CEGEP VANIER COLLEGE
CENTRE FOR CONTINUING EDUCATION
Cybersecurity
420- 950-VA

Teacher: Samir Chebbine **Lab 2** **Jan 29, 2025**

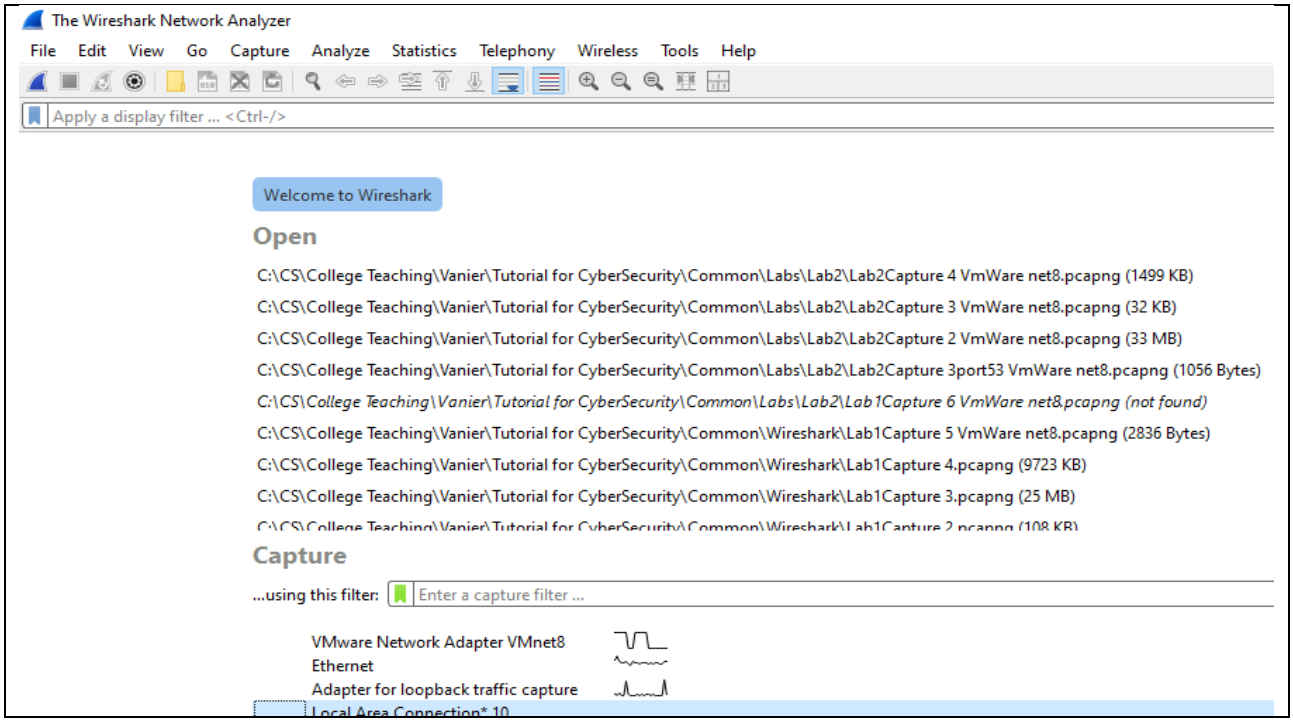
Lab 2: Introduction to Networking, Wireshark Network Analyser & Anonymous Surfing

Complete all these following sections as explained in **class.** All *steps* were presented during class time.

Create and Submit a Word file ***Lab2CybersecurityYourName.doc*** which contains answers of Book Exercises and output screenshots for every Project. Submit all packet capture files if any.

1. **Install Wireshark Network Analyser:**

a) **Download Wireshark Network https://www.wireshark.org/download.html** as shown hereafter in Figure.



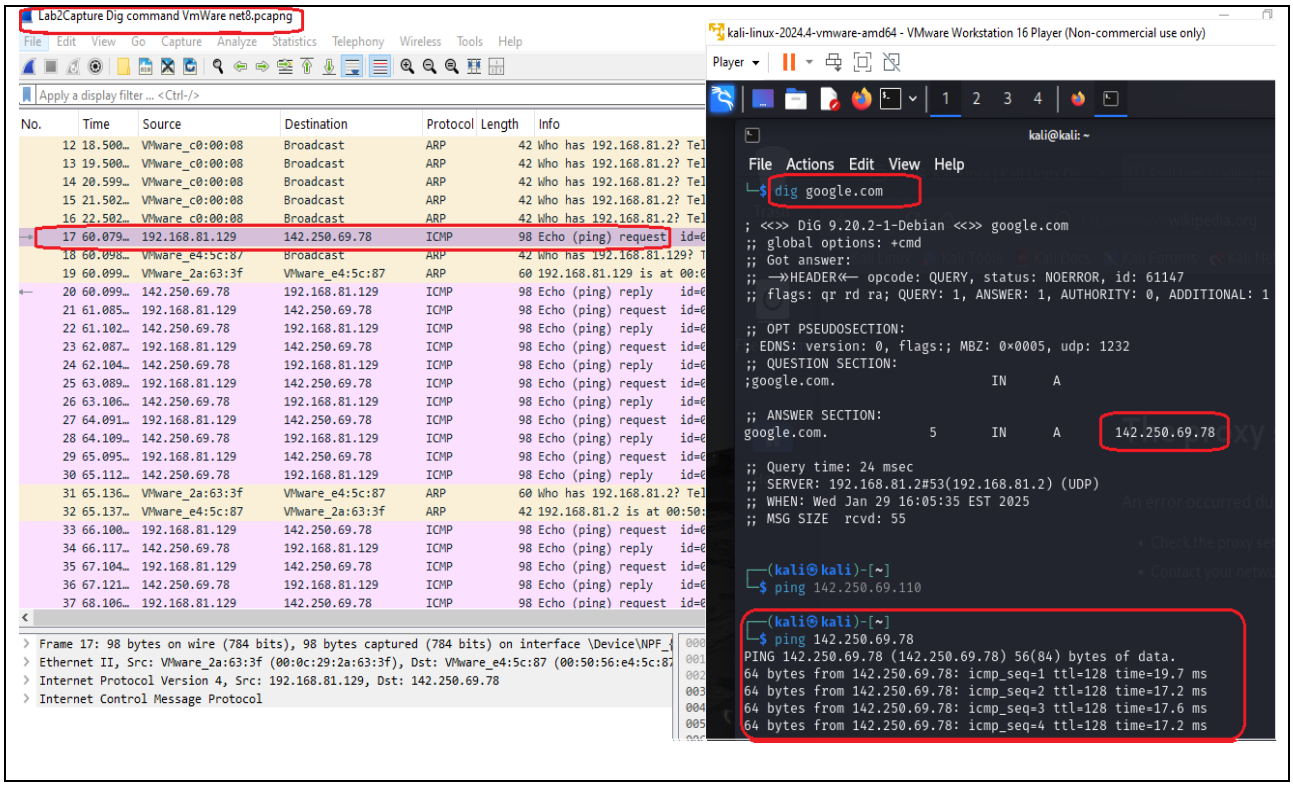
2. **On Kali Linux distribution:**

a) **Command mode - provide screenshot of each output:** Using Kali Linux command mode, execute Linux command dig in a command-line tool that queries and returns the IP address for the google.com Domain Name System (DNS) as shown hereafter.

b) **Ping the returned Google DNS IP address**

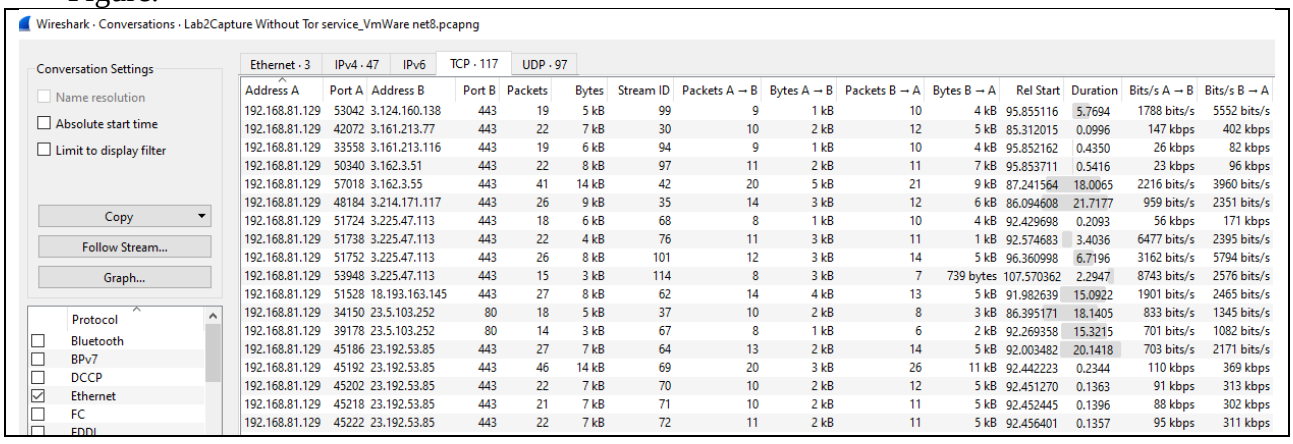
c) What is the name of protocol used in command ping, describe the inner workings of that protocol. Open **Wireshark Traffic analyser** to capture traffic sent from my computer station (in my case 192.168.81.129) towards DNS server 142.250.69.78 as shown hereafter.

d) **Save the packet capture as Lab2Capture Dig command VmWare net8.pcapng** as shown hereafter.



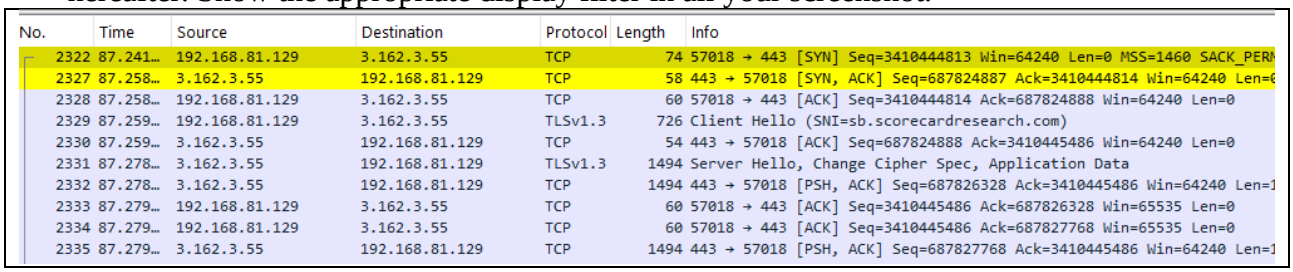
3. Conversations in Wireshark packet analysis:

a) **Provide screenshot of Wireshark showing conversation statistics** as shown hereafter in Figure.



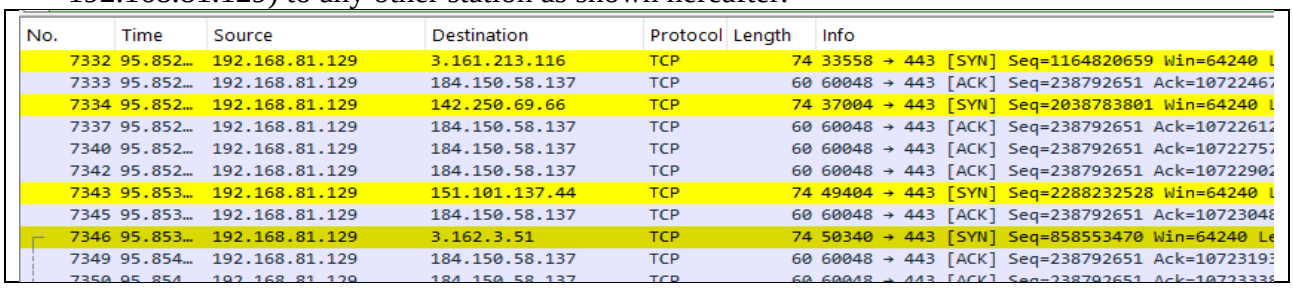
Address A	Port A	Address B	Port B	Packets	Bytes	Stream ID	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
192.168.81.129	53042	3.124.160.138	443	19	5 kB	99	9	1 kB	10	4 kB	95.855116	5.7694	1788 bits/s	5552 bits/s
192.168.81.129	42072	3.161.213.77	443	22	7 kB	30	10	2 kB	12	5 kB	85.312015	0.0996	147 kbps	402 kbps
192.168.81.129	33558	3.161.213.116	443	19	6 kB	94	9	1 kB	10	4 kB	95.852162	0.4350	26 kbps	82 kbps
192.168.81.129	50340	3.162.3.51	443	22	8 kB	97	11	2 kB	11	7 kB	95.853711	0.5416	23 kbps	96 kbps
192.168.81.129	57018	3.162.3.55	443	41	14 kB	42	20	5 kB	21	9 kB	87.241564	18.0065	2216 bits/s	3960 bits/s
192.168.81.129	48184	3.214.171.117	443	26	9 kB	35	14	3 kB	12	6 kB	86.094608	21.7177	959 bits/s	2351 bits/s
192.168.81.129	51724	3.225.47.113	443	18	6 kB	68	8	1 kB	10	4 kB	92.429698	0.2093	56 kbps	171 kbps
192.168.81.129	51738	3.225.47.113	443	22	4 kB	76	11	3 kB	11	1 kB	92.574683	3.4036	6477 bits/s	2395 bits/s
192.168.81.129	51752	3.225.47.113	443	26	8 kB	101	12	3 kB	14	5 kB	96.360998	6.7196	3162 bits/s	5794 bits/s
192.168.81.129	53948	3.225.47.113	443	15	3 kB	114	8	3 kB	7	739 bytes	107.570362	2.2947	8743 bits/s	2576 bits/s
192.168.81.129	51528	18.193.163.145	443	27	8 kB	62	14	4 kB	13	5 kB	91.982639	15.0922	1901 bits/s	2465 bits/s
192.168.81.129	34150	23.5.103.252	80	18	5 kB	37	10	2 kB	8	3 kB	86.395171	18.1405	833 bits/s	1345 bits/s
192.168.81.129	39178	23.5.103.252	80	14	3 kB	67	8	1 kB	6	2 kB	92.269358	15.3215	701 bits/s	1082 bits/s
192.168.81.129	45186	23.192.53.85	443	27	7 kB	64	13	2 kB	14	5 kB	92.003482	20.1418	703 bits/s	2171 bits/s
192.168.81.129	45192	23.192.53.85	443	46	14 kB	69	20	3 kB	26	11 kB	92.442223	0.2344	110 kbps	369 kbps
192.168.81.129	45202	23.192.53.85	443	22	7 kB	70	10	2 kB	12	5 kB	92.451270	0.1363	91 kbps	313 kbps
192.168.81.129	45218	23.192.53.85	443	21	7 kB	71	10	2 kB	11	5 kB	92.452445	0.1396	88 kbps	302 kbps
192.168.81.129	45222	23.192.53.85	443	22	7 kB	72	11	2 kB	11	5 kB	92.456401	0.1357	95 kbps	311 kbps

b) Appy filter in conversation windows to display all traffic from your station (in my case 192.168.81.129) and port 57018 (choose any other port) to any other station as shown hereafter. Show the appropriate display filter in all your screenshot.



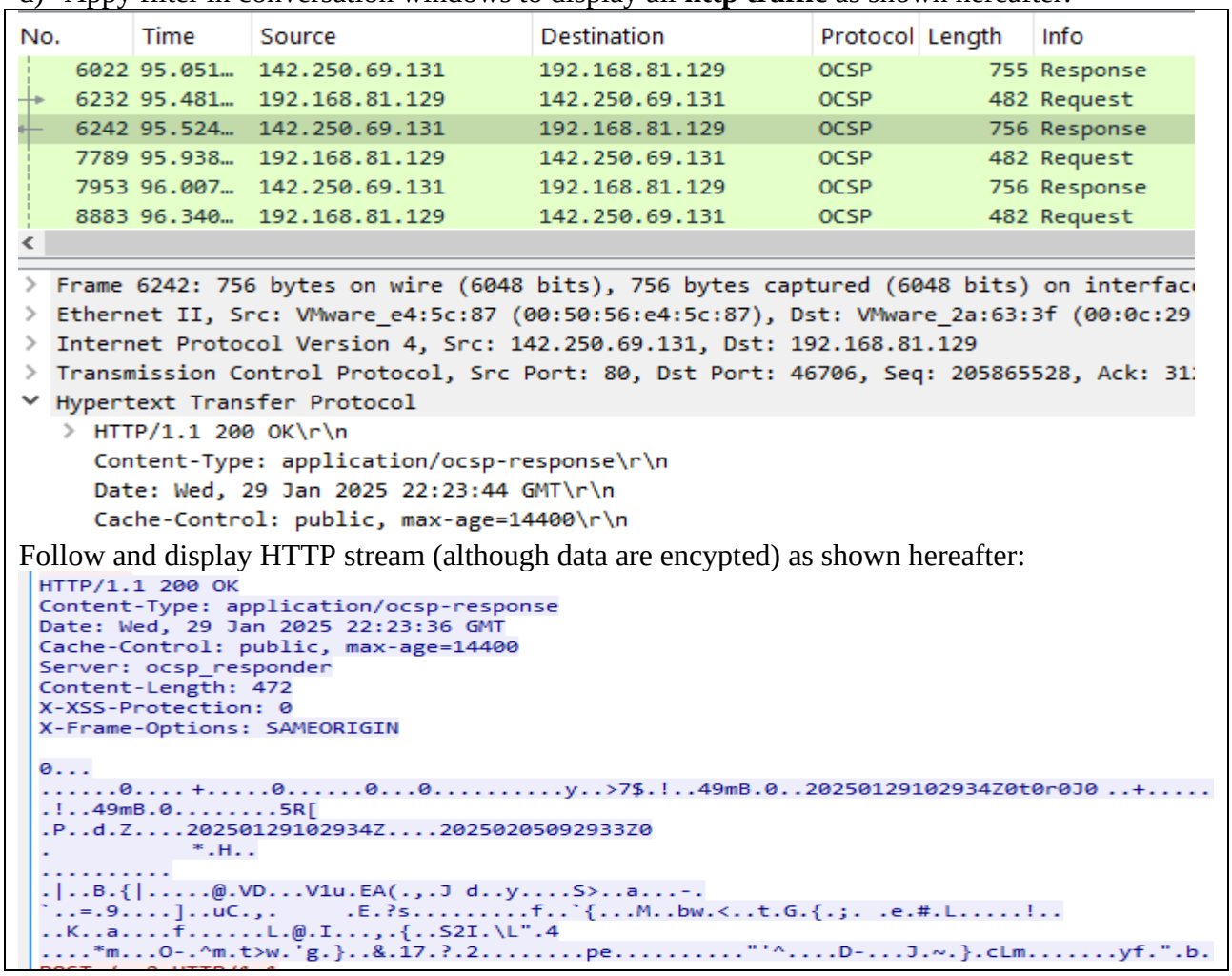
No.	Time	Source	Destination	Protocol	Length	Info
2322	87.241…	192.168.81.129	3.162.3.55	TCP	74	57018 → 443 [SYN] Seq=3410444813 Win=64240 Len=0 MSS=1460 SACK_PERM
2327	87.258…	3.162.3.55	192.168.81.129	TCP	58	443 → 57018 [SYN, ACK] Seq=687824887 Ack=3410444814 Win=64240 Len=0
2328	87.258…	192.168.81.129	3.162.3.55	TCP	60	57018 → 443 [ACK] Seq=3410444814 Ack=687824888 Win=64240 Len=0
2329	87.259…	192.168.81.129	3.162.3.55	TLSv1.3	726	Client Hello (SNI=sb.scorecardresearch.com)
2330	87.259…	3.162.3.55	192.168.81.129	TCP	54	443 → 57018 [ACK] Seq=687824888 Ack=3410445486 Win=64240 Len=0
2331	87.278…	3.162.3.55	192.168.81.129	TLSv1.3	1494	Server Hello, Change Cipher Spec, Application Data
2332	87.278…	3.162.3.55	192.168.81.129	TCP	1494	443 → 57018 [PSH, ACK] Seq=687826328 Ack=3410445486 Win=64240 Len=1
2333	87.279…	192.168.81.129	3.162.3.55	TCP	60	57018 → 443 [ACK] Seq=3410445486 Ack=687826328 Win=65535 Len=0
2334	87.279…	192.168.81.129	3.162.3.55	TCP	60	57018 → 443 [ACK] Seq=3410445486 Ack=687827768 Win=65535 Len=0
2335	87.279…	3.162.3.55	192.168.81.129	TCP	1494	443 → 57018 [PSH, ACK] Seq=687827768 Ack=3410445486 Win=64240 Len=1

c) Appy filter in conversation windows to display all traffic from your station (in my case 192.168.81.129) to any other station as shown hereafter.



No.	Time	Source	Destination	Protocol	Length	Info
7332	95.852…	192.168.81.129	3.161.213.116	TCP	74	33558 → 443 [SYN] Seq=1164820659 Win=64240 L
7333	95.852…	192.168.81.129	184.150.58.137	TCP	60	60048 → 443 [ACK] Seq=238792651 Ack=10722467
7334	95.852…	192.168.81.129	142.250.69.66	TCP	74	37004 → 443 [SYN] Seq=2038783801 Win=64240 L
7337	95.852…	192.168.81.129	184.150.58.137	TCP	60	60048 → 443 [ACK] Seq=238792651 Ack=10722612
7340	95.852…	192.168.81.129	184.150.58.137	TCP	60	60048 → 443 [ACK] Seq=238792651 Ack=10722757
7342	95.852…	192.168.81.129	184.150.58.137	TCP	60	60048 → 443 [ACK] Seq=238792651 Ack=10722902
7343	95.853…	192.168.81.129	151.101.137.44	TCP	74	49404 → 443 [SYN] Seq=2288232528 Win=64240 L
7345	95.853…	192.168.81.129	184.150.58.137	TCP	60	60048 → 443 [ACK] Seq=238792651 Ack=1072304
7346	95.853…	192.168.81.129	3.162.3.51	TCP	74	50340 → 443 [SYN] Seq=858553470 Win=64240 Le
7349	95.854…	192.168.81.129	184.150.58.137	TCP	60	60048 → 443 [ACK] Seq=238792651 Ack=1072319

d) Appy filter in conversation windows to display all **http traffic** as shown hereafter.



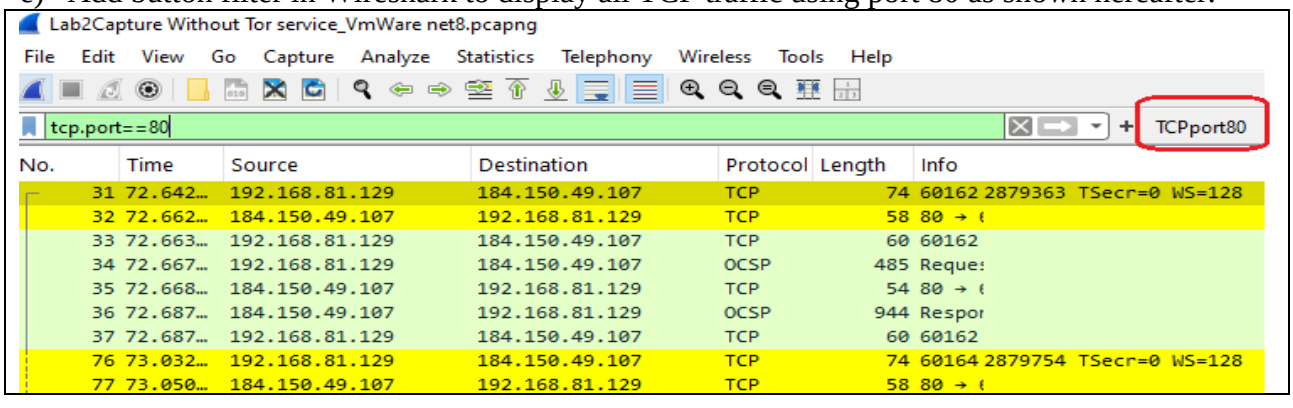
No.	Time	Source	Destination	Protocol	Length	Info
6022	95.051…	142.250.69.131	192.168.81.129	OCSP	755	Response
6232	95.481…	192.168.81.129	142.250.69.131	OCSP	482	Request
6242	95.524…	142.250.69.131	192.168.81.129	OCSP	756	Response
7789	95.938…	192.168.81.129	142.250.69.131	OCSP	482	Request
7953	96.007…	142.250.69.131	192.168.81.129	OCSP	756	Response
8883	96.340…	192.168.81.129	142.250.69.131	OCSP	482	Request

```
> Frame 6242: 756 bytes on wire (6048 bits), 756 bytes captured (6048 bits) on interfac
> Ethernet II, Src: VMware_e4:5c:87 (00:50:56:e4:5c:87), Dst: VMware_2a:63:3f (00:0c:29
> Internet Protocol Version 4, Src: 142.250.69.131, Dst: 192.168.81.129
> Transmission Control Protocol, Src Port: 80, Dst Port: 46706, Seq: 205865528, Ack: 31
v Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Content-Type: application/ocsp-response\r\n
    Date: Wed, 29 Jan 2025 22:23:44 GMT\r\n
    Cache-Control: public, max-age=14400\r\n
```

Follow and display HTTP stream (although data are encypted) as shown hereafter:

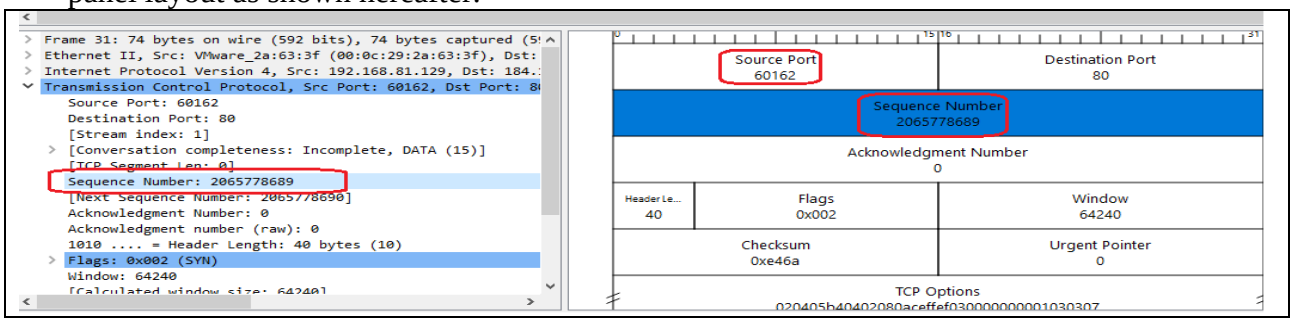
```
HTTP/1.1 200 OK
Content-Type: application/ocsp-response
Date: Wed, 29 Jan 2025 22:23:36 GMT
Cache-Control: public, max-age=14400
Server: ocsp_responder
Content-Length: 472
X-XSS-Protection: 0
X-Frame-Options: SAMEORIGIN

0...
......0.... +.....0......0...0.........y..>7$.!..49mB.0..20250129102934Z0t0r0J0 ..+.....
.!..49mB.0........5R[
.P..d.Z....20250129102934Z....20250205092933Z0
.           *.H..
.........
.|..B.{|.....@.VD...V1u.EA(.,.J d..y....S>..a...-.
`..=.9....]..uC.,.     .E.?s.........f..`{...M..bw.<..t.G.{.;. .e.#.L.....!..
..K..a....f......L.@.I...,.{..S2I.\L".4
....*m...O-.^m.t>w.'g.}..&.17.?.2........pe.........."'^....D-...J.~.}.cLm.......yf.".b.
```

e) Add button filter in Wireshark to display all TCP traffic using port 80 as shown hereafter.

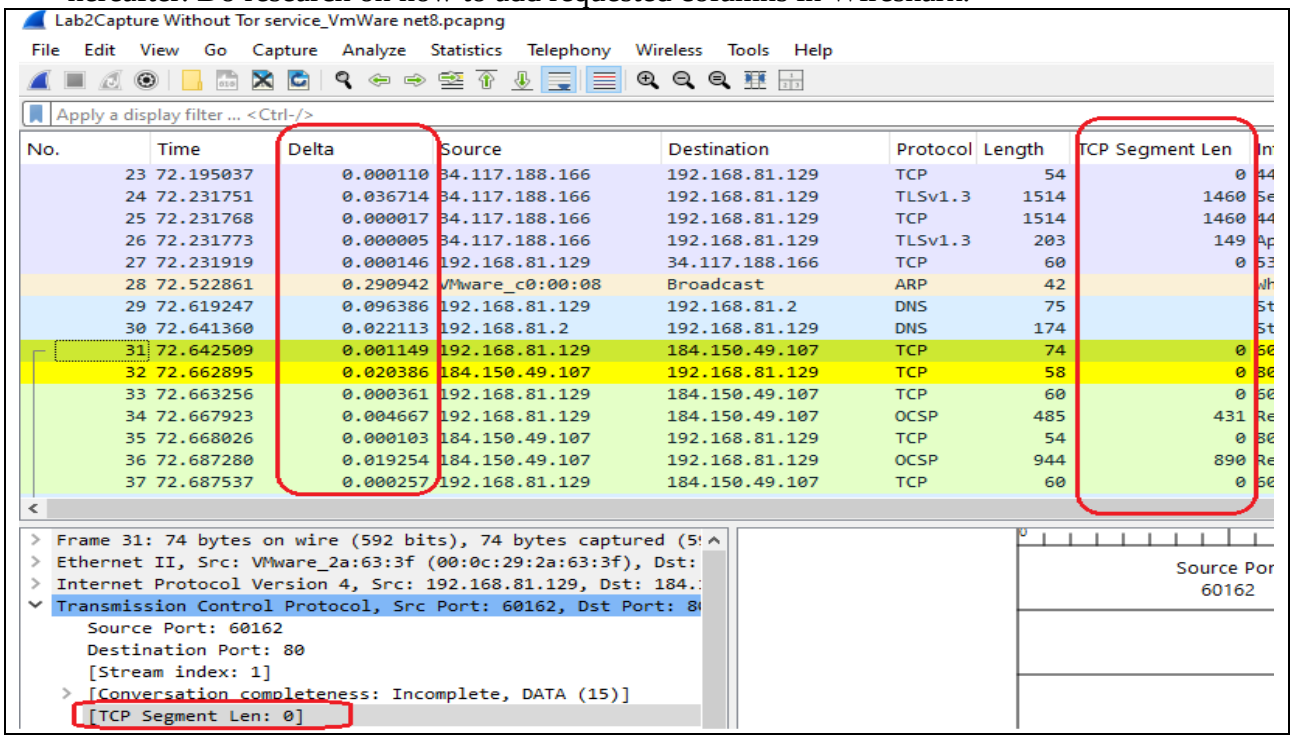


No.	Time	Source	Destination	Protocol	Length	Info
31	72.642…	192.168.81.129	184.150.49.107	TCP	74	60162 2879363 TSecr=0 WS=128
32	72.662…	184.150.49.107	192.168.81.129	TCP	58	80 → (
33	72.663…	192.168.81.129	184.150.49.107	TCP	60	60162
34	72.667…	192.168.81.129	184.150.49.107	OCSP	485	Reque:
35	72.668…	184.150.49.107	192.168.81.129	TCP	54	80 → (
36	72.687…	184.150.49.107	192.168.81.129	OCSP	944	Respor
37	72.687…	192.168.81.129	184.150.49.107	TCP	60	60162
76	73.032…	192.168.81.129	184.150.49.107	TCP	74	60164 2879754 TSecr=0 WS=128
77	73.050…	184.150.49.107	192.168.81.129	TCP	58	80 → (

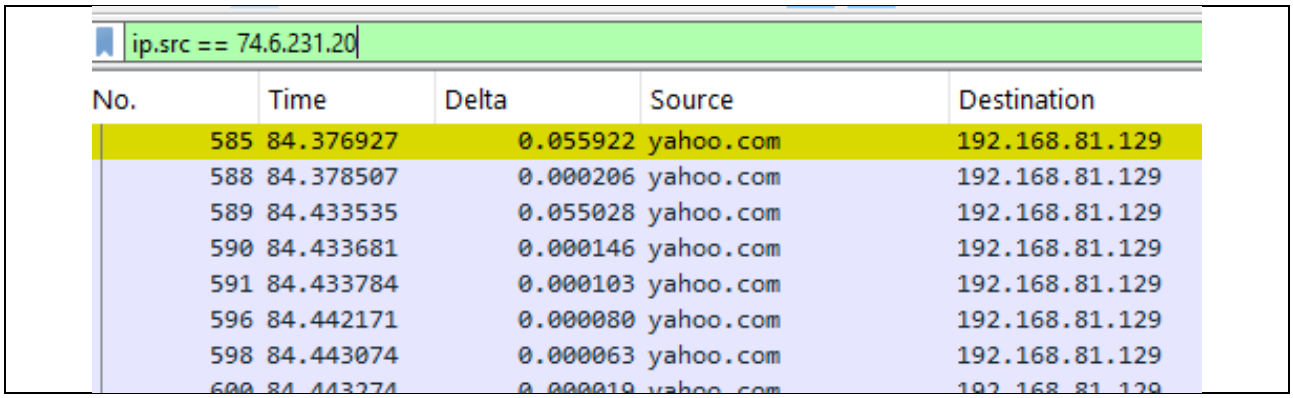
f) Configure Wireshark to display detail of packet diagram detail (name and values) in the third panel layout as shown hereafter.



g) Configure Wireshark to add two columns (Delta and TCP Segment Length) in order to get detail view of each packet timing and TCP data segment length respectively as shown hereafter. Do research on how to add requested columns in Wireshark.

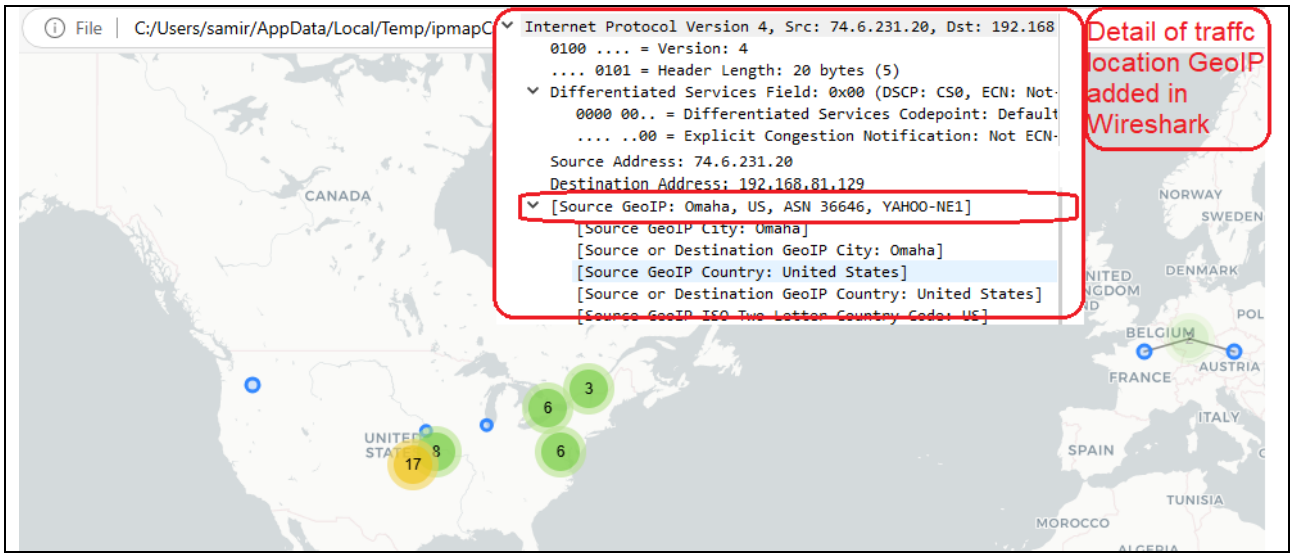


h) Resolve the naming of host computers to display host name instead of IP address if any as shown hereafter. Do research on how to resolve IP addresses in Wireshark.



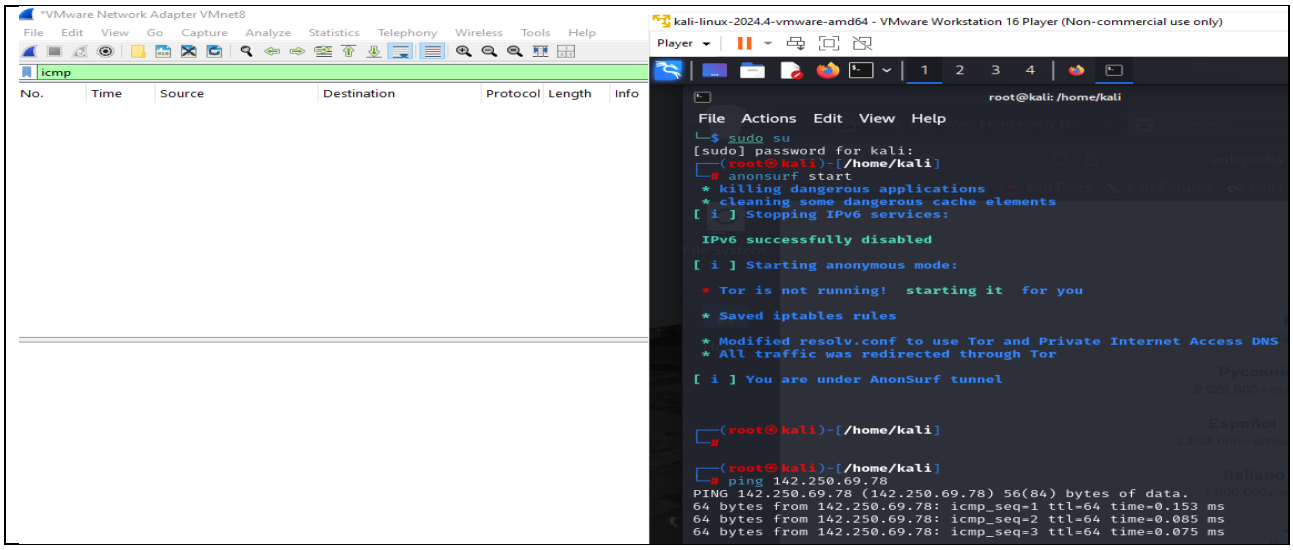
4. Geo IP using MaxMind database in Wireshark

a) Do research on how to add Geo IP localisation using MaxMind database in Wireshark as tool of digital forensics when assessing ethical penetration as shown hereafter in Figure.



5. Start Anonymous surfing using Tor browser

a) Install **anonsurf program** as done in class to surf anonymously. Do research on how to **configure embedded FireFox browser in Linux Kali distribution to use Tor browser and Tor network. Always prioritize the ethical and legal use of Tor. You can search anonymously but keep in mind to use it ethically** as shown hereafter.



b) Check in Wireshark using appropriate display capture that ICMP messages were not detected since the surfing is anonymous as shown above in Figure.

c) Use **Macchanger program** in Kali Linux distribution to change the MAC address of your network interface card to surf anonymously as done in class.