

Task 5th: Capture and Analyze Network Traffic Using Wireshark

5th Task SUBMISSION REPORT OF ELEVATE LABS CYBERSECURITY INTERNSHIP

NAME	ADARSH SHARMA
Submitted to:	Elevate Labs
Name of the Academic Institute	Ganpat University

REPORT SUBMITTED TO

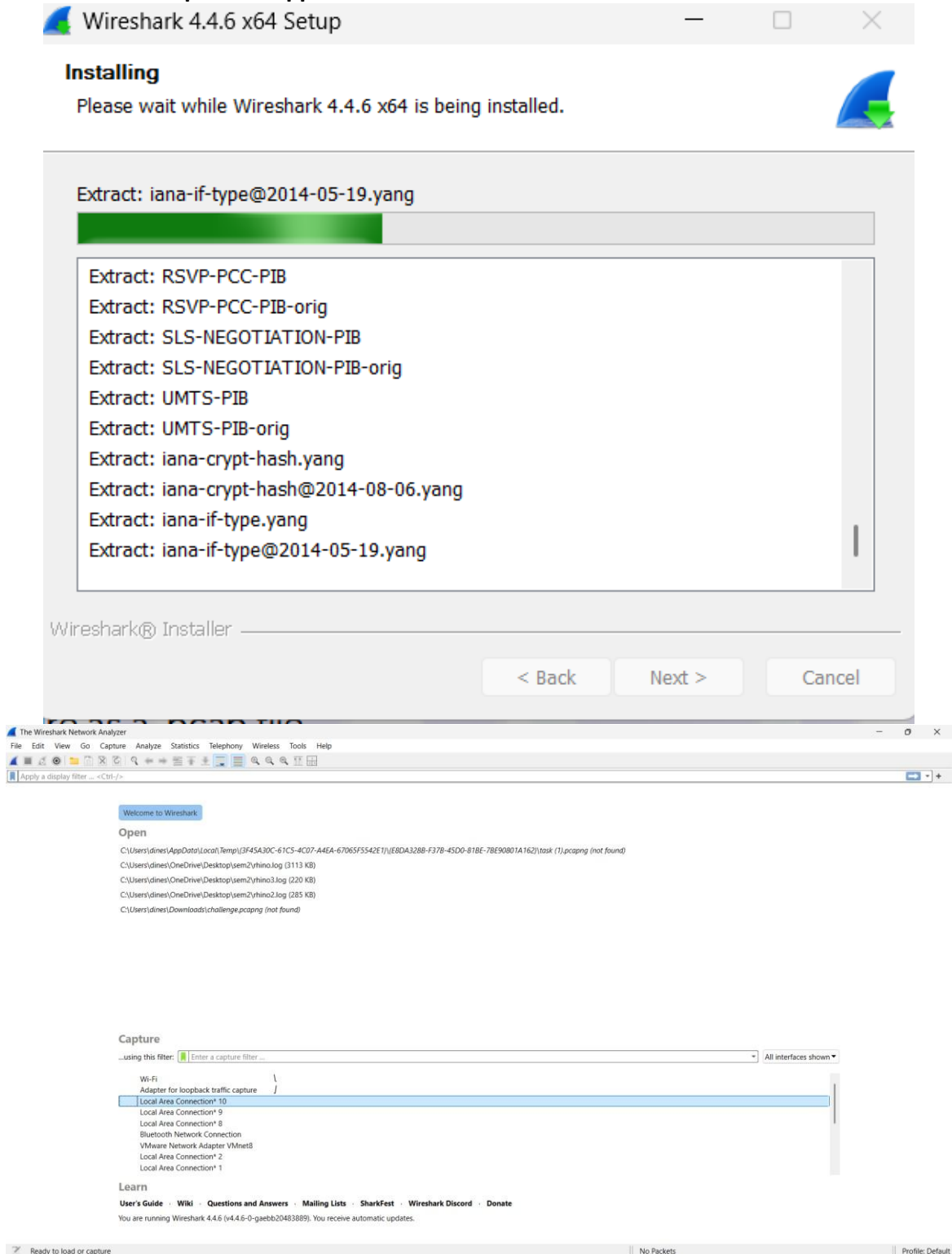


As part of the Cyber Security Internship, I have completed "Task 5th: Capture and Analyze Network Traffic Using Wireshark." by following all steps as instructed. Below is a detailed summary of each step followed during the task:

Task 5th: Capture and Analyze Network Traffic Using Wireshark

1. Install Wireshark.

- Download from: <https://www.wireshark.org/download.html>
- Install and open the application.



Task 5th: Capture and Analyze Network Traffic Using Wireshark

2. Start capturing on your active network interface.

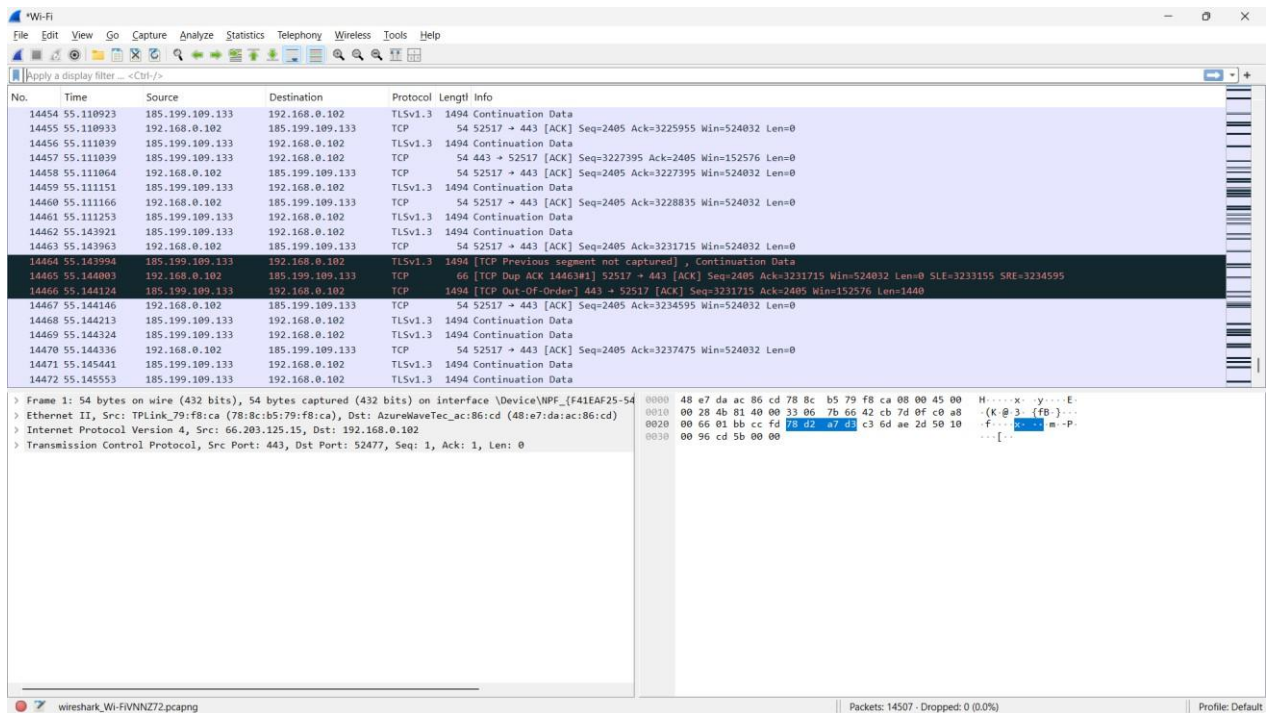
The image shows the Wireshark network traffic capture interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons for file operations, capture control, and analysis. The main window is divided into three panes:

- Packets List:** Displays a list of captured packets. The first packet (No. 35) is a TLSv1.2 Application Data packet from 192.168.0.102 to 192.168.0.102, with a length of 128 bytes.
- Packet Details:** Shows the structure of the selected packet (No. 35). It includes Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Transport Layer Security.
- Packet Bytes:** Displays the raw data of the selected packet in hexadecimal and ASCII format.

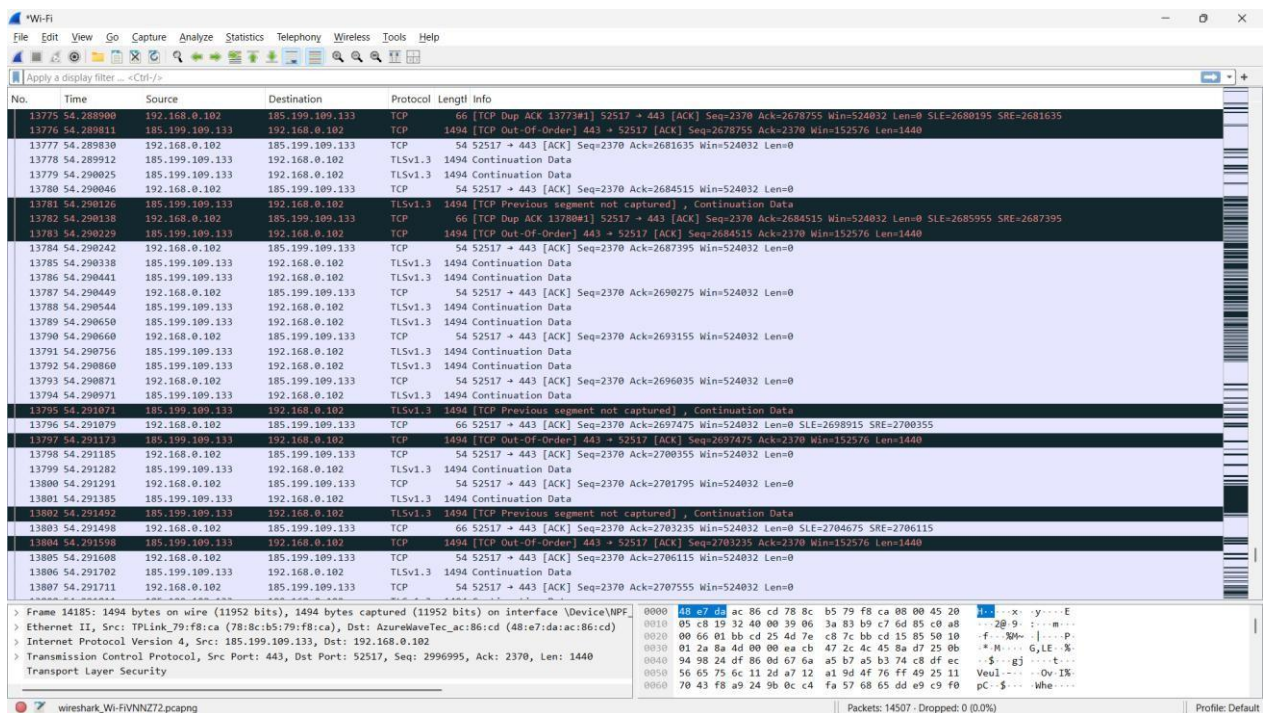
The status bar at the bottom indicates "Wi-Fi: <live capture in progress>" and "Packets: 53".

The image shows the Simplilearn website homepage. The header includes the Simplilearn logo, navigation links for All Courses, What do you want to learn?, For Business, Resources, and More, and a Login button. The main content area features a large image of a man working on a laptop, with the text "Get Certified. Get Ahead." and statistics: 8,000,000 Careers advanced, 1,500 Live classes every month, and 85% Report career success. Below this are buttons for "Explore Programs" and "Try Simplilearn for Business". The footer mentions "Partnering with the world's leading universities and companies" and lists logos for AWS, Project Management Institute, Microsoft, Purdue University, and others. A large blue button at the bottom says "Explore Our Top Programs".

Task 5th: Capture and Analyze Network Traffic Using Wireshark



4. Stop capture after a minute.



Task 5th: Capture and Analyze Network Traffic Using Wireshark

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

The image displays two screenshots of the Wireshark network protocol analyzer. The top screenshot shows a list of captured packets filtered by the HTTP protocol. The bottom screenshot shows a list of captured packets filtered by the DNS protocol.

Top Screenshot: HTTP Filter

No.	Time	Source	Destination	Protocol	Length	Info
3115	49.095887	192.168.0.102	216.58.203.35	HTTP	256	GET /r/gsr1.cr1 HTTP/1.1
3117	49.112751	216.58.203.35	192.168.0.102	HTTP	277	HTTP/1.1 304 Not Modified
3118	49.118449	192.168.0.102	216.58.203.35	HTTP	254	GET /r/r4.cr1 HTTP/1.1
3119	49.134550	216.58.203.35	192.168.0.102	HTTP	277	HTTP/1.1 304 Not Modified

Bottom Screenshot: DNS Filter

No.	Time	Source	Destination	Protocol	Length	Info
2638	19.975856	192.168.0.1	192.168.0.102	DNS	176	Standard query response 0x3bac A survey.webengage.com CNAME survey-alb-new-1082488714.us-east-1.elb.amazonaws.com A 34.198.198...
2936	33.382261	192.168.0.102	192.168.0.1	DNS	87	Standard query 0xae87 A merino.services.mozilla.com
2937	33.399776	192.168.0.1	192.168.0.102	DNS	103	Standard query response 0xae87 A merino.services.mozilla.com A 34.110.138.217
2938	33.400621	192.168.0.102	192.168.0.1	DNS	87	Standard query 0xb997 A merino.services.mozilla.com
2942	33.416825	192.168.0.1	192.168.0.102	DNS	103	Standard query response 0xb997 A merino.services.mozilla.com A 34.110.138.217
2943	33.417061	192.168.0.102	192.168.0.1	DNS	70	Standard query 0xb8d1 AAAA merino.services.mozilla.com
2948	33.433386	192.168.0.1	192.168.0.102	DNS	168	Standard query response 0xb8d1 AAAA merino.services.mozilla.com SOA ns-679.audnsd-20.net
3110	49.051147	192.168.0.102	192.168.0.1	DNS	70	Standard query 0xb18d A c.pki.goog CNAME pki-goog-1.google.com A 216.58.203.35
3111	49.074637	192.168.0.1	192.168.0.102	DNS	121	Standard query response 0xb18d A c.pki.goog CNAME pki-goog-1.google.com A 216.58.203.35
3208	56.392219	192.168.0.102	192.168.0.1	DNS	75	Standard query 0xbd33 A ssl.gstatic.com
3209	56.426300	192.168.0.102	192.168.0.1	DNS	75	Standard query 0xbd33 A ssl.gstatic.com
3210	56.468321	192.168.0.1	192.168.0.102	DNS	91	Standard query response 0xbd33 A ssl.gstatic.com A 142.251.220.3
3211	56.468321	192.168.0.1	192.168.0.102	DNS	91	Standard query response 0xbd33 A ssl.gstatic.com A 142.251.220.3
3257	57.427161	192.168.0.102	192.168.0.1	DNS	87	Standard query 0x54a7 A w3-reporting-nel.reddit.com
3258	57.449560	192.168.0.1	192.168.0.102	DNS	186	Standard query response 0x54a7 A w3-reporting-nel.reddit.com CNAME reddit.map.fastly.net A 151.101.193.140 A 151.101.1.140 A 15...

Task 5th: Capture and Analyze Network Traffic Using Wireshark

The image displays two screenshots of the Wireshark network traffic analysis tool. The top screenshot shows a capture of TCP traffic on the 'tcp' filter. The bottom screenshot shows a capture of ARP traffic on the 'arp' filter.

Top Screenshot: TCP Traffic

No.	Time	Source	Destination	Protocol	Length	Info
3100	46.956168	192.168.0.102	66.203.125.13	TCP	54	52641 → 443 [ACK] Seq=14269 Ack=11461 Win=255 Len=0
3101	47.006207	51.8.71.184	192.168.0.102	TCP	54	443 → 52679 [ACK] Seq=5868 Ack=5369 Win=64128 Len=0
3102	47.006207	51.8.71.184	192.168.0.102	TLSv1.2	366	Application Data
3103	47.048001	192.168.0.102	51.8.71.184	TCP	54	52679 → 443 [ACK] Seq=5369 Ack=6180 Win=65024 Len=0
3104	47.488195	192.168.0.102	23.193.114.57	TLSv1.2	1162	Application Data
3105	47.503676	23.193.114.57	192.168.0.102	TCP	54	443 → 52633 [ACK] Seq=4179 Ack=21139 Win=604 Len=0
3106	47.704517	23.193.114.57	192.168.0.102	TLSv1.2	225	Application Data
3107	47.704517	23.193.114.57	192.168.0.102	TLSv1.2	128	Application Data
3108	47.704566	192.168.0.102	23.193.114.57	TCP	54	52633 → 443 [ACK] Seq=21139 Ack=4424 Win=254 Len=0
3112	49.077698	192.168.0.102	216.58.203.35	TCP	66	52680 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
3113	49.095699	216.58.203.35	192.168.0.102	TCP	66	80 → 52680 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PERM WS=256
3114	49.095767	192.168.0.102	216.58.203.35	TCP	54	52680 → 80 [ACK] Seq=1 Ack=1 Win=65280 Len=0
3115	49.095887	192.168.0.102	216.58.203.35	HTTP	256	GET /r/sgsr1.cr1 HTTP/1.1
3116	49.112344	216.58.203.35	192.168.0.102	TCP	54	80 → 52680 [ACK] Seq=1 Ack=203 Win=269568 Len=0
3117	49.112751	216.58.203.35	192.168.0.102	HTTP	277	HTTP/1.1 304 Not Modified
3118	49.118449	192.168.0.102	216.58.203.35	HTTP	254	GET /r/r4.cr1 HTTP/1.1

Bottom Screenshot: ARP Traffic

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	TPLink_79:f8:ca	AzureWaveTec_ac:86:cd	ARP	42	Who has 192.168.0.102? Tell 192.168.0.1
2	0.000032	AzureWaveTec_ac:86:cd	TPLink_79:f8:ca	ARP	42	192.168.0.102 is at 48:e7:da:ac:86:cd
2858	25.834397	TPLink_79:f8:ca	AzureWaveTec_ac:86:cd	ARP	42	Who has 192.168.0.102? Tell 192.168.0.1
2859	25.834414	AzureWaveTec_ac:86:cd	TPLink_79:f8:ca	ARP	42	192.168.0.102 is at 48:e7:da:ac:86:cd
3109	48.678625	d2:89:80:0e:92:c6	Broadcast	ARP	42	Who has 192.168.0.1? Tell 192.168.0.103
3137	51.852957	TPLink_79:f8:ca	AzureWaveTec_ac:86:cd	ARP	42	Who has 192.168.0.102? Tell 192.168.0.1
3138	51.852974	AzureWaveTec_ac:86:cd	TPLink_79:f8:ca	ARP	42	192.168.0.102 is at 48:e7:da:ac:86:cd

Task 5th: Capture and Analyze Network Traffic Using Wireshark

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

The top screenshot shows a Wireshark capture of network traffic. The packet list includes:

- 1 0.000000 TPLink_79:f8:ca AzureWaveTec_ac:86: ARP 42 Who has 192.168.0.102? Tell 192.168.0.1
- 2 0.000032 AzureWaveTec_ac:86: TPLink_79:f8:ca ARP 42 192.168.0.102 is at 48:e7:da:ac:86:cd
- 2858 25.834397 TPLink_79:f8:ca AzureWaveTec_ac:86: ARP 42 Who has 192.168.0.102? Tell 192.168.0.1
- 2859 25.834414 AzureWaveTec_ac:86: TPLink_79:f8:ca ARP 42 192.168.0.102 is at 48:e7:da:ac:86:cd
- 3109 48.678625 d2:89:80:0e:92:c6 Broadcast ARP 42 Who has 192.168.0.17 Tell 192.168.0.103
- 3137 51.852957 TPLink_79:f8:ca AzureWaveTec_ac:86: ARP 42 Who has 192.168.0.102? Tell 192.168.0.1
- 3138 51.852974 AzureWaveTec_ac:86: TPLink_79:f8:ca ARP 42 192.168.0.102 is at 48:e7:da:ac:86:cd
- 15 2.410539 192.168.0.102 192.168.0.1 DNS 74 Standard query 0x82e1 A assets.msn.com
- 16 2.442801 192.168.0.102 192.168.0.1 DNS 74 Standard query 0x82e1 A assets.msn.com
- 17 2.501515 192.168.0.1 192.168.0.102 DNS 241 Standard query response 0x82e1 A assets.msn.com CNAME assets.msn-com-world-atm-default.trafficmanager.net CNAME assets.msn.com...
- 18 2.501515 192.168.0.1 192.168.0.102 DNS 241 Standard query response 0x82e1 A assets.msn.com CNAME assets.msn-com-world-atm-default.trafficmanager.net CNAME assets.msn.com...
- 72 10.817687 192.168.0.102 192.168.0.1 DNS 72 Standard query 0xbcb8 A a.clarity.ms
- 75 10.845282 192.168.0.1 192.168.0.102 DNS 153 Standard query response 0xbcb8 A a.clarity.ms CNAME vmss-clarity-ingest-eus-d.eastus.cloudapp.azure.com A 51.8.71.184
- 122 12.647738 192.168.0.102 192.168.0.1 DNS 76 Standard query 0x800c A cdn.jsdelivr.net
- 123 12.647904 192.168.0.102 192.168.0.1 DNS 79 Standard query 0x53a9 A www.simplilearn.com
- 124 12.647905 192.168.0.102 192.168.0.1 DNS 80 Standard query 0x2b08 A cdnjs.cloudflare.com
- 125 12.647987 192.168.0.102 192.168.0.1 DNS 83 Standard query 0x4177 A safebrowsing.google.com
- 126 12.664937 192.168.0.1 192.168.0.102 DNS 174 Standard query response 0x800c A cdn.jsdelivr.net CNAME jsdelivr.map.fastly.net A 151.101.65.229 A 151.101.129.229 A 151.101.1...
- 127 12.664937 192.168.0.1 192.168.0.102 DNS 118 Standard query response 0x4177 A safebrowsing.google.com CNAME sb.l.google.com A 142.250.183.46
- 128 12.665469 192.168.0.1 192.168.0.102 DNS 112 Standard query response 0x2b08 A cdnjs.cloudflare.com A 104.17.24.14 A 104.17.25.14
- 132 12.684897 192.168.0.102 192.168.0.1 DNS 79 Standard query 0x53a9 A www.simplilearn.com
- 135 12.709713 192.168.0.1 192.168.0.102 DNS 185 Standard query response 0x53a9 A www.simplilearn.com CNAME datsi2f5x9zv.cloudfront.net A 13.227.249.112 A 13.227.249.107 A 13...
- 138 12.712199 192.168.0.1 192.168.0.102 DNS 185 Standard query response 0x53a9 A www.simplilearn.com CNAME datsi2f5x9zv.cloudfront.net A 13.227.249.112 A 13.227.249.107 A 13...
- 215 12.784118 192.168.0.102 192.168.0.1 DNS 80 Standard query 0x8470 A analytics.google.com
- 216 12.784350 192.168.0.102 192.168.0.1 DNS 76 Standard query 0x8c9c A www.google.co.in
- 234 12.786931 192.168.0.102 192.168.0.1 DNS 72 Standard query 0x015a A bat.bing.com
- 238 12.810032 192.168.0.102 192.168.0.1 DNS 74 Standard query 0xdd71 A cdn.gumlet.com
- 239 12.810485 192.168.0.102 192.168.0.1 DNS 83 Standard query 0x7aec A stats.g.doubleclick.net
- 240 12.824178 192.168.0.102 192.168.0.1 DNS 72 Standard query 0x015a A bat.bing.com
- 241 12.824178 192.168.0.102 192.168.0.1 DNS 80 Standard query 0x8470 A analytics.google.com
- 242 12.824178 192.168.0.102 192.168.0.1 DNS 76 Standard query 0x8c9c A www.google.co.in
- 243 12.855723 192.168.0.102 192.168.0.1 DNS 74 Standard query 0xdd71 A cdn.gumlet.com
- 244 12.855723 192.168.0.102 192.168.0.1 DNS 83 Standard query 0x7aec A stats.g.doubleclick.net
- 300 12.894620 192.168.0.1 192.168.0.102 DNS 92 Standard query response 0x8c9c A www.google.co.in A 142.251.42.3
- 301 12.894620 192.168.0.1 192.168.0.102 DNS 96 Standard query response 0x8470 A analytics.google.com A 142.250.71.110
- 302 12.894620 192.168.0.1 192.168.0.102 DNS 166 Standard query response 0x015a A bat.bing.com CNAME bat-bing-com-ax-0001-ax-msedge.net CNAME ax-0001-ax-msedge.net A 150.171.28...
- 306 12.894970 192.168.0.102 192.168.0.102 DNS 147 Standard query response 0x7aec A stats.g.doubleclick.net A 74.125.68.154 A 74.125.68.157 A 74.125.68.155

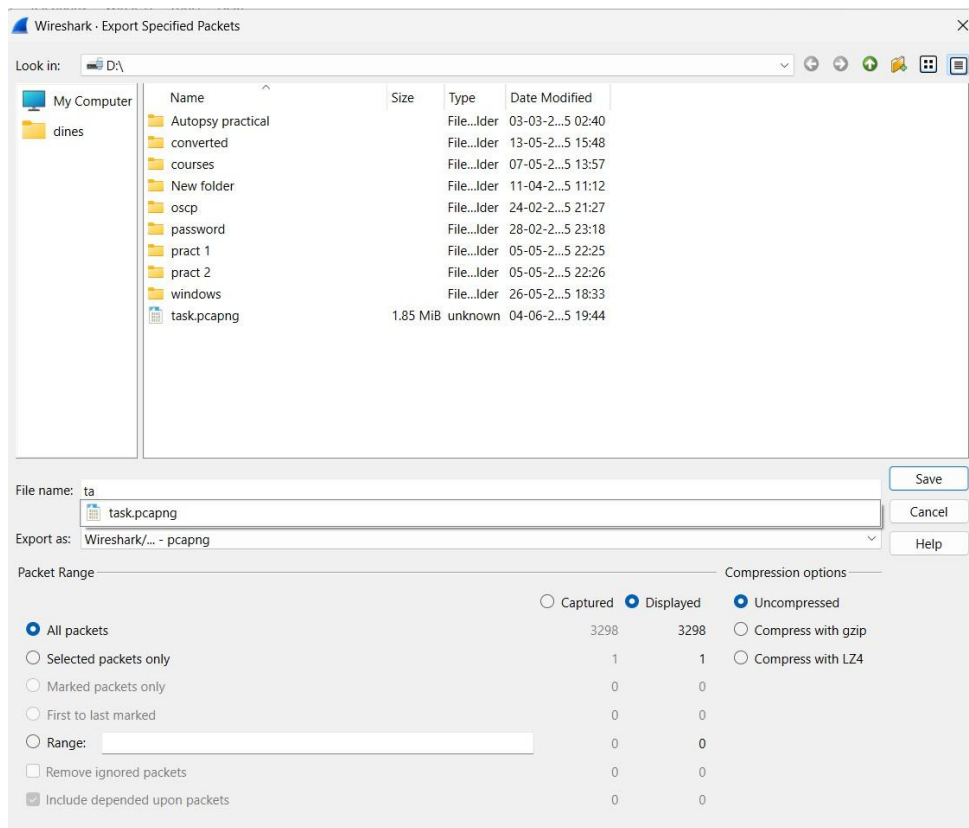
The bottom screenshot shows a Wireshark capture of network traffic. The packet list includes:

- 2942 33.416825 192.168.0.1 192.168.0.102 DNS 103 Standard query response 0xb997 A merino.services.mozilla.com A 34.110.138.217
- 2943 33.417061 192.168.0.102 192.168.0.1 DNS 87 Standard query response 0xbdb1 AAAA merino.services.mozilla.com
- 2948 33.433386 192.168.0.1 192.168.0.102 DNS 168 Standard query response 0xbdb1 AAAA merino.services.mozilla.com SOA ns-679.ausdns-20.net
- 3110 49.051147 192.168.0.102 192.168.0.1 DNS 70 Standard query 0x818d A c.pki.goog
- 3111 49.074637 192.168.0.1 192.168.0.102 DNS 121 Standard query response 0x818d A c.pki.goog CNAME pki-goog.l.google.com A 216.58.203.35
- 3208 56.392219 192.168.0.102 192.168.0.1 DNS 75 Standard query 0xbd33 A ssl.gstatic.com
- 3209 56.426300 192.168.0.102 192.168.0.1 DNS 75 Standard query 0xbd33 A ssl.gstatic.com
- 3210 56.468321 192.168.0.1 192.168.0.102 DNS 91 Standard query response 0xbd33 A ssl.gstatic.com A 142.251.220.3
- 3211 56.468321 192.168.0.1 192.168.0.102 DNS 91 Standard query response 0xbd33 A ssl.gstatic.com A 142.251.220.3
- 3257 57.427161 192.168.0.102 192.168.0.1 DNS 87 Standard query 0x54a7 A w3-reporting-nel.reddit.com
- 3258 57.449560 192.168.0.1 192.168.0.102 DNS 186 Standard query response 0x54a7 A w3-reporting-nel.reddit.com CNAME reddit.map.fastly.net A 151.101.193.140 A 151.101.1.140 A 15...
- 3115 49.095887 192.168.0.102 216.58.203.35 HTTP 256 GET /r/gsl1.cr1 HTTP/1.1
- 3117 49.112751 216.58.203.35 192.168.0.102 HTTP 277 HTTP/1.1 304 Not Modified
- 3118 49.118449 192.168.0.102 216.58.203.35 HTTP 254 GET /r/r4.cr1 HTTP/1.1
- 3119 49.134550 216.58.203.35 192.168.0.102 HTTP 277 HTTP/1.1 304 Not Modified
- 1786 18.470979 192.168.0.101 224.0.0.251 MDNS 100 Standard query 0x0000 PTR _companion-link._tcp.local, "QM" question PTR _rdlink._tcp.local, "QM" question
- 2910 31.672507 192.168.0.102 224.0.0.251 MDNS 207 Standard query response 0x0000 PTR Dinesh._dosvc._tcp.local SRV 0 0 7680 Dinesh.local TXT
- 2911 31.672977 fe80::c9ef:2651:c5d... ff02::fb MDNS 227 Standard query response 0x0000 PTR Dinesh._dosvc._tcp.local SRV 0 0 7680 Dinesh.local TXT
- 2912 31.673420 192.168.0.102 224.0.0.251 MDNS 84 Standard query 0x0000 ANY Dinesh._dosvc._tcp.local, "QM" question
- 2913 31.673718 fe80::c9ef:2651:c5d... ff02::fb MDNS 104 Standard query 0x0000 ANY Dinesh._dosvc._tcp.local, "QM" question
- 2914 31.936055 192.168.0.102 224.0.0.251 MDNS 84 Standard query 0x0000 ANY Dinesh._dosvc._tcp.local, "QM" question
- 2915 31.936454 fe80::c9ef:2651:c5d... ff02::fb MDNS 104 Standard query 0x0000 ANY Dinesh._dosvc._tcp.local, "QM" question
- 2916 32.201645 192.168.0.102 224.0.0.251 MDNS 84 Standard query 0x0000 ANY Dinesh._dosvc._tcp.local, "QM" question
- 2917 32.202150 fe80::c9ef:2651:c5d... ff02::fb MDNS 104 Standard query 0x0000 ANY Dinesh._dosvc._tcp.local, "QM" question
- 2919 32.453526 192.168.0.102 224.0.0.251 MDNS 263 Standard query response 0x0000 PTR, cache flush Dinesh._dosvc._tcp.local SRV, cache flush 0 0 7680 Dinesh.local TXT, cache flush...
- 2920 32.453953 fe80::c9ef:2651:c5d... ff02::fb MDNS 283 Standard query response 0x0000 PTR, cache flush Dinesh._dosvc._tcp.local SRV, cache flush 0 0 7680 Dinesh.local TXT, cache flush...
- 2921 32.454249 192.168.0.102 224.0.0.251 MDNS 208 Standard query response 0x0000 SRV, cache flush 0 0 7680 Dinesh.local TXT, cache flush A, cache flush 192.168.0.102 AAAA, cache...
- 2922 32.454551 fe80::c9ef:2651:c5d... ff02::fb MDNS 228 Standard query response 0x0000 SRV, cache flush 0 0 7680 Dinesh.local TXT, cache flush A, cache flush 192.168.0.102 AAAA, cache...
- 25 2.981064 192.168.0.102 162.159.200.123 NTP 90 NTP Version 4, client
- 26 3.002676 162.159.200.123 192.168.0.102 NTP 90 NTP Version 4, server
- 129 12.665772 192.168.0.102 142.250.183.46 QUIC 1292 Initial, DCID=5277bc55ec8cf8d9e, PKN: 1, CRYPTO, PING, CRYPTO, CRYPTO, PING, CRYPTO, CRYPTO, PING, CRYPTO, PING, CRYPTO
- 130 12.665805 192.168.0.102 142.250.183.46 QUIC 1292 Initial, DCID=5277bc55ec8cf8d9e, PKN: 2, CRYPTO, PING, PING, PING, CRYPTO, PING, PADDING, CRYPTO, PING, PING
- 131 12.666638 192.168.0.102 142.250.183.46 QUIC 121 0-RTT, DCID=5277bc55ec8cf8d9e
- 133 12.668764 142.250.183.46 192.168.0.102 QUIC 82 Initial, SCID=F277bc55ec8cf8d9e, PKN: 1, ACK
- 134 12.668997 142.250.183.46 192.168.0.102 QUIC 1292 Initial, SCID=F277bc55ec8cf8d9e, PKN: 2, ACK, PADDING
- 136 12.710161 192.168.0.102 142.250.183.46 QUIC 1292 Initial, DCID=F277bc55ec8cf8d9e, PKN: 5, PADDING, PING, PADDING
- 139 12.739888 142.250.183.46 192.168.0.102 QUIC 1292 Initial, SCID=F277bc55ec8cf8d9e, PKN: 3, ACK, PADDING

Task 5th: Capture and Analyze Network Traffic Using Wireshark

7. Export the capture as a .pcap file.

- Go to File > Export Specified Packets or File > Save As.
- Save the file as .pcap
(e.g.,internship_capture.pcap).



8. Summarize your findings and packet details.

Cyber Security Wireshark Capture Summary

Date/Time of Capture: June 4, 2025

Duration: 1 minute

Interface: Wi-Fi (wlan0)

Protocols Observed:

1. TCP – Core protocol used for reliable transport between devices.
 - Example: Connection established to 142.250.190.78 (Google IP).

Task 5th: Capture and Analyze Network Traffic Using Wireshark

2. DNS – Resolved domain names to IP addresses.

- **Example: `www.google.com` resolved to `142.250.190.78`.**

3. HTTP – Unencrypted web traffic.

- **Example: GET request to `http://example.com/index.html`.**

Interesting Observations:

- **Several TCP handshakes (SYN, SYN-ACK, ACK) visible.**
- **Multiple DNS queries and responses, showing hostname resolution.**
- **HTTP GET requests and responses with headers and HTML data.**
- **Minimal ICMP traffic from ping tests.**