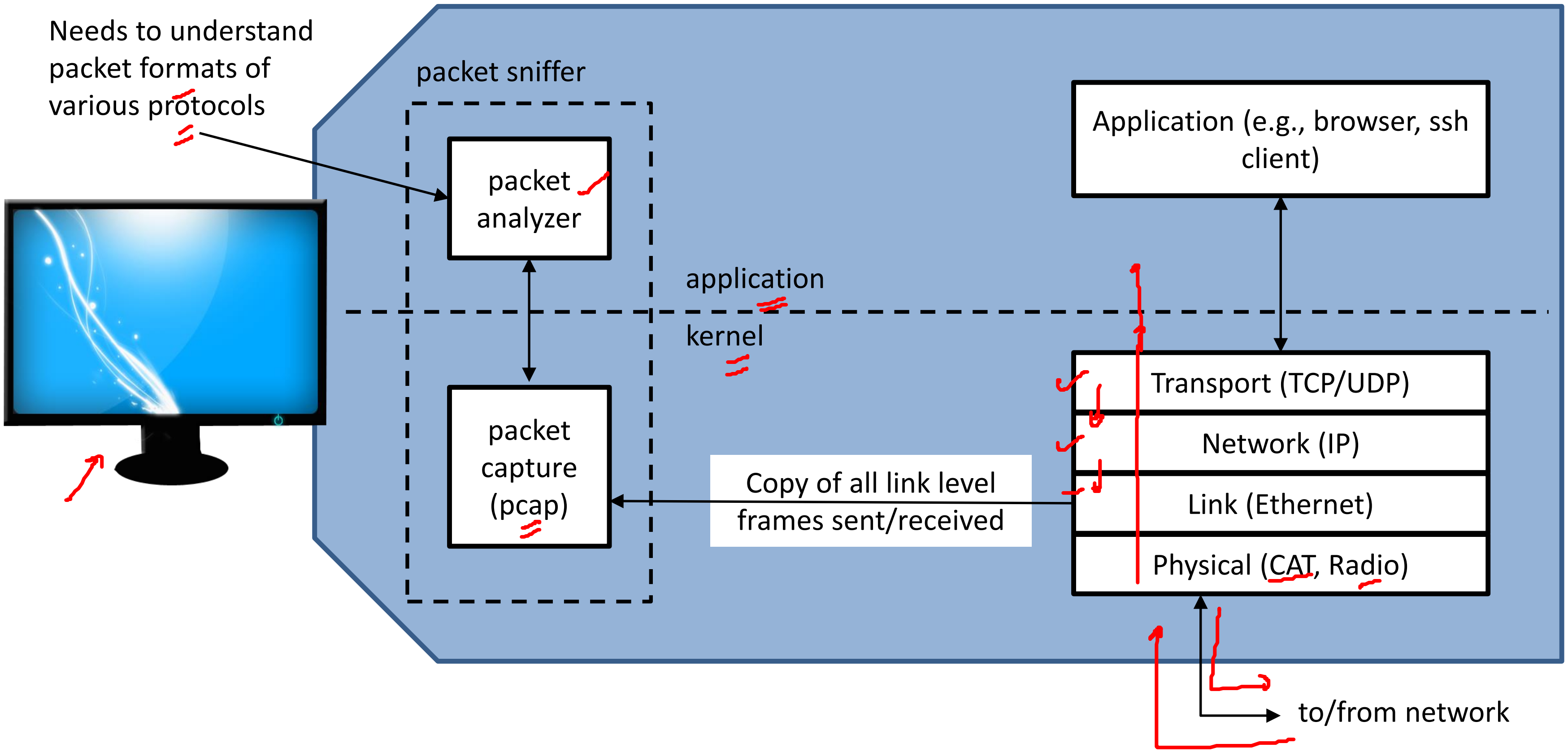
Packet Sniffers (Computer Networks Lab)

Kameswari Chebrolu

Packet Sniffer

- Tool that sniffs packets sent/received on a network interface
  - Stores and displays the contents of the captured packets
  - Passive Tool (does not generate any traffic)

Architecture



Focus

- Wireshark (main focus)
- Tcpdump (brief)

Wireshark

- A free, open source network packet sniffer
  - Works on Linux, Windows, Macintosh
- Very popular and extensively used
  - Administrators to troubleshoot problems
  - Developers to debug protocol implementations
  - Students to learn network protocol internals

Useful Features

- Live capture on a network interface
- Can analyze packets captured using other tools like tcpdump/windump etc
- Provides very detailed protocol information
- Filter/Search packets based on many criteria
- Export captured packets in different file formats
- Generate various statistics

Outline

- Installation
- Traffic Generation
- Running Wireshark
- Features
  - GUI overview
  - Filters
  - Manipulating time
  - Statistics
  - Save/Open packet capture

Install Wireshark (Windows)

- Follow instructions at https://en.wikiversity.org/wiki/Wireshark/Install

Install Wireshark (Linux)

- Often comes pre-installed
- Else, see instructions at https://linuxtechlab.com/install-wireshark-linux-centosubuntu/

“root”

  - ‘Permission Denied’ error as local user?
    - Start Wireshark as root or with sudo privileges
    - Or add local user to Wireshark group via

“sudo usermod -a -G wireshark username”

(Be sure to replace username with appropriate name)

Traffic Generation

- Wget or Web browser (http and https)
  - wget www.iitb.ac.in

remote

- Ping (is the machine up or down) reply
  - ping www.iitb.ac.in hostname IP LAN
- SSH (secure shell)
  - ssh chebrolu@10.129.2.154

Note the arguments to the commands have to be carefully chosen

Run Wireshark

wireshark
generate
traffic

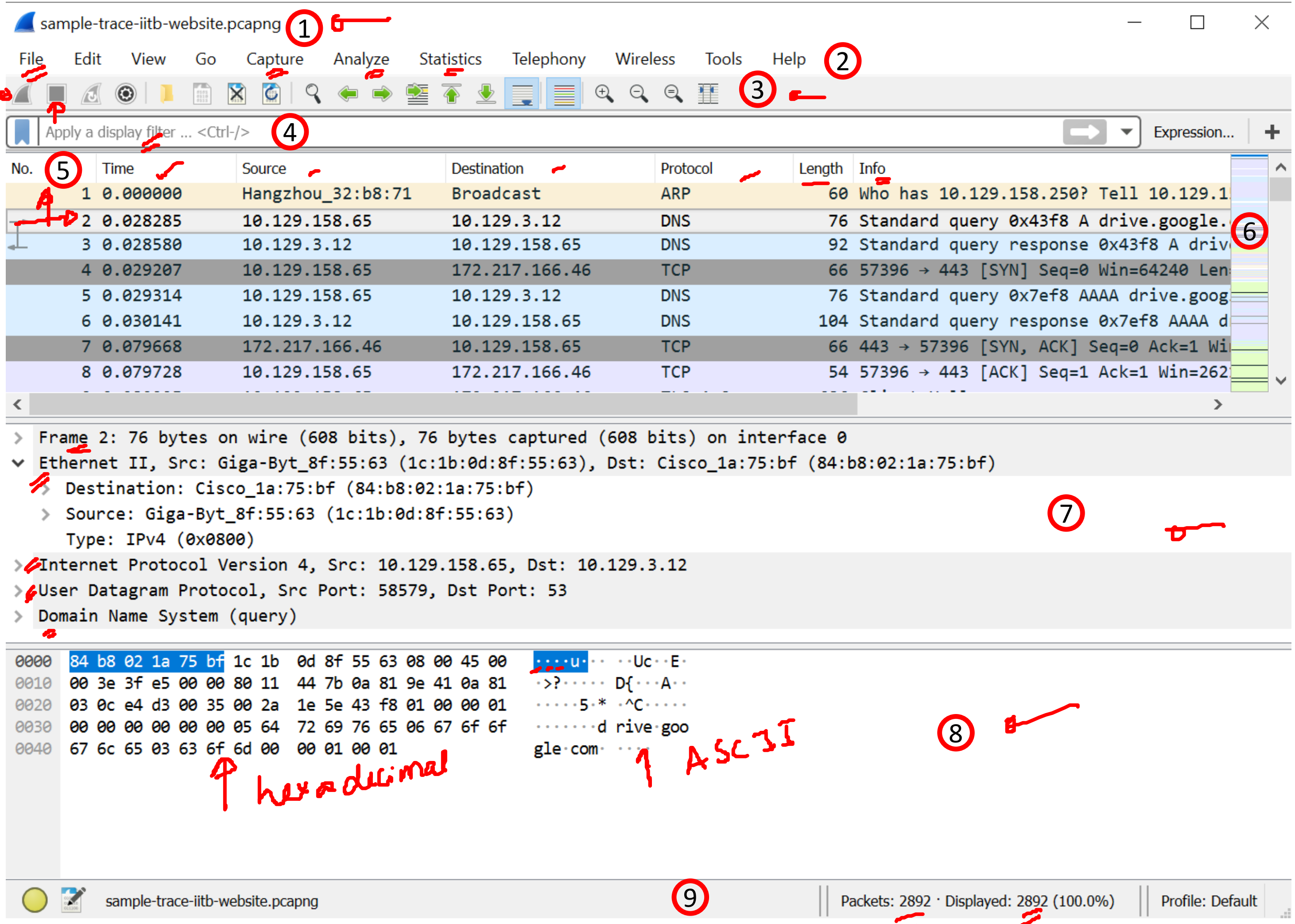
Lo

- Open a browser (don’t type in any URL)
- Start up Wireshark (click on its icon)

network

- Select interface via “capture” option in the command menu; Click Start
- While Wireshark is running, enter a URL in browser and let page display
- Stop capture (red button in the main tool bar)

GUI Overview



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Hangzhou_32:b8:71	Broadcast	ARP	60	Who has 10.129.158.250? Tell 10.129.1
2	0.028285	10.129.158.65	10.129.3.12	DNS	76	Standard query 0x43f8 A drive.google.
3	0.028580	10.129.3.12	10.129.158.65	DNS	92	Standard query response 0x43f8 A driv
4	0.029207	10.129.158.65	172.217.166.46	TCP	66	57396 → 443 [SYN] Seq=0 Win=64240 Len
5	0.029314	10.129.158.65	10.129.3.12	DNS	76	Standard query 0x7ef8 AAAA drive.goog
6	0.030141	10.129.3.12	10.129.158.65	DNS	104	Standard query response 0x7ef8 AAAA d
7	0.079668	172.217.166.46	10.129.158.65	TCP	66	443 → 57396 [SYN, ACK] Seq=0 Ack=1 Wi
8	0.079728	10.129.158.65	172.217.166.46	TCP	54	57396 → 443 [ACK] Seq=1 Ack=1 Win=262

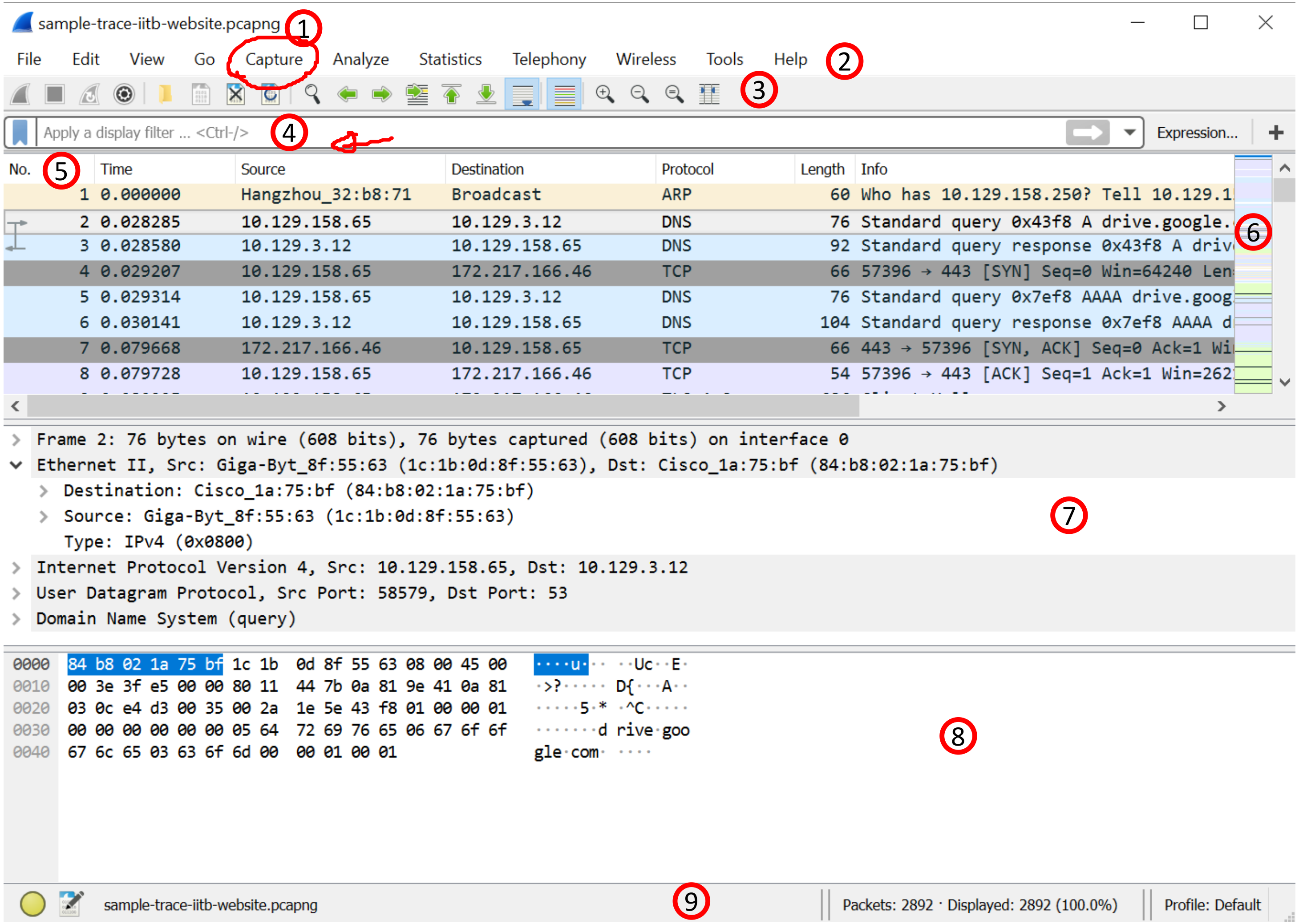
```
> Frame 2: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface 0
v Ethernet II, Src: Giga-Byt_8f:55:63 (1c:1b:0d:8f:55:63), Dst: Cisco_1a:75:bf (84:b8:02:1a:75:bf)
    > Destination: Cisco_1a:75:bf (84:b8:02:1a:75:bf)
    > Source: Giga-Byt_8f:55:63 (1c:1b:0d:8f:55:63)
      Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 10.129.158.65, Dst: 10.129.3.12
> User Datagram Protocol, Src Port: 58579, Dst Port: 53
> Domain Name System (query)
```

```
0000  84 b8 02 1a 75 bf 1c 1b  0d 8f 55 63 08 00 45 00   ····u··· ··Uc··E·
0010  00 3e 3f e5 00 00 80 11  44 7b 0a 81 9e 41 0a 81   ·>?····· D{···A··
0020  03 0c e4 d3 00 35 00 2a  1e 5e 43 f8 01 00 00 01   ·····5·* ·^C·····
0030  00 00 00 00 00 00 05 64  72 69 76 65 06 67 6f 6f   ·······d rive·goo
0040  67 6c 65 03 63 6f 6d 00  00 01 00 01               gle·com· ····
```

sample-trace-iitb-website.pcapng | Packets: 2892 · Displayed: 2892 (100.0%) | Profile: Default

1. Title Bar
2. Menu Bar
3. Main Toolbar
4. Filter Toolbar
5. Packet List
6. Intelligent Scrollbar
7. Packet Details
8. Packet Bytes
9. Status Bar

GUI Overview



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Hangzhou_32:b8:71	Broadcast	ARP	60	Who has 10.129.158.250? Tell 10.129.1
2	0.028285	10.129.158.65	10.129.3.12	DNS	76	Standard query 0x43f8 A drive.google.
3	0.028580	10.129.3.12	10.129.158.65	DNS	92	Standard query response 0x43f8 A driv
4	0.029207	10.129.158.65	172.217.166.46	TCP	66	57396 → 443 [SYN] Seq=0 Win=64240 Len
5	0.029314	10.129.158.65	10.129.3.12	DNS	76	Standard query 0x7ef8 AAAA drive.goog
6	0.030141	10.129.3.12	10.129.158.65	DNS	104	Standard query response 0x7ef8 AAAA d
7	0.079668	172.217.166.46	10.129.158.65	TCP	66	443 → 57396 [SYN, ACK] Seq=0 Ack=1 Wi
8	0.079728	10.129.158.65	172.217.166.46	TCP	54	57396 → 443 [ACK] Seq=1 Ack=1 Win=262

```
> Frame 2: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface 0
v Ethernet II, Src: Giga-Byt_8f:55:63 (1c:1b:0d:8f:55:63), Dst: Cisco_1a:75:bf (84:b8:02:1a:75:bf)
  > Destination: Cisco_1a:75:bf (84:b8:02:1a:75:bf)
  > Source: Giga-Byt_8f:55:63 (1c:1b:0d:8f:55:63)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 10.129.158.65, Dst: 10.129.3.12
> User Datagram Protocol, Src Port: 58579, Dst Port: 53
> Domain Name System (query)
```

```
0000  84 b8 02 1a 75 bf 1c 1b  0d 8f 55 63 08 00 45 00   ····u·· ··Uc··E·
0010  00 3e 3f e5 00 00 80 11  44 7b 0a 81 9e 41 0a 81   ·>?····· D{···A··
0020  03 0c e4 d3 00 35 00 2a  1e 5e 43 f8 01 00 00 01   ·····5·* ·^C·····
0030  00 00 00 00 00 00 05 64  72 69 76 65 06 67 6f 6f   ·······d rive·goo
0040  67 6c 65 03 63 6f 6d 00  00 01 00 01               gle·com· ····
```

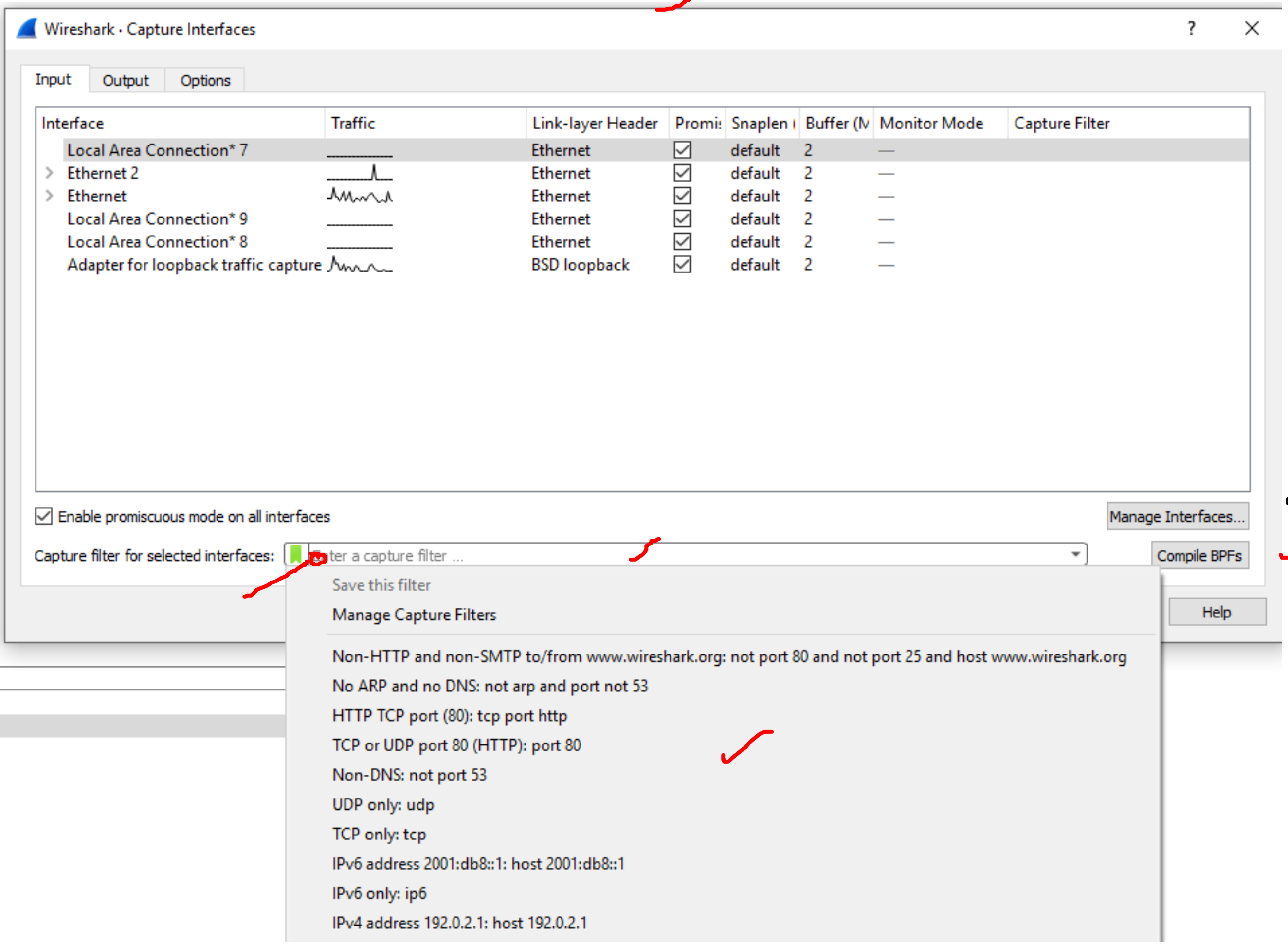
sample-trace-iitb-website.pcapng | Packets: 2892 · Displayed: 2892 (100.0%) | Profile: Default

1. Title Bar
2. Menu Bar
3. Main Toolbar
4. Filter Toolbar
5. Packet List
6. Intelligent Scrollbar
7. Packet Details
8. Packet Bytes
9. Status Bar

Wireshark Filters

- Two types of filters
  - Capture Filters: what to capture?
    - Language based on tcpdump
    - Capture → options (from the Menu bar)
  - Display Filters: what to display?
    - C type instructions or English like terms
    - Filter tool bar

Capture Filters



Interface	Traffic	Link-layer Header	Promi:	Snaplen (	Buffer (M	Monitor Mode	Capture Filter
Local Area Connection* 7		Ethernet	☑	default	2	—	
Ethernet 2		Ethernet	☑	default	2	—	
Ethernet		Ethernet	☑	default	2	—	
Local Area Connection* 9		Ethernet	☑	default	2	—	
Local Area Connection* 8		Ethernet	☑	default	2	—	
Adapter for loopback traffic capture		BSD loopback	☑	default	2	—	

☑ Enable promiscuous mode on all interfaces

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

Non-HTTP and non-SMTP to/from www.wireshark.org: not port 80 and not port 25 and host www.wireshark.org

No ARP and no DNS: not arp and port not 53

HTTP TCP port (80): tcp port http

TCP or UDP port 80 (HTTP): port 80

Non-DNS: not port 53

UDP only: udp

TCP only: tcp

IPv6 address 2001:db8::1: host 2001:db8::1

IPv6 only: ip6

IPv4 address 192.0.2.1: host 192.0.2.1

Examples:

host 10.129.1.24

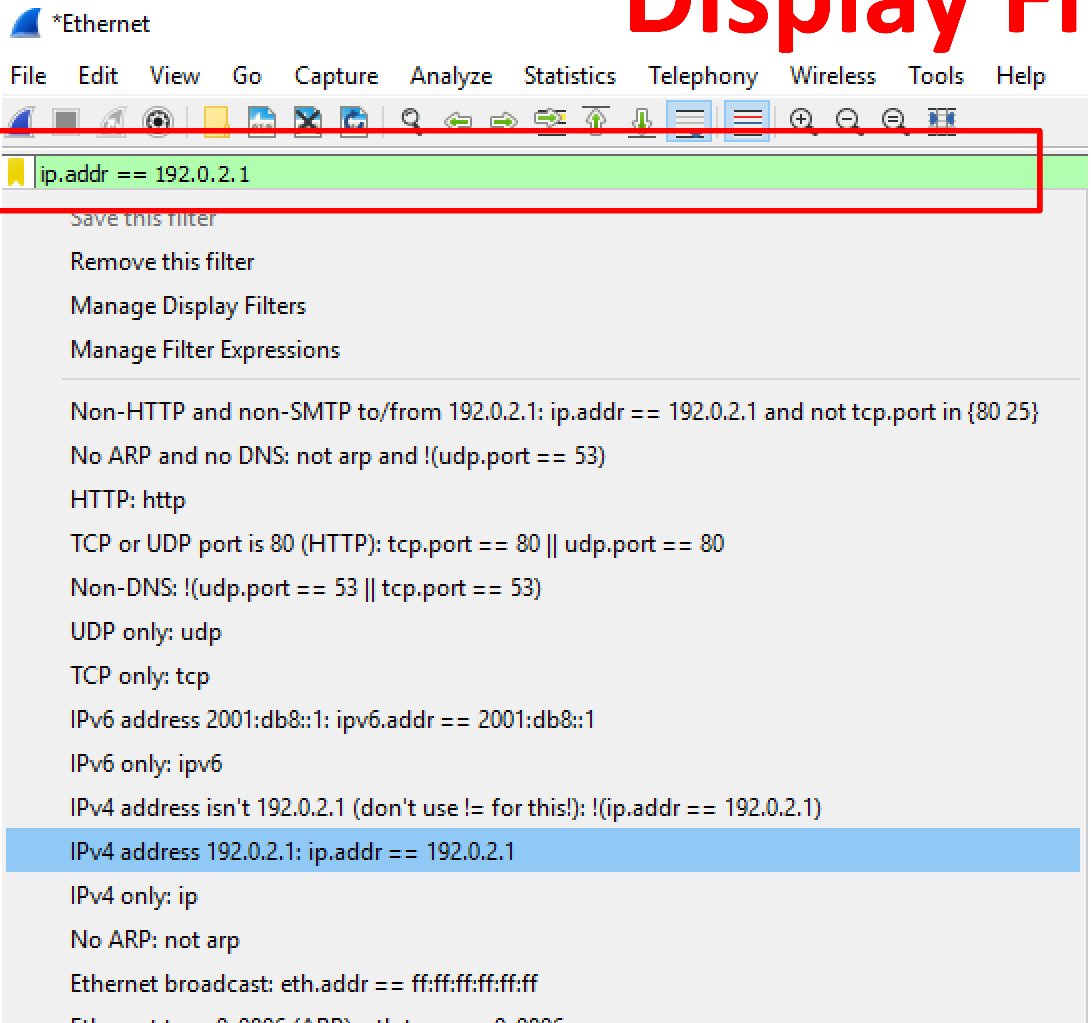
src
dst

tcp port http

src
dst
80

udp

Display Filters


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

ip.addr == 192.0.2.1

Save this filter
Remove this filter
Manage Display Filters
Manage Filter Expressions

Non-HTTP and non-SMTP to/from 192.0.2.1: ip.addr == 192.0.2.1 and not tcp.port in {80 25}
No ARP and no DNS: not arp and !(udp.port == 53)
HTTP: http
TCP or UDP port is 80 (HTTP): tcp.port == 80 || udp.port == 80
Non-DNS: !(udp.port == 53 || tcp.port == 53)
UDP only: udp
TCP only: tcp
IPv6 address 2001:db8::1: ipv6.addr == 2001:db8::1
IPv6 only: ipv6
IPv4 address isn't 192.0.2.1 (don't use != for this!): !(ip.addr == 192.0.2.1)
IPv4 address 192.0.2.1: ip.addr == 192.0.2.1
IPv4 only: ip
No ARP: not arp
Ethernet broadcast: eth.addr == ff:ff:ff:ff:ff:ff
Ethernet type 0x0806 (ARP): eth.type == 0x0806

subnet

4 bytes
3 bytes
10.1.12.*

ip.src==10.1.12.0/24

ip.addr==192.12.1.1 &&
ip.addr==192.12.1.2

src
dst

!(ip.addr==192.12.1.1 &&
ip.addr==192.12.1.2)

tcp.dstport == 80

tcp.port==80 || tcp.port==443

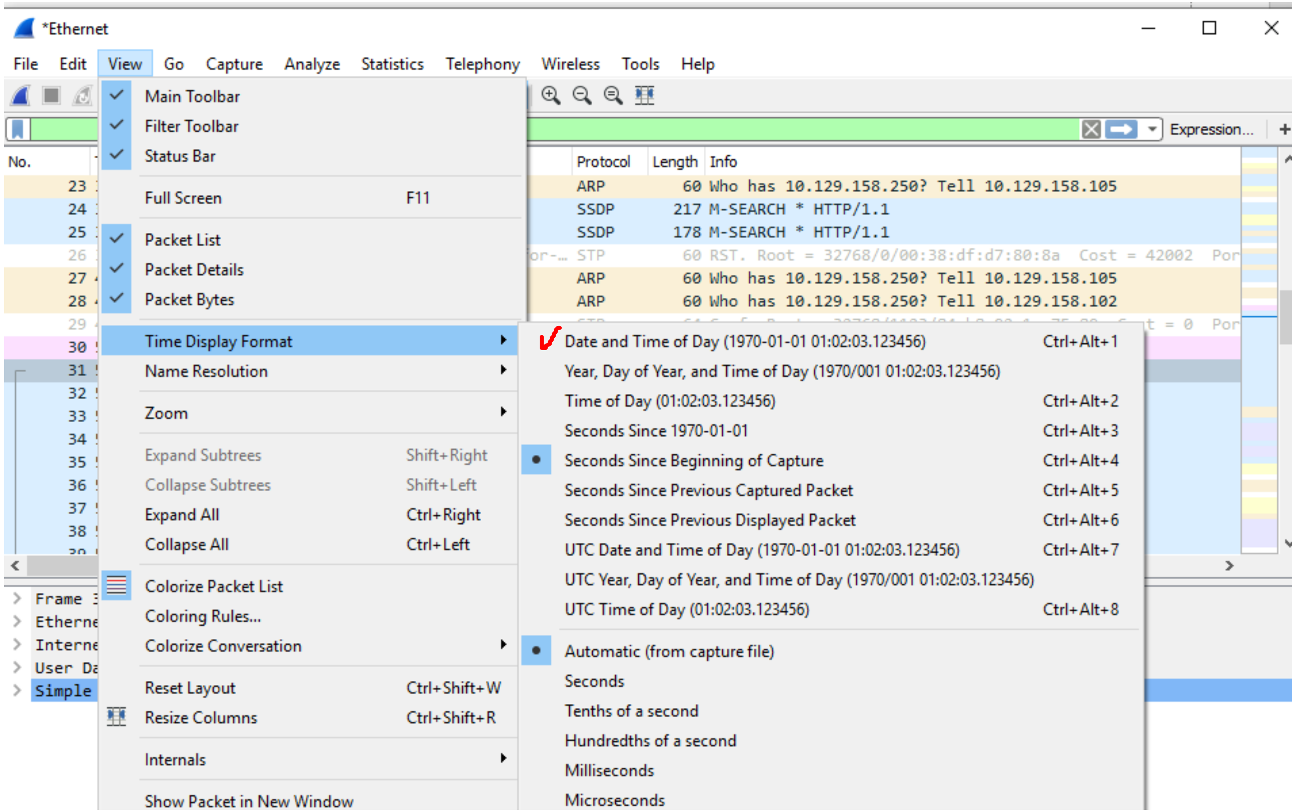
http

arp

Time

①→ 0

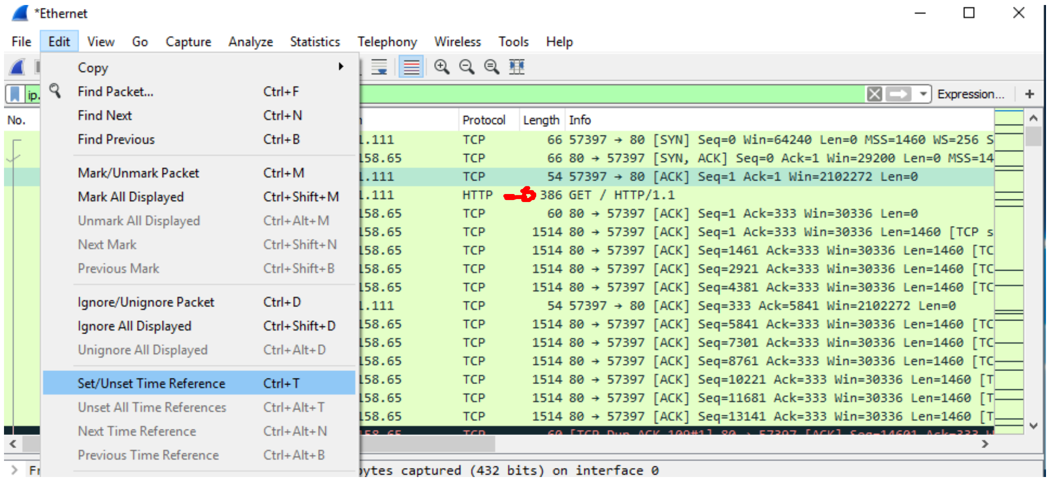
- View → Time Display


*Ethernet
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Wireless
Tools
Help
Expression...
✓ Main Toolbar
✓ Filter Toolbar
✓ Status Bar
Full Screen F11
✓ Packet List
✓ Packet Details
✓ Packet Bytes
Time Display Format
Name Resolution
Zoom
Expand Subtrees Shift+Right
Collapse Subtrees Shift+Left
Expand All Ctrl+Right
Collapse All Ctrl+Left
Colorize Packet List
Coloring Rules...
Colorize Conversation
Reset Layout Ctrl+Shift+W
Resize Columns Ctrl+Shift+R
Internals
Show Packet in New Window
✓ Date and Time of Day (1970-01-01 01:02:03.123456) Ctrl+Alt+1
Year, Day of Year, and Time of Day (1970/001 01:02:03.123456)
Time of Day (01:02:03.123456) Ctrl+Alt+2
Seconds Since 1970-01-01 Ctrl+Alt+3
● Seconds Since Beginning of Capture Ctrl+Alt+4
Seconds Since Previous Captured Packet Ctrl+Alt+5
Seconds Since Previous Displayed Packet Ctrl+Alt+6
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
● Automatic (from capture file)
Seconds
Tenths of a second
Hundredths of a second
Milliseconds
Microseconds
Frame
Etherne
Interne
User Da
Simple

```
No.      Protocol  Length  Info
23       ARP         60 Who has 10.129.158.250? Tell 10.129.158.105
24       SSDP       217 M-SEARCH * HTTP/1.1
25       SSDP       178 M-SEARCH * HTTP/1.1
26  or-… STP         60 RST. Root = 32768/0/00:38:df:d7:80:8a  Cost = 42002  Por
27       ARP         60 Who has 10.129.158.250? Tell 10.129.158.105
28       ARP         60 Who has 10.129.158.250? Tell 10.129.158.102
29
30
31
32
33
34
35
36
37
38
```

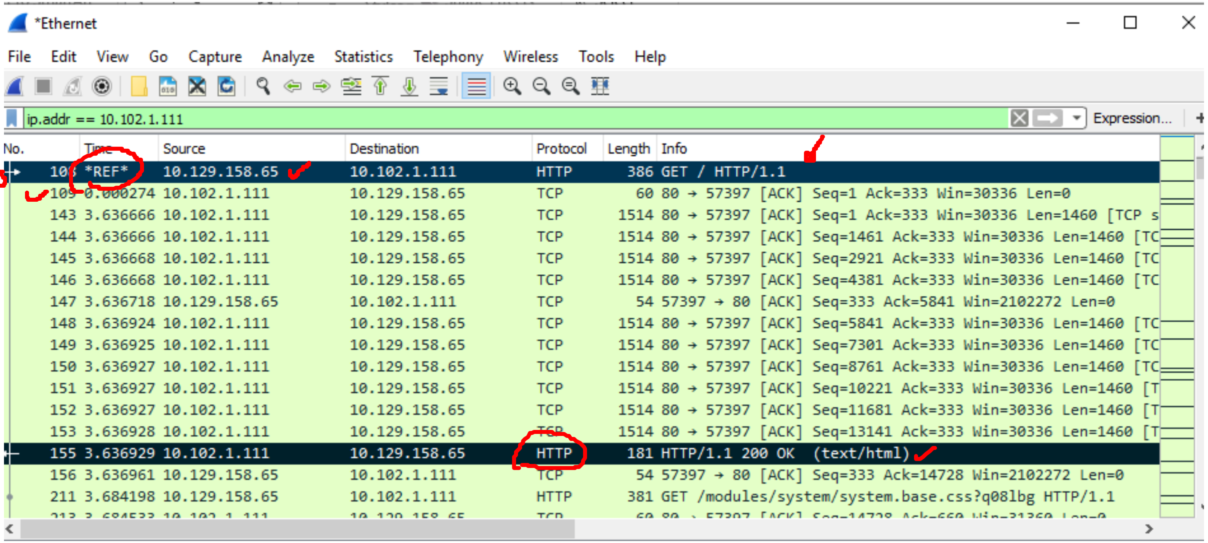
- Select packet
- Edit → Set/Unset Time Reference

time=0


*Ethernet
File 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
Expression...

```
No.                  Protocol Length Info
      .111           TCP        66 57397 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 S
      158.65         TCP        66 80 → 57397 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=14
      .111           TCP        54 57397 → 80 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
      .111           HTTP      386 GET / HTTP/1.1
      158.65         TCP        60 80 → 57397 [ACK] Seq=1 Ack=333 Win=30336 Len=0
      158.65         TCP      1514 80 → 57397 [ACK] Seq=1 Ack=333 Win=30336 Len=1460 [TCP s
      158.65         TCP      1514 80 → 57397 [ACK] Seq=1461 Ack=333 Win=30336 Len=1460 [TC
      158.65         TCP      1514 80 → 57397 [ACK] Seq=2921 Ack=333 Win=30336 Len=1460 [TC
      158.65         TCP      1514 80 → 57397 [ACK] Seq=4381 Ack=333 Win=30336 Len=1460 [TC
      .111           TCP        54 57397 → 80 [ACK] Seq=333 Ack=5841 Win=2102272 Len=0
      158.65         TCP      1514 80 → 57397 [ACK] Seq=5841 Ack=333 Win=30336 Len=1460 [TC
      158.65         TCP      1514 80 → 57397 [ACK] Seq=7301 Ack=333 Win=30336 Len=1460 [TC
      158.65         TCP      1514 80 → 57397 [ACK] Seq=8761 Ack=333 Win=30336 Len=1460 [TC
      158.65         TCP      1514 80 → 57397 [ACK] Seq=10221 Ack=333 Win=30336 Len=1460 [T
      158.65         TCP      1514 80 → 57397 [ACK] Seq=11681 Ack=333 Win=30336 Len=1460 [T
      158.65         TCP      1514 80 → 57397 [ACK] Seq=13141 Ack=333 Win=30336 Len=1460 [T

> Fr      ytes captured (432 bits) on interface 0
```

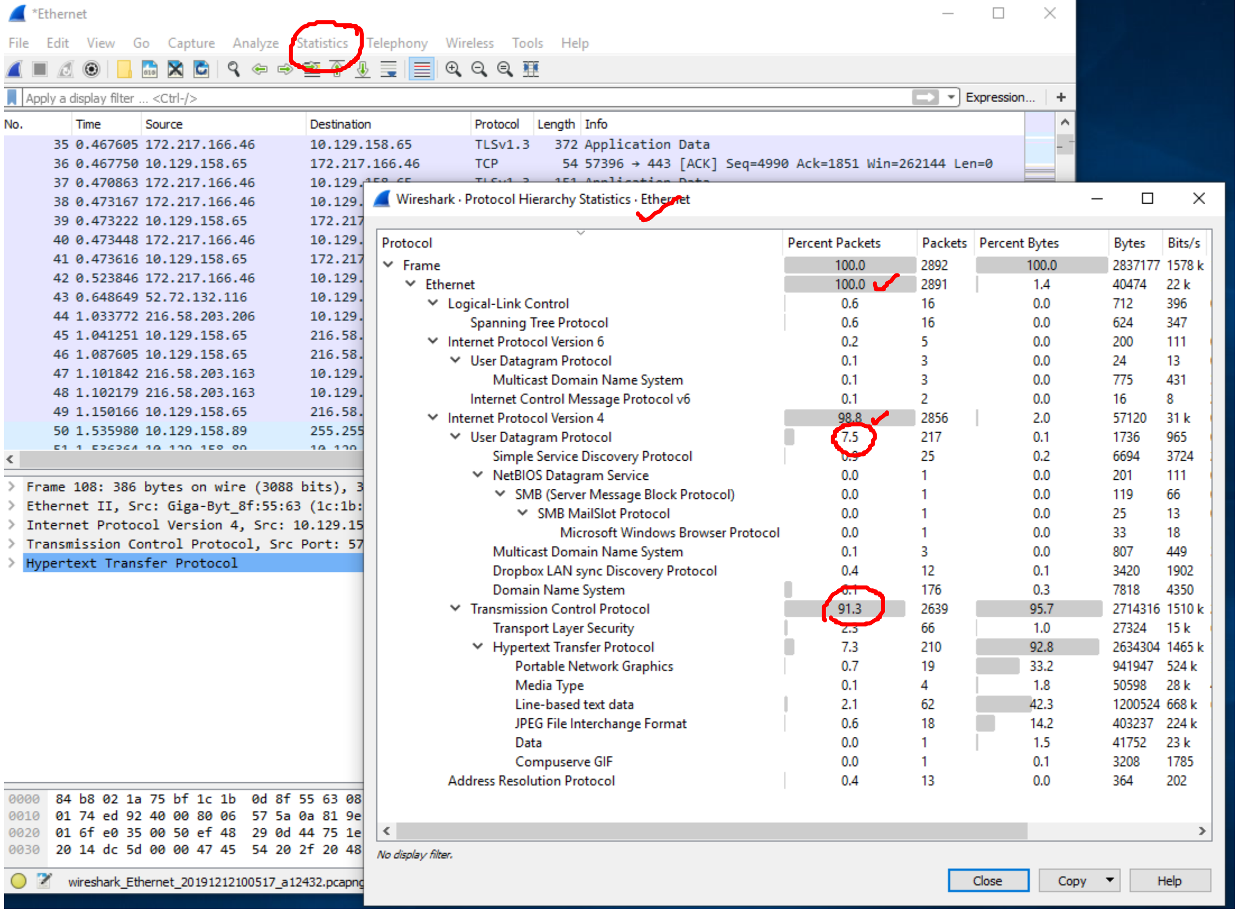

*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...

```
ip.addr == 10.102.1.111

No. Time     Source          Destination     Protocol Length Info
108 *REF*    10.129.158.65   10.102.1.111    HTTP      386 GET / HTTP/1.1
109 0.000274 10.102.1.111    10.129.158.65   TCP        60 80 → 57397 [ACK] Seq=1 Ack=333 Win=30336 Len=0
143 3.636666 10.102.1.111    10.129.158.65   TCP      1514 80 → 57397 [ACK] Seq=1 Ack=333 Win=30336 Len=1460 [TCP s
144 3.636666 10.102.1.111    10.129.158.65   TCP      1514 80 → 57397 [ACK] Seq=1461 Ack=333 Win=30336 Len=1460 [TC
145 3.636668 10.102.1.111    10.129.158.65   TCP      1514 80 → 57397 [ACK] Seq=2921 Ack=333 Win=30336 Len=1460 [TC
146 3.636668 10.102.1.111    10.129.158.65   TCP      1514 80 → 57397 [ACK] Seq=4381 Ack=333 Win=30336 Len=1460 [TC
147 3.636718 10.129.158.65   10.102.1.111    TCP        54 57397 → 80 [ACK] Seq=333 Ack=5841 Win=2102272 Len=0
148 3.636924 10.102.1.111    10.129.158.65   TCP      1514 80 → 57397 [ACK] Seq=5841 Ack=333 Win=30336 Len=1460 [TC
149 3.636925 10.102.1.111    10.129.158.65   TCP      1514 80 → 57397 [ACK] Seq=7301 Ack=333 Win=30336 Len=1460 [TC
150 3.636927 10.102.1.111    10.129.158.65   TCP      1514 80 → 57397 [ACK] Seq=8761 Ack=333 Win=30336 Len=1460 [TC
151 3.636927 10.102.1.111    10.129.158.65   TCP      1514 80 → 57397 [ACK] Seq=10221 Ack=333 Win=30336 Len=1460 [T
152 3.636927 10.102.1.111    10.129.158.65   TCP      1514 80 → 57397 [ACK] Seq=11681 Ack=333 Win=30336 Len=1460 [T
153 3.636928 10.102.1.111    10.129.158.65   TCP      1514 80 → 57397 [ACK] Seq=13141 Ack=333 Win=30336 Len=1460 [T
155 3.636929 10.102.1.111    10.129.158.65   HTTP      181 HTTP/1.1 200 OK  (text/html)
156 3.636961 10.129.158.65   10.102.1.111    TCP        54 57397 → 80 [ACK] Seq=333 Ack=14728 Win=2102272 Len=0
211 3.684198 10.129.158.65   10.102.1.111    HTTP      381 GET /modules/system/system.base.css?q08lbg HTTP/1.1
```

Statistics

- Statistics → Protocol Hierarchy (Menu bar)


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

```
No.      Time     Source          Destination     Protocol Length Info
      35 0.467605 172.217.166.46  10.129.158.65   TLSv1.3   372 Application Data
      36 0.467750 10.129.158.65   172.217.166.46  TCP        54 57396 → 443 [ACK] Seq=4990 Ack=1851 Win=262144 Len=0
      37 0.470863 172.217.166.46  10.129.158.65   TLSv1.3   151 Application Data
      38 0.473167 172.217.166.46  10.129.
      39 0.473222 10.129.158.65   172.217
      40 0.473448 172.217.166.46  10.129.
      41 0.473616 10.129.158.65   172.217
      42 0.523846 172.217.166.46  10.129.
      43 0.648649 52.72.132.116   10.129.
      44 1.033772 216.58.203.206  10.129.
      45 1.041251 10.129.158.65   216.58.
      46 1.087605 10.129.158.65   216.58.
      47 1.101842 216.58.203.163  10.129.
      48 1.102179 216.58.203.163  10.129.
      49 1.150166 10.129.158.65   216.58.
      50 1.535980 10.129.158.89   255.255
      51 1.536364 10.129.158.89   10.129.
```

```
> Frame 108: 386 bytes on wire (3088 bits), 3
> Ethernet II, Src: Giga-Byt_8f:55:63 (1c:1b:
> Internet Protocol Version 4, Src: 10.129.15
> Transmission Control Protocol, Src Port: 57
> Hypertext Transfer Protocol
```

```
0000  84 b8 02 1a 75 bf 1c 1b  0d 8f 55 63 08
0010  01 74 ed 92 40 00 80 06  57 5a 0a 81 9e
0020  01 6f e0 35 00 50 ef 48  29 0d 44 75 1e
0030  20 14 dc 5d 00 00 47 45  54 20 2f 20 48
```

wireshark_Ethernet_20191212100517_a12432.pcapng

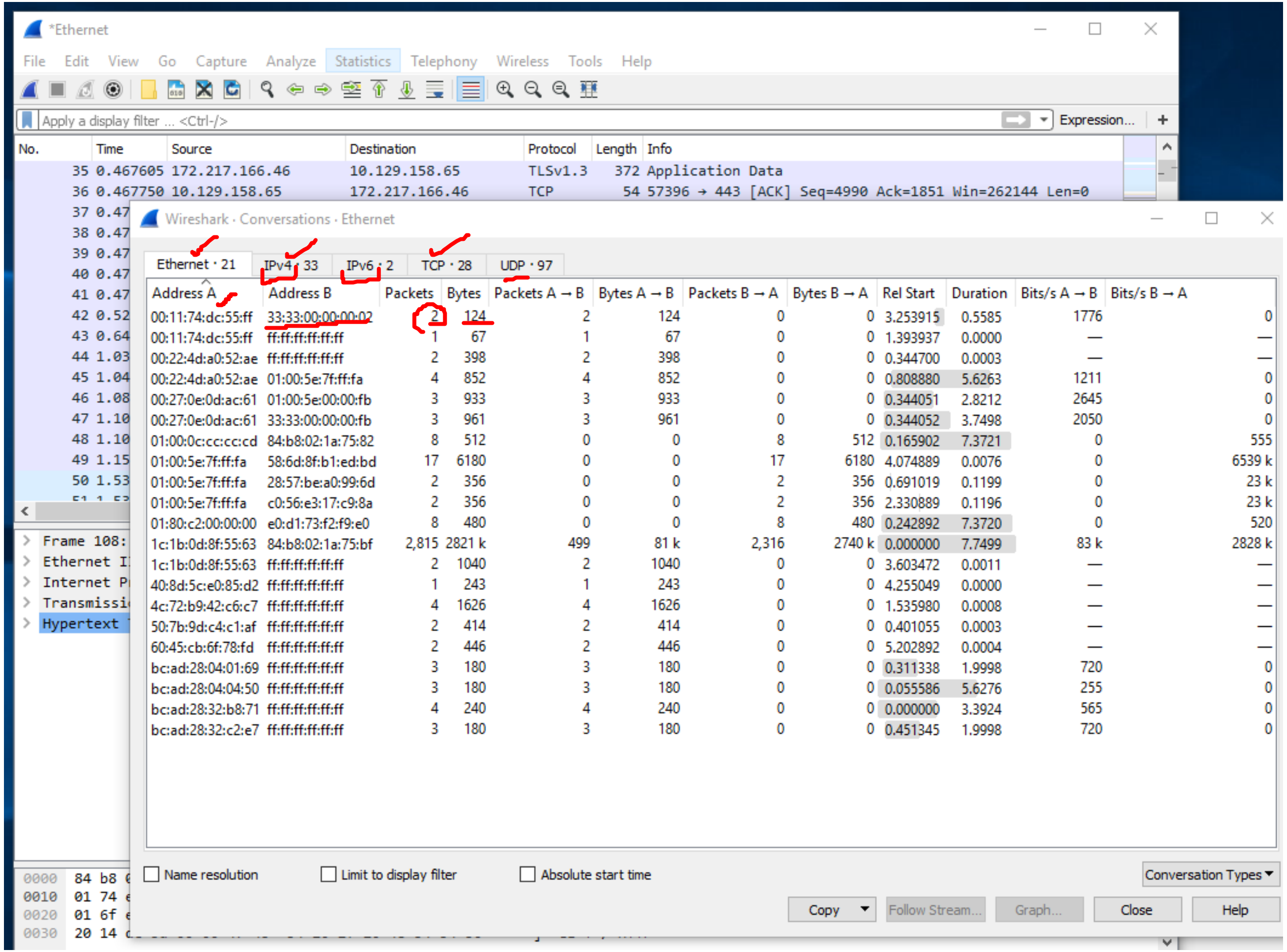
Wireshark · Protocol Hierarchy Statistics · Ethernet

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s
Frame	100.0	2892	100.0	2837177	1578 k
Ethernet	100.0	2891	1.4	40474	22 k
Logical-Link Control	0.6	16	0.0	712	396
Spanning Tree Protocol	0.6	16	0.0	624	347
Internet Protocol Version 6	0.2	5	0.0	200	111
User Datagram Protocol	0.1	3	0.0	24	13
Multicast Domain Name System	0.1	3	0.0	775	431
Internet Control Message Protocol v6	0.1	2	0.0	16	8
Internet Protocol Version 4	98.8	2856	2.0	57120	31 k
User Datagram Protocol	7.5	217	0.1	1736	965
Simple Service Discovery Protocol	0.9	25	0.2	6694	3724
NetBIOS Datagram Service	0.0	1	0.0	201	111
SMB (Server Message Block Protocol)	0.0	1	0.0	119	66
SMB MailSlot Protocol	0.0	1	0.0	25	13
Microsoft Windows Browser Protocol	0.0	1	0.0	33	18
Multicast Domain Name System	0.1	3	0.0	807	449
Dropbox LAN sync Discovery Protocol	0.4	12	0.1	3420	1902
Domain Name System	6.1	176	0.3	7818	4350
Transmission Control Protocol	91.3	2639	95.7	2714316	1510 k
Transport Layer Security	2.3	66	1.0	27324	15 k
Hypertext Transfer Protocol	7.3	210	92.8	2634304	1465 k
Portable Network Graphics	0.7	19	33.2	941947	524 k
Media Type	0.1	4	1.8	50598	28 k
Line-based text data	2.1	62	42.3	1200524	668 k
JPEG File Interchange Format	0.6	18	14.2	403237	224 k
Data	0.0	1	1.5	41752	23 k
Compuserve GIF	0.0	1	0.1	3208	1785
Address Resolution Protocol	0.4	13	0.0	364	202

No display filter.

Statistics

- Statistics → Conversations (Menu bar)



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

```
No.   Time      Source          Destination     Protocol Length Info
   35 0.467605 172.217.166.46 10.129.158.65   TLSv1.3   372 Application Data
   36 0.467750 10.129.158.65  172.217.166.46  TCP        54 57396 → 443 [ACK] Seq=4990 Ack=1851 Win=262144 Len=0
   37 0.47
   38 0.47
   39 0.47
   40 0.47
   41 0.47
   42 0.52
   43 0.64
   44 1.03
   45 1.04
   46 1.08
   47 1.10
   48 1.10
   49 1.15
   50 1.53
```

```
> Frame 108:
> Ethernet I
> Internet P
> Transmissi
> Hypertext
```

```
0000  84 b8 0
0010  01 74 e
0020  01 6f e
0030  20 14 c
```

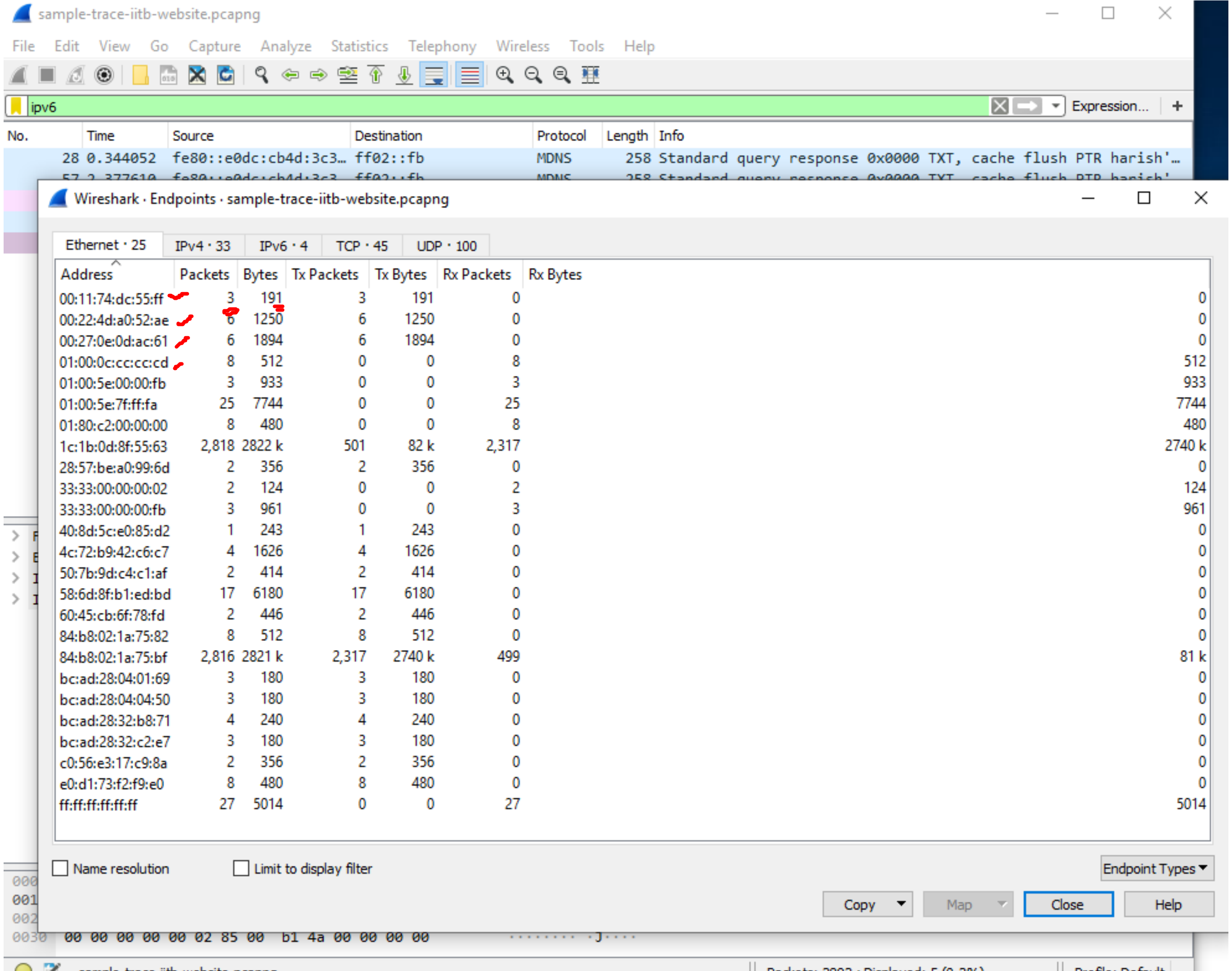
Wireshark · Conversations · Ethernet

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
00:11:74:dc:55:ff	33:33:00:00:00:02	2	124	2	124	0	0	3.253915	0.5585	1776	0
00:11:74:dc:55:ff	ff:ff:ff:ff:ff:ff	1	67	1	67	0	0	1.393937	0.0000	—	—
00:22:4d:a0:52:ae	ff:ff:ff:ff:ff:ff	2	398	2	398	0	0	0.344700	0.0003	—	—
00:22:4d:a0:52:ae	01:00:5e:7f:ff:fa	4	852	4	852	0	0	0.808880	5.6263	1211	0
00:27:0e:0d:ac:61	01:00:5e:00:00:fb	3	933	3	933	0	0	0.344051	2.8212	2645	0
00:27:0e:0d:ac:61	33:33:00:00:00:fb	3	961	3	961	0	0	0.344052	3.7498	2050	0
01:00:0c:cc:cc:cd	84:b8:02:1a:75:82	8	512	0	0	8	512	0.165902	7.3721	0	555
01:00:5e:7f:ff:fa	58:6d:8f:b1:ed:bd	17	6180	0	0	17	6180	4.074889	0.0076	0	6539 k
01:00:5e:7f:ff:fa	28:57:be:a0:99:6d	2	356	0	0	2	356	0.691019	0.1199	0	23 k
01:00:5e:7f:ff:fa	c0:56:e3:17:c9:8a	2	356	0	0	2	356	2.330889	0.1196	0	23 k
01:80:c2:00:00:00	e0:d1:73:f2:f9:e0	8	480	0	0	8	480	0.242892	7.3720	0	520
1c:1b:0d:8f:55:63	84:b8:02:1a:75:bf	2,815	2821 k	499	81 k	2,316	2740 k	0.000000	7.7499	83 k	2828 k
1c:1b:0d:8f:55:63	ff:ff:ff:ff:ff:ff	2	1040	2	1040	0	0	3.603472	0.0011	—	—
40:8d:5c:e0:85:d2	ff:ff:ff:ff:ff:ff	1	243	1	243	0	0	4.255049	0.0000	—	—
4c:72:b9:42:c6:c7	ff:ff:ff:ff:ff:ff	4	1626	4	1626	0	0	1.535980	0.0008	—	—
50:7b:9d:c4:c1:af	ff:ff:ff:ff:ff:ff	2	414	2	414	0	0	0.401055	0.0003	—	—
60:45:cb:6f:78:fd	ff:ff:ff:ff:ff:ff	2	446	2	446	0	0	5.202892	0.0004	—	—
bc:ad:28:04:01:69	ff:ff:ff:ff:ff:ff	3	180	3	180	0	0	0.311338	1.9998	720	0
bc:ad:28:04:04:50	ff:ff:ff:ff:ff:ff	3	180	3	180	0	0	0.055586	5.6276	255	0
bc:ad:28:32:b8:71	ff:ff:ff:ff:ff:ff	4	240	4	240	0	0	0.000000	3.3924	565	0
bc:ad:28:32:c2:e7	ff:ff:ff:ff:ff:ff	3	180	3	180	0	0	0.451345	1.9998	720	0

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

Statistics

- Statistics → End Points (Menu bar)



ipv6

No.	Time	Source	Destination	Protocol	Length	Info
28	0.344052	fe80::e0dc:cb4d:3c3…	ff02::fb	MDNS	258	Standard query response 0x0000 TXT, cache flush PTR harish'…

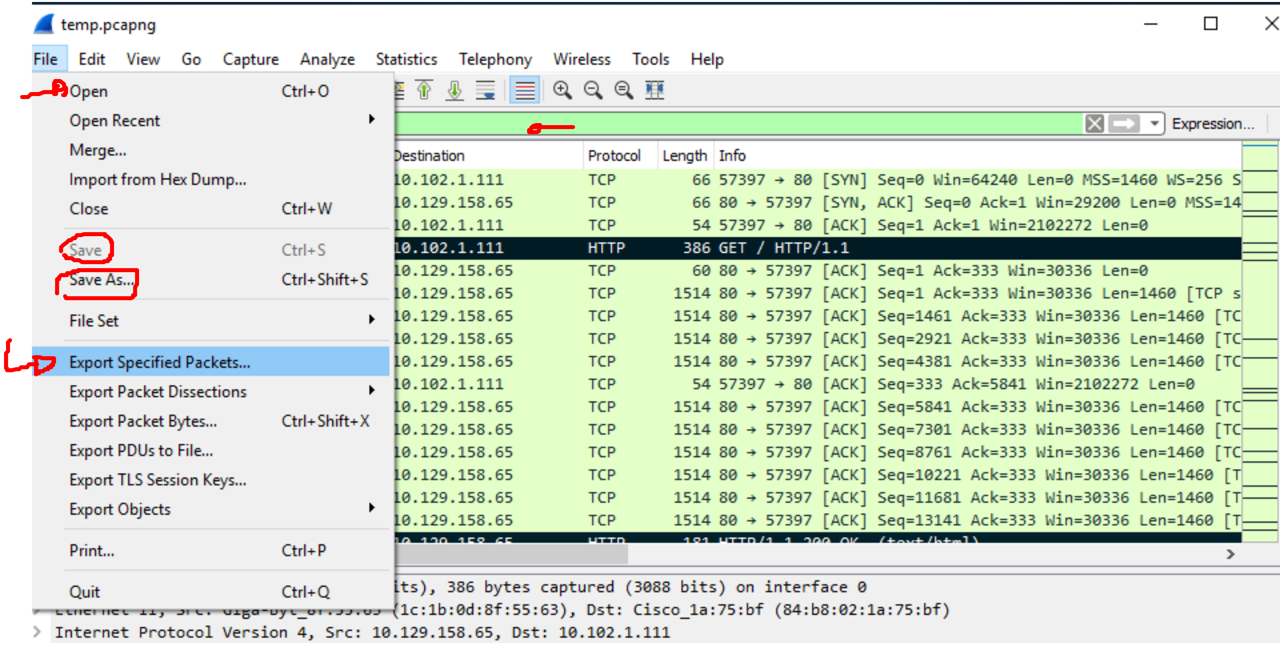
Wireshark · Endpoints · sample-trace-iitb-website.pcapng

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
00:11:74:dc:55:ff	3	191	3	191	0	0
00:22:4d:a0:52:ae	6	1250	6	1250	0	0
00:27:0e:0d:ac:61	6	1894	6	1894	0	0
01:00:0c:cc:cc:cd	8	512	0	0	8	512
01:00:5e:00:00:fb	3	933	0	0	3	933
01:00:5e:7f:ff:fa	25	7744	0	0	25	7744
01:80:c2:00:00:00	8	480	0	0	8	480
1c:1b:0d:8f:55:63	2,818	2822 k	501	82 k	2,317	2740 k
28:57:be:a0:99:6d	2	356	2	356	0	0
33:33:00:00:00:02	2	124	0	0	2	124
33:33:00:00:00:fb	3	961	0	0	3	961
40:8d:5c:e0:85:d2	1	243	1	243	0	0
4c:72:b9:42:c6:c7	4	1626	4	1626	0	0
50:7b:9d:c4:c1:af	2	414	2	414	0	0
58:6d:8f:b1:ed:bd	17	6180	17	6180	0	0
60:45:cb:6f:78:fd	2	446	2	446	0	0
84:b8:02:1a:75:82	8	512	8	512	0	0
84:b8:02:1a:75:bf	2,816	2821 k	2,317	2740 k	499	81 k
bc:ad:28:04:01:69	3	180	3	180	0	0
bc:ad:28:04:04:50	3	180	3	180	0	0
bc:ad:28:32:b8:71	4	240	4	240	0	0
bc:ad:28:32:c2:e7	3	180	3	180	0	0
c0:56:e3:17:c9:8a	2	356	2	356	0	0
e0:d1:73:f2:f9:e0	8	480	8	480	0	0
ff:ff:ff:ff:ff:ff	27	5014	0	0	27	5014

☐ Name resolution ☐ Limit to display filter

Save/Open Packet Capture

- Save/Save As
- Export (specific packets)
- Open saved file
  - just click on the file
  - Use file → open
  - In linux at command line: “wireshark filename”



```
Destination       Protocol  Length Info
10.102.1.111      TCP         66 57397 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 S
10.129.158.65     TCP         66 80 → 57397 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=14
10.102.1.111      TCP         54 57397 → 80 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
10.102.1.111      HTTP       386 GET / HTTP/1.1
10.129.158.65     TCP         60 80 → 57397 [ACK] Seq=1 Ack=333 Win=30336 Len=0
10.129.158.65     TCP       1514 80 → 57397 [ACK] Seq=1 Ack=333 Win=30336 Len=1460 [TCP s
10.129.158.65     TCP       1514 80 → 57397 [ACK] Seq=1461 Ack=333 Win=30336 Len=1460 [TC
10.129.158.65     TCP       1514 80 → 57397 [ACK] Seq=2921 Ack=333 Win=30336 Len=1460 [TC
10.129.158.65     TCP       1514 80 → 57397 [ACK] Seq=4381 Ack=333 Win=30336 Len=1460 [TC
10.102.1.111      TCP         54 57397 → 80 [ACK] Seq=333 Ack=5841 Win=2102272 Len=0
10.129.158.65     TCP       1514 80 → 57397 [ACK] Seq=5841 Ack=333 Win=30336 Len=1460 [TC
10.129.158.65     TCP       1514 80 → 57397 [ACK] Seq=7301 Ack=333 Win=30336 Len=1460 [TC
10.129.158.65     TCP       1514 80 → 57397 [ACK] Seq=8761 Ack=333 Win=30336 Len=1460 [TC
10.129.158.65     TCP       1514 80 → 57397 [ACK] Seq=10221 Ack=333 Win=30336 Len=1460 [T
10.129.158.65     TCP       1514 80 → 57397 [ACK] Seq=11681 Ack=333 Win=30336 Len=1460 [T
10.129.158.65     TCP       1514 80 → 57397 [ACK] Seq=13141 Ack=333 Win=30336 Len=1460 [T
10.129.158.65     HTTP       181 HTTP/1.1 200 OK  (text/html)

its), 386 bytes captured (3088 bits) on interface 0
(1c:1b:0d:8f:55:63), Dst: Cisco_1a:75:bf (84:b8:02:1a:75:bf)
> Internet Protocol Version 4, Src: 10.129.158.65, Dst: 10.102.1.111
```

References

- Wireshark Website
  - http://www.wireshark.org
- Wireshark Documentation
  - http://www.wireshark.org/docs/
- Wireshark Wiki
  - http://wiki.wireshark.org

Focus

- Wireshark (Main focus)
- Tcpdump (brief)

tcpdump

- Unix-based **command-line** packet sniffer
  - Reads “live traffic” from a specified interface
  - Usage:
    - sudo tcpdump –D ✓ (see what interfaces are available)
    - sudo tcpdump –i eth0 (capture packets on eth0 interface)
- Windump is for windows http://www.winpcap.org/windump/

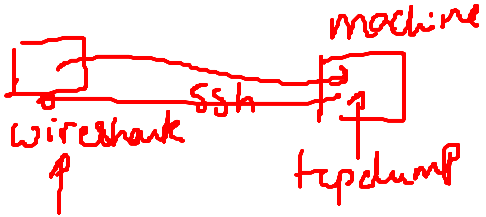
Output

src src port dst dst port

```
08:41:13.729687 IP 192.168.64.28.22 > 192.168.64.1.41916:
Flags [P.], seq 196:568, ack 1, win 309,
options [nop,nop,TS val 117964079 ecr 816509256], length 372
```

(Refer to
https://opensource.com/article/18/10/introduction-tcpdump)

Miscellaneous



- Capture Filters

  count 5 src/dst

  - sudo tcpdump -i eth0 -c5 host 54.204.39.132
  - sudo tcpdump -i eth0 src 192.168.122.98 and port 80

  IP

- Write to file
  - sudo tcpdump -i eth0 port 80 -w webserver.pcap

  (You can open these files in wireshark too!)

- Read from file
  - tcpdump -r webserver.pcap

Reference

- http://www.tcpdump.org/
- https://opensource.com/article/18/10/introduction-tcpdump ✓