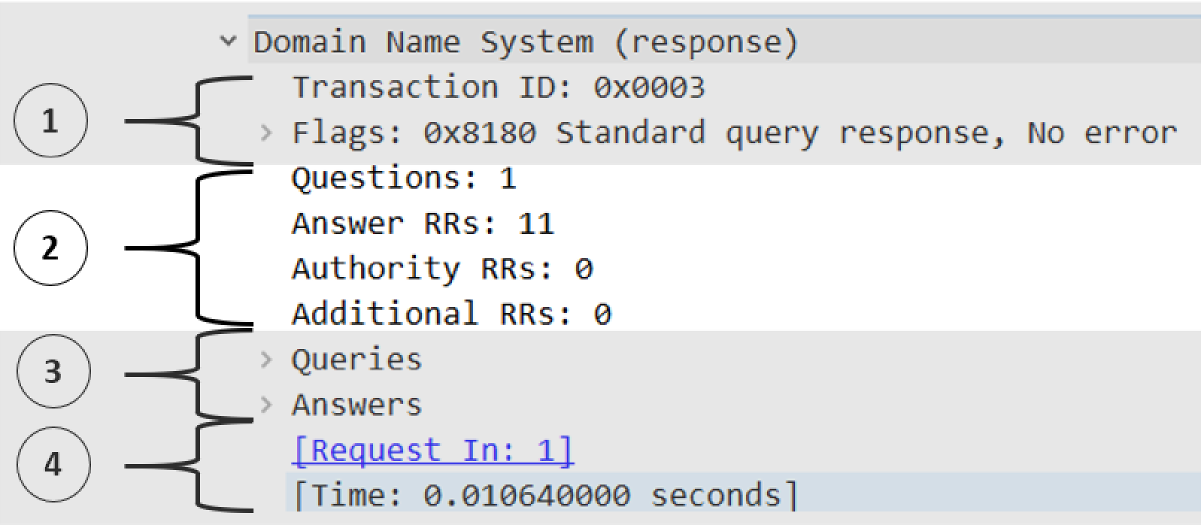
```
⌄ Domain Name System (response)
    Transaction ID: 0x0003
  › Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 11
    Authority RRs: 0
    Additional RRs: 0
  › Queries
  › Answers
    [Request In: 1]
    [Time: 0.010640000 seconds]
```



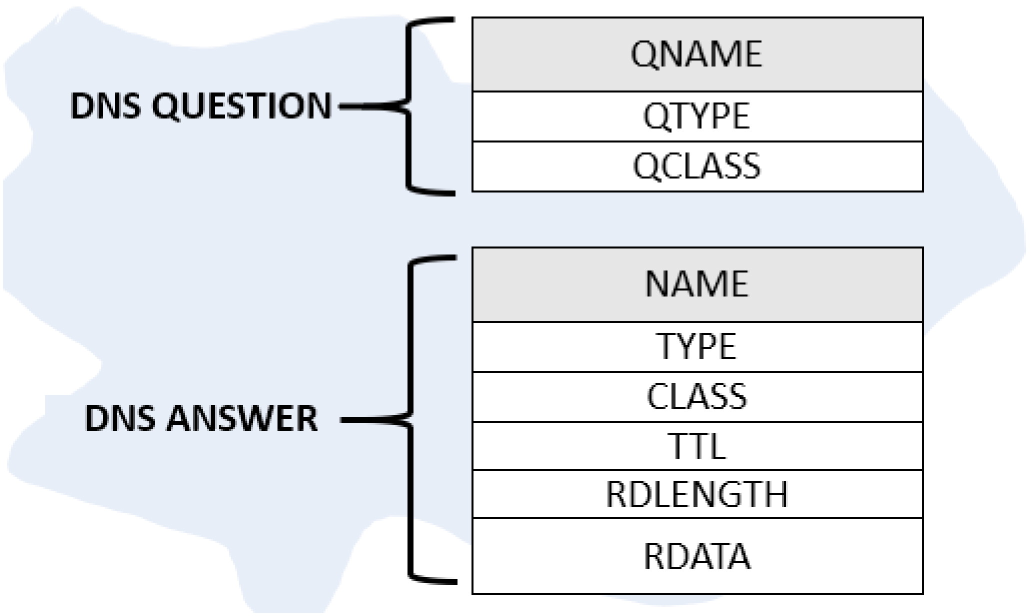
```
⌄ Domain Name System (response)
    Transaction ID: 0x0003
  ⌄ Flags: 0x8180 Standard query response, No error
      1... .... .... .... = Response: Message is a response
      .000 0... .... .... = Opcode: Standard query (0)
      .... .0.. .... .... = Authoritative: Server is not an authority for domain
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... 1... .... = Recursion available: Server can do recursive queries
      .... .... .0.. .... = Z: reserved (0)
      .... .... ..0. .... = Answer authenticated: Answer/authority portion was not authenticated
      .... .... ...0 .... = Non-authenticated data: Unacceptable
      .... .... .... 0000 = Reply code: No error (0)
```

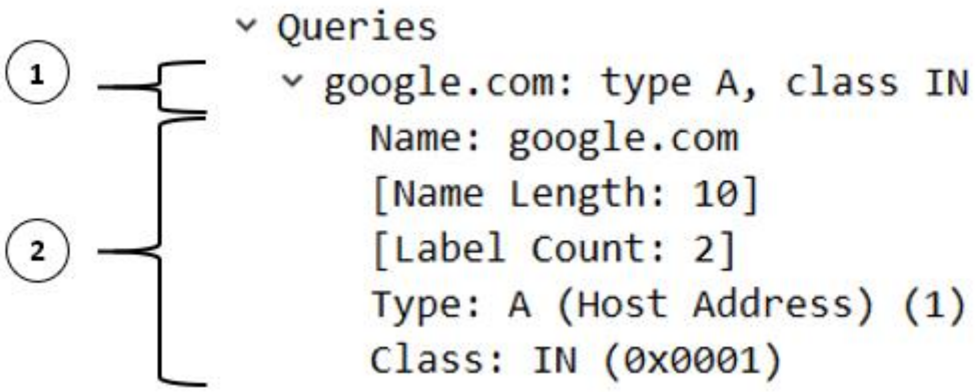


```
[Request In: 1]
[Time: 0.010640000 seconds]
```

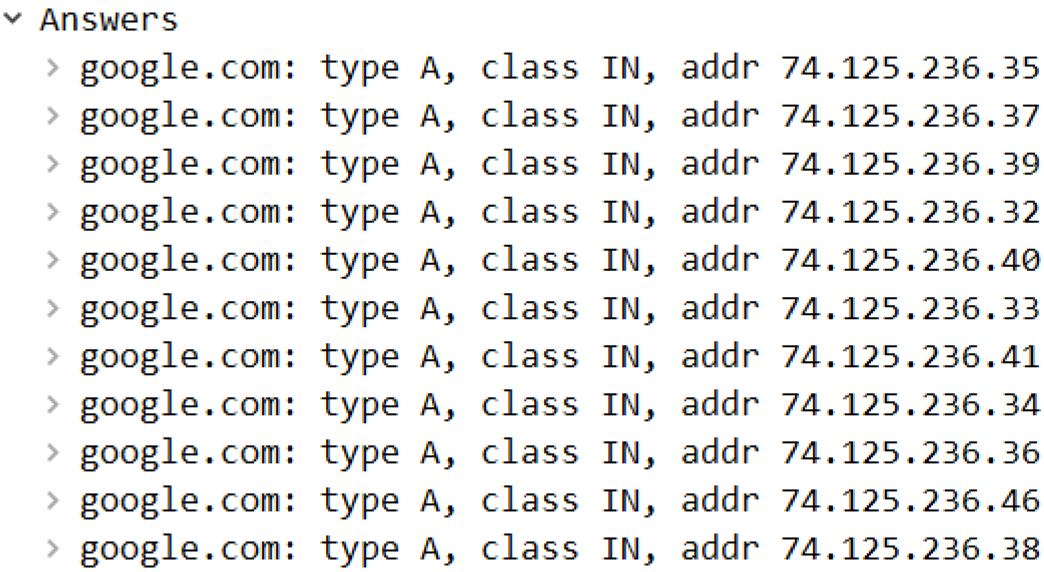


```
⌄ Domain Name System (response)
    Transaction ID: 0x0003
  › Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 11
    Authority RRs: 0
    Additional RRs: 0
  › Queries
  › Answers
    [Request In: 1]
    [Time: 0.010640000 seconds]
```

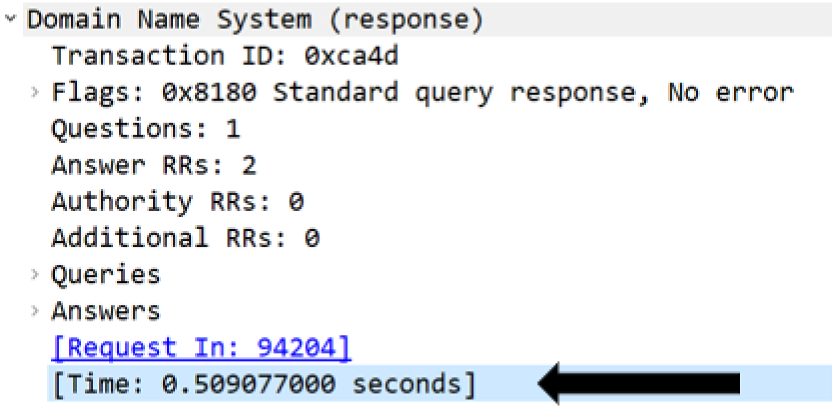




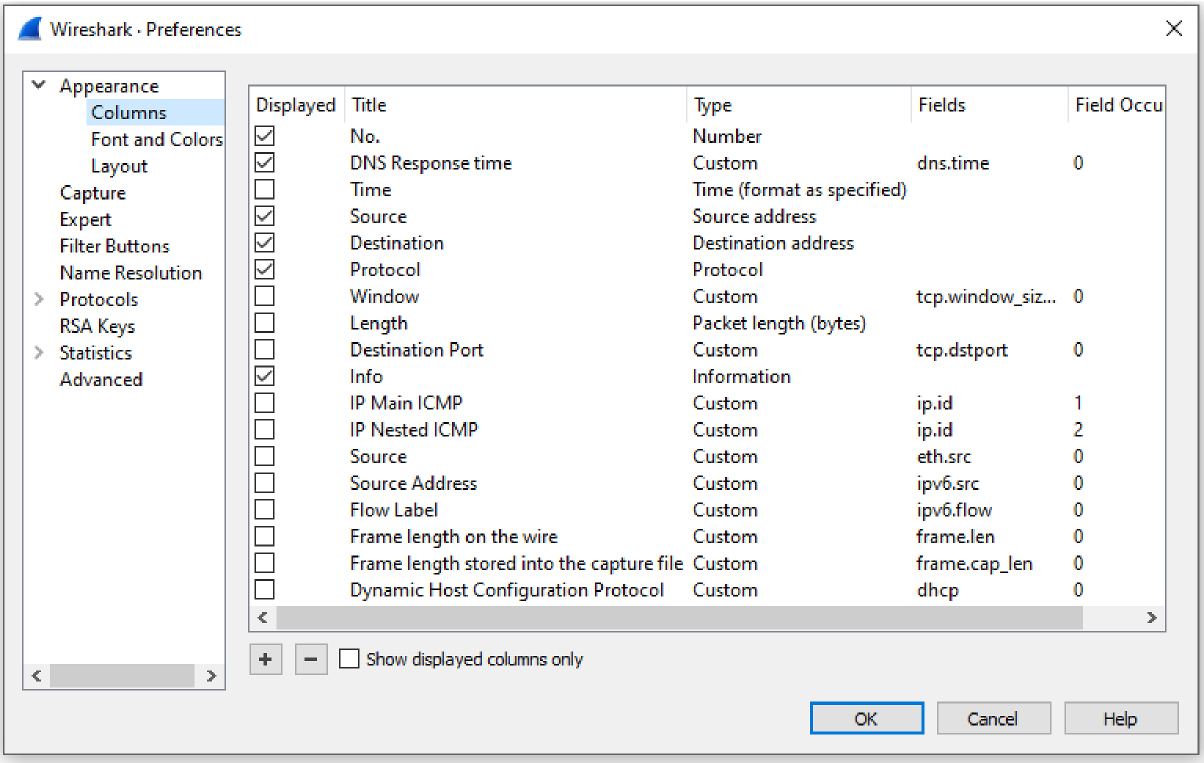
```
⌄ Queries
  ⌄ google.com: type A, class IN
      Name: google.com
      [Name Length: 10]
      [Label Count: 2]
      Type: A (Host Address) (1)
      Class: IN (0x0001)
```



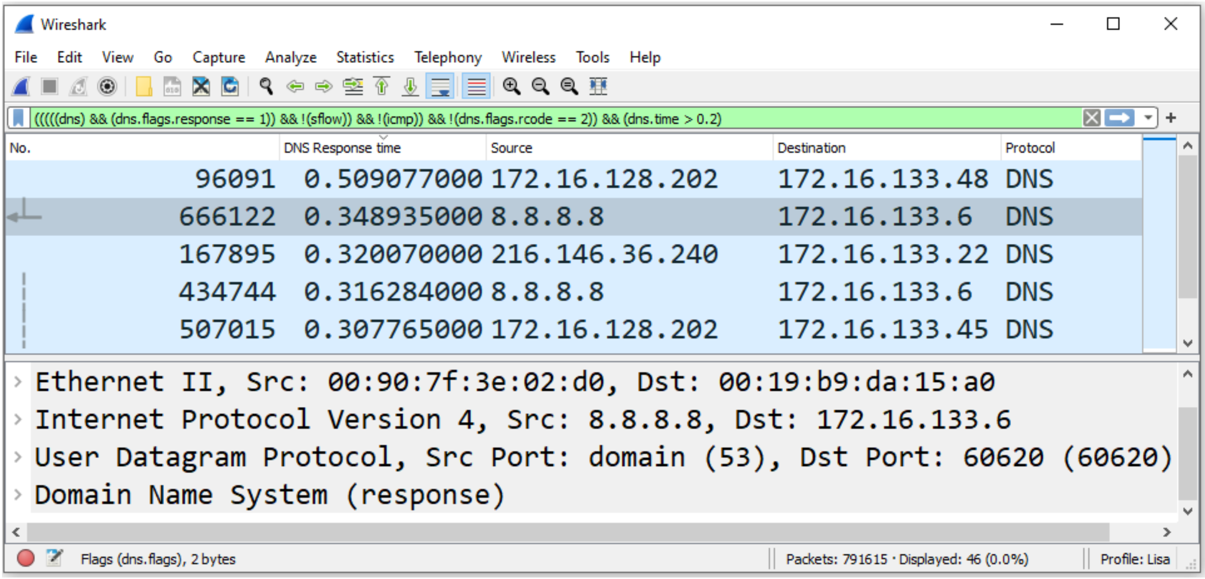
```
⌄ Answers
  › google.com: type A, class IN, addr 74.125.236.35
  › google.com: type A, class IN, addr 74.125.236.37
  › google.com: type A, class IN, addr 74.125.236.39
  › google.com: type A, class IN, addr 74.125.236.32
  › google.com: type A, class IN, addr 74.125.236.40
  › google.com: type A, class IN, addr 74.125.236.33
  › google.com: type A, class IN, addr 74.125.236.41
  › google.com: type A, class IN, addr 74.125.236.34
  › google.com: type A, class IN, addr 74.125.236.36
  › google.com: type A, class IN, addr 74.125.236.46
  › google.com: type A, class IN, addr 74.125.236.38
```



```
⌄ Domain Name System (response)
    Transaction ID: 0xca4d
  › Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 2
    Authority RRs: 0
    Additional RRs: 0
  › Queries
  › Answers
    [Request In: 94204]
    [Time: 0.509077000 seconds]
```



Displayed	Title	Type	Fields	Field Occu
☑	No.	Number		
☑	DNS Response time	Custom	dns.time	0
☐	Time	Time (format as specified)		
☑	Source	Source address		
☑	Destination	Destination address		
☑	Protocol	Protocol		
☐	Window	Custom	tcp.window_siz...	0
☐	Length	Packet length (bytes)		
☐	Destination Port	Custom	tcp.dstport	0
☑	Info	Information		
☐	IP Main ICMP	Custom	ip.id	1
☐	IP Nested ICMP	Custom	ip.id	2
☐	Source	Custom	eth.src	0
☐	Source Address	Custom	ipv6.src	0
☐	Flow Label	Custom	ipv6.flow	0
☐	Frame length on the wire	Custom	frame.len	0
☐	Frame length stored into the capture file	Custom	frame.cap_len	0
☐	Dynamic Host Configuration Protocol	Custom	dhcp	0

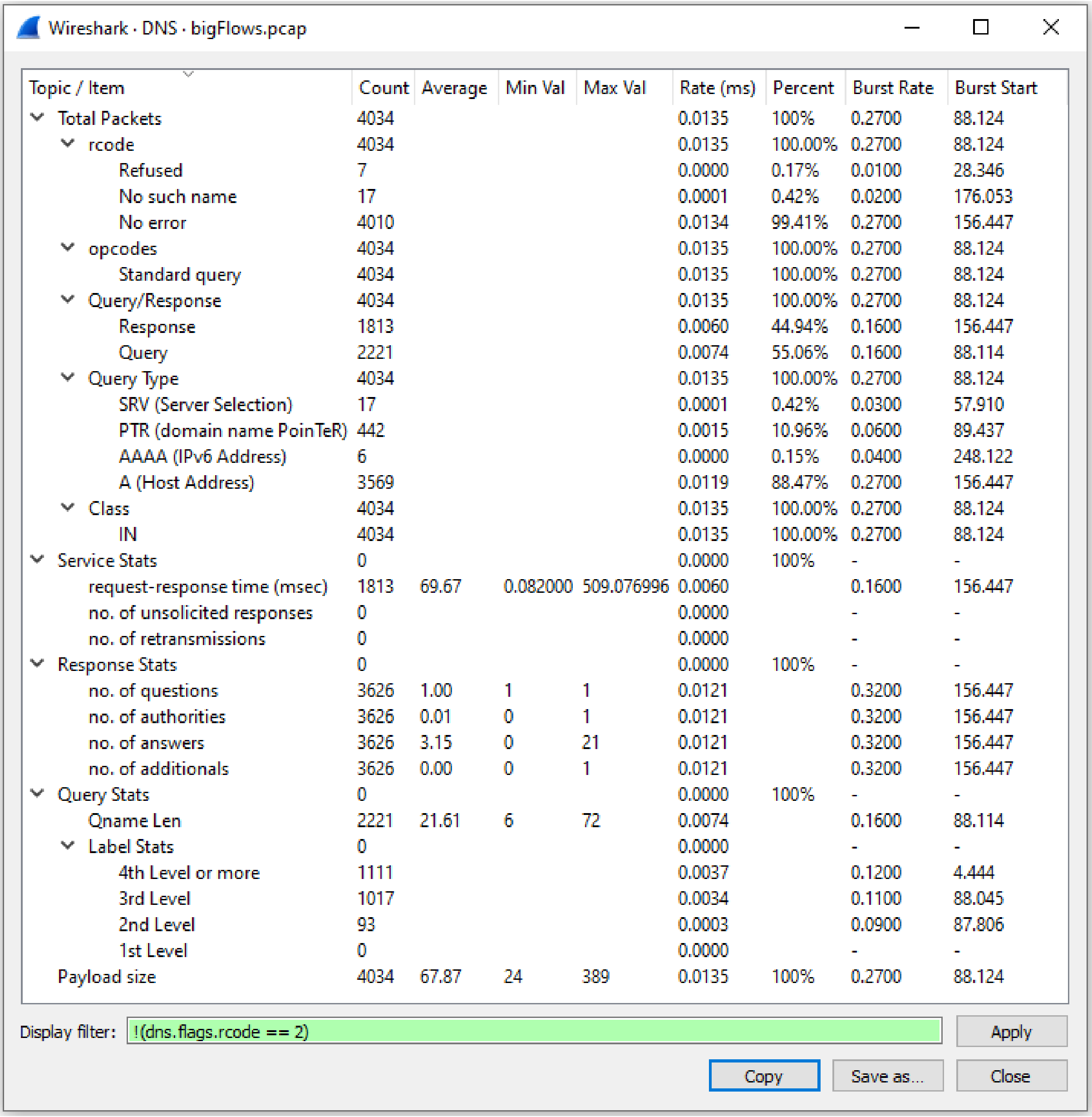


```
(((((dns) && (dns.flags.response == 1)) && !(sflow)) && !(icmp)) && !(dns.flags.rcode == 2)) && (dns.time > 0.2)
```

```
No.        DNS Response time  Source           Destination    Protocol
    96091  0.509077000 172.16.128.202  172.16.133.48  DNS
   666122  0.348935000 8.8.8.8         172.16.133.6   DNS
   167895  0.320070000 216.146.36.240  172.16.133.22  DNS
   434744  0.316284000 8.8.8.8         172.16.133.6   DNS
   507015  0.307765000 172.16.128.202  172.16.133.45  DNS
```

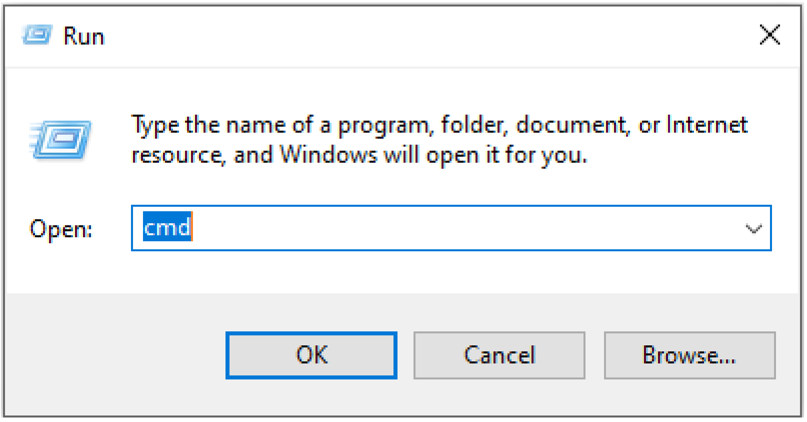
```
› Ethernet II, Src: 00:90:7f:3e:02:d0, Dst: 00:19:b9:da:15:a0
› Internet Protocol Version 4, Src: 8.8.8.8, Dst: 172.16.133.6
› User Datagram Protocol, Src Port: domain (53), Dst Port: 60620 (60620)
› Domain Name System (response)
```

Flags (dns.flags), 2 bytes   Packets: 791615 · Displayed: 46 (0.0%)   Profile: Lisa



Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
Total Packets	4034				0.0135	100%	0.2700	88.124
rcode	4034				0.0135	100.00%	0.2700	88.124
Refused	7				0.0000	0.17%	0.0100	28.346
No such name	17				0.0001	0.42%	0.0200	176.053
No error	4010				0.0134	99.41%	0.2700	156.447
opcodes	4034				0.0135	100.00%	0.2700	88.124
Standard query	4034				0.0135	100.00%	0.2700	88.124
Query/Response	4034				0.0135	100.00%	0.2700	88.124
Response	1813				0.0060	44.94%	0.1600	156.447
Query	2221				0.0074	55.06%	0.1600	88.114
Query Type	4034				0.0135	100.00%	0.2700	88.124
SRV (Server Selection)	17				0.0001	0.42%	0.0300	57.910
PTR (domain name PoinTeR)	442				0.0015	10.96%	0.0600	89.437
AAAA (IPv6 Address)	6				0.0000	0.15%	0.0400	248.122
A (Host Address)	3569				0.0119	88.47%	0.2700	156.447
Class	4034				0.0135	100.00%	0.2700	88.124
IN	4034				0.0135	100.00%	0.2700	88.124
Service Stats	0				0.0000	100%	-	-
request-response time (msec)	1813	69.67	0.082000	509.076996	0.0060		0.1600	156.447
no. of unsolicited responses	0				0.0000		-	-
no. of retransmissions	0				0.0000		-	-
Response Stats	0				0.0000	100%	-	-
no. of questions	3626	1.00	1	1	0.0121		0.3200	156.447
no. of authorities	3626	0.01	0	1	0.0121		0.3200	156.447
no. of answers	3626	3.15	0	21	0.0121		0.3200	156.447
no. of additionals	3626	0.00	0	1	0.0121		0.3200	156.447
Query Stats	0				0.0000	100%	-	-
Qname Len	2221	21.61	6	72	0.0074		0.1600	88.114
Label Stats	0				0.0000		-	-
4th Level or more	1111				0.0037		0.1200	4.444
3rd Level	1017				0.0034		0.1100	88.045
2nd Level	93				0.0003		0.0900	87.806
1st Level	0				0.0000		-	-
Payload size	4034	67.87	24	389	0.0135	100%	0.2700	88.124

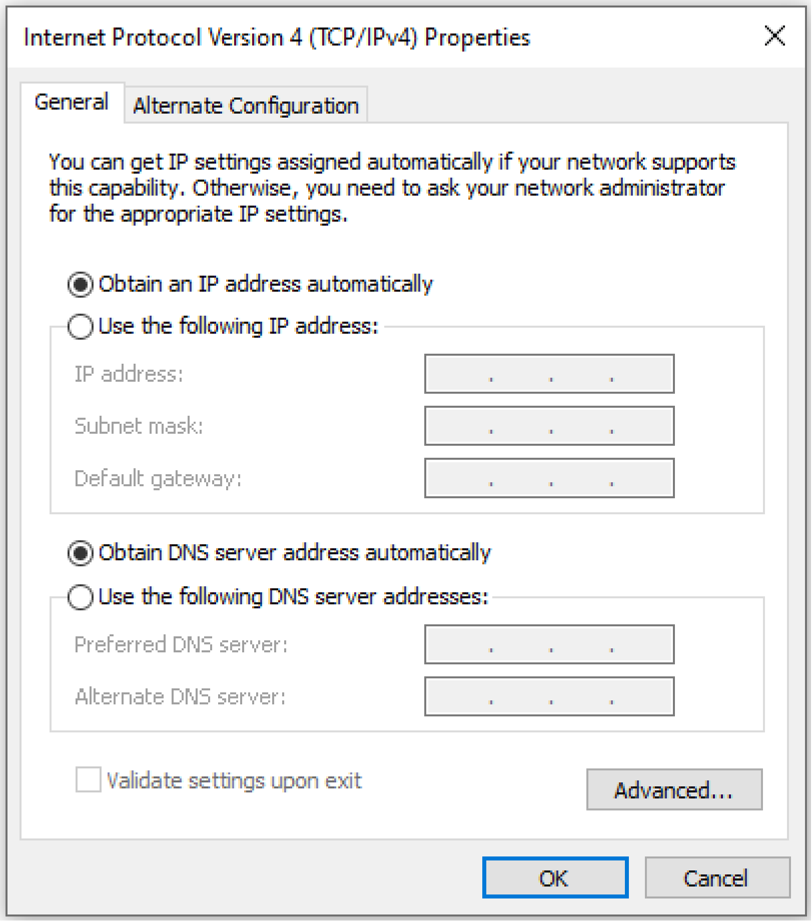
Display filter: !(dns.flags.rcode == 2)



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: cmd

Chapter 14: Examining DHCP



Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

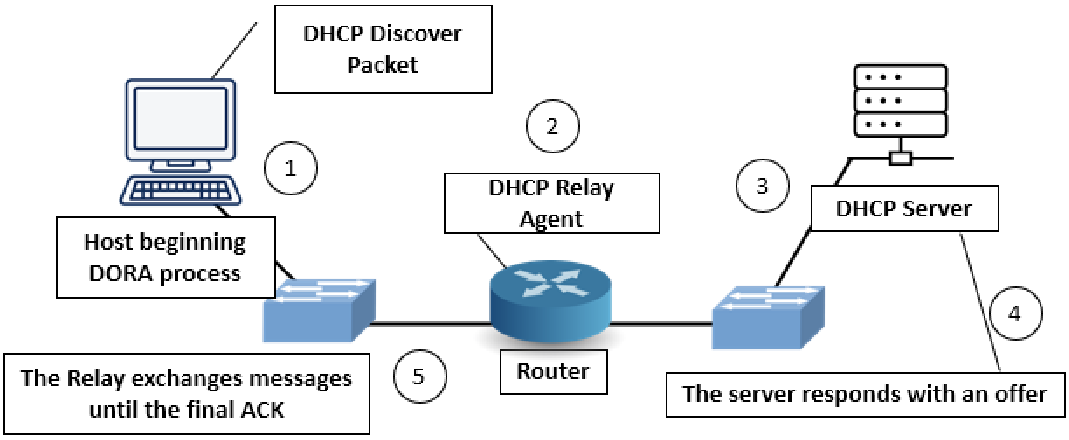
Preferred DNS server: . . .

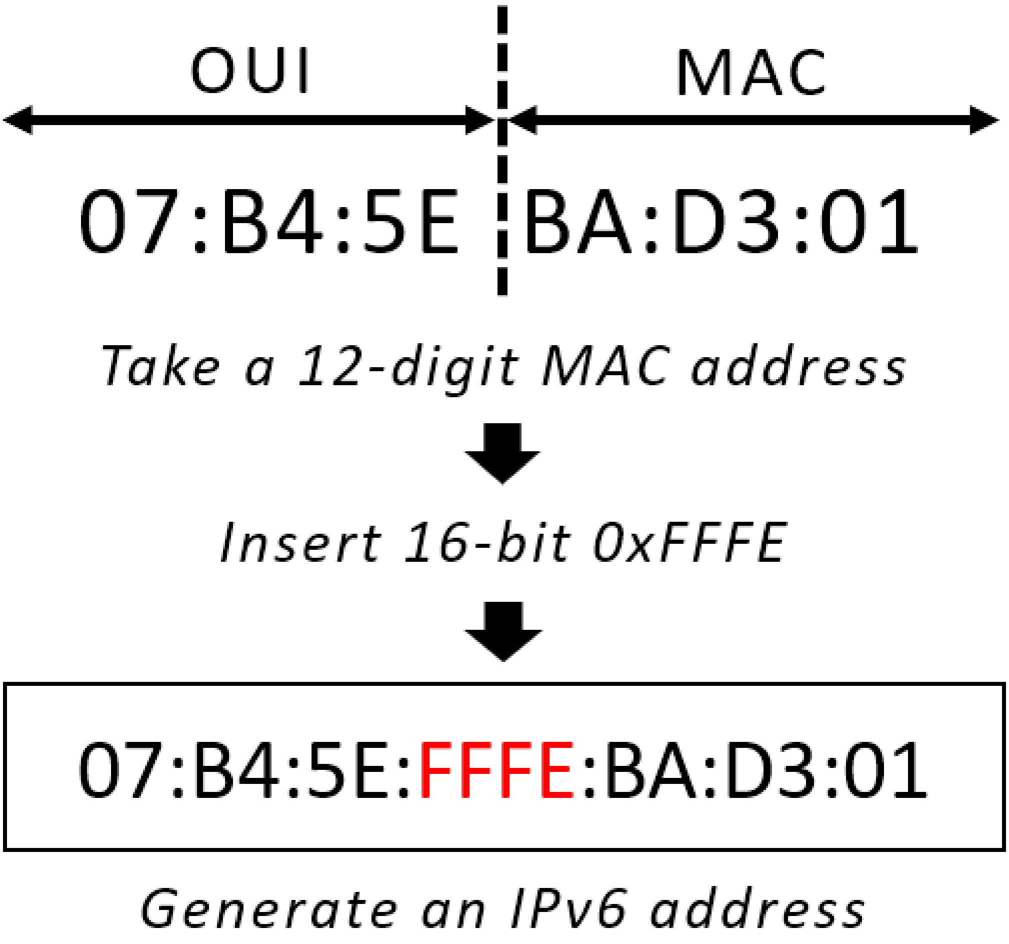
Alternate DNS server: . . .

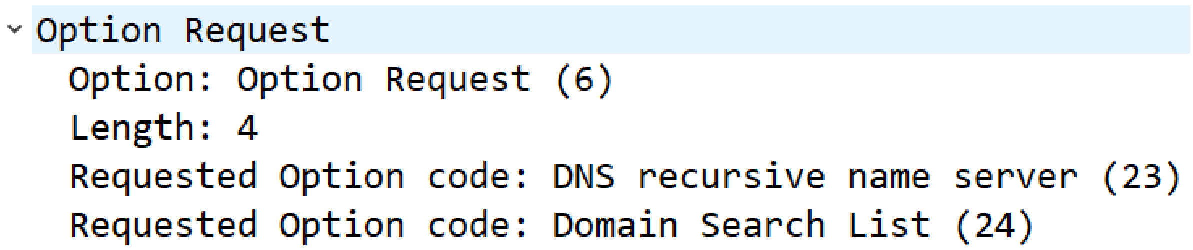
□ Validate settings upon exit

Advanced...

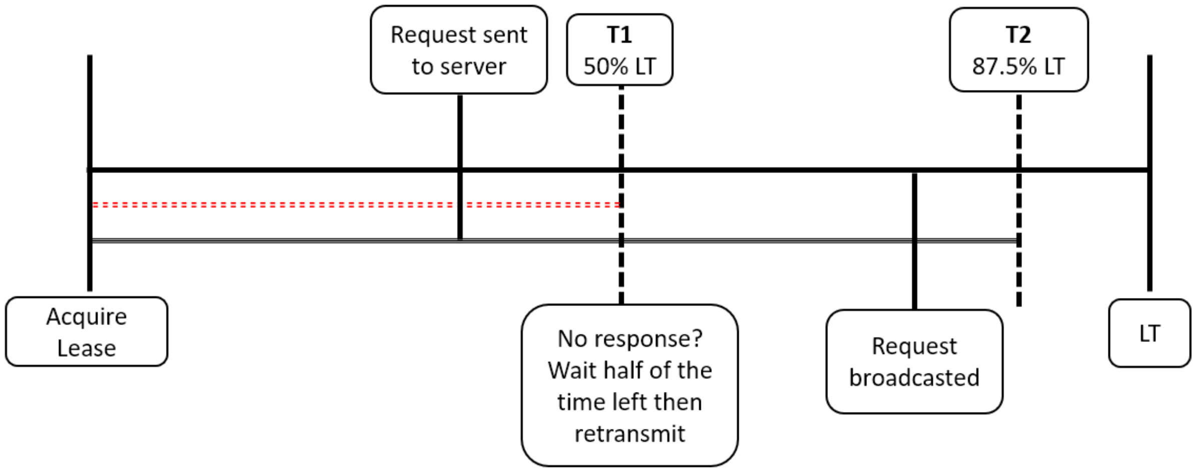
OK | Cancel

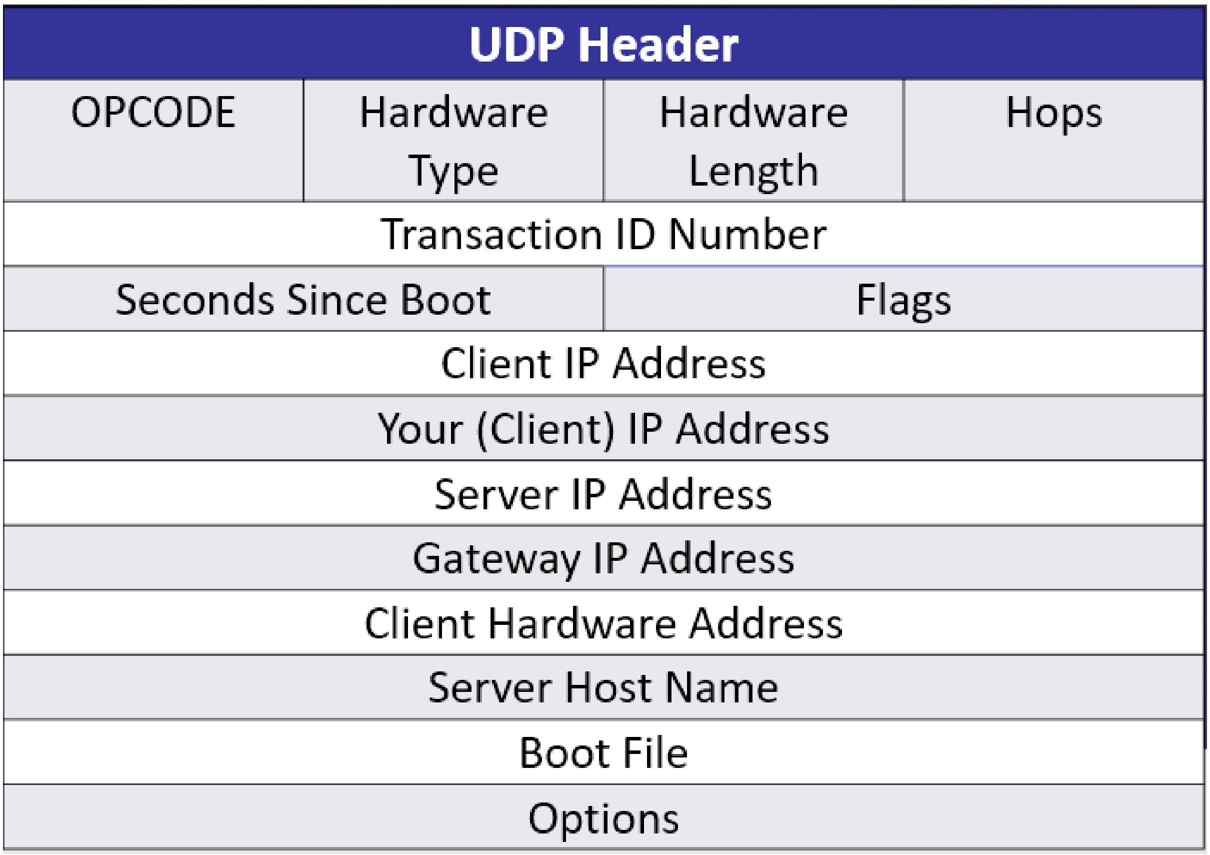

DHCP Discover Packet
1
Host beginning DORA process
2
DHCP Relay Agent
Router
3
DHCP Server
4
The server responds with an offer
5
The Relay exchanges messages until the final ACK



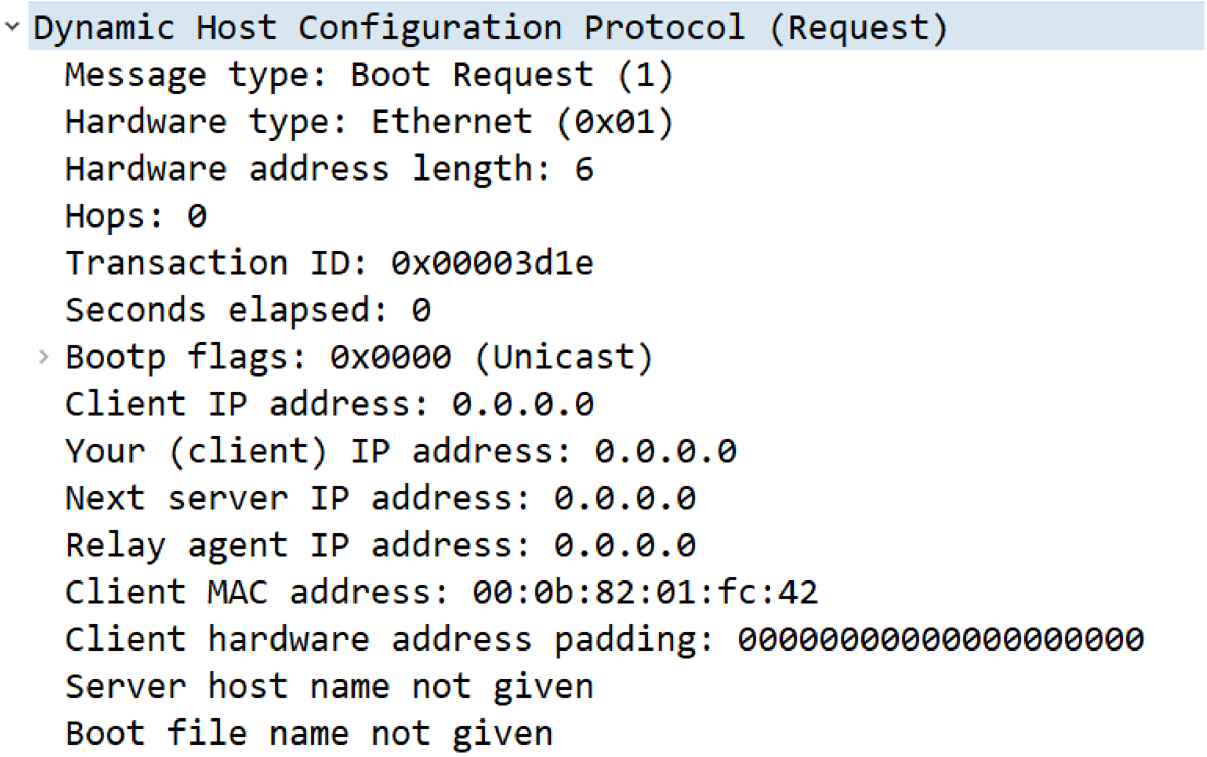


```
⌄ Option Request
    Option: Option Request (6)
    Length: 4
    Requested Option code: DNS recursive name server (23)
    Requested Option code: Domain Search List (24)
```

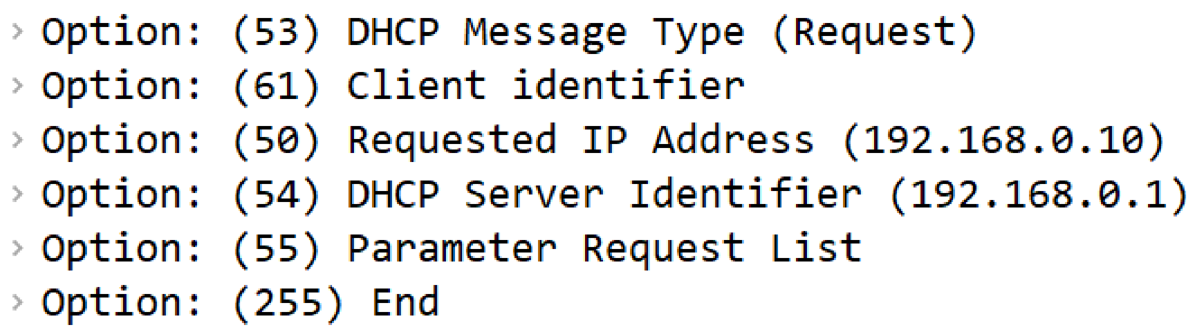




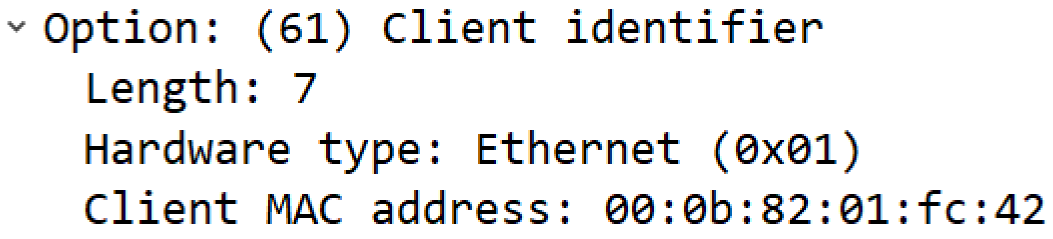
UDP Header			
OPCODE	Hardware Type	Hardware Length	Hops
Transaction ID Number			
Seconds Since Boot		Flags	
Client IP Address			
Your (Client) IP Address			
Server IP Address			
Gateway IP Address			
Client Hardware Address			
Server Host Name			
Boot File			
Options			



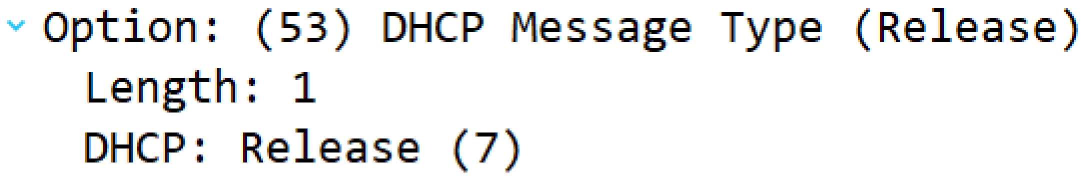
```
⌄ Dynamic Host Configuration Protocol (Request)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x00003d1e
    Seconds elapsed: 0
  › Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 0.0.0.0
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: 00:0b:82:01:fc:42
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
```



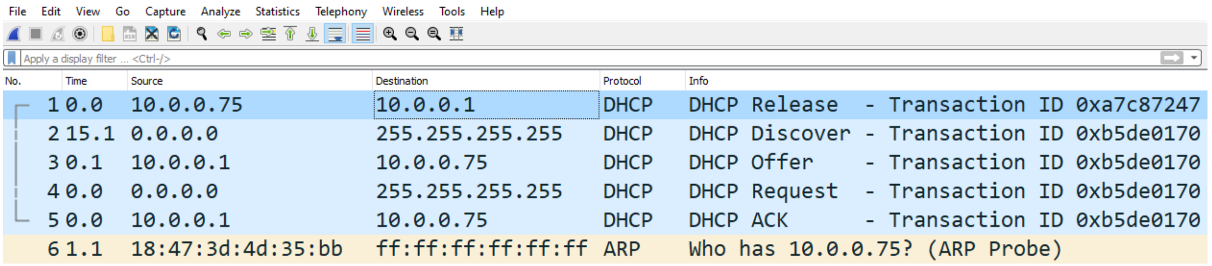
```
› Option: (53) DHCP Message Type (Request)
› Option: (61) Client identifier
› Option: (50) Requested IP Address (192.168.0.10)
› Option: (54) DHCP Server Identifier (192.168.0.1)
› Option: (55) Parameter Request List
› Option: (255) End
```



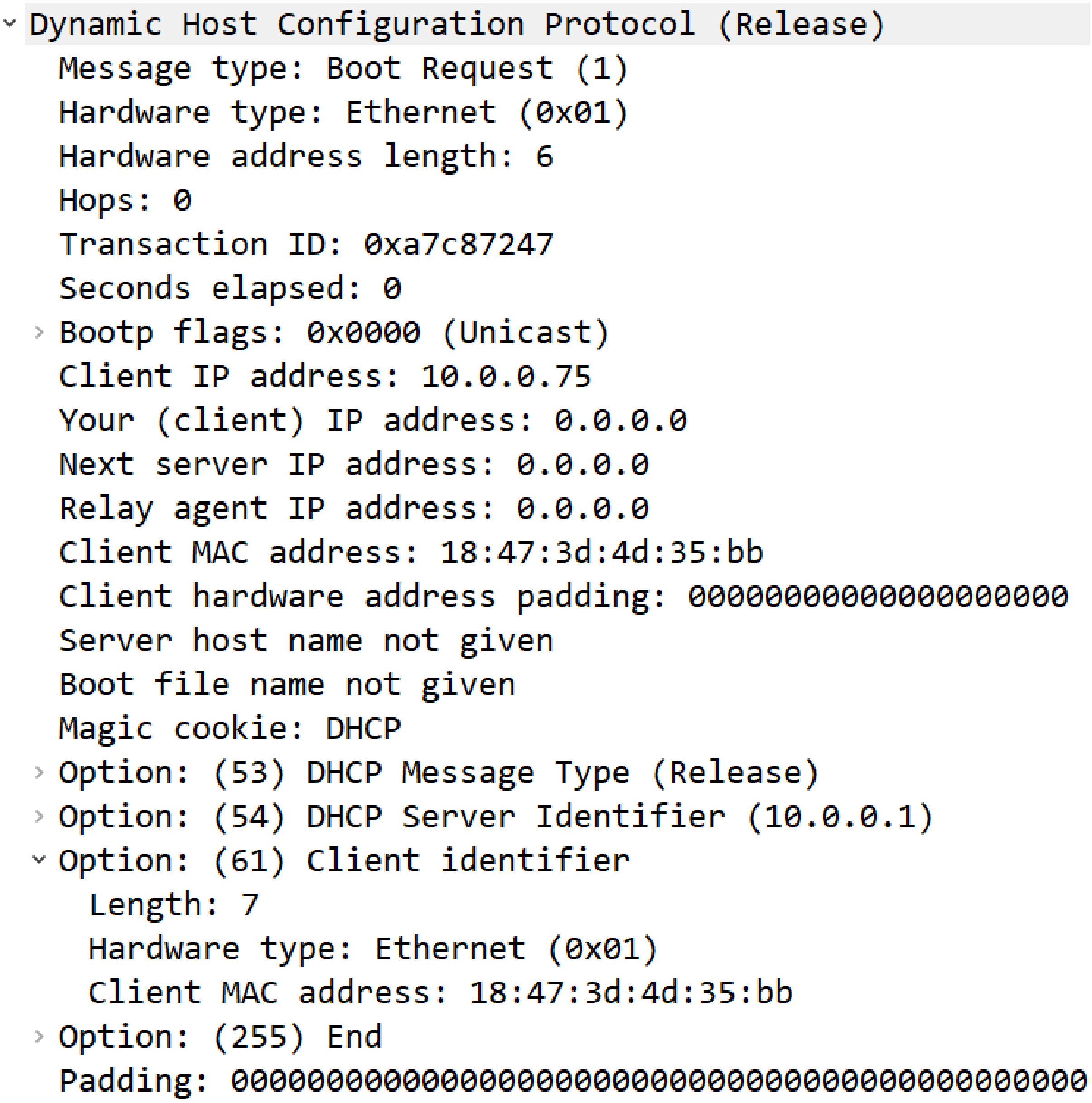
```
⌄ Option: (61) Client identifier
    Length: 7
    Hardware type: Ethernet (0x01)
    Client MAC address: 00:0b:82:01:fc:42
```



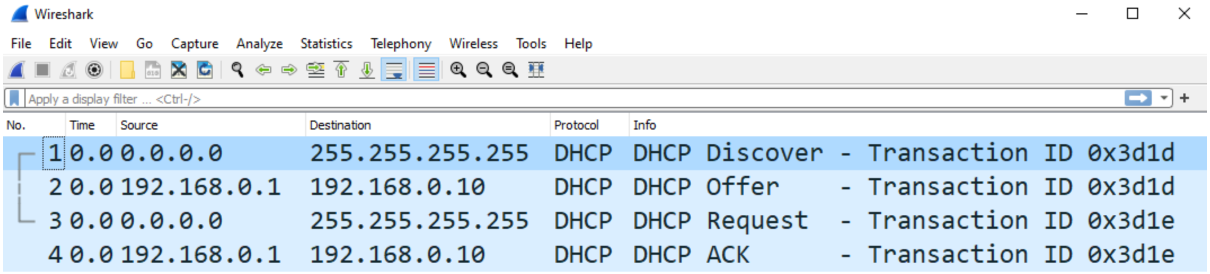
```
⌄ Option: (53) DHCP Message Type (Release)
    Length: 1
    DHCP: Release (7)
```



```
No. Time  Source             Destination          Protocol  Info
  1 0.0   10.0.0.75          10.0.0.1             DHCP      DHCP Release  - Transaction ID 0xa7c87247
  2 15.1  0.0.0.0            255.255.255.255      DHCP      DHCP Discover - Transaction ID 0xb5de0170
  3 0.1   10.0.0.1           10.0.0.75            DHCP      DHCP Offer    - Transaction ID 0xb5de0170
  4 0.0   0.0.0.0            255.255.255.255      DHCP      DHCP Request  - Transaction ID 0xb5de0170
  5 0.0   10.0.0.1           10.0.0.75            DHCP      DHCP ACK      - Transaction ID 0xb5de0170
  6 1.1   18:47:3d:4d:35:bb  ff:ff:ff:ff:ff:ff    ARP       Who has 10.0.0.75? (ARP Probe)
```

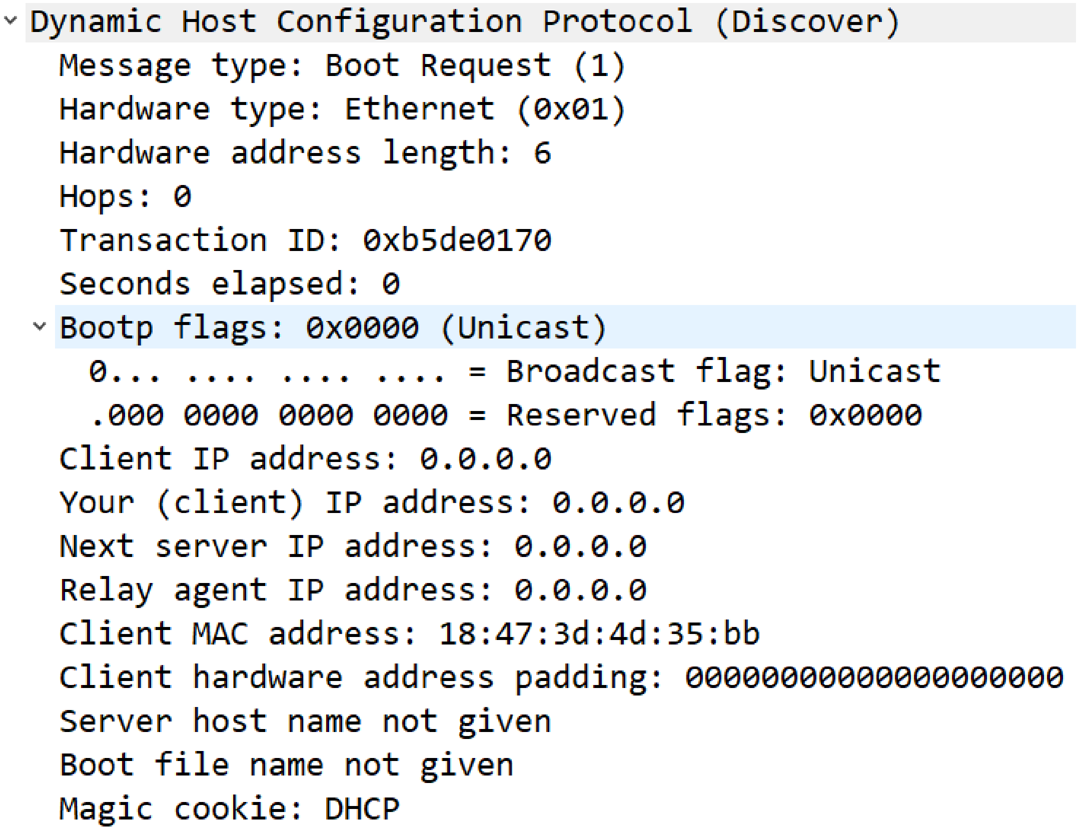


```
⌄ Dynamic Host Configuration Protocol (Release)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xa7c87247
    Seconds elapsed: 0
  › Bootp flags: 0x0000 (Unicast)
    Client IP address: 10.0.0.75
    Your (client) IP address: 0.0.0.0
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: 18:47:3d:4d:35:bb
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  › Option: (53) DHCP Message Type (Release)
  › Option: (54) DHCP Server Identifier (10.0.0.1)
  ⌄ Option: (61) Client identifier
      Length: 7
      Hardware type: Ethernet (0x01)
      Client MAC address: 18:47:3d:4d:35:bb
  › Option: (255) End
    Padding: 000000000000000000000000000000000000000000000
```

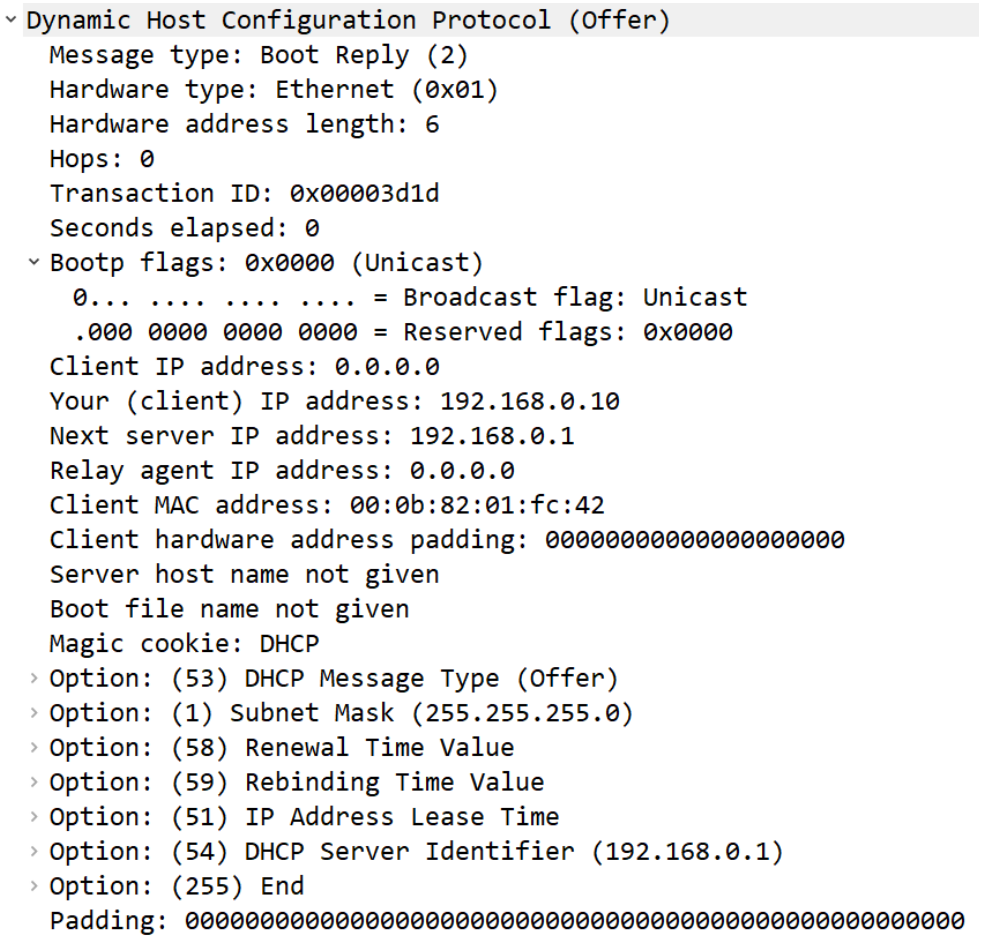


Wireshark
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

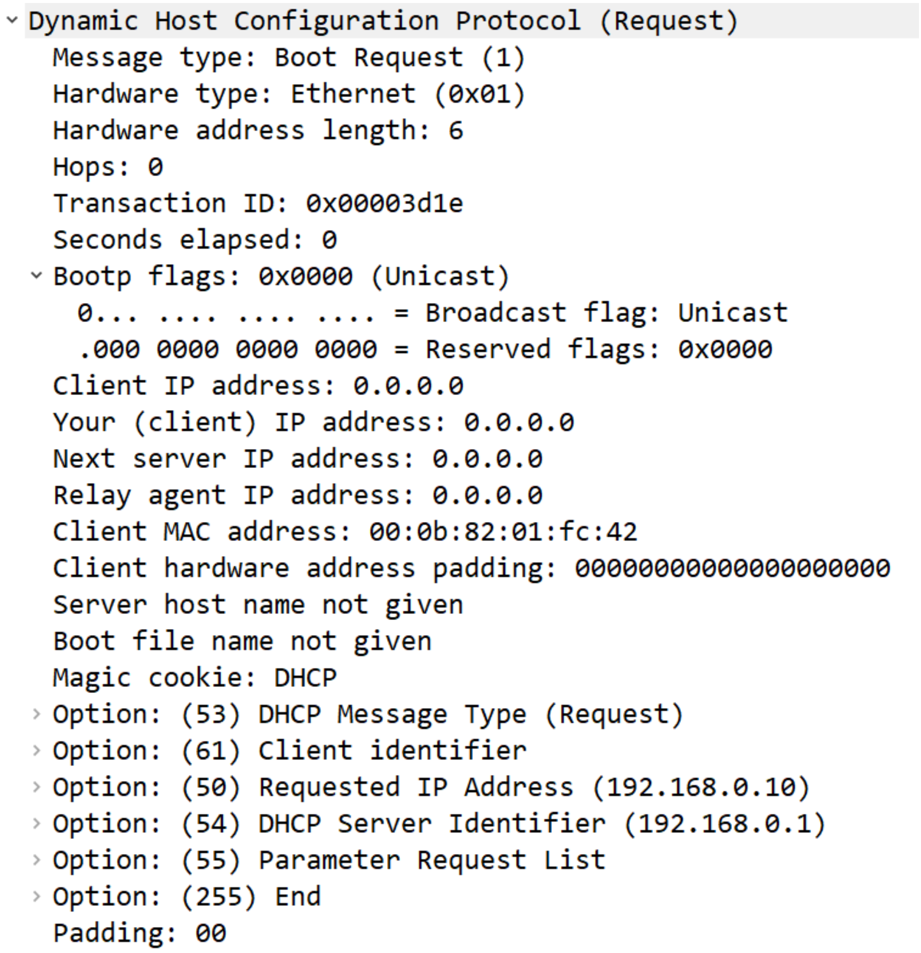
```
No. Time Source       Destination      Protocol Info
  1 0.0  0.0.0.0      255.255.255.255  DHCP     DHCP Discover - Transaction ID 0x3d1d
  2 0.0  192.168.0.1  192.168.0.10     DHCP     DHCP Offer    - Transaction ID 0x3d1d
  3 0.0  0.0.0.0      255.255.255.255  DHCP     DHCP Request  - Transaction ID 0x3d1e
  4 0.0  192.168.0.1  192.168.0.10     DHCP     DHCP ACK      - Transaction ID 0x3d1e
```



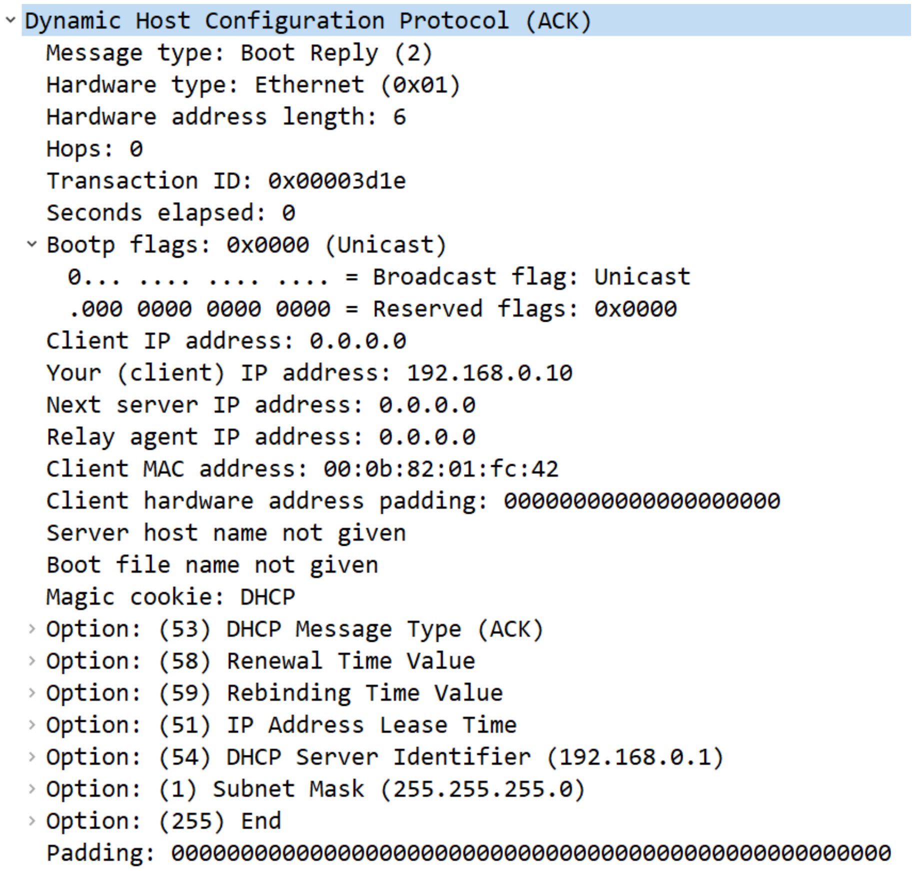
```
⌄ Dynamic Host Configuration Protocol (Discover)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xb5de0170
    Seconds elapsed: 0
  ⌄ Bootp flags: 0x0000 (Unicast)
      0... .... .... .... = Broadcast flag: Unicast
      .000 0000 0000 0000 = Reserved flags: 0x0000
    Client IP address: 0.0.0.0
    Your (client) IP address: 0.0.0.0
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: 18:47:3d:4d:35:bb
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
```



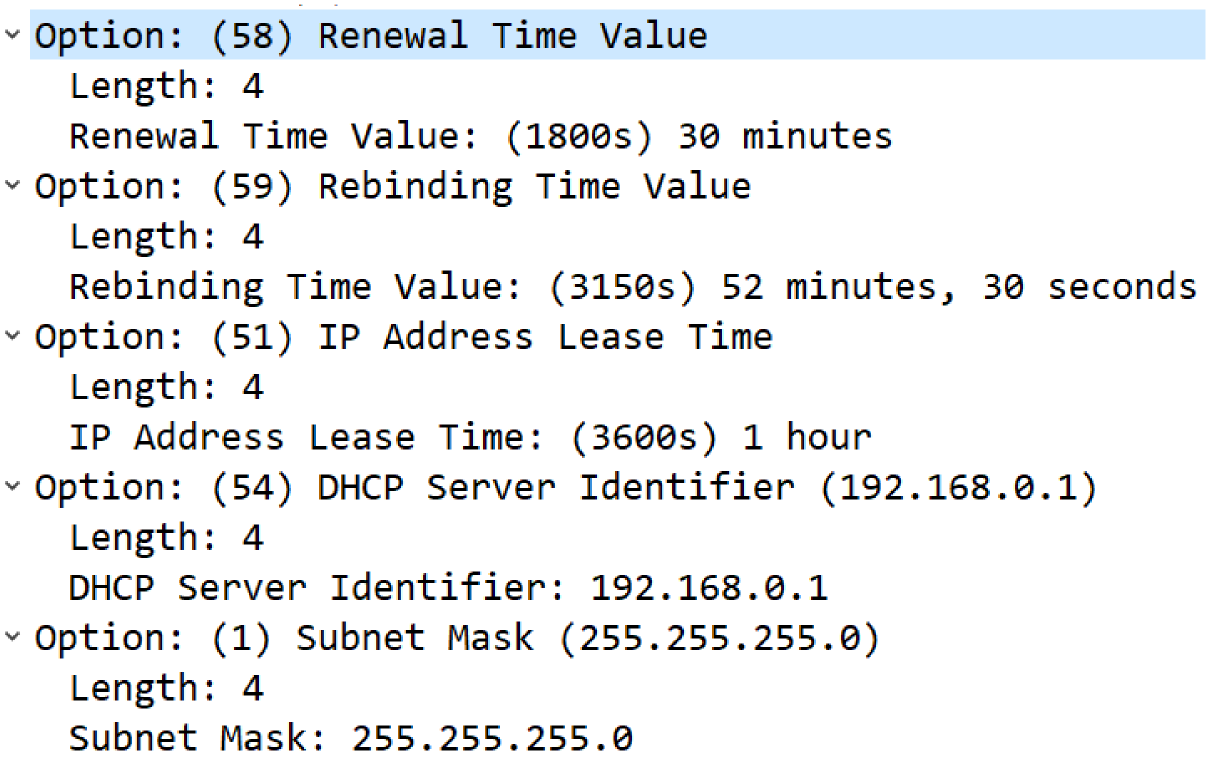
```
⌄ Dynamic Host Configuration Protocol (Offer)
    Message type: Boot Reply (2)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x00003d1d
    Seconds elapsed: 0
  ⌄ Bootp flags: 0x0000 (Unicast)
      0... .... .... .... = Broadcast flag: Unicast
      .000 0000 0000 0000 = Reserved flags: 0x0000
    Client IP address: 0.0.0.0
    Your (client) IP address: 192.168.0.10
    Next server IP address: 192.168.0.1
    Relay agent IP address: 0.0.0.0
    Client MAC address: 00:0b:82:01:fc:42
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  › Option: (53) DHCP Message Type (Offer)
  › Option: (1) Subnet Mask (255.255.255.0)
  › Option: (58) Renewal Time Value
  › Option: (59) Rebinding Time Value
  › Option: (51) IP Address Lease Time
  › Option: (54) DHCP Server Identifier (192.168.0.1)
  › Option: (255) End
    Padding: 0000000000000000000000000000000000000000000000000000
```



```
⌄ Dynamic Host Configuration Protocol (Request)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x00003d1e
    Seconds elapsed: 0
  ⌄ Bootp flags: 0x0000 (Unicast)
      0... .... .... .... = Broadcast flag: Unicast
      .000 0000 0000 0000 = Reserved flags: 0x0000
    Client IP address: 0.0.0.0
    Your (client) IP address: 0.0.0.0
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: 00:0b:82:01:fc:42
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  › Option: (53) DHCP Message Type (Request)
  › Option: (61) Client identifier
  › Option: (50) Requested IP Address (192.168.0.10)
  › Option: (54) DHCP Server Identifier (192.168.0.1)
  › Option: (55) Parameter Request List
  › Option: (255) End
    Padding: 00
```

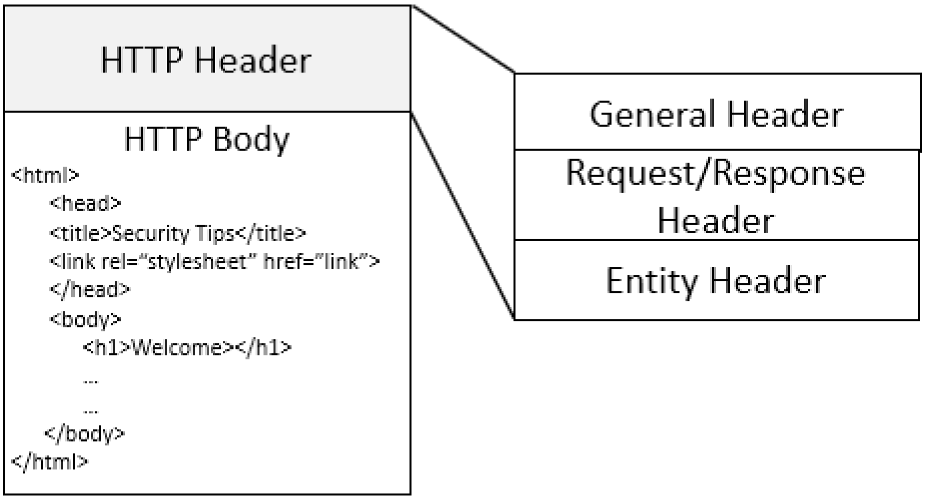


```
⌄ Dynamic Host Configuration Protocol (ACK)
    Message type: Boot Reply (2)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x00003d1e
    Seconds elapsed: 0
  ⌄ Bootp flags: 0x0000 (Unicast)
      0... .... .... .... = Broadcast flag: Unicast
      .000 0000 0000 0000 = Reserved flags: 0x0000
    Client IP address: 0.0.0.0
    Your (client) IP address: 192.168.0.10
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: 00:0b:82:01:fc:42
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  › Option: (53) DHCP Message Type (ACK)
  › Option: (58) Renewal Time Value
  › Option: (59) Rebinding Time Value
  › Option: (51) IP Address Lease Time
  › Option: (54) DHCP Server Identifier (192.168.0.1)
  › Option: (1) Subnet Mask (255.255.255.0)
  › Option: (255) End
    Padding: 0000000000000000000000000000000000000000000000000000
```

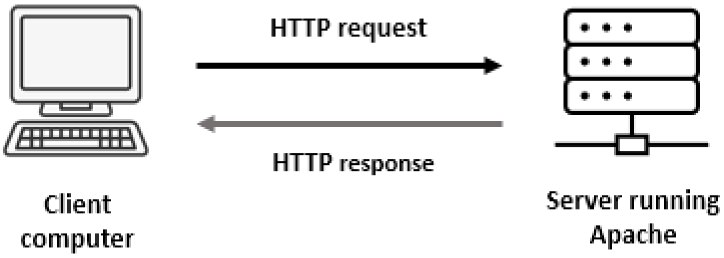


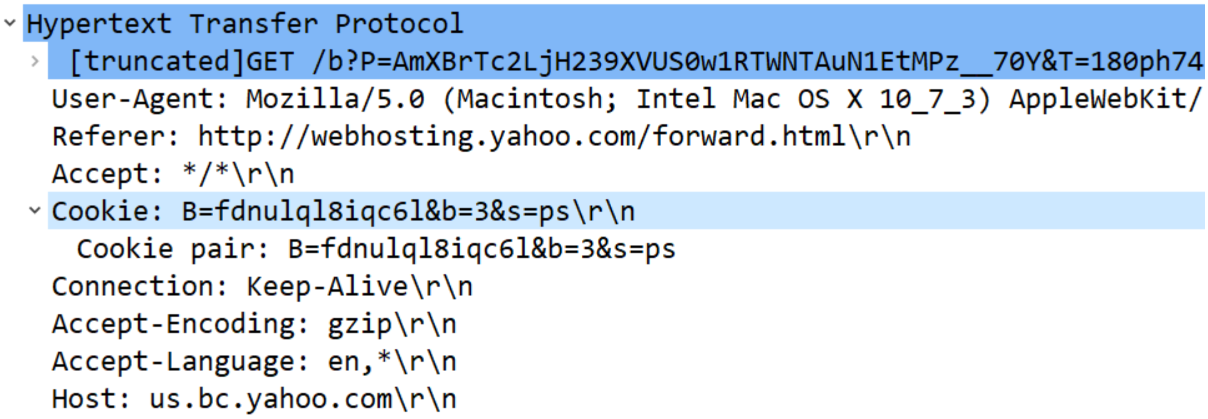
```
⌄ Option: (58) Renewal Time Value
    Length: 4
    Renewal Time Value: (1800s) 30 minutes
⌄ Option: (59) Rebinding Time Value
    Length: 4
    Rebinding Time Value: (3150s) 52 minutes, 30 seconds
⌄ Option: (51) IP Address Lease Time
    Length: 4
    IP Address Lease Time: (3600s) 1 hour
⌄ Option: (54) DHCP Server Identifier (192.168.0.1)
    Length: 4
    DHCP Server Identifier: 192.168.0.1
⌄ Option: (1) Subnet Mask (255.255.255.0)
    Length: 4
    Subnet Mask: 255.255.255.0
```

Chapter 15: Decoding HTTP

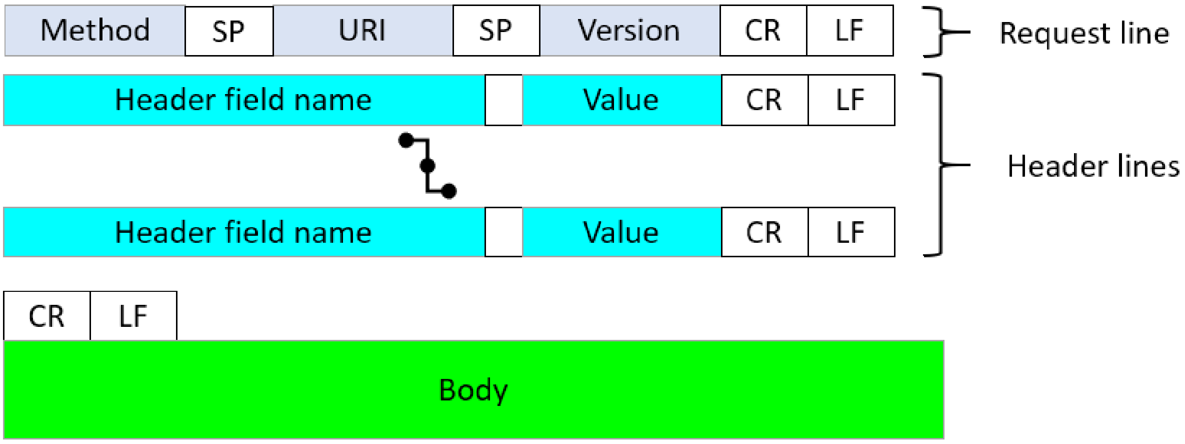


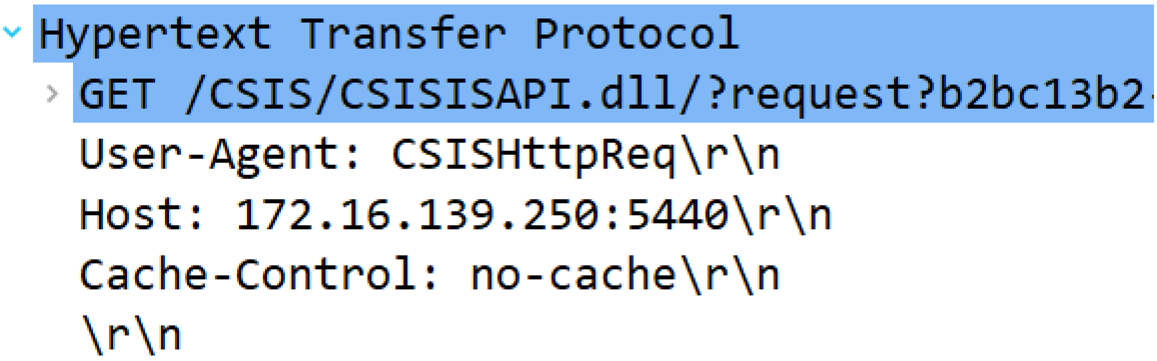
```
<html>
    <head>
    <title>Security Tips</title>
    <link rel="stylesheet" href="link">
    </head>
    <body>
        <h1>Welcome></h1>
        ...
        ...
    </body>
</html>
```



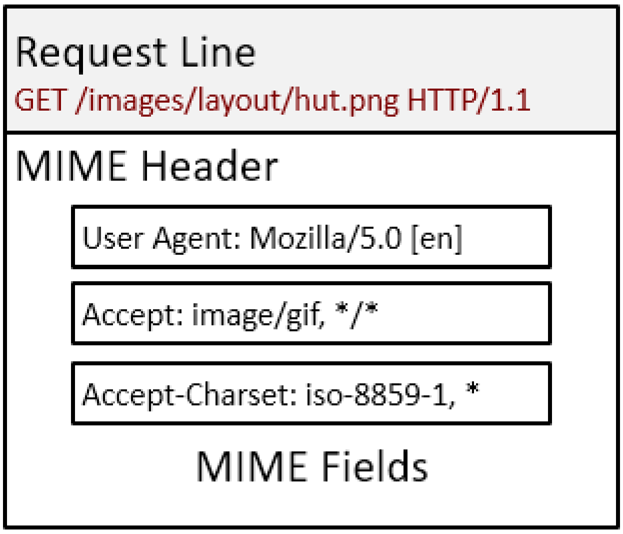


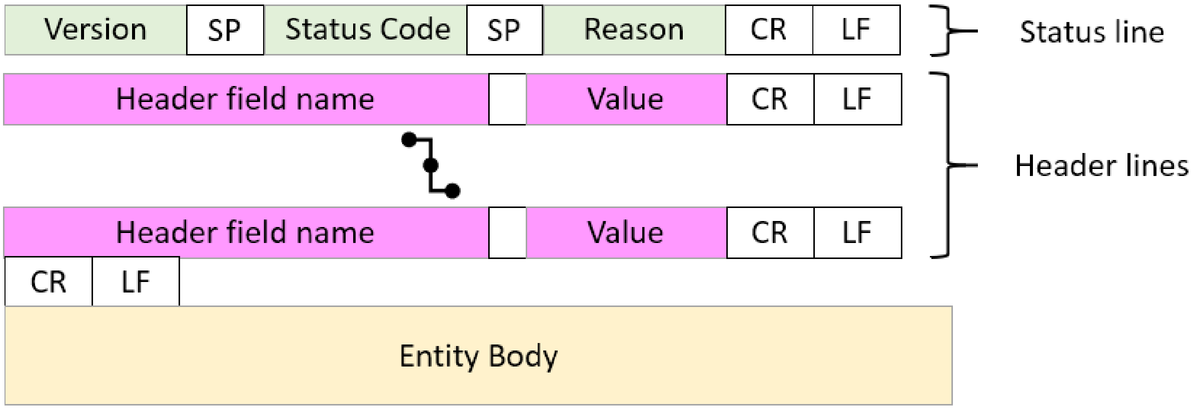
```
˅ Hypertext Transfer Protocol
  ˃  [truncated]GET /b?P=AmXBrTc2LjH239XVUS0w1RTWNTAuN1EtMPz__70Y&T=180ph74
   User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_3) AppleWebKit/
   Referer: http://webhosting.yahoo.com/forward.html\r\n
   Accept: */*\r\n
  ˅ Cookie: B=fdnulql8iqc6l&b=3&s=ps\r\n
      Cookie pair: B=fdnulql8iqc6l&b=3&s=ps
   Connection: Keep-Alive\r\n
   Accept-Encoding: gzip\r\n
   Accept-Language: en,*\r\n
   Host: us.bc.yahoo.com\r\n
```

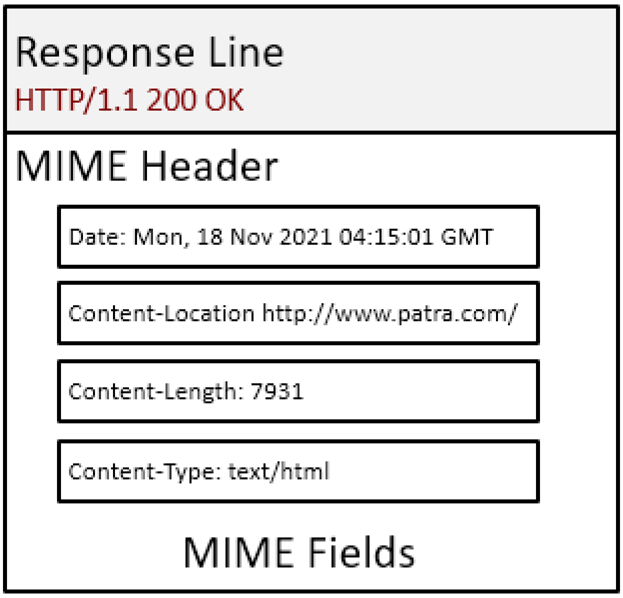


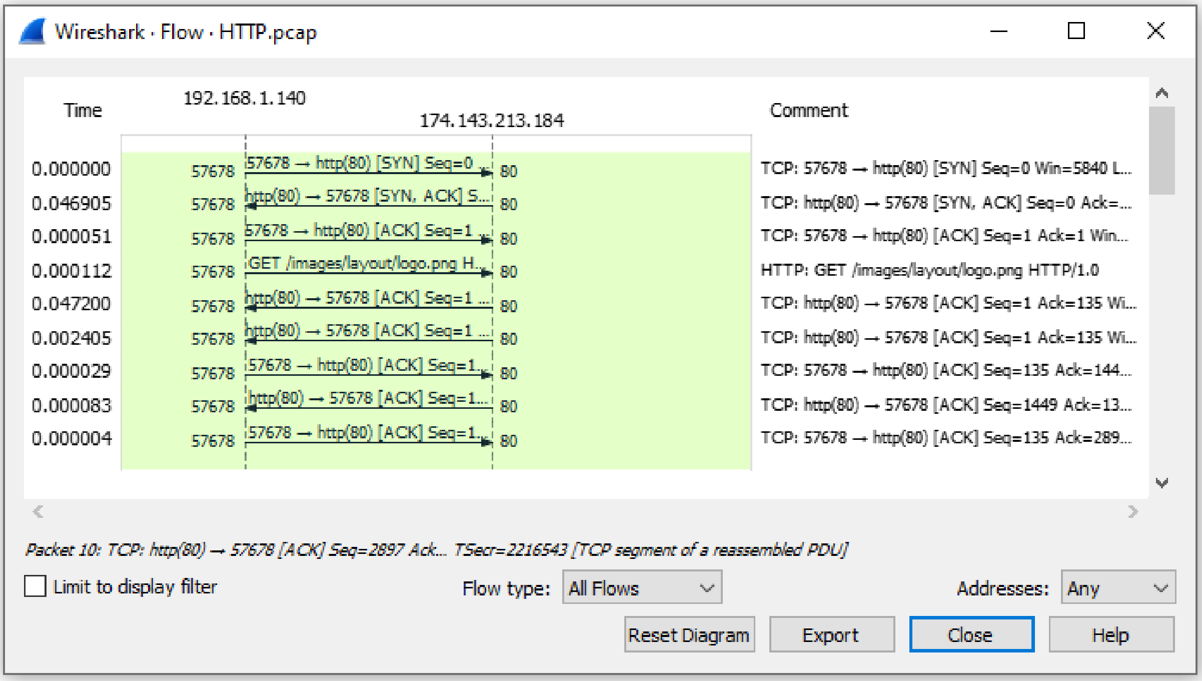


```
⌄ Hypertext Transfer Protocol
  › GET /CSIS/CSISISAPI.dll/?request?b2bc13b2
    User-Agent: CSISHttpReq\r\n
    Host: 172.16.139.250:5440\r\n
    Cache-Control: no-cache\r\n
    \r\n
```


Request Line
GET /images/layout/hut.png HTTP/1.1
MIME Header
User Agent: Mozilla/5.0 [en]
Accept: image/gif, */*
Accept-Charset: iso-8859-1, *
MIME Fields







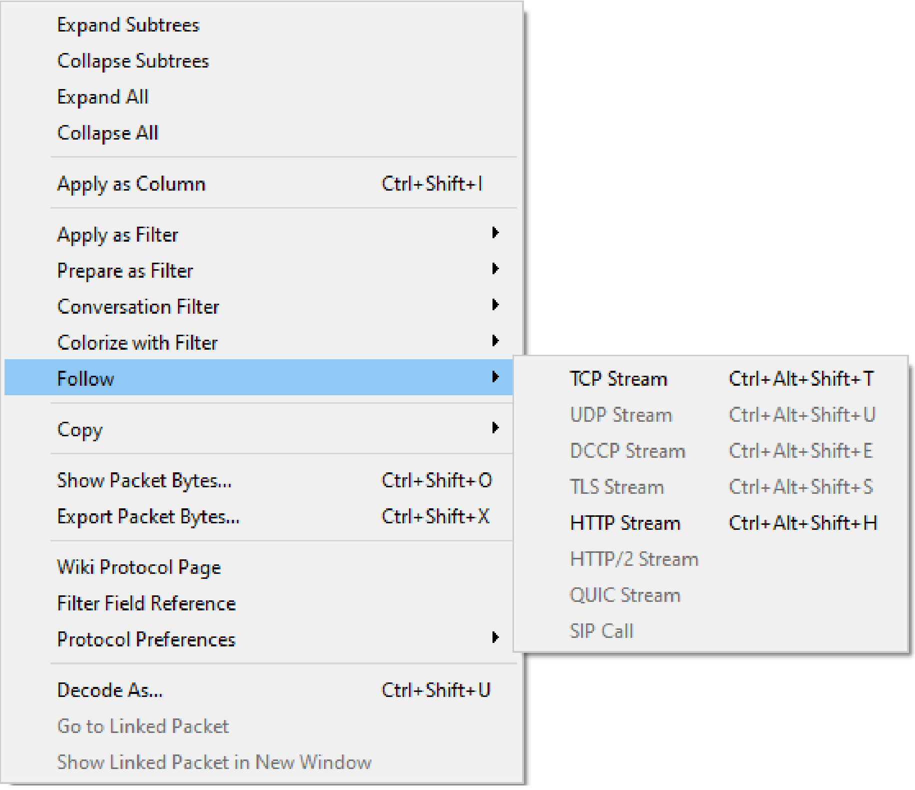
Time	192.168.1.140		174.143.213.184	Comment
0.000000	57678	57678 → http(80) [SYN] Seq=0 ...	80	TCP: 57678 → http(80) [SYN] Seq=0 Win=5840 L...
0.046905	57678	http(80) → 57678 [SYN, ACK] S...	80	TCP: http(80) → 57678 [SYN, ACK] Seq=0 Ack=...
0.000051	57678	57678 → http(80) [ACK] Seq=1 ...	80	TCP: 57678 → http(80) [ACK] Seq=1 Ack=1 Win...
0.000112	57678	GET /images/layout/logo.png H...	80	HTTP: GET /images/layout/logo.png HTTP/1.0
0.047200	57678	http(80) → 57678 [ACK] Seq=1 ...	80	TCP: http(80) → 57678 [ACK] Seq=1 Ack=135 Wi...
0.002405	57678	http(80) → 57678 [ACK] Seq=1 ...	80	TCP: http(80) → 57678 [ACK] Seq=1 Ack=135 Wi...
0.000029	57678	57678 → http(80) [ACK] Seq=1...	80	TCP: 57678 → http(80) [ACK] Seq=135 Ack=144...
0.000083	57678	http(80) → 57678 [ACK] Seq=1...	80	TCP: http(80) → 57678 [ACK] Seq=1449 Ack=13...
0.000004	57678	57678 → http(80) [ACK] Seq=1...	80	TCP: 57678 → http(80) [ACK] Seq=135 Ack=289...

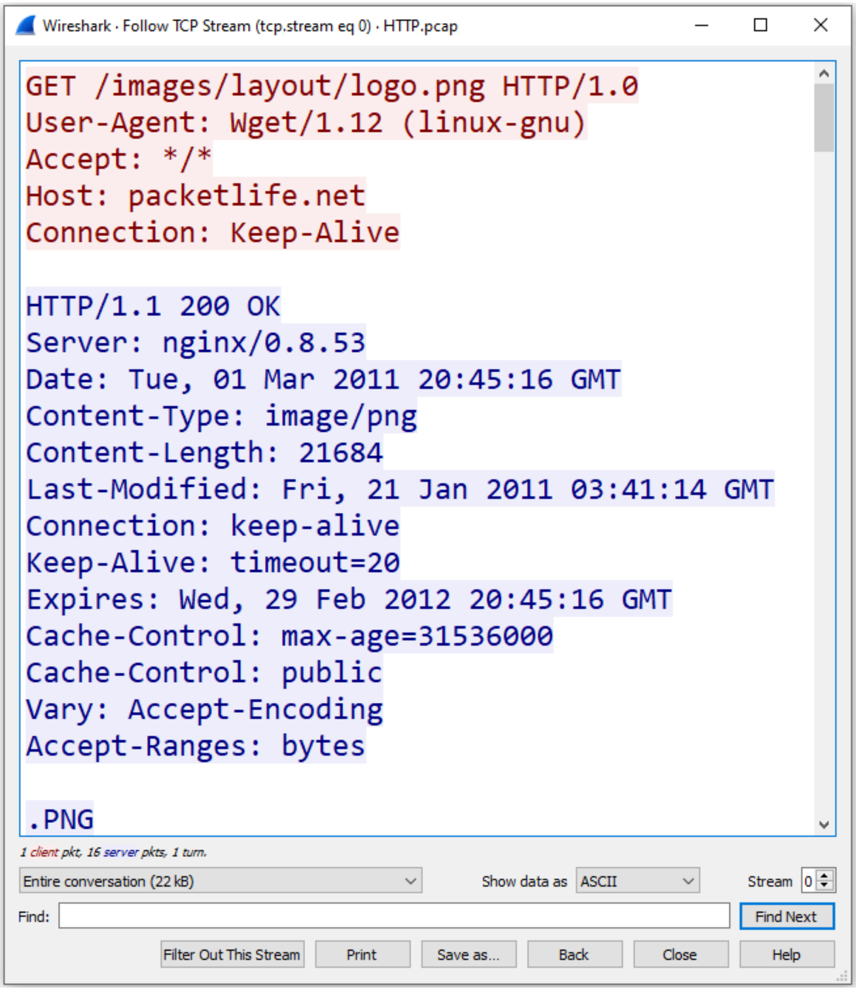
Packet 10: TCP: http(80) → 57678 [ACK] Seq=2897 Ack... TSecr=2216543 [TCP segment of a reassembled PDU]

☐ Limit to display filter

Flow type: All Flows

Addresses: Any

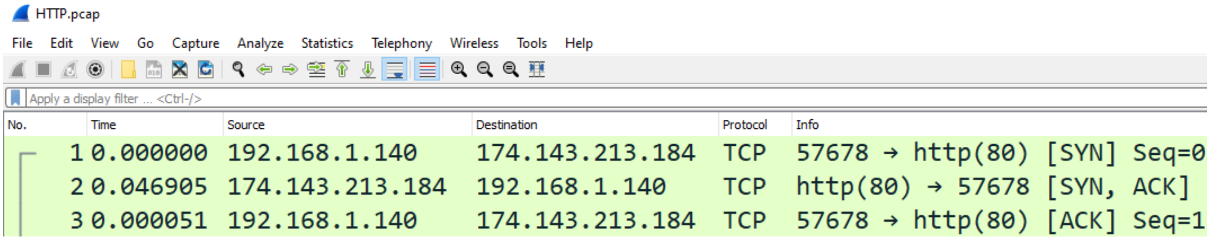

Expand Subtrees
Collapse Subtrees
Expand All
Collapse All
Apply as Column Ctrl+Shift+I
Apply as Filter
Prepare as Filter
Conversation Filter
Colorize with Filter
Follow
Copy
Show Packet Bytes... Ctrl+Shift+O
Export Packet Bytes... Ctrl+Shift+X
Wiki Protocol Page
Filter Field Reference
Protocol Preferences
Decode As... Ctrl+Shift+U
Go to Linked Packet
Show Linked Packet in New Window
TCP Stream Ctrl+Alt+Shift+T
UDP Stream Ctrl+Alt+Shift+U
DCCP Stream Ctrl+Alt+Shift+E
TLS Stream Ctrl+Alt+Shift+S
HTTP Stream Ctrl+Alt+Shift+H
HTTP/2 Stream
QUIC Stream
SIP Call



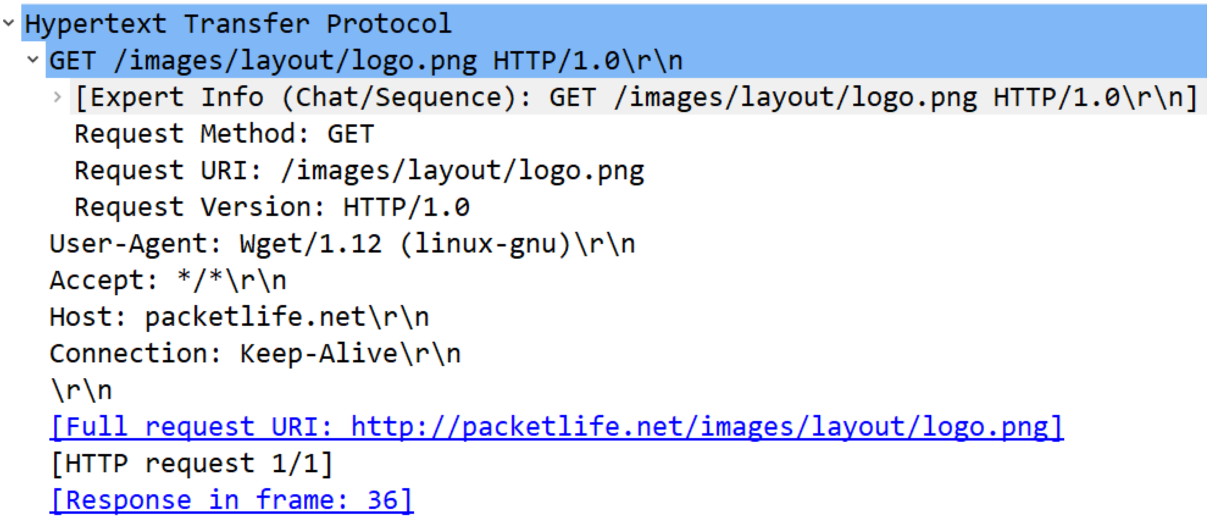
```
GET /images/layout/logo.png HTTP/1.0
User-Agent: Wget/1.12 (linux-gnu)
Accept: */*
Host: packetlife.net
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx/0.8.53
Date: Tue, 01 Mar 2011 20:45:16 GMT
Content-Type: image/png
Content-Length: 21684
Last-Modified: Fri, 21 Jan 2011 03:41:14 GMT
Connection: keep-alive
Keep-Alive: timeout=20
Expires: Wed, 29 Feb 2012 20:45:16 GMT
Cache-Control: max-age=31536000
Cache-Control: public
Vary: Accept-Encoding
Accept-Ranges: bytes

.PNG
```

1 client pkt, 16 server pkts, 1 turn.

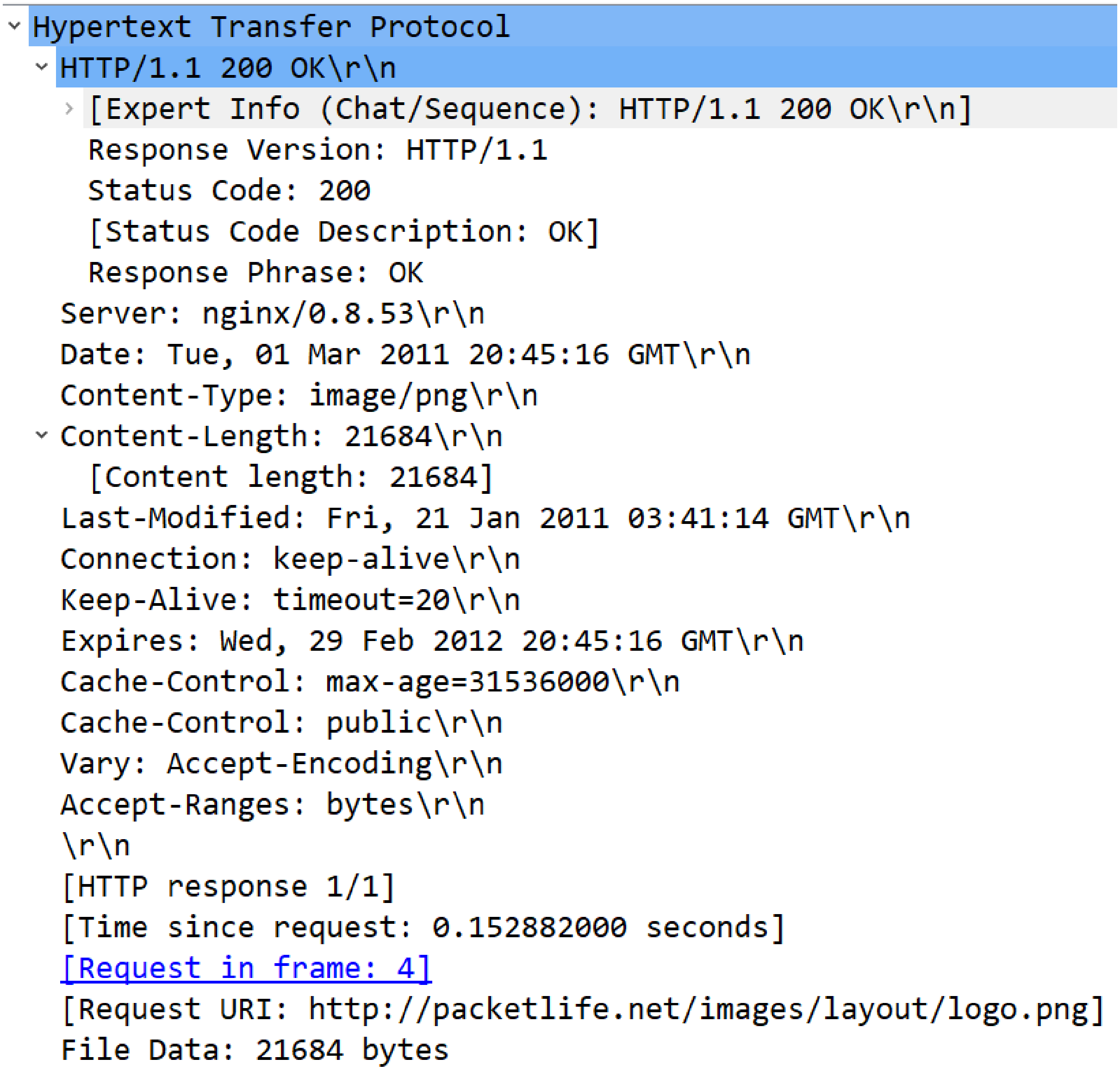
Entire conversation (22 kB)   Show data as ASCII   Stream 0



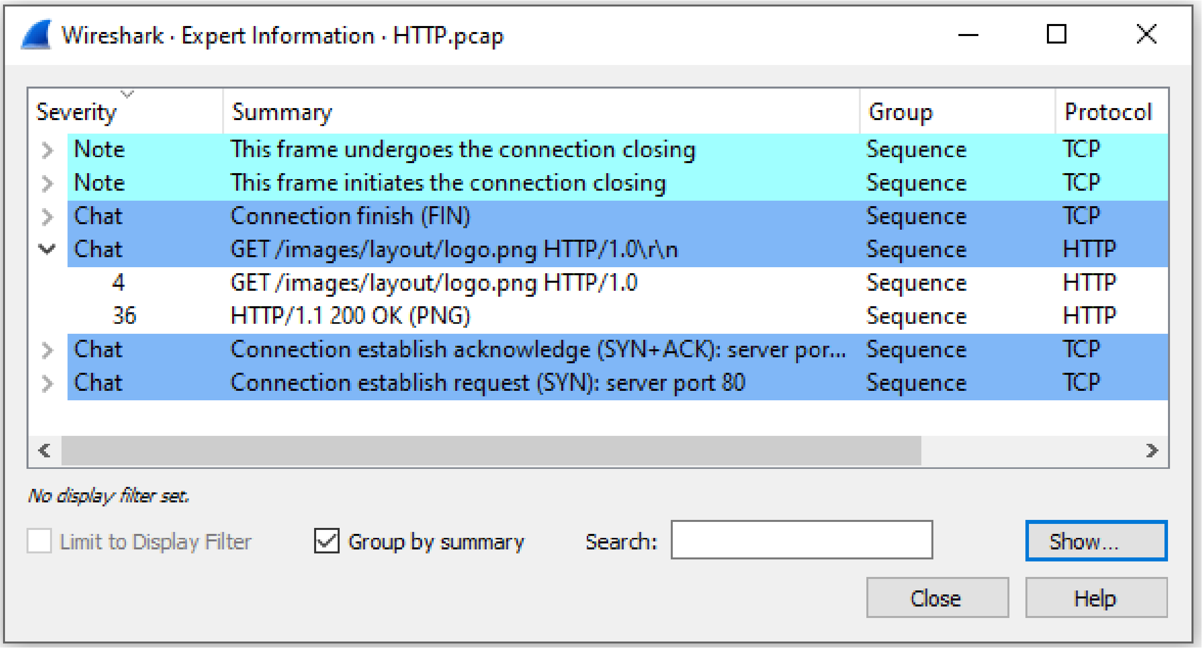
```
No.  Time      Source          Destination     Protocol Info
   1 0.000000  192.168.1.140   174.143.213.184 TCP      57678 → http(80) [SYN] Seq=0
   2 0.046905  174.143.213.184 192.168.1.140   TCP      http(80) → 57678 [SYN, ACK]
   3 0.000051  192.168.1.140   174.143.213.184 TCP      57678 → http(80) [ACK] Seq=1
```



```
⌄ Hypertext Transfer Protocol
  ⌄ GET /images/layout/logo.png HTTP/1.0\r\n
    › [Expert Info (Chat/Sequence): GET /images/layout/logo.png HTTP/1.0\r\n]
      Request Method: GET
      Request URI: /images/layout/logo.png
      Request Version: HTTP/1.0
    User-Agent: Wget/1.12 (linux-gnu)\r\n
    Accept: */*\r\n
    Host: packetlife.net\r\n
    Connection: Keep-Alive\r\n
    \r\n
    [Full request URI: http://packetlife.net/images/layout/logo.png]
    [HTTP request 1/1]
    [Response in frame: 36]
```



```
⌄ Hypertext Transfer Protocol
  ⌄ HTTP/1.1 200 OK\r\n
    › [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
      Response Version: HTTP/1.1
      Status Code: 200
      [Status Code Description: OK]
      Response Phrase: OK
    Server: nginx/0.8.53\r\n
    Date: Tue, 01 Mar 2011 20:45:16 GMT\r\n
    Content-Type: image/png\r\n
  ⌄ Content-Length: 21684\r\n
      [Content length: 21684]
    Last-Modified: Fri, 21 Jan 2011 03:41:14 GMT\r\n
    Connection: keep-alive\r\n
    Keep-Alive: timeout=20\r\n
    Expires: Wed, 29 Feb 2012 20:45:16 GMT\r\n
    Cache-Control: max-age=31536000\r\n
    Cache-Control: public\r\n
    Vary: Accept-Encoding\r\n
    Accept-Ranges: bytes\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.152882000 seconds]
    [Request in frame: 4]
    [Request URI: http://packetlife.net/images/layout/logo.png]
    File Data: 21684 bytes
```

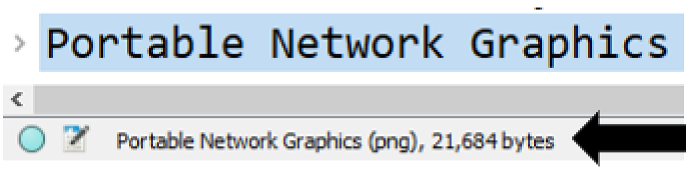


Wireshark · Expert Information · HTTP.pcap

Severity	Summary	Group	Protocol
› Note	This frame undergoes the connection closing	Sequence	TCP
› Note	This frame initiates the connection closing	Sequence	TCP
› Chat	Connection finish (FIN)	Sequence	TCP
⌄ Chat	GET /images/layout/logo.png HTTP/1.0\r\n	Sequence	HTTP
4	GET /images/layout/logo.png HTTP/1.0	Sequence	HTTP
36	HTTP/1.1 200 OK (PNG)	Sequence	HTTP
› Chat	Connection establish acknowledge (SYN+ACK): server por...	Sequence	TCP
› Chat	Connection establish request (SYN): server port 80	Sequence	TCP

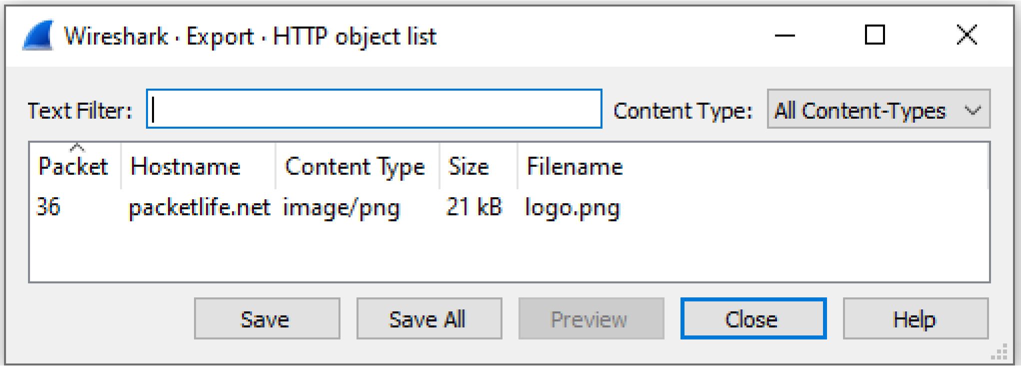
No display filter set.

□ Limit to Display Filter ☑ Group by summary Search:



Portable Network Graphics

Portable Network Graphics (png), 21,684 bytes



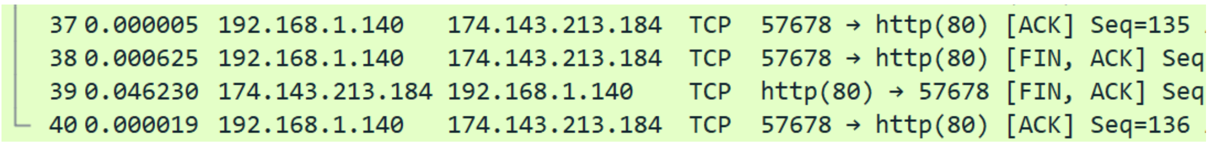
Wireshark · Export · HTTP object list

Text Filter:

Content Type: All Content-Types

Packet	Hostname	Content Type	Size	Filename
36	packetlife.net	image/png	21 kB	logo.png

PacketLife.net

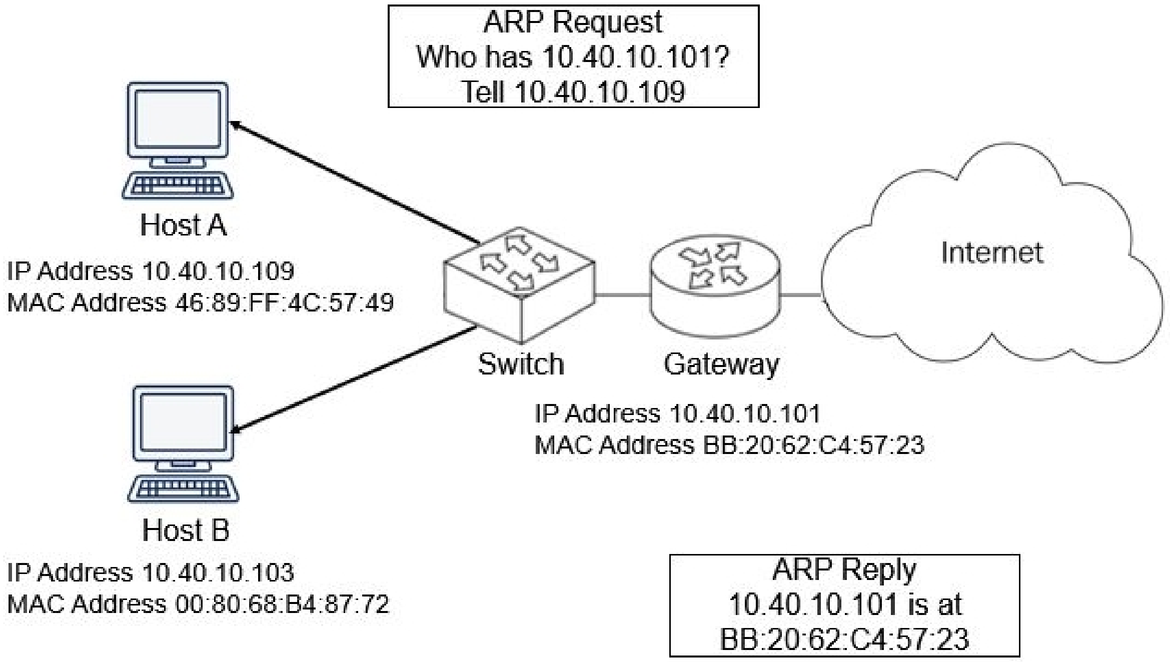


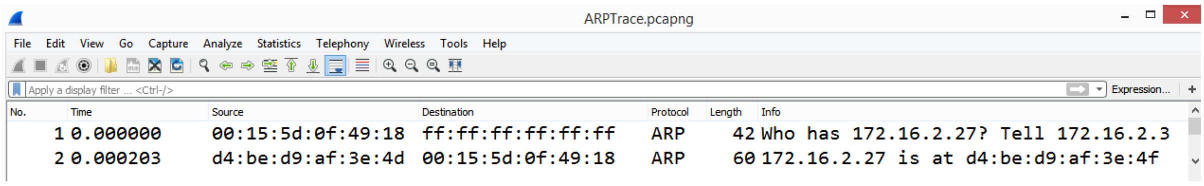
```
37 0.000005 192.168.1.140   174.143.213.184 TCP  57678 → http(80) [ACK] Seq=135
38 0.000625 192.168.1.140   174.143.213.184 TCP  57678 → http(80) [FIN, ACK] Seq
39 0.046230 174.143.213.184 192.168.1.140   TCP  http(80) → 57678 [FIN, ACK] Seq
40 0.000019 192.168.1.140   174.143.213.184 TCP  57678 → http(80) [ACK] Seq=136
```

Chapter 16: Understanding ARP

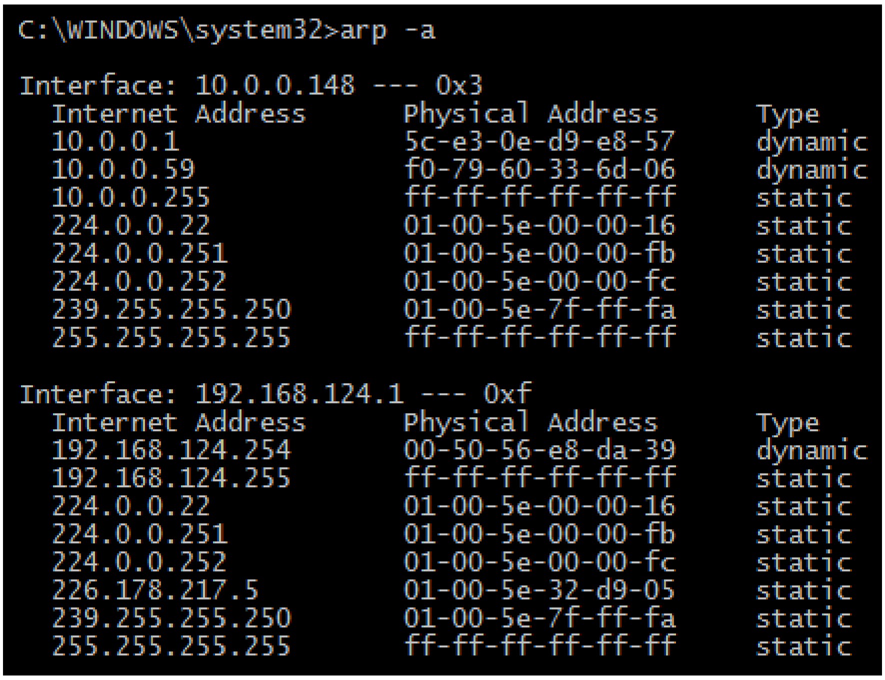
OSI Model

Layer	Name	Role	Protocols	PDU	Address
7	Application	Initiate contact with the network	HTTP, FTP, DNS	Data	
6	Presentation	Formats data, optional compression and encryption		Data	
5	Session	Initiates, maintains and tear down session		Data	
4	Transport	Transports data	TCP, UDP	Segment	Port
3	Network	Addressing, routing	IP, ICMP ARP	Packet	IP
2	Data Link	Frame formation	Ethernet II	Frame	MAC
1	Physical	Data is transmitted on the media		Bits	

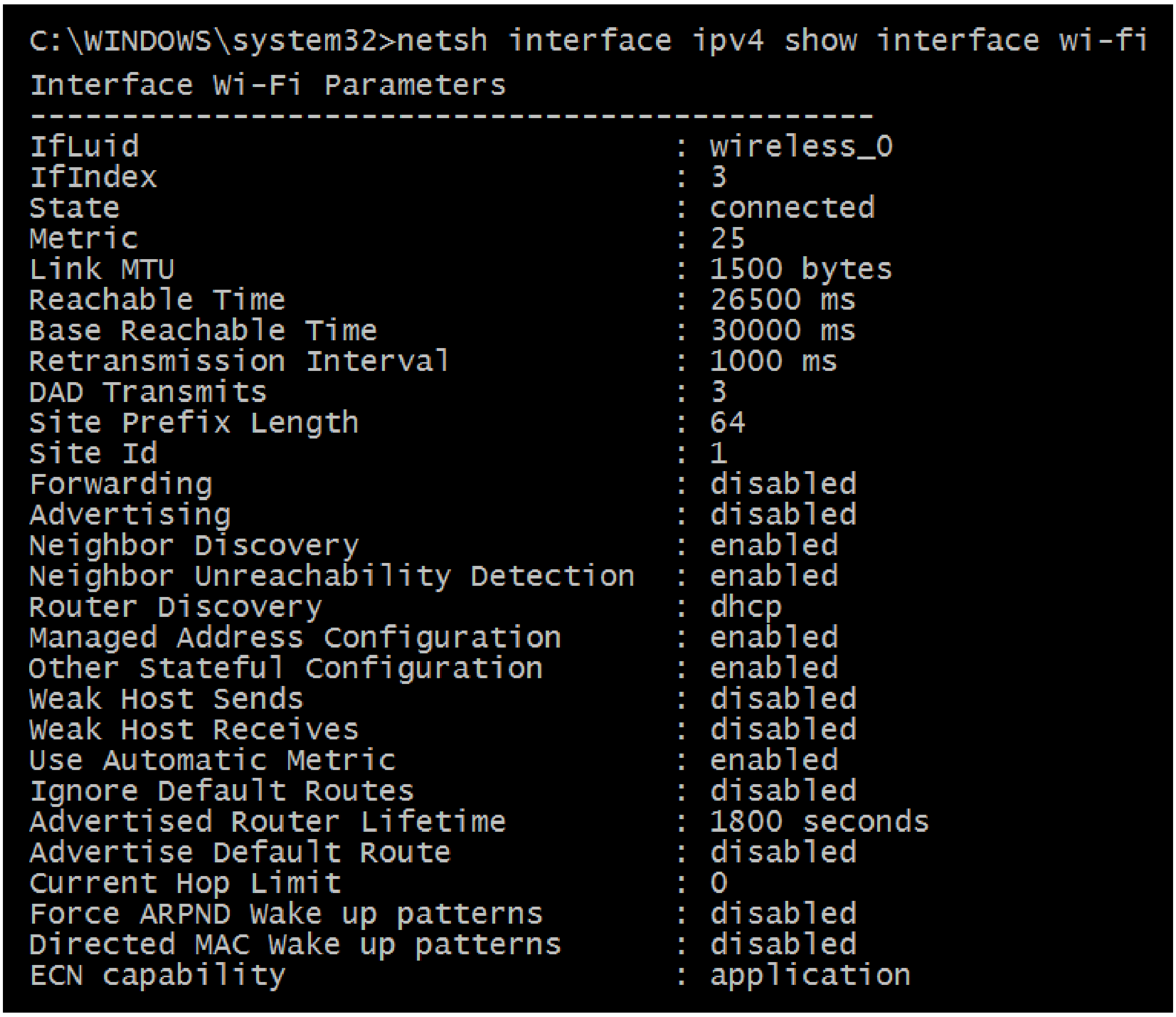




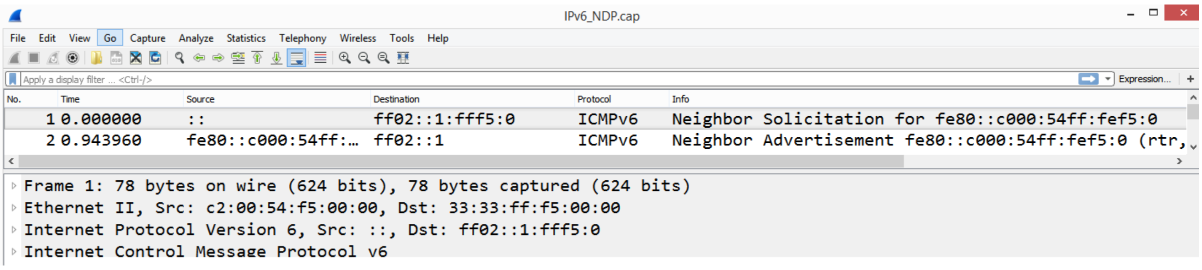
```
No.  Time      Source             Destination        Protocol Length Info
   1 0.000000  00:15:5d:0f:49:18  ff:ff:ff:ff:ff:ff  ARP        42 Who has 172.16.2.27? Tell 172.16.2.3
   2 0.000203  d4:be:d9:af:3e:4d  00:15:5d:0f:49:18  ARP        60 172.16.2.27 is at d4:be:d9:af:3e:4f
```



```
C:\WINDOWS\system32>arp -a

Interface: 10.0.0.148 --- 0x3
  Internet Address      Physical Address      Type
  10.0.0.1              5c-e3-0e-d9-e8-57     dynamic
  10.0.0.59             f0-79-60-33-6d-06     dynamic
  10.0.0.255            ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 192.168.124.1 --- 0xf
  Internet Address      Physical Address      Type
  192.168.124.254       00-50-56-e8-da-39     dynamic
  192.168.124.255       ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  226.178.217.5         01-00-5e-32-d9-05     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

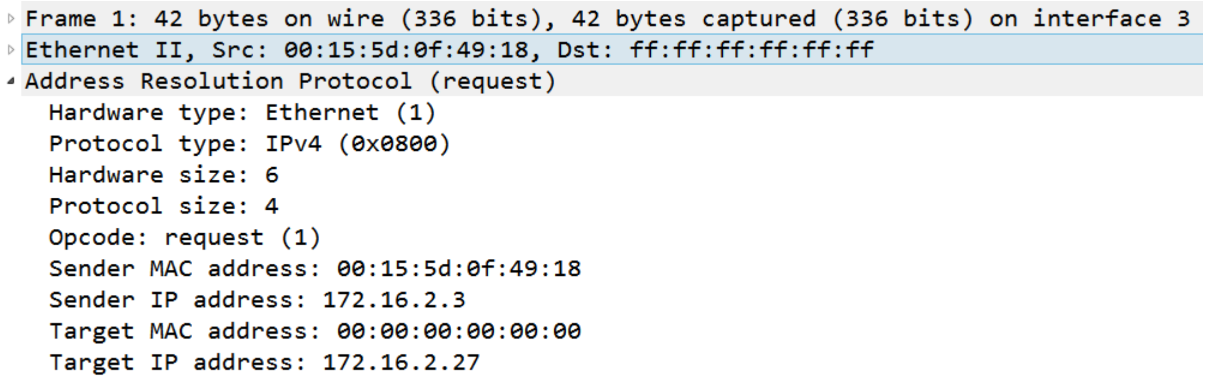


```
C:\WINDOWS\system32>netsh interface ipv4 show interface wi-fi

Interface Wi-Fi Parameters
----------------------------------------------
IfLuid                             : wireless_0
IfIndex                            : 3
State                              : connected
Metric                             : 25
Link MTU                           : 1500 bytes
Reachable Time                     : 26500 ms
Base Reachable Time                : 30000 ms
Retransmission Interval            : 1000 ms
DAD Transmits                      : 3
Site Prefix Length                 : 64
Site Id                            : 1
Forwarding                         : disabled
Advertising                        : disabled
Neighbor Discovery                 : enabled
Neighbor Unreachability Detection  : enabled
Router Discovery                   : dhcp
Managed Address Configuration      : enabled
Other Stateful Configuration       : enabled
Weak Host Sends                    : disabled
Weak Host Receives                 : disabled
Use Automatic Metric               : enabled
Ignore Default Routes              : disabled
Advertised Router Lifetime         : 1800 seconds
Advertise Default Route            : disabled
Current Hop Limit                  : 0
Force ARPND Wake up patterns       : disabled
Directed MAC Wake up patterns      : disabled
ECN capability                     : application
```

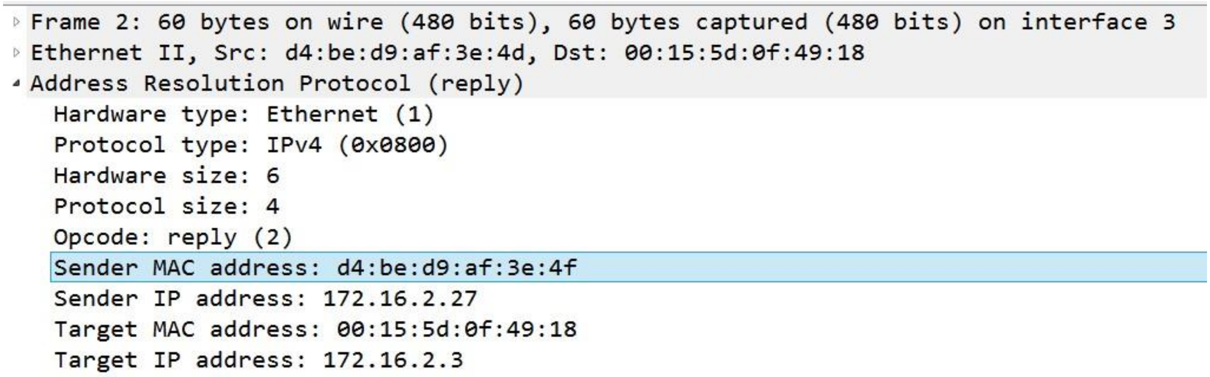


IPv6_NDP.cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...

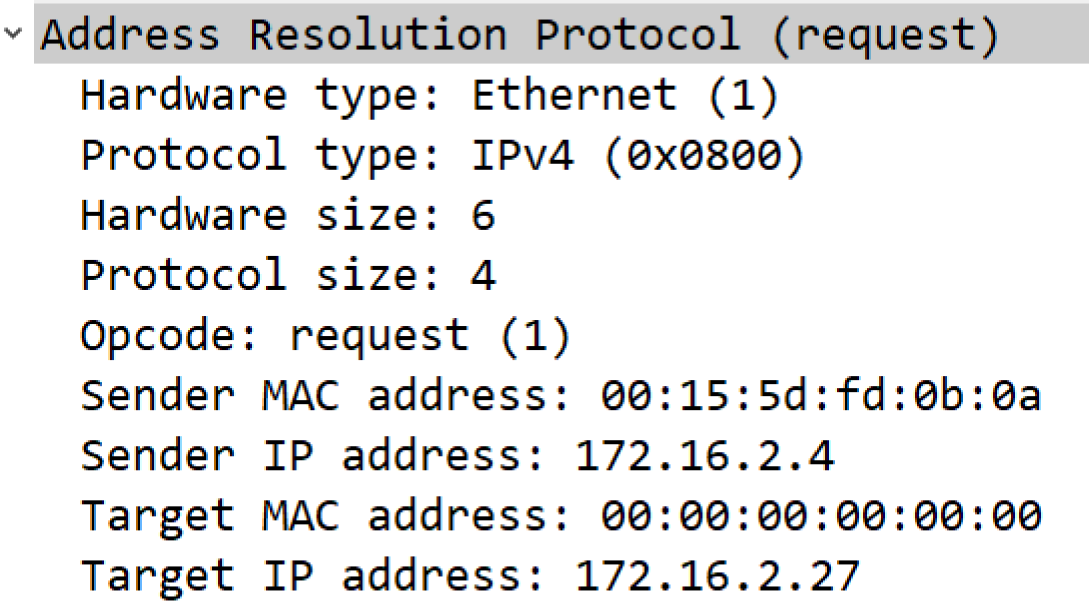
```
No. Time        Source             Destination      Protocol  Info
  1 0.000000    ::                 ff02::1:fff5:0   ICMPv6    Neighbor Solicitation for fe80::c000:54ff:fef5:0
  2 0.943960    fe80::c000:54ff:…  ff02::1          ICMPv6    Neighbor Advertisement fe80::c000:54ff:fef5:0 (rtr,

Frame 1: 78 bytes on wire (624 bits), 78 bytes captured (624 bits)
Ethernet II, Src: c2:00:54:f5:00:00, Dst: 33:33:ff:f5:00:00
Internet Protocol Version 6, Src: ::, Dst: ff02::1:fff5:0
Internet Control Message Protocol v6
```



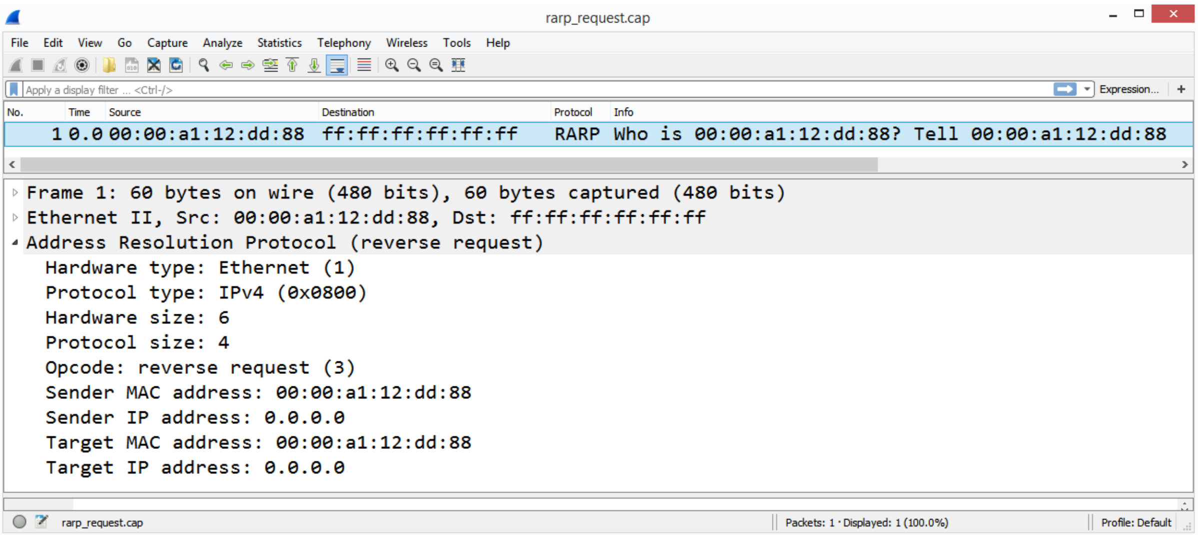
```
Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 3
Ethernet II, Src: 00:15:5d:0f:49:18, Dst: ff:ff:ff:ff:ff:ff
Address Resolution Protocol (request)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (1)
  Sender MAC address: 00:15:5d:0f:49:18
  Sender IP address: 172.16.2.3
  Target MAC address: 00:00:00:00:00:00
  Target IP address: 172.16.2.27
```



```
Frame 2: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 3
Ethernet II, Src: d4:be:d9:af:3e:4d, Dst: 00:15:5d:0f:49:18
Address Resolution Protocol (reply)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: reply (2)
  Sender MAC address: d4:be:d9:af:3e:4f
  Sender IP address: 172.16.2.27
  Target MAC address: 00:15:5d:0f:49:18
  Target IP address: 172.16.2.3
```

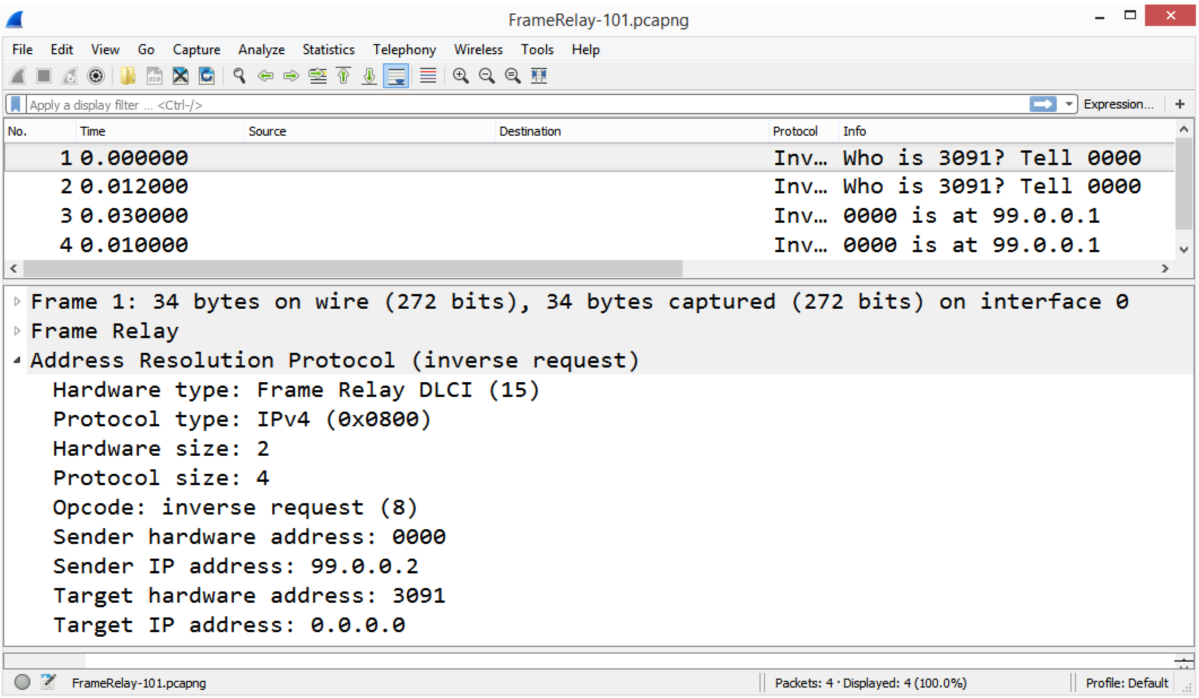


```
Address Resolution Protocol (request)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (1)
  Sender MAC address: 00:15:5d:fd:0b:0a
  Sender IP address: 172.16.2.4
  Target MAC address: 00:00:00:00:00:00
  Target IP address: 172.16.2.27
```


rarp_request.cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
rarp_request.cap
Packets: 1 · Displayed: 1 (100.0%)
Profile: Default

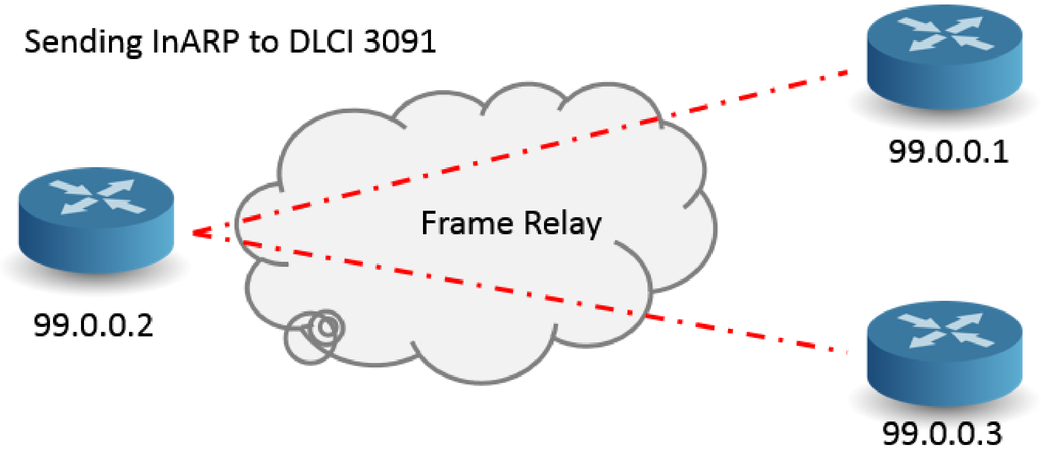
```
No.  Time  Source             Destination        Protocol  Info
   1 0.0   00:00:a1:12:dd:88  ff:ff:ff:ff:ff:ff  RARP      Who is 00:00:a1:12:dd:88? Tell 00:00:a1:12:dd:88
```

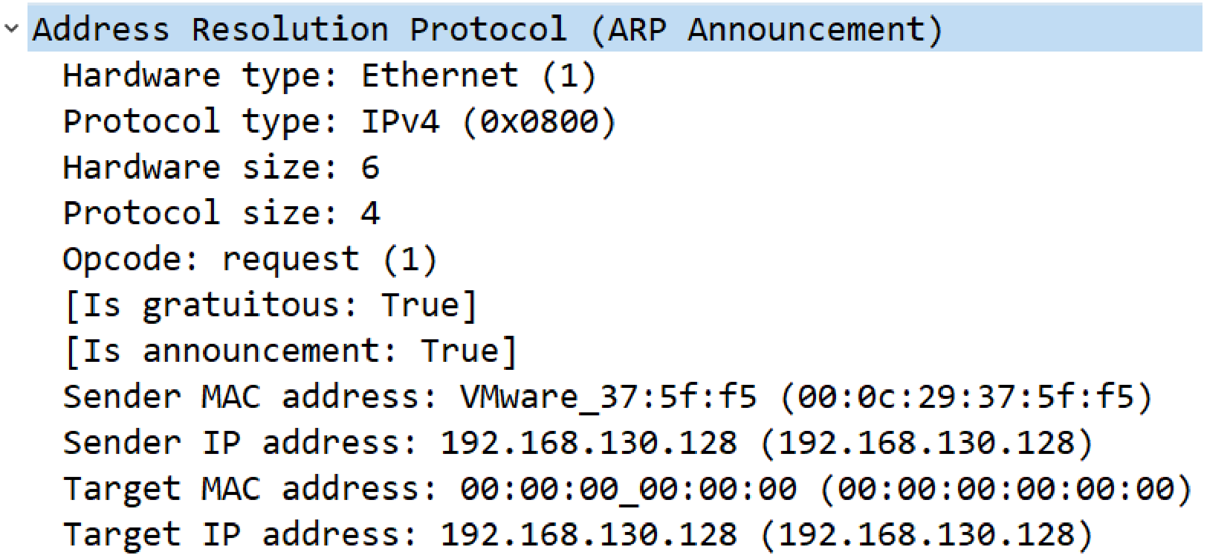
```
▹ Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
▹ Ethernet II, Src: 00:00:a1:12:dd:88, Dst: ff:ff:ff:ff:ff:ff
◢ Address Resolution Protocol (reverse request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reverse request (3)
    Sender MAC address: 00:00:a1:12:dd:88
    Sender IP address: 0.0.0.0
    Target MAC address: 00:00:a1:12:dd:88
    Target IP address: 0.0.0.0
```


FrameRelay-101.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
FrameRelay-101.pcapng
Packets: 4 · Displayed: 4 (100.0%)
Profile: Default

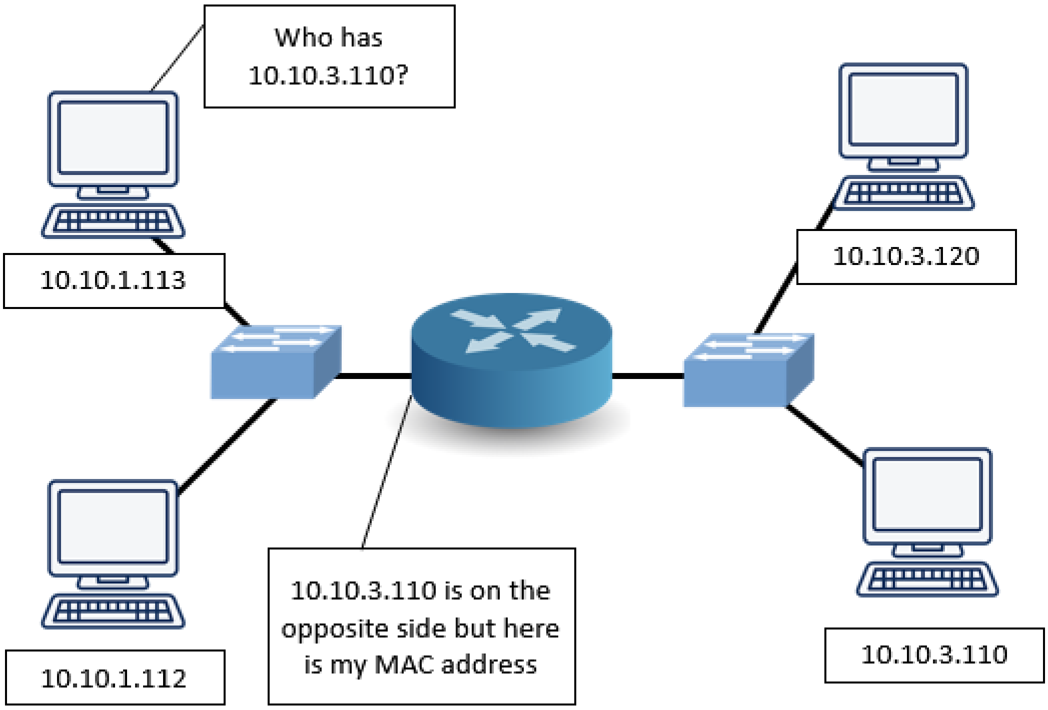
```
No.  Time      Source  Destination  Protocol  Info
   1 0.000000                       Inv…      Who is 3091? Tell 0000
   2 0.012000                       Inv…      Who is 3091? Tell 0000
   3 0.030000                       Inv…      0000 is at 99.0.0.1
   4 0.010000                       Inv…      0000 is at 99.0.0.1
```

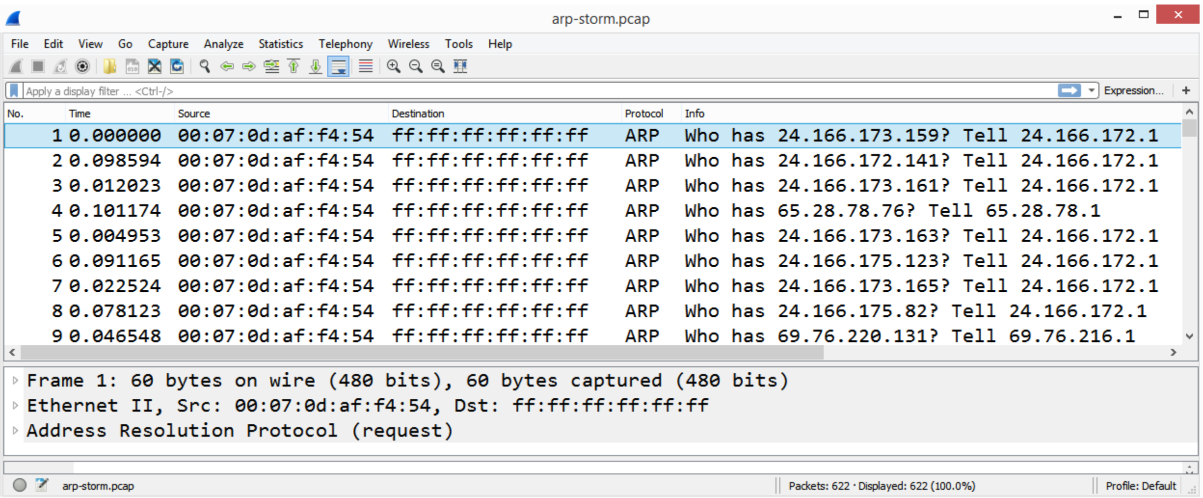
```
▹ Frame 1: 34 bytes on wire (272 bits), 34 bytes captured (272 bits) on interface 0
▹ Frame Relay
◢ Address Resolution Protocol (inverse request)
    Hardware type: Frame Relay DLCI (15)
    Protocol type: IPv4 (0x0800)
    Hardware size: 2
    Protocol size: 4
    Opcode: inverse request (8)
    Sender hardware address: 0000
    Sender IP address: 99.0.0.2
    Target hardware address: 3091
    Target IP address: 0.0.0.0
```



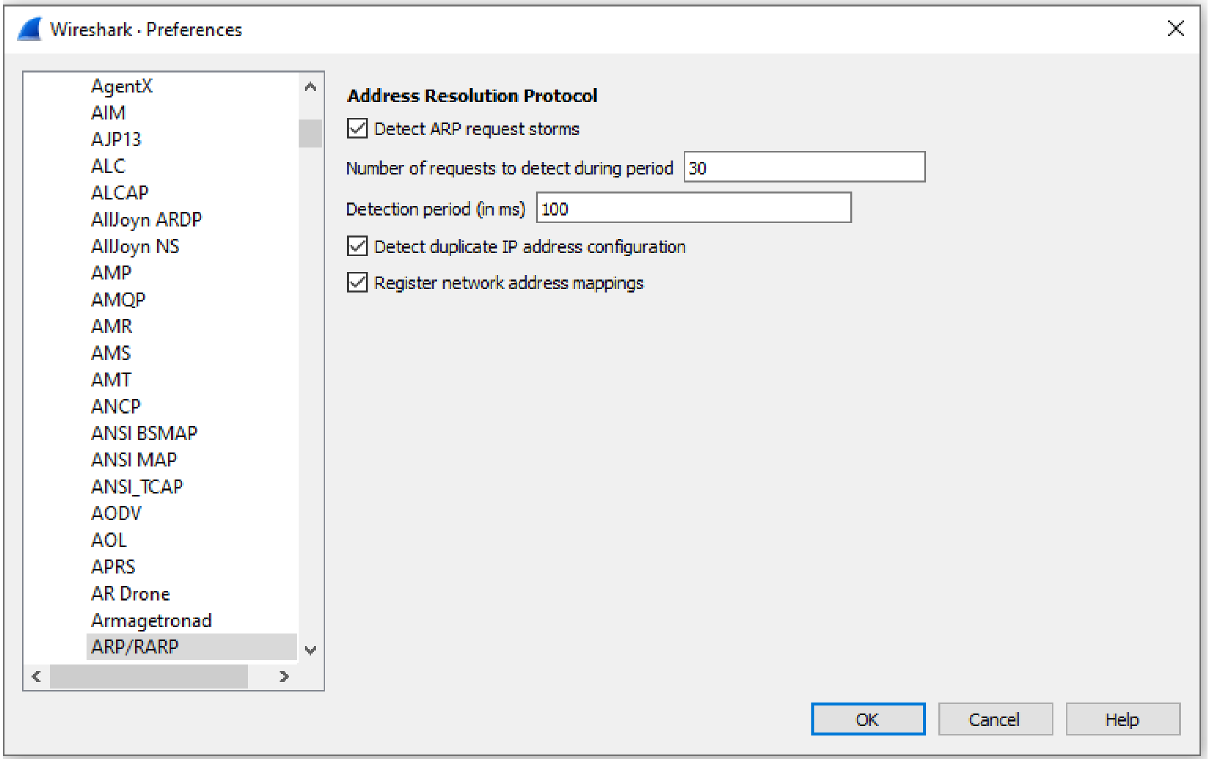


```
⌄ Address Resolution Protocol (ARP Announcement)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    [Is gratuitous: True]
    [Is announcement: True]
    Sender MAC address: VMware_37:5f:f5 (00:0c:29:37:5f:f5)
    Sender IP address: 192.168.130.128 (192.168.130.128)
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.130.128 (192.168.130.128)
```




arp-storm.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...

```
No. Time      Source            Destination       Protocol Info
  1 0.000000  00:07:0d:af:f4:54 ff:ff:ff:ff:ff:ff ARP      Who has 24.166.173.159? Tell 24.166.172.1
  2 0.098594  00:07:0d:af:f4:54 ff:ff:ff:ff:ff:ff ARP      Who has 24.166.172.141? Tell 24.166.172.1
  3 0.012023  00:07:0d:af:f4:54 ff:ff:ff:ff:ff:ff ARP      Who has 24.166.173.161? Tell 24.166.172.1
  4 0.101174  00:07:0d:af:f4:54 ff:ff:ff:ff:ff:ff ARP      Who has 65.28.78.76? Tell 65.28.78.1
  5 0.004953  00:07:0d:af:f4:54 ff:ff:ff:ff:ff:ff ARP      Who has 24.166.173.163? Tell 24.166.172.1
  6 0.091165  00:07:0d:af:f4:54 ff:ff:ff:ff:ff:ff ARP      Who has 24.166.175.123? Tell 24.166.172.1
  7 0.022524  00:07:0d:af:f4:54 ff:ff:ff:ff:ff:ff ARP      Who has 24.166.173.165? Tell 24.166.172.1
  8 0.078123  00:07:0d:af:f4:54 ff:ff:ff:ff:ff:ff ARP      Who has 24.166.175.82? Tell 24.166.172.1
  9 0.046548  00:07:0d:af:f4:54 ff:ff:ff:ff:ff:ff ARP      Who has 69.76.220.131? Tell 69.76.216.1

Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
Ethernet II, Src: 00:07:0d:af:f4:54, Dst: ff:ff:ff:ff:ff:ff
Address Resolution Protocol (request)

arp-storm.pcap    Packets: 622 · Displayed: 622 (100.0%)    Profile: Default
```



Address Resolution Protocol

☑ Detect ARP request storms

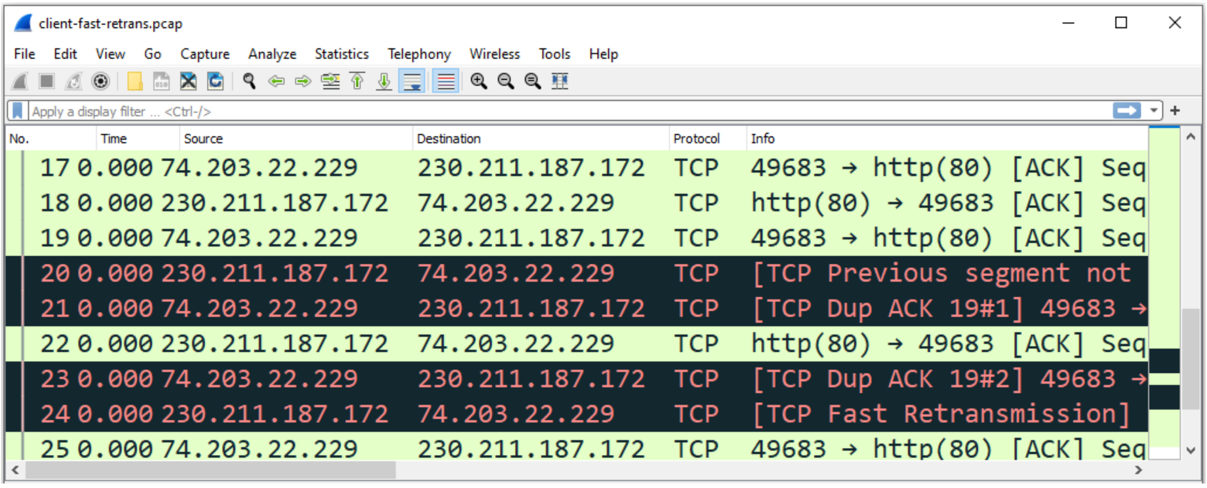
Number of requests to detect during period: 30

Detection period (in ms): 100

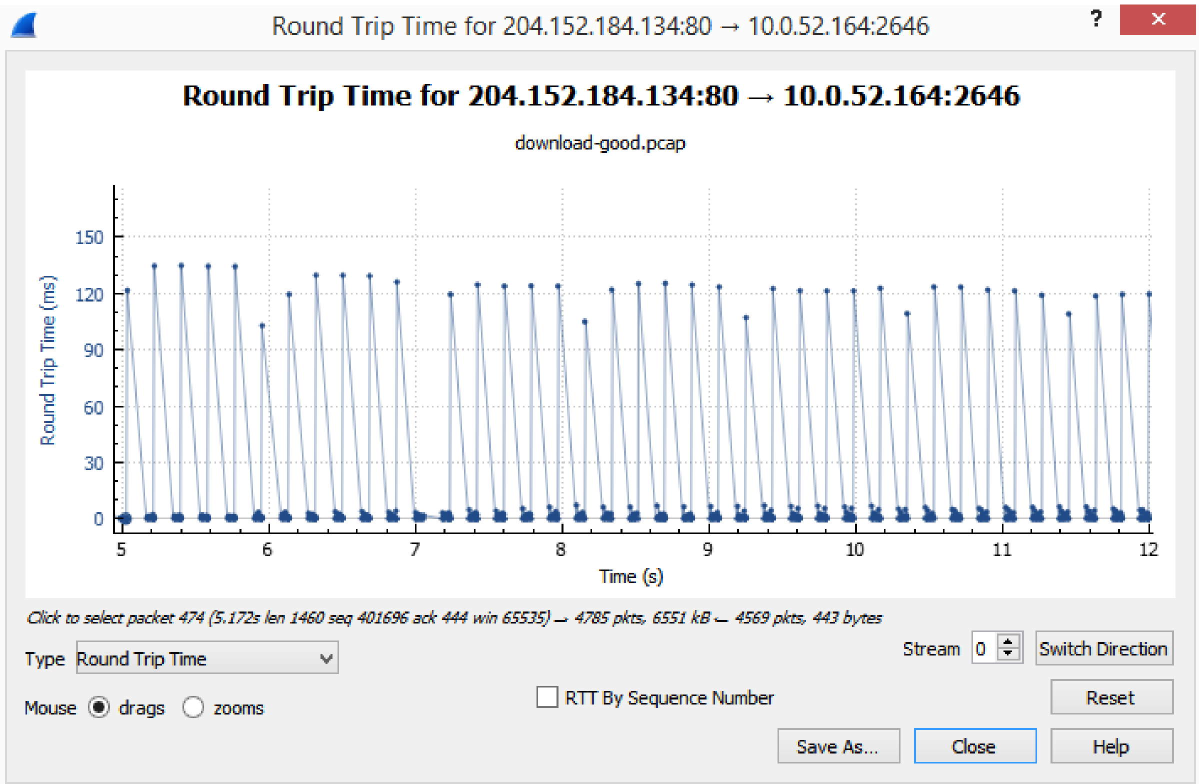
☑ Detect duplicate IP address configuration

☑ Register network address mappings

Chapter 17: Determining Network Latency Issues


client-fast-retrans.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Info
17	0.000	74.203.22.229	230.211.187.172	TCP	49683 → http(80) [ACK] Seq
18	0.000	230.211.187.172	74.203.22.229	TCP	http(80) → 49683 [ACK] Seq
19	0.000	74.203.22.229	230.211.187.172	TCP	49683 → http(80) [ACK] Seq
20	0.000	230.211.187.172	74.203.22.229	TCP	[TCP Previous segment not
21	0.000	74.203.22.229	230.211.187.172	TCP	[TCP Dup ACK 19#1] 49683 →
22	0.000	230.211.187.172	74.203.22.229	TCP	http(80) → 49683 [ACK] Seq
23	0.000	74.203.22.229	230.211.187.172	TCP	[TCP Dup ACK 19#2] 49683 →
24	0.000	230.211.187.172	74.203.22.229	TCP	[TCP Fast Retransmission]
25	0.000	74.203.22.229	230.211.187.172	TCP	49683 → http(80) [ACK] Seq


Round Trip Time for 204.152.184.134:80 → 10.0.52.164:2646
Round Trip Time for 204.152.184.134:80 → 10.0.52.164:2646
download-good.pcap
Round Trip Time (ms)
150
120
90
60
30
0
5
6
7
8
9
10
11
12
Time (s)
Switch Direction
Reset
Save As...
Close
Help

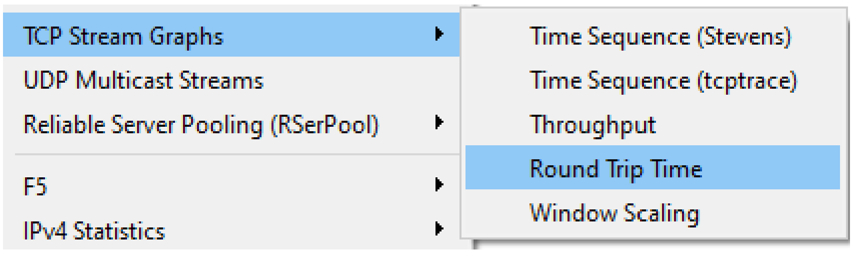
Click to select packet 474 (5.172s len 1460 seq 401696 ack 444 win 65535) ⇀ 4785 pkts, 6551 kB ↽ 4569 pkts, 443 bytes

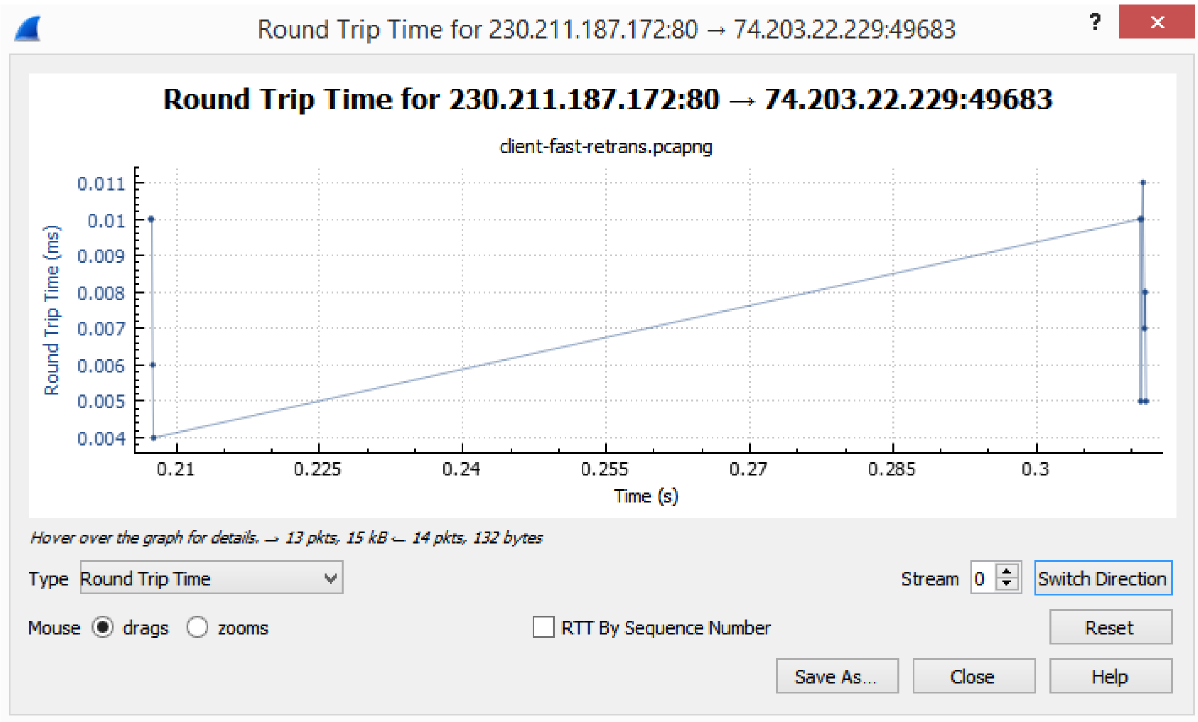
Type: Round Trip Time

Stream: 0

Mouse ● drags ○ zooms

□ RTT By Sequence Number




Round Trip Time for 230.211.187.172:80 → 74.203.22.229:49683
?
Round Trip Time for 230.211.187.172:80 → 74.203.22.229:49683
client-fast-retrans.pcapng
Round Trip Time (ms)
0.011
0.01
0.009
0.008
0.007
0.006
0.005
0.004
0.21
0.225
0.24
0.255
0.27
0.285
0.3
Time (s)
Switch Direction
Reset
Save As...
Close
Help

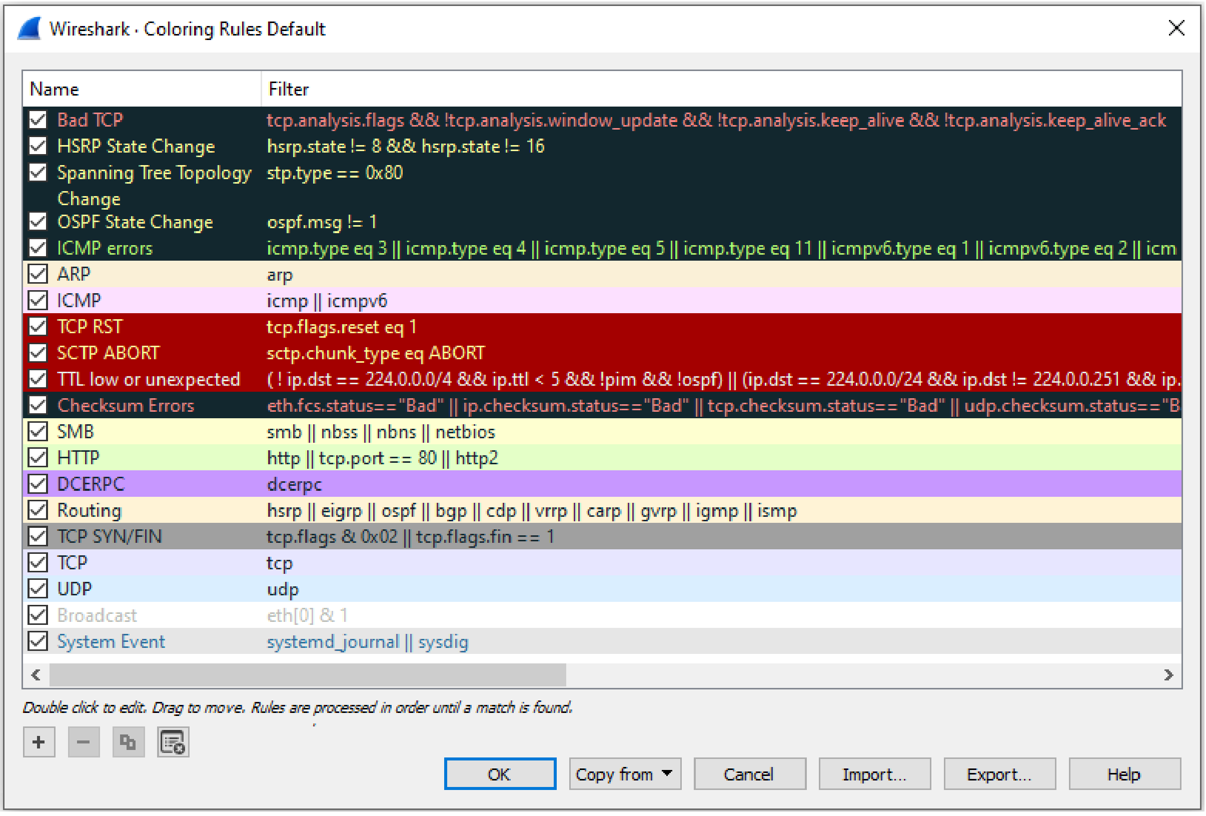
Hover over the graph for details. → 13 pkts, 15 kB ← 14 pkts, 132 bytes

Type Round Trip Time

Stream 0

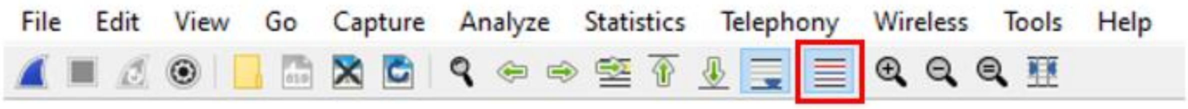
Mouse ● drags ○ zooms

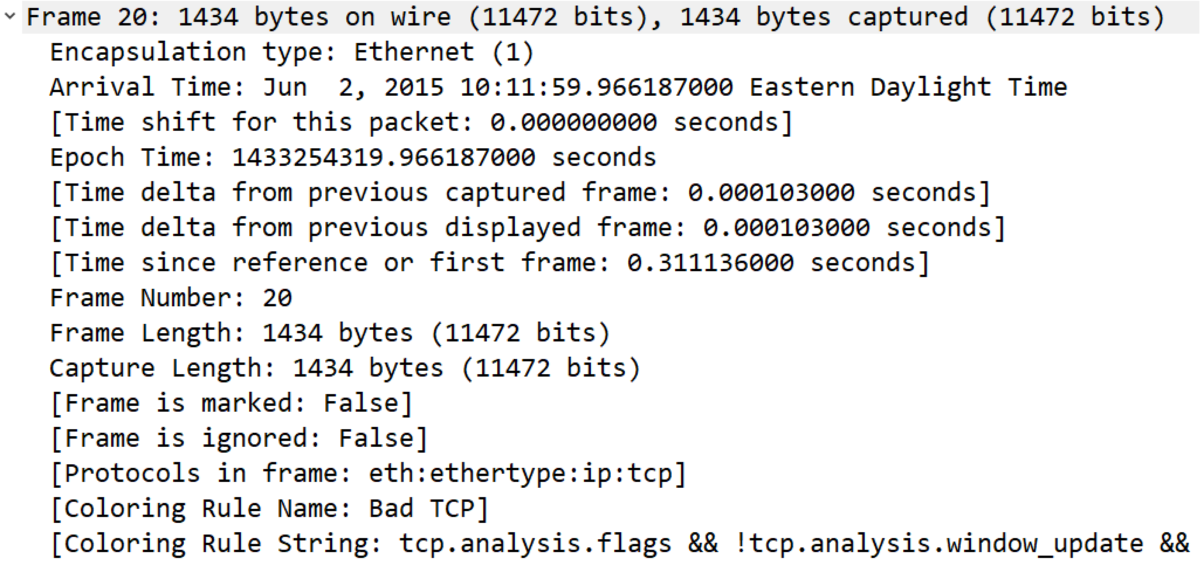
☐ RTT By Sequence Number



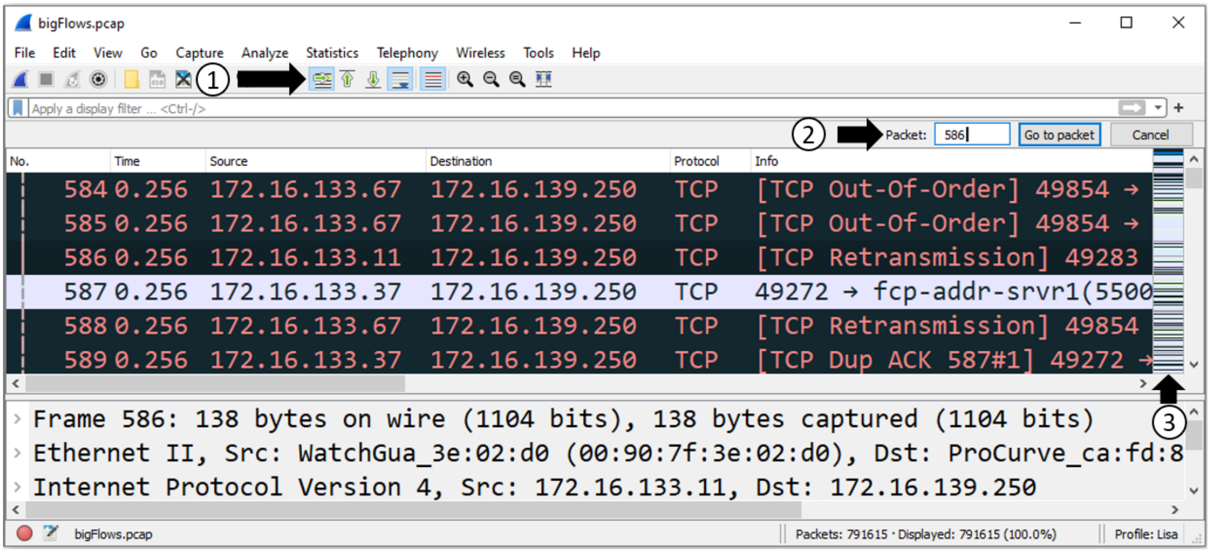
Name	Filter
☑ Bad TCP	tcp.analysis.flags && !tcp.analysis.window_update && !tcp.analysis.keep_alive && !tcp.analysis.keep_alive_ack
☑ HSRP State Change	hsrp.state != 8 && hsrp.state != 16
☑ Spanning Tree Topology Change	stp.type == 0x80
☑ OSPF State Change	ospf.msg != 1
☑ ICMP errors	icmp.type eq 3 || icmp.type eq 4 || icmp.type eq 5 || icmp.type eq 11 || icmpv6.type eq 1 || icmpv6.type eq 2 || icm
☑ 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.
☑ Checksum Errors	eth.fcs.status=="Bad" || ip.checksum.status=="Bad" || tcp.checksum.status=="Bad" || udp.checksum.status=="B
☑ SMB	smb || nbss || nbns || netbios
☑ HTTP	http || tcp.port == 80 || http2
☑ 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
☑ System Event	systemd_journal || sysdig

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





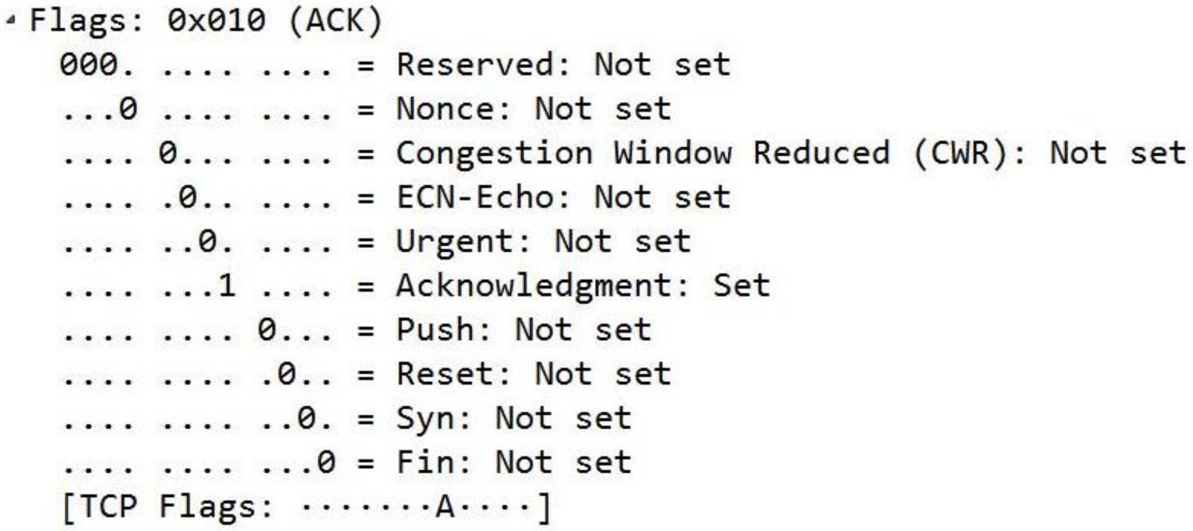
```
⌄ Frame 20: 1434 bytes on wire (11472 bits), 1434 bytes captured (11472 bits)
    Encapsulation type: Ethernet (1)
    Arrival Time: Jun  2, 2015 10:11:59.966187000 Eastern Daylight Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1433254319.966187000 seconds
    [Time delta from previous captured frame: 0.000103000 seconds]
    [Time delta from previous displayed frame: 0.000103000 seconds]
    [Time since reference or first frame: 0.311136000 seconds]
    Frame Number: 20
    Frame Length: 1434 bytes (11472 bits)
    Capture Length: 1434 bytes (11472 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp]
    [Coloring Rule Name: Bad TCP]
    [Coloring Rule String: tcp.analysis.flags && !tcp.analysis.window_update &&
```


bigFlows.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
1
Apply a display filter ... <Ctrl-/>
2
Go to packet
Cancel
3

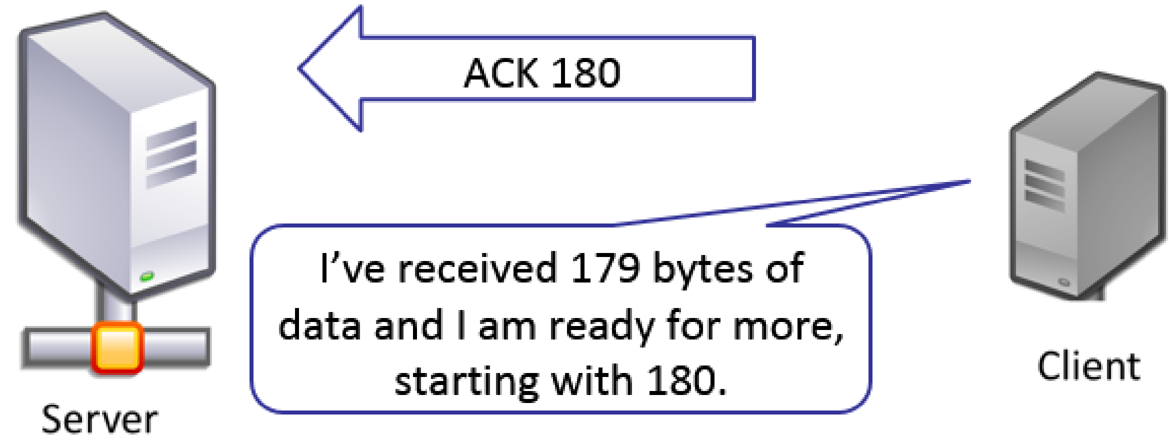
Packet: 586

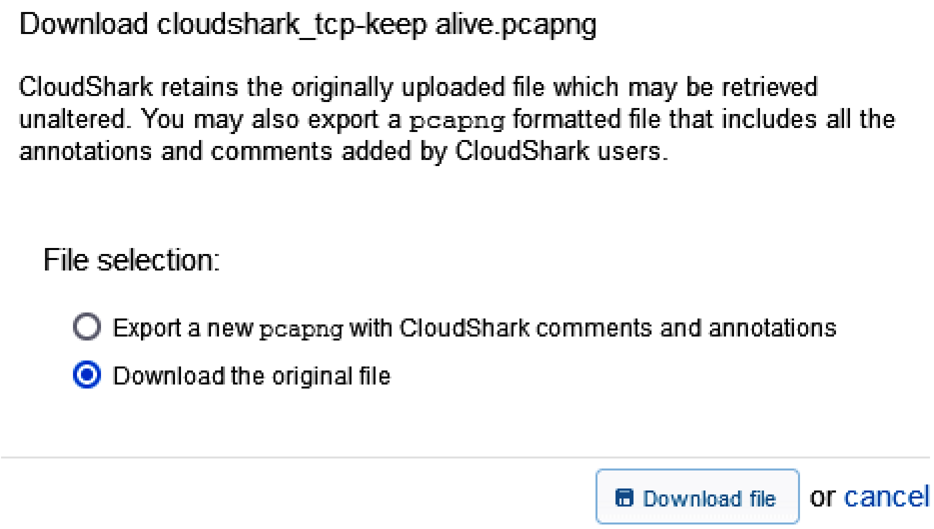
```
No.  Time   Source          Destination      Protocol  Info
 584 0.256  172.16.133.67   172.16.139.250   TCP       [TCP Out-Of-Order] 49854 →
 585 0.256  172.16.133.67   172.16.139.250   TCP       [TCP Out-Of-Order] 49854 →
 586 0.256  172.16.133.11   172.16.139.250   TCP       [TCP Retransmission] 49283
 587 0.256  172.16.133.37   172.16.139.250   TCP       49272 → fcp-addr-srvr1(5500
 588 0.256  172.16.133.67   172.16.139.250   TCP       [TCP Retransmission] 49854
 589 0.256  172.16.133.37   172.16.139.250   TCP       [TCP Dup ACK 587#1] 49272 →

> Frame 586: 138 bytes on wire (1104 bits), 138 bytes captured (1104 bits)
> Ethernet II, Src: WatchGua_3e:02:d0 (00:90:7f:3e:02:d0), Dst: ProCurve_ca:fd:8
> Internet Protocol Version 4, Src: 172.16.133.11, Dst: 172.16.139.250
```

bigFlows.pcap | Packets: 791615 · Displayed: 791615 (100.0%) | Profile: Lisa



```
◢ Flags: 0x010 (ACK)
   000. .... .... = Reserved: Not set
   ...0 .... .... = Nonce: Not set
   .... 0... .... = Congestion Window Reduced (CWR): Not set
   .... .0.. .... = ECN-Echo: Not set
   .... ..0. .... = Urgent: Not set
   .... ...1 .... = Acknowledgment: Set
   .... .... 0... = Push: Not set
   .... .... .0.. = Reset: Not set
   .... .... ..0. = Syn: Not set
   .... .... ...0 = Fin: Not set
   [TCP Flags: ·······A····]
```


ACK 180
I've received 179 bytes of data and I am ready for more, starting with 180.
Server
Client



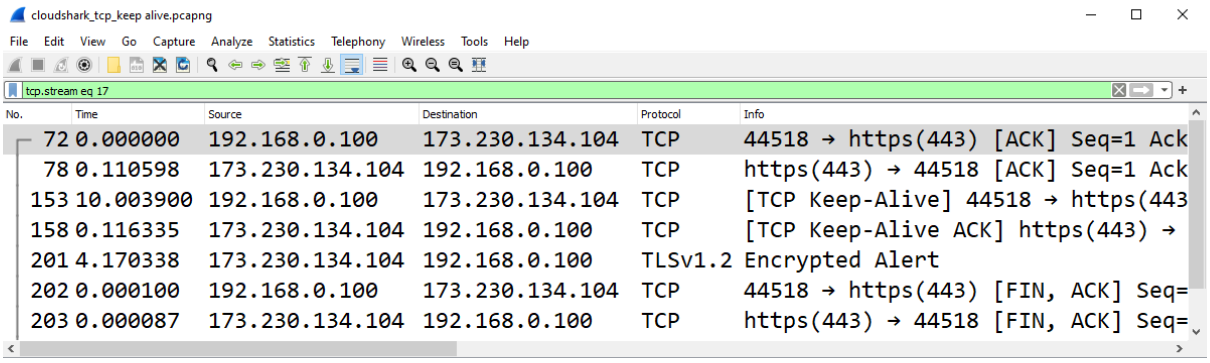
Download cloudshark_tcp-keep alive.pcapng

CloudShark retains the originally uploaded file which may be retrieved unaltered. You may also export a `pcapng` formatted file that includes all the annotations and comments added by CloudShark users.

File selection:

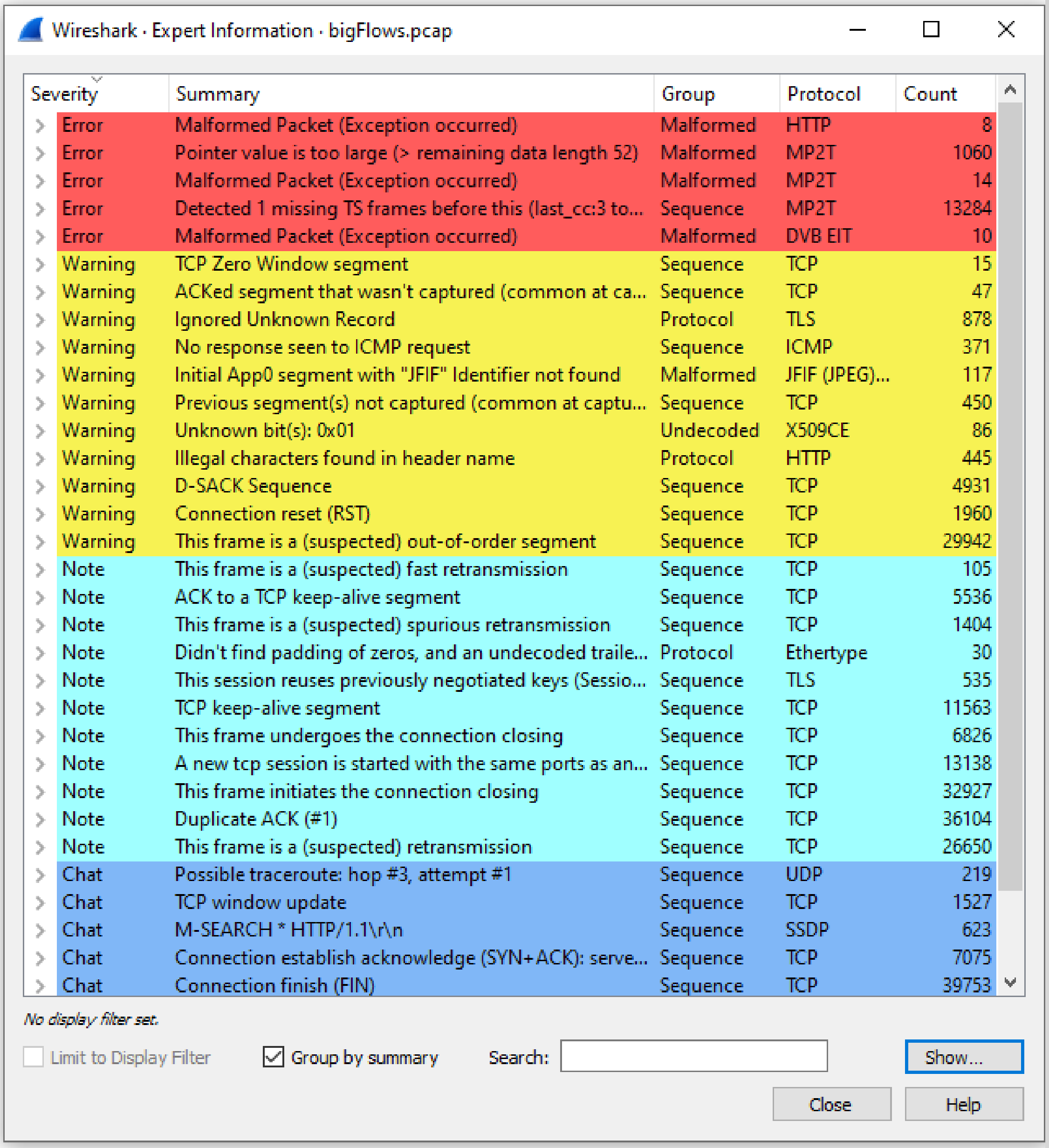
○ Export a new `pcapng` with CloudShark comments and annotations

● Download the original file


cloudshark_tcp_keep alive.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.stream eq 17

```
No.  Time      Source          Destination     Protocol Info
 72 0.000000  192.168.0.100   173.230.134.104 TCP      44518 → https(443) [ACK] Seq=1 Ack
 78 0.110598  173.230.134.104 192.168.0.100   TCP      https(443) → 44518 [ACK] Seq=1 Ack
153 10.003900 192.168.0.100   173.230.134.104 TCP      [TCP Keep-Alive] 44518 → https(443
158 0.116335  173.230.134.104 192.168.0.100   TCP      [TCP Keep-Alive ACK] https(443) →
201 4.170338  173.230.134.104 192.168.0.100   TLSv1.2 Encrypted Alert
202 0.000100  192.168.0.100   173.230.134.104 TCP      44518 → https(443) [FIN, ACK] Seq=
203 0.000087  173.230.134.104 192.168.0.100   TCP      https(443) → 44518 [FIN, ACK] Seq=
```

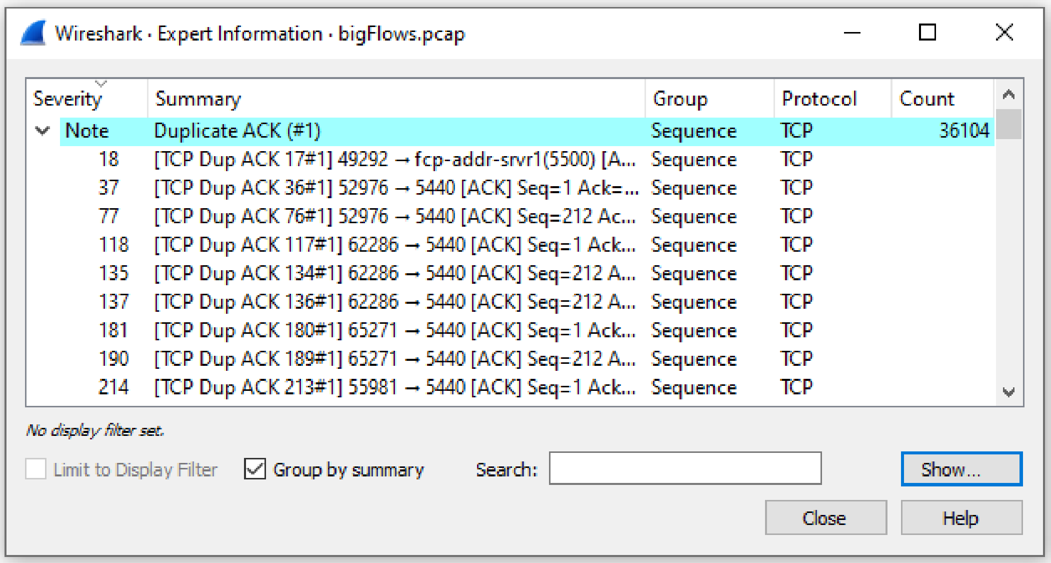


Wireshark · Expert Information · bigFlows.pcap

Severity	Summary	Group	Protocol	Count
Error	Malformed Packet (Exception occurred)	Malformed	HTTP	8
Error	Pointer value is too large (> remaining data length 52)	Malformed	MP2T	1060
Error	Malformed Packet (Exception occurred)	Malformed	MP2T	14
Error	Detected 1 missing TS frames before this (last_cc:3 to...	Sequence	MP2T	13284
Error	Malformed Packet (Exception occurred)	Malformed	DVB EIT	10
Warning	TCP Zero Window segment	Sequence	TCP	15
Warning	ACKed segment that wasn't captured (common at ca...	Sequence	TCP	47
Warning	Ignored Unknown Record	Protocol	TLS	878
Warning	No response seen to ICMP request	Sequence	ICMP	371
Warning	Initial App0 segment with "JFIF" Identifier not found	Malformed	JFIF (JPEG)...	117
Warning	Previous segment(s) not captured (common at captu...	Sequence	TCP	450
Warning	Unknown bit(s): 0x01	Undecoded	X509CE	86
Warning	Illegal characters found in header name	Protocol	HTTP	445
Warning	D-SACK Sequence	Sequence	TCP	4931
Warning	Connection reset (RST)	Sequence	TCP	1960
Warning	This frame is a (suspected) out-of-order segment	Sequence	TCP	29942
Note	This frame is a (suspected) fast retransmission	Sequence	TCP	105
Note	ACK to a TCP keep-alive segment	Sequence	TCP	5536
Note	This frame is a (suspected) spurious retransmission	Sequence	TCP	1404
Note	Didn't find padding of zeros, and an undecoded traile...	Protocol	Ethertype	30
Note	This session reuses previously negotiated keys (Sessio...	Sequence	TLS	535
Note	TCP keep-alive segment	Sequence	TCP	11563
Note	This frame undergoes the connection closing	Sequence	TCP	6826
Note	A new tcp session is started with the same ports as an...	Sequence	TCP	13138
Note	This frame initiates the connection closing	Sequence	TCP	32927
Note	Duplicate ACK (#1)	Sequence	TCP	36104
Note	This frame is a (suspected) retransmission	Sequence	TCP	26650
Chat	Possible traceroute: hop #3, attempt #1	Sequence	UDP	219
Chat	TCP window update	Sequence	TCP	1527
Chat	M-SEARCH * HTTP/1.1\r\n	Sequence	SSDP	623
Chat	Connection establish acknowledge (SYN+ACK): serve...	Sequence	TCP	7075
Chat	Connection finish (FIN)	Sequence	TCP	39753

No display filter set.

☐ Limit to Display Filter ☑ Group by summary Search:

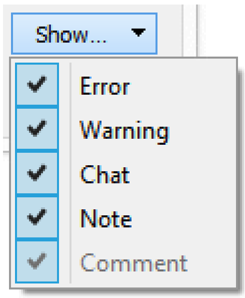


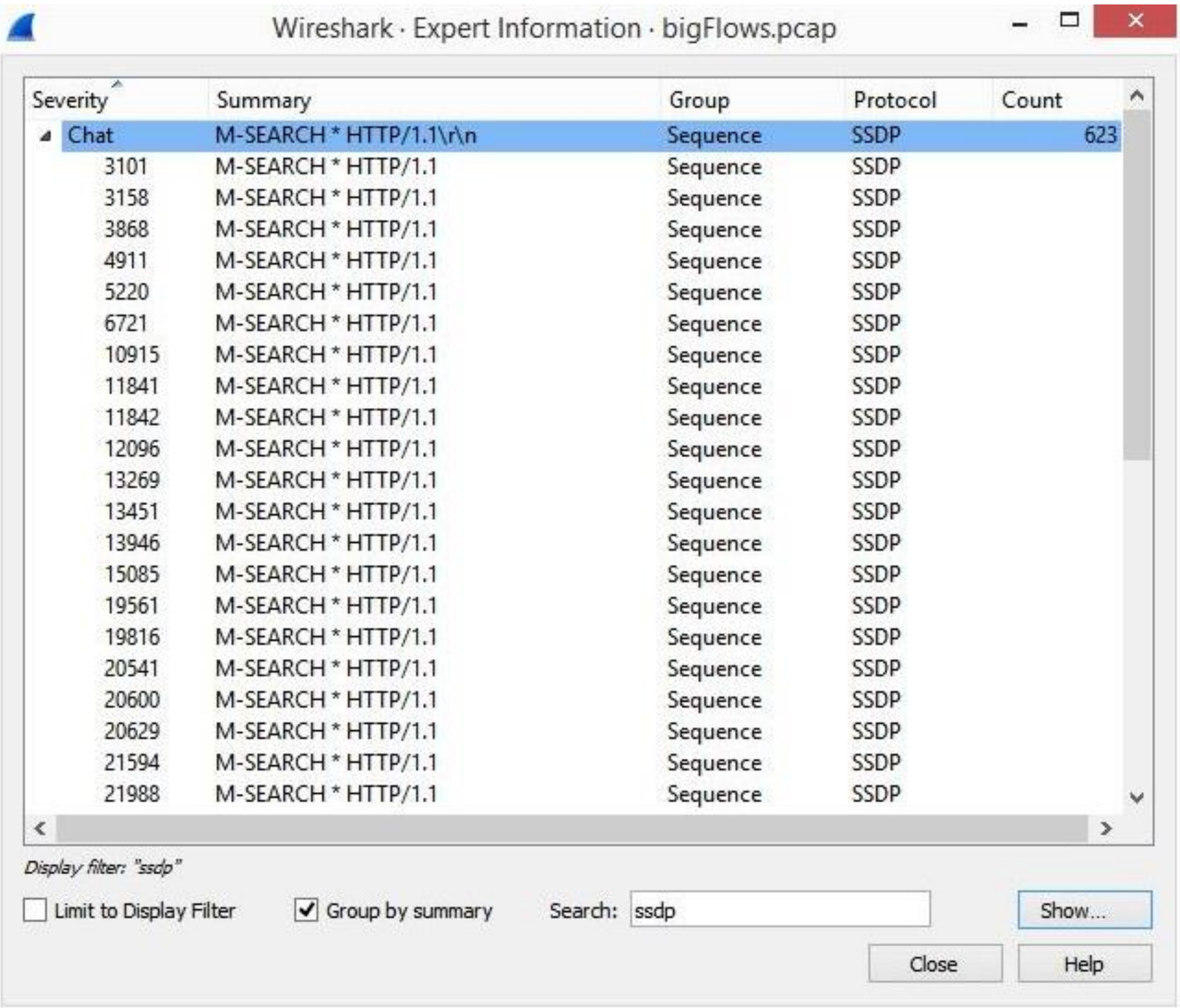
Wireshark · Expert Information · bigFlows.pcap

Severity	Summary	Group	Protocol	Count
Note	Duplicate ACK (#1)	Sequence	TCP	36104
18	[TCP Dup ACK 17#1] 49292 → fcp-addr-srvr1(5500) [A...	Sequence	TCP	
37	[TCP Dup ACK 36#1] 52976 → 5440 [ACK] Seq=1 Ack=...	Sequence	TCP	
77	[TCP Dup ACK 76#1] 52976 → 5440 [ACK] Seq=212 Ac...	Sequence	TCP	
118	[TCP Dup ACK 117#1] 62286 → 5440 [ACK] Seq=1 Ack...	Sequence	TCP	
135	[TCP Dup ACK 134#1] 62286 → 5440 [ACK] Seq=212 A...	Sequence	TCP	
137	[TCP Dup ACK 136#1] 62286 → 5440 [ACK] Seq=212 A...	Sequence	TCP	
181	[TCP Dup ACK 180#1] 65271 → 5440 [ACK] Seq=1 Ack...	Sequence	TCP	
190	[TCP Dup ACK 189#1] 65271 → 5440 [ACK] Seq=212 A...	Sequence	TCP	
214	[TCP Dup ACK 213#1] 55981 → 5440 [ACK] Seq=1 Ack...	Sequence	TCP	

No display filter set.

☐ Limit to Display Filter ☑ Group by summary Search:

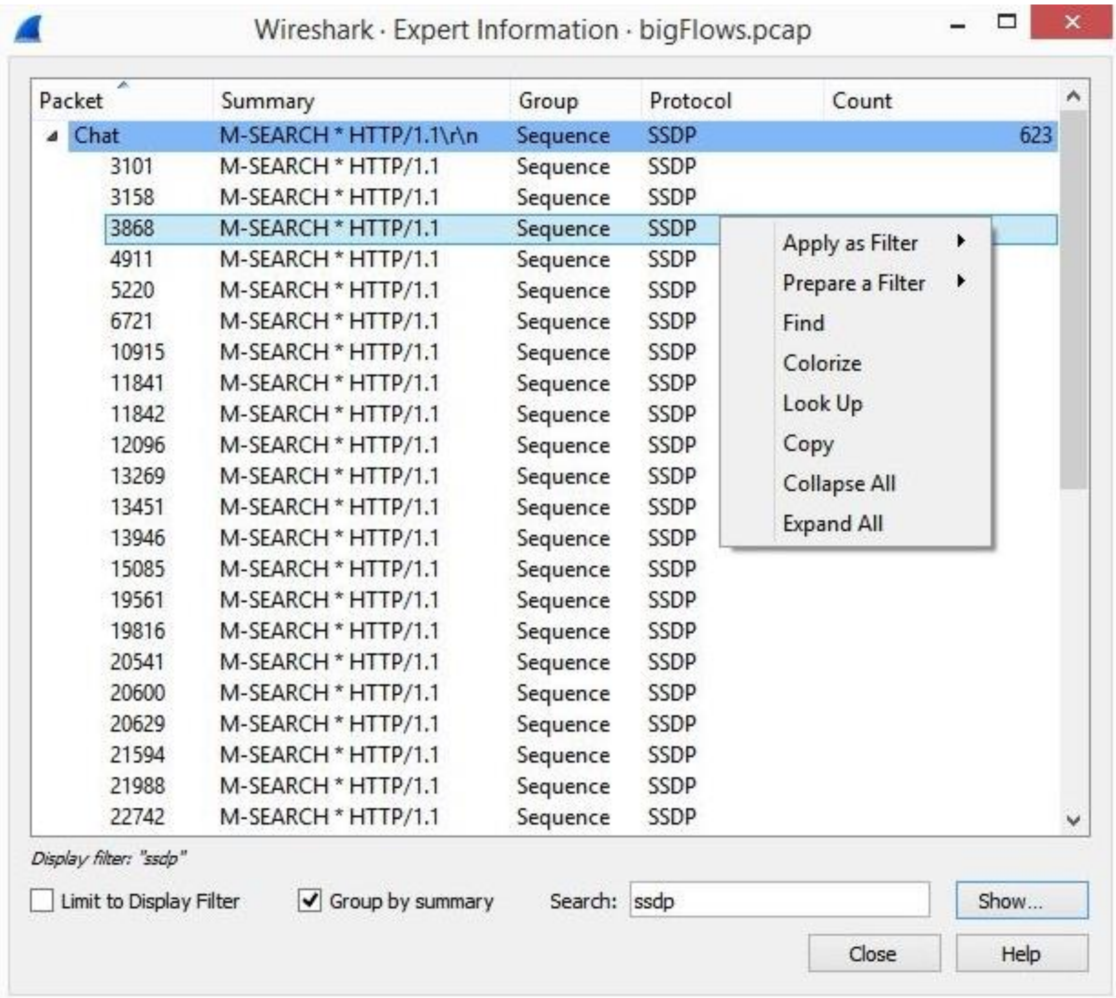




Severity	Summary	Group	Protocol	Count
Chat	M-SEARCH * HTTP/1.1\r\n	Sequence	SSDP	623
3101	M-SEARCH * HTTP/1.1	Sequence	SSDP	
3158	M-SEARCH * HTTP/1.1	Sequence	SSDP	
3868	M-SEARCH * HTTP/1.1	Sequence	SSDP	
4911	M-SEARCH * HTTP/1.1	Sequence	SSDP	
5220	M-SEARCH * HTTP/1.1	Sequence	SSDP	
6721	M-SEARCH * HTTP/1.1	Sequence	SSDP	
10915	M-SEARCH * HTTP/1.1	Sequence	SSDP	
11841	M-SEARCH * HTTP/1.1	Sequence	SSDP	
11842	M-SEARCH * HTTP/1.1	Sequence	SSDP	
12096	M-SEARCH * HTTP/1.1	Sequence	SSDP	
13269	M-SEARCH * HTTP/1.1	Sequence	SSDP	
13451	M-SEARCH * HTTP/1.1	Sequence	SSDP	
13946	M-SEARCH * HTTP/1.1	Sequence	SSDP	
15085	M-SEARCH * HTTP/1.1	Sequence	SSDP	
19561	M-SEARCH * HTTP/1.1	Sequence	SSDP	
19816	M-SEARCH * HTTP/1.1	Sequence	SSDP	
20541	M-SEARCH * HTTP/1.1	Sequence	SSDP	
20600	M-SEARCH * HTTP/1.1	Sequence	SSDP	
20629	M-SEARCH * HTTP/1.1	Sequence	SSDP	
21594	M-SEARCH * HTTP/1.1	Sequence	SSDP	
21988	M-SEARCH * HTTP/1.1	Sequence	SSDP	

Display filter: "ssdp"

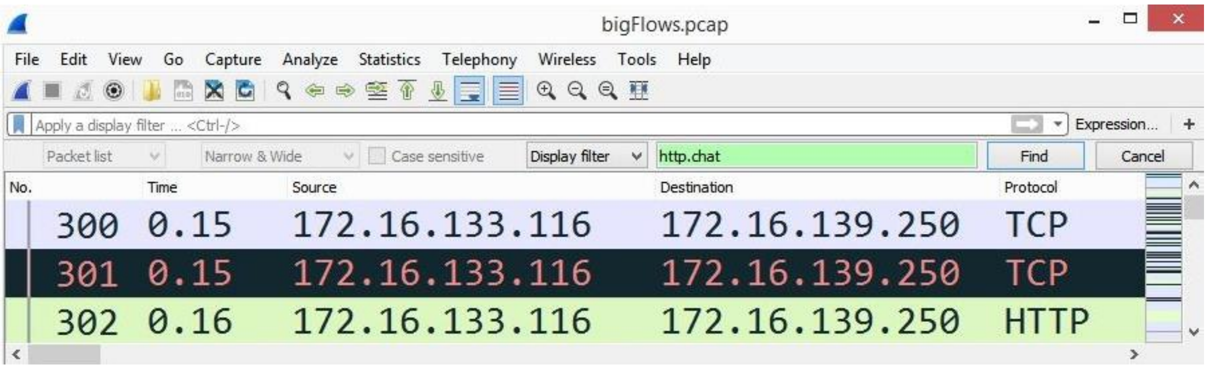
□ Limit to Display Filter ☑ Group by summary Search: ssdp



Packet	Summary	Group	Protocol	Count
Chat	M-SEARCH * HTTP/1.1\r\n	Sequence	SSDP	623
3101	M-SEARCH * HTTP/1.1	Sequence	SSDP	
3158	M-SEARCH * HTTP/1.1	Sequence	SSDP	
3868	M-SEARCH * HTTP/1.1	Sequence	SSDP	
4911	M-SEARCH * HTTP/1.1	Sequence	SSDP	
5220	M-SEARCH * HTTP/1.1	Sequence	SSDP	
6721	M-SEARCH * HTTP/1.1	Sequence	SSDP	
10915	M-SEARCH * HTTP/1.1	Sequence	SSDP	
11841	M-SEARCH * HTTP/1.1	Sequence	SSDP	
11842	M-SEARCH * HTTP/1.1	Sequence	SSDP	
12096	M-SEARCH * HTTP/1.1	Sequence	SSDP	
13269	M-SEARCH * HTTP/1.1	Sequence	SSDP	
13451	M-SEARCH * HTTP/1.1	Sequence	SSDP	
13946	M-SEARCH * HTTP/1.1	Sequence	SSDP	
15085	M-SEARCH * HTTP/1.1	Sequence	SSDP	
19561	M-SEARCH * HTTP/1.1	Sequence	SSDP	
19816	M-SEARCH * HTTP/1.1	Sequence	SSDP	
20541	M-SEARCH * HTTP/1.1	Sequence	SSDP	
20600	M-SEARCH * HTTP/1.1	Sequence	SSDP	
20629	M-SEARCH * HTTP/1.1	Sequence	SSDP	
21594	M-SEARCH * HTTP/1.1	Sequence	SSDP	
21988	M-SEARCH * HTTP/1.1	Sequence	SSDP	
22742	M-SEARCH * HTTP/1.1	Sequence	SSDP	

Display filter: "ssdp"

☐ Limit to Display Filter ☑ Group by summary Search: ssdp

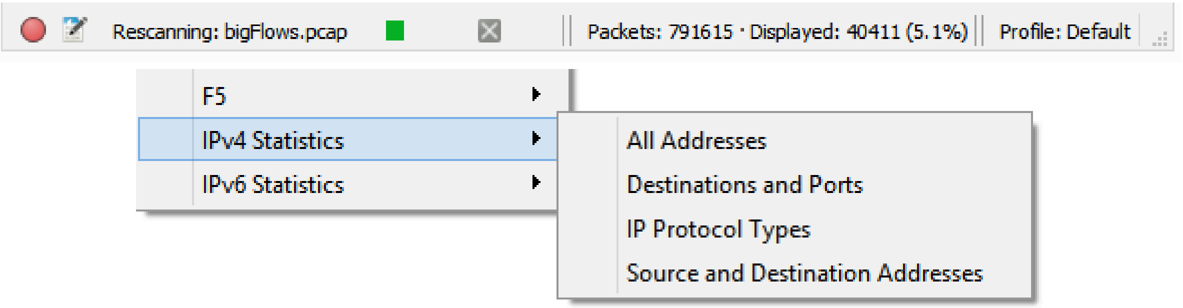


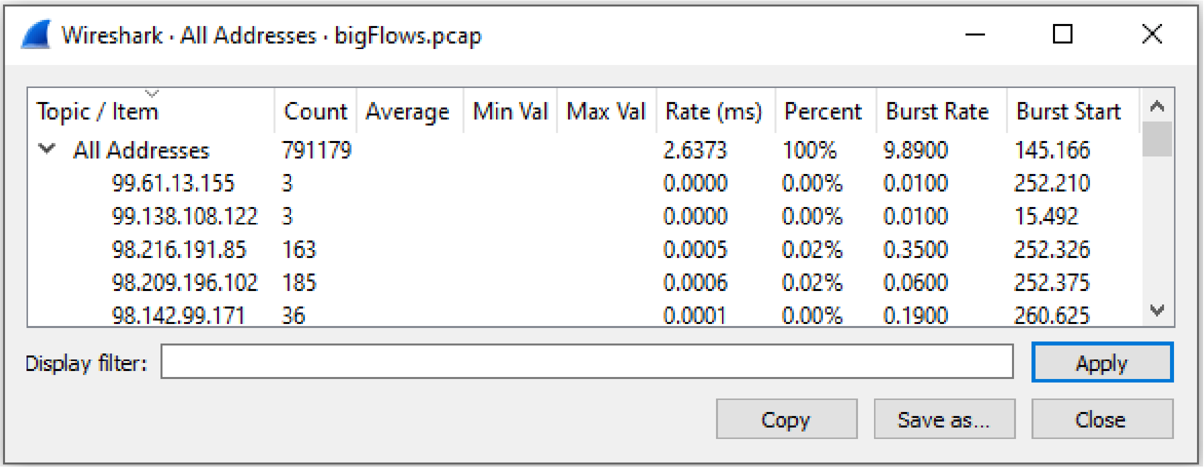
bigFlows.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
Find
Cancel

Packet list | Narrow & Wide | ☐ Case sensitive | Display filter | http.chat

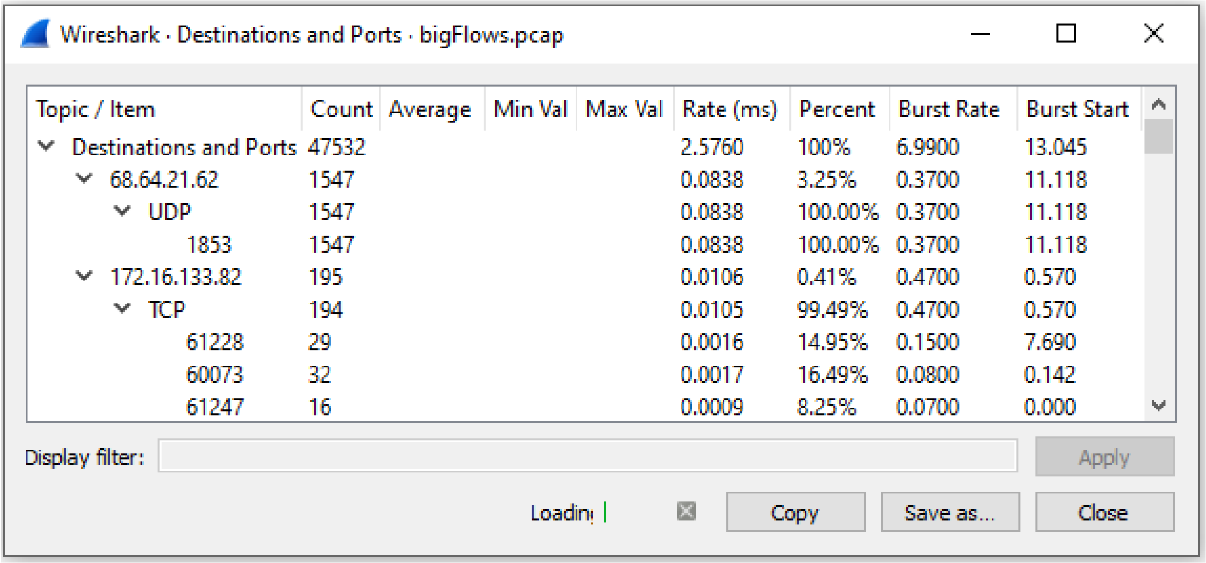
No.	Time	Source	Destination	Protocol
300	0.15	172.16.133.116	172.16.139.250	TCP
301	0.15	172.16.133.116	172.16.139.250	TCP
302	0.16	172.16.133.116	172.16.139.250	HTTP

Chapter 18: Subsetting, Saving, and Exporting Captures

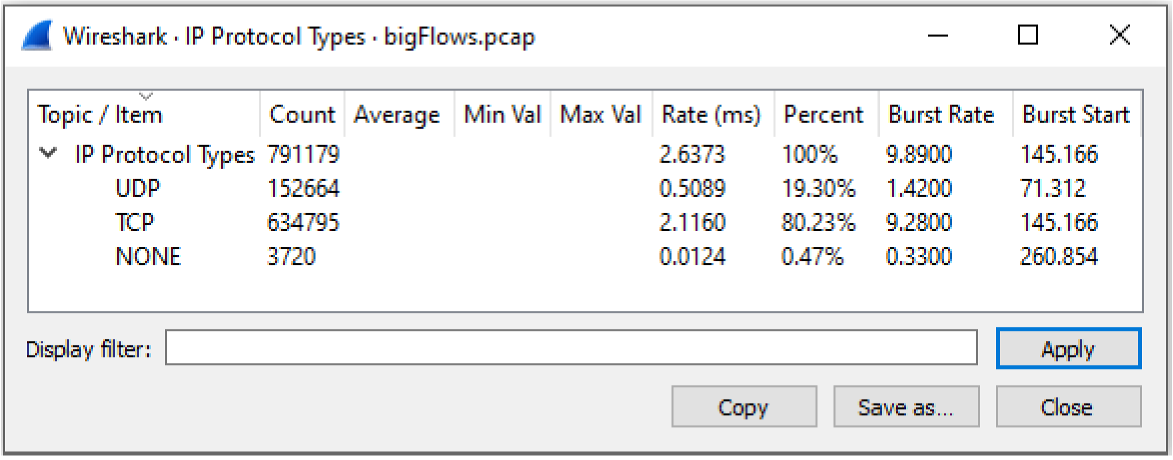




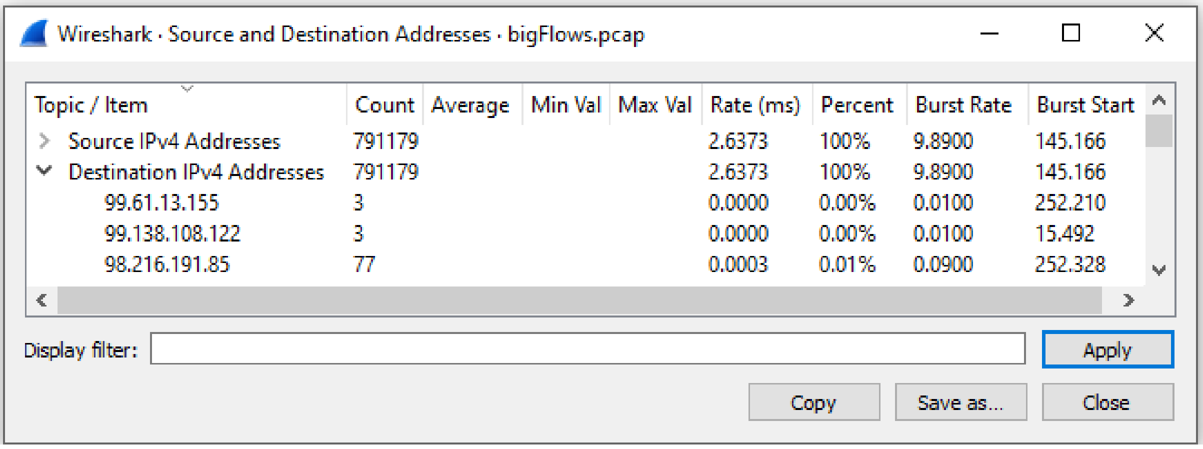
Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
All Addresses	791179				2.6373	100%	9.8900	145.166
99.61.13.155	3				0.0000	0.00%	0.0100	252.210
99.138.108.122	3				0.0000	0.00%	0.0100	15.492
98.216.191.85	163				0.0005	0.02%	0.3500	252.326
98.209.196.102	185				0.0006	0.02%	0.0600	252.375
98.142.99.171	36				0.0001	0.00%	0.1900	260.625



Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
Destinations and Ports	47532				2.5760	100%	6.9900	13.045
68.64.21.62	1547				0.0838	3.25%	0.3700	11.118
UDP	1547				0.0838	100.00%	0.3700	11.118
1853	1547				0.0838	100.00%	0.3700	11.118
172.16.133.82	195				0.0106	0.41%	0.4700	0.570
TCP	194				0.0105	99.49%	0.4700	0.570
61228	29				0.0016	14.95%	0.1500	7.690
60073	32				0.0017	16.49%	0.0800	0.142
61247	16				0.0009	8.25%	0.0700	0.000

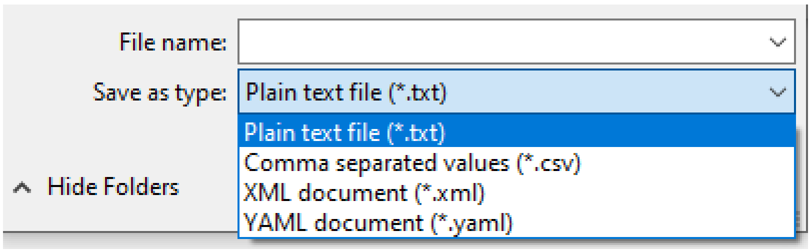


Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
IP Protocol Types	791179				2.6373	100%	9.8900	145.166
UDP	152664				0.5089	19.30%	1.4200	71.312
TCP	634795				2.1160	80.23%	9.2800	145.166
NONE	3720				0.0124	0.47%	0.3300	260.854

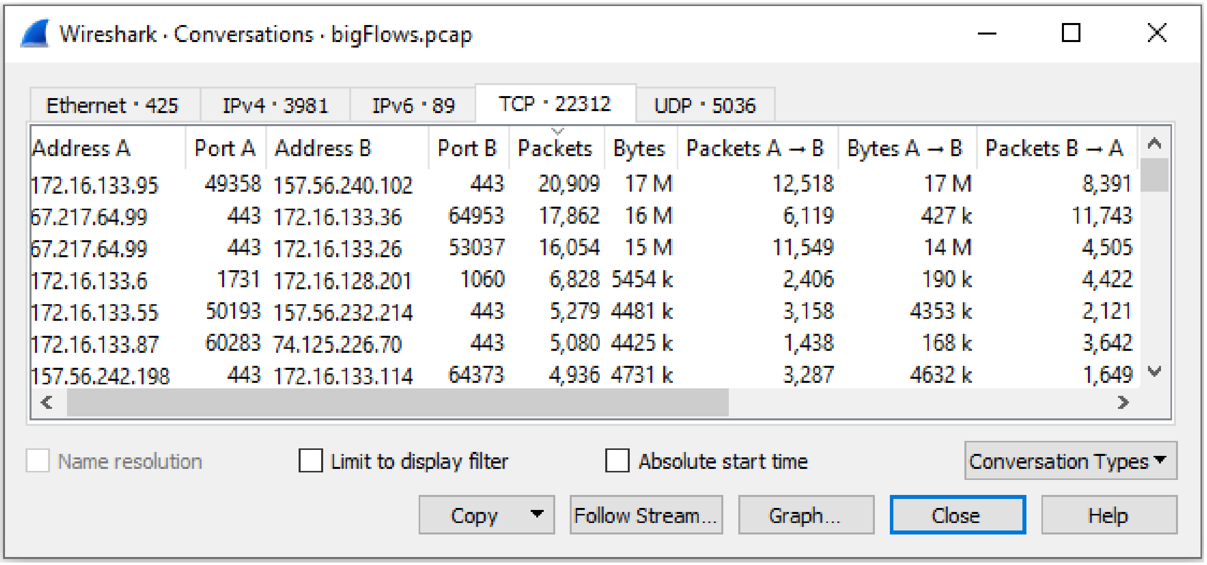

Wireshark · Source and Destination Addresses · bigFlows.pcap

Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
Source IPv4 Addresses	791179				2.6373	100%	9.8900	145.166
Destination IPv4 Addresses	791179				2.6373	100%	9.8900	145.166
99.61.13.155	3				0.0000	0.00%	0.0100	252.210
99.138.108.122	3				0.0000	0.00%	0.0100	15.492
98.216.191.85	77				0.0003	0.01%	0.0900	252.328

Display filter:
Apply
Copy
Save as...
Close

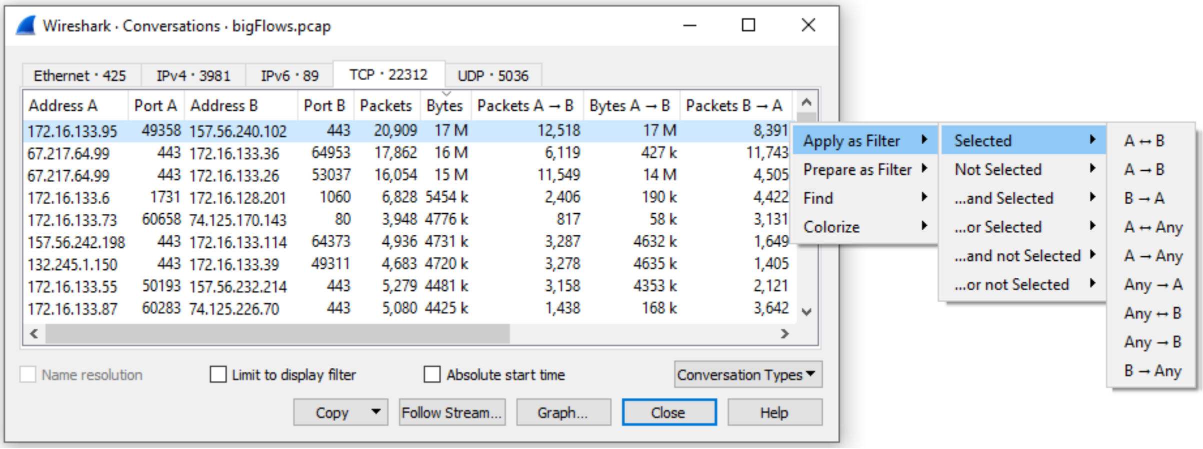

File name:

Save as type: Plain text file (*.txt)



Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A
172.16.133.95	49358	157.56.240.102	443	20,909	17 M	12,518	17 M	8,391
67.217.64.99	443	172.16.133.36	64953	17,862	16 M	6,119	427 k	11,743
67.217.64.99	443	172.16.133.26	53037	16,054	15 M	11,549	14 M	4,505
172.16.133.6	1731	172.16.128.201	1060	6,828	5454 k	2,406	190 k	4,422
172.16.133.55	50193	157.56.232.214	443	5,279	4481 k	3,158	4353 k	2,121
172.16.133.87	60283	74.125.226.70	443	5,080	4425 k	1,438	168 k	3,642
157.56.242.198	443	172.16.133.114	64373	4,936	4731 k	3,287	4632 k	1,649

☐ Name resolution ☐ Limit to display filter ☐ Absolute start time

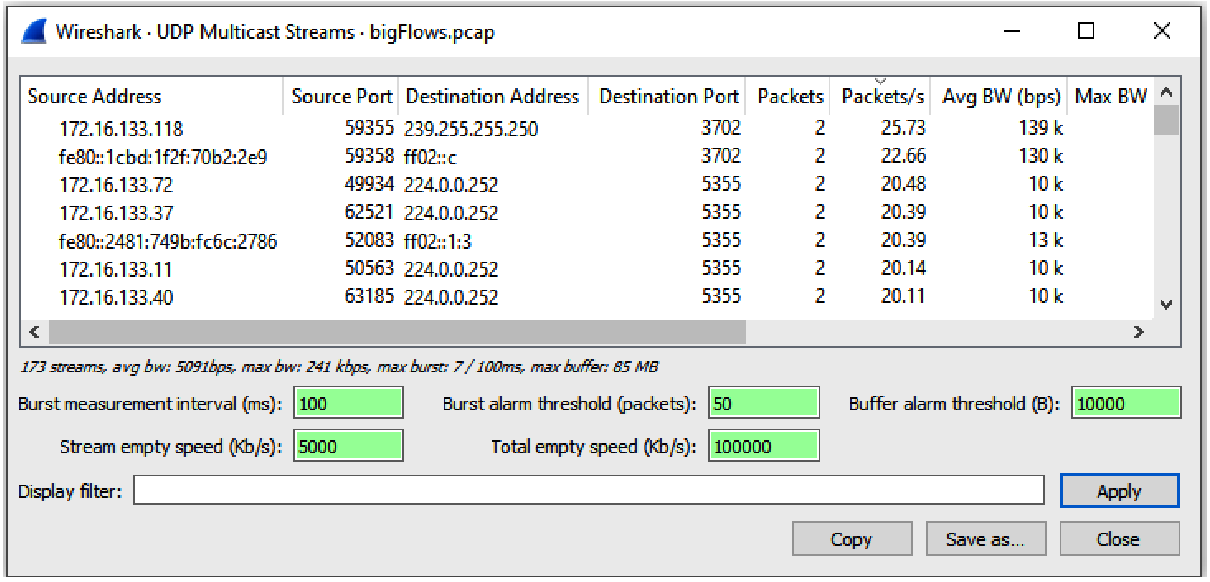


Wireshark · Conversations · bigFlows.pcap

Ethernet · 425 | IPv4 · 3981 | IPv6 · 89 | TCP · 22312 | UDP · 5036

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A
172.16.133.95	49358	157.56.240.102	443	20,909	17 M	12,518	17 M	8,391
67.217.64.99	443	172.16.133.36	64953	17,862	16 M	6,119	427 k	11,743
67.217.64.99	443	172.16.133.26	53037	16,054	15 M	11,549	14 M	4,505
172.16.133.6	1731	172.16.128.201	1060	6,828	5454 k	2,406	190 k	4,422
172.16.133.73	60658	74.125.170.143	80	3,948	4776 k	817	58 k	3,131
157.56.242.198	443	172.16.133.114	64373	4,936	4731 k	3,287	4632 k	1,649
132.245.1.150	443	172.16.133.39	49311	4,683	4720 k	3,278	4635 k	1,405
172.16.133.55	50193	157.56.232.214	443	5,279	4481 k	3,158	4353 k	2,121
172.16.133.87	60283	74.125.226.70	443	5,080	4425 k	1,438	168 k	3,642

□ Name resolution □ Limit to display filter □ Absolute start time

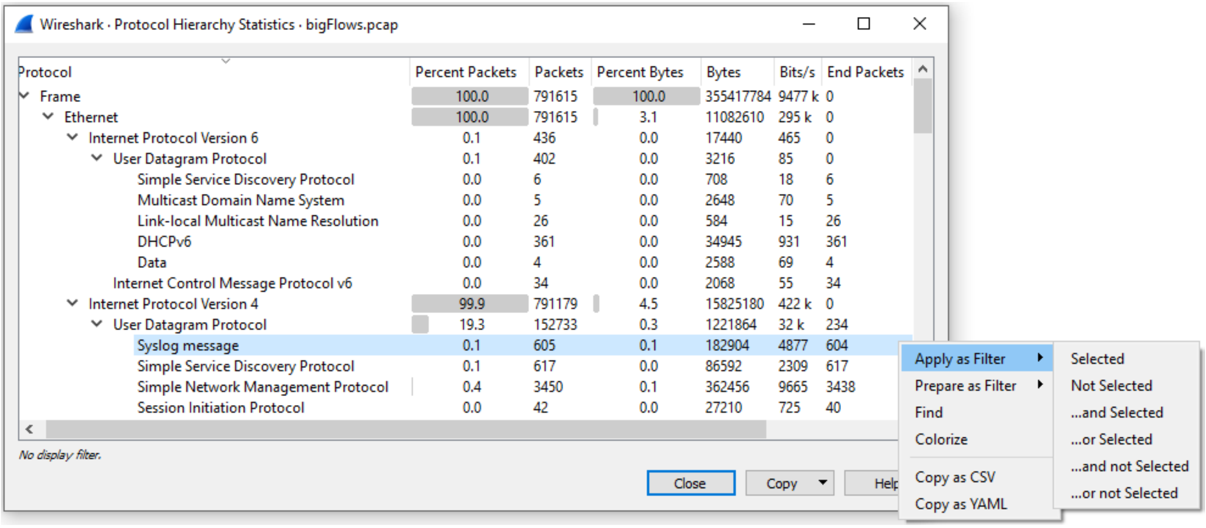


Wireshark · UDP Multicast Streams · bigFlows.pcap

Source Address	Source Port	Destination Address	Destination Port	Packets	Packets/s	Avg BW (bps)	Max BW
172.16.133.118	59355	239.255.255.250	3702	2	25.73	139 k	
fe80::1cbd:1f2f:70b2:2e9	59358	ff02::c	3702	2	22.66	130 k	
172.16.133.72	49934	224.0.0.252	5355	2	20.48	10 k	
172.16.133.37	62521	224.0.0.252	5355	2	20.39	10 k	
fe80::2481:749b:fc6c:2786	52083	ff02::1:3	5355	2	20.39	13 k	
172.16.133.11	50563	224.0.0.252	5355	2	20.14	10 k	
172.16.133.40	63185	224.0.0.252	5355	2	20.11	10 k	

173 streams, avg bw: 5091bps, max bw: 241 kbps, max burst: 7 / 100ms, max buffer: 85 MB

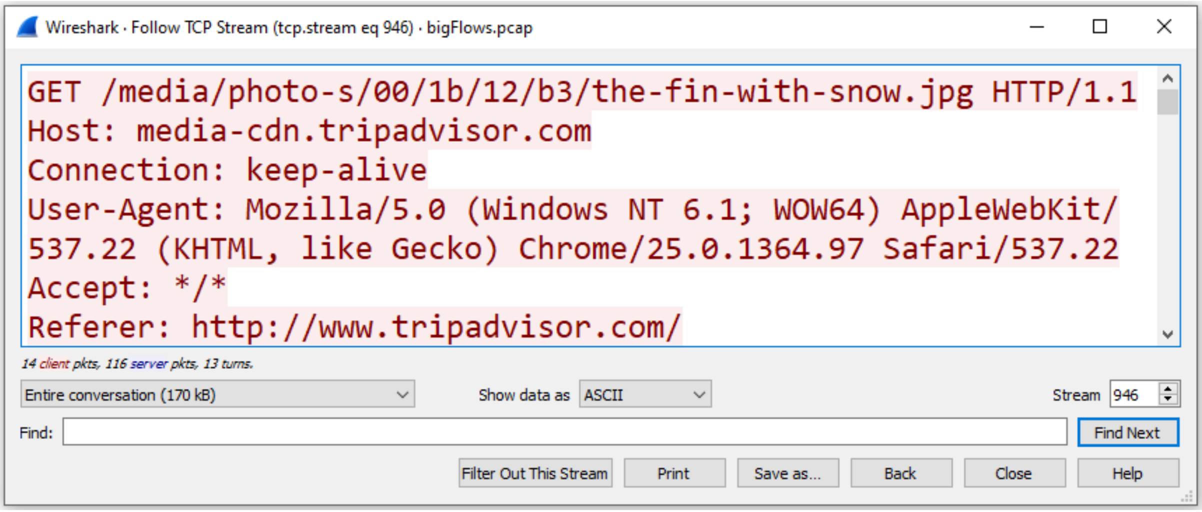
Burst measurement interval (ms): 100
Burst alarm threshold (packets): 50
Buffer alarm threshold (B): 10000
Stream empty speed (Kb/s): 5000
Total empty speed (Kb/s): 100000
Display filter:



Wireshark · Protocol Hierarchy Statistics · bigFlows.pcap

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets
Frame	100.0	791615	100.0	355417784	9477 k	0
Ethernet	100.0	791615	3.1	11082610	295 k	0
Internet Protocol Version 6	0.1	436	0.0	17440	465	0
User Datagram Protocol	0.1	402	0.0	3216	85	0
Simple Service Discovery Protocol	0.0	6	0.0	708	18	6
Multicast Domain Name System	0.0	5	0.0	2648	70	5
Link-local Multicast Name Resolution	0.0	26	0.0	584	15	26
DHCPv6	0.0	361	0.0	34945	931	361
Data	0.0	4	0.0	2588	69	4
Internet Control Message Protocol v6	0.0	34	0.0	2068	55	34
Internet Protocol Version 4	99.9	791179	4.5	15825180	422 k	0
User Datagram Protocol	19.3	152733	0.3	1221864	32 k	234
Syslog message	0.1	605	0.1	182904	4877	604
Simple Service Discovery Protocol	0.1	617	0.0	86592	2309	617
Simple Network Management Protocol	0.4	3450	0.1	362456	9665	3438
Session Initiation Protocol	0.0	42	0.0	27210	725	40

No display filter.



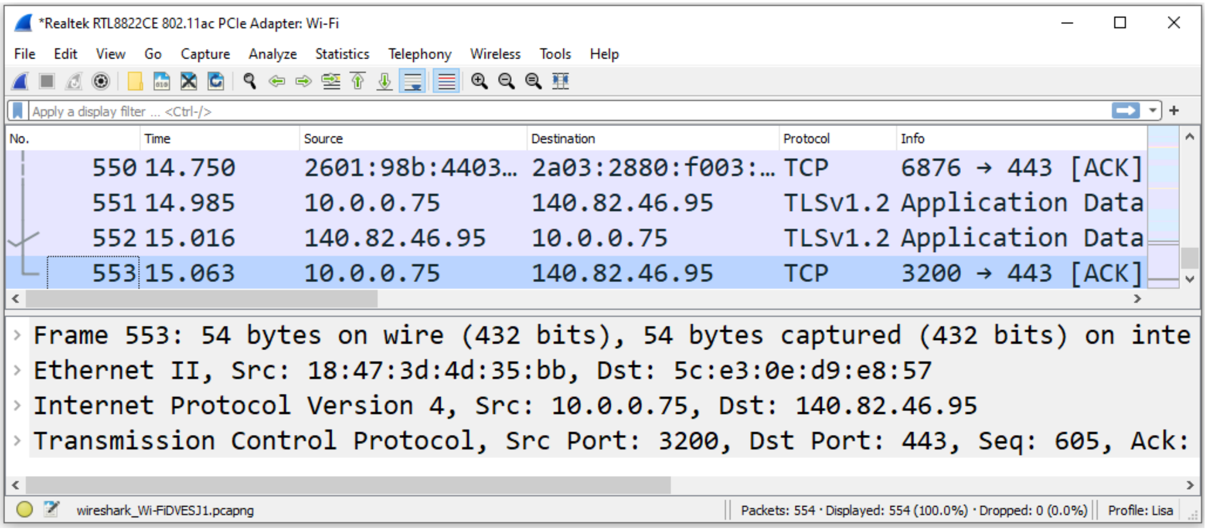
Wireshark · Follow TCP Stream (tcp.stream eq 946) · bigFlows.pcap

```
GET /media/photo-s/00/1b/12/b3/the-fin-with-snow.jpg HTTP/1.1
Host: media-cdn.tripadvisor.com
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/
537.22 (KHTML, like Gecko) Chrome/25.0.1364.97 Safari/537.22
Accept: */*
Referer: http://www.tripadvisor.com/
```

14 client pkts, 116 server pkts, 13 turns.

Entire conversation (170 kB)   Show data as ASCII   Stream 946

Find:

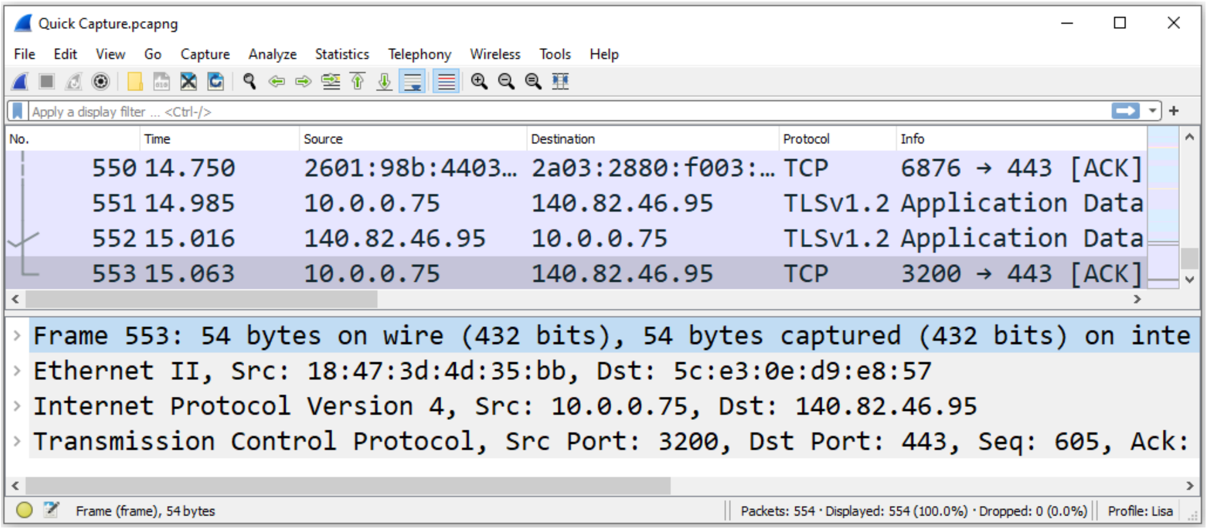


*Realtek RTL8822CE 802.11ac PCIe Adapter: Wi-Fi

```
No.   Time    Source              Destination         Protocol Info
  550 14.750  2601:98b:4403…      2a03:2880:f003:…    TCP      6876 → 443 [ACK]
  551 14.985  10.0.0.75           140.82.46.95        TLSv1.2  Application Data
  552 15.016  140.82.46.95        10.0.0.75           TLSv1.2  Application Data
  553 15.063  10.0.0.75           140.82.46.95        TCP      3200 → 443 [ACK]
```

```
> Frame 553: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on inte
> Ethernet II, Src: 18:47:3d:4d:35:bb, Dst: 5c:e3:0e:d9:e8:57
> Internet Protocol Version 4, Src: 10.0.0.75, Dst: 140.82.46.95
> Transmission Control Protocol, Src Port: 3200, Dst Port: 443, Seq: 605, Ack:
```

wireshark_Wi-FiDVESJ1.pcapng | Packets: 554 · Displayed: 554 (100.0%) · Dropped: 0 (0.0%) | Profile: Lisa

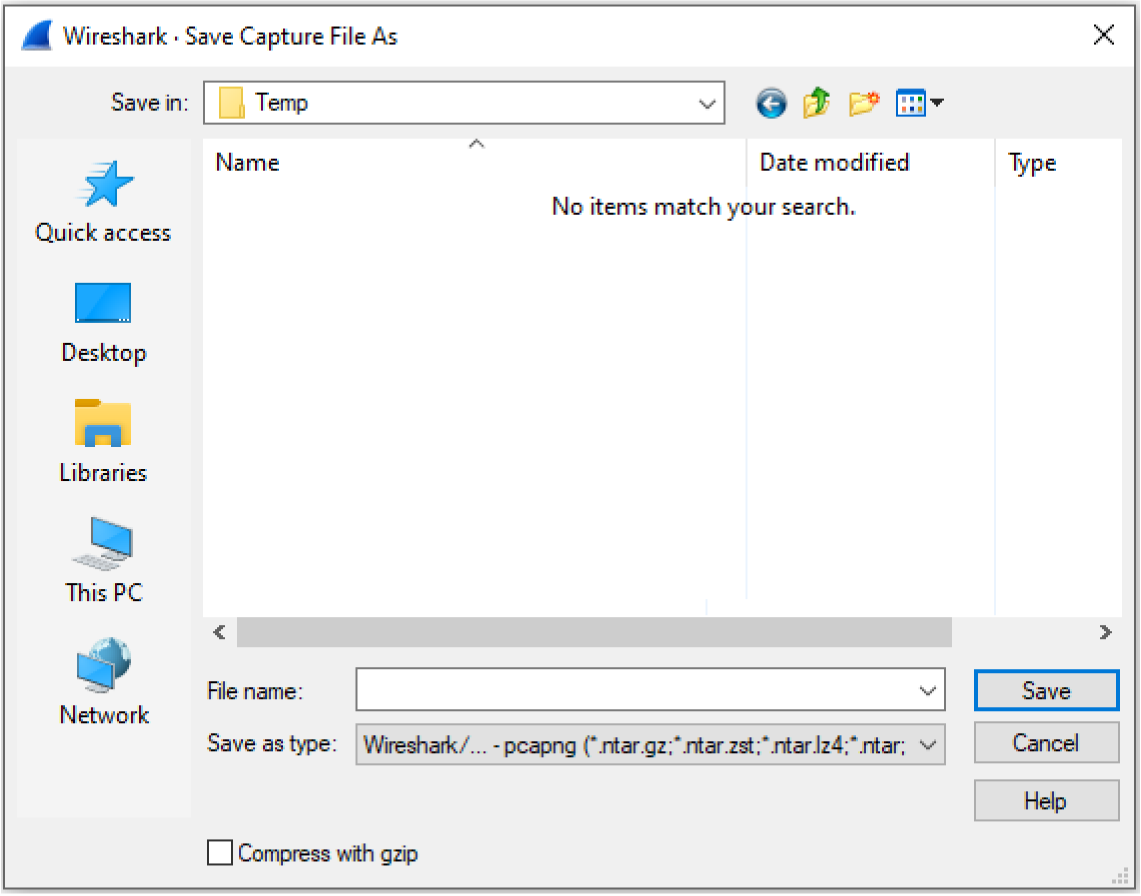


Quick Capture.pcapng

```
No.   Time    Source              Destination         Protocol Info
  550 14.750  2601:98b:4403…      2a03:2880:f003:…    TCP      6876 → 443 [ACK]
  551 14.985  10.0.0.75           140.82.46.95        TLSv1.2  Application Data
  552 15.016  140.82.46.95        10.0.0.75           TLSv1.2  Application Data
  553 15.063  10.0.0.75           140.82.46.95        TCP      3200 → 443 [ACK]
```

```
> Frame 553: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on inte
> Ethernet II, Src: 18:47:3d:4d:35:bb, Dst: 5c:e3:0e:d9:e8:57
> Internet Protocol Version 4, Src: 10.0.0.75, Dst: 140.82.46.95
> Transmission Control Protocol, Src Port: 3200, Dst Port: 443, Seq: 605, Ack:
```

Frame (frame), 54 bytes | Packets: 554 · Displayed: 554 (100.0%) · Dropped: 0 (0.0%) | Profile: Lisa



Wireshark · Save Capture File As

Save in: Temp

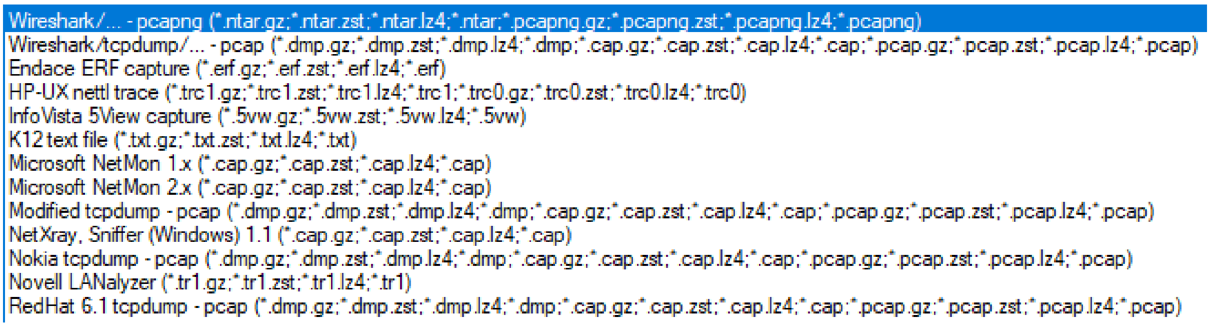
Name	Date modified	Type

No items match your search.

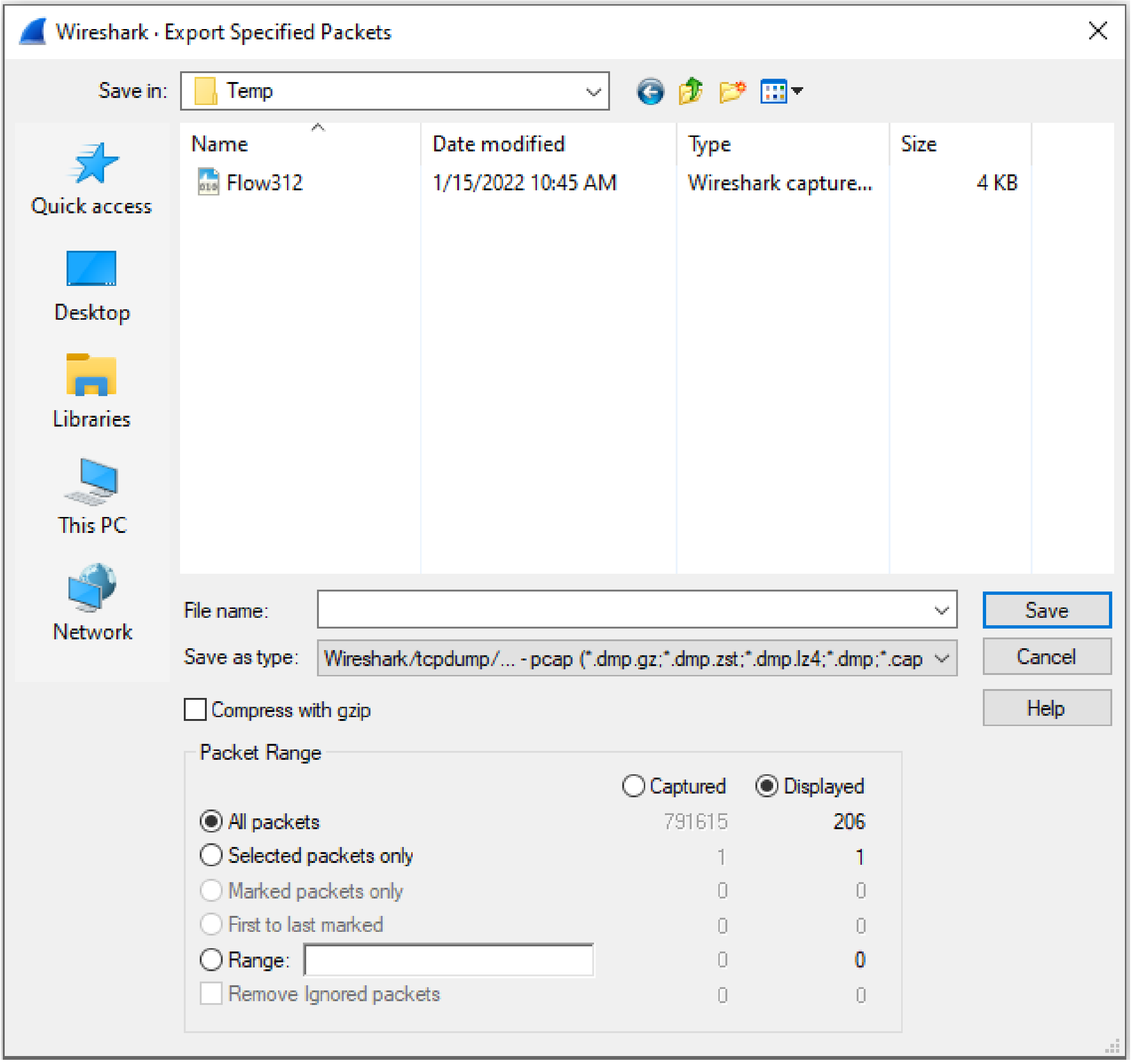
File name:

Save as type: Wireshark/... - pcapng (*.ntar.gz;*.ntar.zst;*.ntar.lz4;*.ntar;

□ Compress with gzip



Wireshark/... - pcapng (*.ntar.gz;*.ntar.zst;*.ntar.lz4;*.ntar;*.pcapng.gz;*.pcapng.zst;*.pcapng.lz4;*.pcapng)
Wireshark/tcpdump/... - pcap (*.dmp.gz;*.dmp.zst;*.dmp.lz4;*.dmp;*.cap.gz;*.cap.zst;*.cap.lz4;*.cap;*.pcap.gz;*.pcap.zst;*.pcap.lz4;*.pcap)
Endace ERF capture (*.erf.gz;*.erf.zst;*.erf.lz4;*.erf)
HP-UX nettl trace (*.trc1.gz;*.trc1.zst;*.trc1.lz4;*.trc1;*.trc0.gz;*.trc0.zst;*.trc0.lz4;*.trc0)
InfoVista 5View capture (*.5vw.gz;*.5vw.zst;*.5vw.lz4;*.5vw)
K12 text file (*.txt.gz;*.txt.zst;*.txt.lz4;*.txt)
Microsoft NetMon 1.x (*.cap.gz;*.cap.zst;*.cap.lz4;*.cap)
Microsoft NetMon 2.x (*.cap.gz;*.cap.zst;*.cap.lz4;*.cap)
Modified tcpdump - pcap (*.dmp.gz;*.dmp.zst;*.dmp.lz4;*.dmp;*.cap.gz;*.cap.zst;*.cap.lz4;*.cap;*.pcap.gz;*.pcap.zst;*.pcap.lz4;*.pcap)
NetXray, Sniffer (Windows) 1.1 (*.cap.gz;*.cap.zst;*.cap.lz4;*.cap)
Nokia tcpdump - pcap (*.dmp.gz;*.dmp.zst;*.dmp.lz4;*.dmp;*.cap.gz;*.cap.zst;*.cap.lz4;*.cap;*.pcap.gz;*.pcap.zst;*.pcap.lz4;*.pcap)
Novell LANalyzer (*.tr1.gz;*.tr1.zst;*.tr1.lz4;*.tr1)
RedHat 6.1 tcpdump - pcap (*.dmp.gz;*.dmp.zst;*.dmp.lz4;*.dmp;*.cap.gz;*.cap.zst;*.cap.lz4;*.cap;*.pcap.gz;*.pcap.zst;*.pcap.lz4;*.pcap)



Wireshark · Export Specified Packets

Save in: Temp

Name	Date modified	Type	Size
Flow312	1/15/2022 10:45 AM	Wireshark capture...	4 KB

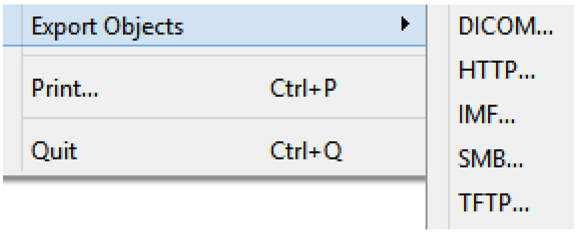
File name:

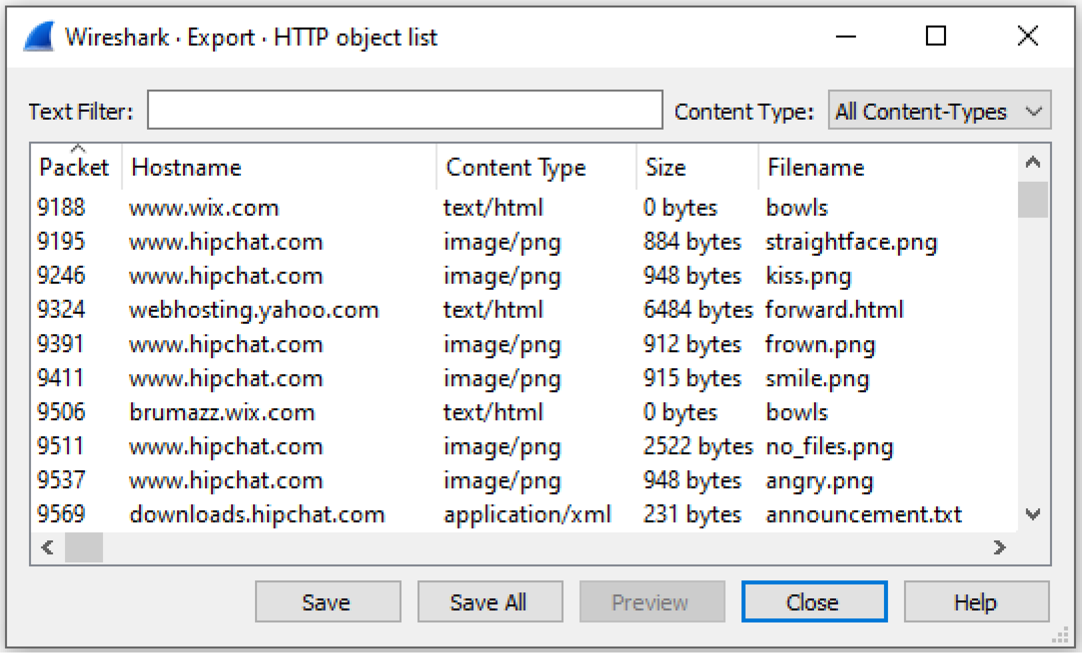
Save as type: Wireshark/tcpdump/... - pcap (*.dmp.gz;*.dmp.zst;*.dmp.lz4;*.dmp;*.cap

□ Compress with gzip

Packet Range

	○ Captured	● Displayed
● All packets	791615	206
○ Selected packets only	1	1
○ Marked packets only	0	0
○ First to last marked	0	0
○ Range:	0	0
□ Remove Ignored packets	0	0



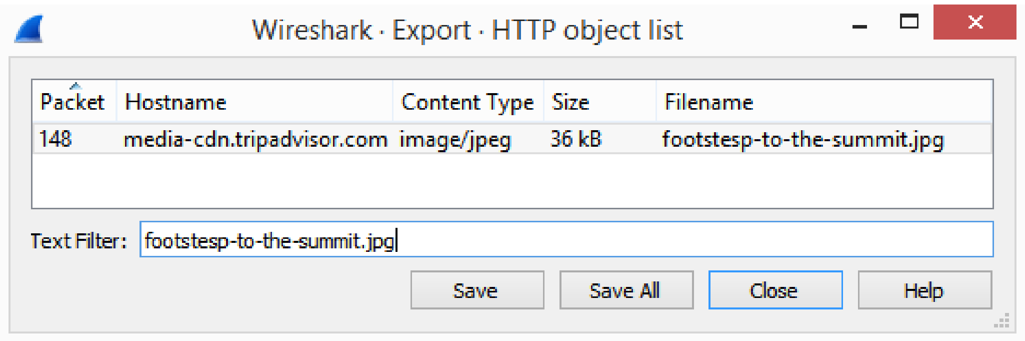


Wireshark · Export · HTTP object list

Text Filter:

Content Type: All Content-Types

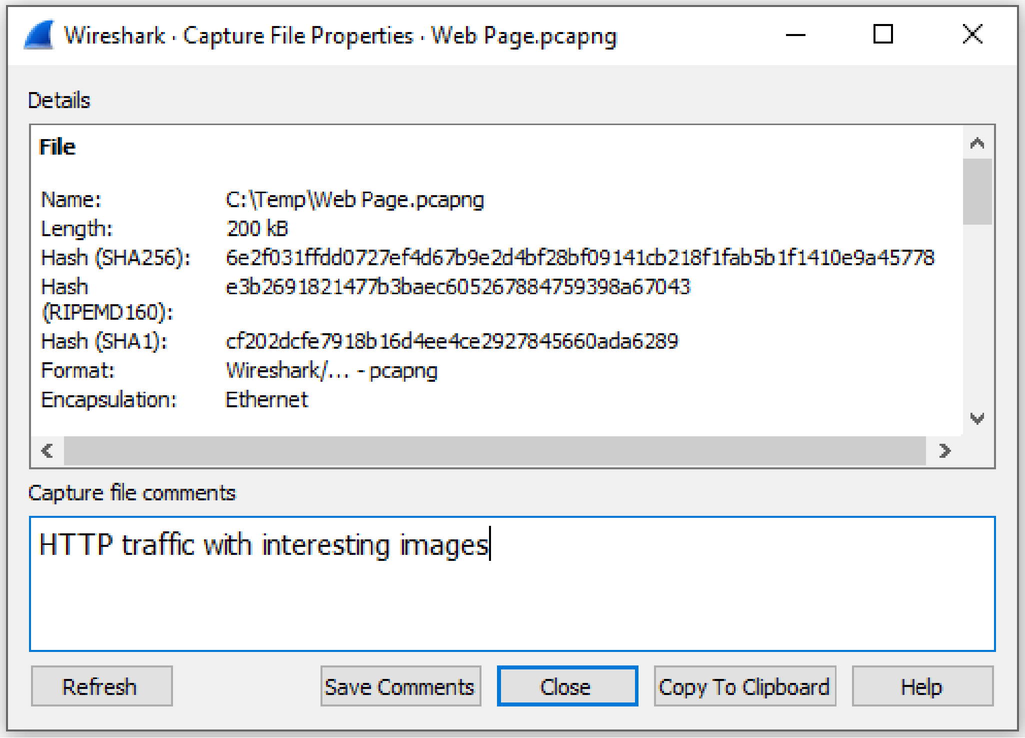
Packet	Hostname	Content Type	Size	Filename
9188	www.wix.com	text/html	0 bytes	bowls
9195	www.hipchat.com	image/png	884 bytes	straightface.png
9246	www.hipchat.com	image/png	948 bytes	kiss.png
9324	webhosting.yahoo.com	text/html	6484 bytes	forward.html
9391	www.hipchat.com	image/png	912 bytes	frown.png
9411	www.hipchat.com	image/png	915 bytes	smile.png
9506	brumazz.wix.com	text/html	0 bytes	bowls
9511	www.hipchat.com	image/png	2522 bytes	no_files.png
9537	www.hipchat.com	image/png	948 bytes	angry.png
9569	downloads.hipchat.com	application/xml	231 bytes	announcement.txt



Wireshark · Export · HTTP object list

Packet	Hostname	Content Type	Size	Filename
148	media-cdn.tripadvisor.com	image/jpeg	36 kB	footstesp-to-the-summit.jpg

Text Filter: footstesp-to-the-summit.jpg



Wireshark · Capture File Properties · Web Page.pcapng

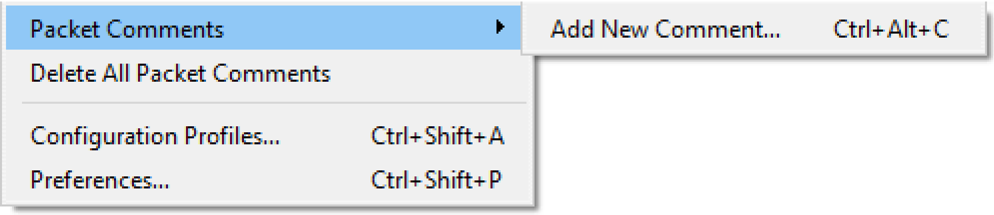
Details

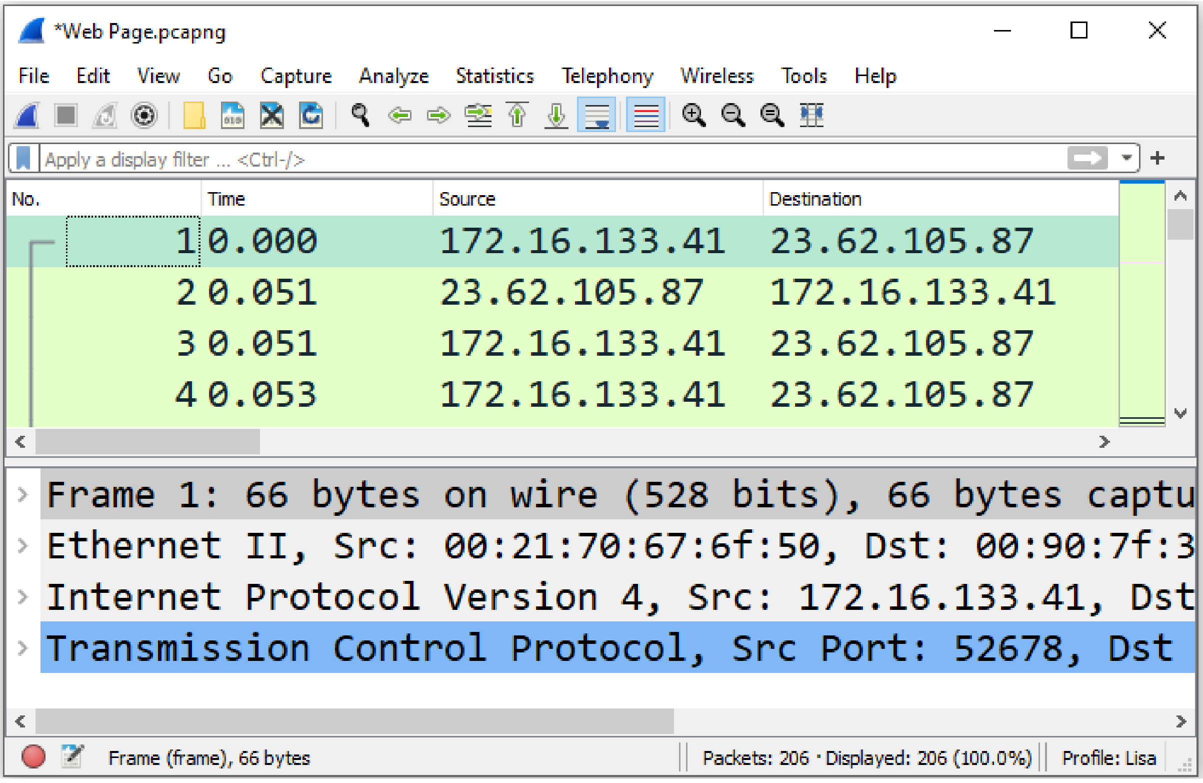
File

Name:	C:\Temp\Web Page.pcapng
Length:	200 kB
Hash (SHA256):	6e2f031ffdd0727ef4d67b9e2d4bf28bf09141cb218f1fab5b1f1410e9a45778
Hash (RIPEMD160):	e3b2691821477b3baec60526788475939 8a67043
Hash (SHA1):	cf202dcfe7918b16d4ee4ce2927845660ada6289
Format:	Wireshark/... - pcapng
Encapsulation:	Ethernet

Capture file comments

HTTP traffic with interesting images

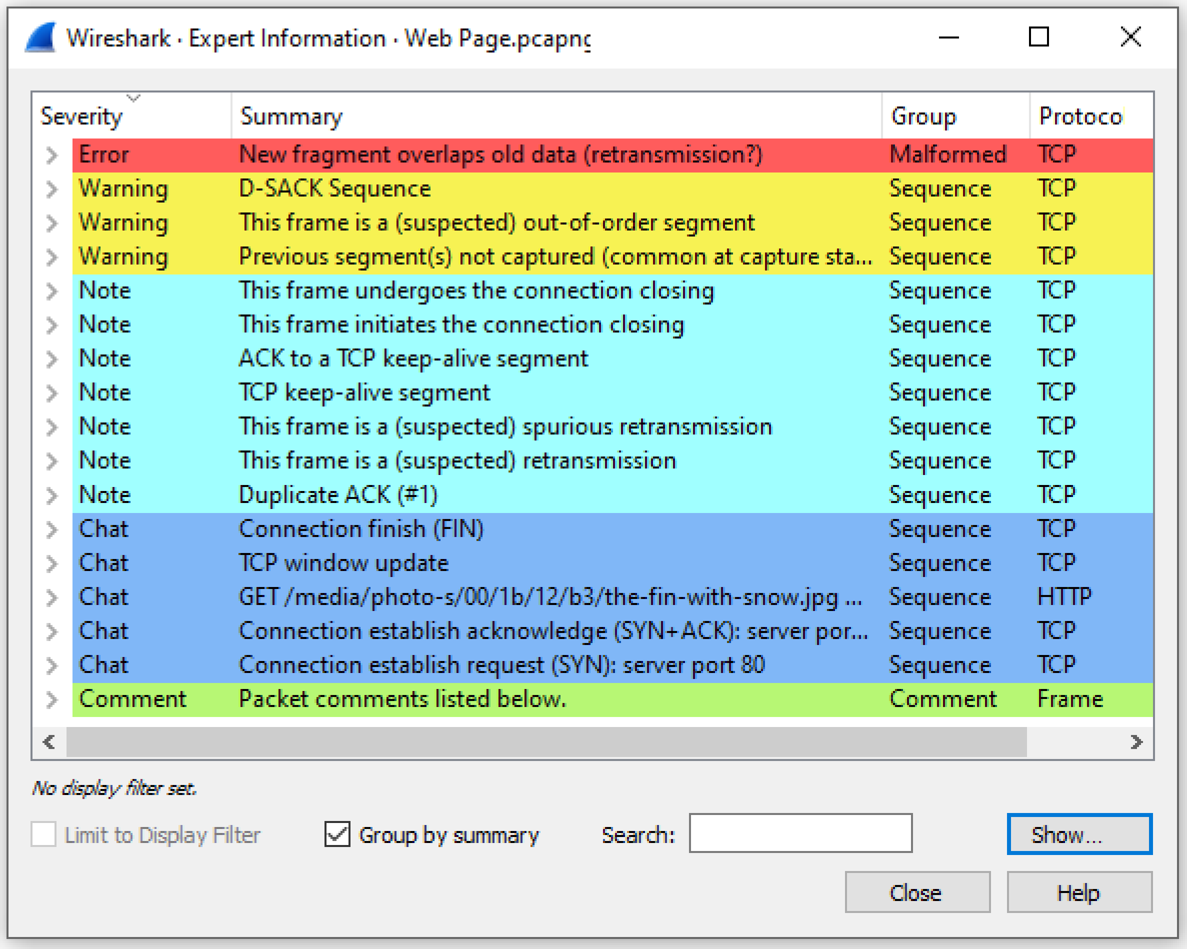

Packet Comments
Add New Comment... Ctrl+Alt+C
Delete All Packet Comments
Configuration Profiles... Ctrl+Shift+A
Preferences... Ctrl+Shift+P


*Web Page.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  Time   Source         Destination
  1  0.000  172.16.133.41  23.62.105.87
  2  0.051  23.62.105.87   172.16.133.41
  3  0.051  172.16.133.41  23.62.105.87
  4  0.053  172.16.133.41  23.62.105.87
```

```
> Frame 1: 66 bytes on wire (528 bits), 66 bytes captu
> Ethernet II, Src: 00:21:70:67:6f:50, Dst: 00:90:7f:3
> Internet Protocol Version 4, Src: 172.16.133.41, Dst
> Transmission Control Protocol, Src Port: 52678, Dst
```

Frame (frame), 66 bytes | Packets: 206 · Displayed: 206 (100.0%) | Profile: Lisa



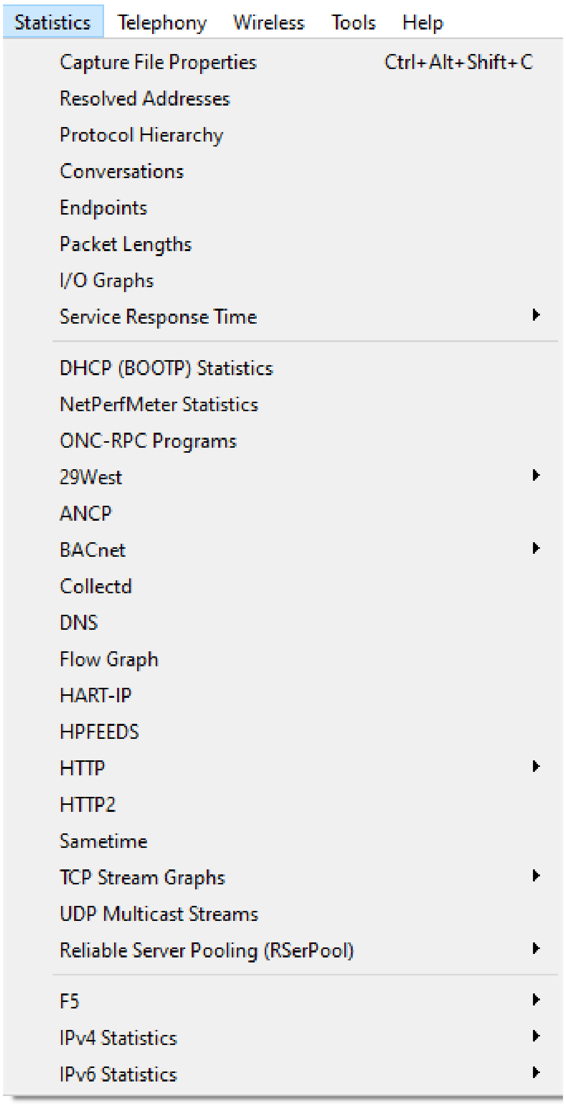
Wireshark · Expert Information · Web Page.pcapng

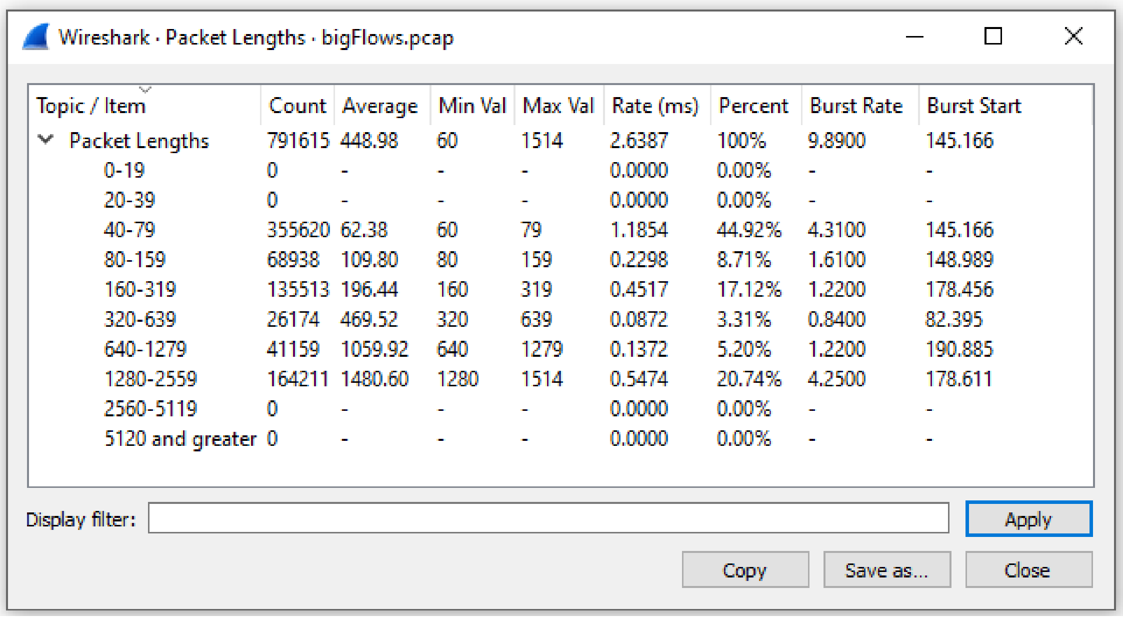
Severity	Summary	Group	Protoco
Error	New fragment overlaps old data (retransmission?)	Malformed	TCP
Warning	D-SACK Sequence	Sequence	TCP
Warning	This frame is a (suspected) out-of-order segment	Sequence	TCP
Warning	Previous segment(s) not captured (common at capture sta...	Sequence	TCP
Note	This frame undergoes the connection closing	Sequence	TCP
Note	This frame initiates the connection closing	Sequence	TCP
Note	ACK to a TCP keep-alive segment	Sequence	TCP
Note	TCP keep-alive segment	Sequence	TCP
Note	This frame is a (suspected) spurious retransmission	Sequence	TCP
Note	This frame is a (suspected) retransmission	Sequence	TCP
Note	Duplicate ACK (#1)	Sequence	TCP
Chat	Connection finish (FIN)	Sequence	TCP
Chat	TCP window update	Sequence	TCP
Chat	GET /media/photo-s/00/1b/12/b3/the-fin-with-snow.jpg ...	Sequence	HTTP
Chat	Connection establish acknowledge (SYN+ACK): server por...	Sequence	TCP
Chat	Connection establish request (SYN): server port 80	Sequence	TCP
Comment	Packet comments listed below.	Comment	Frame

No display filter set.

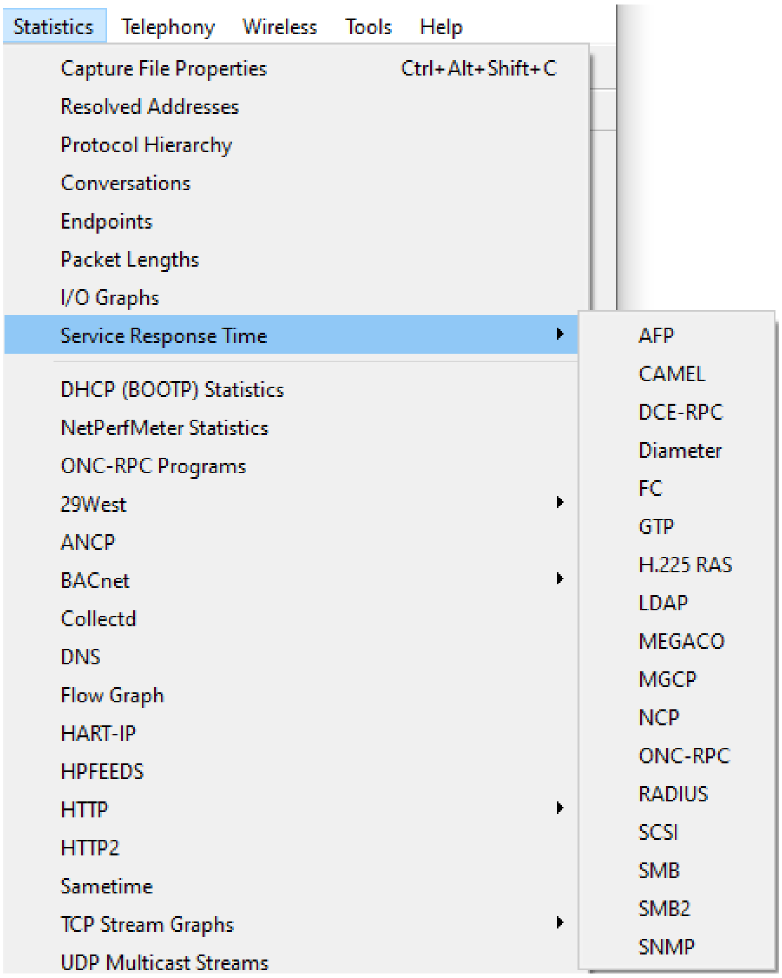
☐ Limit to Display Filter ☑ Group by summary Search:

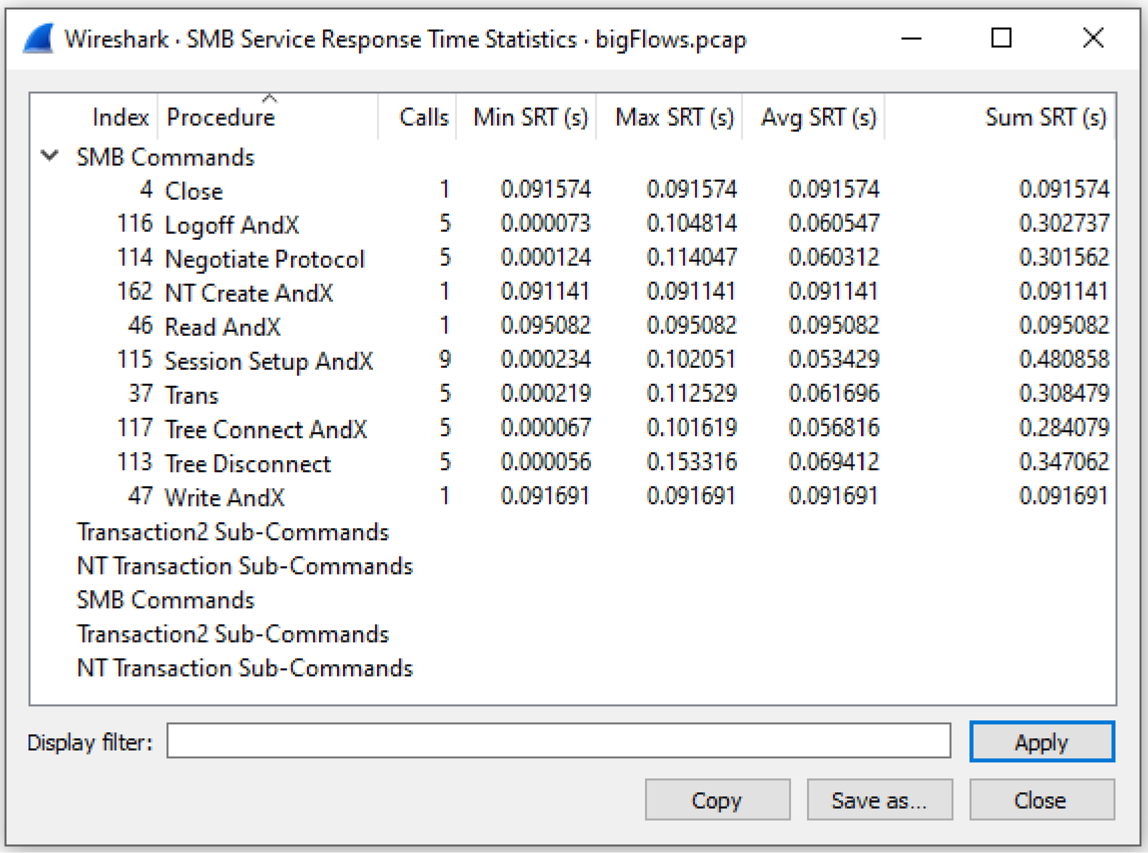
Chapter 19: Discovering I/O and Stream Graphs





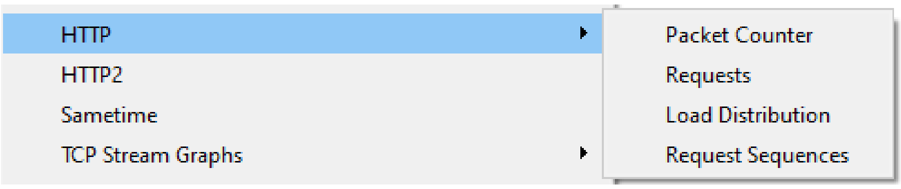
Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
Packet Lengths	791615	448.98	60	1514	2.6387	100%	9.8900	145.166
0-19	0	-	-	-	0.0000	0.00%	-	-
20-39	0	-	-	-	0.0000	0.00%	-	-
40-79	355620	62.38	60	79	1.1854	44.92%	4.3100	145.166
80-159	68938	109.80	80	159	0.2298	8.71%	1.6100	148.989
160-319	135513	196.44	160	319	0.4517	17.12%	1.2200	178.456
320-639	26174	469.52	320	639	0.0872	3.31%	0.8400	82.395
640-1279	41159	1059.92	640	1279	0.1372	5.20%	1.2200	190.885
1280-2559	164211	1480.60	1280	1514	0.5474	20.74%	4.2500	178.611
2560-5119	0	-	-	-	0.0000	0.00%	-	-
5120 and greater	0	-	-	-	0.0000	0.00%	-	-

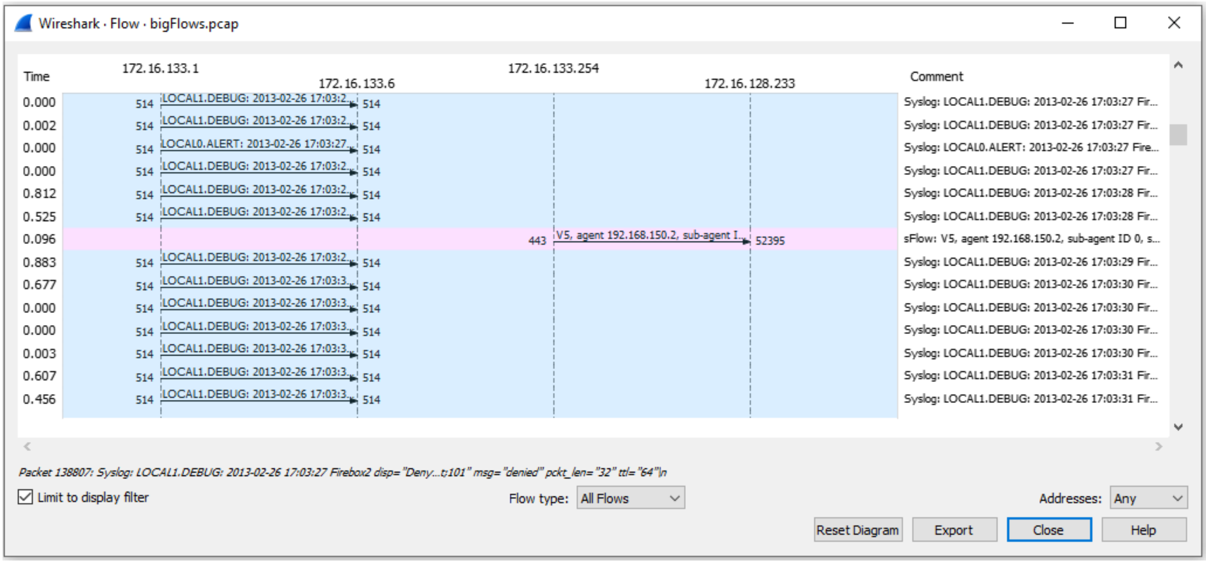



Wireshark · SMB Service Response Time Statistics · bigFlows.pcap

Index	Procedure	Calls	Min SRT (s)	Max SRT (s)	Avg SRT (s)	Sum SRT (s)
SMB Commands						
4	Close	1	0.091574	0.091574	0.091574	0.091574
116	Logoff AndX	5	0.000073	0.104814	0.060547	0.302737
114	Negotiate Protocol	5	0.000124	0.114047	0.060312	0.301562
162	NT Create AndX	1	0.091141	0.091141	0.091141	0.091141
46	Read AndX	1	0.095082	0.095082	0.095082	0.095082
115	Session Setup AndX	9	0.000234	0.102051	0.053429	0.480858
37	Trans	5	0.000219	0.112529	0.061696	0.308479
117	Tree Connect AndX	5	0.000067	0.101619	0.056816	0.284079
113	Tree Disconnect	5	0.000056	0.153316	0.069412	0.347062
47	Write AndX	1	0.091691	0.091691	0.091691	0.091691
Transaction2 Sub-Commands						
NT Transaction Sub-Commands						
SMB Commands						
Transaction2 Sub-Commands						
NT Transaction Sub-Commands						

Display filter:



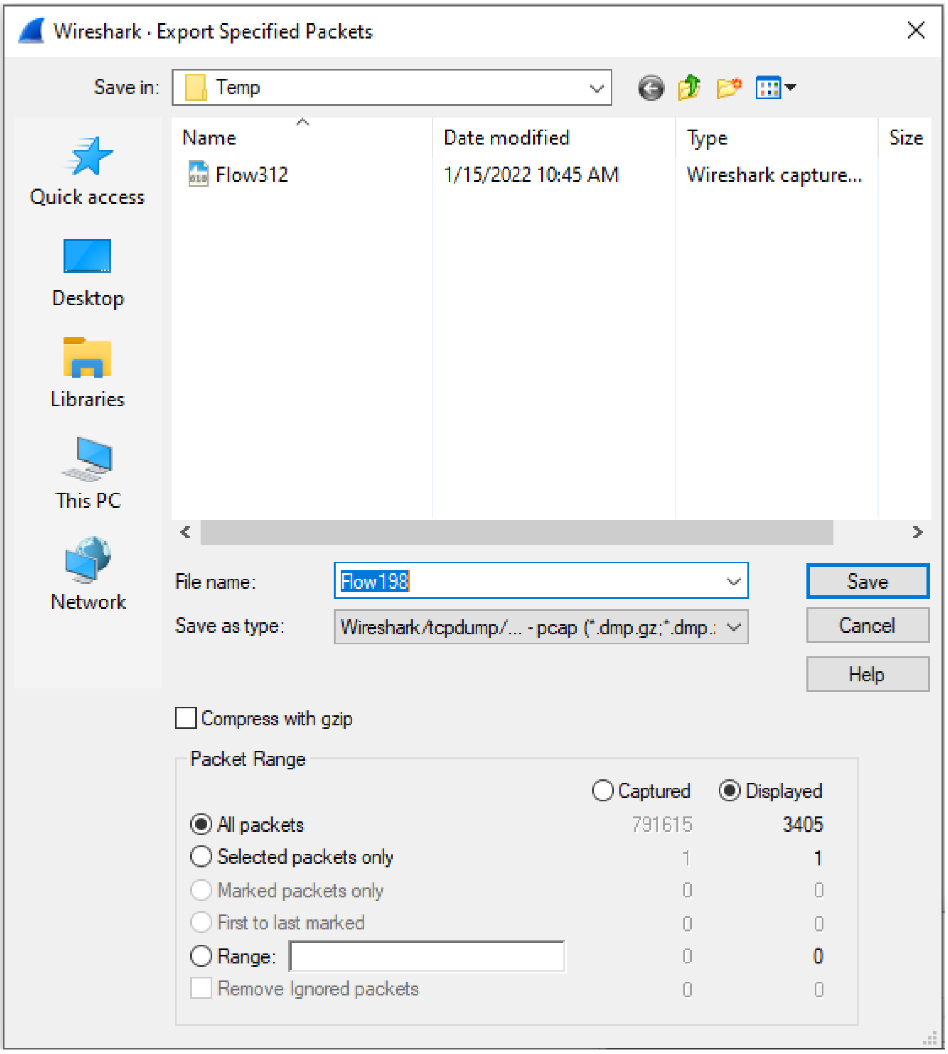


```
Time   172.16.133.1  172.16.133.6  172.16.133.254  172.16.128.233   Comment
0.000  514 LOCAL1.DEBUG: 2013-02-26 17:03:2.. 514    Syslog: LOCAL1.DEBUG: 2013-02-26 17:03:27 Fir...
0.002  514 LOCAL1.DEBUG: 2013-02-26 17:03:2.. 514    Syslog: LOCAL1.DEBUG: 2013-02-26 17:03:27 Fir...
0.000  514 LOCAL0.ALERT: 2013-02-26 17:03:27.. 514   Syslog: LOCAL0.ALERT: 2013-02-26 17:03:27 Fire...
0.000  514 LOCAL1.DEBUG: 2013-02-26 17:03:2.. 514    Syslog: LOCAL1.DEBUG: 2013-02-26 17:03:27 Fir...
0.812  514 LOCAL1.DEBUG: 2013-02-26 17:03:2.. 514    Syslog: LOCAL1.DEBUG: 2013-02-26 17:03:28 Fir...
0.525  514 LOCAL1.DEBUG: 2013-02-26 17:03:2.. 514    Syslog: LOCAL1.DEBUG: 2013-02-26 17:03:28 Fir...
0.096  443 V5, agent 192.168.150.2, sub-agent I.. 52395   sFlow: V5, agent 192.168.150.2, sub-agent ID 0, s...
0.883  514 LOCAL1.DEBUG: 2013-02-26 17:03:2.. 514    Syslog: LOCAL1.DEBUG: 2013-02-26 17:03:29 Fir...
0.677  514 LOCAL1.DEBUG: 2013-02-26 17:03:3.. 514    Syslog: LOCAL1.DEBUG: 2013-02-26 17:03:30 Fir...
0.000  514 LOCAL1.DEBUG: 2013-02-26 17:03:3.. 514    Syslog: LOCAL1.DEBUG: 2013-02-26 17:03:30 Fir...
0.000  514 LOCAL1.DEBUG: 2013-02-26 17:03:3.. 514    Syslog: LOCAL1.DEBUG: 2013-02-26 17:03:30 Fir...
0.003  514 LOCAL1.DEBUG: 2013-02-26 17:03:3.. 514    Syslog: LOCAL1.DEBUG: 2013-02-26 17:03:30 Fir...
0.607  514 LOCAL1.DEBUG: 2013-02-26 17:03:3.. 514    Syslog: LOCAL1.DEBUG: 2013-02-26 17:03:31 Fir...
0.456  514 LOCAL1.DEBUG: 2013-02-26 17:03:3.. 514    Syslog: LOCAL1.DEBUG: 2013-02-26 17:03:31 Fir...

Packet 138807: Syslog: LOCAL1.DEBUG: 2013-02-26 17:03:27 Firebox2 disp="Deny...t;101" msg="denied" pckt_len="32" ttl="64"\n
```

☑ Limit to display filter

Flow type: All Flows

Addresses: Any



Save in: Temp

Name	Date modified	Type	Size
Flow312	1/15/2022 10:45 AM	Wireshark capture...	

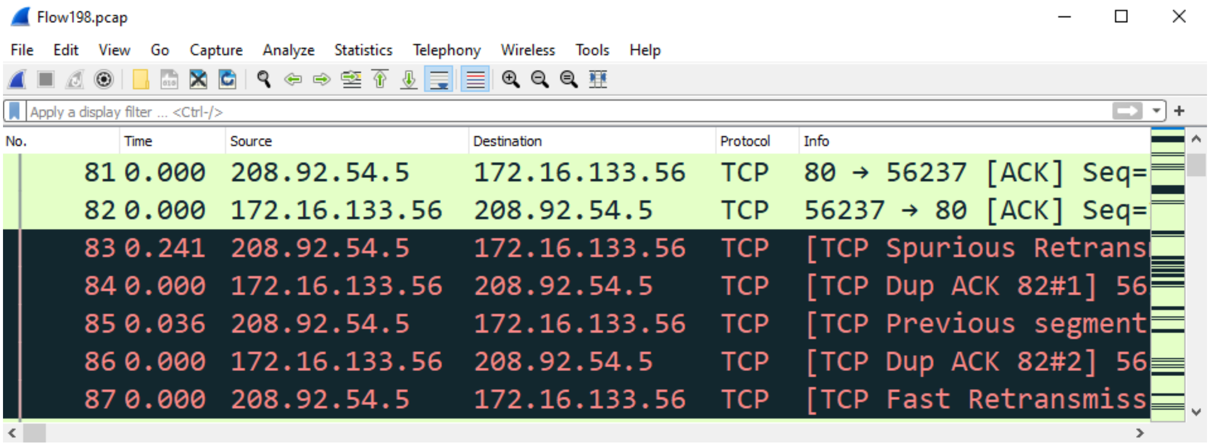
File name: Flow198

Save as type: Wireshark/tcpdump/... - pcap (*.dmp.gz;*.dmp.;

□ Compress with gzip

Packet Range

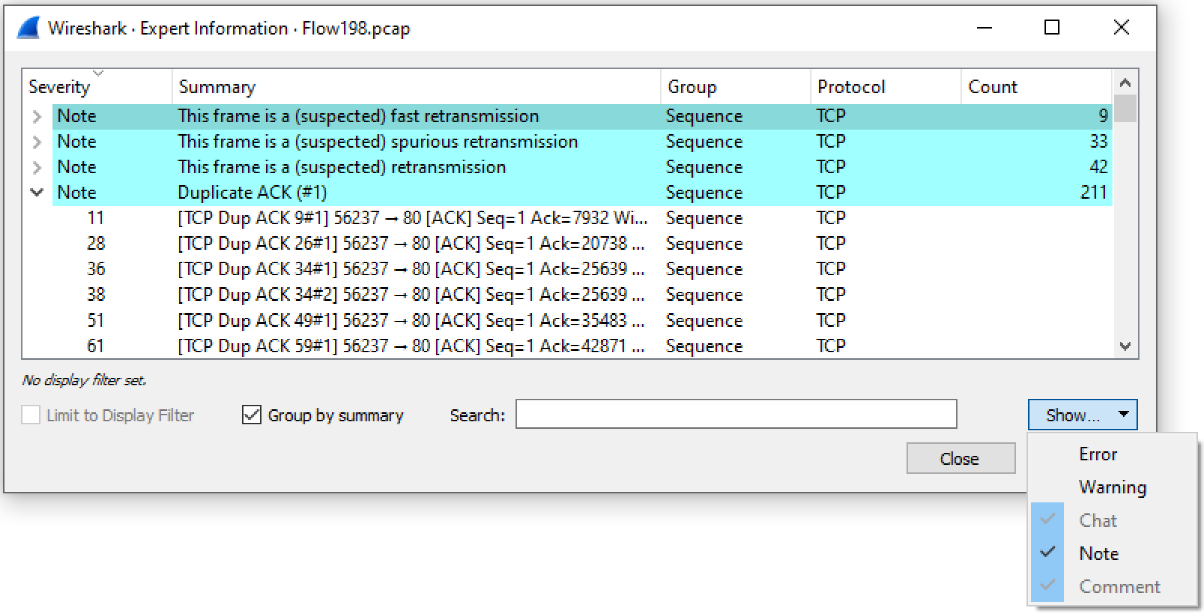
	○ Captured	● Displayed
● All packets	791615	3405
○ Selected packets only	1	1
○ Marked packets only	0	0
○ First to last marked	0	0
○ Range:	0	0
□ Remove Ignored packets	0	0



Flow198.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Info
81	0.000	208.92.54.5	172.16.133.56	TCP	80 → 56237 [ACK] Seq=
82	0.000	172.16.133.56	208.92.54.5	TCP	56237 → 80 [ACK] Seq=
83	0.241	208.92.54.5	172.16.133.56	TCP	[TCP Spurious Retrans
84	0.000	172.16.133.56	208.92.54.5	TCP	[TCP Dup ACK 82#1] 56
85	0.036	208.92.54.5	172.16.133.56	TCP	[TCP Previous segment
86	0.000	172.16.133.56	208.92.54.5	TCP	[TCP Dup ACK 82#2] 56
87	0.000	208.92.54.5	172.16.133.56	TCP	[TCP Fast Retransmiss

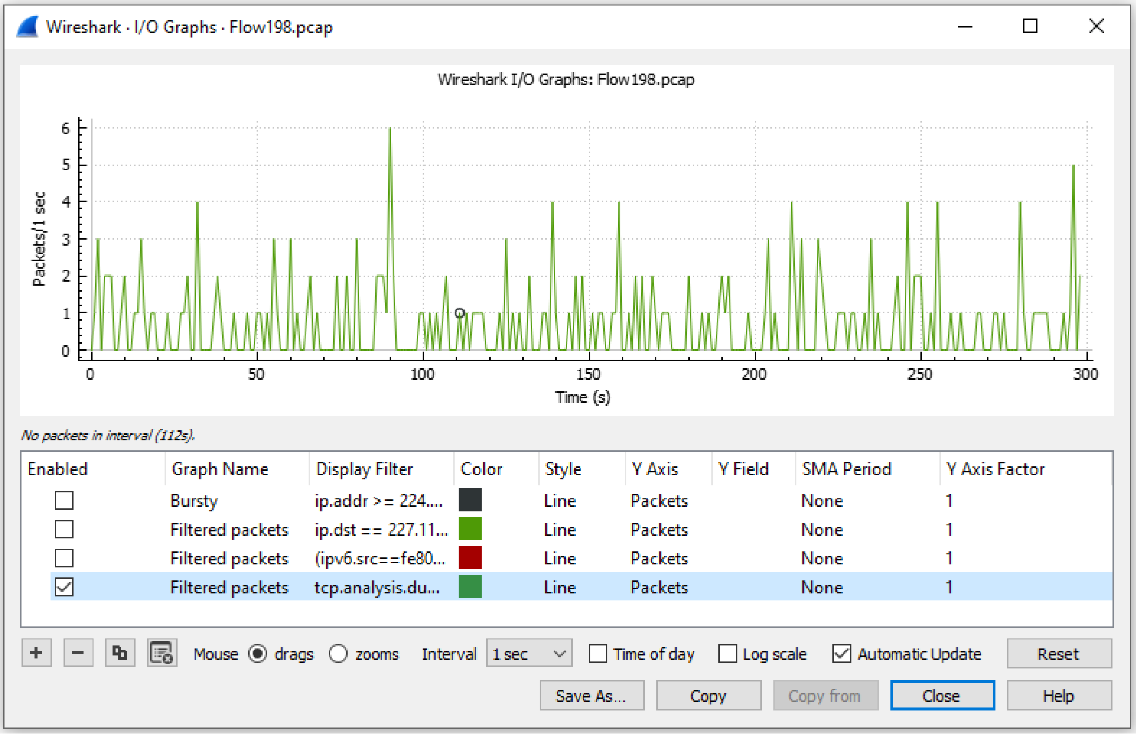


Wireshark · Expert Information · Flow198.pcap

Severity	Summary	Group	Protocol	Count
› Note	This frame is a (suspected) fast retransmission	Sequence	TCP	9
› Note	This frame is a (suspected) spurious retransmission	Sequence	TCP	33
› Note	This frame is a (suspected) retransmission	Sequence	TCP	42
⌄ Note	Duplicate ACK (#1)	Sequence	TCP	211
11	[TCP Dup ACK 9#1] 56237 → 80 [ACK] Seq=1 Ack=7932 Wi...	Sequence	TCP	
28	[TCP Dup ACK 26#1] 56237 → 80 [ACK] Seq=1 Ack=20738 ...	Sequence	TCP	
36	[TCP Dup ACK 34#1] 56237 → 80 [ACK] Seq=1 Ack=25639 ...	Sequence	TCP	
38	[TCP Dup ACK 34#2] 56237 → 80 [ACK] Seq=1 Ack=25639 ...	Sequence	TCP	
51	[TCP Dup ACK 49#1] 56237 → 80 [ACK] Seq=1 Ack=35483 ...	Sequence	TCP	
61	[TCP Dup ACK 59#1] 56237 → 80 [ACK] Seq=1 Ack=42871 ...	Sequence	TCP	

No display filter set.

☐ Limit to Display Filter ☑ Group by summary Search:

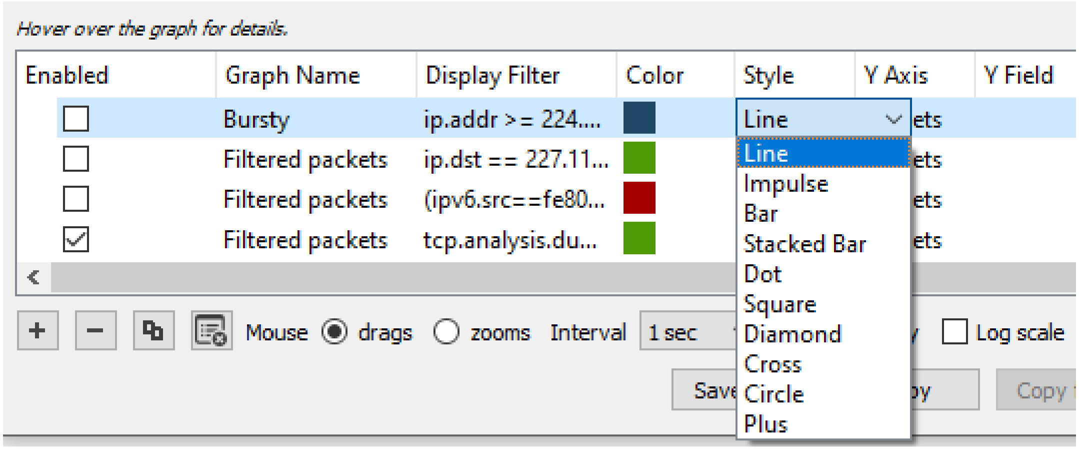


Wireshark · I/O Graphs · Flow198.pcap

No packets in interval (112s).

Enabled	Graph Name	Display Filter	Color	Style	Y Axis	Y Field	SMA Period	Y Axis Factor
☐	Bursty	ip.addr >= 224....	⬛	Line	Packets		None	1
☐	Filtered packets	ip.dst == 227.11...	🟩	Line	Packets		None	1
☐	Filtered packets	(ipv6.src==fe80...	🟥	Line	Packets		None	1
☑	Filtered packets	tcp.analysis.du...	🟩	Line	Packets		None	1

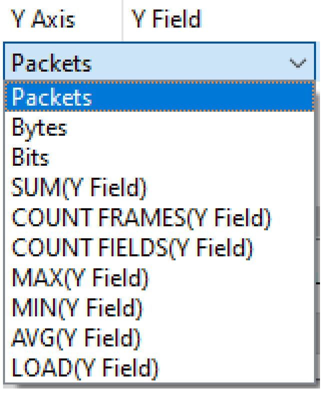
Mouse ● drags ○ zooms Interval 1 sec ☐ Time of day ☐ Log scale ☑ Automatic Update

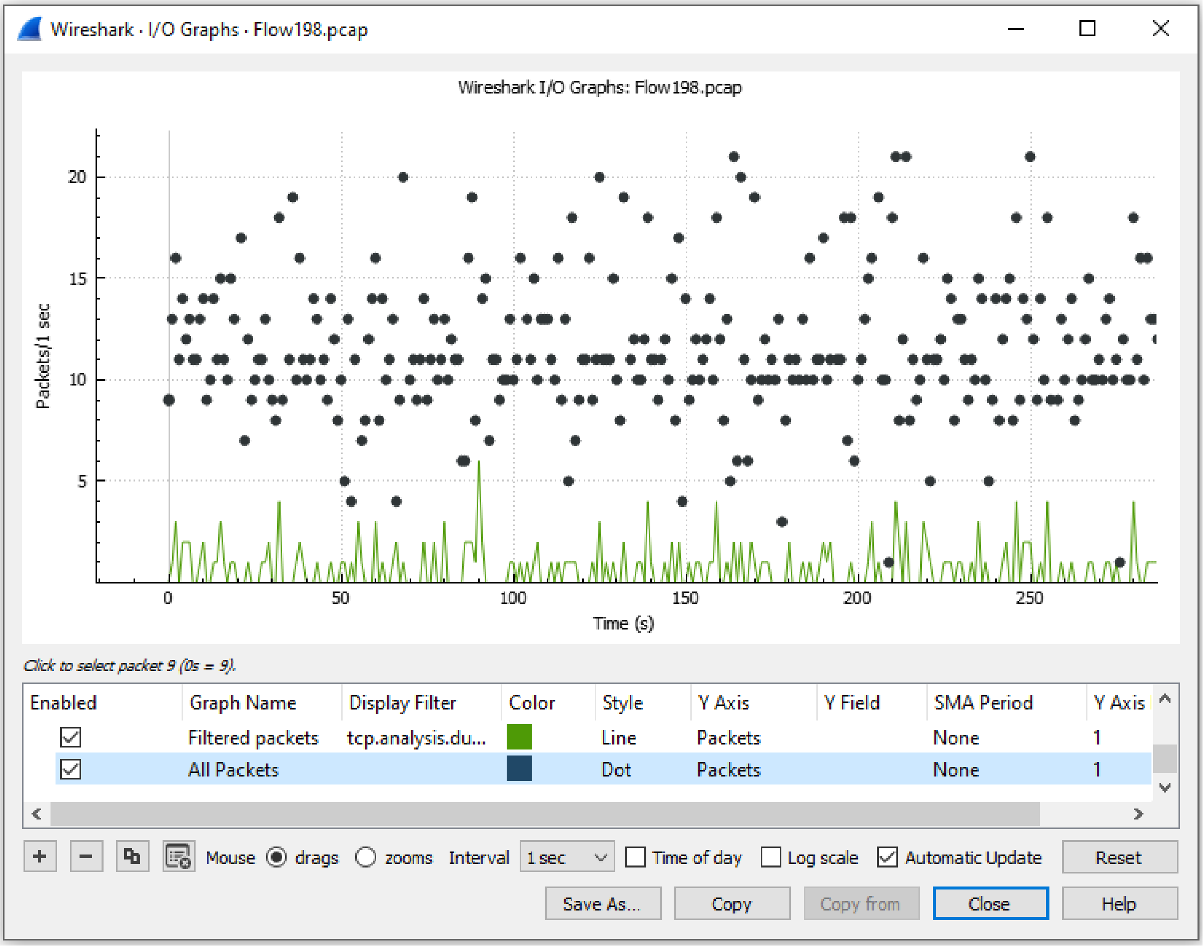


Hover over the graph for details.

Enabled	Graph Name	Display Filter	Color	Style	Y Axis	Y Field
☐	Bursty	ip.addr >= 224....	🟦	Line	ets	
☐	Filtered packets	ip.dst == 227.11...	🟩		ets	
☐	Filtered packets	(ipv6.src==fe80...	🟥		ets	
☑	Filtered packets	tcp.analysis.du...	🟩		ets	

Mouse ● drags ○ zooms Interval 1 sec ☐ Log scale



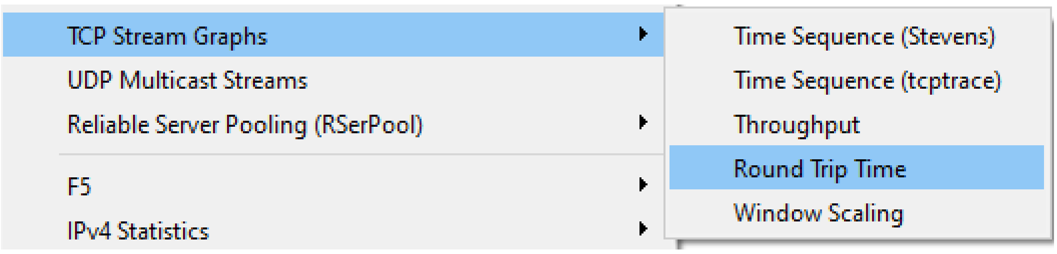


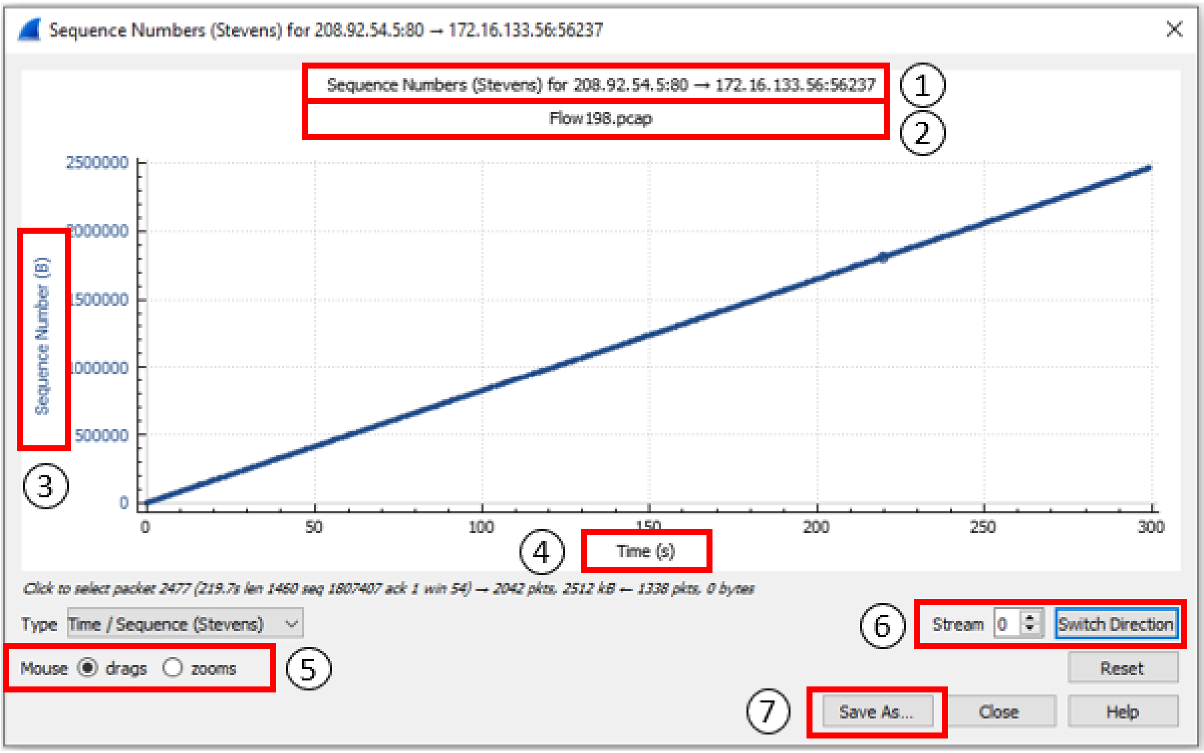
Wireshark · I/O Graphs · Flow198.pcap

Click to select packet 9 (0s = 9).

Enabled	Graph Name	Display Filter	Color	Style	Y Axis	Y Field	SMA Period	Y Axis
☑	Filtered packets	tcp.analysis.du...	🟩	Line	Packets		None	1
☑	All Packets		🟦	Dot	Packets		None	1

Mouse ● drags ○ zooms Interval 1 sec ☐ Time of day ☐ Log scale ☑ Automatic Update




Sequence Numbers (Stevens) for 208.92.54.5:80 → 172.16.133.56:56237

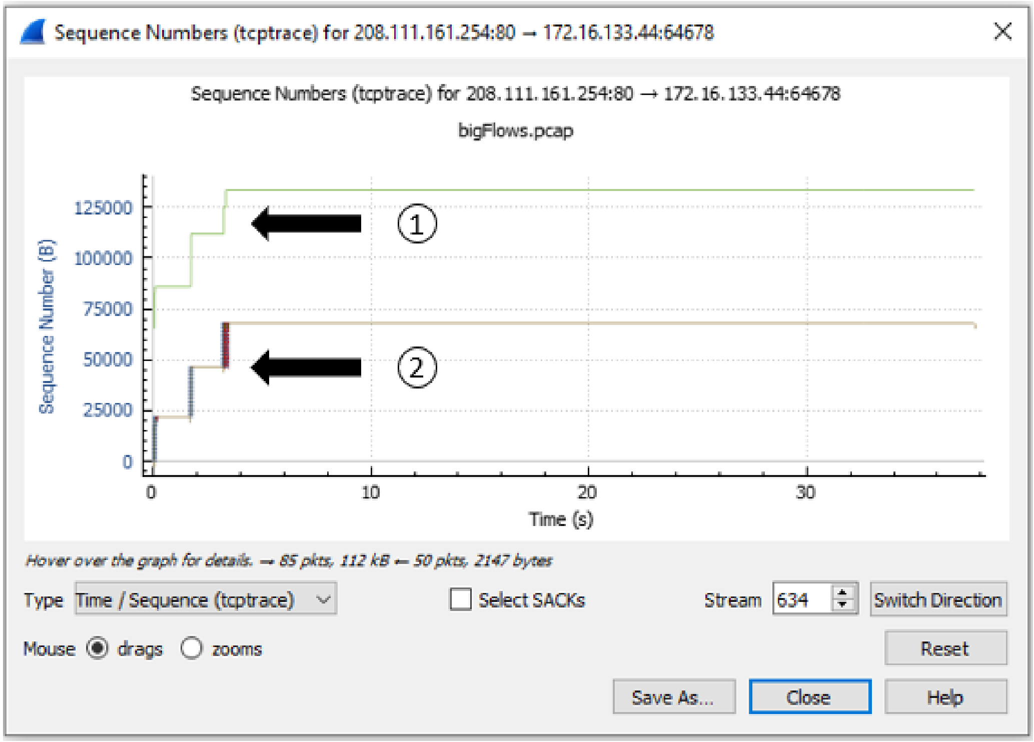
Flow198.pcap

Click to select packet 2477 (219.7s len 1460 seq 1807407 ack 1 win 54) → 2042 pkts, 2512 kB ← 1338 pkts, 0 bytes

Type Time / Sequence (Stevens)

Mouse ● drags ○ zooms

Stream 0


Sequence Numbers (tcptrace) for 208.111.161.254:80 → 172.16.133.44:64678

bigFlows.pcap

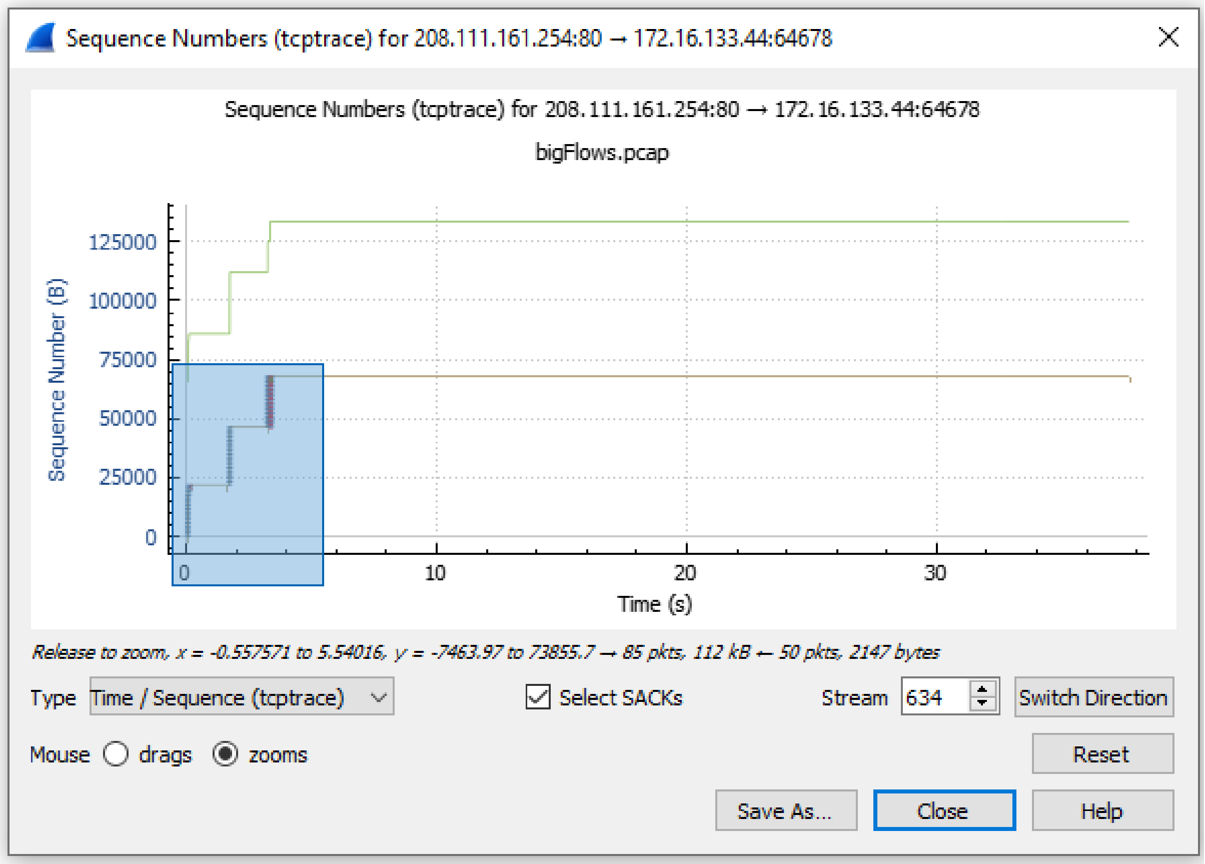
Hover over the graph for details. → 85 pkts, 112 kB ← 50 pkts, 2147 bytes

Type Time / Sequence (tcptrace)

□ Select SACKs

Stream 634

Mouse ● drags ○ zooms



Sequence Numbers (tcptrace) for 208.111.161.254:80 → 172.16.133.44:64678

Sequence Numbers (tcptrace) for 208.111.161.254:80 → 172.16.133.44:64678

bigFlows.pcap

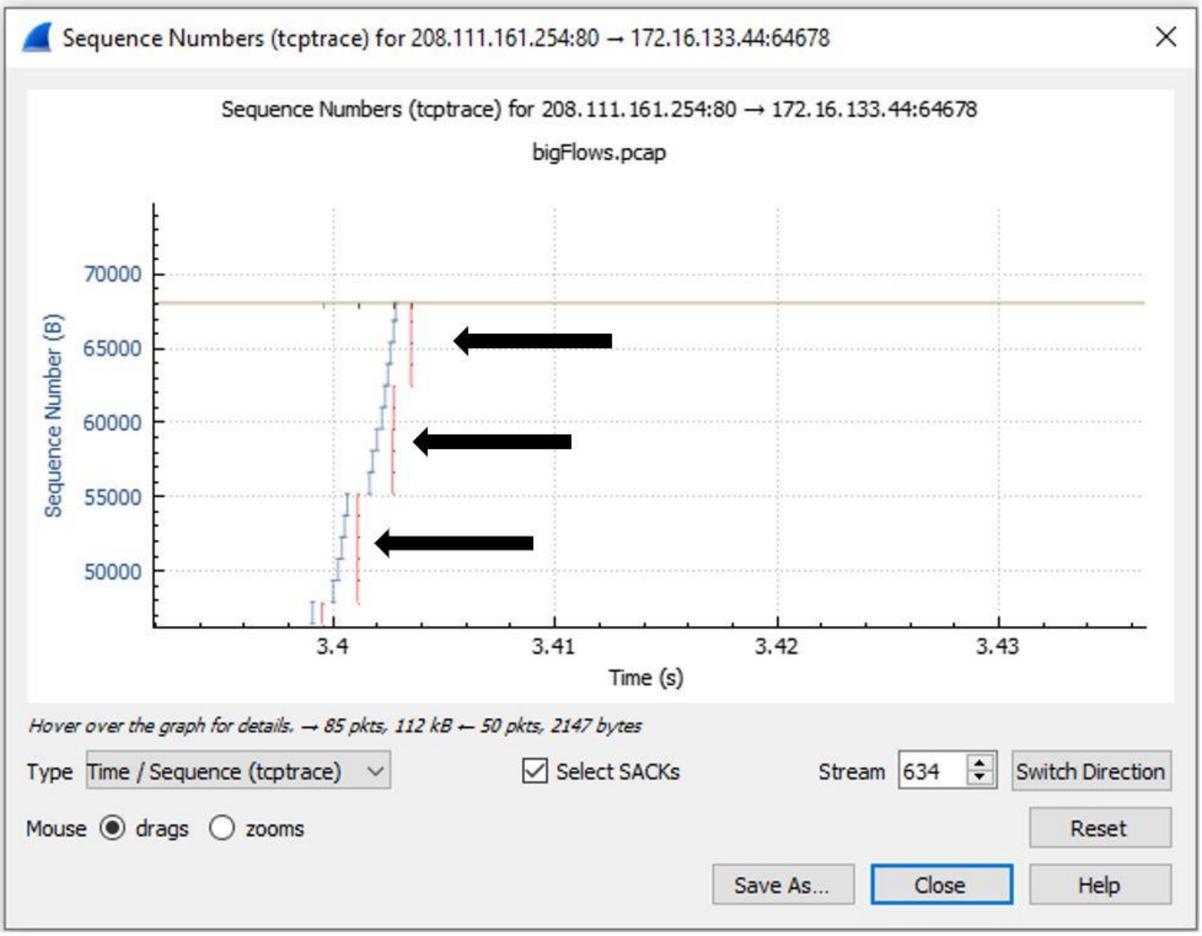
Release to zoom, x = -0.557571 to 5.54016, y = -7463.97 to 73855.7 → 85 pkts, 112 kB ← 50 pkts, 2147 bytes

Type: Time / Sequence (tcptrace)

☑ Select SACKs

Stream: 634

Mouse ○ drags ● zooms



Sequence Numbers (tcptrace) for 208.111.161.254:80 → 172.16.133.44:64678

Sequence Numbers (tcptrace) for 208.111.161.254:80 → 172.16.133.44:64678

bigFlows.pcap

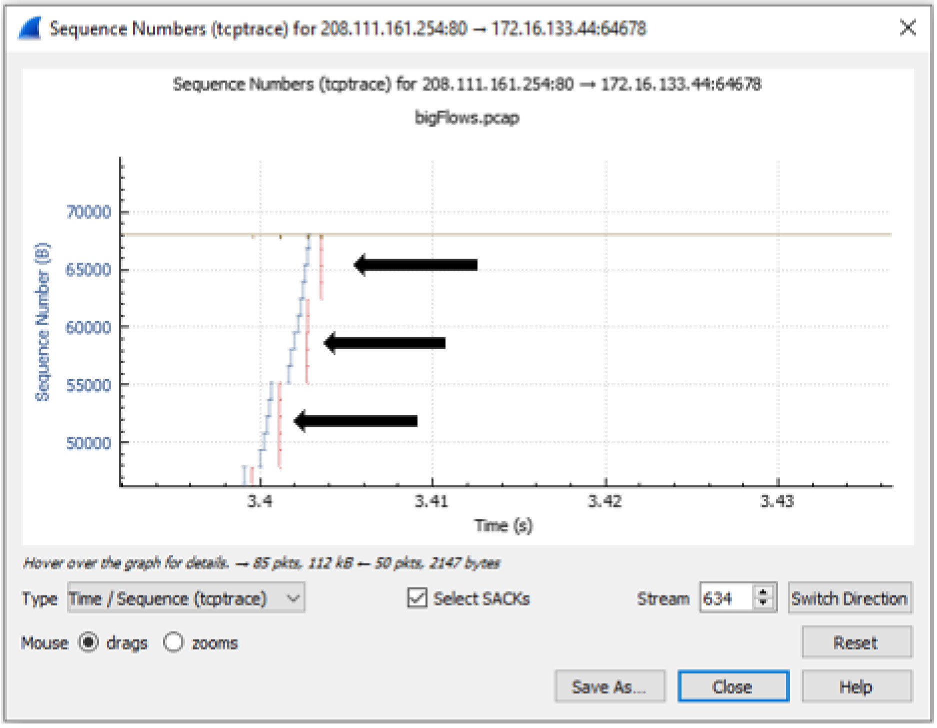
Hover over the graph for details. → 85 pkts, 112 kB ← 50 pkts, 2147 bytes

Type: Time / Sequence (tcptrace)

☑ Select SACKs

Stream: 634

Mouse ● drags ○ zooms

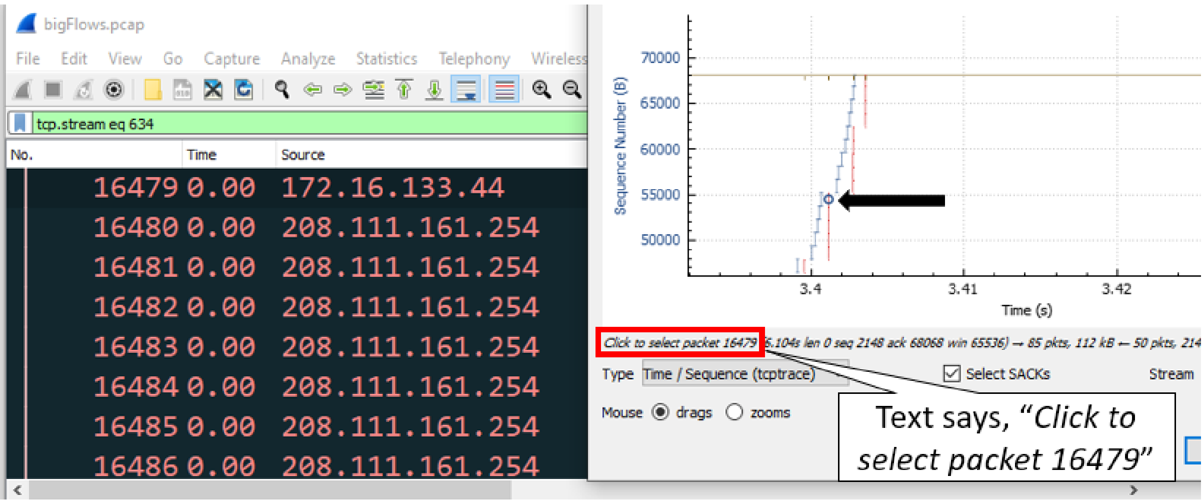


Sequence Numbers (tcptrace) for 208.111.161.254:80 → 172.16.133.44:64678

Hover over the graph for details. → 85 pkts, 112 kB ← 50 pkts, 2147 bytes

Type: Time / Sequence (tcptrace)   ☑ Select SACKs   Stream: 634

Mouse ● drags ○ zooms



bigFlows.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless

tcp.stream eq 634

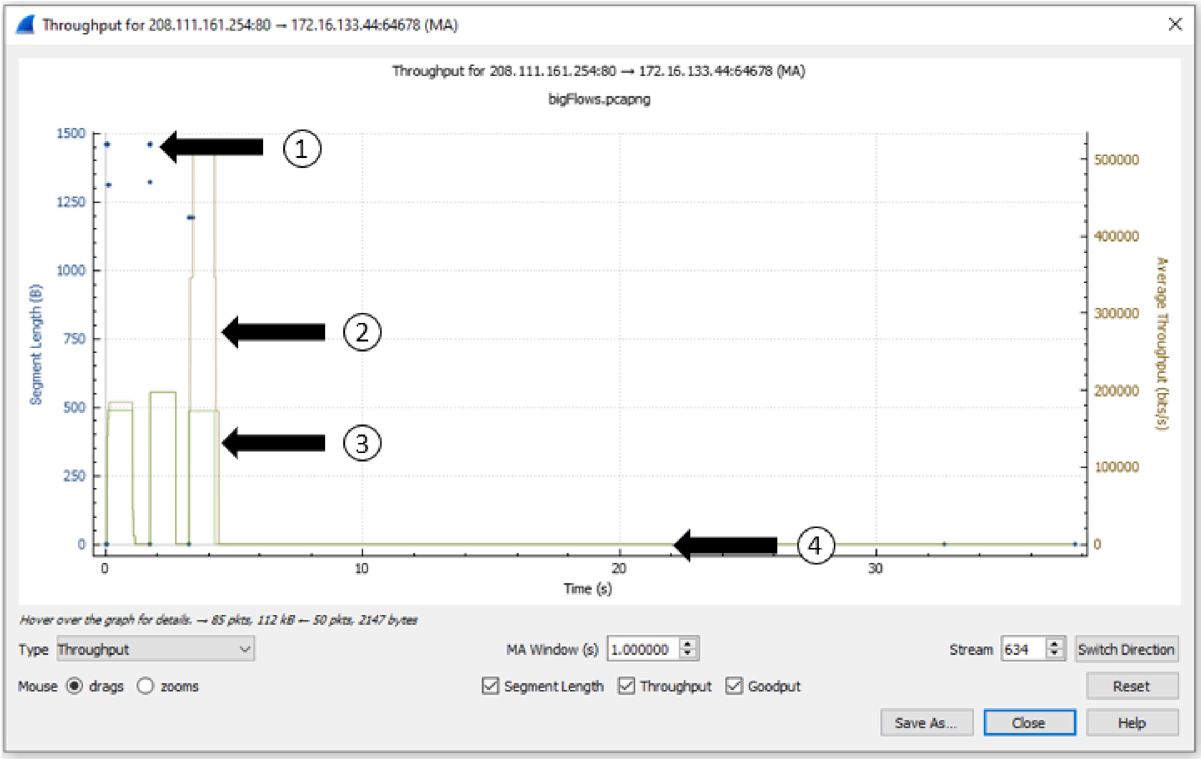
No.	Time	Source
16479	0.00	172.16.133.44
16480	0.00	208.111.161.254
16481	0.00	208.111.161.254
16482	0.00	208.111.161.254
16483	0.00	208.111.161.254
16484	0.00	208.111.161.254
16485	0.00	208.111.161.254
16486	0.00	208.111.161.254

Click to select packet 16479 6.104s len 0 seq 2148 ack 68068 win 65536) → 85 pkts, 112 kB ← 50 pkts, 214

Type: Time / Sequence (tcptrace)   ☑ Select SACKs   Stream

Mouse ● drags ○ zooms

Text says, "*Click to select packet 16479*"



Throughput for 208.111.161.254:80 → 172.16.133.44:64678 (MA)

Throughput for 208.111.161.254:80 → 172.16.133.44:64678 (MA)

bigFlows.pcapng

Hover over the graph for details. → 85 pkts, 112 kB ← 50 pkts, 2147 bytes

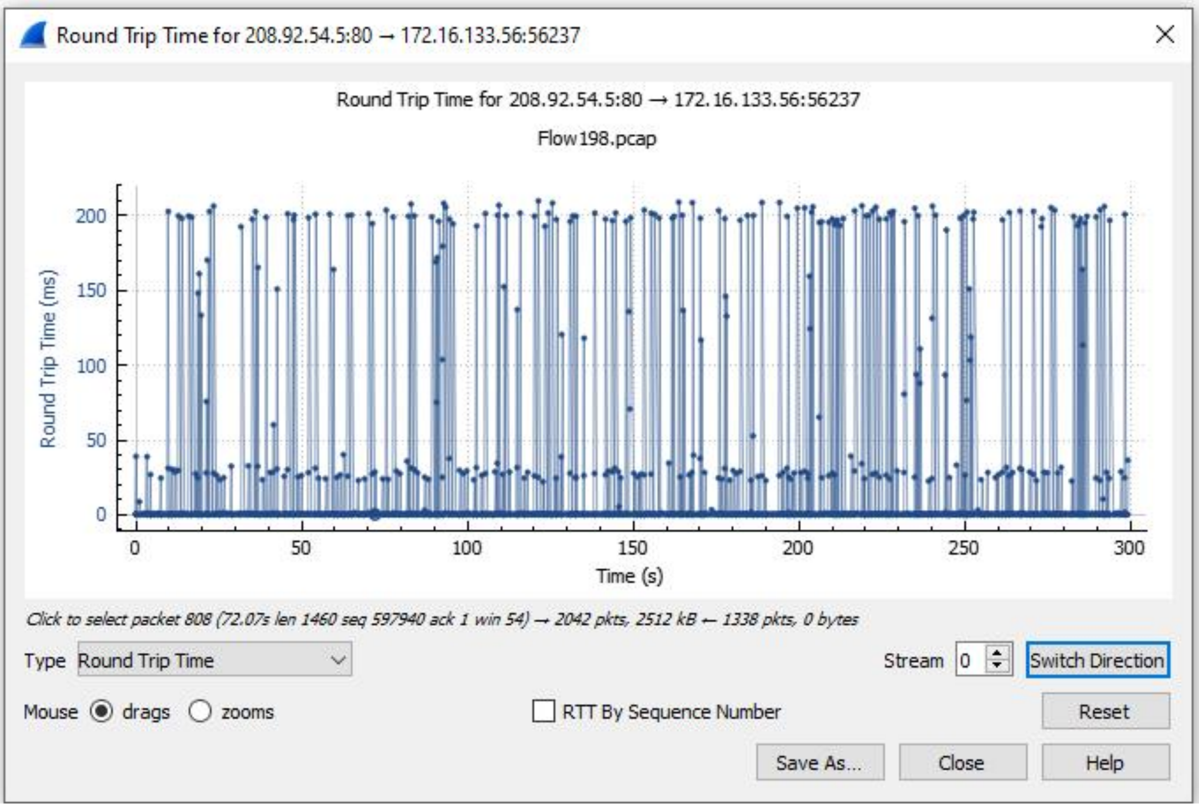
Type: Throughput

MA Window (s): 1.000000

Stream: 634

Mouse ● drags ○ zooms

☑ Segment Length ☑ Throughput ☑ Goodput



Round Trip Time for 208.92.54.5:80 → 172.16.133.56:56237

Round Trip Time for 208.92.54.5:80 → 172.16.133.56:56237

Flow198.pcap

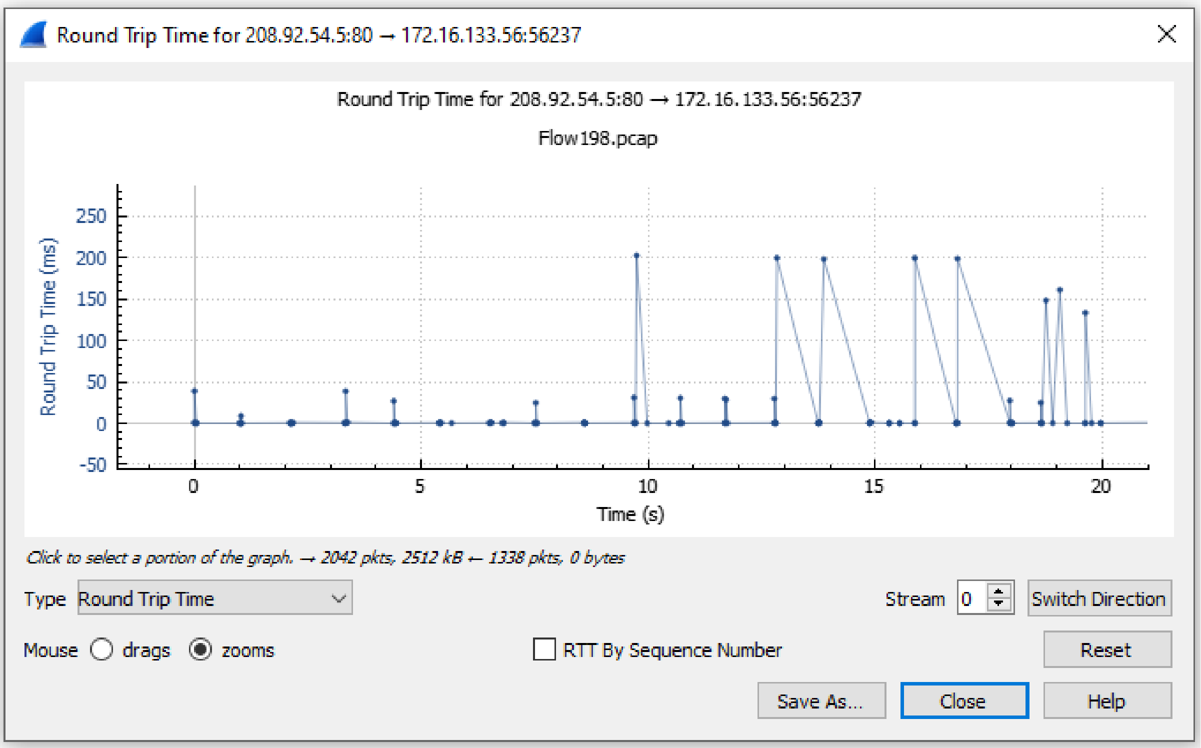
Click to select packet 808 (72.07s len 1460 seq 597940 ack 1 win 54) → 2042 pkts, 2512 kB ← 1338 pkts, 0 bytes

Type: Round Trip Time

Stream: 0

Mouse ● drags ○ zooms

□ RTT By Sequence Number



Round Trip Time for 208.92.54.5:80 → 172.16.133.56:56237

Round Trip Time for 208.92.54.5:80 → 172.16.133.56:56237

Flow198.pcap

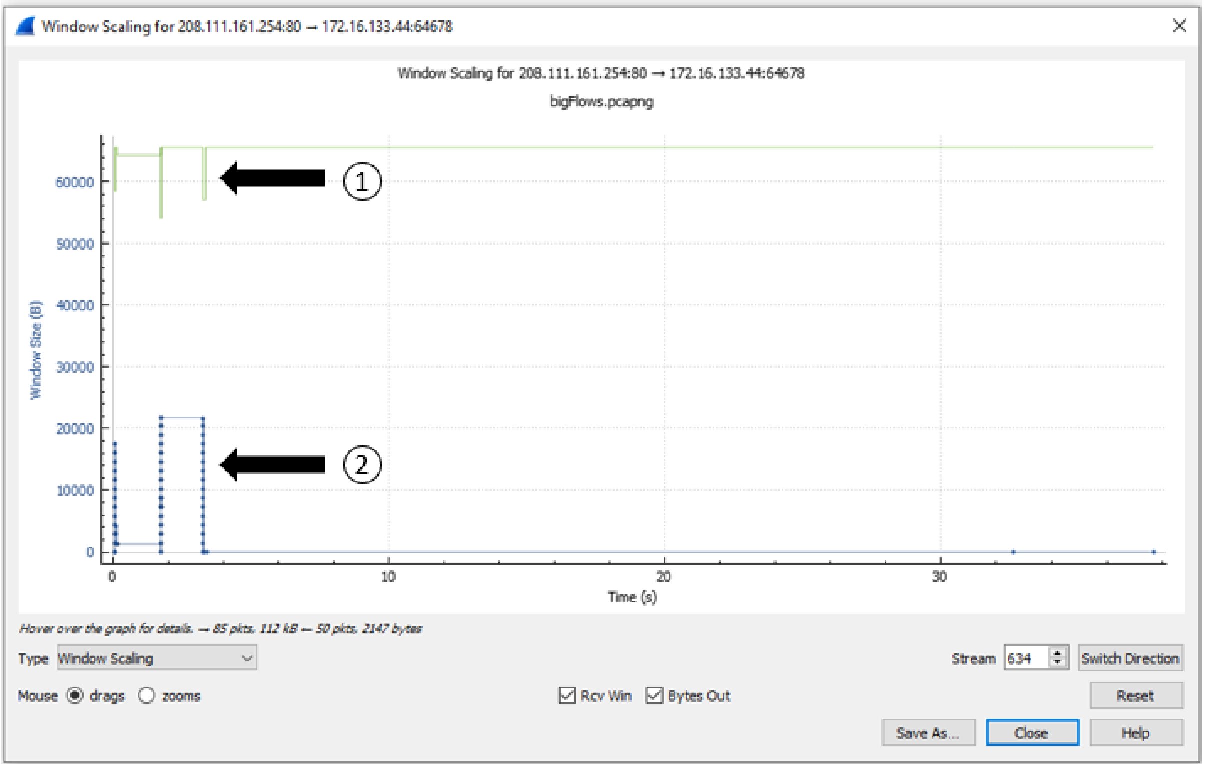
Click to select a portion of the graph. → 2042 pkts, 2512 kB ← 1338 pkts, 0 bytes

Type Round Trip Time

Stream 0

Mouse ○ drags ● zooms

□ RTT By Sequence Number



Window Scaling for 208.111.161.254:80 → 172.16.133.44:64678

Window Scaling for 208.111.161.254:80 → 172.16.133.44:64678

bigFlows.pcapng

Hover over the graph for details. → 85 pkts, 112 kB ← 50 pkts, 2147 bytes

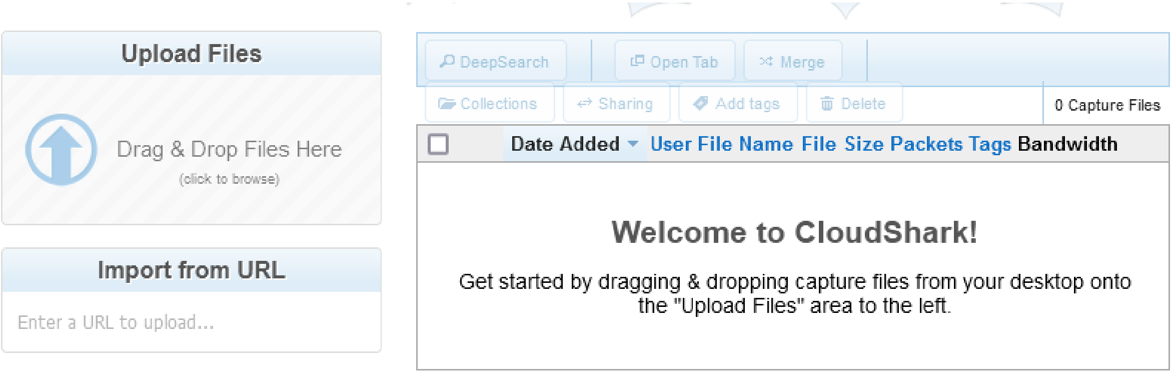
Type Window Scaling

Stream 634

Mouse ● drags ○ zooms

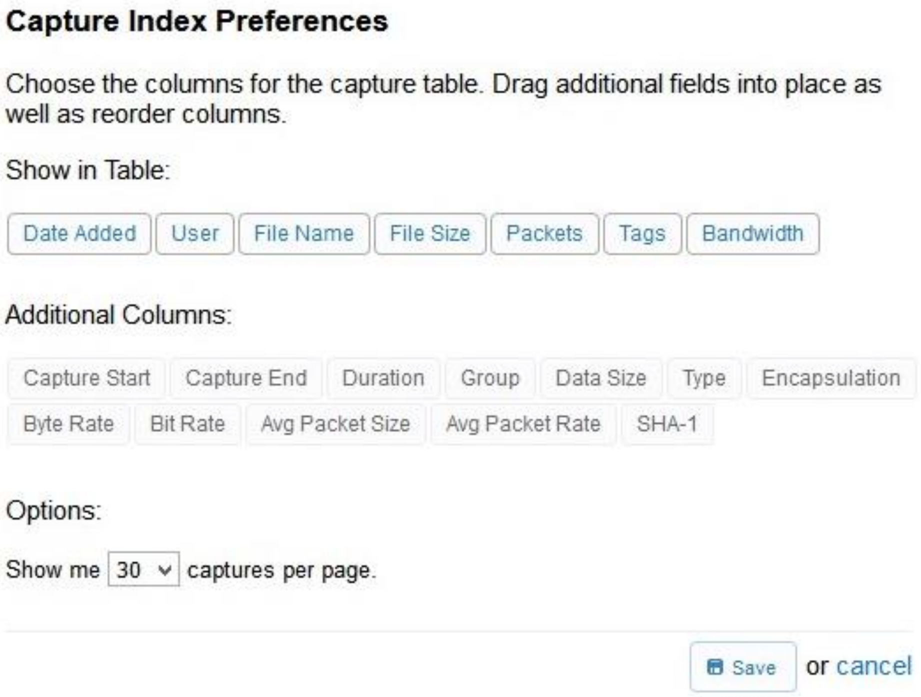
☑ Rcv Win ☑ Bytes Out

Chapter 20: Using Cloudshark for Packet Analysis



Welcome to CloudShark!

Get started by dragging & dropping capture files from your desktop onto the "Upload Files" area to the left.



Capture Index Preferences

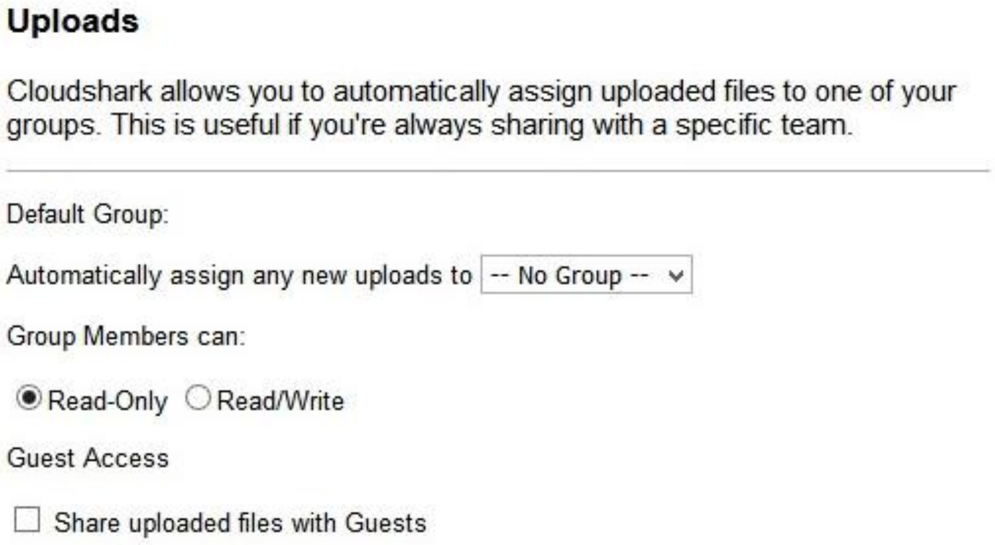
Choose the columns for the capture table. Drag additional fields into place as well as reorder columns.

Show in Table:

Additional Columns:

Options:

Show me 30 captures per page.



Uploads

Cloudshark allows you to automatically assign uploaded files to one of your groups. This is useful if you're always sharing with a specific team.

Default Group:

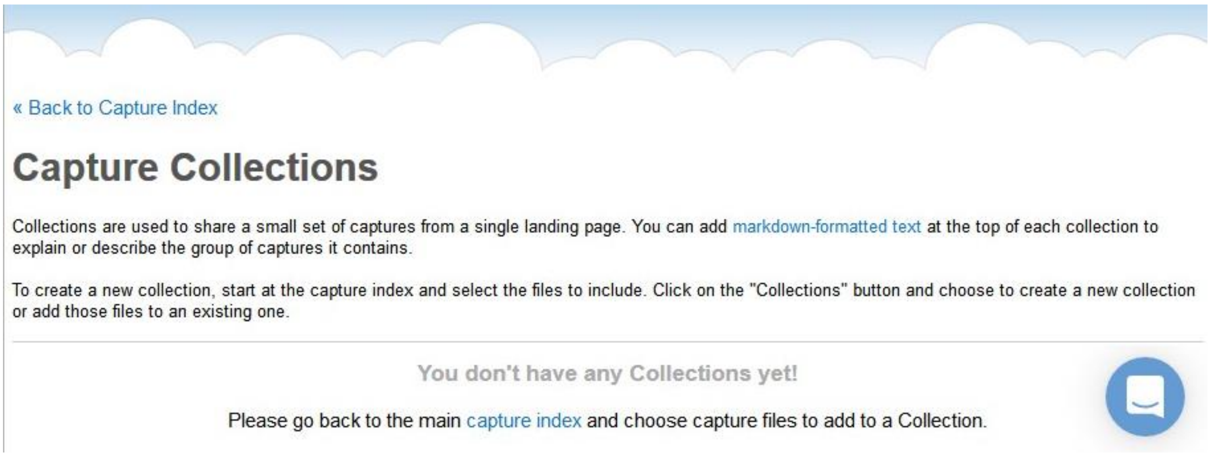
Automatically assign any new uploads to -- No Group --

Group Members can:

● Read-Only ○ Read/Write

Guest Access

□ Share uploaded files with Guests



« Back to Capture Index

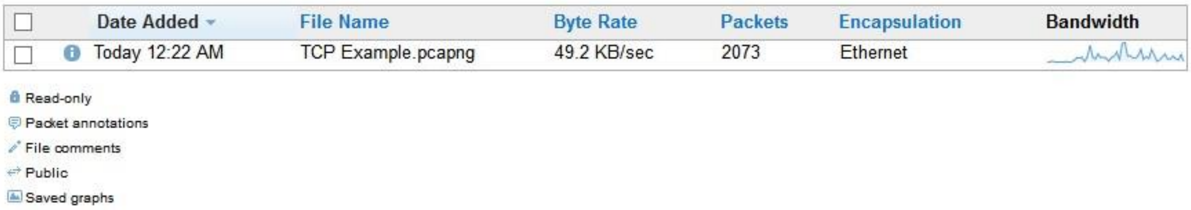
Capture Collections

Collections are used to share a small set of captures from a single landing page. You can add markdown-formatted text at the top of each collection to explain or describe the group of captures it contains.

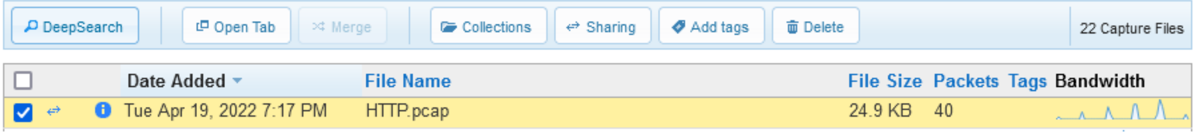
To create a new collection, start at the capture index and select the files to include. Click on the "Collections" button and choose to create a new collection or add those files to an existing one.

You don't have any Collections yet!

Please go back to the main capture index and choose capture files to add to a Collection.

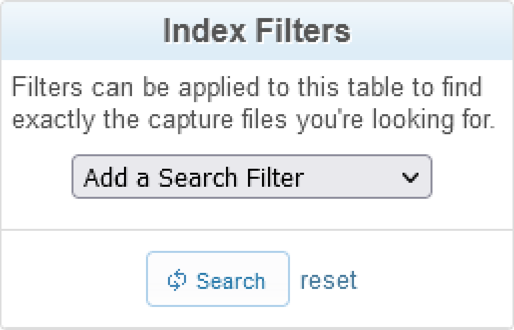


□	Date Added	File Name	Byte Rate	Packets	Encapsulation	Bandwidth
□	Today 12:22 AM	TCP Example.pcapng	49.2 KB/sec	2073	Ethernet	



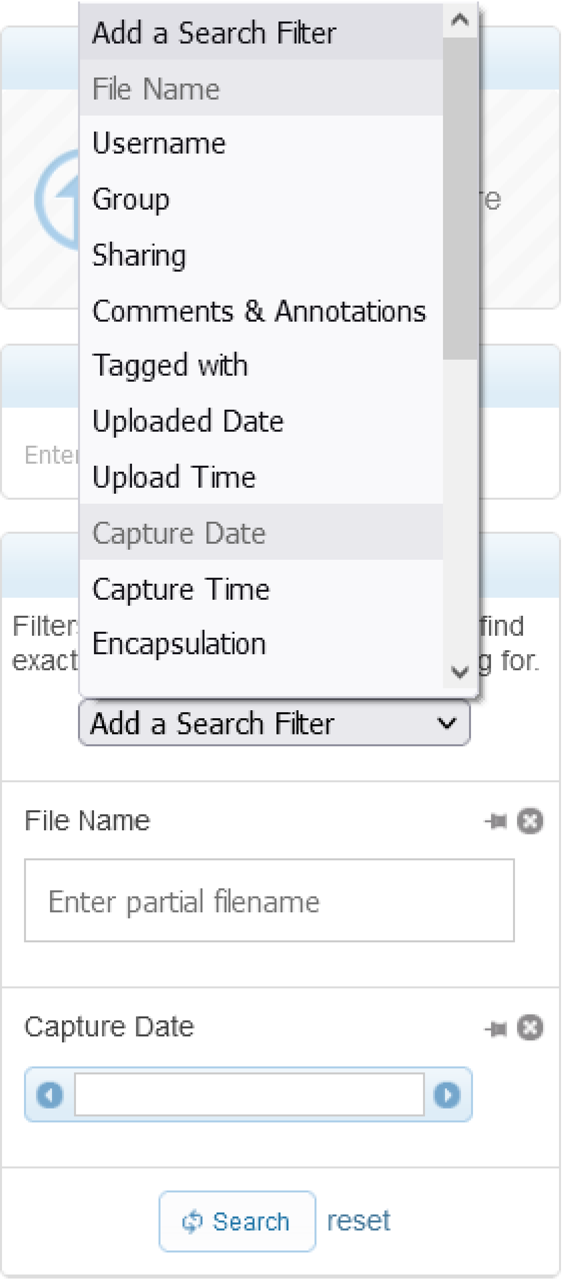
22 Capture Files

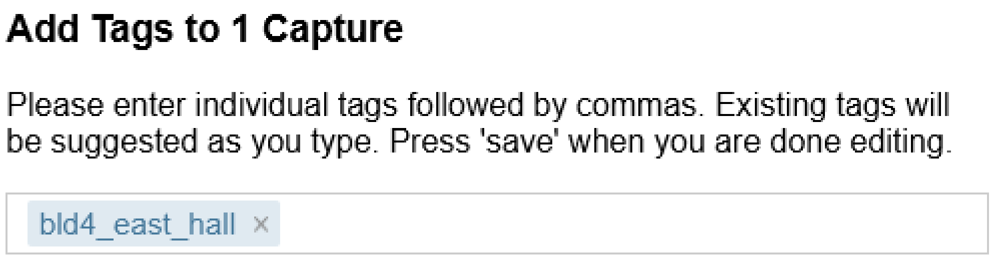
□		Date Added	File Name	File Size	Packets	Tags	Bandwidth
☑	⇄	Tue Apr 19, 2022 7:17 PM	HTTP.pcap	24.9 KB	40		



Index Filters

Filters can be applied to this table to find exactly the capture files you're looking for.

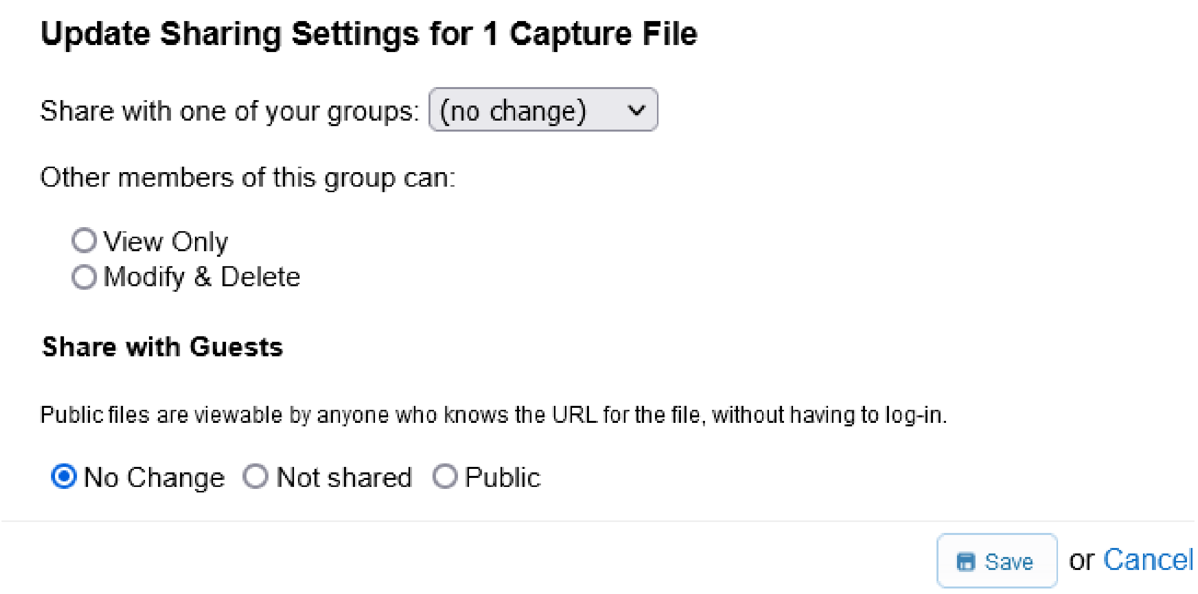




Add Tags to 1 Capture

Please enter individual tags followed by commas. Existing tags will be suggested as you type. Press 'save' when you are done editing.

bld4_east_hall ×



Update Sharing Settings for 1 Capture File

Share with one of your groups: (no change)

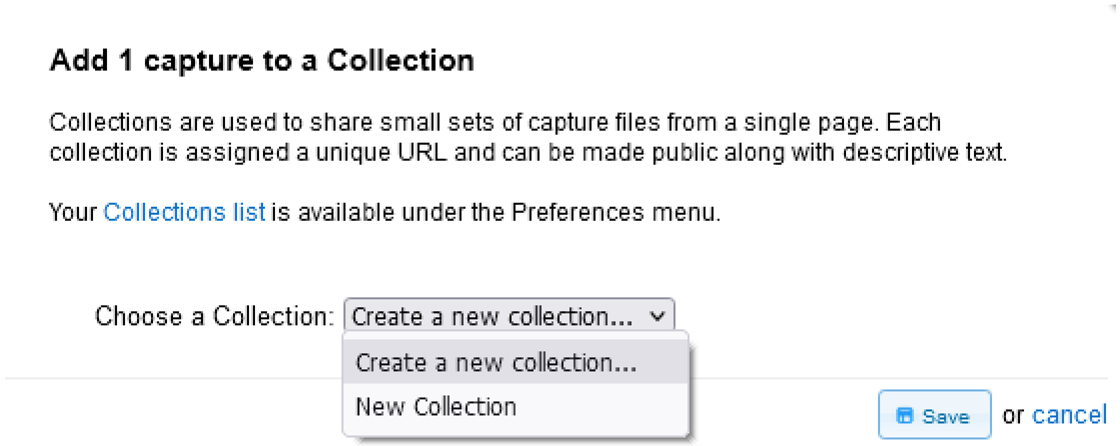
Other members of this group can:

○ View Only
○ Modify & Delete

Share with Guests

Public files are viewable by anyone who knows the URL for the file, without having to log-in.

● No Change ○ Not shared ○ Public

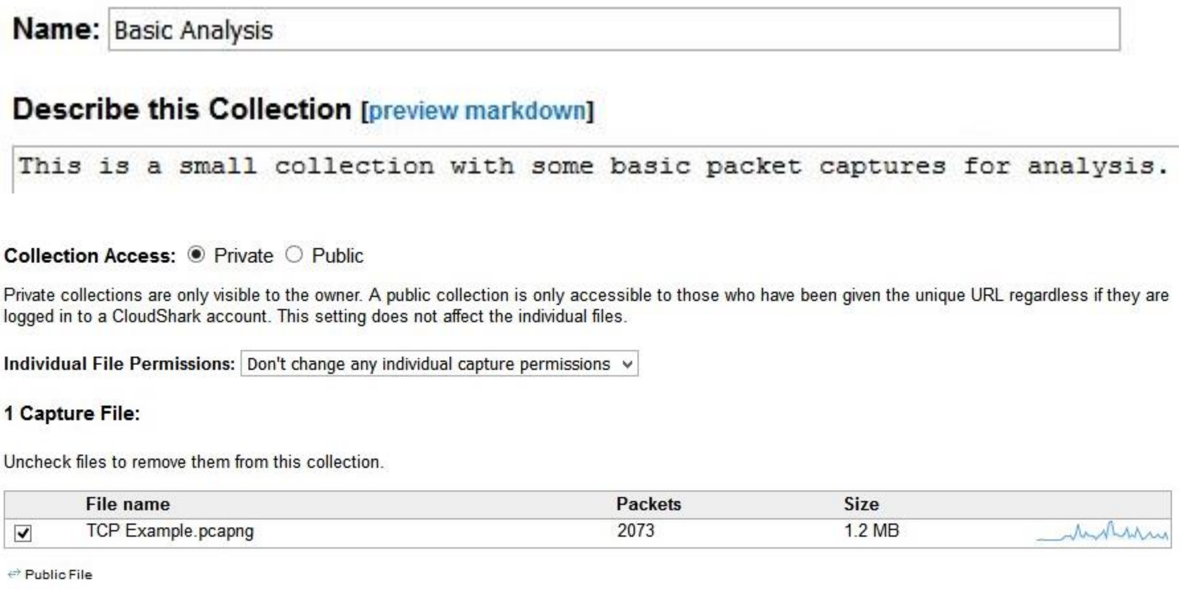


Add 1 capture to a Collection

Collections are used to share small sets of capture files from a single page. Each collection is assigned a unique URL and can be made public along with descriptive text.

Your Collections list is available under the Preferences menu.

Choose a Collection: Create a new collection...



Name: Basic Analysis

Describe this Collection [preview markdown]

```
This is a small collection with some basic packet captures for analysis.
```

Collection Access: ● Private ○ Public

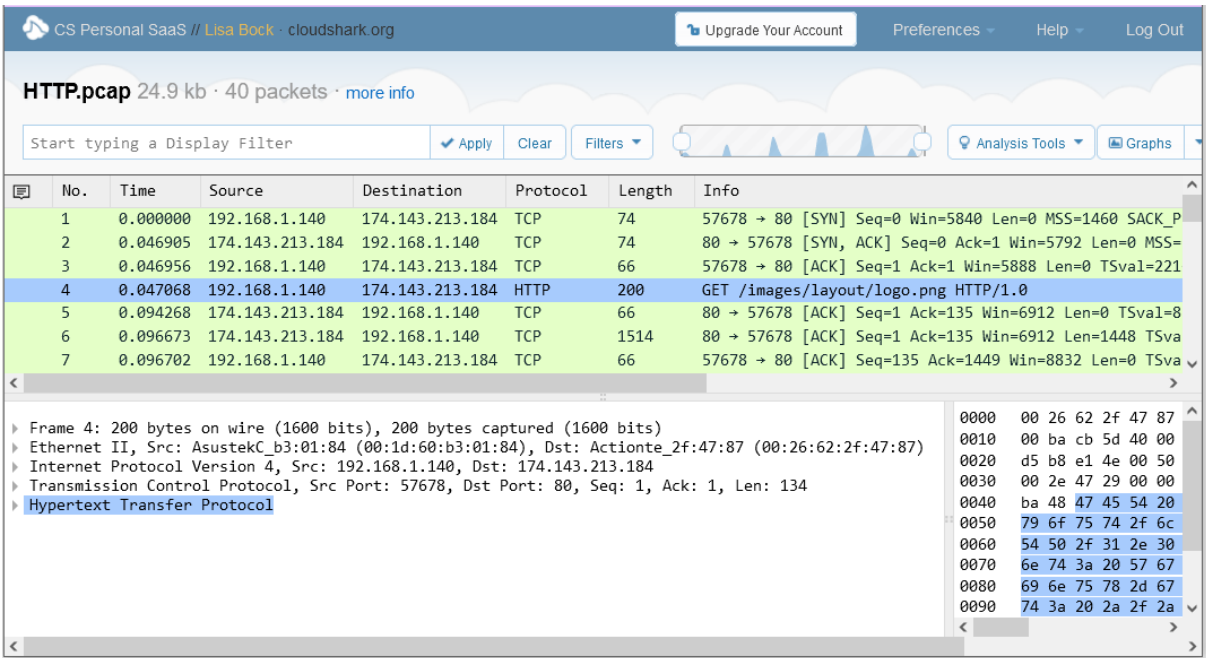
Private collections are only visible to the owner. A public collection is only accessible to those who have been given the unique URL regardless if they are logged in to a CloudShark account. This setting does not affect the individual files.

Individual File Permissions: Don't change any individual capture permissions

1 Capture File:

Uncheck files to remove them from this collection.

	File name	Packets	Size
☑	TCP Example.pcapng	2073	1.2 MB



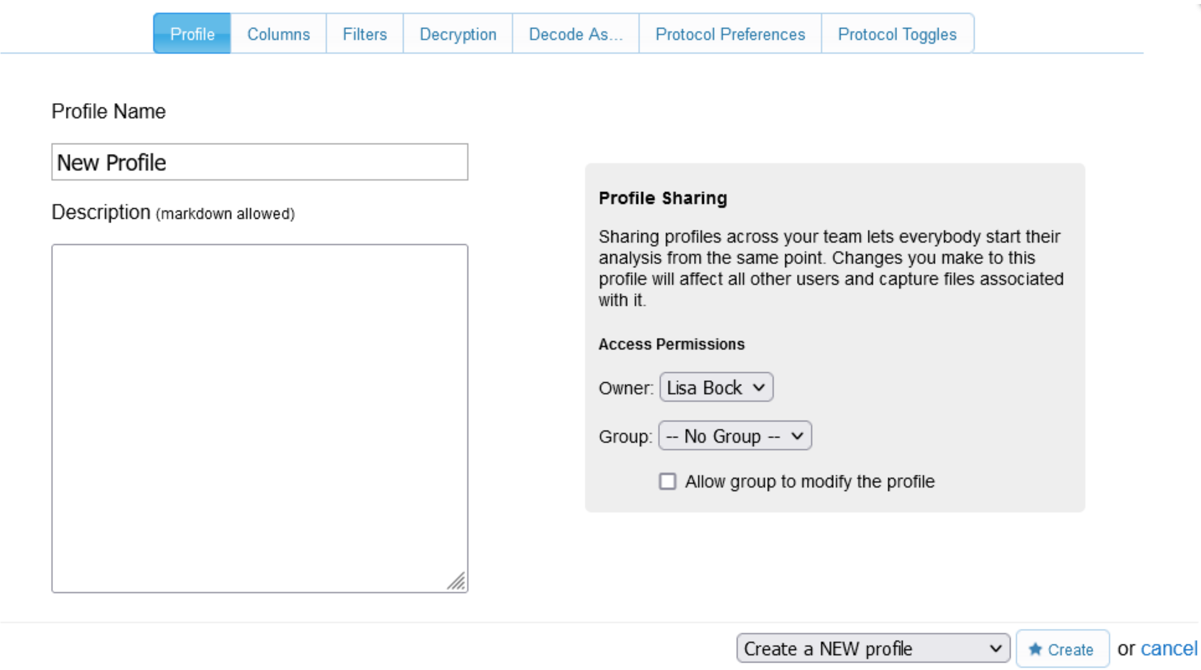
HTTP.pcap 24.9 kb · 40 packets · more info

Start typing a Display Filter

```
No.  Time      Source           Destination      Protocol  Length  Info
1    0.000000  192.168.1.140    174.143.213.184  TCP       74      57678 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_P
2    0.046905  174.143.213.184  192.168.1.140    TCP       74      80 → 57678 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=
3    0.046956  192.168.1.140    174.143.213.184  TCP       66      57678 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=221
4    0.047068  192.168.1.140    174.143.213.184  HTTP      200     GET /images/layout/logo.png HTTP/1.0
5    0.094268  174.143.213.184  192.168.1.140    TCP       66      80 → 57678 [ACK] Seq=1 Ack=135 Win=6912 Len=0 TSval=8
6    0.096673  174.143.213.184  192.168.1.140    TCP       1514    80 → 57678 [ACK] Seq=1 Ack=135 Win=6912 Len=1448 TSva
7    0.096702  192.168.1.140    174.143.213.184  TCP       66      57678 → 80 [ACK] Seq=135 Ack=1449 Win=8832 Len=0 TSva
```

```
Frame 4: 200 bytes on wire (1600 bits), 200 bytes captured (1600 bits)
Ethernet II, Src: AsustekC_b3:01:84 (00:1d:60:b3:01:84), Dst: Actionte_2f:47:87 (00:26:62:2f:47:87)
Internet Protocol Version 4, Src: 192.168.1.140, Dst: 174.143.213.184
Transmission Control Protocol, Src Port: 57678, Dst Port: 80, Seq: 1, Ack: 1, Len: 134
Hypertext Transfer Protocol
```

```
0000   00 26 62 2f 47 87
0010   00 ba cb 5d 40 00
0020   d5 b8 e1 4e 00 50
0030   00 2e 47 29 00 00
0040   ba 48 47 45 54 20
0050   79 6f 75 74 2f 6c
0060   54 50 2f 31 2e 30
0070   6e 74 3a 20 57 67
0080   69 6e 75 78 2d 67
0090   74 3a 20 2a 2f 2a
```



Profile Name

New Profile

Description (markdown allowed)

Profile Sharing

Sharing profiles across your team lets everybody start their analysis from the same point. Changes you make to this profile will affect all other users and capture files associated with it.

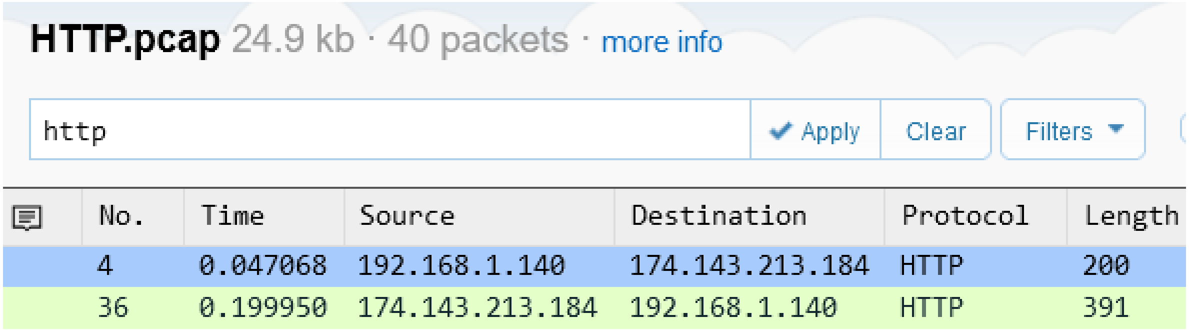
Access Permissions

Owner: Lisa Bock

Group: -- No Group --

□ Allow group to modify the profile

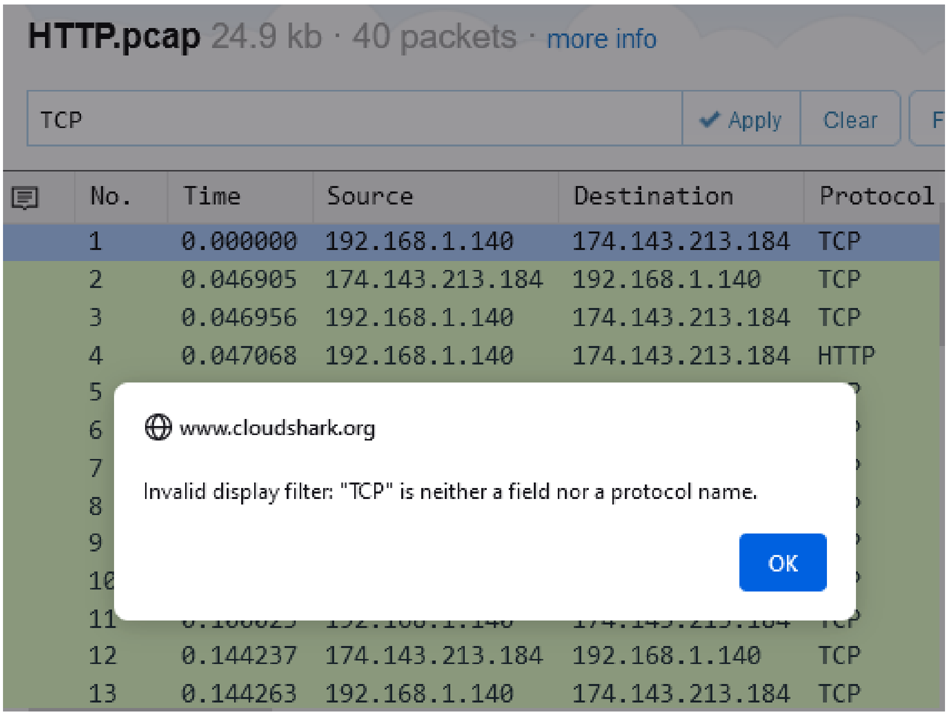
Create a NEW profile | ★ Create or cancel



HTTP.pcap 24.9 kb · 40 packets · more info

http

```
No.  Time      Source           Destination      Protocol  Length
4    0.047068  192.168.1.140    174.143.213.184  HTTP      200
36   0.199950  174.143.213.184  192.168.1.140    HTTP      391
```



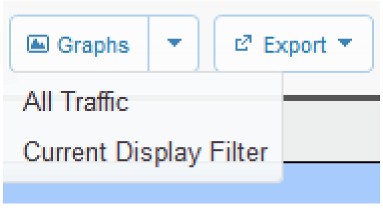
HTTP.pcap 24.9 kb · 40 packets · more info

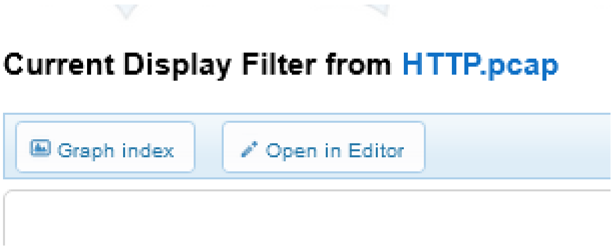
TCP

No.	Time	Source	Destination	Protocol
1	0.000000	192.168.1.140	174.143.213.184	TCP
2	0.046905	174.143.213.184	192.168.1.140	TCP
3	0.046956	192.168.1.140	174.143.213.184	TCP
4	0.047068	192.168.1.140	174.143.213.184	HTTP
5				
6				
7				
8				
9				
10				
11				
12	0.144237	174.143.213.184	192.168.1.140	TCP
13	0.144263	192.168.1.140	174.143.213.184	TCP

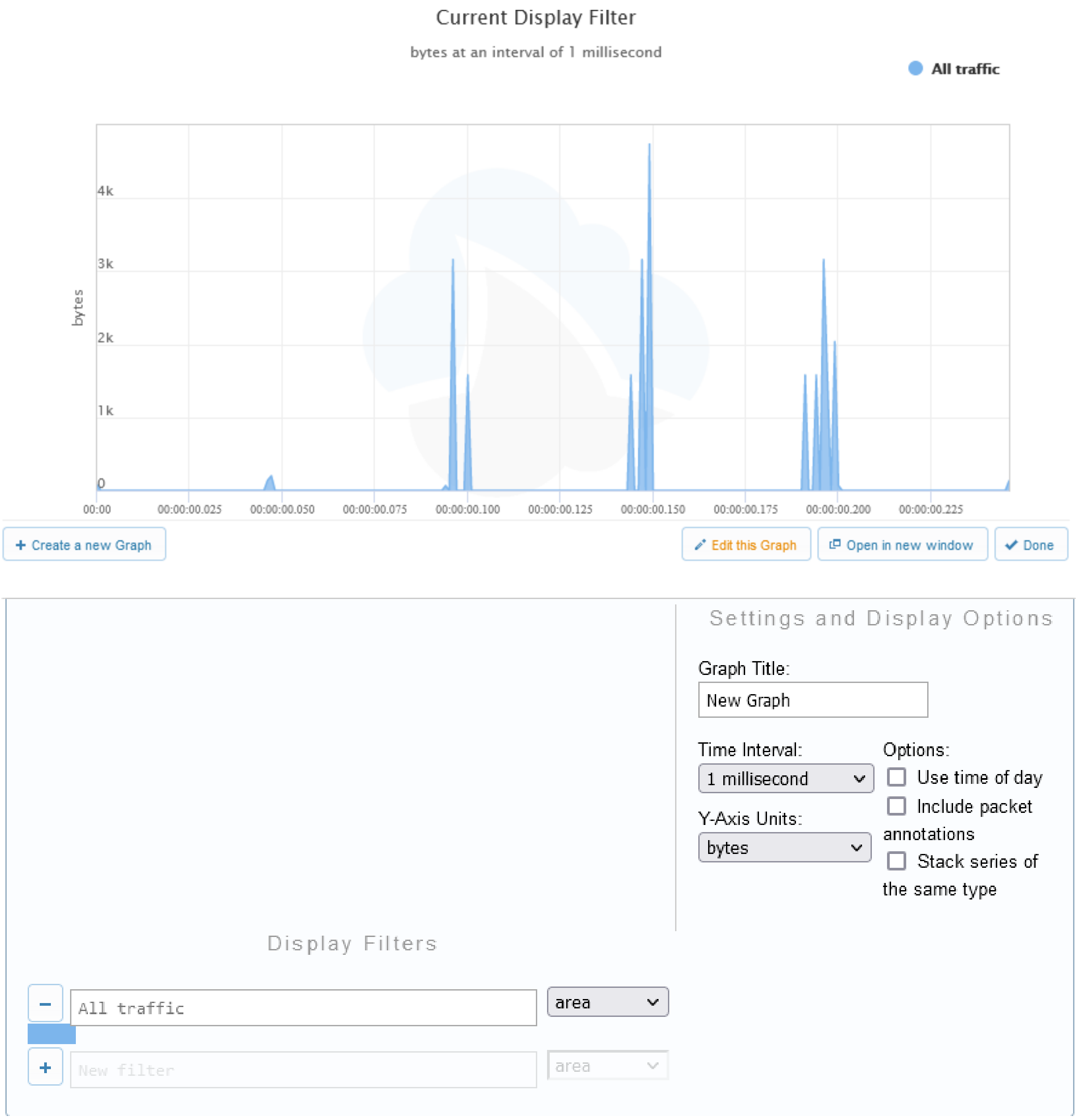
www.cloudshark.org

Invalid display filter: "TCP" is neither a field nor a protocol name.





Current Display Filter from HTTP.pcap



Graph Title: New Graph

Time Interval: 1 millisecond

Y-Axis Units: bytes

Options:

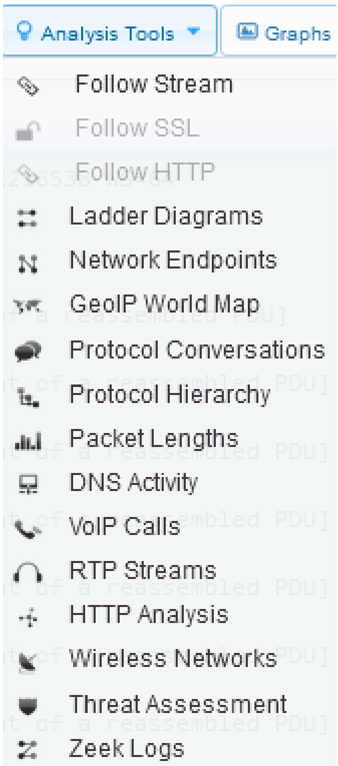
□ Use time of day

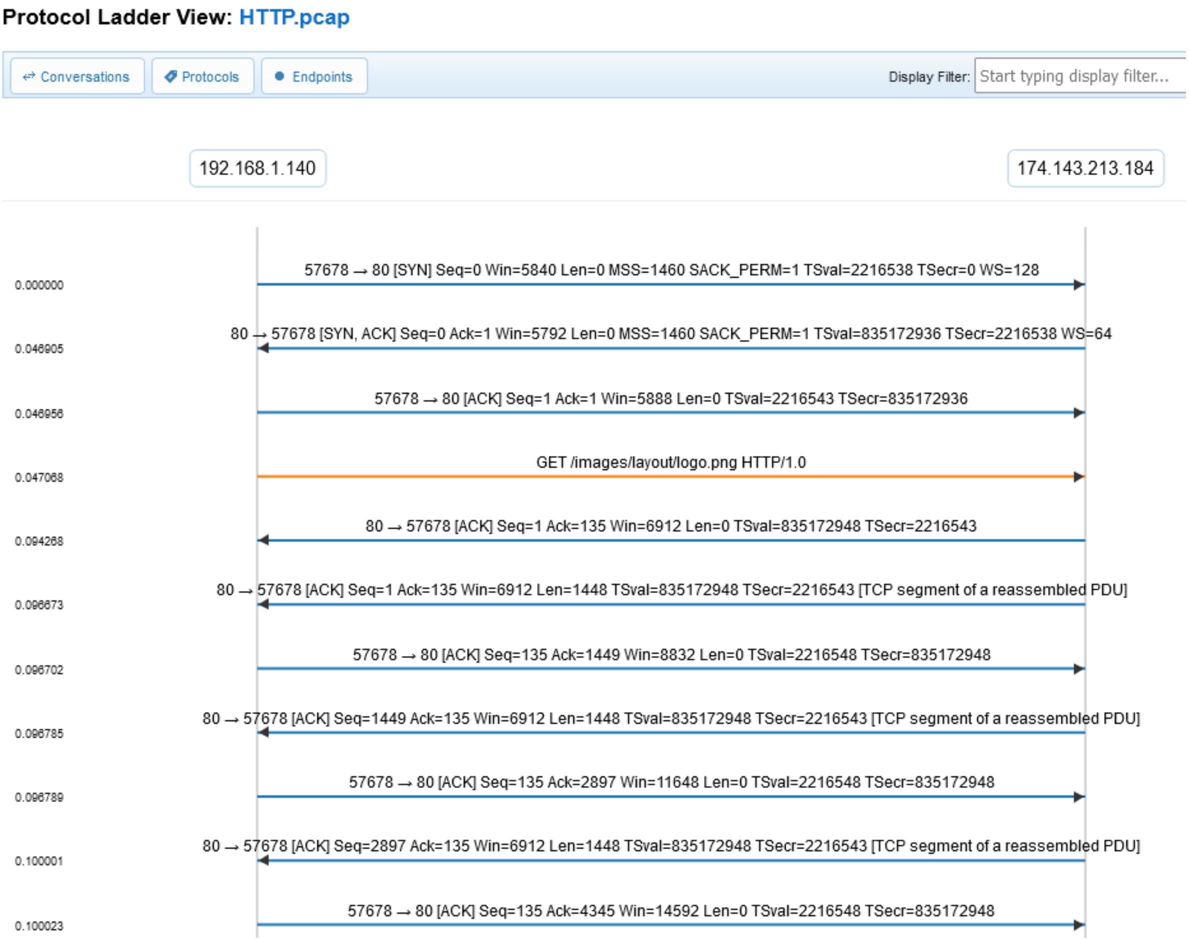
□ Include packet annotations

□ Stack series of the same type

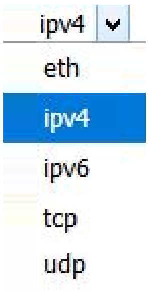
All traffic — area

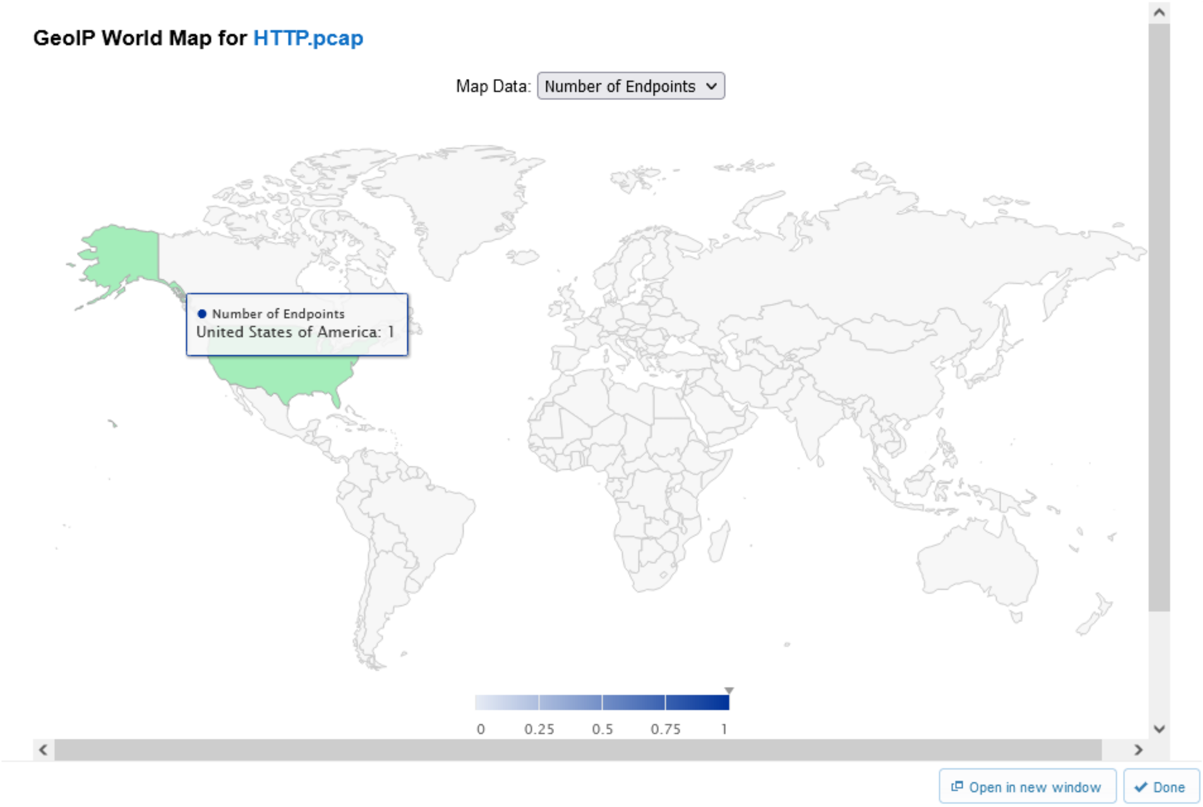
New filter — area




Protocol Ladder View: HTTP.pcap

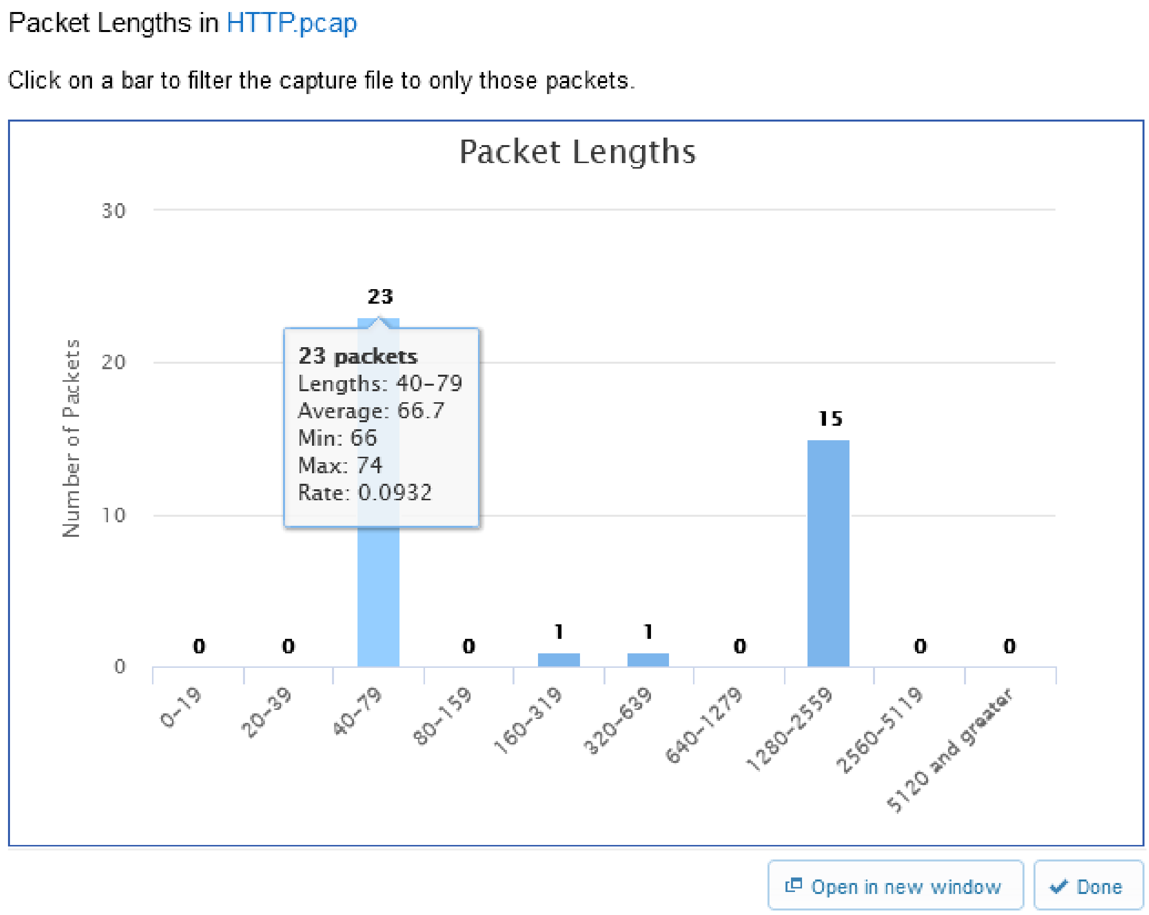
```
0.000000  57678 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=2216538 TSecr=0 WS=128
0.046905  80 → 57678 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=835172936 TSecr=2216538 WS=64
0.046956  57678 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=2216543 TSecr=835172936
0.047068  GET /images/layout/logo.png HTTP/1.0
0.094268  80 → 57678 [ACK] Seq=1 Ack=135 Win=6912 Len=0 TSval=835172948 TSecr=2216543
0.096673  80 → 57678 [ACK] Seq=1 Ack=135 Win=6912 Len=1448 TSval=835172948 TSecr=2216543 [TCP segment of a reassembled PDU]
0.096702  57678 → 80 [ACK] Seq=135 Ack=1449 Win=8832 Len=0 TSval=2216548 TSecr=835172948
0.096785  80 → 57678 [ACK] Seq=1449 Ack=135 Win=6912 Len=1448 TSval=835172948 TSecr=2216543 [TCP segment of a reassembled PDU]
0.096789  57678 → 80 [ACK] Seq=135 Ack=2897 Win=11648 Len=0 TSval=2216548 TSecr=835172948
0.100001  80 → 57678 [ACK] Seq=2897 Ack=135 Win=6912 Len=1448 TSval=835172948 TSecr=2216543 [TCP segment of a reassembled PDU]
0.100023  57678 → 80 [ACK] Seq=135 Ack=4345 Win=14592 Len=0 TSval=2216548 TSecr=835172948
```




GeoIP World Map for HTTP.pcap

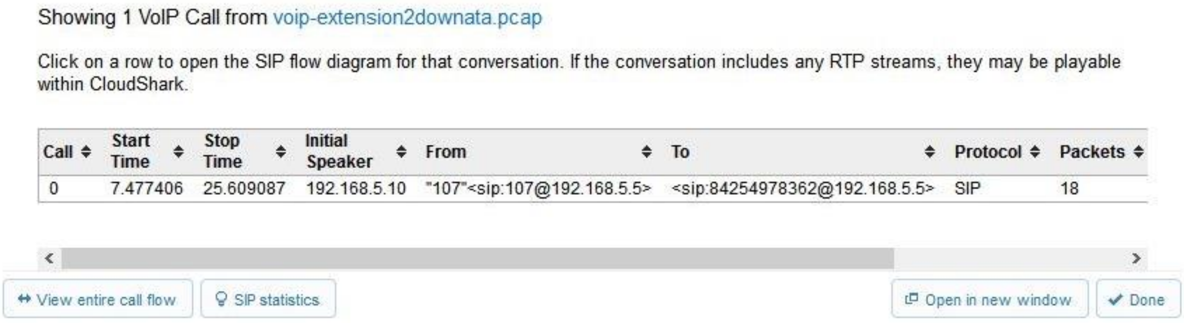
Map Data: Number of Endpoints

● Number of Endpoints
United States of America: 1



Packet Lengths in HTTP.pcap

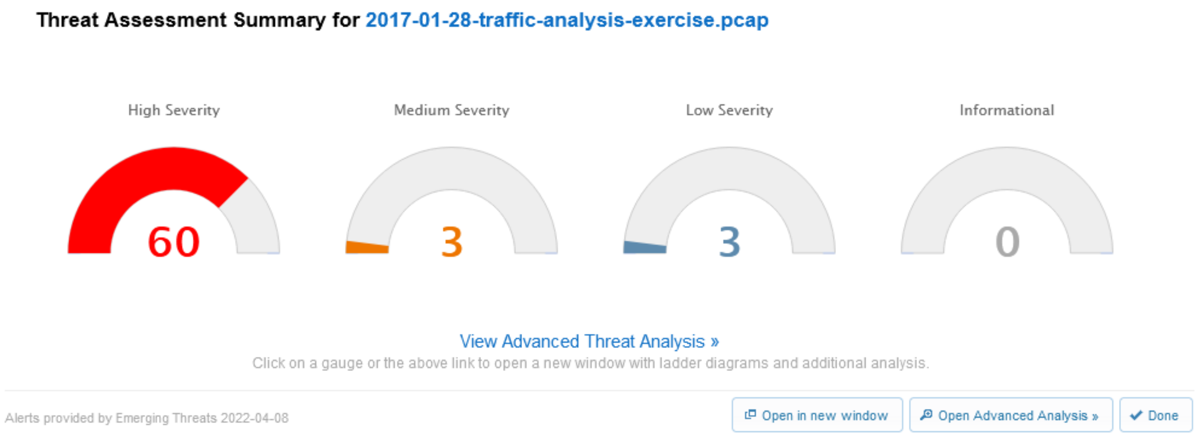
Click on a bar to filter the capture file to only those packets.



Showing 1 VoIP Call from voip-extension2downata.pcap

Click on a row to open the SIP flow diagram for that conversation. If the conversation includes any RTP streams, they may be playable within CloudShark.

Call	Start Time	Stop Time	Initial Speaker	From	To	Protocol	Packets
0	7.477406	25.609087	192.168.5.10	"107"<sip:107@192.168.5.5>	<sip:84254978362@192.168.5.5>	SIP	18

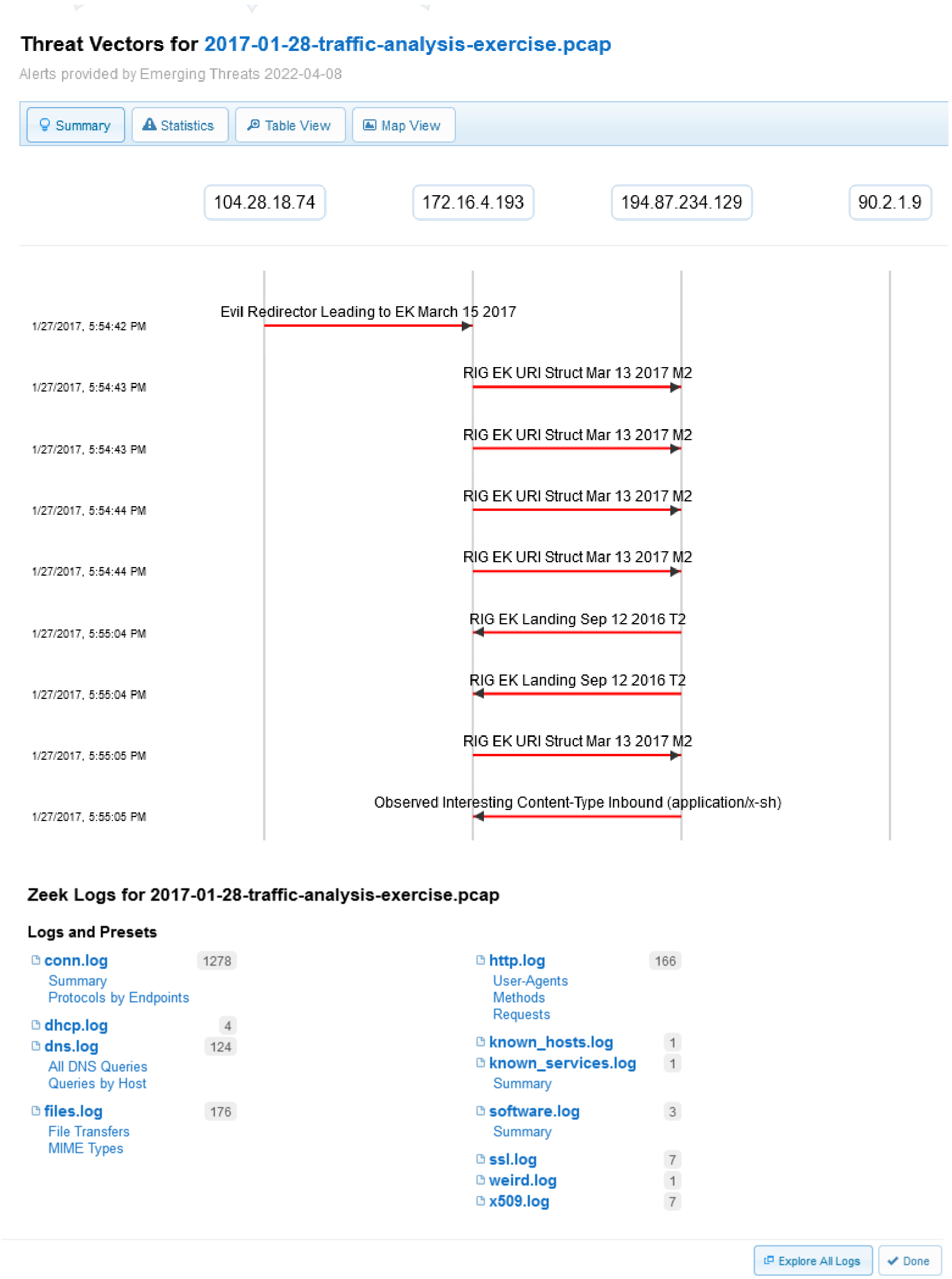


Threat Assessment Summary for 2017-01-28-traffic-analysis-exercise.pcap

View Advanced Threat Analysis »

Click on a gauge or the above link to open a new window with ladder diagrams and additional analysis.

Alerts provided by Emerging Threats 2022-04-08



Threat Vectors for 2017-01-28-traffic-analysis-exercise.pcap

Alerts provided by Emerging Threats 2022-04-08

1/27/2017, 5:54:42 PM Evil Redirector Leading to EK March 15 2017

1/27/2017, 5:54:43 PM RIG EK URI Struct Mar 13 2017 M2

1/27/2017, 5:54:43 PM RIG EK URI Struct Mar 13 2017 M2

1/27/2017, 5:54:44 PM RIG EK URI Struct Mar 13 2017 M2

1/27/2017, 5:54:44 PM RIG EK URI Struct Mar 13 2017 M2

1/27/2017, 5:55:04 PM RIG EK Landing Sep 12 2016 T2

1/27/2017, 5:55:04 PM RIG EK Landing Sep 12 2016 T2

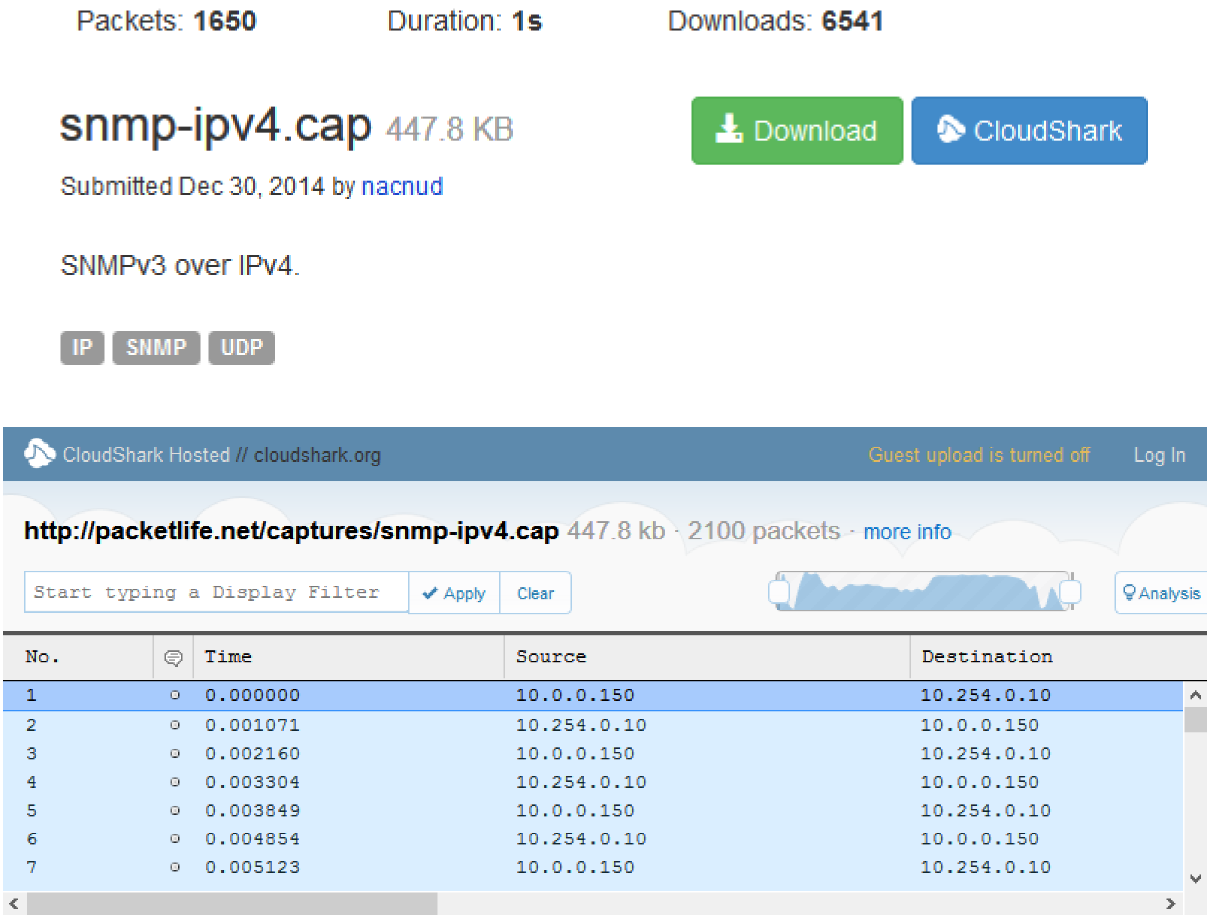
1/27/2017, 5:55:05 PM RIG EK URI Struct Mar 13 2017 M2

1/27/2017, 5:55:05 PM Observed Interesting Content-Type Inbound (application/x-sh)

Zeek Logs for 2017-01-28-traffic-analysis-exercise.pcap

Logs and Presets

conn.log	1278	Summary Protocols by Endpoints
dhcp.log	4	
dns.log	124	All DNS Queries Queries by Host
files.log	176	File Transfers MIME Types
http.log	166	User-Agents Methods Requests
known_hosts.log	1	
known_services.log	1	Summary
software.log	3	Summary
ssl.log	7	
weird.log	1	
x509.log	7	



Packets: **1650** Duration: **1s** Downloads: **6541**

snmp-ipv4.cap 447.8 KB

Submitted Dec 30, 2014 by nacnud

SNMPv3 over IPv4.

IP
SNMP
UDP
CloudShark Hosted // cloudshark.org
Guest upload is turned off
Log In

http://packetlife.net/captures/snmp-ipv4.cap 447.8 kb · 2100 packets · more info

Start typing a Display Filter
✓ Apply
Clear
Analysis

No.		Time	Source	Destination
1	○	0.000000	10.0.0.150	10.254.0.10
2	○	0.001071	10.254.0.10	10.0.0.150
3	○	0.002160	10.0.0.150	10.254.0.10
4	○	0.003304	10.254.0.10	10.0.0.150
5	○	0.003849	10.0.0.150	10.254.0.10
6	○	0.004854	10.254.0.10	10.0.0.150
7	○	0.005123	10.0.0.150	10.254.0.10