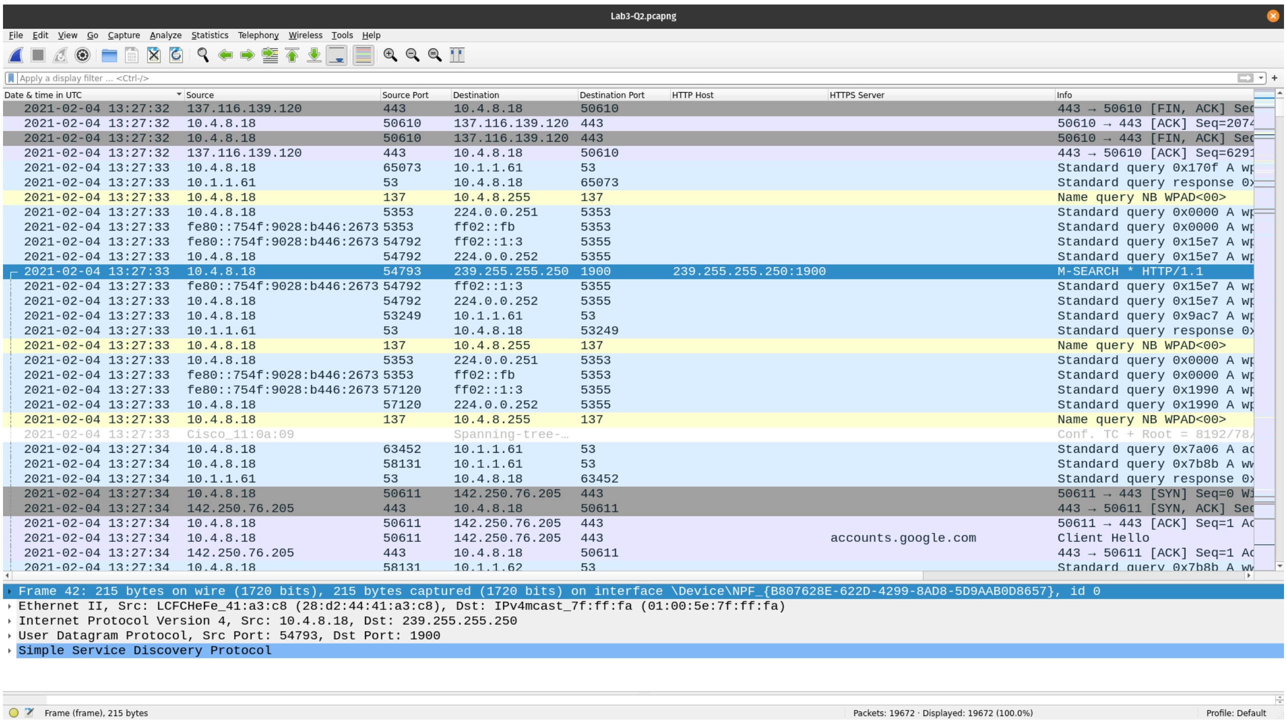
Lab 3

Name- Adarsh Nandanwar
BITS ID- 2018A7PS0396G

1. Customizing Wireshark

Columns:

- Date & time in UTC
- Source IP and source port
- Destination IP and destination port
- HTTP host
- HTTPS server
- Info


Lab3-Q2.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

Date & time in UTC	Source	Source Port	Destination	Destination Port	HTTP Host	HTTPS Server	Info
2021-02-04 13:27:32	137.116.139.120	443	10.4.8.18	50610			443 → 50610 [FIN, ACK] Sec
2021-02-04 13:27:32	10.4.8.18	50610	137.116.139.120	443			50610 → 443 [ACK] Seq=2074
2021-02-04 13:27:32	10.4.8.18	50610	137.116.139.120	443			50610 → 443 [FIN, ACK] Sec
2021-02-04 13:27:32	137.116.139.120	443	10.4.8.18	50610			443 → 50610 [ACK] Seq=6291
2021-02-04 13:27:33	10.4.8.18	65073	10.1.1.61	53			Standard query 0x170f A wp
2021-02-04 13:27:33	10.1.1.61	53	10.4.8.18	65073			Standard query response 0x
2021-02-04 13:27:33	10.4.8.18	137	10.4.8.255	137			Name query NB WPAD<00>
2021-02-04 13:27:33	10.4.8.18	5353	224.0.0.251	5353			Standard query 0x0000 A wp
2021-02-04 13:27:33	fe80::754f:9028:b446:2673	5353	ff02::fb	5353			Standard query 0x0000 A wp
2021-02-04 13:27:33	fe80::754f:9028:b446:2673	54792	ff02::1:3	5355			Standard query 0x15e7 A wp
2021-02-04 13:27:33	10.4.8.18	54792	224.0.0.252	5355			Standard query 0x15e7 A wp
2021-02-04 13:27:33	10.4.8.18	54793	239.255.255.250	1900	239.255.255.250:1900		M-SEARCH * HTTP/1.1
2021-02-04 13:27:33	fe80::754f:9028:b446:2673	54792	ff02::1:3	5355			Standard query 0x15e7 A wp
2021-02-04 13:27:33	10.4.8.18	54792	224.0.0.252	5355			Standard query 0x15e7 A wp
2021-02-04 13:27:33	10.4.8.18	53249	10.1.1.61	53			Standard query 0x9ac7 A wp
2021-02-04 13:27:33	10.1.1.61	53	10.4.8.18	53249			Standard query response 0x
2021-02-04 13:27:33	10.4.8.18	137	10.4.8.255	137			Name query NB WPAD<00>
2021-02-04 13:27:33	10.4.8.18	5353	224.0.0.251	5353			Standard query 0x0000 A wp
2021-02-04 13:27:33	fe80::754f:9028:b446:2673	5353	ff02::fb	5353			Standard query 0x0000 A wp
2021-02-04 13:27:33	fe80::754f:9028:b446:2673	57120	ff02::1:3	5355			Standard query 0x1990 A wp
2021-02-04 13:27:33	10.4.8.18	57120	224.0.0.252	5355			Standard query 0x1990 A wp
2021-02-04 13:27:33	10.4.8.18	137	10.4.8.255	137			Name query NB WPAD<00>
2021-02-04 13:27:33	Cisco_11:0a:09		Spanning-tree-…				Conf. TC + Root = 8192/78/
2021-02-04 13:27:34	10.4.8.18	63452	10.1.1.61	53			Standard query 0x7a06 A ac
2021-02-04 13:27:34	10.4.8.18	58131	10.1.1.61	53			Standard query 0x7b8b A ww
2021-02-04 13:27:34	10.1.1.61	53	10.4.8.18	63452			Standard query response 0x
2021-02-04 13:27:34	10.4.8.18	50611	142.250.76.205	443			50611 → 443 [SYN] Seq=0 Wi
2021-02-04 13:27:34	142.250.76.205	443	10.4.8.18	50611			443 → 50611 [SYN, ACK] Sec
2021-02-04 13:27:34	10.4.8.18	50611	142.250.76.205	443			50611 → 443 [ACK] Seq=1 Ac
2021-02-04 13:27:34	10.4.8.18	50611	142.250.76.205	443		accounts.google.com	Client Hello
2021-02-04 13:27:34	142.250.76.205	443	10.4.8.18	50611			443 → 50611 [ACK] Seq=1 Ac
2021-02-04 13:27:34	10.4.8.18	58131	10.1.1.62	53			Standard query 0x7b8b A ww

```
› Frame 42: 215 bytes on wire (1720 bits), 215 bytes captured (1720 bits) on interface \Device\NPF_{B807628E-622D-4299-8AD8-5D9AAB0D8657}, id 0
› Ethernet II, Src: LCFCHeFe_41:a3:c8 (28:d2:44:41:a3:c8), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
› Internet Protocol Version 4, Src: 10.4.8.18, Dst: 239.255.255.250
› User Datagram Protocol, Src Port: 54793, Dst Port: 1900
› Simple Service Discovery Protocol
```

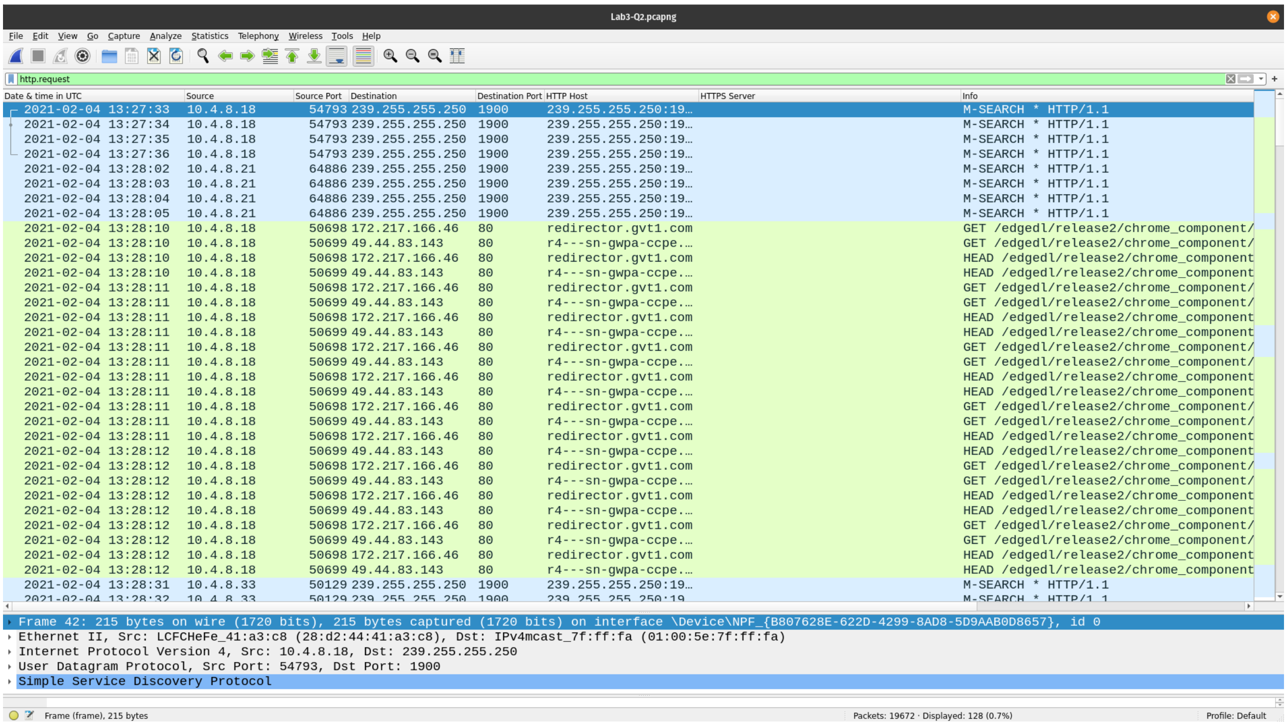
Frame (frame), 215 bytes Packets: 19672 · Displayed: 19672 (100.0%) Profile: Default

2. Wireshark Dump Analysis

a. Identify the http request packet

```
http.request
```

- `http.request` filter is of boolean type. It displays the packet if it is a http request packet.

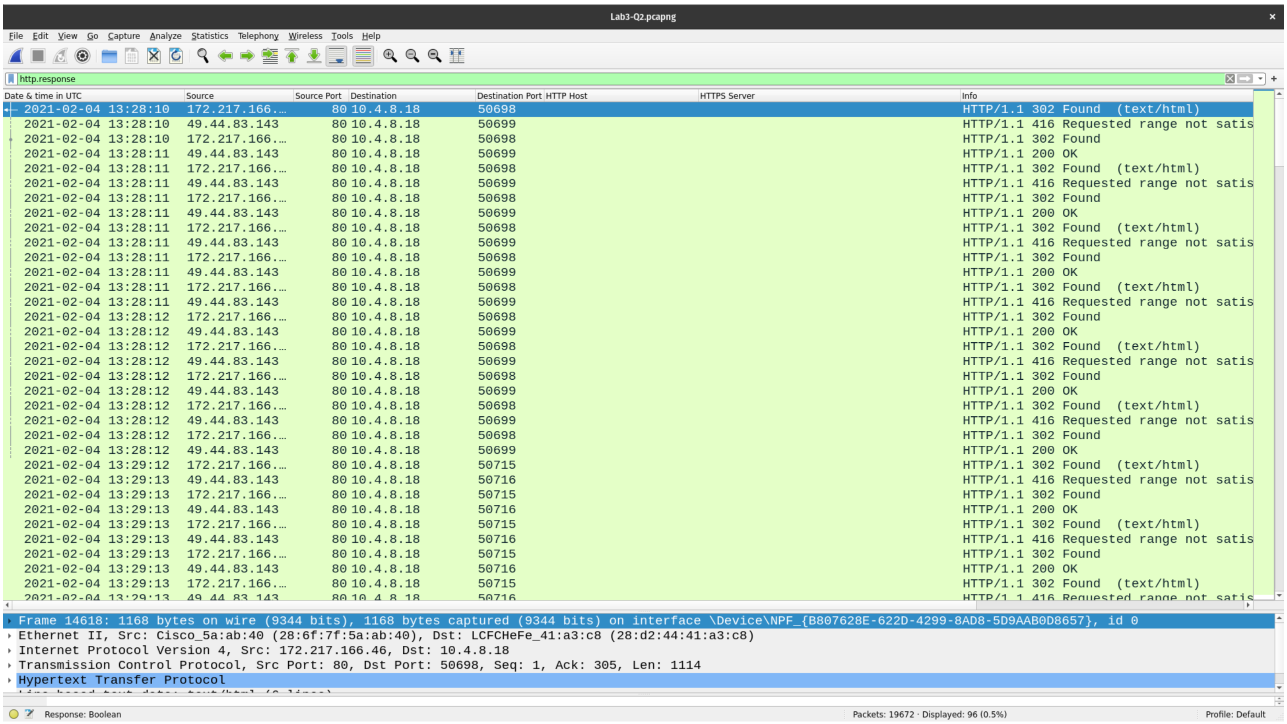

Lab3-Q2.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
http.request

Date & time in UTC   Source      Source Port Destination  Destination Port HTTP Host       HTTPS Server  Info
2021-02-04 13:27:33  10.4.8.18   54793 239.255.255.250  1900  239.255.255.250:19…       M-SEARCH * HTTP/1.1
2021-02-04 13:27:34  10.4.8.18   54793 239.255.255.250  1900  239.255.255.250:19…       M-SEARCH * HTTP/1.1
2021-02-04 13:27:35  10.4.8.18   54793 239.255.255.250  1900  239.255.255.250:19…       M-SEARCH * HTTP/1.1
2021-02-04 13:27:36  10.4.8.18   54793 239.255.255.250  1900  239.255.255.250:19…       M-SEARCH * HTTP/1.1
2021-02-04 13:28:02  10.4.8.21   64886 239.255.255.250  1900  239.255.255.250:19…       M-SEARCH * HTTP/1.1
2021-02-04 13:28:03  10.4.8.21   64886 239.255.255.250  1900  239.255.255.250:19…       M-SEARCH * HTTP/1.1
2021-02-04 13:28:04  10.4.8.21   64886 239.255.255.250  1900  239.255.255.250:19…       M-SEARCH * HTTP/1.1
2021-02-04 13:28:05  10.4.8.21   64886 239.255.255.250  1900  239.255.255.250:19…       M-SEARCH * HTTP/1.1
2021-02-04 13:28:10  10.4.8.18   50698 172.217.166.46   80    redirector.gvt1.com       GET /edgedl/release2/chrome_component/
2021-02-04 13:28:10  10.4.8.18   50699 49.44.83.143     80    r4---sn-gwpa-ccpe.…       GET /edgedl/release2/chrome_component/
2021-02-04 13:28:10  10.4.8.18   50698 172.217.166.46   80    redirector.gvt1.com       HEAD /edgedl/release2/chrome_component
2021-02-04 13:28:10  10.4.8.18   50699 49.44.83.143     80    r4---sn-gwpa-ccpe.…       HEAD /edgedl/release2/chrome_component
2021-02-04 13:28:11  10.4.8.18   50698 172.217.166.46   80    redirector.gvt1.com       GET /edgedl/release2/chrome_component/
2021-02-04 13:28:11  10.4.8.18   50699 49.44.83.143     80    r4---sn-gwpa-ccpe.…       GET /edgedl/release2/chrome_component/
2021-02-04 13:28:11  10.4.8.18   50698 172.217.166.46   80    redirector.gvt1.com       HEAD /edgedl/release2/chrome_component
2021-02-04 13:28:11  10.4.8.18   50699 49.44.83.143     80    r4---sn-gwpa-ccpe.…       HEAD /edgedl/release2/chrome_component
2021-02-04 13:28:11  10.4.8.18   50698 172.217.166.46   80    redirector.gvt1.com       GET /edgedl/release2/chrome_component/
2021-02-04 13:28:11  10.4.8.18   50699 49.44.83.143     80    r4---sn-gwpa-ccpe.…       GET /edgedl/release2/chrome_component/
2021-02-04 13:28:11  10.4.8.18   50698 172.217.166.46   80    redirector.gvt1.com       HEAD /edgedl/release2/chrome_component
2021-02-04 13:28:11  10.4.8.18   50699 49.44.83.143     80    r4---sn-gwpa-ccpe.…       HEAD /edgedl/release2/chrome_component
2021-02-04 13:28:11  10.4.8.18   50698 172.217.166.46   80    redirector.gvt1.com       GET /edgedl/release2/chrome_component/
2021-02-04 13:28:11  10.4.8.18   50699 49.44.83.143     80    r4---sn-gwpa-ccpe.…       GET /edgedl/release2/chrome_component/
2021-02-04 13:28:11  10.4.8.18   50698 172.217.166.46   80    redirector.gvt1.com       HEAD /edgedl/release2/chrome_component
2021-02-04 13:28:12  10.4.8.18   50699 49.44.83.143     80    r4---sn-gwpa-ccpe.…       HEAD /edgedl/release2/chrome_component
2021-02-04 13:28:12  10.4.8.18   50698 172.217.166.46   80    redirector.gvt1.com       GET /edgedl/release2/chrome_component/
2021-02-04 13:28:12  10.4.8.18   50699 49.44.83.143     80    r4---sn-gwpa-ccpe.…       GET /edgedl/release2/chrome_component/
2021-02-04 13:28:12  10.4.8.18   50698 172.217.166.46   80    redirector.gvt1.com       HEAD /edgedl/release2/chrome_component
2021-02-04 13:28:12  10.4.8.18   50699 49.44.83.143     80    r4---sn-gwpa-ccpe.…       HEAD /edgedl/release2/chrome_component
2021-02-04 13:28:12  10.4.8.18   50698 172.217.166.46   80    redirector.gvt1.com       GET /edgedl/release2/chrome_component/
2021-02-04 13:28:12  10.4.8.18   50699 49.44.83.143     80    r4---sn-gwpa-ccpe.…       GET /edgedl/release2/chrome_component/
2021-02-04 13:28:12  10.4.8.18   50698 172.217.166.46   80    redirector.gvt1.com       HEAD /edgedl/release2/chrome_component
2021-02-04 13:28:12  10.4.8.18   50699 49.44.83.143     80    r4---sn-gwpa-ccpe.…       HEAD /edgedl/release2/chrome_component
2021-02-04 13:28:31  10.4.8.33   50129 239.255.255.250  1900  239.255.255.250:19…       M-SEARCH * HTTP/1.1
2021-02-04 13:28:32  10.4.8.33   50129 239.255.255.250  1900  239.255.255.250:19       M-SEARCH * HTTP/1.1

› Frame 42: 215 bytes on wire (1720 bits), 215 bytes captured (1720 bits) on interface \Device\NPF_{B807628E-622D-4299-8AD8-5D9AAB0D8657}, id 0
› Ethernet II, Src: LCFCHeFe_41:a3:c8 (28:d2:44:41:a3:c8), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
› Internet Protocol Version 4, Src: 10.4.8.18, Dst: 239.255.255.250
› User Datagram Protocol, Src Port: 54793, Dst Port: 1900
› Simple Service Discovery Protocol

Frame (frame), 215 bytes          Packets: 19672 · Displayed: 128 (0.7%)          Profile: Default
```

b. Identify the http response packet

```
http.response
```

- `http.response` filter is of boolean type. It displays the packet if it is a http response packet.

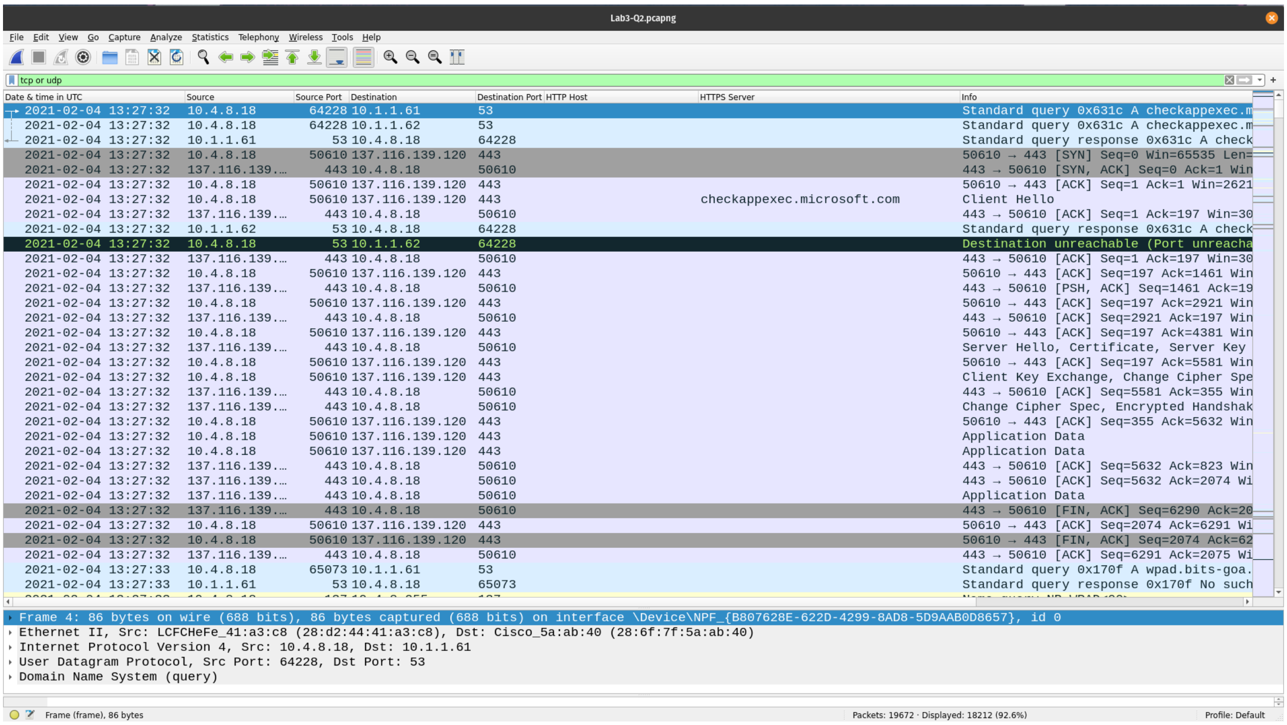

Lab3-Q2.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
http.response

Date & time in UTC   Source          Source Port Destination Destination Port HTTP Host  HTTPS Server  Info
2021-02-04 13:28:10  172.217.166.…   80 10.4.8.18   50698        HTTP/1.1 302 Found  (text/html)
2021-02-04 13:28:10  49.44.83.143    80 10.4.8.18   50699        HTTP/1.1 416 Requested range not satis
2021-02-04 13:28:10  172.217.166.…   80 10.4.8.18   50698        HTTP/1.1 302 Found
2021-02-04 13:28:11  49.44.83.143    80 10.4.8.18   50699        HTTP/1.1 200 OK
2021-02-04 13:28:11  172.217.166.…   80 10.4.8.18   50698        HTTP/1.1 302 Found  (text/html)
2021-02-04 13:28:11  49.44.83.143    80 10.4.8.18   50699        HTTP/1.1 416 Requested range not satis
2021-02-04 13:28:11  172.217.166.…   80 10.4.8.18   50698        HTTP/1.1 302 Found
2021-02-04 13:28:11  49.44.83.143    80 10.4.8.18   50699        HTTP/1.1 200 OK
2021-02-04 13:28:11  172.217.166.…   80 10.4.8.18   50698        HTTP/1.1 302 Found  (text/html)
2021-02-04 13:28:11  49.44.83.143    80 10.4.8.18   50699        HTTP/1.1 416 Requested range not satis
2021-02-04 13:28:11  172.217.166.…   80 10.4.8.18   50698        HTTP/1.1 302 Found
2021-02-04 13:28:11  49.44.83.143    80 10.4.8.18   50699        HTTP/1.1 200 OK
2021-02-04 13:28:11  172.217.166.…   80 10.4.8.18   50698        HTTP/1.1 302 Found  (text/html)
2021-02-04 13:28:11  49.44.83.143    80 10.4.8.18   50699        HTTP/1.1 416 Requested range not satis
2021-02-04 13:28:12  172.217.166.…   80 10.4.8.18   50698        HTTP/1.1 302 Found
2021-02-04 13:28:12  49.44.83.143    80 10.4.8.18   50699        HTTP/1.1 200 OK
2021-02-04 13:28:12  172.217.166.…   80 10.4.8.18   50698        HTTP/1.1 302 Found  (text/html)
2021-02-04 13:28:12  49.44.83.143    80 10.4.8.18   50699        HTTP/1.1 416 Requested range not satis
2021-02-04 13:28:12  172.217.166.…   80 10.4.8.18   50698        HTTP/1.1 302 Found
2021-02-04 13:28:12  49.44.83.143    80 10.4.8.18   50699        HTTP/1.1 200 OK
2021-02-04 13:28:12  172.217.166.…   80 10.4.8.18   50698        HTTP/1.1 302 Found  (text/html)
2021-02-04 13:28:12  49.44.83.143    80 10.4.8.18   50699        HTTP/1.1 416 Requested range not satis
2021-02-04 13:28:12  172.217.166.…   80 10.4.8.18   50698        HTTP/1.1 302 Found
2021-02-04 13:28:12  49.44.83.143    80 10.4.8.18   50699        HTTP/1.1 200 OK
2021-02-04 13:29:12  172.217.166.…   80 10.4.8.18   50715        HTTP/1.1 302 Found  (text/html)
2021-02-04 13:29:13  49.44.83.143    80 10.4.8.18   50716        HTTP/1.1 416 Requested range not satis
2021-02-04 13:29:13  172.217.166.…   80 10.4.8.18   50715        HTTP/1.1 302 Found
2021-02-04 13:29:13  49.44.83.143    80 10.4.8.18   50716        HTTP/1.1 200 OK
2021-02-04 13:29:13  172.217.166.…   80 10.4.8.18   50715        HTTP/1.1 302 Found  (text/html)
2021-02-04 13:29:13  49.44.83.143    80 10.4.8.18   50716        HTTP/1.1 416 Requested range not satis
2021-02-04 13:29:13  172.217.166.…   80 10.4.8.18   50715        HTTP/1.1 302 Found
2021-02-04 13:29:13  49.44.83.143    80 10.4.8.18   50716        HTTP/1.1 200 OK
2021-02-04 13:29:13  172.217.166.…   80 10.4.8.18   50715        HTTP/1.1 302 Found  (text/html)
2021-02-04 13:29:13  49.44.83.143    80 10.4.8.18   50716        HTTP/1.1 416 Requested range not satis

› Frame 14618: 1168 bytes on wire (9344 bits), 1168 bytes captured (9344 bits) on interface \Device\NPF_{B807628E-622D-4299-8AD8-5D9AAB0D8657}, id 0
› Ethernet II, Src: Cisco_5a:ab:40 (28:6f:7f:5a:ab:40), Dst: LCFCHeFe_41:a3:c8 (28:d2:44:41:a3:c8)
› Internet Protocol Version 4, Src: 172.217.166.46, Dst: 10.4.8.18
› Transmission Control Protocol, Src Port: 80, Dst Port: 50698, Seq: 1, Ack: 305, Len: 1114
› Hypertext Transfer Protocol
› Line-based text data: text/html (6 lines)

Response: Boolean          Packets: 19672 · Displayed: 96 (0.5%)          Profile: Default
```

c. Display the statistics of the TCP and UDP packets

```
tcp or udp
```

- `tcp` filter is used to display only the packets containing the TCP protocol.
- `udp` filter is used to display only the packets containing the UDP protocol.
- `or` is the logical or operator. This displays the packets satisfying either of the two conditions.


Lab3-Q2.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
tcp or udp
```

```
Date & time in UTC     Source           Source Port Destination     Destination Port HTTP Host  HTTPS Server                 Info
2021-02-04 13:27:32    10.4.8.18        64228 10.1.1.61         53                                                        Standard query 0x631c A checkappexec.m
2021-02-04 13:27:32    10.4.8.18        64228 10.1.1.62         53                                                        Standard query 0x631c A checkappexec.m
2021-02-04 13:27:32    10.1.1.61           53 10.4.8.18         64228                                                     Standard query response 0x631c A check
2021-02-04 13:27:32    10.4.8.18        50610 137.116.139.120   443                                                       50610 → 443 [SYN] Seq=0 Win=65535 Len=
2021-02-04 13:27:32    137.116.139.…      443 10.4.8.18         50610                                                     443 → 50610 [SYN, ACK] Seq=0 Ack=1 Win
2021-02-04 13:27:32    10.4.8.18        50610 137.116.139.120   443                                                       50610 → 443 [ACK] Seq=1 Ack=1 Win=2621
2021-02-04 13:27:32    10.4.8.18        50610 137.116.139.120   443                         checkappexec.microsoft.com    Client Hello
2021-02-04 13:27:32    137.116.139.…      443 10.4.8.18         50610                                                     443 → 50610 [ACK] Seq=1 Ack=197 Win=30
2021-02-04 13:27:32    10.1.1.62           53 10.4.8.18         64228                                                     Standard query response 0x631c A check
2021-02-04 13:27:32    10.4.8.18           53 10.1.1.62         64228                                                     Destination unreachable (Port unreacha
2021-02-04 13:27:32    137.116.139.…      443 10.4.8.18         50610                                                     443 → 50610 [ACK] Seq=1 Ack=197 Win=30
2021-02-04 13:27:32    10.4.8.18        50610 137.116.139.120   443                                                       50610 → 443 [ACK] Seq=197 Ack=1461 Win
2021-02-04 13:27:32    137.116.139.…      443 10.4.8.18         50610                                                     443 → 50610 [PSH, ACK] Seq=1461 Ack=19
2021-02-04 13:27:32    10.4.8.18        50610 137.116.139.120   443                                                       50610 → 443 [ACK] Seq=197 Ack=2921 Win
2021-02-04 13:27:32    137.116.139.…      443 10.4.8.18         50610                                                     443 → 50610 [ACK] Seq=2921 Ack=197 Win
2021-02-04 13:27:32    10.4.8.18        50610 137.116.139.120   443                                                       50610 → 443 [ACK] Seq=197 Ack=4381 Win
2021-02-04 13:27:32    137.116.139.…      443 10.4.8.18         50610                                                     Server Hello, Certificate, Server Key
2021-02-04 13:27:32    10.4.8.18        50610 137.116.139.120   443                                                       50610 → 443 [ACK] Seq=197 Ack=5581 Win
2021-02-04 13:27:32    10.4.8.18        50610 137.116.139.120   443                                                       Client Key Exchange, Change Cipher Spe
2021-02-04 13:27:32    137.116.139.…      443 10.4.8.18         50610                                                     443 → 50610 [ACK] Seq=5581 Ack=355 Win
2021-02-04 13:27:32    137.116.139.…      443 10.4.8.18         50610                                                     Change Cipher Spec, Encrypted Handshak
2021-02-04 13:27:32    10.4.8.18        50610 137.116.139.120   443                                                       50610 → 443 [ACK] Seq=355 Ack=5632 Win
2021-02-04 13:27:32    10.4.8.18        50610 137.116.139.120   443                                                       Application Data
2021-02-04 13:27:32    10.4.8.18        50610 137.116.139.120   443                                                       Application Data
2021-02-04 13:27:32    137.116.139.…      443 10.4.8.18         50610                                                     443 → 50610 [ACK] Seq=5632 Ack=823 Win
2021-02-04 13:27:32    137.116.139.…      443 10.4.8.18         50610                                                     443 → 50610 [ACK] Seq=5632 Ack=2074 Wi
2021-02-04 13:27:32    137.116.139.…      443 10.4.8.18         50610                                                     Application Data
2021-02-04 13:27:32    137.116.139.…      443 10.4.8.18         50610                                                     443 → 50610 [FIN, ACK] Seq=6290 Ack=20
2021-02-04 13:27:32    10.4.8.18        50610 137.116.139.120   443                                                       50610 → 443 [ACK] Seq=2074 Ack=6291 Wi
2021-02-04 13:27:32    10.4.8.18        50610 137.116.139.120   443                                                       50610 → 443 [FIN, ACK] Seq=2074 Ack=62
2021-02-04 13:27:32    137.116.139.…      443 10.4.8.18         50610                                                     443 → 50610 [ACK] Seq=6291 Ack=2075 Wi
2021-02-04 13:27:33    10.4.8.18        65073 10.1.1.61         53                                                        Standard query 0x170f A wpad.bits-goa.
2021-02-04 13:27:33    10.1.1.61           53 10.4.8.18         65073                                                     Standard query response 0x170f No such
```

```
› Frame 4: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface \Device\NPF_{B807628E-622D-4299-8AD8-5D9AAB0D8657}, id 0
› Ethernet II, Src: LCFCHeFe_41:a3:c8 (28:d2:44:41:a3:c8), Dst: Cisco_5a:ab:40 (28:6f:7f:5a:ab:40)
› Internet Protocol Version 4, Src: 10.4.8.18, Dst: 10.1.1.61
› User Datagram Protocol, Src Port: 64228, Dst Port: 53
› Domain Name System (query)
```

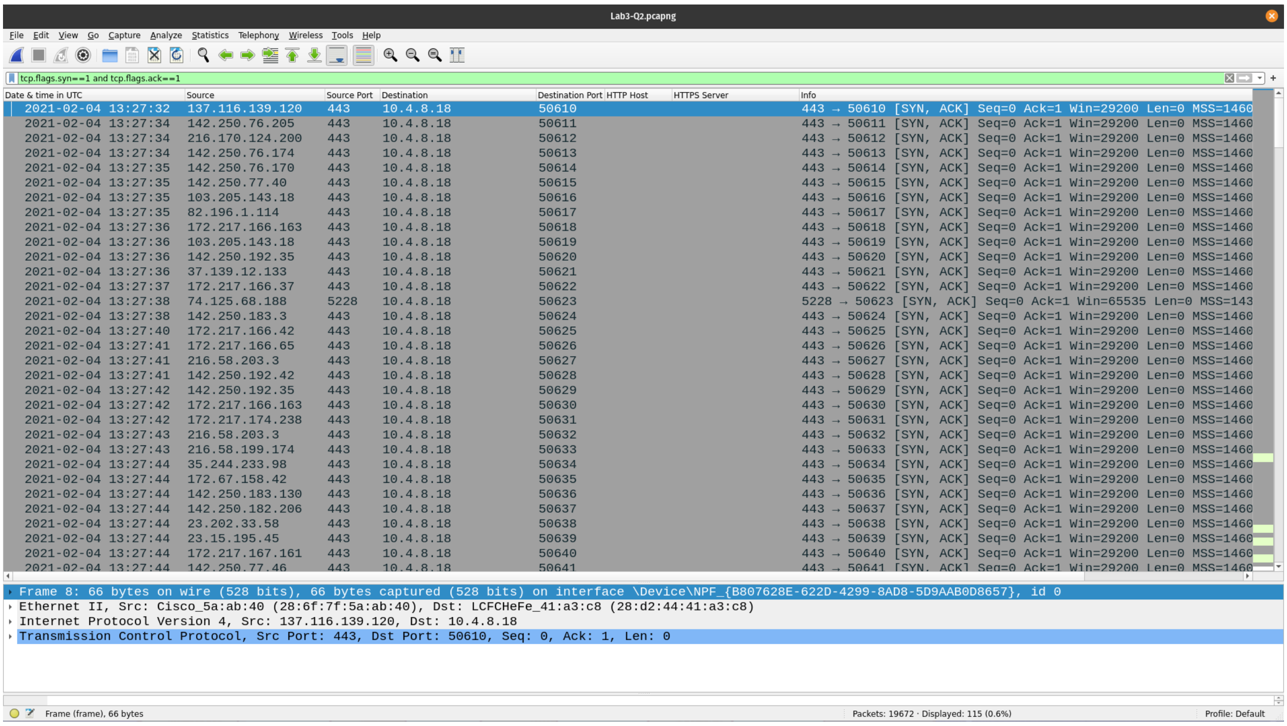
Frame (frame), 86 bytes   Packets: 19672 · Displayed: 18212 (92.6%)   Profile: Default

d. List out the TCP packets whose syn. and ack. Flags are on.

```
tcp.flags.syn==1 and tcp.flags.ack==1
```

- `tcp.flags` contains all the flags related to the protocol.
- `tcp.flags.syn` is synchronization flag. It is used in first step of connection establishment phase or 3-way handshake process between the two hosts. Only the first packet from sender as well as receiver should have this flag set.
- `tcp.flags.ack` is acknowledgement flag. It is used to acknowledge packets which are successfully received by the host.

- `and` is the logical and operator. This displays the packets satisfying both conditions.


Lab3-Q2.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
tcp.flags.syn==1 and tcp.flags.ack==1
```

```
Date & time in UTC    Source           Source Port Destination  Destination Port HTTP Host  HTTPS Server  Info
2021-02-04 13:27:32   137.116.139.120  443         10.4.8.18    50610                                     443 → 50610 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
2021-02-04 13:27:34   142.250.76.205   443         10.4.8.18    50611                                     443 → 50611 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
2021-02-04 13:27:34   216.170.124.200  443         10.4.8.18    50612                                     443 → 50612 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
2021-02-04 13:27:34   142.250.76.174   443         10.4.8.18    50613                                     443 → 50613 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
2021-02-04 13:27:35   142.250.76.170   443         10.4.8.18    50614                                     443 → 50614 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
2021-02-04 13:27:35   142.250.77.40    443         10.4.8.18    50615                                     443 → 50615 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
2021-02-04 13:27:35   103.205.143.18   443         10.4.8.18    50616                                     443 → 50616 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
2021-02-04 13:27:35   82.196.1.114     443         10.4.8.18    50617                                     443 → 50617 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
2021-02-04 13:27:36   172.217.166.163  443         10.4.8.18    50618                                     443 → 50618 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
2021-02-04 13:27:36   103.205.143.18   443         10.4.8.18    50619                                     443 → 50619 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
2021-02-04 13:27:36   142.250.192.35   443         10.4.8.18    50620                                     443 → 50620 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
2021-02-04 13:27:36   37.139.12.133    443         10.4.8.18    50621                                     443 → 50621 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
2021-02-04 13:27:37   172.217.166.37   443         10.4.8.18    50622                                     443 → 50622 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
2021-02-04 13:27:38   74.125.68.188    5228        10.4.8.18    50623                                     5228 → 50623 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=143
2021-02-04 13:27:38   142.250.183.3    443         10.4.8.18    50624                                     443 → 50624 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
2021-02-04 13:27:40   172.217.166.42   443         10.4.8.18    50625                                     443 → 50625 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
2021-02-04 13:27:41   172.217.166.65   443         10.4.8.18    50626                                     443 → 50626 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
2021-02-04 13:27:41   216.58.203.3     443         10.4.8.18    50627                                     443 → 50627 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
2021-02-04 13:27:41   142.250.192.42   443         10.4.8.18    50628                                     443 → 50628 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
2021-02-04 13:27:42   142.250.192.35   443         10.4.8.18    50629                                     443 → 50629 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
2021-02-04 13:27:42   172.217.166.163  443         10.4.8.18    50630                                     443 → 50630 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
2021-02-04 13:27:42   172.217.174.238  443         10.4.8.18    50631                                     443 → 50631 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
2021-02-04 13:27:43   216.58.203.3     443         10.4.8.18    50632                                     443 → 50632 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
2021-02-04 13:27:43   216.58.199.174   443         10.4.8.18    50633                                     443 → 50633 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
2021-02-04 13:27:44   35.244.233.98    443         10.4.8.18    50634                                     443 → 50634 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
2021-02-04 13:27:44   172.67.158.42    443         10.4.8.18    50635                                     443 → 50635 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
2021-02-04 13:27:44   142.250.183.130  443         10.4.8.18    50636                                     443 → 50636 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
2021-02-04 13:27:44   142.250.182.206  443         10.4.8.18    50637                                     443 → 50637 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
2021-02-04 13:27:44   23.202.33.58     443         10.4.8.18    50638                                     443 → 50638 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
2021-02-04 13:27:44   23.15.195.45     443         10.4.8.18    50639                                     443 → 50639 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
2021-02-04 13:27:44   172.217.167.161  443         10.4.8.18    50640                                     443 → 50640 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
2021-02-04 13:27:44   142.250.77.46    443         10.4.8.18    50641                                     443 → 50641 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
```

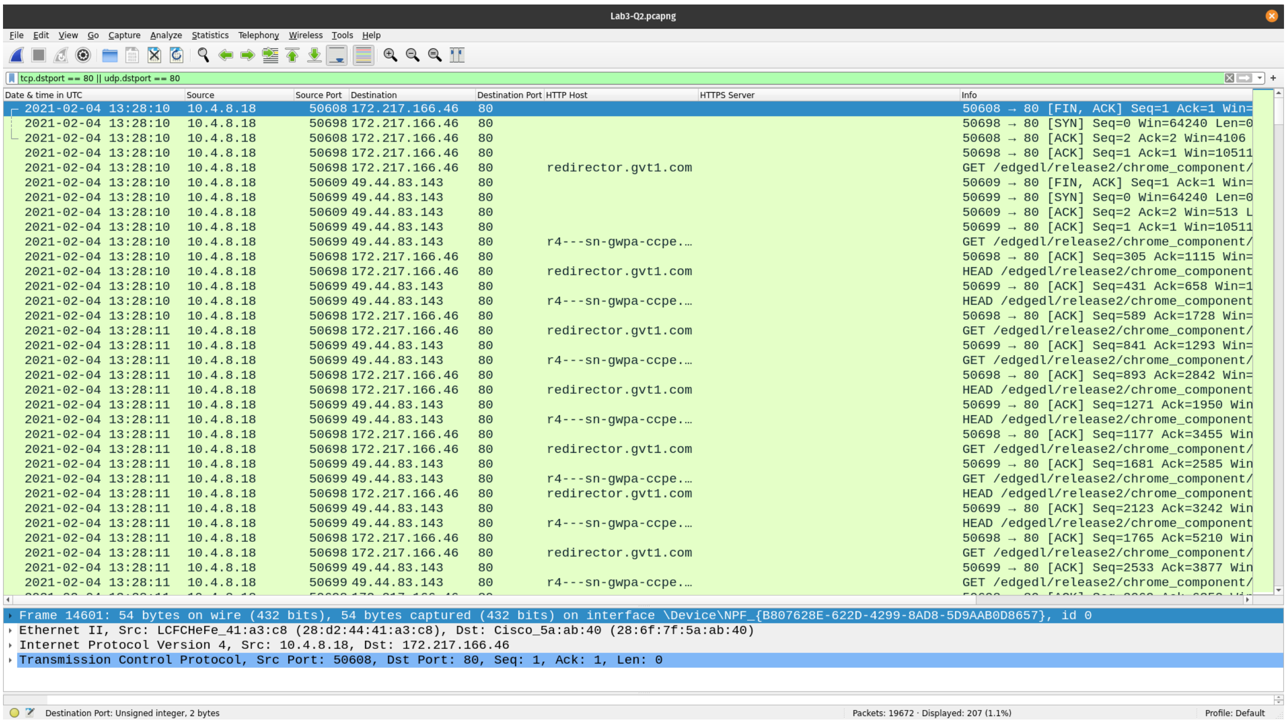
```
› Frame 8: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{B807628E-622D-4299-8AD8-5D9AAB0D8657}, id 0
› Ethernet II, Src: Cisco_5a:ab:40 (28:6f:7f:5a:ab:40), Dst: LCFCHeFe_41:a3:c8 (28:d2:44:41:a3:c8)
› Internet Protocol Version 4, Src: 137.116.139.120, Dst: 10.4.8.18
› Transmission Control Protocol, Src Port: 443, Dst Port: 50610, Seq: 0, Ack: 1, Len: 0
```

```
Frame (frame), 66 bytes          Packets: 19672 · Displayed: 115 (0.6%)          Profile: Default
```

e. List out the TCP and UDP packets where destination port=80.

```
tcp.dstport == 80 || udp.dstport == 80
```

- `.dstport` is used to get the destination port of the packet.
- `==` logical operator is used to compare values.


Lab3-Q2.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
tcp.dstport == 80 || udp.dstport == 80
```

```
Date & time in UTC    Source      Source Port Destination     Destination Port HTTP Host               HTTPS Server  Info
2021-02-04 13:28:10   10.4.8.18   50608 172.217.166.46  80                                                           50608 → 80 [FIN, ACK] Seq=1 Ack=1 Win=
2021-02-04 13:28:10   10.4.8.18   50698 172.217.166.46  80                                                           50698 → 80 [SYN] Seq=0 Win=64240 Len=0
2021-02-04 13:28:10   10.4.8.18   50608 172.217.166.46  80                                                           50608 → 80 [ACK] Seq=2 Ack=2 Win=4106
2021-02-04 13:28:10   10.4.8.18   50698 172.217.166.46  80                                                           50698 → 80 [ACK] Seq=1 Ack=1 Win=10511
2021-02-04 13:28:10   10.4.8.18   50698 172.217.166.46  80               redirector.gvt1.com                         GET /edgedl/release2/chrome_component/
2021-02-04 13:28:10   10.4.8.18   50609 49.44.83.143    80                                                           50609 → 80 [FIN, ACK] Seq=1 Ack=1 Win=
2021-02-04 13:28:10   10.4.8.18   50699 49.44.83.143    80                                                           50699 → 80 [SYN] Seq=0 Win=64240 Len=0
2021-02-04 13:28:10   10.4.8.18   50609 49.44.83.143    80                                                           50609 → 80 [ACK] Seq=2 Ack=2 Win=513 L
2021-02-04 13:28:10   10.4.8.18   50699 49.44.83.143    80                                                           50699 → 80 [ACK] Seq=1 Ack=1 Win=10511
2021-02-04 13:28:10   10.4.8.18   50699 49.44.83.143    80               r4---sn-gwpa-ccpe.…                         GET /edgedl/release2/chrome_component/
2021-02-04 13:28:10   10.4.8.18   50698 172.217.166.46  80                                                           50698 → 80 [ACK] Seq=305 Ack=1115 Win=
2021-02-04 13:28:10   10.4.8.18   50698 172.217.166.46  80               redirector.gvt1.com                         HEAD /edgedl/release2/chrome_component
2021-02-04 13:28:10   10.4.8.18   50699 49.44.83.143    80                                                           50699 → 80 [ACK] Seq=431 Ack=658 Win=1
2021-02-04 13:28:10   10.4.8.18   50699 49.44.83.143    80               r4---sn-gwpa-ccpe.…                         HEAD /edgedl/release2/chrome_component
2021-02-04 13:28:10   10.4.8.18   50698 172.217.166.46  80                                                           50698 → 80 [ACK] Seq=589 Ack=1728 Win=
2021-02-04 13:28:11   10.4.8.18   50698 172.217.166.46  80               redirector.gvt1.com                         GET /edgedl/release2/chrome_component/
2021-02-04 13:28:11   10.4.8.18   50699 49.44.83.143    80                                                           50699 → 80 [ACK] Seq=841 Ack=1293 Win=
2021-02-04 13:28:11   10.4.8.18   50699 49.44.83.143    80               r4---sn-gwpa-ccpe.…                         GET /edgedl/release2/chrome_component/
2021-02-04 13:28:11   10.4.8.18   50698 172.217.166.46  80                                                           50698 → 80 [ACK] Seq=893 Ack=2842 Win=
2021-02-04 13:28:11   10.4.8.18   50698 172.217.166.46  80               redirector.gvt1.com                         HEAD /edgedl/release2/chrome_component
2021-02-04 13:28:11   10.4.8.18   50699 49.44.83.143    80                                                           50699 → 80 [ACK] Seq=1271 Ack=1950 Win
2021-02-04 13:28:11   10.4.8.18   50699 49.44.83.143    80               r4---sn-gwpa-ccpe.…                         HEAD /edgedl/release2/chrome_component
2021-02-04 13:28:11   10.4.8.18   50698 172.217.166.46  80                                                           50698 → 80 [ACK] Seq=1177 Ack=3455 Win
2021-02-04 13:28:11   10.4.8.18   50698 172.217.166.46  80               redirector.gvt1.com                         GET /edgedl/release2/chrome_component/
2021-02-04 13:28:11   10.4.8.18   50699 49.44.83.143    80                                                           50699 → 80 [ACK] Seq=1681 Ack=2585 Win
2021-02-04 13:28:11   10.4.8.18   50699 49.44.83.143    80               r4---sn-gwpa-ccpe.…                         GET /edgedl/release2/chrome_component/
2021-02-04 13:28:11   10.4.8.18   50698 172.217.166.46  80               redirector.gvt1.com                         HEAD /edgedl/release2/chrome_component
2021-02-04 13:28:11   10.4.8.18   50699 49.44.83.143    80                                                           50699 → 80 [ACK] Seq=2123 Ack=3242 Win
2021-02-04 13:28:11   10.4.8.18   50699 49.44.83.143    80               r4---sn-gwpa-ccpe.…                         HEAD /edgedl/release2/chrome_component
2021-02-04 13:28:11   10.4.8.18   50698 172.217.166.46  80                                                           50698 → 80 [ACK] Seq=1765 Ack=5210 Win
2021-02-04 13:28:11   10.4.8.18   50698 172.217.166.46  80               redirector.gvt1.com                         GET /edgedl/release2/chrome_component/
2021-02-04 13:28:11   10.4.8.18   50699 49.44.83.143    80                                                           50699 → 80 [ACK] Seq=2533 Ack=3877 Win
2021-02-04 13:28:11   10.4.8.18   50699 49.44.83.143    80               r4---sn-gwpa-ccpe.…                         GET /edgedl/release2/chrome_component/
```

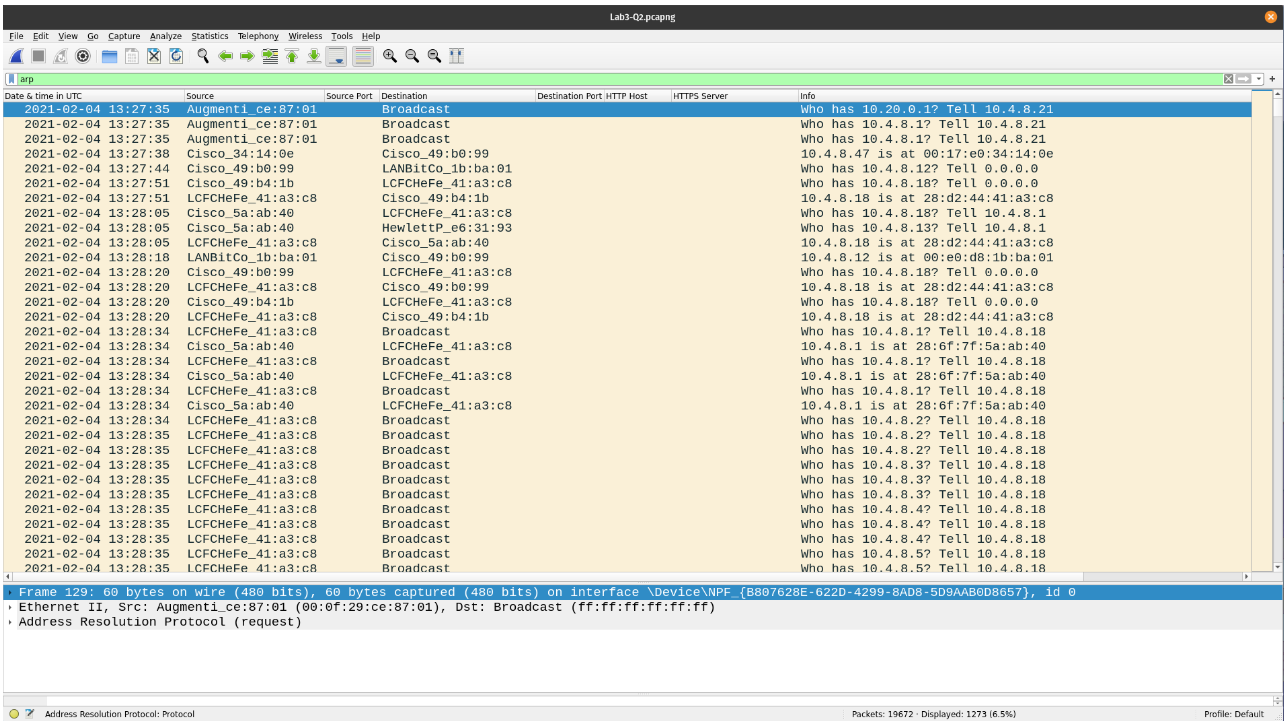
```
› Frame 14601: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{B807628E-622D-4299-8AD8-5D9AAB0D8657}, id 0
› Ethernet II, Src: LCFCHeFe_41:a3:c8 (28:d2:44:41:a3:c8), Dst: Cisco_5a:ab:40 (28:6f:7f:5a:ab:40)
› Internet Protocol Version 4, Src: 10.4.8.18, Dst: 172.217.166.46
› Transmission Control Protocol, Src Port: 50608, Dst Port: 80, Seq: 1, Ack: 1, Len: 0
```

```
Destination Port: Unsigned integer, 2 bytes          Packets: 19672 · Displayed: 207 (1.1%)          Profile: Default
```

f. List out the ARP packets.

```
arp
```

- ARP is used to dynamically build and maintain a mapping database between link local layer 2 addresses and layer 3 addresses. In the common case this table is for mapping Ethernet to IP addresses. This database is called the ARP_Table.
- Dynamic entries in this table are often cached with a timeout of up to 15 minutes, which means that once a host has ARPed for an IP address it will remember this for the next 15 minutes before it gets time to ARP for that address again.
- `arp` filter is used to show only the ARP based traffic:


Lab3-Q2.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

arp

Date & time in UTC	Source	Source Port	Destination	Destination Port	HTTP Host	HTTPS Server	Info
2021-02-04 13:27:35	Augmenti_ce:87:01		Broadcast				Who has 10.20.0.1? Tell 10.4.8.21
2021-02-04 13:27:35	Augmenti_ce:87:01		Broadcast				Who has 10.4.8.1? Tell 10.4.8.21
2021-02-04 13:27:35	Augmenti_ce:87:01		Broadcast				Who has 10.4.8.1? Tell 10.4.8.21
2021-02-04 13:27:38	Cisco_34:14:0e		Cisco_49:b0:99				10.4.8.47 is at 00:17:e0:34:14:0e
2021-02-04 13:27:44	Cisco_49:b0:99		LANBitCo_1b:ba:01				Who has 10.4.8.12? Tell 0.0.0.0
2021-02-04 13:27:51	Cisco_49:b4:1b		LCFCHeFe_41:a3:c8				Who has 10.4.8.18? Tell 0.0.0.0
2021-02-04 13:27:51	LCFCHeFe_41:a3:c8		Cisco_49:b4:1b				10.4.8.18 is at 28:d2:44:41:a3:c8
2021-02-04 13:28:05	Cisco_5a:ab:40		LCFCHeFe_41:a3:c8				Who has 10.4.8.18? Tell 10.4.8.1
2021-02-04 13:28:05	Cisco_5a:ab:40		HewlettP_e6:31:93				Who has 10.4.8.13? Tell 10.4.8.1
2021-02-04 13:28:05	LCFCHeFe_41:a3:c8		Cisco_5a:ab:40				10.4.8.18 is at 28:d2:44:41:a3:c8
2021-02-04 13:28:18	LANBitCo_1b:ba:01		Cisco_49:b0:99				10.4.8.12 is at 00:e0:d8:1b:ba:01
2021-02-04 13:28:20	Cisco_49:b0:99		LCFCHeFe_41:a3:c8				Who has 10.4.8.18? Tell 0.0.0.0
2021-02-04 13:28:20	LCFCHeFe_41:a3:c8		Cisco_49:b0:99				10.4.8.18 is at 28:d2:44:41:a3:c8
2021-02-04 13:28:20	Cisco_49:b4:1b		LCFCHeFe_41:a3:c8				Who has 10.4.8.18? Tell 0.0.0.0
2021-02-04 13:28:20	LCFCHeFe_41:a3:c8		Cisco_49:b4:1b				10.4.8.18 is at 28:d2:44:41:a3:c8
2021-02-04 13:28:34	LCFCHeFe_41:a3:c8		Broadcast				Who has 10.4.8.1? Tell 10.4.8.18
2021-02-04 13:28:34	Cisco_5a:ab:40		LCFCHeFe_41:a3:c8				10.4.8.1 is at 28:6f:7f:5a:ab:40
2021-02-04 13:28:34	LCFCHeFe_41:a3:c8		Broadcast				Who has 10.4.8.1? Tell 10.4.8.18
2021-02-04 13:28:34	Cisco_5a:ab:40		LCFCHeFe_41:a3:c8				10.4.8.1 is at 28:6f:7f:5a:ab:40
2021-02-04 13:28:34	LCFCHeFe_41:a3:c8		Broadcast				Who has 10.4.8.1? Tell 10.4.8.18
2021-02-04 13:28:34	Cisco_5a:ab:40		LCFCHeFe_41:a3:c8				10.4.8.1 is at 28:6f:7f:5a:ab:40
2021-02-04 13:28:34	LCFCHeFe_41:a3:c8		Broadcast				Who has 10.4.8.2? Tell 10.4.8.18
2021-02-04 13:28:35	LCFCHeFe_41:a3:c8		Broadcast				Who has 10.4.8.2? Tell 10.4.8.18
2021-02-04 13:28:35	LCFCHeFe_41:a3:c8		Broadcast				Who has 10.4.8.2? Tell 10.4.8.18
2021-02-04 13:28:35	LCFCHeFe_41:a3:c8		Broadcast				Who has 10.4.8.3? Tell 10.4.8.18
2021-02-04 13:28:35	LCFCHeFe_41:a3:c8		Broadcast				Who has 10.4.8.3? Tell 10.4.8.18
2021-02-04 13:28:35	LCFCHeFe_41:a3:c8		Broadcast				Who has 10.4.8.3? Tell 10.4.8.18
2021-02-04 13:28:35	LCFCHeFe_41:a3:c8		Broadcast				Who has 10.4.8.4? Tell 10.4.8.18
2021-02-04 13:28:35	LCFCHeFe_41:a3:c8		Broadcast				Who has 10.4.8.4? Tell 10.4.8.18
2021-02-04 13:28:35	LCFCHeFe_41:a3:c8		Broadcast				Who has 10.4.8.4? Tell 10.4.8.18
2021-02-04 13:28:35	LCFCHeFe_41:a3:c8		Broadcast				Who has 10.4.8.5? Tell 10.4.8.18
2021-02-04 13:28:35	LCFCHeFe_41:a3:c8		Broadcast				Who has 10.4.8.5? Tell 10.4.8.18

```
› Frame 129: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{B807628E-622D-4299-8AD8-5D9AAB0D8657}, id 0
› Ethernet II, Src: Augmenti_ce:87:01 (00:0f:29:ce:87:01), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
› Address Resolution Protocol (request)
```

Address Resolution Protocol: Protocol   Packets: 19672 · Displayed: 1273 (6.5%)   Profile: Default