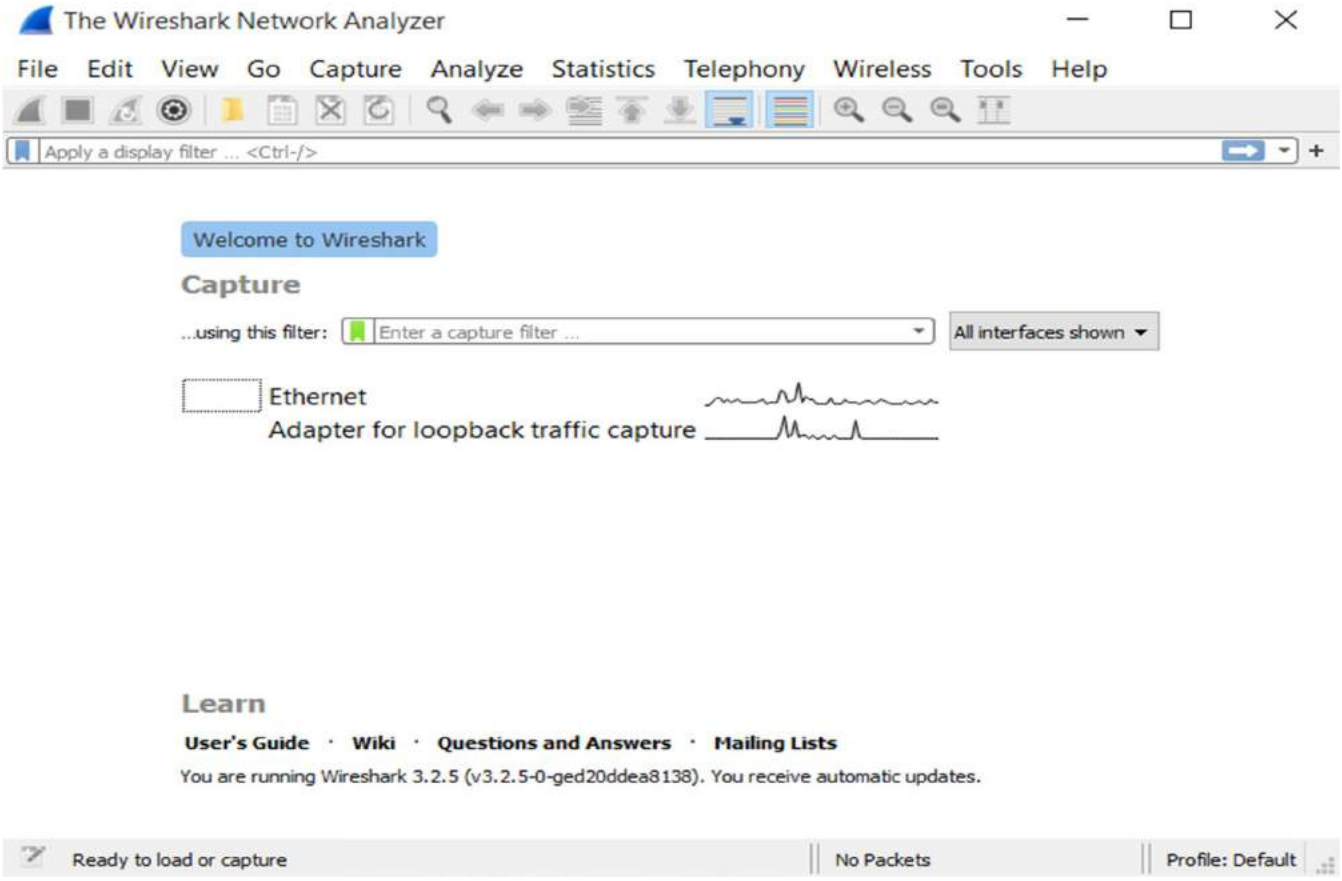
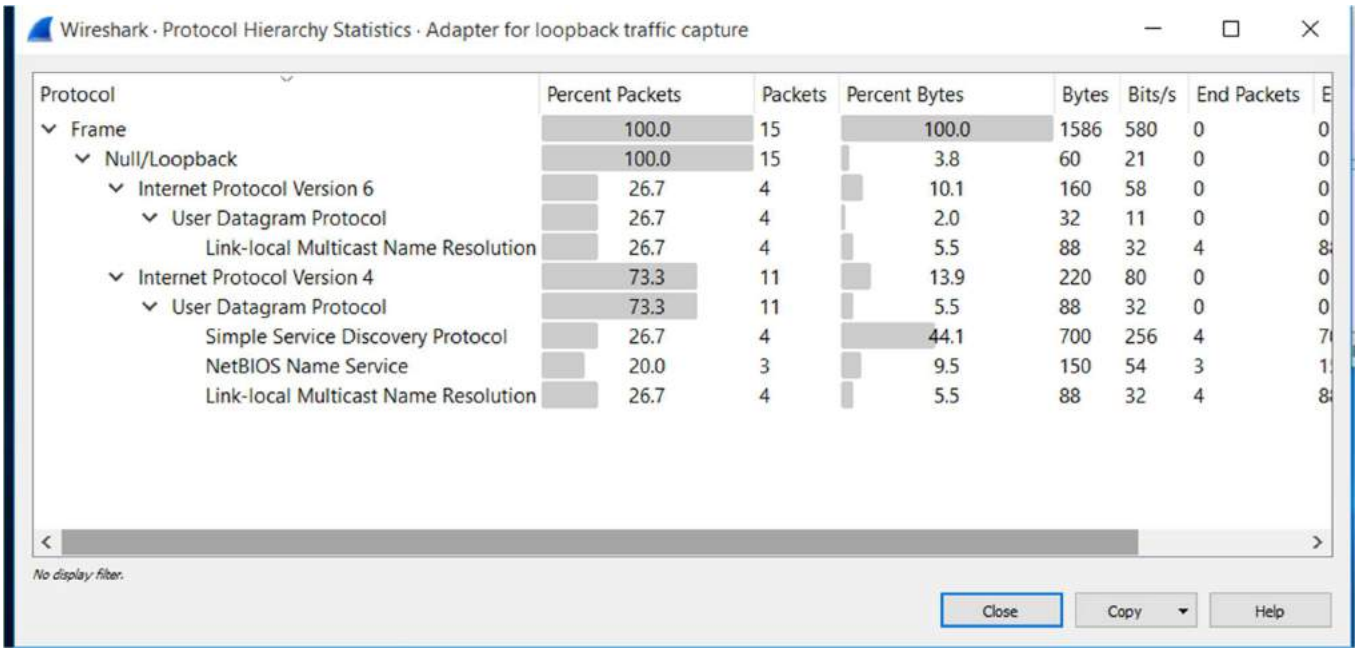
Lab: Using Wireshark for Network Monitoring

Wireshark Interface

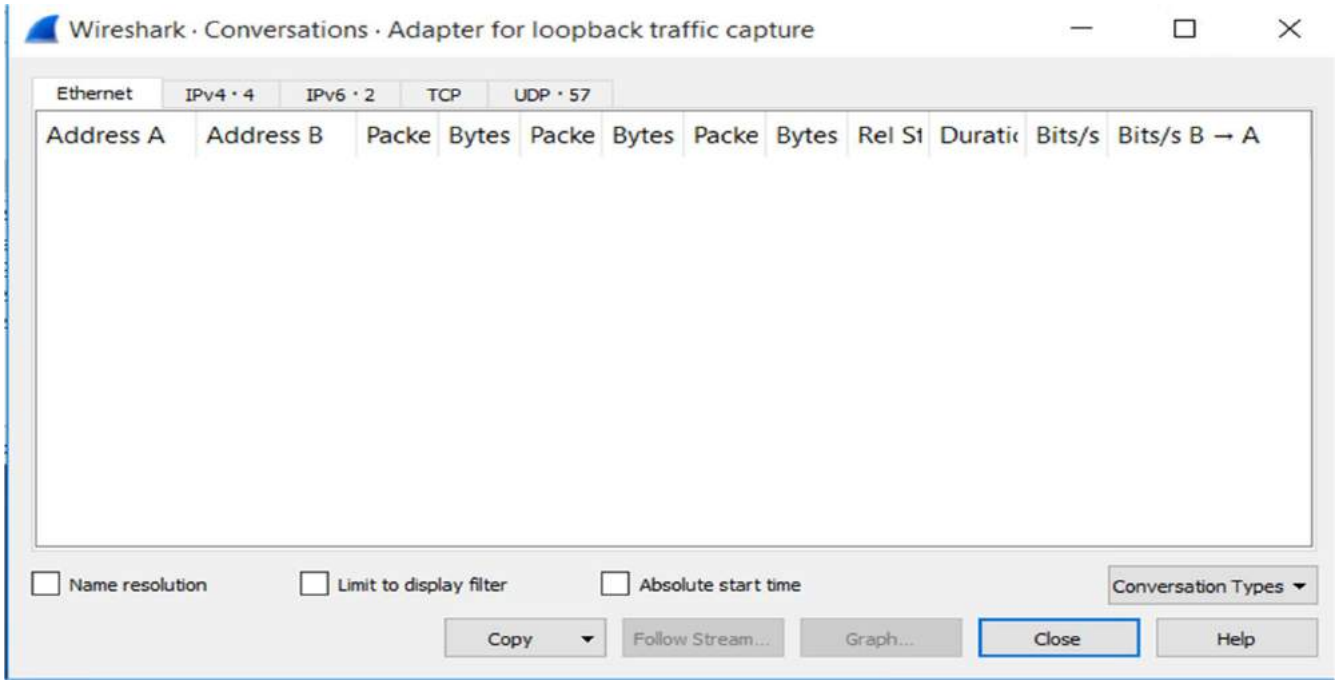


Statistics -> Protocol Hierarchy

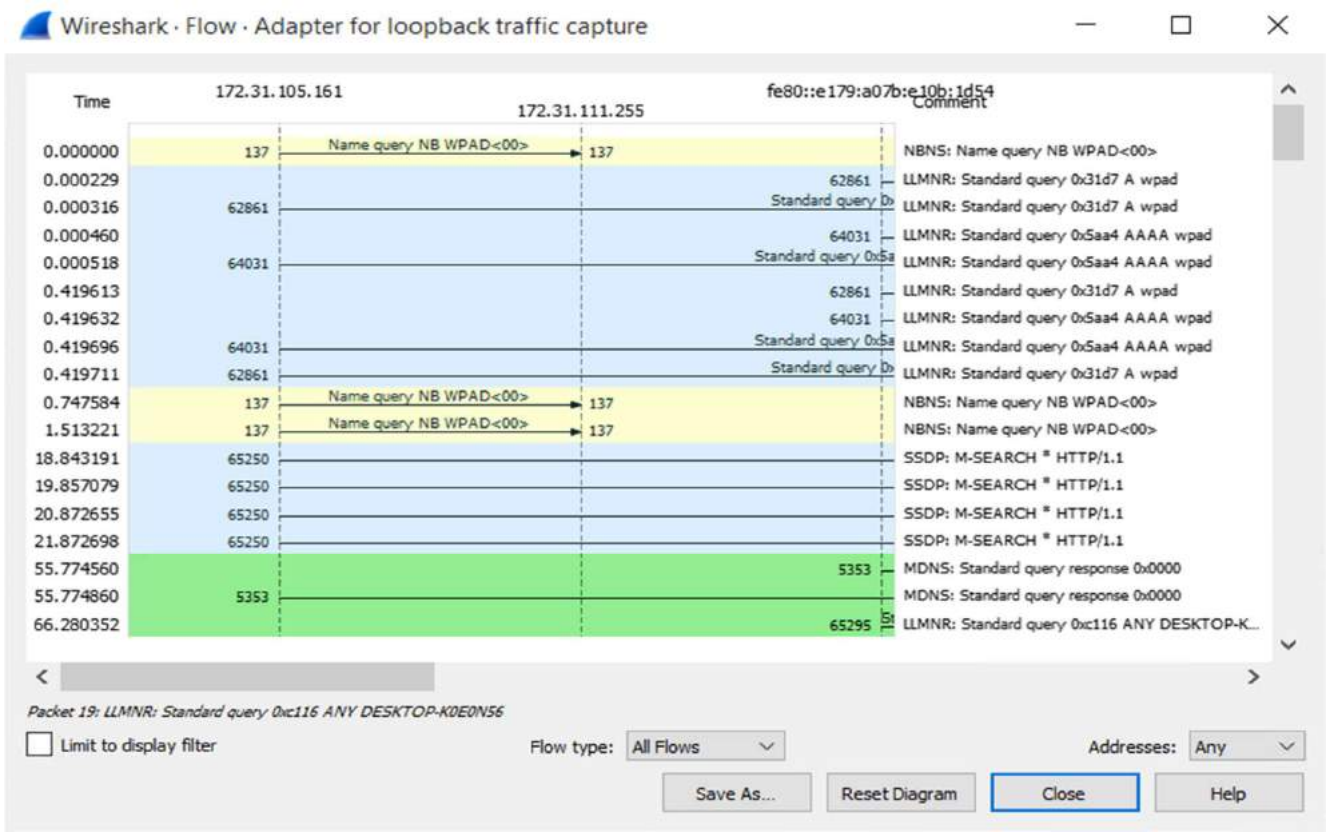


Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	E
Frame	100.0	15	100.0	1586	580	0	0
Null/Loopback	100.0	15	3.8	60	21	0	0
Internet Protocol Version 6	26.7	4	10.1	160	58	0	0
User Datagram Protocol	26.7	4	2.0	32	11	0	0
Link-local Multicast Name Resolution	26.7	4	5.5	88	32	4	8
Internet Protocol Version 4	73.3	11	13.9	220	80	0	0
User Datagram Protocol	73.3	11	5.5	88	32	0	0
Simple Service Discovery Protocol	26.7	4	44.1	700	256	4	7
NetBIOS Name Service	20.0	3	9.5	150	54	3	1
Link-local Multicast Name Resolution	26.7	4	5.5	88	32	4	8

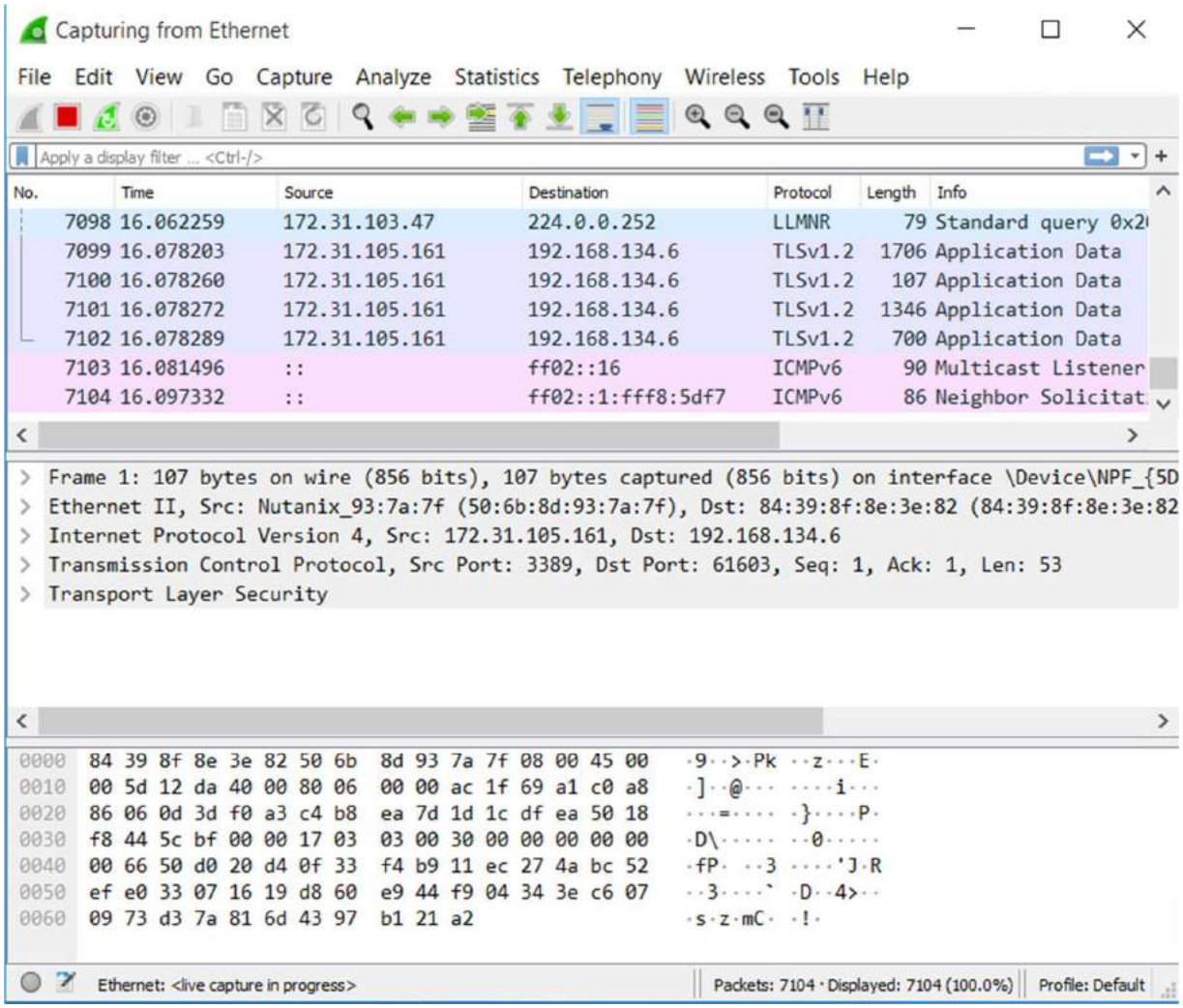
Statistics -> Conversations



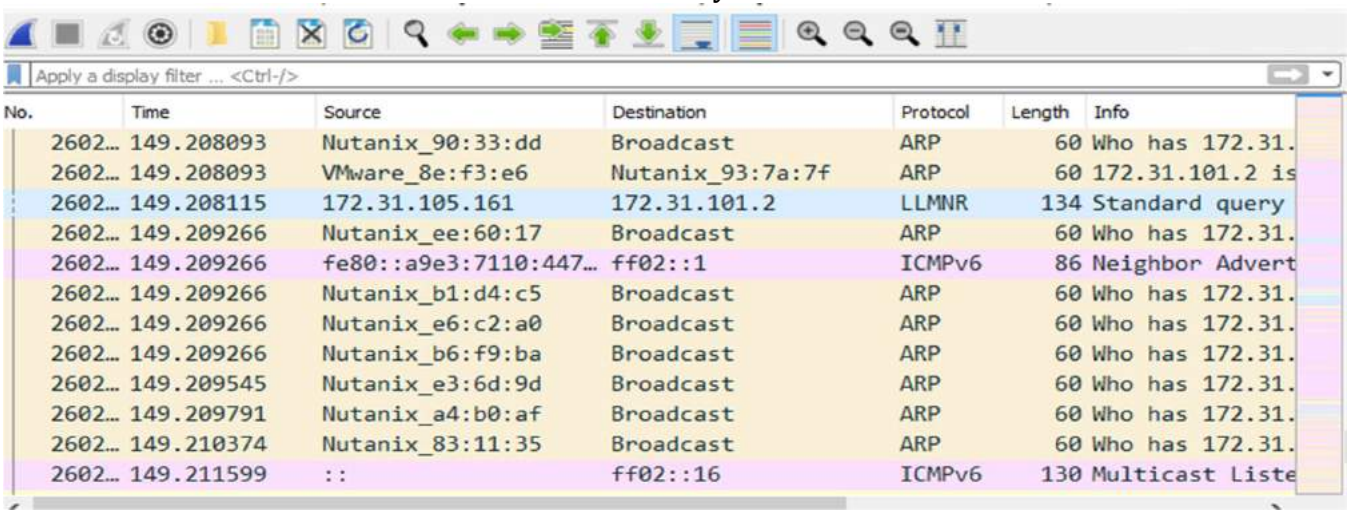
Statistics -> Flow Graph



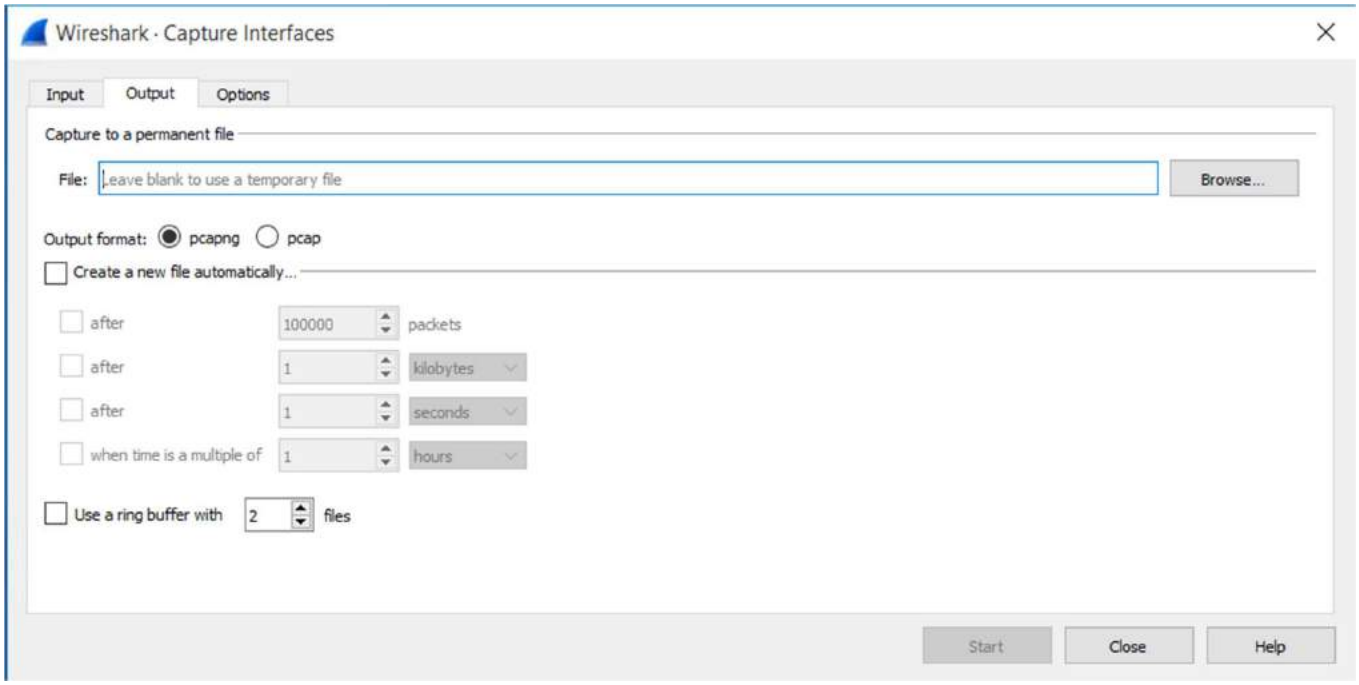
Traffic pattern



a. List down the network interfaces connected to your host

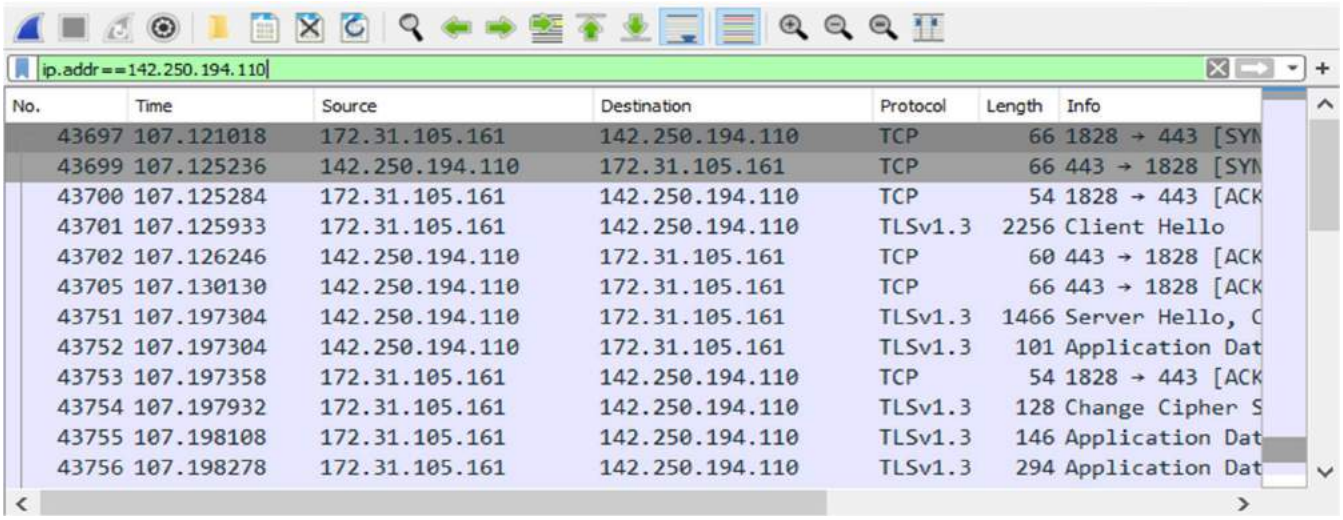


b. Configure the capture stop option of the wireshark

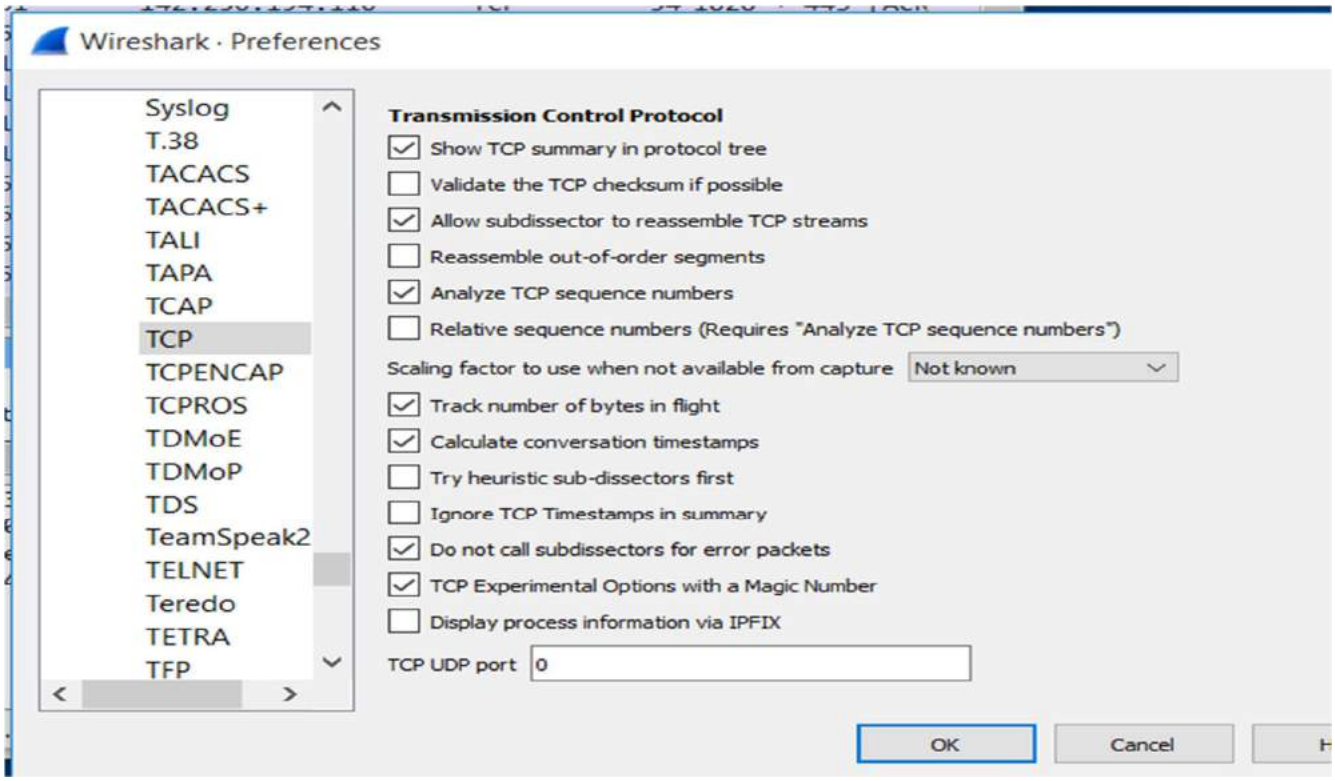


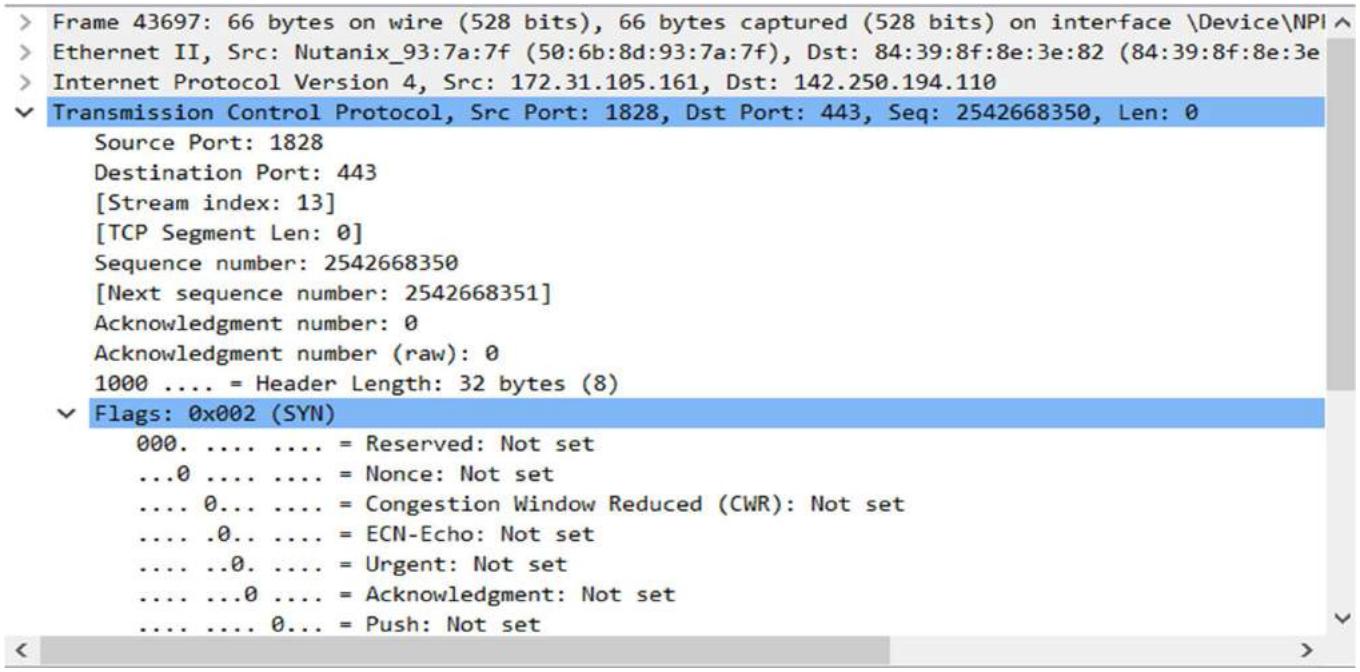
c. Capture live traffic from a site(for example google.com)

- Open browser clear cookies and history
- Browse google.com
- Ping google.com and get ip address
- Set display filter ip.addr== ip of google.com

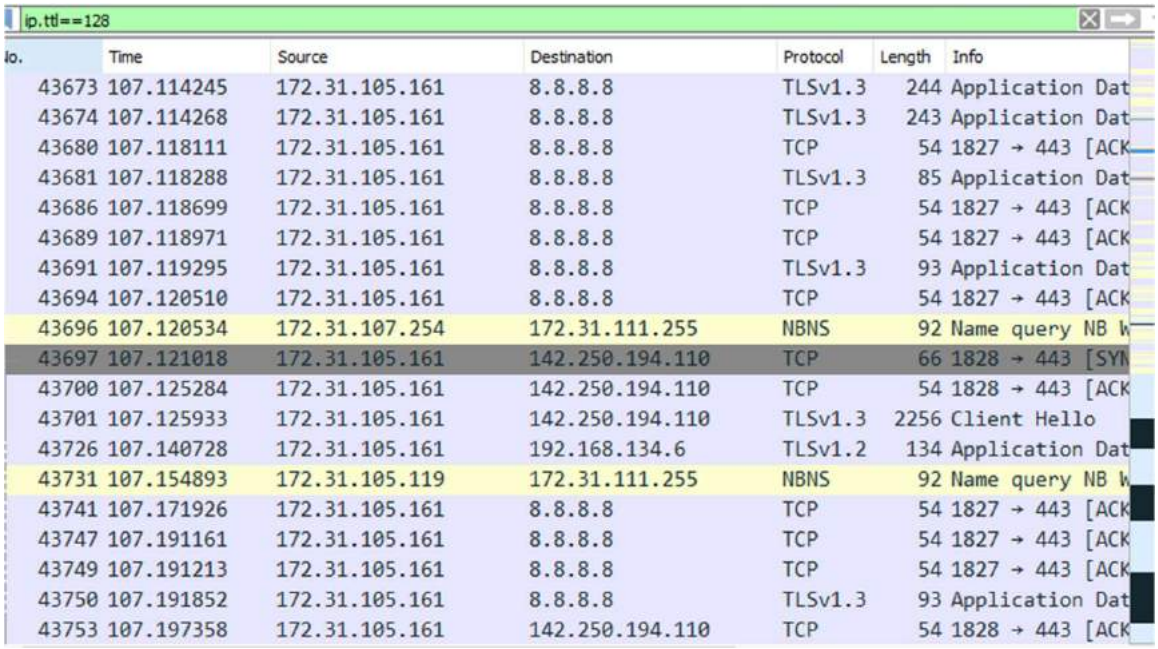


d. Finding Absolute packet number of a captured Packet

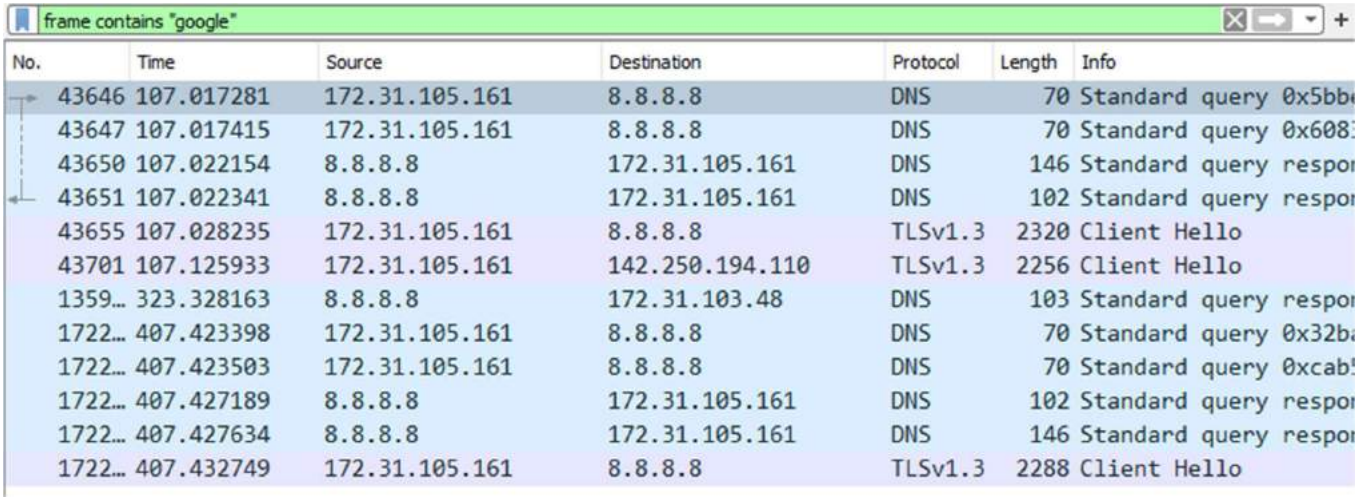




e. Finding packets with a particular ttl value

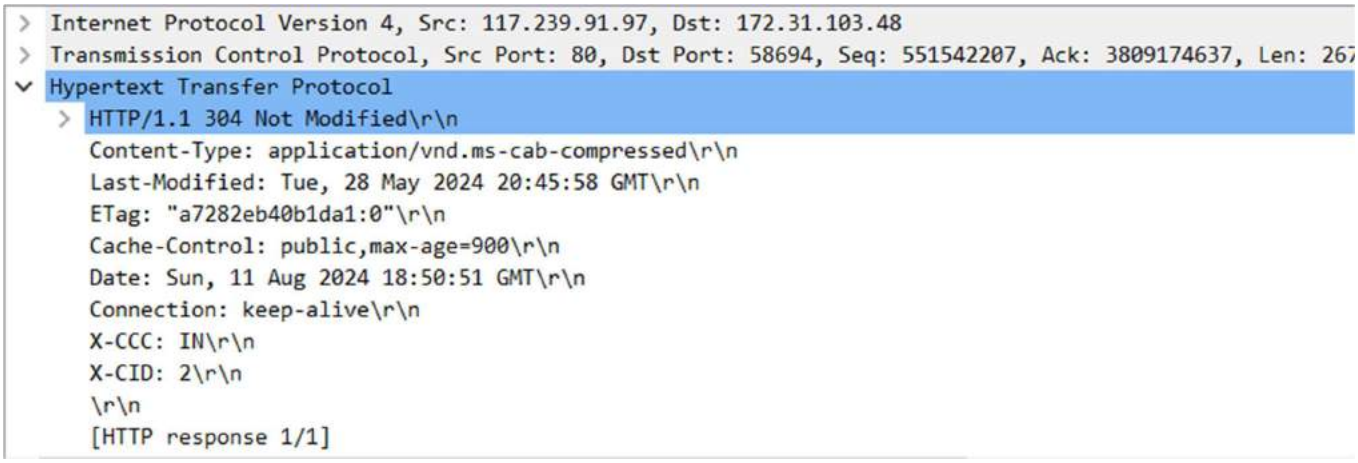


f. Finding a string in the capture



Lab Assignment

1. http version 1.1



2. source ip address: 117.239.91.97
   destination ip address: 172.31.103.48

```
Internet Protocol Version 4, Src: 117.239.91.97, Dst: 172.31.103.48
   0100 .... = Version: 4
   .... 0101 = Header Length: 20 bytes (5)
 > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
   Total Length: 307
   Identification: 0x19d6 (6614)
 > Flags: 0x4000, Don't fragment
   Fragment offset: 0
   Time to live: 61
   Protocol: TCP (6)
   Header checksum: 0x3e4f [validation disabled]
   [Header checksum status: Unverified]
   Source: 117.239.91.97
   Destination: 172.31.103.48
```

3. Return Status

```
Hypertext Transfer Protocol
 > HTTP/1.1 304 Not Modified\r\n
   Content-Type: application/vnd.ms-cab-compressed\r\n
   Last-Modified: Tue, 28 May 2024 20:45:58 GMT\r\n
   ETag: "a7282eb40b1da1:0"\r\n
   Cache-Control: public,max-age=900\r\n
   Date: Sun, 11 Aug 2024 18:50:51 GMT\r\n
   Connection: keep-alive\r\n
   X-CCC: IN\r\n
   X-CID: 2\r\n
   \r\n
   [HTTP response 1/1]
```