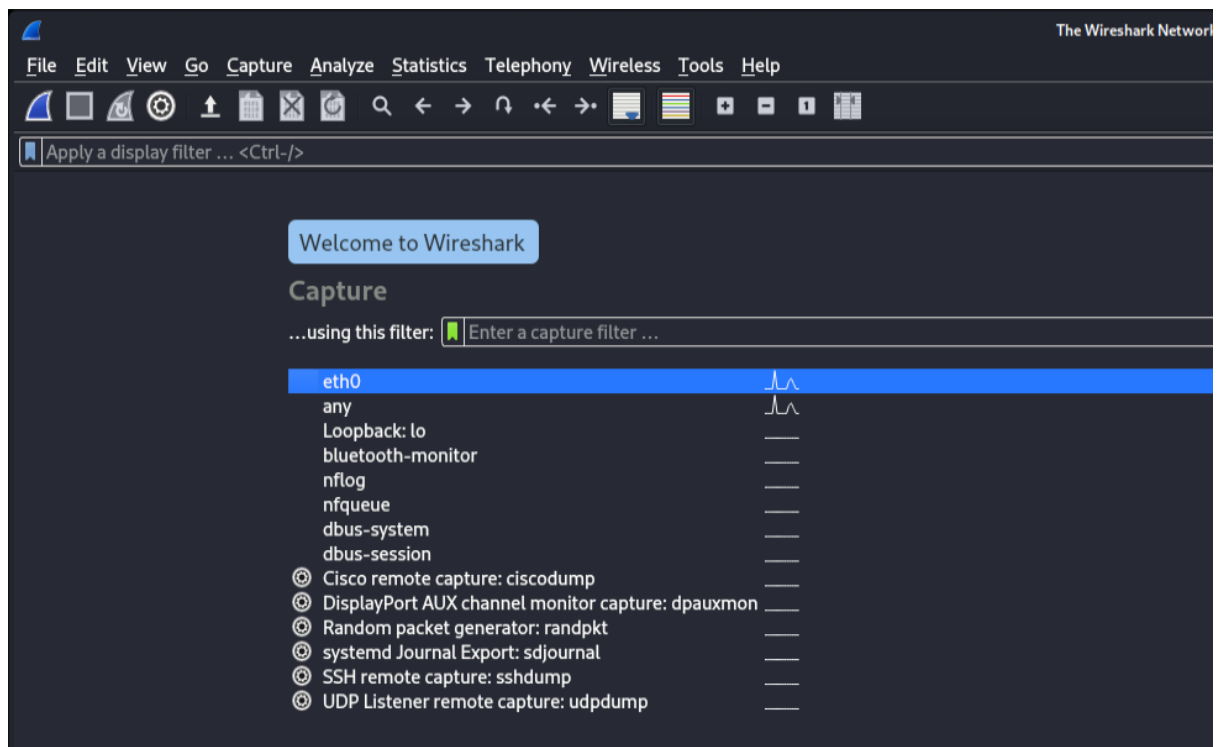


TASK 5

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

Applications						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
Capturing from eth0						
Apply a display filter ... <Ctrl-/>						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	2409:4073:4dc5:e06c::	2409:4073:4dc5:e06c::	TLSv1.2	157	Application Data
2	0.002506405	2409:4073:4dc5:e06c::	2409:4073:4dc5:e06c::	TLSv1.2	157	Application Data
3	0.305527939	2409:4073:4dc5:e06c::	2409:4073:4dc5:e06c::	TCP	86	443 → 46012 [ACK] Seq=68 Ack=72 Win=17 Len=0 TSval=2096470833 TSecr=1371043287
4	2.972958257	2409:4073:4dc5:e06c::	2409:4073:4dc5:e06c::	TLSv1.2	111	Application Data
5	2.974737617	2409:4073:4dc5:e06c::	2409:4073:4dc5:e06c::	TLSv1.2	115	Application Data
6	3.255495143	2409:4073:4dc5:e06c::	2409:4073:4dc5:e06c::	TCP	86	443 → 54942 [ACK] Seq=26 Ack=30 Win=16 Len=0 TSval=220739731 TSecr=2465324260
7	6.145077923	2409:4073:4dc5:e06c::	2409:4073:4dc5:e06c::	TLSv1.2	153	Application Data
8	6.146337453	2409:4073:4dc5:e06c::	2409:4073:4dc5:e06c::	TLSv1.2	157	Application Data
9	6.550063411	2409:4073:4dc5:e06c::	2409:4073:4dc5:e06c::	TCP	86	443 → 46012 [ACK] Seq=135 Ack=143 Win=17 Len=0 TSval=2096476993 TSecr=1371049431
10	7.671807758	192.168.143.221	34.237.73.95	TLSv1.2	308	Application Data
11	8.198403599	34.237.73.95	192.168.143.221	TLSv1.2	331	Application Data
12	8.198490321	192.168.143.221	34.237.73.95	TCP	66	47782 → 443 [ACK] Seq=243 Ack=266 Win=501 Len=0 TSval=984169509 TSecr=2642752719
13	10.345140824	fe80::a04e:f2ff:fef...::	ff02::1:ffa3:60ad	ICMPv6	86	Neighbor Solicitation for 2409:4073:4dc5:e06c:442d:c55b:86a3:60ad from a2:4e:f2:f6:45:4d

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

```
(kali) [~] 192.168.143.221 192.168.143.157 DNS 192 Star
$ ping google.com 90253 192.168.143.157 192.168.143.221 DNS 172 Star
PING google.com(pnmaa-az-in-x0e.1e100.net (2404:6800:4007:832::200e)) 56 data bytes v6 86 Neit
64 bytes from pnmaa-az-in-x0e.1e100.net (2404:6800:4007:832::200e): icmp_seq=1 ttl=115 time=203 ms
64 bytes from pnmaa-az-in-x0e.1e100.net (2404:6800:4007:832::200e): icmp_seq=2 ttl=115 time=328 ms
64 bytes from pnmaa-az-in-x0e.1e100.net (2404:6800:4007:832::200e): icmp_seq=3 ttl=115 time=354 ms
64 bytes from pnmaa-az-in-x0e.1e100.net (2404:6800:4007:832::200e): icmp_seq=4 ttl=115 time=270 ms
64 bytes from pnmaa-az-in-x0e.1e100.net (2404:6800:4007:832::200e): icmp_seq=5 ttl=115 time=294 ms
64 bytes from pnmaa-az-in-x0e.1e100.net (2404:6800:4007:832::200e): icmp_seq=6 ttl=115 time=118 ms
64 bytes from pnmaa-az-in-x0e.1e100.net (2404:6800:4007:832::200e): icmp_seq=7 ttl=115 time=81.0 ms
64 bytes from pnmaa-az-in-x0e.1e100.net (2404:6800:4007:832::200e): icmp_seq=8 ttl=115 time=268 ms
64 bytes from pnmaa-az-in-x0e.1e100.net (2404:6800:4007:832::200e): icmp_seq=9 ttl=115 time=64.5 ms
64 bytes from pnmaa-az-in-x0e.1e100.net (2404:6800:4007:832::200e): icmp_seq=10 ttl=115 time=200 ms
64 bytes from pnmaa-az-in-x0e.1e100.net (2404:6800:4007:832::200e): icmp_seq=11 ttl=115 time=223 ms
64 bytes from pnmaa-az-in-x0e.1e100.net (2404:6800:4007:832::200e): icmp_seq=12 ttl=115 time=143 ms
64 bytes from pnmaa-az-in-x0e.1e100.net (2404:6800:4007:832::200e): icmp_seq=13 ttl=115 time=165 ms
64 bytes from pnmaa-az-in-x0e.1e100.net (2404:6800:4007:832::200e): icmp_seq=14 ttl=115 time=84.8 ms
64 bytes from pnmaa-az-in-x0e.1e100.net (2404:6800:4007:832::200e): icmp_seq=15 ttl=115 time=89.3 ms
```

501	104.128043106	2404:6800:4007:832::	2409:4073:4dc5:e06c::	ICMPv6	118 Echo (ping) reply id=0x0000, seq=51, hop limit=115 (request in 501)
562	164.169841196	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	164.133418664	192.168.143.157	192.168.143.221	DNS	172 Standard query response 0x250f PTR e.0.0.2.0.0.0.0.0.0.0.0.0.0.0.0.2.3.8.0
564	164.268227646	192.168.143.46	224.0.0.251	MDNS	87 Standard query 0x0000 PTR _spotify-connect._tcp.local, "QM" request
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:fe::f002:1:1: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=0x0000, seq=52, hop limit=254 (reply in 568)
569	164.945695814	2404:6800:4007:832::	2409:4073:4dc5:e06c::	ICMPv6	118 Echo (ping) reply id=0x0000, seq=52, hop limit=115 (request in 569)
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.0.0.2.0.0.0.0.0.0.0.0.0.0.0.0.2.3.8.0
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=0x0000, seq=53, hop limit=254 (reply in 575)
576	165.970936642	2404:6800:4007:832::	2409:4073:4dc5:e06c::	ICMPv6	118 Echo (ping) reply id=0x0000, seq=53, hop limit=115 (request in 576)
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.0.0.2.0.0.0.0.0.0.0.0.0.0.0.0.2.3.8.0
579	166.687486877	a2:4e:f2:f6:45:4d	Broadcast	ARP	60 Who has 192.168.143.47? Tell 192.168.143.157
580	166.856280918	2409:4073:4dc5:e06c::	2404:6800:4007:832::	ICMPv6	118 Echo (ping) request id=0x0000, seq=54, hop limit=254 (reply in 580)
581	166.994698872	2404:6800:4007:832::	2409:4073:4dc5:e06c::	ICMPv6	118 Echo (ping) reply id=0x0000, seq=54, hop limit=115 (request in 581)
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.0.0.2.0.0.0.0.0.0.0.0.0.0.0.0.2.3.8.0
584	167.927294037	fe80::a04e:f2ff:fe::f002:1:1: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

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

No.	Time	Source	Destination	Protocol	Length	Info
430	149.170844214	2409:4073:4dc5:e06c...	2404:6800:4009:830:...	OCSP	499	Request
432	149.373798654	2404:6800:4009:830:...	2409:4073:4dc5:e06c...	OCSP	997	Response
1374	252.850859185	192.168.143.221	23.37.240.161	OCSP	482	Request
1387	252.951651430	23.37.240.161	192.168.143.221	OCSP	941	Response

DNS

No.	Time	Source	Destination	Protocol	Length	Info
3119	499.718300994	192.168.143.157	192.168.143.221	DNS	172	Standard query response 0xb260 PTR e.0.0.2.0.0.0.0.0.0.0.0.0.0.2
3123	500.703862476	192.168.143.221	192.168.143.157	DNS	132	Standard query 0x7fb7 PTR e.0.0.2.0.0.0.0.0.0.0.0.0.0.2,3.8.0.7.(
3124	500.708602129	192.168.143.157	192.168.143.221	DNS	172	Standard query response 0x7fb7 PTR e.0.0.2.0.0.0.0.0.0.0.0.0.0.2
3128	501.760314241	192.168.143.221	192.168.143.157	DNS	132	Standard query 0x023e PTR e.0.0.2.0.0.0.0.0.0.0.0.0.0.2,3.8.0.7.(
3129	501.767224129	192.168.143.157	192.168.143.221	DNS	172	Standard query response 0x023e PTR e.0.0.2.0.0.0.0.0.0.0.0.0.0.2
3133	502.886672936	192.168.143.221	192.168.143.157	DNS	132	Standard query 0xf32b PTR e.0.0.2.0.0.0.0.0.0.0.0.0.0.2,3.8.0.7.(
3134	502.891903218	192.168.143.157	192.168.143.221	DNS	172	Standard query response 0xf32b PTR e.0.0.2.0.0.0.0.0.0.0.0.0.0.2
3138	503.829621674	192.168.143.221	192.168.143.157	DNS	132	Standard query 0x1fa5 PTR e.0.0.2.0.0.0.0.0.0.0.0.0.0.2,3.8.0.7.(
3139	503.833486123	192.168.143.157	192.168.143.221	DNS	172	Standard query response 0x1fa5 PTR e.0.0.2.0.0.0.0.0.0.0.0.0.0.2
3145	504.731632301	192.168.143.221	192.168.143.157	DNS	132	Standard query 0xcc37 PTR e.0.0.2.0.0.0.0.0.0.0.0.0.0.2,3.8.0.7.(
3146	504.736173380	192.168.143.157	192.168.143.221	DNS	172	Standard query response 0xcc37 PTR e.0.0.2.0.0.0.0.0.0.0.0.0.0.2
3158	505.757794428	192.168.143.221	192.168.143.157	DNS	132	Standard query 0x5e8f PTR e.0.0.2.0.0.0.0.0.0.0.0.0.0.2,3.8.0.7.(
3159	505.761846905	192.168.143.157	192.168.143.221	DNS	172	Standard query response 0x5e8f PTR e.0.0.2.0.0.0.0.0.0.0.0.0.0.2
3162	506.780585029	192.168.143.221	192.168.143.157	DNS	132	Standard query 0x7c67 PTR e.0.0.2.0.0.0.0.0.0.0.0.0.0.2,3.8.0.7.(
3163	506.788751961	192.168.143.157	192.168.143.221	DNS	172	Standard query response 0x7c67 PTR e.0.0.2.0.0.0.0.0.0.0.0.0.0.2
3168	507.708584673	192.168.143.221	192.168.143.157	DNS	132	Standard query 0xfa50 PTR e.0.0.2.0.0.0.0.0.0.0.0.0.0.2,3.8.0.7.(
3169	507.713676036	192.168.143.157	192.168.143.221	DNS	172	Standard query response 0xfa50 PTR e.0.0.2.0.0.0.0.0.0.0.0.0.0.2
3173	508.708631817	192.168.143.221	192.168.143.157	DNS	132	Standard query 0x5a12 PTR e.0.0.2.0.0.0.0.0.0.0.0.0.0.2,3.8.0.7.(
3174	508.727339518	192.168.143.157	192.168.143.221	DNS	172	Standard query response 0x5a12 PTR e.0.0.2.0.0.0.0.0.0.0.0.0.0.2
3178	509.750568411	192.168.143.221	192.168.143.157	DNS	132	Standard query 0x83ca PTR e.0.0.2.0.0.0.0.0.0.0.0.0.0.2,3.8.0.7.(

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