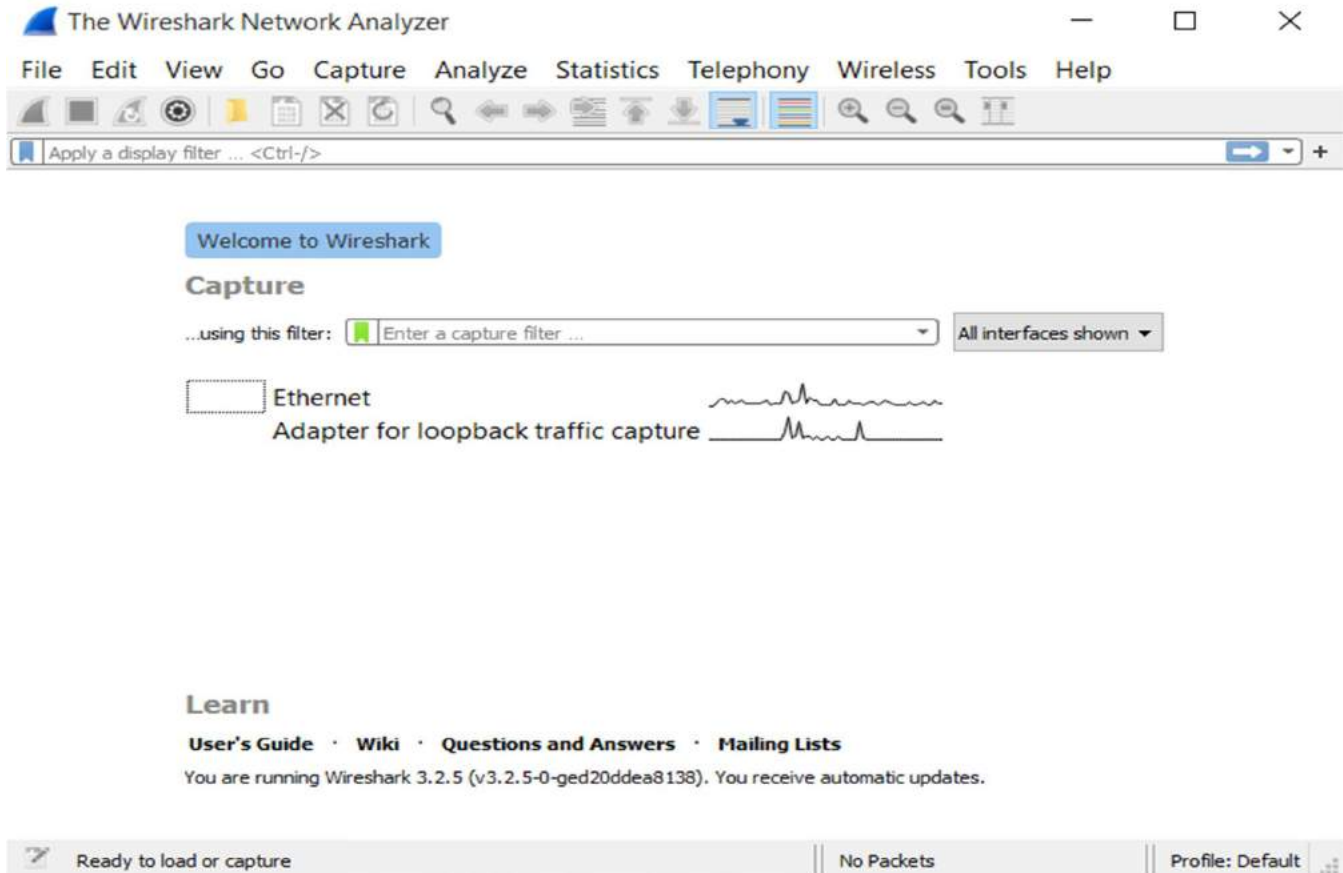
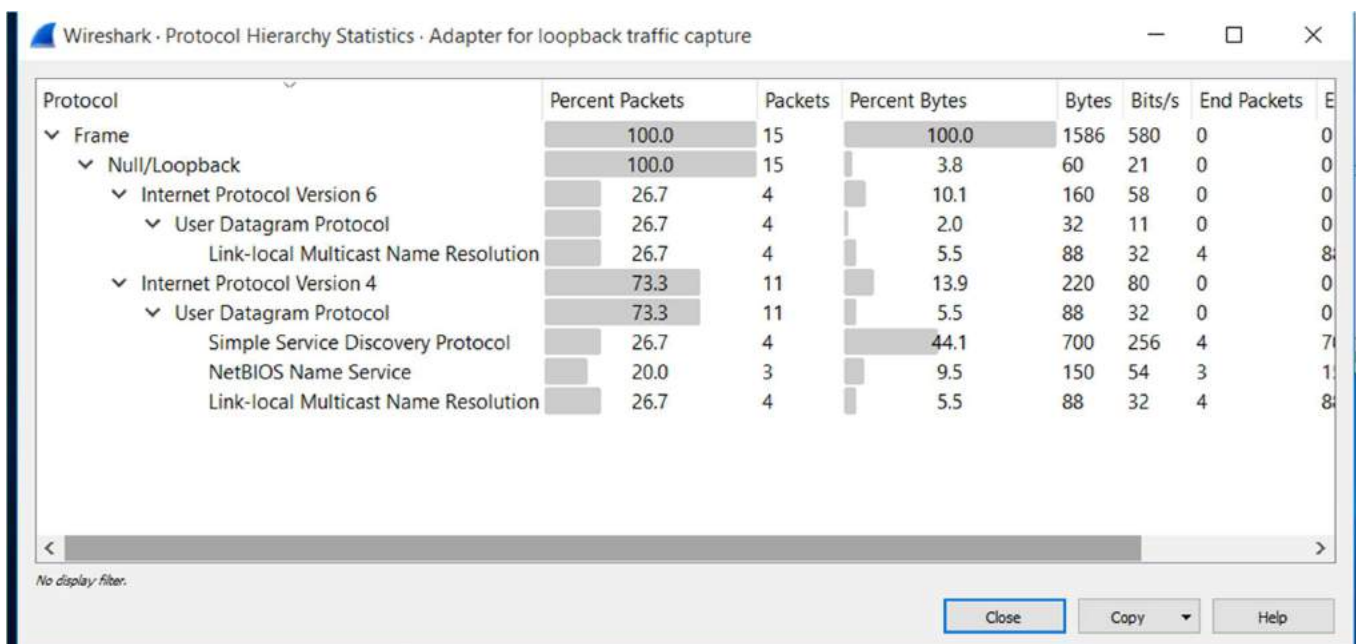


Lab: Using Wireshark for Network Monitoring

Wireshark Interface



Statistics -> Protocol Hierarchy



Wireshark · Conversations · Adapter for loopback traffic capture

Ethernet IPv4 · 4 IPv6 · 2 TCP UDP · 57

Address A	Address B	Packets	Bytes	Packets	Bytes	Packets	Bytes	Rel. Size	Duration	Bits/s	Bits/s B → A

☐ Name resolution
 ☐ Limit to display filter
 ☐ Absolute start time
 Conversation Types ▼

Copy ▼ Follow Stream... Graph... **Close** Help

Wireshark · Flow · Adapter for loopback traffic capture

Time	172.31.105.161	172.31.111.255	fe80::e179:a07b:e10b:1d54	Comment
0.000000	137	Name query NB WPAD<00>	137	NBNS: Name query NB WPAD<00>
0.000229			62861	LLMNR: Standard query 0x31d7 A wpad
0.000316	62861	Standard query 0x31d7 A wpad		LLMNR: Standard query 0x31d7 A wpad
0.000460			64031	LLMNR: Standard query 0x5aa4 AAAA wpad
0.000518	64031	Standard query 0x5aa4 AAAA wpad		LLMNR: Standard query 0x5aa4 AAAA wpad
0.419613			62861	LLMNR: Standard query 0x31d7 A wpad
0.419632			64031	LLMNR: Standard query 0x5aa4 AAAA wpad
0.419696	64031	Standard query 0x5aa4 AAAA wpad		LLMNR: Standard query 0x5aa4 AAAA wpad
0.419711	62861	Standard query 0x31d7 A wpad		LLMNR: Standard query 0x31d7 A wpad
0.747584	137	Name query NB WPAD<00>	137	NBNS: Name query NB WPAD<00>
1.513221	137	Name query NB WPAD<00>	137	NBNS: Name query NB WPAD<00>
18.843191	65250			SSDP: M-SEARCH * HTTP/1.1
19.857079	65250			SSDP: M-SEARCH * HTTP/1.1
20.872655	65250			SSDP: M-SEARCH * HTTP/1.1
21.872698	65250			SSDP: M-SEARCH * HTTP/1.1
55.774560			5353	MDNS: Standard query response 0x0000
55.774860	5353			MDNS: Standard query response 0x0000
66.280352			65295	LLMNR: Standard query 0xc116 ANY DESKTOP-K...

Packet 19: LLMNR: Standard query 0xc116 ANY DESKTOP-K0E0N56

☐ Limit to display filter
 Flow type: All Flows
 Addresses: Any
 Save As... Reset Diagram Close Help

Traffic pattern

Capturing from Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
7098	16.062259	172.31.103.47	224.0.0.252	LLMNR	79	Standard query 0x21
7099	16.078203	172.31.105.161	192.168.134.6	TLSv1.2	1706	Application Data
7100	16.078260	172.31.105.161	192.168.134.6	TLSv1.2	107	Application Data
7101	16.078272	172.31.105.161	192.168.134.6	TLSv1.2	1346	Application Data
7102	16.078289	172.31.105.161	192.168.134.6	TLSv1.2	700	Application Data
7103	16.081496	::	ff02::16	ICMPv6	90	Multicast Listener
7104	16.097332	::	ff02::1:fff8:5df7	ICMPv6	86	Neighbor Solicitat

> Frame 1: 107 bytes on wire (856 bits), 107 bytes captured (856 bits) on interface \Device\NPF_{50...}

> Ethernet II, Src: Nutanix_93:7a:7f (50:6b:8d:93:7a:7f), Dst: 84:39:8f:8e:3e:82 (84:39:8f:8e:3e:82)

> Internet Protocol Version 4, Src: 172.31.105.161, Dst: 192.168.134.6

> Transmission Control Protocol, Src Port: 3389, Dst Port: 61603, Seq: 1, Ack: 1, Len: 53

> Transport Layer Security

0000 84 39 8f 8e 3e 82 50 6b 8d 93 7a 7f 08 00 45 00 .9.>.Pk..z...E.

0010 00 5d 12 da 40 00 80 06 00 00 ac 1f 69 a1 c0 a8 .]..@... ..i...

0020 86 06 0d 3d f0 a3 c4 b8 ea 7d 1d 1c df ea 50 18 ...=....}....P.

0030 f8 44 5c bf 00 00 17 03 03 00 30 00 00 00 00 00 .D\....-0....

0040 00 66 50 d0 20 d4 0f 33 f4 b9 11 ec 27 4a bc 52 .fP..3....'J.R

0050 ef e0 33 d7 16 19 d8 60 e9 44 f9 04 34 3e c6 07 ..3....`-D..4>..

0060 09 73 d3 7a 81 6d 43 97 b1 21 a2 .s.z.mC..!.

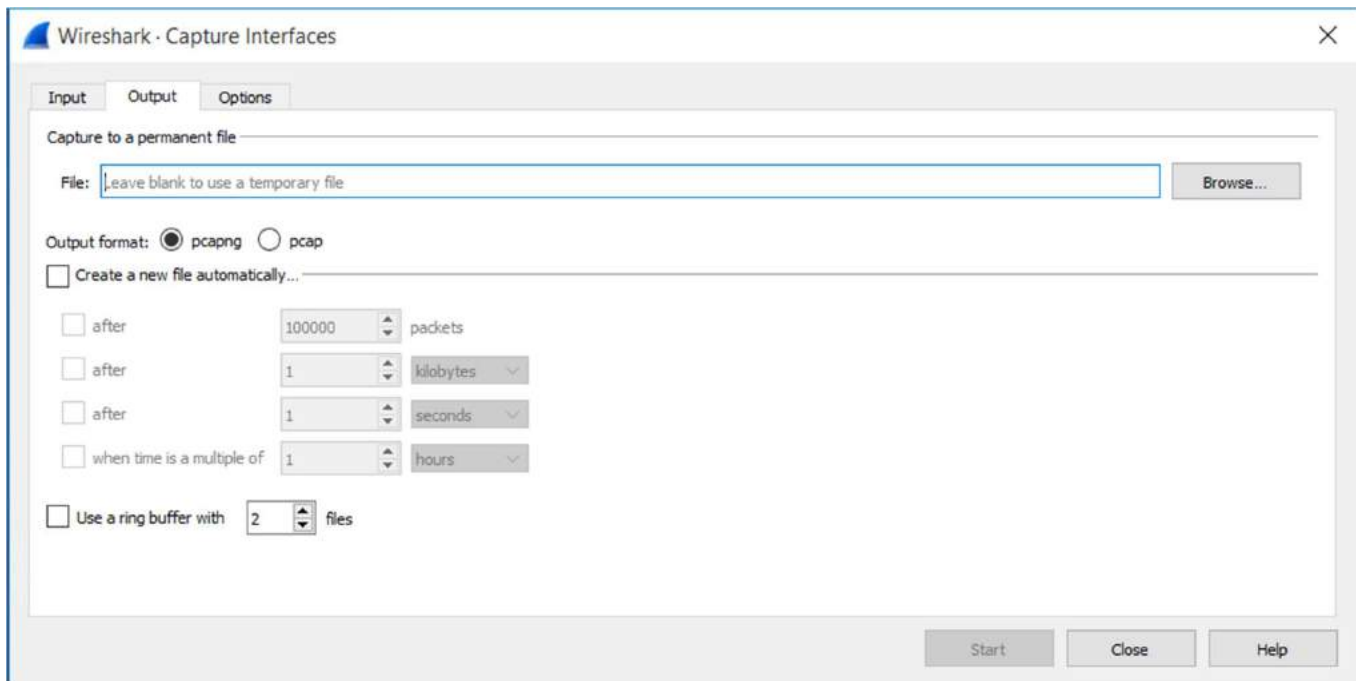
Ethernet: <live capture in progress> | Packets: 7104 · Displayed: 7104 (100.0%) | Profile: Default

a. List down the network interfaces connected to your host

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
2602...	149.208093	Nutanix_90:33:dd	Broadcast	ARP	60	Who has 172.31.
2602...	149.208093	VMware_8e:f3:e6	Nutanix_93:7a:7f	ARP	60	172.31.101.2 is
2602...	149.208115	172.31.105.161	172.31.101.2	LLMNR	134	Standard query
2602...	149.209266	Nutanix_ee:60:17	Broadcast	ARP	60	Who has 172.31.
2602...	149.209266	fe80::a9e3:7110:447...	ff02::1	ICMPv6	86	Neighbor Advert
2602...	149.209266	Nutanix_b1:d4:c5	Broadcast	ARP	60	Who has 172.31.
2602...	149.209266	Nutanix_e6:c2:a0	Broadcast	ARP	60	Who has 172.31.
2602...	149.209266	Nutanix_b6:f9:ba	Broadcast	ARP	60	Who has 172.31.
2602...	149.209545	Nutanix_e3:6d:9d	Broadcast	ARP	60	Who has 172.31.
2602...	149.209791	Nutanix_a4:b0:af	Broadcast	ARP	60	Who has 172.31.
2602...	149.210374	Nutanix_83:11:35	Broadcast	ARP	60	Who has 172.31.
2602...	149.211599	::	ff02::16	ICMPv6	130	Multicast Liste

b. Configure the capture stop option of the wireshark



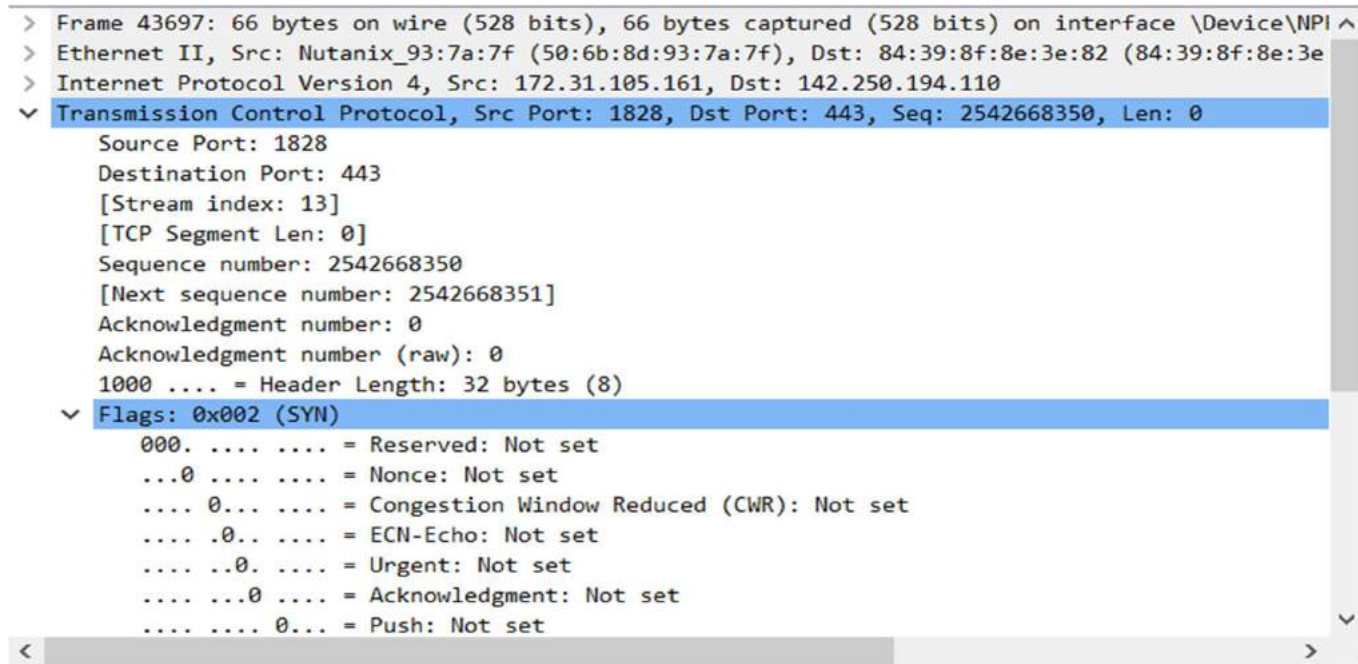
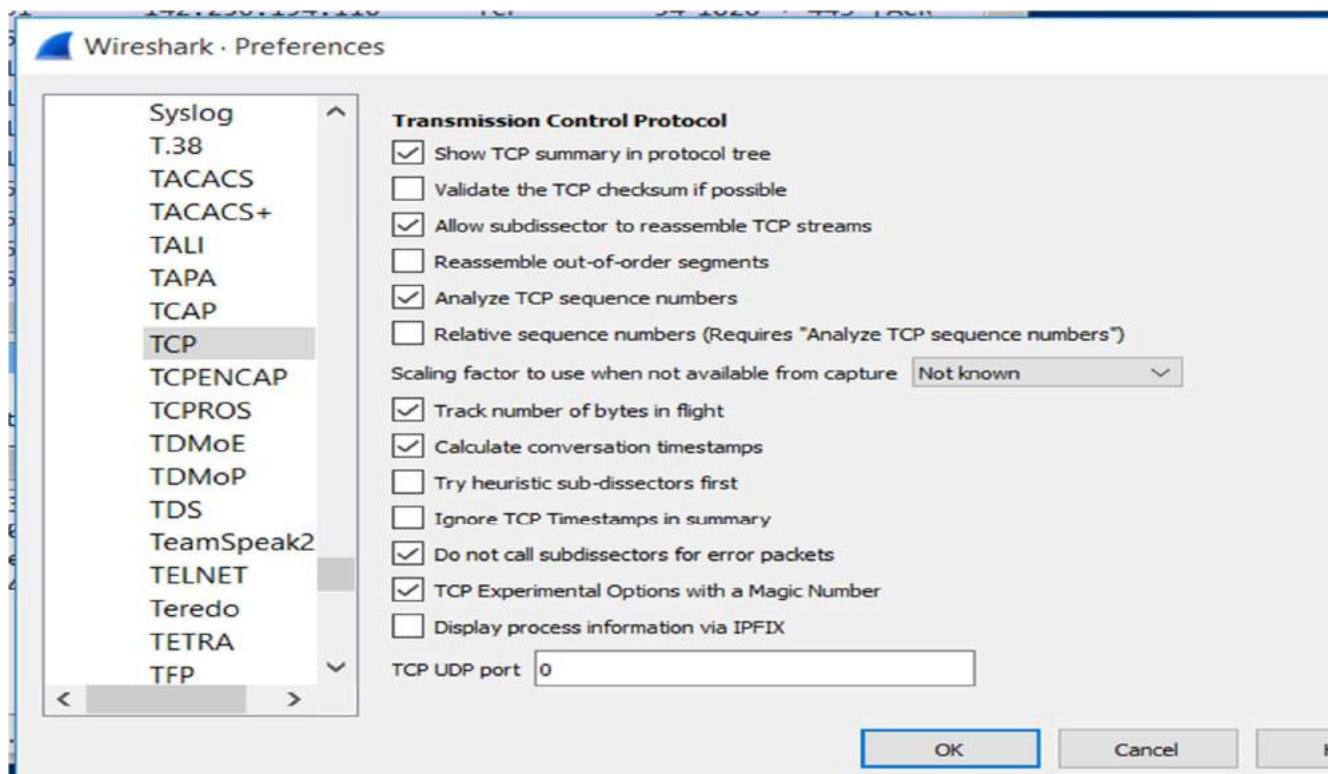
c. Capture live traffic from a site(for example google.com)

- 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

The image shows the Wireshark packet capture window. The display filter at the top is 'ip.addr==142.250.194.110'. The packet list shows the following data:

No.	Time	Source	Destination	Protocol	Length	Info
43697	107.121018	172.31.105.161	142.250.194.110	TCP	66	1828 → 443 [SYN]
43699	107.125236	142.250.194.110	172.31.105.161	TCP	66	443 → 1828 [SYN]
43700	107.125284	172.31.105.161	142.250.194.110	TCP	54	1828 → 443 [ACK]
43701	107.125933	172.31.105.161	142.250.194.110	TLSv1.3	2256	Client Hello
43702	107.126246	142.250.194.110	172.31.105.161	TCP	60	443 → 1828 [ACK]
43705	107.130130	142.250.194.110	172.31.105.161	TCP	66	443 → 1828 [ACK]
43751	107.197304	142.250.194.110	172.31.105.161	TLSv1.3	1466	Server Hello, C
43752	107.197304	142.250.194.110	172.31.105.161	TLSv1.3	101	Application Dat
43753	107.197358	172.31.105.161	142.250.194.110	TCP	54	1828 → 443 [ACK]
43754	107.197932	172.31.105.161	142.250.194.110	TLSv1.3	128	Change Cipher S
43755	107.198108	172.31.105.161	142.250.194.110	TLSv1.3	146	Application Dat
43756	107.198278	172.31.105.161	142.250.194.110	TLSv1.3	294	Application Dat

d. Finding Absolute packet number of a captured Packet



e. Finding packets with a particular ttl value

ip.ttl==128						
No.	Time	Source	Destination	Protocol	Length	Info
43673	107.114245	172.31.105.161	8.8.8.8	TLSv1.3	244	Application Dat
43674	107.114268	172.31.105.161	8.8.8.8	TLSv1.3	243	Application Dat
43680	107.118111	172.31.105.161	8.8.8.8	TCP	54	1827 → 443 [ACK
43681	107.118288	172.31.105.161	8.8.8.8	TLSv1.3	85	Application Dat
43686	107.118699	172.31.105.161	8.8.8.8	TCP	54	1827 → 443 [ACK
43689	107.118971	172.31.105.161	8.8.8.8	TCP	54	1827 → 443 [ACK
43691	107.119295	172.31.105.161	8.8.8.8	TLSv1.3	93	Application Dat
43694	107.120510	172.31.105.161	8.8.8.8	TCP	54	1827 → 443 [ACK
43696	107.120534	172.31.107.254	172.31.111.255	NBNS	92	Name query NB w
43697	107.121018	172.31.105.161	142.250.194.110	TCP	66	1828 → 443 [SYN
43700	107.125284	172.31.105.161	142.250.194.110	TCP	54	1828 → 443 [ACK
43701	107.125933	172.31.105.161	142.250.194.110	TLSv1.3	2256	Client Hello
43726	107.140728	172.31.105.161	192.168.134.6	TLSv1.2	134	Application Dat
43731	107.154893	172.31.105.119	172.31.111.255	NBNS	92	Name query NB w
43741	107.171926	172.31.105.161	8.8.8.8	TCP	54	1827 → 443 [ACK
43747	107.191161	172.31.105.161	8.8.8.8	TCP	54	1827 → 443 [ACK
43749	107.191213	172.31.105.161	8.8.8.8	TCP	54	1827 → 443 [ACK
43750	107.191852	172.31.105.161	8.8.8.8	TLSv1.3	93	Application Dat
43753	107.197358	172.31.105.161	142.250.194.110	TCP	54	1828 → 443 [ACK

f. Finding a string in the capture

frame contains "google"						
No.	Time	Source	Destination	Protocol	Length	Info
43646	107.017281	172.31.105.161	8.8.8.8	DNS	70	Standard query 0x5bb
43647	107.017415	172.31.105.161	8.8.8.8	DNS	70	Standard query 0x608
43650	107.022154	8.8.8.8	172.31.105.161	DNS	146	Standard query respon
43651	107.022341	8.8.8.8	172.31.105.161	DNS	102	Standard query respon
43655	107.028235	172.31.105.161	8.8.8.8	TLSv1.3	2320	Client Hello
43701	107.125933	172.31.105.161	142.250.194.110	TLSv1.3	2256	Client Hello
1359...	323.328163	8.8.8.8	172.31.103.48	DNS	103	Standard query respon
1722...	407.423398	172.31.105.161	8.8.8.8	DNS	70	Standard query 0x32b
1722...	407.423503	172.31.105.161	8.8.8.8	DNS	70	Standard query 0xcab
1722...	407.427189	8.8.8.8	172.31.105.161	DNS	102	Standard query respon
1722...	407.427634	8.8.8.8	172.31.105.161	DNS	146	Standard query respon
1722...	407.432749	172.31.105.161	8.8.8.8	TLSv1.3	2288	Client Hello

Lab Assignment

1. http version 1.1

```

> Internet Protocol Version 4, Src: 117.239.91.97, Dst: 172.31.103.48
> Transmission Control Protocol, Src Port: 80, Dst Port: 58694, Seq: 551542207, Ack: 3809174637, Len: 267
▼ 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]

```


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]
```