ROHIT GARG(2018A7PS0193G)

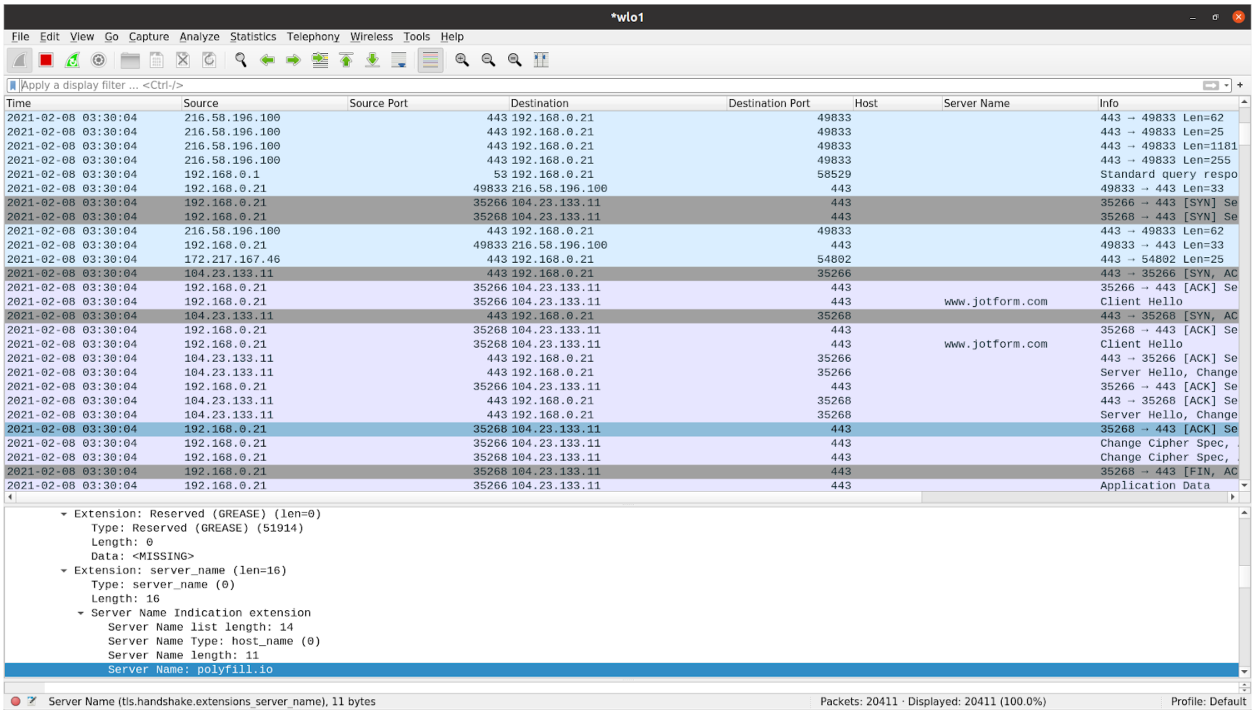
COMPUTER NETWORKS
CS F303
Lab-3

Q1. Customize your Wireshark - (6 marks)

Generally, WireShark columns are arranged in the following order (which you can observe on your machine) - No. , Time, Source, Destination, Protocol, Length. etc. Being a security expert you have to arrange the WireShark display in such a way that it must have only the following items (1 mark per correct display item with the correct filter/field value and a screenshot).
a. Date & time in UTC
b. Source IP and source port
c. Destination IP and destination port
d. HTTP host
e. HTTPS server
f. Info

Ans1. Steps involved:

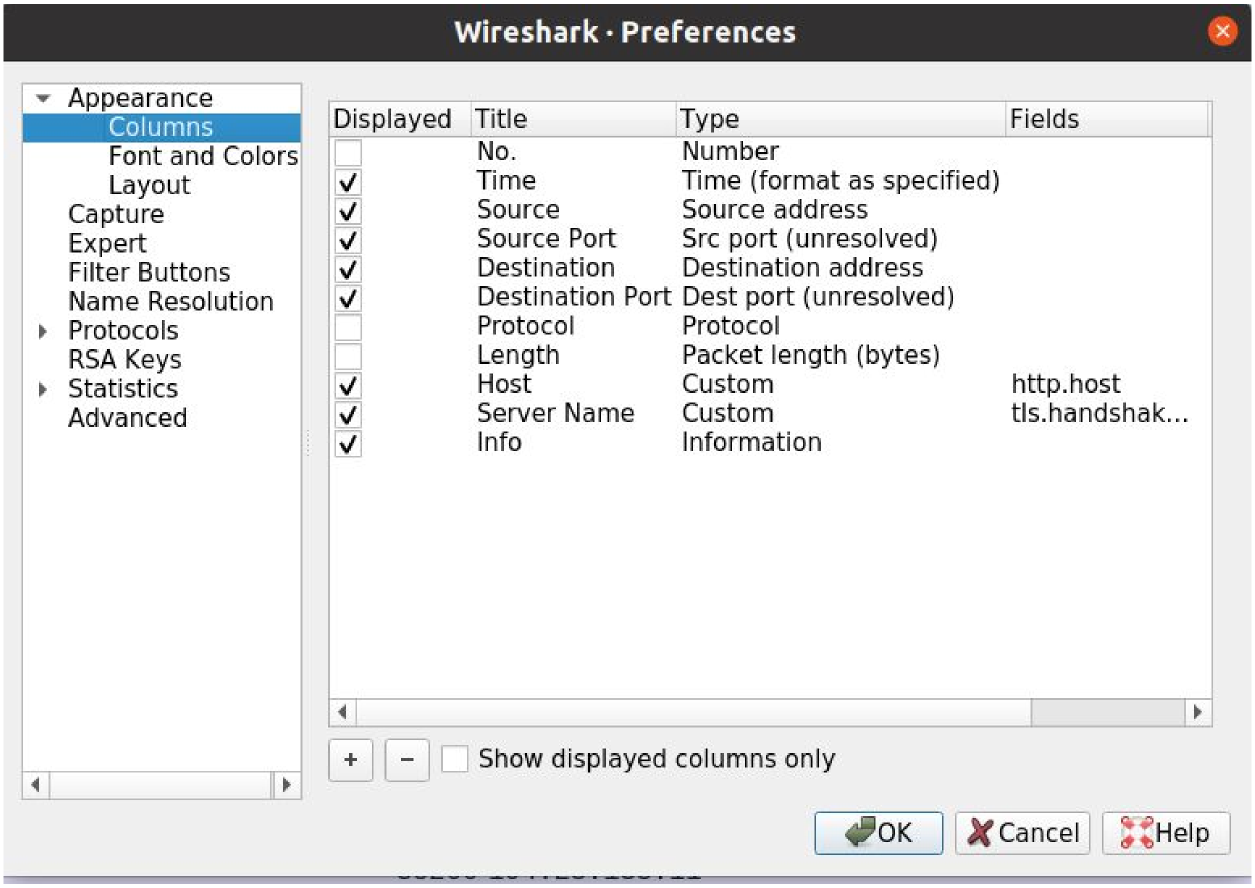
1) Changing the format of Time column to UTC Date and Time(Seconds) Format.
2) Hiding and removing columns that we don't want. For this, No., Protocol, and Length columns have been unchecked and hidden.
3) Adding HTTP Host and HTTPS Servers Columns as custom columns by using http.request and tls.handshake.type == 1 as filters.


*wlo1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

Time	Source	Source Port	Destination	Destination Port	Host	Server Name	Info
2021-02-08 03:30:04	216.58.196.100	443	192.168.0.21	49833			443 → 49833 Len=62
2021-02-08 03:30:04	216.58.196.100	443	192.168.0.21	49833			443 → 49833 Len=25
2021-02-08 03:30:04	216.58.196.100	443	192.168.0.21	49833			443 → 49833 Len=1181
2021-02-08 03:30:04	216.58.196.100	443	192.168.0.21	49833			443 → 49833 Len=255
2021-02-08 03:30:04	192.168.0.1	53	192.168.0.21	58529			Standard query respo
2021-02-08 03:30:04	192.168.0.21	49833	216.58.196.100	443			49833 → 443 Len=33
2021-02-08 03:30:04	192.168.0.21	35266	104.23.133.11	443			35266 → 443 [SYN] Se
2021-02-08 03:30:04	192.168.0.21	35268	104.23.133.11	443			35268 → 443 [SYN] Se
2021-02-08 03:30:04	216.58.196.100	443	192.168.0.21	49833			443 → 49833 Len=62
2021-02-08 03:30:04	192.168.0.21	49833	216.58.196.100	443			49833 → 443 Len=33
2021-02-08 03:30:04	172.217.167.46	443	192.168.0.21	54802			443 → 54802 Len=25
2021-02-08 03:30:04	104.23.133.11	443	192.168.0.21	35266			443 → 35266 [SYN, AC
2021-02-08 03:30:04	192.168.0.21	35266	104.23.133.11	443			35266 → 443 [ACK] Se
2021-02-08 03:30:04	192.168.0.21	35266	104.23.133.11	443		www.jotform.com	Client Hello
2021-02-08 03:30:04	104.23.133.11	443	192.168.0.21	35268			443 → 35268 [SYN, AC
2021-02-08 03:30:04	192.168.0.21	35268	104.23.133.11	443			35268 → 443 [ACK] Se
2021-02-08 03:30:04	192.168.0.21	35268	104.23.133.11	443		www.jotform.com	Client Hello
2021-02-08 03:30:04	104.23.133.11	443	192.168.0.21	35266			443 → 35266 [ACK] Se
2021-02-08 03:30:04	104.23.133.11	443	192.168.0.21	35266			Server Hello, Change
2021-02-08 03:30:04	192.168.0.21	35266	104.23.133.11	443			35266 → 443 [ACK] Se
2021-02-08 03:30:04	104.23.133.11	443	192.168.0.21	35268			443 → 35268 [ACK] Se
2021-02-08 03:30:04	104.23.133.11	443	192.168.0.21	35268			Server Hello, Change
2021-02-08 03:30:04	192.168.0.21	35268	104.23.133.11	443			35268 → 443 [ACK] Se
2021-02-08 03:30:04	192.168.0.21	35266	104.23.133.11	443			Change Cipher Spec,
2021-02-08 03:30:04	192.168.0.21	35268	104.23.133.11	443			Change Cipher Spec,
2021-02-08 03:30:04	192.168.0.21	35268	104.23.133.11	443			35268 → 443 [FIN, AC
2021-02-08 03:30:04	192.168.0.21	35266	104.23.133.11	443			Application Data

```
    ▾ Extension: Reserved (GREASE) (len=0)
        Type: Reserved (GREASE) (51914)
        Length: 0
        Data: <MISSING>
    ▾ Extension: server_name (len=16)
        Type: server_name (0)
        Length: 16
      ▾ Server Name Indication extension
          Server Name list length: 14
          Server Name Type: host_name (0)
          Server Name length: 11
          Server Name: polyfill.io
```

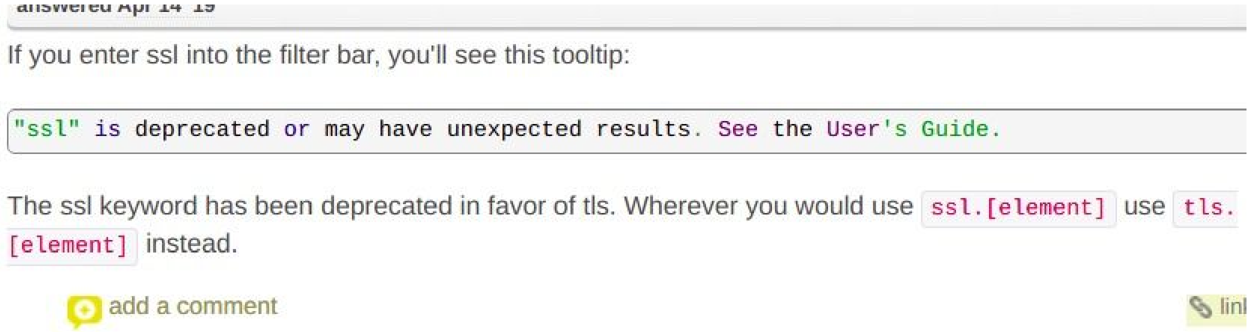
Server Name (tls.handshake.extensions_server_name), 11 bytes   Packets: 20411 · Displayed: 20411 (100.0%)   Profile: Default



Displayed	Title	Type	Fields
☐	No.	Number	
☑	Time	Time (format as specified)	
☑	Source	Source address	
☑	Source Port	Src port (unresolved)	
☑	Destination	Destination address	
☑	Destination Port	Dest port (unresolved)	
☐	Protocol	Protocol	
☐	Length	Packet length (bytes)	
☑	Host	Custom	http.host
☑	Server Name	Custom	tls.handshak...
☑	Info	Information	

☐ Show displayed columns only

Note: ssl has been deprecated and hence tls.handshake.type == 1 has been used instead of ssl.handshake.type == 1



answered Apr 14 '19

If you enter ssl into the filter bar, you'll see this tooltip:

```
"ssl" is deprecated or may have unexpected results. See the User's Guide.
```

The ssl keyword has been deprecated in favor of tls. Wherever you would use `ssl.[element]` use `tls.[element]` instead.

add a comment

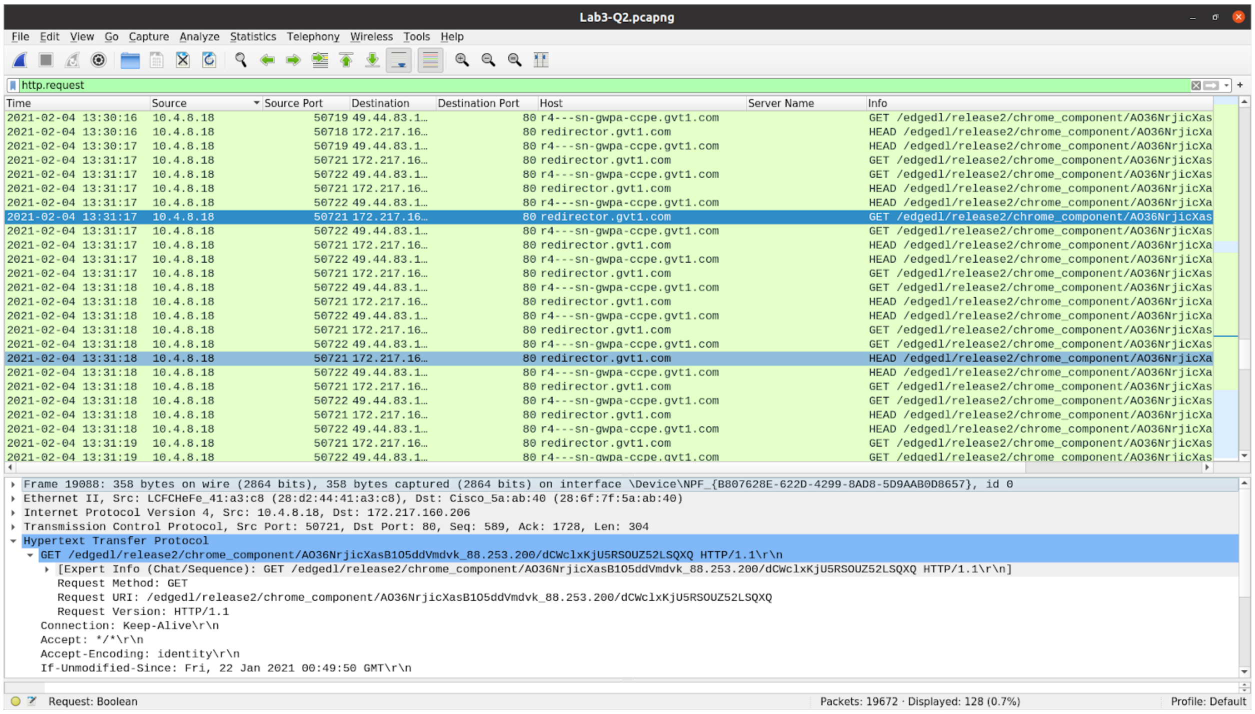
Q2. Wireshark dump analysis - (24 marks)

Using the given Lab3-Q2.pcapng, file answer the following questions. You have to write down the filter you have used (2 marks) and attach a screenshot and explain your output (2 marks).

Ans 2.

a. Identify the http request packet

a. http.request



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

http.request

```
Time                 Source      Source Port Destination    Destination Port Host                       Server Name  Info
2021-02-04 13:30:16  10.4.8.18         50719 49.44.83.1…    80 r4---sn-gwpa-ccpe.gvt1.com            GET /edgedl/release2/chrome_component/AO36NrjicXas
2021-02-04 13:30:16  10.4.8.18         50718 172.217.16…    80 redirector.gvt1.com                   HEAD /edgedl/release2/chrome_component/AO36NrjicXa
2021-02-04 13:30:17  10.4.8.18         50719 49.44.83.1…    80 r4---sn-gwpa-ccpe.gvt1.com            HEAD /edgedl/release2/chrome_component/AO36NrjicXa
2021-02-04 13:31:17  10.4.8.18         50721 172.217.16…    80 redirector.gvt1.com                   GET /edgedl/release2/chrome_component/AO36NrjicXas
2021-02-04 13:31:17  10.4.8.18         50722 49.44.83.1…    80 r4---sn-gwpa-ccpe.gvt1.com            GET /edgedl/release2/chrome_component/AO36NrjicXas
2021-02-04 13:31:17  10.4.8.18         50721 172.217.16…    80 redirector.gvt1.com                   HEAD /edgedl/release2/chrome_component/AO36NrjicXa
2021-02-04 13:31:17  10.4.8.18         50722 49.44.83.1…    80 r4---sn-gwpa-ccpe.gvt1.com            HEAD /edgedl/release2/chrome_component/AO36NrjicXa
2021-02-04 13:31:17  10.4.8.18         50721 172.217.16…    80 redirector.gvt1.com                   GET /edgedl/release2/chrome_component/AO36NrjicXas
2021-02-04 13:31:17  10.4.8.18         50722 49.44.83.1…    80 r4---sn-gwpa-ccpe.gvt1.com            GET /edgedl/release2/chrome_component/AO36NrjicXas
2021-02-04 13:31:17  10.4.8.18         50721 172.217.16…    80 redirector.gvt1.com                   HEAD /edgedl/release2/chrome_component/AO36NrjicXa
2021-02-04 13:31:17  10.4.8.18         50722 49.44.83.1…    80 r4---sn-gwpa-ccpe.gvt1.com            HEAD /edgedl/release2/chrome_component/AO36NrjicXa
2021-02-04 13:31:17  10.4.8.18         50721 172.217.16…    80 redirector.gvt1.com                   GET /edgedl/release2/chrome_component/AO36NrjicXas
2021-02-04 13:31:18  10.4.8.18         50722 49.44.83.1…    80 r4---sn-gwpa-ccpe.gvt1.com            GET /edgedl/release2/chrome_component/AO36NrjicXas
2021-02-04 13:31:18  10.4.8.18         50721 172.217.16…    80 redirector.gvt1.com                   HEAD /edgedl/release2/chrome_component/AO36NrjicXa
2021-02-04 13:31:18  10.4.8.18         50722 49.44.83.1…    80 r4---sn-gwpa-ccpe.gvt1.com            HEAD /edgedl/release2/chrome_component/AO36NrjicXa
2021-02-04 13:31:18  10.4.8.18         50721 172.217.16…    80 redirector.gvt1.com                   GET /edgedl/release2/chrome_component/AO36NrjicXas
2021-02-04 13:31:18  10.4.8.18         50722 49.44.83.1…    80 r4---sn-gwpa-ccpe.gvt1.com            GET /edgedl/release2/chrome_component/AO36NrjicXas
2021-02-04 13:31:18  10.4.8.18         50721 172.217.16…    80 redirector.gvt1.com                   HEAD /edgedl/release2/chrome_component/AO36NrjicXa
2021-02-04 13:31:18  10.4.8.18         50722 49.44.83.1…    80 r4---sn-gwpa-ccpe.gvt1.com            HEAD /edgedl/release2/chrome_component/AO36NrjicXa
2021-02-04 13:31:18  10.4.8.18         50721 172.217.16…    80 redirector.gvt1.com                   GET /edgedl/release2/chrome_component/AO36NrjicXas
2021-02-04 13:31:18  10.4.8.18         50722 49.44.83.1…    80 r4---sn-gwpa-ccpe.gvt1.com            GET /edgedl/release2/chrome_component/AO36NrjicXas
2021-02-04 13:31:18  10.4.8.18         50721 172.217.16…    80 redirector.gvt1.com                   HEAD /edgedl/release2/chrome_component/AO36NrjicXa
2021-02-04 13:31:18  10.4.8.18         50722 49.44.83.1…    80 r4---sn-gwpa-ccpe.gvt1.com            HEAD /edgedl/release2/chrome_component/AO36NrjicXa
2021-02-04 13:31:19  10.4.8.18         50721 172.217.16…    80 redirector.gvt1.com                   GET /edgedl/release2/chrome_component/AO36NrjicXas
2021-02-04 13:31:19  10.4.8.18         50722 49.44.83.1…    80 r4---sn-gwpa-ccpe.gvt1.com            GET /edgedl/release2/chrome_component/AO36NrjicXas
```

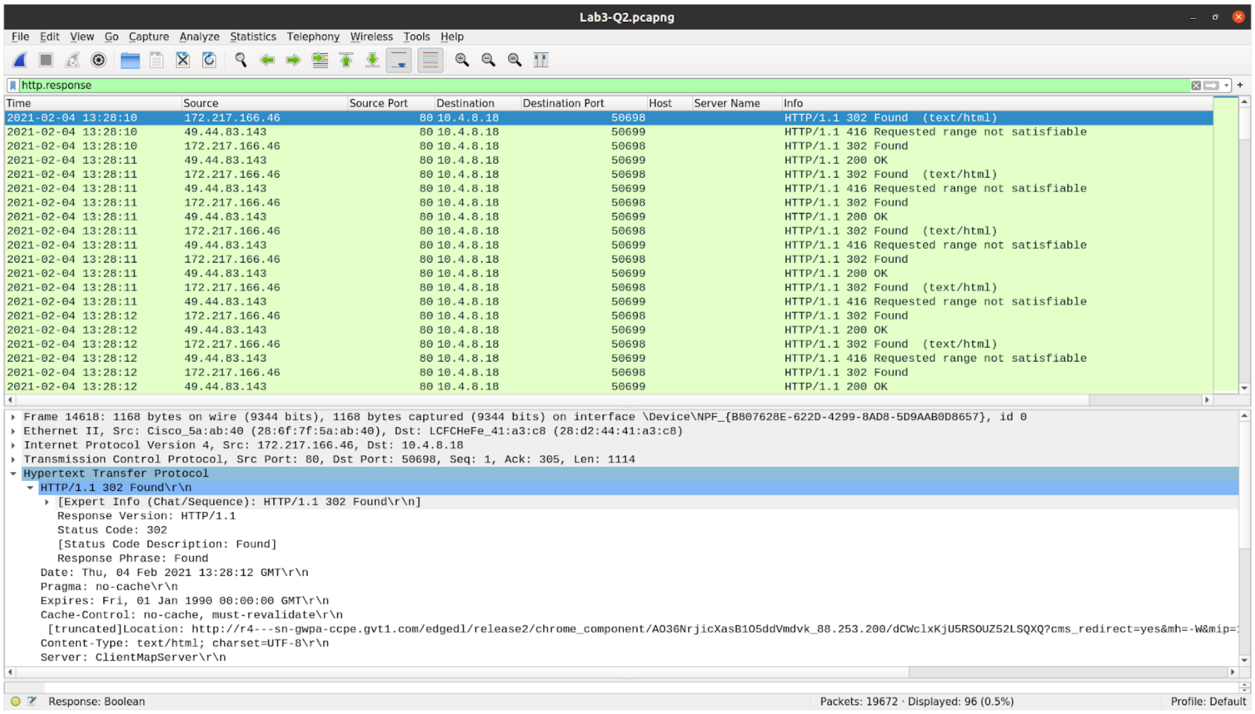
```
› Frame 19088: 358 bytes on wire (2864 bits), 358 bytes captured (2864 bits) on interface \Device\NPF_{B807628E-622D-4299-8AD8-5D9AAB0D8657}, id 0
› Ethernet II, Src: LCFCHeFe_41:a3:c8 (28:d2:44:41:a3:c8), Dst: Cisco_5a:ab:40 (28:6f:7f:5a:ab:40)
› Internet Protocol Version 4, Src: 10.4.8.18, Dst: 172.217.160.206
› Transmission Control Protocol, Src Port: 50721, Dst Port: 80, Seq: 589, Ack: 1728, Len: 304
⌄ Hypertext Transfer Protocol
  ⌄ GET /edgedl/release2/chrome_component/AO36NrjicXasB105ddVmdvk_88.253.200/dCWclxKjU5RSOUZ52LSQXQ HTTP/1.1\r\n
    › [Expert Info (Chat/Sequence): GET /edgedl/release2/chrome_component/AO36NrjicXasB105ddVmdvk_88.253.200/dCWclxKjU5RSOUZ52LSQXQ HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /edgedl/release2/chrome_component/AO36NrjicXasB105ddVmdvk_88.253.200/dCWclxKjU5RSOUZ52LSQXQ
      Request Version: HTTP/1.1
    Connection: Keep-Alive\r\n
    Accept: */*\r\n
    Accept-Encoding: identity\r\n
    If-Unmodified-Since: Fri, 22 Jan 2021 00:49:50 GMT\r\n
```

Request: Boolean   Packets: 19672 · Displayed: 128 (0.7%)   Profile: Default http.request display filter is used to filter out request packets. One such request packet has been displayed. The request consists of Request Method, URI, Info and Version.

Note: One can specifically use http.request.method ==”GET” inorder to filter out GET requests. I have used http.request since requests can be of different types: GET, PUT etc..

b. Identify the http response packet

http.response



http.response

Time	Source	Source Port	Destination	Destination Port	Host	Server Name	Info
2021-02-04 13:28:10	172.217.166.46	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 satisfiable
2021-02-04 13:28:10	172.217.166.46	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	172.217.166.46	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 satisfiable
2021-02-04 13:28:11	172.217.166.46	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	172.217.166.46	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 satisfiable
2021-02-04 13:28:11	172.217.166.46	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	172.217.166.46	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 satisfiable
2021-02-04 13:28:12	172.217.166.46	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	172.217.166.46	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 satisfiable
2021-02-04 13:28:12	172.217.166.46	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

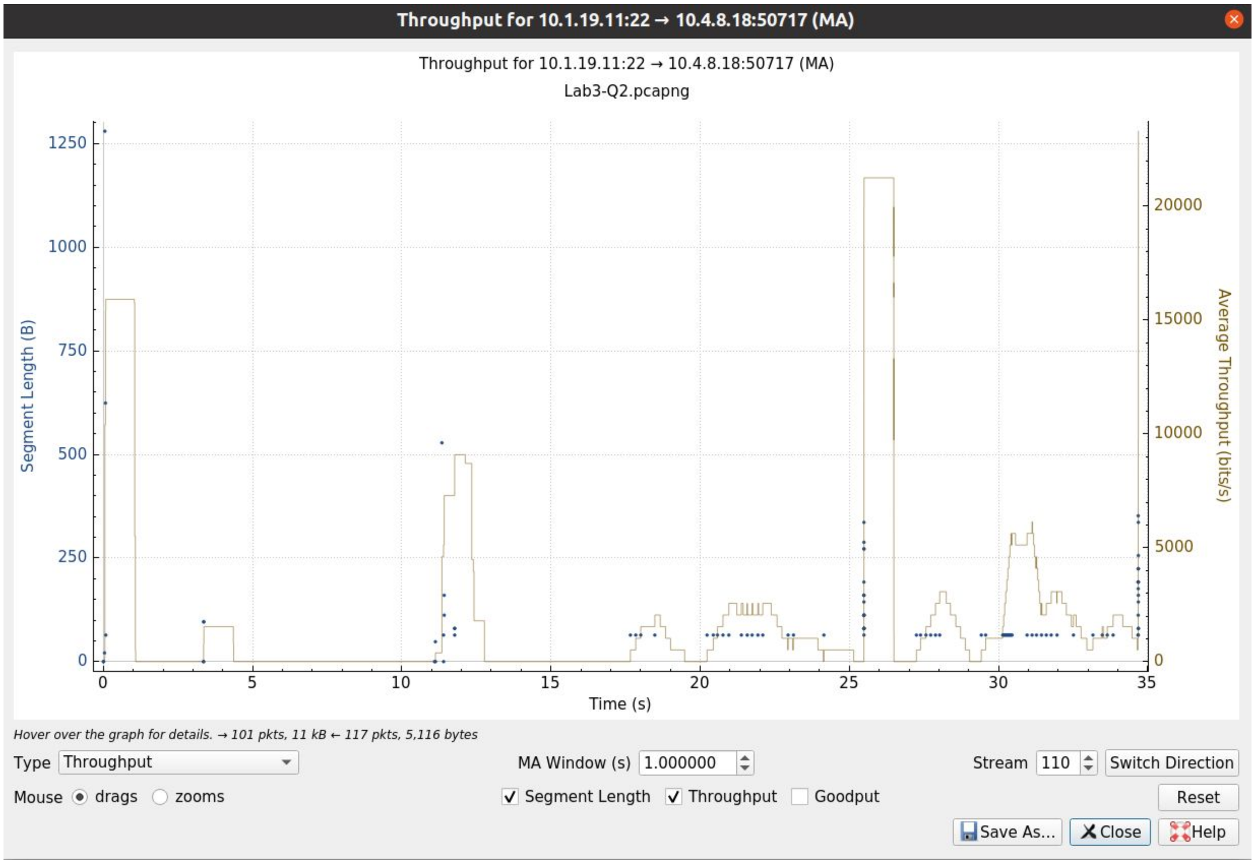
```
Frame 14618: 1168 bytes on wire (9344 bits), 1168 bytes captured (9344 bits) on interface \Device\NPF_{B807628E-622D-4299-8AD8-5D9AAB0D8657}, id 0
Ethernet II, Src: Cisco_5a:ab:40 (28:6f:7f:5a:ab:40), Dst: LCFCHeFe_41:a3:c8 (28:d2:44:41:a3:c8)
Internet Protocol Version 4, Src: 172.217.166.46, Dst: 10.4.8.18
Transmission Control Protocol, Src Port: 80, Dst Port: 50698, Seq: 1, Ack: 305, Len: 1114
Hypertext Transfer Protocol
  HTTP/1.1 302 Found\r\n
    [Expert Info (Chat/Sequence): HTTP/1.1 302 Found\r\n]
    Response Version: HTTP/1.1
    Status Code: 302
    [Status Code Description: Found]
    Response Phrase: Found
  Date: Thu, 04 Feb 2021 13:28:12 GMT\r\n
  Pragma: no-cache\r\n
  Expires: Fri, 01 Jan 1990 00:00:00 GMT\r\n
  Cache-Control: no-cache, must-revalidate\r\n
   [truncated]Location: http://r4---sn-gwpa-ccpe.gvt1.com/edgedl/release2/chrome_component/AO36NrjicXasB1O5ddVmdvk_88.253.200/dCWclxKjU5RSOUZ52LSQXQ?cms_redirect=yes&mh=-W&mip=
  Content-Type: text/html; charset=UTF-8\r\n
  Server: ClientMapServer\r\n
```

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

The output of http.response filter indicates the responses given by the server to the host’s requests. One such packet’s details are displayed. A typical response consists of Info(Message by server), Response version, Status Code etc.

c. Display the statistics of the TCP and UDP packets

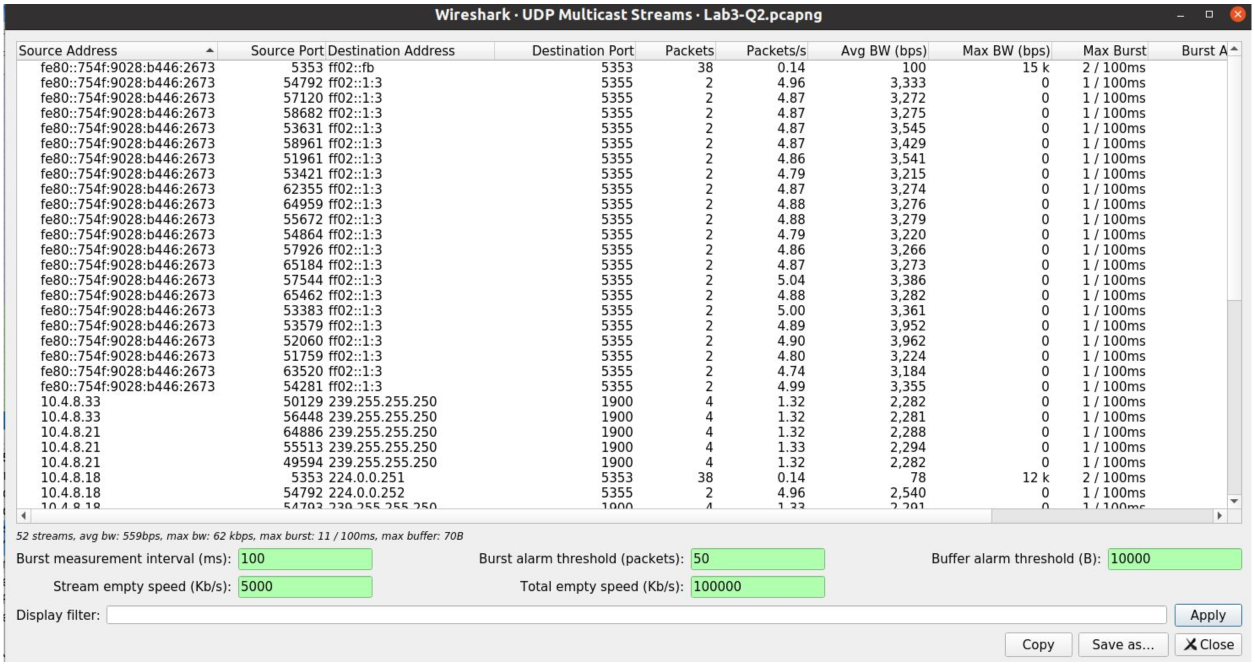
TCP Statistics: TCP Time/Sequence (tcptrace)



Hover over the graph for details. → 101 pkts, 11 kB ← 117 pkts, 5,116 bytes

Throughput graph shows the average throughput and goodput. Throughput indicates the rate of data that is transferred by the TCP protocol. This includes application payload, TCP header size and TCP retransmissions. Y-axis denotes the segment length of the selected packet and x-axis shows the time in seconds

UDP Statistics: UDP multicast streams



Source Address	Source Port	Destination Address	Destination Port	Packets	Packets/s	Avg BW (bps)	Max BW (bps)	Max Burst	Burst A
fe80::754f:9028:b446:2673	5353	ff02::fb	5353	38	0.14	100	15 k	2 / 100ms	
fe80::754f:9028:b446:2673	54792	ff02::1:3	5355	2	4.96	3,333	0	1 / 100ms	
fe80::754f:9028:b446:2673	57120	ff02::1:3	5355	2	4.87	3,272	0	1 / 100ms	
fe80::754f:9028:b446:2673	58682	ff02::1:3	5355	2	4.87	3,275	0	1 / 100ms	
fe80::754f:9028:b446:2673	53631	ff02::1:3	5355	2	4.87	3,545	0	1 / 100ms	
fe80::754f:9028:b446:2673	58961	ff02::1:3	5355	2	4.87	3,429	0	1 / 100ms	
fe80::754f:9028:b446:2673	51961	ff02::1:3	5355	2	4.86	3,541	0	1 / 100ms	
fe80::754f:9028:b446:2673	53421	ff02::1:3	5355	2	4.79	3,215	0	1 / 100ms	
fe80::754f:9028:b446:2673	62355	ff02::1:3	5355	2	4.87	3,274	0	1 / 100ms	
fe80::754f:9028:b446:2673	64959	ff02::1:3	5355	2	4.88	3,276	0	1 / 100ms	
fe80::754f:9028:b446:2673	55672	ff02::1:3	5355	2	4.88	3,279	0	1 / 100ms	
fe80::754f:9028:b446:2673	54864	ff02::1:3	5355	2	4.79	3,220	0	1 / 100ms	
fe80::754f:9028:b446:2673	57926	ff02::1:3	5355	2	4.86	3,266	0	1 / 100ms	
fe80::754f:9028:b446:2673	65184	ff02::1:3	5355	2	4.87	3,273	0	1 / 100ms	
fe80::754f:9028:b446:2673	57544	ff02::1:3	5355	2	5.04	3,386	0	1 / 100ms	
fe80::754f:9028:b446:2673	65462	ff02::1:3	5355	2	4.88	3,282	0	1 / 100ms	
fe80::754f:9028:b446:2673	53383	ff02::1:3	5355	2	5.00	3,361	0	1 / 100ms	
fe80::754f:9028:b446:2673	53579	ff02::1:3	5355	2	4.89	3,952	0	1 / 100ms	
fe80::754f:9028:b446:2673	52060	ff02::1:3	5355	2	4.90	3,962	0	1 / 100ms	
fe80::754f:9028:b446:2673	51759	ff02::1:3	5355	2	4.80	3,224	0	1 / 100ms	
fe80::754f:9028:b446:2673	63520	ff02::1:3	5355	2	4.74	3,184	0	1 / 100ms	
fe80::754f:9028:b446:2673	54281	ff02::1:3	5355	2	4.99	3,355	0	1 / 100ms	
10.4.8.33	50129	239.255.255.250	1900	4	1.32	2,282	0	1 / 100ms	
10.4.8.33	56448	239.255.255.250	1900	4	1.32	2,281	0	1 / 100ms	
10.4.8.21	64886	239.255.255.250	1900	4	1.32	2,288	0	1 / 100ms	
10.4.8.21	55513	239.255.255.250	1900	4	1.33	2,294	0	1 / 100ms	
10.4.8.21	49594	239.255.255.250	1900	4	1.32	2,282	0	1 / 100ms	
10.4.8.18	5353	224.0.0.251	5353	38	0.14	78	12 k	2 / 100ms	
10.4.8.18	54792	224.0.0.252	5355	2	4.96	2,540	0	1 / 100ms	
10.4.8.18	54793	239.255.255.250	1900	4	1.33	2,291	0	1 / 100ms	

52 streams, avg bw: 559bps, max bw: 62 kbps, max burst: 11 / 100ms, max buffer: 70B

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:

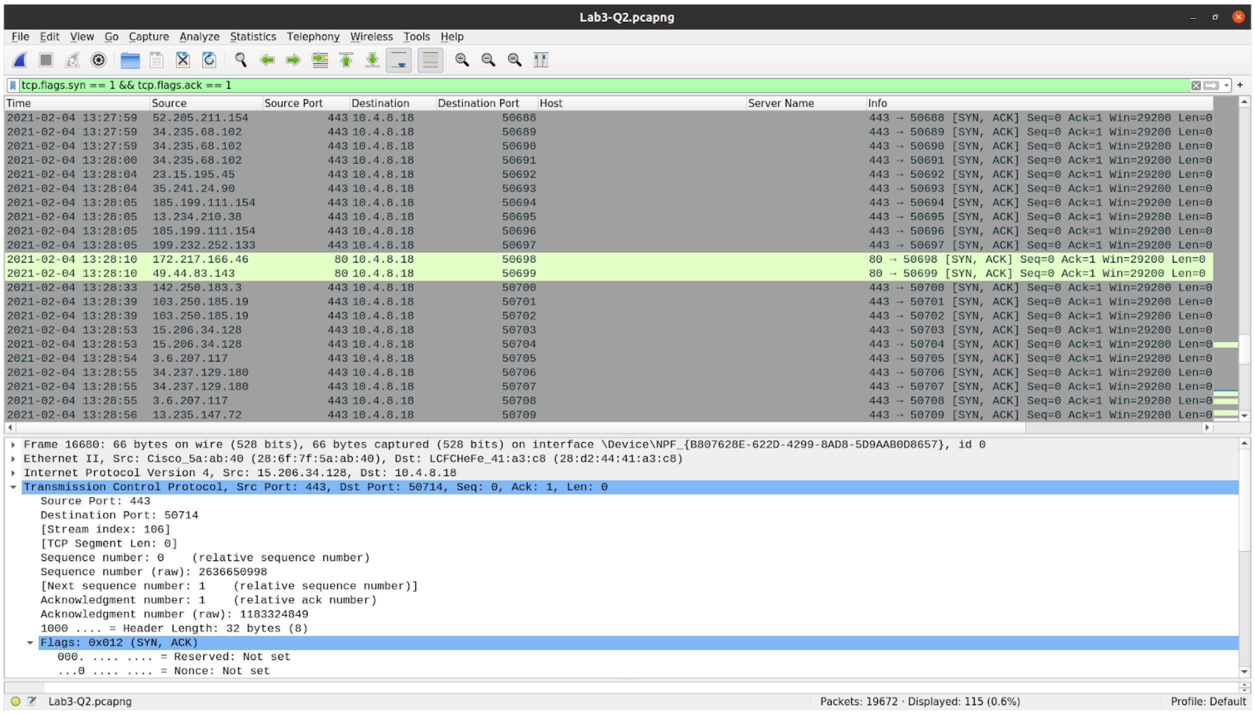
UDP Multicast Streams is used to analyse and detect multicast streams, measure how big the bursts inside video streams are (sliding window algorithm) and measure how big the output buffer should be at a certain output speed (Leaky bucket algorithm)

Output of UDP indicates:-

- Source Port, Source Address, Destination Port, Destination Address
- Packets Delivered and Rate at which they are delivered
- Max burst - the highest number of packets inside a sliding window time interval. The time interval can be specified inside the Set parameters window
- Max Bw - same as the above one, only in Mbps instead of pps
- Burst Alarms - how many times the bursts exceeded the limit set inside the Parameters dialog
- Max buffer - how big the output queue should be that no packet will be dropped at specified output speed
- Buff alarms - how many times this was not the case (the required buffer was higher than available one)

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

tcp.flags.syn == 1 && tcp.flags.ack == 1



Lab3-Q2.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.flags.syn == 1 && tcp.flags.ack == 1

Time	Source	Source Port	Destination	Destination Port	Host	Server Name	Info
2021-02-04 13:27:59	52.205.211.154	443	10.4.8.18	50688			443 → 50688 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0
2021-02-04 13:27:59	34.235.68.102	443	10.4.8.18	50689			443 → 50689 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0
2021-02-04 13:27:59	34.235.68.102	443	10.4.8.18	50690			443 → 50690 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0
2021-02-04 13:28:00	34.235.68.102	443	10.4.8.18	50691			443 → 50691 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0
2021-02-04 13:28:04	23.15.195.45	443	10.4.8.18	50692			443 → 50692 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0
2021-02-04 13:28:04	35.241.24.90	443	10.4.8.18	50693			443 → 50693 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0
2021-02-04 13:28:05	185.199.111.154	443	10.4.8.18	50694			443 → 50694 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0
2021-02-04 13:28:05	13.234.210.38	443	10.4.8.18	50695			443 → 50695 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0
2021-02-04 13:28:05	185.199.111.154	443	10.4.8.18	50696			443 → 50696 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0
2021-02-04 13:28:05	199.232.252.133	443	10.4.8.18	50697			443 → 50697 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0
2021-02-04 13:28:10	172.217.166.46	80	10.4.8.18	50698			80 → 50698 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0
2021-02-04 13:28:10	49.44.83.143	80	10.4.8.18	50699			80 → 50699 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0
2021-02-04 13:28:33	142.250.183.3	443	10.4.8.18	50700			443 → 50700 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0
2021-02-04 13:28:39	103.250.185.19	443	10.4.8.18	50701			443 → 50701 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0
2021-02-04 13:28:39	103.250.185.19	443	10.4.8.18	50702			443 → 50702 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0
2021-02-04 13:28:53	15.206.34.128	443	10.4.8.18	50703			443 → 50703 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0
2021-02-04 13:28:53	15.206.34.128	443	10.4.8.18	50704			443 → 50704 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0
2021-02-04 13:28:54	3.6.207.117	443	10.4.8.18	50705			443 → 50705 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0
2021-02-04 13:28:55	34.237.129.180	443	10.4.8.18	50706			443 → 50706 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0
2021-02-04 13:28:55	34.237.129.180	443	10.4.8.18	50707			443 → 50707 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0
2021-02-04 13:28:55	3.6.207.117	443	10.4.8.18	50708			443 → 50708 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0
2021-02-04 13:28:56	13.235.147.72	443	10.4.8.18	50709			443 → 50709 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0

```
▸ Frame 16680: 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: 15.206.34.128, Dst: 10.4.8.18
▾ Transmission Control Protocol, Src Port: 443, Dst Port: 50714, Seq: 0, Ack: 1, Len: 0
    Source Port: 443
    Destination Port: 50714
    [Stream index: 106]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    Sequence number (raw): 2636650998
    [Next sequence number: 1    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    Acknowledgment number (raw): 1183324849
    1000 .... = Header Length: 32 bytes (8)
  ▾ Flags: 0x012 (SYN, ACK)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Nonce: Not set
```

Lab3-Q2.pcapng   Packets: 19672 · Displayed: 115 (0.6%)   Profile: Default

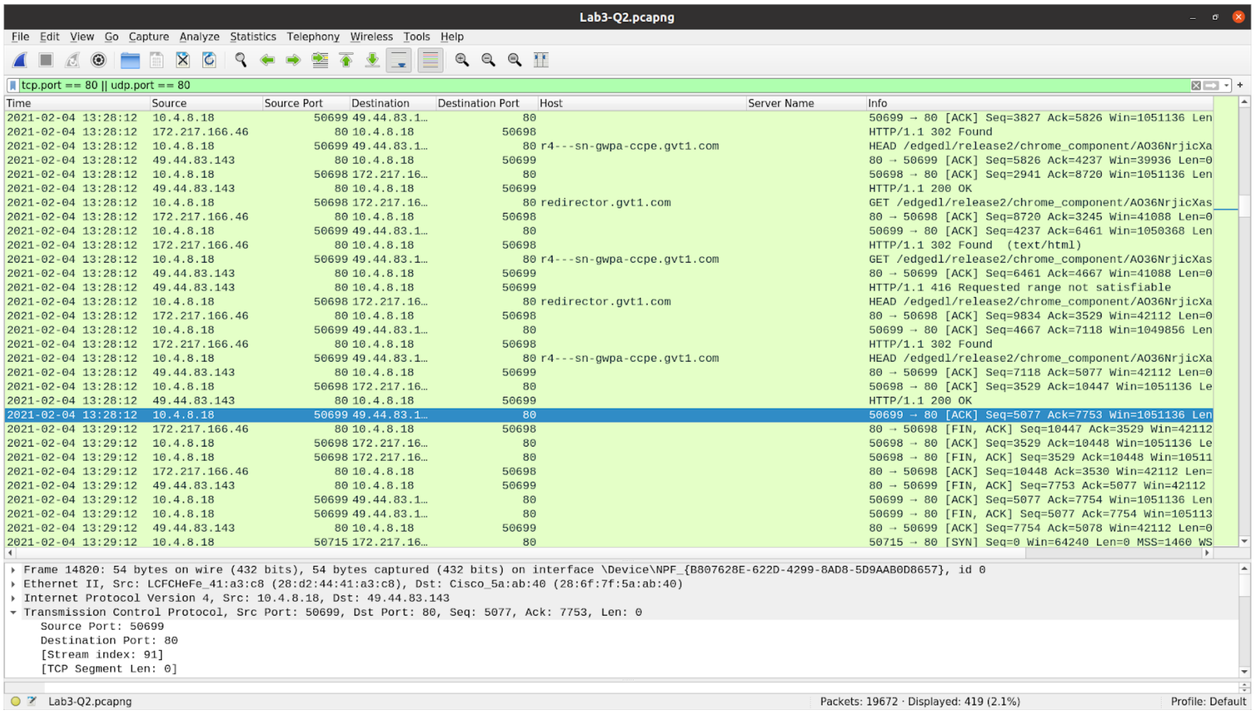
tcp.flags.syn == 1 is used to list out the TCP packets whose syn flags are on.

tcp.flags.ack == 1 is used to list out the TCP packets whose ack flags are on.

Hence AND(&&) operator has been used to list out packets where both conditions are simultaneously valid.

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

tcp.port == 80 || udp.port == 80


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

tcp.port == 80 || udp.port == 80

Time	Source	Source Port	Destination	Destination Port	Host	Server Name	Info
2021-02-04 13:28:12	10.4.8.18	50699	49.44.83.1…	80			50699 → 80 [ACK] Seq=3827 Ack=5826 Win=1051136 Len
2021-02-04 13:28:12	172.217.166.46	80	10.4.8.18	50698			HTTP/1.1 302 Found
2021-02-04 13:28:12	10.4.8.18	50699	49.44.83.1…	80	r4---sn-gwpa-ccpe.gvt1.com		HEAD /edgedl/release2/chrome_component/AO36NrjicXa
2021-02-04 13:28:12	49.44.83.143	80	10.4.8.18	50699			80 → 50699 [ACK] Seq=5826 Ack=4237 Win=39936 Len=0
2021-02-04 13:28:12	10.4.8.18	50698	172.217.16…	80			50698 → 80 [ACK] Seq=2941 Ack=8720 Win=1051136 Len
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	10.4.8.18	50698	172.217.16…	80	redirector.gvt1.com		GET /edgedl/release2/chrome_component/AO36NrjicXas
2021-02-04 13:28:12	172.217.166.46	80	10.4.8.18	50698			80 → 50698 [ACK] Seq=8720 Ack=3245 Win=41088 Len=0
2021-02-04 13:28:12	10.4.8.18	50699	49.44.83.1…	80			50699 → 80 [ACK] Seq=4237 Ack=6461 Win=1050368 Len
2021-02-04 13:28:12	172.217.166.46	80	10.4.8.18	50698			HTTP/1.1 302 Found (text/html)
2021-02-04 13:28:12	10.4.8.18	50699	49.44.83.1…	80	r4---sn-gwpa-ccpe.gvt1.com		GET /edgedl/release2/chrome_component/AO36NrjicXas
2021-02-04 13:28:12	49.44.83.143	80	10.4.8.18	50699			80 → 50699 [ACK] Seq=6461 Ack=4667 Win=41088 Len=0
2021-02-04 13:28:12	49.44.83.143	80	10.4.8.18	50699			HTTP/1.1 416 Requested range not satisfiable
2021-02-04 13:28:12	10.4.8.18	50698	172.217.16…	80	redirector.gvt1.com		HEAD /edgedl/release2/chrome_component/AO36NrjicXa
2021-02-04 13:28:12	172.217.166.46	80	10.4.8.18	50698			80 → 50698 [ACK] Seq=9834 Ack=3529 Win=42112 Len=0
2021-02-04 13:28:12	10.4.8.18	50699	49.44.83.1…	80			50699 → 80 [ACK] Seq=4667 Ack=7118 Win=1049856 Len
2021-02-04 13:28:12	172.217.166.46	80	10.4.8.18	50698			HTTP/1.1 302 Found
2021-02-04 13:28:12	10.4.8.18	50699	49.44.83.1…	80	r4---sn-gwpa-ccpe.gvt1.com		HEAD /edgedl/release2/chrome_component/AO36NrjicXa
2021-02-04 13:28:12	49.44.83.143	80	10.4.8.18	50699			80 → 50699 [ACK] Seq=7118 Ack=5077 Win=42112 Len=0
2021-02-04 13:28:12	10.4.8.18	50698	172.217.16…	80			50698 → 80 [ACK] Seq=3529 Ack=10447 Win=1051136 Le
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	10.4.8.18	50699	49.44.83.1…	80			50699 → 80 [ACK] Seq=5077 Ack=7753 Win=1051136 Len
2021-02-04 13:29:12	172.217.166.46	80	10.4.8.18	50698			80 → 50698 [FIN, ACK] Seq=10447 Ack=3529 Win=42112
2021-02-04 13:29:12	10.4.8.18	50698	172.217.16…	80			50698 → 80 [ACK] Seq=3529 Ack=10448 Win=1051136 Le
2021-02-04 13:29:12	10.4.8.18	50698	172.217.16…	80			50698 → 80 [FIN, ACK] Seq=3529 Ack=10448 Win=10511
2021-02-04 13:29:12	172.217.166.46	80	10.4.8.18	50698			80 → 50698 [ACK] Seq=10448 Ack=3530 Win=42112 Len=
2021-02-04 13:29:12	49.44.83.143	80	10.4.8.18	50699			80 → 50699 [FIN, ACK] Seq=7753 Ack=5077 Win=42112
2021-02-04 13:29:12	10.4.8.18	50699	49.44.83.1…	80			50699 → 80 [ACK] Seq=5077 Ack=7754 Win=1051136 Len
2021-02-04 13:29:12	10.4.8.18	50699	49.44.83.1…	80			50699 → 80 [FIN, ACK] Seq=5077 Ack=7754 Win=105113
2021-02-04 13:29:12	49.44.83.143	80	10.4.8.18	50699			80 → 50699 [ACK] Seq=7754 Ack=5078 Win=42112 Len=0
2021-02-04 13:29:12	10.4.8.18	50715	172.217.16…	80			50715 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS

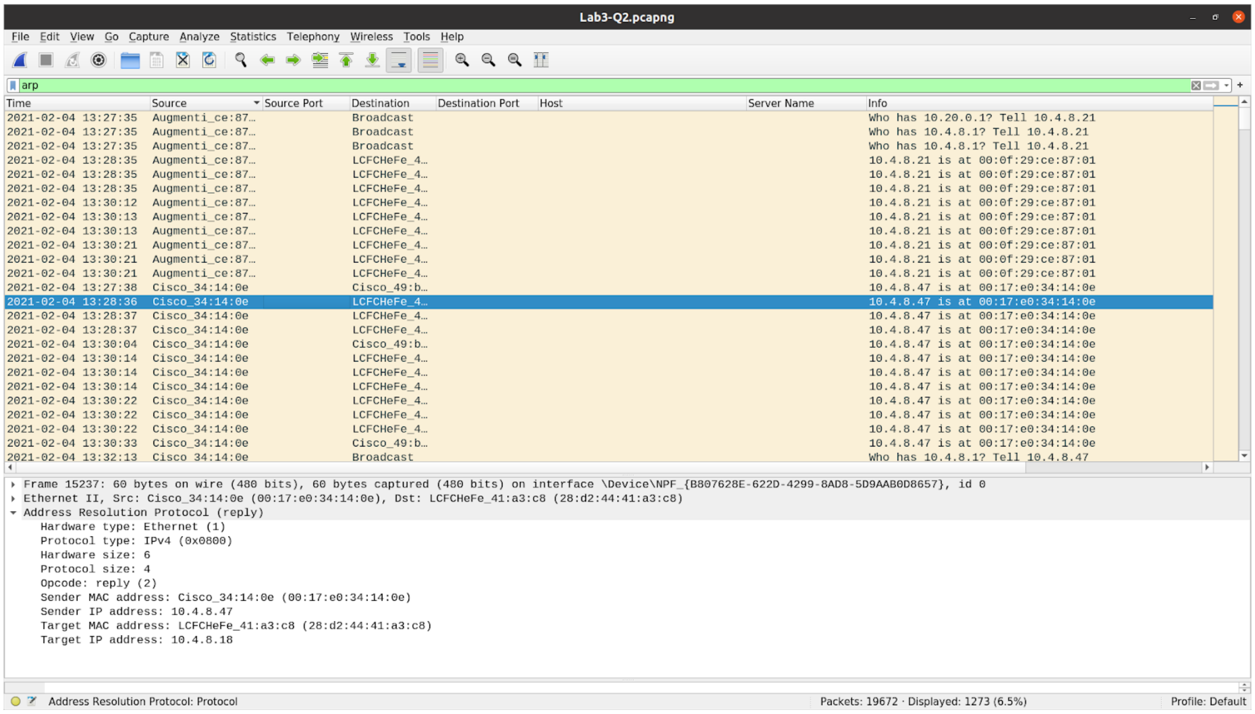
```
› Frame 14820: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{B807628E-622D-4299-8AD8-5D9AAB0D8657}, id 0
› Ethernet II, Src: LCFCHeFe_41:a3:c8 (28:d2:44:41:a3:c8), Dst: Cisco_5a:ab:40 (28:6f:7f:5a:ab:40)
› Internet Protocol Version 4, Src: 10.4.8.18, Dst: 49.44.83.143
▾ Transmission Control Protocol, Src Port: 50699, Dst Port: 80, Seq: 5077, Ack: 7753, Len: 0
    Source Port: 50699
    Destination Port: 80
    [Stream index: 91]
    [TCP Segment Len: 0]
```

Lab3-Q2.pcapng   Packets: 19672 · Displayed: 419 (2.1%)   Profile: Default

tcp.port == 80 is used to list out TCP packets where destination port=80
udp.port == 80 is used to list out UDP packets where destination port=80
Hence OR(||) operator has been used to list out both types of packets.

f. List out the ARP packets.

arp


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

arp

Time	Source	Source Port	Destination	Destination Port	Host	Server Name	Info
2021-02-04 13:27:35	Augmenti_ce:87…		Broadcast				Who has 10.20.0.1? Tell 10.4.8.21
2021-02-04 13:27:35	Augmenti_ce:87…		Broadcast				Who has 10.4.8.1? Tell 10.4.8.21
2021-02-04 13:27:35	Augmenti_ce:87…		Broadcast				Who has 10.4.8.1? Tell 10.4.8.21
2021-02-04 13:28:35	Augmenti_ce:87…		LCFCHeFe_4…				10.4.8.21 is at 00:0f:29:ce:87:01
2021-02-04 13:28:35	Augmenti_ce:87…		LCFCHeFe_4…				10.4.8.21 is at 00:0f:29:ce:87:01
2021-02-04 13:28:35	Augmenti_ce:87…		LCFCHeFe_4…				10.4.8.21 is at 00:0f:29:ce:87:01
2021-02-04 13:30:12	Augmenti_ce:87…		LCFCHeFe_4…				10.4.8.21 is at 00:0f:29:ce:87:01
2021-02-04 13:30:13	Augmenti_ce:87…		LCFCHeFe_4…				10.4.8.21 is at 00:0f:29:ce:87:01
2021-02-04 13:30:13	Augmenti_ce:87…		LCFCHeFe_4…				10.4.8.21 is at 00:0f:29:ce:87:01
2021-02-04 13:30:21	Augmenti_ce:87…		LCFCHeFe_4…				10.4.8.21 is at 00:0f:29:ce:87:01
2021-02-04 13:30:21	Augmenti_ce:87…		LCFCHeFe_4…				10.4.8.21 is at 00:0f:29:ce:87:01
2021-02-04 13:30:21	Augmenti_ce:87…		LCFCHeFe_4…				10.4.8.21 is at 00:0f:29:ce:87:01
2021-02-04 13:27:38	Cisco_34:14:0e		Cisco_49:b…				10.4.8.47 is at 00:17:e0:34:14:0e
2021-02-04 13:28:36	Cisco_34:14:0e		LCFCHeFe_4…				10.4.8.47 is at 00:17:e0:34:14:0e
2021-02-04 13:28:37	Cisco_34:14:0e		LCFCHeFe_4…				10.4.8.47 is at 00:17:e0:34:14:0e
2021-02-04 13:28:37	Cisco_34:14:0e		LCFCHeFe_4…				10.4.8.47 is at 00:17:e0:34:14:0e
2021-02-04 13:30:04	Cisco_34:14:0e		Cisco_49:b…				10.4.8.47 is at 00:17:e0:34:14:0e
2021-02-04 13:30:14	Cisco_34:14:0e		LCFCHeFe_4…				10.4.8.47 is at 00:17:e0:34:14:0e
2021-02-04 13:30:14	Cisco_34:14:0e		LCFCHeFe_4…				10.4.8.47 is at 00:17:e0:34:14:0e
2021-02-04 13:30:14	Cisco_34:14:0e		LCFCHeFe_4…				10.4.8.47 is at 00:17:e0:34:14:0e
2021-02-04 13:30:22	Cisco_34:14:0e		LCFCHeFe_4…				10.4.8.47 is at 00:17:e0:34:14:0e
2021-02-04 13:30:22	Cisco_34:14:0e		LCFCHeFe_4…				10.4.8.47 is at 00:17:e0:34:14:0e
2021-02-04 13:30:22	Cisco_34:14:0e		LCFCHeFe_4…				10.4.8.47 is at 00:17:e0:34:14:0e
2021-02-04 13:30:33	Cisco_34:14:0e		Cisco_49:b…				10.4.8.47 is at 00:17:e0:34:14:0e
2021-02-04 13:32:13	Cisco_34:14:0e		Broadcast				Who has 10.4.8.1? Tell 10.4.8.47

```
▸ Frame 15237: 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: Cisco_34:14:0e (00:17:e0:34:14:0e), Dst: LCFCHeFe_41:a3:c8 (28:d2:44:41:a3:c8)
▾ Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: Cisco_34:14:0e (00:17:e0:34:14:0e)
    Sender IP address: 10.4.8.47
    Target MAC address: LCFCHeFe_41:a3:c8 (28:d2:44:41:a3:c8)
    Target IP address: 10.4.8.18
```

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

The Address Resolution Protocol(arp) is used to dynamically discover the mapping between a layer 3 (protocol) and a layer 2 (hardware) address. A typical use of arp display filter is the mapping of an IP address (e.g. 192.168.0.10) to the underlying Ethernet address (e.g. 01:02:03:04:05:06). The packet details section also contains information about the mapping like Sender’s & Target’s IP and MAC address, Opcode value etc.