Experiment 12

Aim: Study and use the Wireshark for the various network protocols

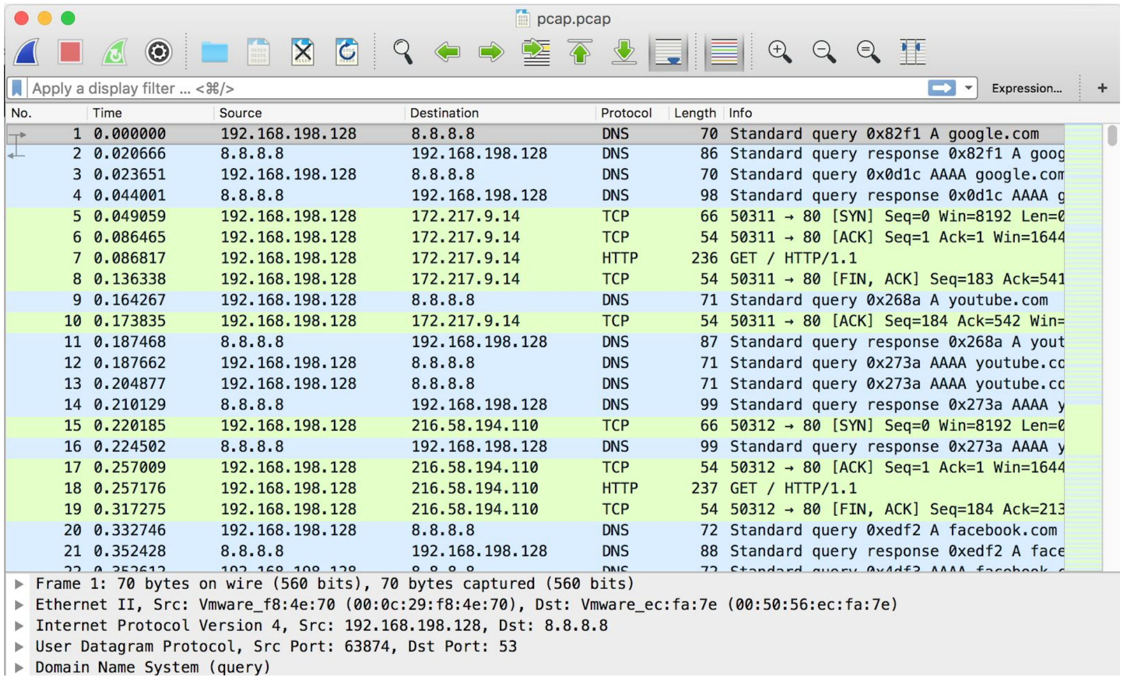
Theory: Wireshark is a packet sniffer and analysis tool. It captures network traffic on the local network and stores that data for offline analysis. It is used for network troubleshooting, analysis, software and communications protocol development, and education. Wireshark captures network traffic from Ethernet, Bluetooth, Wireless (IEEE.802.11), Token Ring, Frame Relay connections, and more.

- A "packet" is a single message from any network protocol (i.e., TCP, DNS, etc.)
- LAN traffic is in broadcast mode, meaning a single computer with Wireshark can see traffic between two other computers. If you want to see traffic to an external site, you need to capture the packets on the local computer.

Wireshark allows you to filter the log either before the capture starts or during analysis, so you can narrow down and zero into what you are looking for in the network trace. For example, you can set a filter to see TCP traffic between two IP addresses. You can set it only to show you the packets sent from one computer. The filters in Wireshark are one of the primary reasons it became the standard tool for packet analysis

Output:

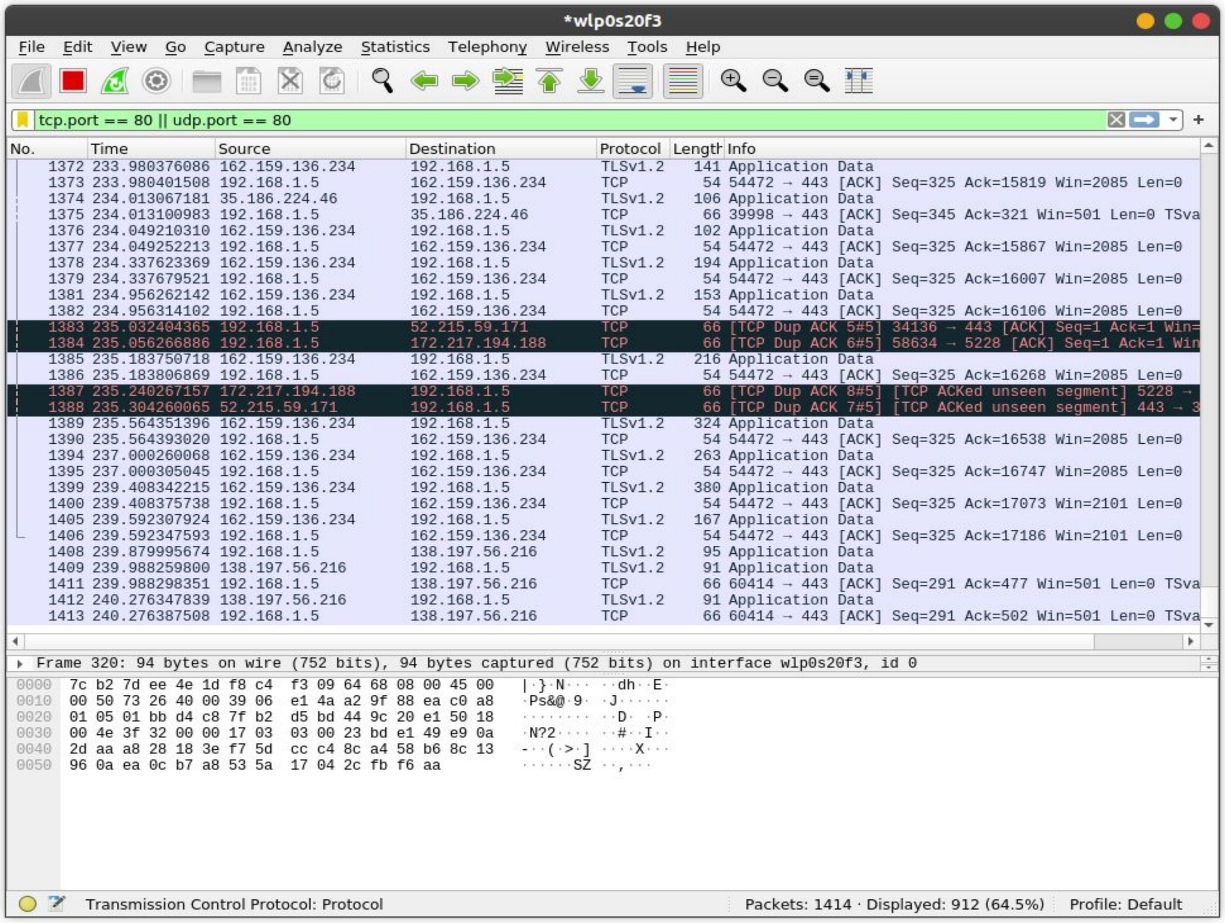
HTTP protocol



```
No.   Time      Source           Destination      Protocol Length Info
  1 0.000000   192.168.198.128  8.8.8.8          DNS       70 Standard query 0x82f1 A google.com
  2 0.020666   8.8.8.8          192.168.198.128  DNS       86 Standard query response 0x82f1 A goog
  3 0.023651   192.168.198.128  8.8.8.8          DNS       70 Standard query 0x0d1c AAAA google.com
  4 0.044001   8.8.8.8          192.168.198.128  DNS       98 Standard query response 0x0d1c AAAA g
  5 0.049059   192.168.198.128  172.217.9.14     TCP       66 50311 → 80 [SYN] Seq=0 Win=8192 Len=0
  6 0.086465   192.168.198.128  172.217.9.14     TCP       54 50311 → 80 [ACK] Seq=1 Ack=1 Win=1644
  7 0.086817   192.168.198.128  172.217.9.14     HTTP     236 GET / HTTP/1.1
  8 0.136338   192.168.198.128  172.217.9.14     TCP       54 50311 → 80 [FIN, ACK] Seq=183 Ack=541
  9 0.164267   192.168.198.128  8.8.8.8          DNS       71 Standard query 0x268a A youtube.com
 10 0.173835   192.168.198.128  172.217.9.14     TCP       54 50311 → 80 [ACK] Seq=184 Ack=542 Win=
 11 0.187468   8.8.8.8          192.168.198.128  DNS       87 Standard query response 0x268a A yout
 12 0.187662   192.168.198.128  8.8.8.8          DNS       71 Standard query 0x273a AAAA youtube.co
 13 0.204877   192.168.198.128  8.8.8.8          DNS       71 Standard query 0x273a AAAA youtube.co
 14 0.210129   8.8.8.8          192.168.198.128  DNS       99 Standard query response 0x273a AAAA y
 15 0.220185   192.168.198.128  216.58.194.110   TCP       66 50312 → 80 [SYN] Seq=0 Win=8192 Len=0
 16 0.224502   8.8.8.8          192.168.198.128  DNS       99 Standard query response 0x273a AAAA y
 17 0.257009   192.168.198.128  216.58.194.110   TCP       54 50312 → 80 [ACK] Seq=1 Ack=1 Win=1644
 18 0.257176   192.168.198.128  216.58.194.110   HTTP     237 GET / HTTP/1.1
 19 0.317275   192.168.198.128  216.58.194.110   TCP       54 50312 → 80 [FIN, ACK] Seq=184 Ack=213
 20 0.332746   192.168.198.128  8.8.8.8          DNS       72 Standard query 0xedf2 A facebook.com
 21 0.352428   8.8.8.8          192.168.198.128  DNS       88 Standard query response 0xedf2 A face
 22 0.352612   192.168.198.128  8.8.8.8          DNS       72 Standard query 0x4df3 AAAA facebook.c

▶ Frame 1: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)
▶ Ethernet II, Src: Vmware_f8:4e:70 (00:0c:29:f8:4e:70), Dst: Vmware_ec:fa:7e (00:50:56:ec:fa:7e)
▶ Internet Protocol Version 4, Src: 192.168.198.128, Dst: 8.8.8.8
▶ User Datagram Protocol, Src Port: 63874, Dst Port: 53
▶ Domain Name System (query)
```

TCP protocol


*wlp0s20f3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

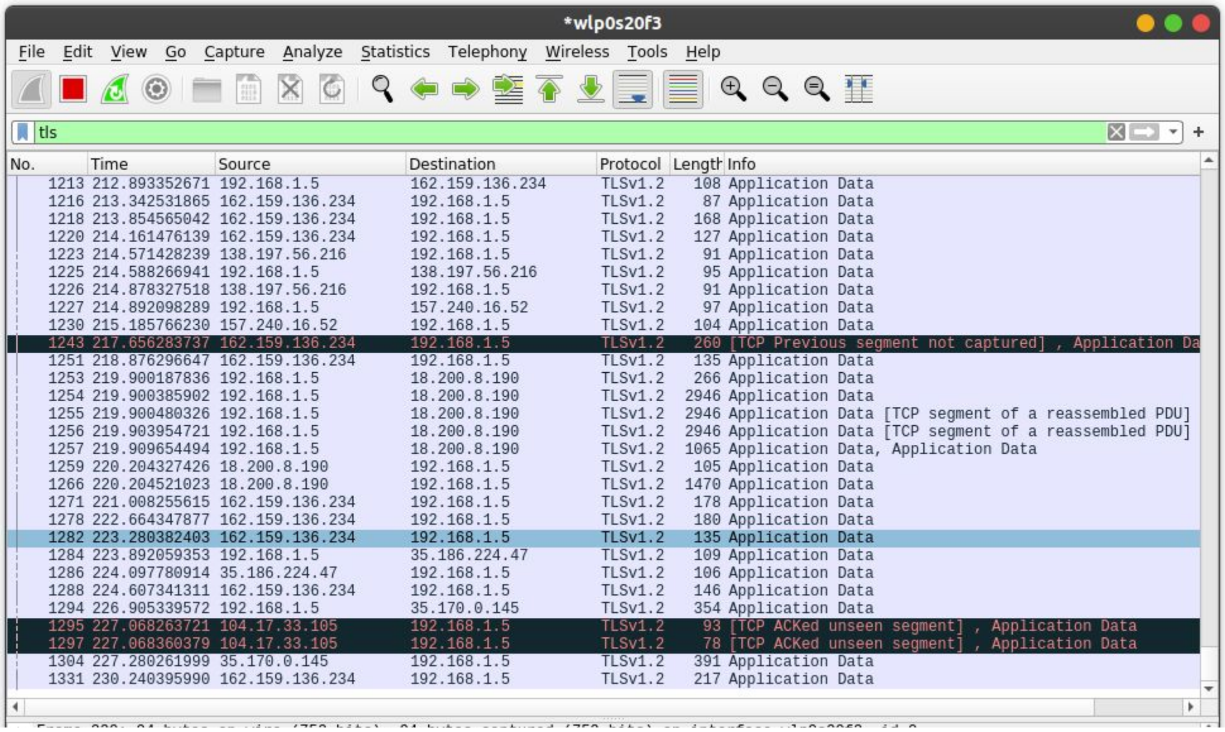
```
No.   Time          Source           Destination      Protocol Length Info
 1372 233.980376086 162.159.136.234  192.168.1.5      TLSv1.2  141 Application Data
 1373 233.980401508 192.168.1.5      162.159.136.234  TCP       54 54472 → 443 [ACK] Seq=325 Ack=15819 Win=2085 Len=0
 1374 234.013067181 35.186.224.46    192.168.1.5      TLSv1.2  106 Application Data
 1375 234.013100983 192.168.1.5      35.186.224.46    TCP       66 39998 → 443 [ACK] Seq=345 Ack=321 Win=501 Len=0 TSva
 1376 234.049210310 162.159.136.234  192.168.1.5      TLSv1.2  102 Application Data
 1377 234.049252213 192.168.1.5      162.159.136.234  TCP       54 54472 → 443 [ACK] Seq=325 Ack=15867 Win=2085 Len=0
 1378 234.337623369 162.159.136.234  192.168.1.5      TLSv1.2  194 Application Data
 1379 234.337679521 192.168.1.5      162.159.136.234  TCP       54 54472 → 443 [ACK] Seq=325 Ack=16007 Win=2085 Len=0
 1381 234.956262142 162.159.136.234  192.168.1.5      TLSv1.2  153 Application Data
 1382 234.956314102 192.168.1.5      162.159.136.234  TCP       54 54472 → 443 [ACK] Seq=325 Ack=16106 Win=2085 Len=0
 1383 235.032404365 192.168.1.5      52.215.59.171    TCP       66 [TCP Dup ACK 5#5] 34136 → 443 [ACK] Seq=1 Ack=1 Win=
 1384 235.056266886 192.168.1.5      172.217.194.188  TCP       66 [TCP Dup ACK 6#5] 58634 → 5228 [ACK] Seq=1 Ack=1 Win
 1385 235.183750718 162.159.136.234  192.168.1.5      TLSv1.2  216 Application Data
 1386 235.183806869 192.168.1.5      162.159.136.234  TCP       54 54472 → 443 [ACK] Seq=325 Ack=16268 Win=2085 Len=0
 1387 235.240267157 172.217.194.188  192.168.1.5      TCP       66 [TCP Dup ACK 8#5] [TCP ACKed unseen segment] 5228 →
 1388 235.304260065 52.215.59.171    192.168.1.5      TCP       66 [TCP Dup ACK 7#5] [TCP ACKed unseen segment] 443 → 3
 1389 235.564351396 162.159.136.234  192.168.1.5      TLSv1.2  324 Application Data
 1390 235.564393020 192.168.1.5      162.159.136.234  TCP       54 54472 → 443 [ACK] Seq=325 Ack=16538 Win=2085 Len=0
 1394 237.000260068 162.159.136.234  192.168.1.5      TLSv1.2  263 Application Data
 1395 237.000305045 192.168.1.5      162.159.136.234  TCP       54 54472 → 443 [ACK] Seq=325 Ack=16747 Win=2085 Len=0
 1399 239.408342215 162.159.136.234  192.168.1.5      TLSv1.2  380 Application Data
 1400 239.408375738 192.168.1.5      162.159.136.234  TCP       54 54472 → 443 [ACK] Seq=325 Ack=17073 Win=2101 Len=0
 1405 239.592307924 162.159.136.234  192.168.1.5      TLSv1.2  167 Application Data
 1406 239.592347593 192.168.1.5      162.159.136.234  TCP       54 54472 → 443 [ACK] Seq=325 Ack=17186 Win=2101 Len=0
 1408 239.879995674 192.168.1.5      138.197.56.216   TLSv1.2   95 Application Data
 1409 239.988259800 138.197.56.216   192.168.1.5      TLSv1.2   91 Application Data
 1411 239.988298351 192.168.1.5      138.197.56.216   TCP       66 60414 → 443 [ACK] Seq=291 Ack=477 Win=501 Len=0 TSva
 1412 240.276347839 138.197.56.216   192.168.1.5      TLSv1.2   91 Application Data
 1413 240.276387508 192.168.1.5      138.197.56.216   TCP       66 60414 → 443 [ACK] Seq=291 Ack=502 Win=501 Len=0 TSva
```

```
Frame 320: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface wlp0s20f3, id 0
```

```
0000  7c b2 7d ee 4e 1d f8 c4  f3 09 64 68 08 00 45 00   |·}·N···  ··dh··E·
0010  00 50 73 26 40 00 39 06  e1 4a a2 9f 88 ea c0 a8   ·Ps&@·9·  ·J······
0020  01 05 01 bb d4 c8 7f b2  d5 bd 44 9c 20 e1 50 18   ········  ··D· ·P·
0030  00 4e 3f 32 00 00 17 03  03 00 23 bd e1 49 e9 0a   ·N?2····  ··#··I··
0040  2d aa a8 28 18 3e f7 5d  cc c4 8c a4 58 b6 8c 13   -··(·>·]  ····X···
0050  96 0a ea 0c b7 a8 53 5a  17 04 2c fb f6 aa         ······SZ  ··,···
```

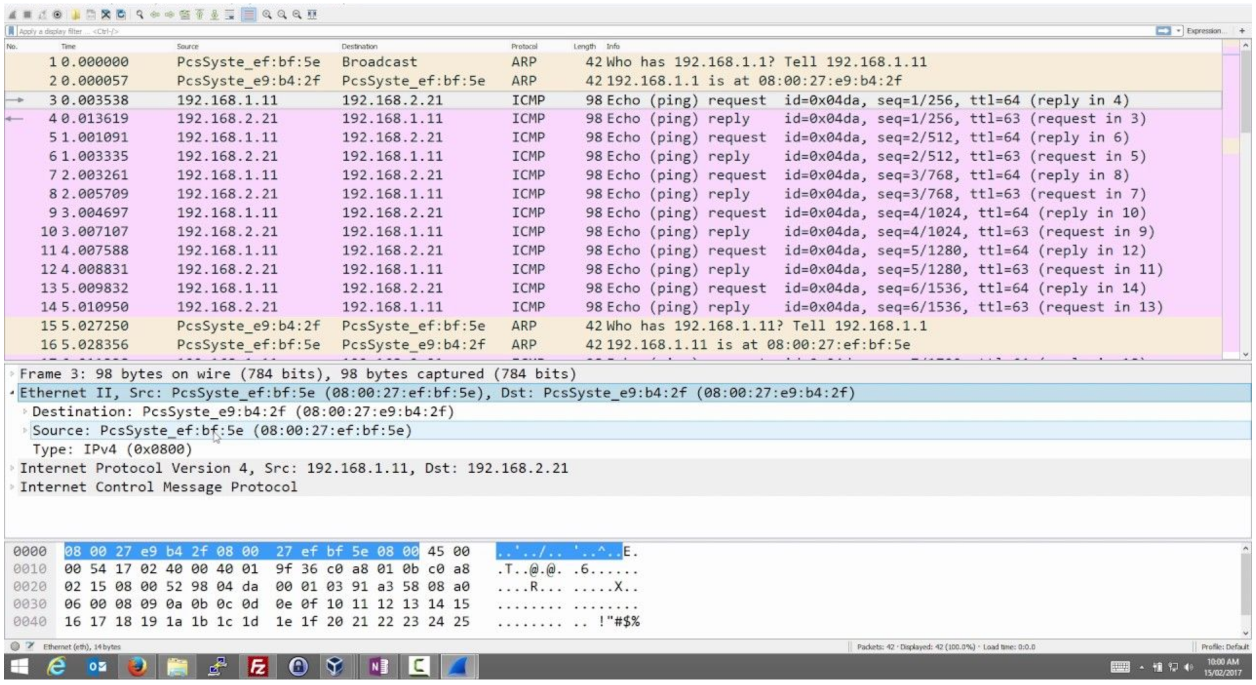
Transmission Control Protocol: Protocol   Packets: 1414 · Displayed: 912 (64.5%)   Profile: Default

TLS Protocol


*wlp0s20f3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tls

```
No.    Time          Source          Destination     Protocol Length Info
  1213 212.893352671 192.168.1.5     162.159.136.234 TLSv1.2   108 Application Data
  1216 213.342531865 162.159.136.234 192.168.1.5     TLSv1.2    87 Application Data
  1218 213.854565042 162.159.136.234 192.168.1.5     TLSv1.2   168 Application Data
  1220 214.161476139 162.159.136.234 192.168.1.5     TLSv1.2   127 Application Data
  1223 214.571428239 138.197.56.216  192.168.1.5     TLSv1.2    91 Application Data
  1225 214.588266941 192.168.1.5     138.197.56.216  TLSv1.2    95 Application Data
  1226 214.878327518 138.197.56.216  192.168.1.5     TLSv1.2    91 Application Data
  1227 214.892098289 192.168.1.5     157.240.16.52   TLSv1.2    97 Application Data
  1230 215.185766230 157.240.16.52   192.168.1.5     TLSv1.2   104 Application Data
  1243 217.656283737 162.159.136.234 192.168.1.5     TLSv1.2   260 [TCP Previous segment not captured] , Application Da
  1251 218.876296647 162.159.136.234 192.168.1.5     TLSv1.2   135 Application Data
  1253 219.900187836 192.168.1.5     18.200.8.190    TLSv1.2   266 Application Data
  1254 219.900385902 192.168.1.5     18.200.8.190    TLSv1.2  2946 Application Data
  1255 219.900480326 192.168.1.5     18.200.8.190    TLSv1.2  2946 Application Data [TCP segment of a reassembled PDU]
  1256 219.903954721 192.168.1.5     18.200.8.190    TLSv1.2  2946 Application Data [TCP segment of a reassembled PDU]
  1257 219.909654494 192.168.1.5     18.200.8.190    TLSv1.2  1065 Application Data, Application Data
  1259 220.204327426 18.200.8.190    192.168.1.5     TLSv1.2   105 Application Data
  1266 220.204521023 18.200.8.190    192.168.1.5     TLSv1.2  1470 Application Data
  1271 221.008255615 162.159.136.234 192.168.1.5     TLSv1.2   178 Application Data
  1278 222.664347877 162.159.136.234 192.168.1.5     TLSv1.2   180 Application Data
  1282 223.280382403 162.159.136.234 192.168.1.5     TLSv1.2   135 Application Data
  1284 223.892059353 192.168.1.5     35.186.224.47   TLSv1.2   109 Application Data
  1286 224.097780914 35.186.224.47   192.168.1.5     TLSv1.2   106 Application Data
  1288 224.607341311 162.159.136.234 192.168.1.5     TLSv1.2   146 Application Data
  1294 226.905339572 192.168.1.5     35.170.0.145    TLSv1.2   354 Application Data
  1295 227.068263721 104.17.33.105   192.168.1.5     TLSv1.2    93 [TCP ACKed unseen segment] , Application Data
  1297 227.068360379 104.17.33.105   192.168.1.5     TLSv1.2    78 [TCP ACKed unseen segment] , Application Data
  1304 227.280261999 35.170.0.145    192.168.1.5     TLSv1.2   391 Application Data
  1331 230.240395990 162.159.136.234 192.168.1.5     TLSv1.2   217 Application Data
```

ICMP protocol

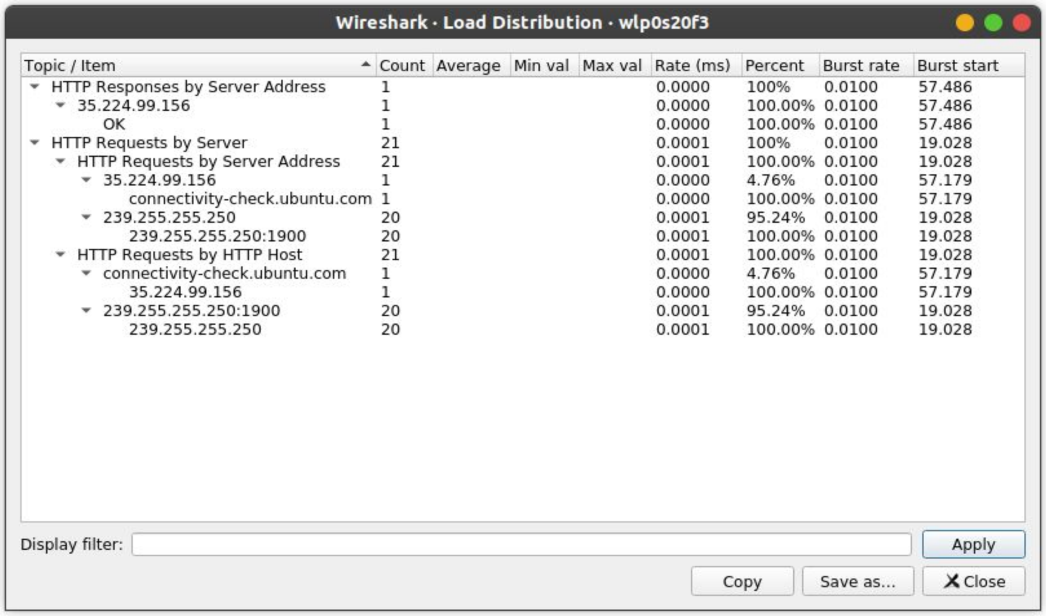


```
No. Time     Source            Destination       Protocol Length Info
  1 0.000000 PcsSyste_ef:bf:5e Broadcast         ARP      42 Who has 192.168.1.1? Tell 192.168.1.11
  2 0.000057 PcsSyste_e9:b4:2f PcsSyste_ef:bf:5e ARP      42 192.168.1.1 is at 08:00:27:e9:b4:2f
  3 0.003538 192.168.1.11      192.168.2.21      ICMP     98 Echo (ping) request  id=0x04da, seq=1/256, ttl=64 (reply in 4)
  4 0.013619 192.168.2.21      192.168.1.11      ICMP     98 Echo (ping) reply    id=0x04da, seq=1/256, ttl=63 (request in 3)
  5 1.001091 192.168.1.11      192.168.2.21      ICMP     98 Echo (ping) request  id=0x04da, seq=2/512, ttl=64 (reply in 6)
  6 1.003335 192.168.2.21      192.168.1.11      ICMP     98 Echo (ping) reply    id=0x04da, seq=2/512, ttl=63 (request in 5)
  7 2.003261 192.168.1.11      192.168.2.21      ICMP     98 Echo (ping) request  id=0x04da, seq=3/768, ttl=64 (reply in 8)
  8 2.005709 192.168.2.21      192.168.1.11      ICMP     98 Echo (ping) reply    id=0x04da, seq=3/768, ttl=63 (request in 7)
  9 3.004697 192.168.1.11      192.168.2.21      ICMP     98 Echo (ping) request  id=0x04da, seq=4/1024, ttl=64 (reply in 10)
 10 3.007107 192.168.2.21      192.168.1.11      ICMP     98 Echo (ping) reply    id=0x04da, seq=4/1024, ttl=63 (request in 9)
 11 4.007588 192.168.1.11      192.168.2.21      ICMP     98 Echo (ping) request  id=0x04da, seq=5/1280, ttl=64 (reply in 12)
 12 4.008831 192.168.2.21      192.168.1.11      ICMP     98 Echo (ping) reply    id=0x04da, seq=5/1280, ttl=63 (request in 11)
 13 5.009832 192.168.1.11      192.168.2.21      ICMP     98 Echo (ping) request  id=0x04da, seq=6/1536, ttl=64 (reply in 14)
 14 5.010950 192.168.2.21      192.168.1.11      ICMP     98 Echo (ping) reply    id=0x04da, seq=6/1536, ttl=63 (request in 13)
 15 5.027250 PcsSyste_e9:b4:2f PcsSyste_ef:bf:5e ARP      42 Who has 192.168.1.11? Tell 192.168.1.1
 16 5.028356 PcsSyste_ef:bf:5e PcsSyste_e9:b4:2f ARP      42 192.168.1.11 is at 08:00:27:ef:bf:5e

Frame 3: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
Ethernet II, Src: PcsSyste_ef:bf:5e (08:00:27:ef:bf:5e), Dst: PcsSyste_e9:b4:2f (08:00:27:e9:b4:2f)
  Destination: PcsSyste_e9:b4:2f (08:00:27:e9:b4:2f)
  Source: PcsSyste_ef:bf:5e (08:00:27:ef:bf:5e)
  Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.1.11, Dst: 192.168.2.21
Internet Control Message Protocol

0000  08 00 27 e9 b4 2f 08 00  27 ef bf 5e 08 00 45 00   ..'../.. '..^..E.
0010  00 54 17 02 40 00 40 01  9f 36 c0 a8 01 0b c0 a8   .T..@.@. .6......
0020  02 15 08 00 52 98 04 da  00 01 03 91 a3 58 08 a0   ....R... .....X..
0030  06 00 08 09 0a 0b 0c 0d  0e 0f 10 11 12 13 14 15   ........ ........
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ........ .. !"#$%
```

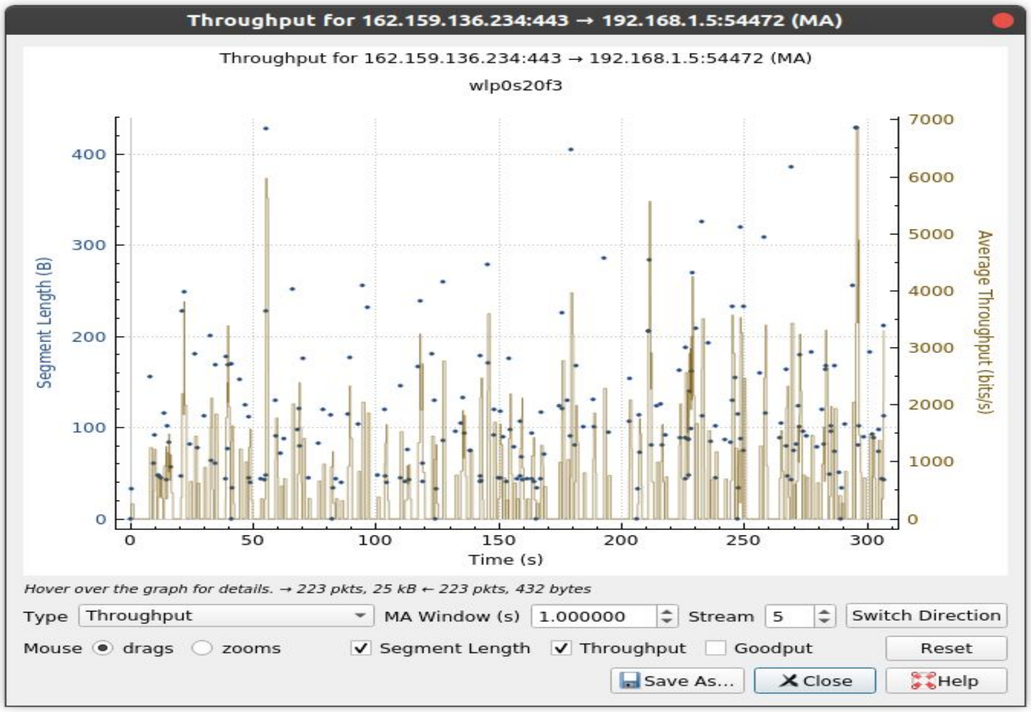
Analysing HTTP packets


Wireshark · Load Distribution · wlp0s20f3

Topic / Item	Count	Average	Min val	Max val	Rate (ms)	Percent	Burst rate	Burst start
HTTP Responses by Server Address	1				0.0000	100%	0.0100	57.486
35.224.99.156	1				0.0000	100.00%	0.0100	57.486
OK	1				0.0000	100.00%	0.0100	57.486
HTTP Requests by Server	21				0.0001	100%	0.0100	19.028
HTTP Requests by Server Address	21				0.0001	100.00%	0.0100	19.028
35.224.99.156	1				0.0000	4.76%	0.0100	57.179
connectivity-check.ubuntu.com	1				0.0000	100.00%	0.0100	57.179
239.255.255.250	20				0.0001	95.24%	0.0100	19.028
239.255.255.250:1900	20				0.0001	100.00%	0.0100	19.028
HTTP Requests by HTTP Host	21				0.0001	100.00%	0.0100	19.028
connectivity-check.ubuntu.com	1				0.0000	4.76%	0.0100	57.179
35.224.99.156	1				0.0000	100.00%	0.0100	57.179
239.255.255.250:1900	20				0.0001	95.24%	0.0100	19.028
239.255.255.250	20				0.0001	100.00%	0.0100	19.028

Display filter:

Analysing TCP packets


Throughput for 162.159.136.234:443 → 192.168.1.5:54472 (MA)

Hover over the graph for details. → 223 pkts, 25 kB ← 223 pkts, 432 bytes

Type: Throughput
MA Window (s): 1.000000
Stream: 5
Mouse: [✓ drags] zooms
[✓] Segment Length [✓] Throughput [ ] Goodput

Learning Outcomes:

Here we learned how to use wireshark for packet capturing using different protocol filters and how to analyze these packets.