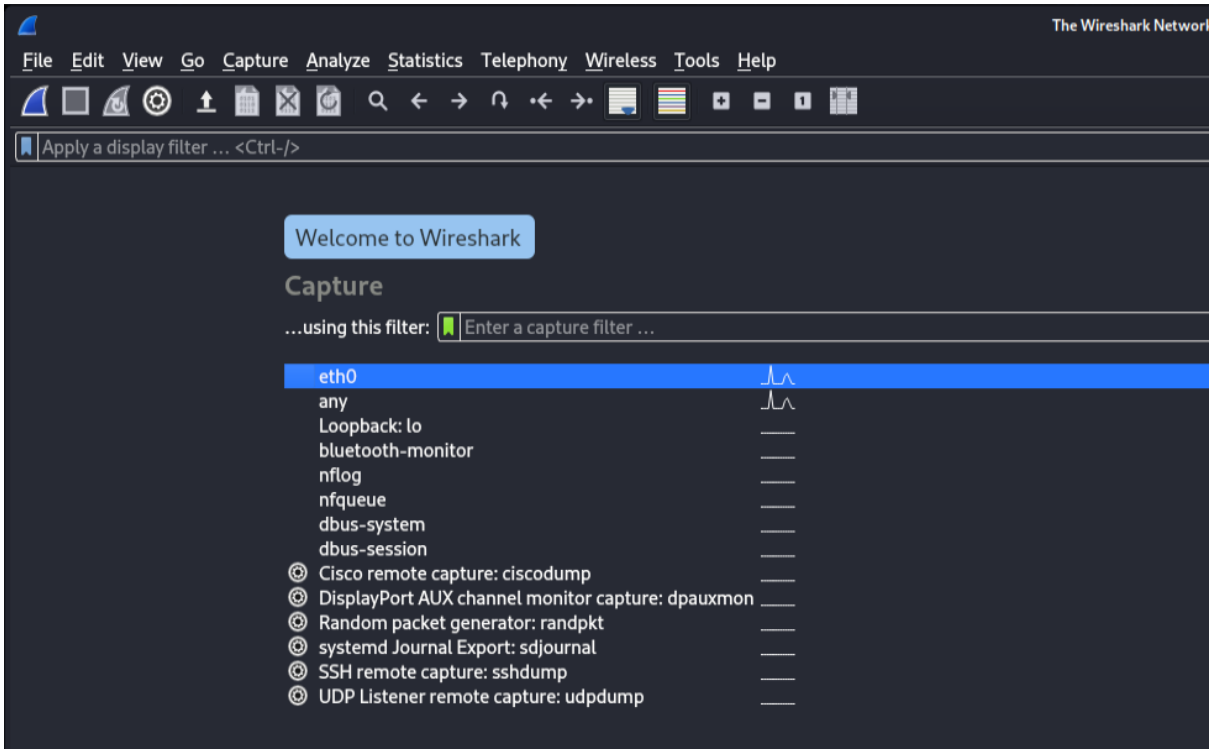
TASK 5

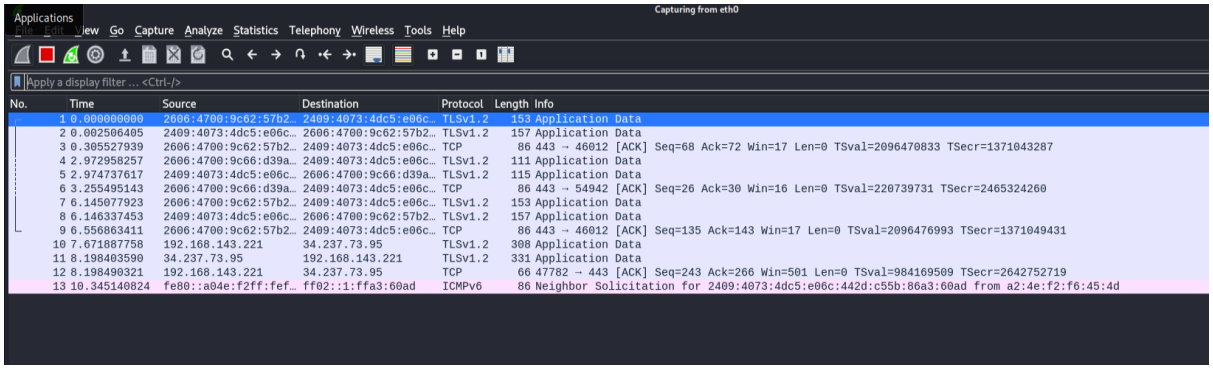
1.Install Wireshark

- Download from: https://www.wireshark.org/download.html
- During installation, allow **WinPcap/Npcap** (for packet capture)
- IF on Linux, search Wireshark in the applications tab.

2.Start capturing on your active network interface.



- Select your **active network adapter** (e.g., Wi-Fi or Ethernet.
- Click the **blue shark fin icon** to start capturing

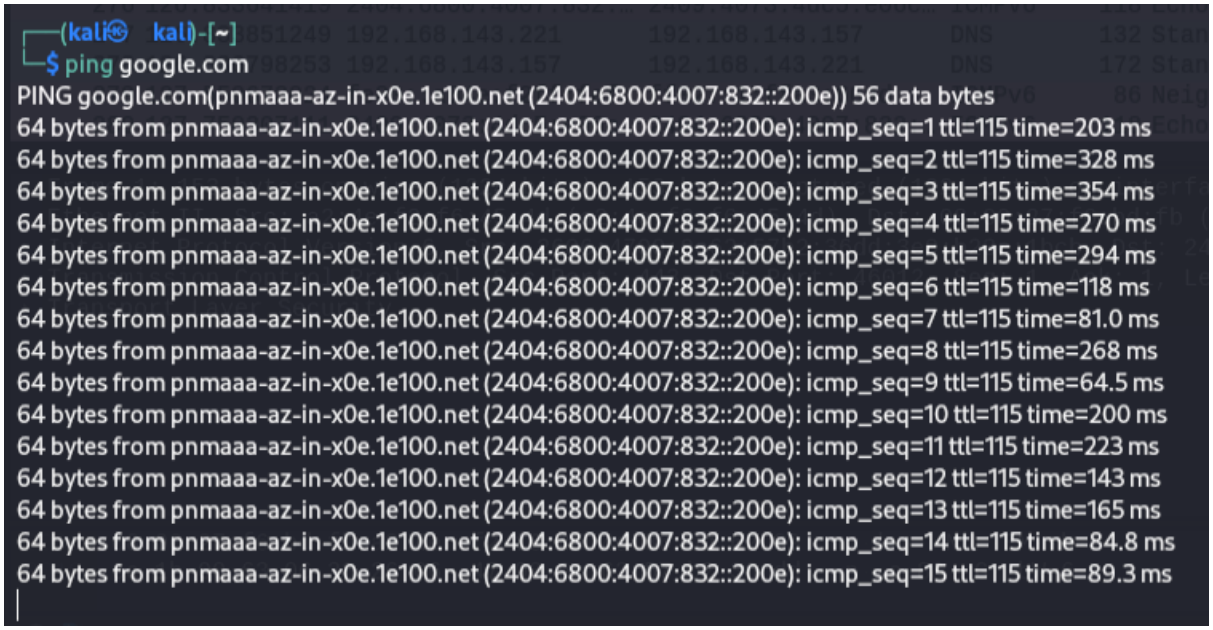


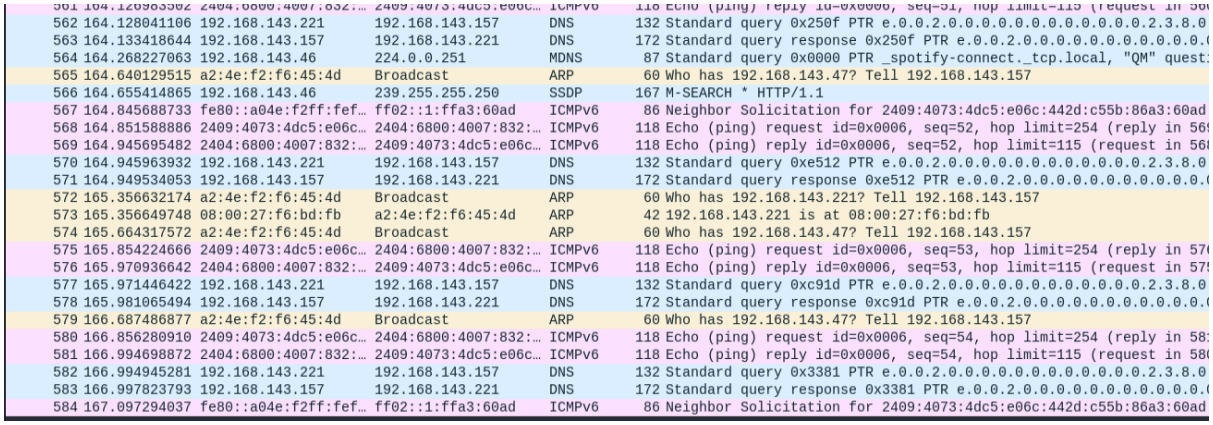
3.Browse a website or ping a server to generate traffic.

Open a browser and:

- Visit a website (e.g., https://example.com)
- Or run in terminal:

  ping google.com





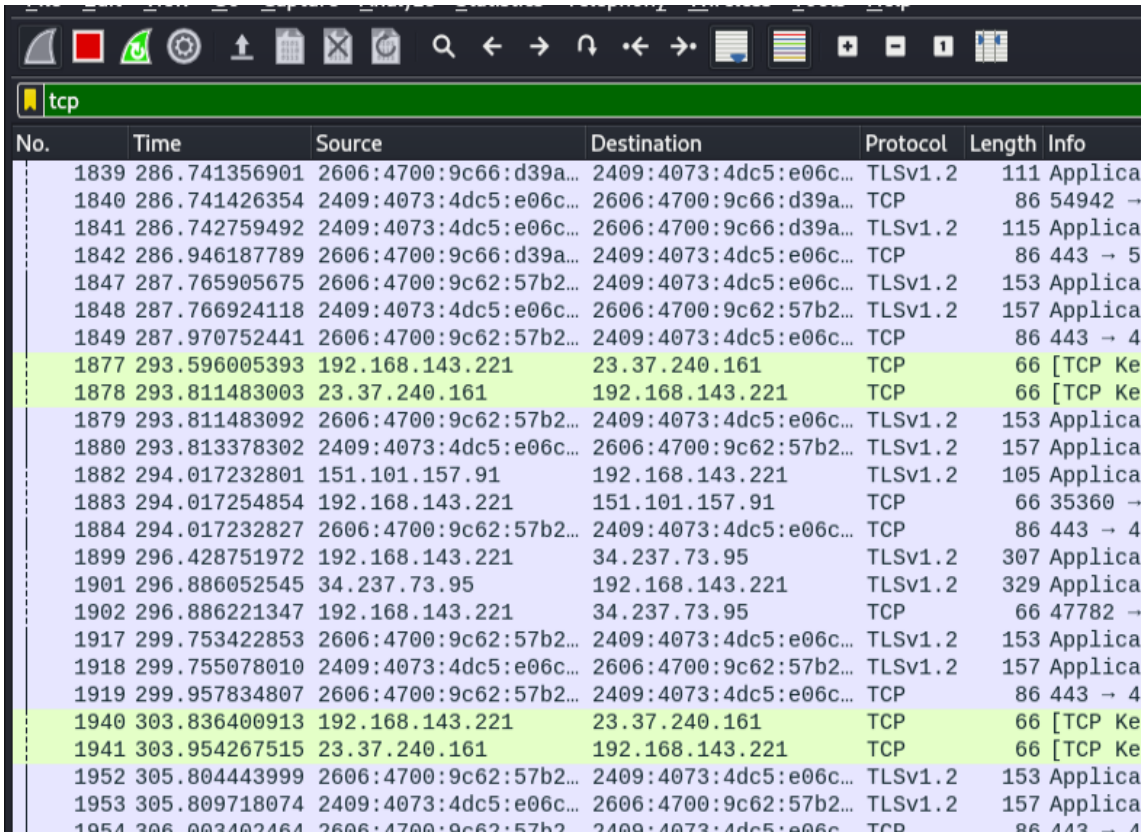
562	164.128041106	192.168.143.221	192.168.143.157	DNS	132	Standard query 0x250f PTR e.0.0.2.0.0.0.0.0.0.0.0.0.0.0.0.2.3.8.0
563	164.133418644	192.168.143.157	192.168.143.221	DNS	172	Standard query response 0x250f PTR e.0.0.2.0.0.0.0.0.0.0.0.0.0.0.0.
564	164.268227063	192.168.143.46	224.0.0.251	MDNS	87	Standard query 0x0000 PTR _spotify-connect._tcp.local, "QM" quest
565	164.640129515	a2:4e:f2:f6:45:4d	Broadcast	ARP	60	Who has 192.168.143.47? Tell 192.168.143.157
566	164.655414865	192.168.143.46	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
567	164.845688733	fe80::a04e:f2ff:fef…	ff02::1:ffa3:60ad	ICMPv6	86	Neighbor Solicitation for 2409:4073:4dc5:e06c:442d:c55b:86a3:60ad
568	164.851588886	2409:4073:4dc5:e06c…	2404:6800:4007:832:…	ICMPv6	118	Echo (ping) request id=0x0006, seq=52, hop limit=254 (reply in 56
569	164.945695482	2404:6800:4007:832:…	2409:4073:4dc5:e06c…	ICMPv6	118	Echo (ping) reply id=0x0006, seq=52, hop limit=115 (request in 56
570	164.945963932	192.168.143.221	192.168.143.157	DNS	132	Standard query 0xe512 PTR e.0.0.2.0.0.0.0.0.0.0.0.0.0.0.0.2.3.8.0
571	164.949534053	192.168.143.157	192.168.143.221	DNS	172	Standard query response 0xe512 PTR e.0.0.2.0.0.0.0.0.0.0.0.0.0.0.0.
572	165.356632174	a2:4e:f2:f6:45:4d	Broadcast	ARP	60	Who has 192.168.143.221? Tell 192.168.143.157
573	165.356649748	08:00:27:f6:bd:fb	a2:4e:f2:f6:45:4d	ARP	42	192.168.143.221 is at 08:00:27:f6:bd:fb
574	165.664317572	a2:4e:f2:f6:45:4d	Broadcast	ARP	60	Who has 192.168.143.47? Tell 192.168.143.157
575	165.854224666	2409:4073:4dc5:e06c…	2404:6800:4007:832:…	ICMPv6	118	Echo (ping) request id=0x0006, seq=53, hop limit=254 (reply in 57
576	165.970936642	2404:6800:4007:832:…	2409:4073:4dc5:e06c…	ICMPv6	118	Echo (ping) reply id=0x0006, seq=53, hop limit=115 (request in 57
577	165.971446422	192.168.143.221	192.168.143.157	DNS	132	Standard query 0xc91d PTR e.0.0.2.0.0.0.0.0.0.0.0.0.0.0.0.2.3.8.0
578	165.981065494	192.168.143.157	192.168.143.221	DNS	172	Standard query response 0xc91d PTR e.0.0.2.0.0.0.0.0.0.0.0.0.0.0.0.
579	166.687486877	a2:4e:f2:f6:45:4d	Broadcast	ARP	60	Who has 192.168.143.47? Tell 192.168.143.157
580	166.856280910	2409:4073:4dc5:e06c…	2404:6800:4007:832:…	ICMPv6	118	Echo (ping) request id=0x0006, seq=54, hop limit=254 (reply in 58
581	166.994698872	2404:6800:4007:832:…	2409:4073:4dc5:e06c…	ICMPv6	118	Echo (ping) reply id=0x0006, seq=54, hop limit=115 (request in 58
582	166.994945281	192.168.143.221	192.168.143.157	DNS	132	Standard query 0x3381 PTR e.0.0.2.0.0.0.0.0.0.0.0.0.0.0.0.2.3.8.0
583	166.997823793	192.168.143.157	192.168.143.221	DNS	172	Standard query response 0x3381 PTR e.0.0.2.0.0.0.0.0.0.0.0.0.0.0.0.
584	167.097294037	fe80::a04e:f2ff:fef…	ff02::1:ffa3:60ad	ICMPv6	86	Neighbor Solicitation for 2409:4073:4dc5:e06c:442d:c55b:86a3:60ad

4.Stop capture after a minute.

- Wait 30–60 seconds
- Click the **red square icon** to stop the capture

5.Filter captured packets by protocol (e.g., HTTP, DNS, TCP).

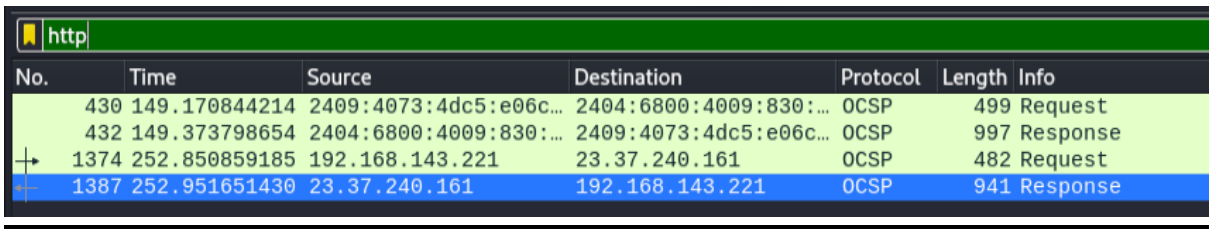
TCP



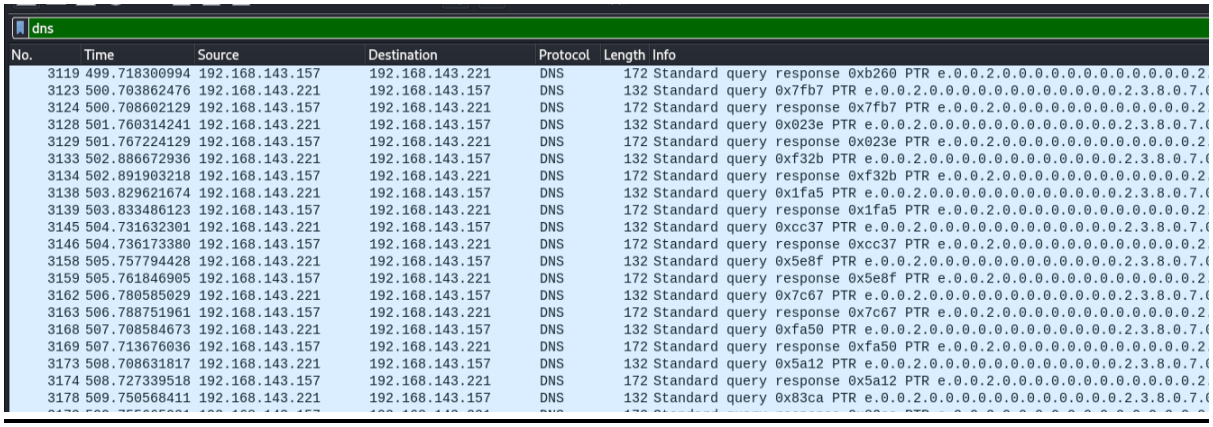
tcp

No.	Time	Source	Destination	Protocol	Length	Info
1839	286.741356901	2606:4700:9c66:d39a…	2409:4073:4dc5:e06c…	TLSv1.2	111	Applica
1840	286.741426354	2409:4073:4dc5:e06c…	2606:4700:9c66:d39a…	TCP	86	54942 →
1841	286.742759492	2409:4073:4dc5:e06c…	2606:4700:9c66:d39a…	TLSv1.2	115	Applica
1842	286.946187789	2606:4700:9c66:d39a…	2409:4073:4dc5:e06c…	TCP	86	443 → 5
1847	287.765905675	2606:4700:9c62:57b2…	2409:4073:4dc5:e06c…	TLSv1.2	153	Applica
1848	287.766924118	2409:4073:4dc5:e06c…	2606:4700:9c62:57b2…	TLSv1.2	157	Applica
1849	287.970752441	2606:4700:9c62:57b2…	2409:4073:4dc5:e06c…	TCP	86	443 → 4
1877	293.596005393	192.168.143.221	23.37.240.161	TCP	66	[TCP Ke
1878	293.811483003	23.37.240.161	192.168.143.221	TCP	66	[TCP Ke
1879	293.811483092	2606:4700:9c62:57b2…	2409:4073:4dc5:e06c…	TLSv1.2	153	Applica
1880	293.813378302	2409:4073:4dc5:e06c…	2606:4700:9c62:57b2…	TLSv1.2	157	Applica
1882	294.017232801	151.101.157.91	192.168.143.221	TLSv1.2	105	Applica
1883	294.017254854	192.168.143.221	151.101.157.91	TCP	66	35360 →
1884	294.017232827	2606:4700:9c62:57b2…	2409:4073:4dc5:e06c…	TCP	86	443 → 4
1899	296.428751972	192.168.143.221	34.237.73.95	TLSv1.2	307	Applica
1901	296.886052545	34.237.73.95	192.168.143.221	TLSv1.2	329	Applica
1902	296.886221347	192.168.143.221	34.237.73.95	TCP	66	47782 →
1917	299.753422853	2606:4700:9c62:57b2…	2409:4073:4dc5:e06c…	TLSv1.2	153	Applica
1918	299.755078010	2409:4073:4dc5:e06c…	2606:4700:9c62:57b2…	TLSv1.2	157	Applica
1919	299.957834807	2606:4700:9c62:57b2…	2409:4073:4dc5:e06c…	TCP	86	443 → 4
1940	303.836400913	192.168.143.221	23.37.240.161	TCP	66	[TCP Ke
1941	303.954267515	23.37.240.161	192.168.143.221	TCP	66	[TCP Ke
1952	305.804443999	2606:4700:9c62:57b2…	2409:4073:4dc5:e06c…	TLSv1.2	153	Applica
1953	305.809718074	2409:4073:4dc5:e06c…	2606:4700:9c62:57b2…	TLSv1.2	157	Applica

HTTP



DNS



6.Identify at least 3 different protocols in the capture.

Protocol	**Description**
TCP	Transmission Control Protocol – reliable transport layer
DNS	Domain Name System – resolves hostnames
HTTP/HTTPS	Web traffic protocol (unencrypted/encrypted)
ICMP	Used for pings (echo requests/replies)

7.Export the capture as a .pcap file.

- Go to **File → Save As**
- Name your file (e.g., capture_lab1.pcap)
- Save in .pcap or .pcapng format