

# ELEVATE LABS CYBERSECURITY

## INTERNSHIP

### Task-5:

2,3)

Capturing packets over my wifi

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	20.44.220.42	10.12.101.6	TCP	66	443 → 50001 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1440 SACK_PERM WS=128
2	0.000123	10.12.101.6	20.44.220.42	TCP	54	50001 → 443 [ACK] Seq=1 Ack=1 Win=255 Len=0
3	0.004137	10.12.101.6	20.44.220.42	TLSv1.3	535	Client Hello (SNI=displaycatalog.mp.microsoft.com)
4	0.024585	10.12.101.6	13.107.139.11	TCP	66	50002 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
5	0.061016	13.107.139.11	10.12.101.6	TCP	1514	443 → 49960 [ACK] Seq=1 Ack=1 Win=781 Len=1460 [TCP PDU reassembled in 6]
6	0.062162	13.107.139.11	10.12.101.6	TLSv1.2	871	Application Data
7	0.062326	10.12.101.6	13.107.139.11	TCP	54	49960 → 443 [ACK] Seq=1 Ack=2278 Win=255 Len=0
8	0.105310	4.213.25.242	10.12.101.6	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
9	0.109162	10.12.101.6	4.213.25.242	TLSv1.2	314	Application Data
10	0.116885	13.107.139.11	10.12.101.6	TCP	66	443 → 50002 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
11	0.117004	10.12.101.6	13.107.139.11	TCP	54	50002 → 443 [ACK] Seq=1 Ack=1 Win=65280 Len=0
12	0.119163	10.12.101.6	13.107.139.11	TLSv1.3	531	Client Hello (SNI=194357-ipv4mte.gr.global.aa-rt.sharepoint.com)
13	0.133013	20.44.220.42	10.12.101.6	TCP	60	443 → 50001 [ACK] Seq=1 Ack=482 Win=64128 Len=0
14	0.139467	20.44.220.42	10.12.101.6	TLSv1.3	1514	Server Hello, Change Cipher Spec, Application Data
15	0.143279	20.44.220.42	10.12.101.6	TCP	1514	443 → 50001 [PSH, ACK] Seq=1461 Ack=482 Win=64128 Len=1460 [TCP PDU reassembled in 18]
16	0.143331	10.12.101.6	20.44.220.42	TCP	54	50001 → 443 [ACK] Seq=482 Ack=2921 Win=255 Len=0
17	0.143425	20.44.220.42	10.12.101.6	TCP	1514	443 → 50001 [ACK] Seq=2921 Ack=482 Win=64128 Len=1460 [TCP PDU reassembled in 18]
18	0.143873	20.44.220.42	10.12.101.6	TLSv1.3	551	Application Data, Application Data, Application Data
19	0.143873	4.213.25.242	10.12.101.6	TLSv1.2	327	Application Data
20	0.143961	10.12.101.6	20.44.220.42	TCP	54	50001 → 443 [ACK] Seq=482 Ack=4878 Win=255 Len=0
21	0.144761	10.12.101.6	4.213.25.242	TLSv1.2	2530	Application Data
22	0.149296	10.12.101.6	20.44.220.42	TLSv1.3	134	Change Cipher Spec, Application Data
23	0.149517	10.12.101.6	20.44.220.42	TLSv1.3	134	Application Data
24	0.149595	10.12.101.6	20.44.220.42	TLSv1.3	1440	Application Data
25	0.163003	13.107.139.11	10.12.101.6	TCP	60	443 → 50002 [ACK] Seq=1 Ack=478 Win=199936 Len=0
26	0.167069	CloudNetwork_a7:e7::	Broadcast	ARP	56	Who has 10.12.117.108? (ARP Probe)
27	0.167069	13.107.139.11	10.12.101.6	TLSv1.3	1514	Server Hello, Change Cipher Spec
28	0.168398	13.107.139.11	10.12.101.6	TCP	1514	443 → 50002 [ACK] Seq=1461 Ack=478 Win=199936 Len=1460 [TCP PDU reassembled in 31]
29	0.168398	13.107.139.11	10.12.101.6	TCP	1514	443 → 50002 [ACK] Seq=2921 Ack=478 Win=199936 Len=1460 [TCP PDU reassembled in 31]
30	0.168398	13.107.139.11	10.12.101.6	TCP	1514	443 → 50002 [ACK] Seq=4381 Ack=478 Win=199936 Len=1460 [TCP PDU reassembled in 31]
31	0.168398	13.107.139.11	10.12.101.6	TLSv1.3	316	Application Data
32	0.168479	10.12.101.6	13.107.139.11	TCP	54	50002 → 443 [ACK] Seq=478 Ack=6103 Win=65280 Len=0
33	0.177287	4.213.25.242	10.12.101.6	TCP	60	443 → 50000 [ACK] Seq=325 Ack=2737 Win=8192 Len=0
34	0.178912	10.12.101.6	13.107.139.11	TLSv1.3	134	Change Cipher Spec, Application Data
35	0.179155	10.12.101.6	13.107.139.11	TLSv1.3	2754	Application Data
36	0.179302	10.12.101.6	13.107.139.11	TLSv1.3	3013	Application Data
37	0.179459	4.213.25.242	10.12.101.6	TLSv1.2	147	Application Data
38	0.180375	4.213.25.242	10.12.101.6	TLSv1.2	224	Application Data
39	0.180402	10.12.101.6	4.213.25.242	TCP	54	50000 → 443 [ACK] Seq=2737 Ack=588 Win=254 Len=0
40	0.180471	10.12.101.6	4.213.25.242	TLSv1.2	222	Application Data

Can be seen at bottom that over 1136 packets have been captured

4)

Display filter http:

No.	Time	Source	Destination	Protocol	Length	Info
714	0.921332	23.75.213.71	10.12.101.6	PKIX-C...	1077	Certificate Revocation List
1079	5.885478	43.152.143.98	10.12.101.6	HTTP	357	HTTP/1.1 304 Not Modified
1077	5.886867	10.12.101.6	43.152.143.98	HTTP	336	GET /msdownload/update/v3/static/trustedr/en/authrootstl.cab?79eb33203d5c6551 HTTP/1.1
1079	5.895020	43.152.143.98	10.12.101.6	HTTP	356	HTTP/1.1 304 Not Modified
1028	5.935638	10.12.101.6	43.152.143.98	HTTP	341	GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?77b2c53ad1d7034 HTTP/1.1
936	4.456389	43.152.143.98	10.12.101.6	HTTP	357	HTTP/1.1 304 Not Modified
929	4.355763	10.12.101.6	43.152.143.98	HTTP	336	GET /msdownload/update/v3/static/trustedr/en/pinrulesstl.cab?aaeee9e0332d660b HTTP/1.1
947	4.240860	43.152.143.98	10.12.101.6	HTTP	357	HTTP/1.1 304 Not Modified
894	4.171951	10.12.101.6	43.152.143.98	HTTP	341	GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?96621c03837f4194 HTTP/1.1
882	4.091600	18.161.246.3	10.12.101.6	HTTP	584	HTTP/1.1 304 Not Modified
879	4.050206	10.12.101.6	18.161.246.3	HTTP	422	GET /MFewTzBNMEswSTAjBgUrDgMCGuABBBQg3SSKKA74hABkhm1BtJ7z8w3h1AQUs2BWC7VOPVn49QaAJadZ20Zpq74CEEJlPa0x2YUHCpjsaUcQQQX3D HTTP/1.1
863	3.848515	23.15.147.118	10.12.101.6	HTTP	519	HTTP/1.1 304 Not Modified
846	3.739315	10.12.101.6	23.15.147.118	HTTP	309	GET /DigiCertTrustedRootG4.crl HTTP/1.1
845	3.731983	142.251.220.99	10.12.101.6	HTTP	277	HTTP/1.1 304 Not Modified
843	3.686423	10.12.101.6	142.251.220.99	HTTP	254	GET /r/r4.crl HTTP/1.1
842	3.679018	142.251.220.99	10.12.101.6	HTTP	277	HTTP/1.1 304 Not Modified
841	3.662169	10.12.101.6	142.251.220.99	HTTP	256	GET /r/gsr1.crl HTTP/1.1
840	3.654742	23.15.147.118	10.12.101.6	HTTP	519	HTTP/1.1 304 Not Modified
834	3.600662	10.12.101.6	23.15.147.118	HTTP	308	GET /DigiCertGlobalRootG2.crl HTTP/1.1
830	3.591696	43.152.143.98	10.12.101.6	HTTP	357	HTTP/1.1 304 Not Modified
826	3.542048	10.12.101.6	43.152.143.98	HTTP	336	GET /msdownload/update/v3/static/trustedr/en/authrootstl.cab?614cfd47002bbe1 HTTP/1.1
796	3.417123	23.15.147.118	10.12.101.6	HTTP	517	HTTP/1.1 304 Not Modified
775	3.274531	10.12.101.6	23.15.147.118	HTTP	308	GET /DigiCertGlobalRootCA.crl HTTP/1.1
742	3.139501	43.152.143.98	10.12.101.6	HTTP	357	HTTP/1.1 304 Not Modified
725	3.016315	10.12.101.6	43.152.143.98	HTTP	341	GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?c90438f8fc5c5fa4 HTTP/1.1
709	2.843743	10.12.101.6	23.75.213.71	HTTP	281	GET / HTTP/1.1
702	2.781780	142.251.220.99	10.12.101.6	HTTP	277	HTTP/1.1 304 Not Modified
699	2.753561	10.12.101.6	142.251.220.99	HTTP	254	GET /r/r1.crl HTTP/1.1
661	2.652960	23.75.214.126	10.12.101.6	HTTP	413	HTTP/1.1 304 Not Modified
597	2.433238	10.12.101.6	23.75.214.126	HTTP	454	GET /MFewTzBNMEswSTAjBgUrDgMCGuABBBRn2buARTxMtEy9asprAZg5QFhagQQUgrrwPZfOn89x6JI3x%2fztWk1V88CEDWvt3udNB9q%2f1X2BERqxsNsX3D HTTP/1.1

## Display filter DNS:

No.	Time	Source	Destination	Protocol	Length	Info
972	4.660821	172.17.18.2	10.12.101.6	DNS	174	Standard query response 0xfb8A slscr.update.microsoft.com CNAME sls.update.microsoft.com CNAME glb.sls.prod.dcat.dsp.trafficmanager.net
971	4.658346	10.12.101.6	172.17.18.2	DNS	86	Standard query 0xfb8A slscr.update.microsoft.com
939	4.456389	172.17.18.4	10.12.101.6	DNS	161	Standard query response 0xa343 A onedriveclucproddm20040.blob.core.windows.net CNAME blob.dsm40prdst01a.store.core.windows.net A 20.20.20.20
938	4.456389	172.17.18.2	10.12.101.6	DNS	161	Standard query response 0xa343 A onedriveclucproddm20040.blob.core.windows.net CNAME blob.dsm40prdst01a.store.core.windows.net A 20.20.20.20
930	4.357977	10.12.101.6	172.17.18.4	DNS	105	Standard query 0xa343 A onedriveclucproddm20040.blob.core.windows.net
923	4.318778	10.12.101.6	172.17.18.2	DNS	105	Standard query 0xa343 A onedriveclucproddm20040.blob.core.windows.net
874	4.006216	172.17.18.4	10.12.101.6	DNS	137	Standard query response 0x7611 A ocspssl.com A 13.226.120.76 A 13.226.120.99 A 13.226.120.91 A 13.226.120.26
872	3.997295	172.17.18.2	10.12.101.6	DNS	137	Standard query response 0x7611 A ocspssl.com A 18.161.246.3 A 18.161.246.34 A 18.161.246.112 A 18.161.246.70
868	3.898905	10.12.101.6	172.17.18.4	DNS	73	Standard query 0x7611 A ocspssl.com
866	3.857984	10.12.101.6	172.17.18.2	DNS	73	Standard query 0x7611 A ocspssl.com
784	3.306334	172.17.18.4	10.12.101.6	DNS	250	Standard query response 0x5ceb A storage.live.com CNAME common-geo.ha1drv.com CNAME common-geo.onedrive.trafficmanager.net CNAME blz04
783	3.306334	172.17.18.2	10.12.101.6	DNS	250	Standard query response 0x5ceb A storage.live.com CNAME common-geo.ha1drv.com CNAME common-geo.onedrive.trafficmanager.net CNAME blz04
765	3.249937	10.12.101.6	172.17.18.4	DNS	76	Standard query 0x5ceb A storage.live.com
758	3.219208	10.12.101.6	172.17.18.2	DNS	76	Standard query 0x5ceb A storage.live.com
747	3.151614	172.17.18.2	10.12.101.6	DNS	197	Standard query response 0x38a0 A crl3.digicert.com CNAME crl.edge.digicert.com CNAME cac-ocsp.digicert.com.edgekey.net CNAME e3913.cd.a
746	3.148310	10.12.101.6	172.17.18.2	DNS	77	Standard query 0x38a0 A crl3.digicert.com
704	2.792714	172.17.18.2	10.12.101.6	DNS	179	Standard query response 0xd4c6 A x1.c.lencr.org CNAME crl.root-x1.letsencrypt.org.edgekey.net CNAME e8652.dsccx.akamaiedge.net A 23.75.2
703	2.789714	10.12.101.6	172.17.18.2	DNS	74	Standard query 0xd4c6 A x1.c.lencr.org
663	2.664051	172.17.18.2	10.12.101.6	DNS	121	Standard query response 0x4e2c A c.pki.goog CNAME pki-goog.l.google.com A 142.251.220.99
662	2.660453	10.12.101.6	172.17.18.2	DNS	70	Standard query 0x4e2c A c.pki.goog
136	0.475927	172.17.18.2	10.12.101.6	DNS	146	Standard query response 0xa3ca No such name A wpad.amritanet.edu SOA prithvi.amritanet.edu
135	0.475927	172.17.18.2	10.12.101.6	DNS	193	Standard query response 0x0557 HTTPS microsoft.com CNAME edge-microsoft-com.ax-0002.ax-msedge.net CNAME ax-0002.ax-msedge.net SOA
134	0.474494	172.17.18.2	10.12.101.6	DNS	178	Standard query response 0x2622 A edge-microsoft.com CNAME edge-microsoft-com.ax-0002.ax-msedge.net CNAME ax-0002.ax-msedge.net A 150.17
132	0.471535	10.12.101.6	172.17.18.2	DNS	78	Standard query 0xa3ca A wpad.amritanet.edu
131	0.469765	10.12.101.6	172.17.18.2	DNS	78	Standard query 0x0557 HTTPS microsoft.com
130	0.469536	10.12.101.6	172.17.18.2	DNS	78	Standard query 0x2622 A edge-microsoft.com

## Display Filter TCP:

No.	Time	Source	Destination	Protocol	Length	Info
165	0.633120	150.171.27.11	10.12.101.6	TCP	1514	443 → 50003 [ACK] Seq=1461 Ack=1793 Win=199936 Len=1460 [TCP PDU reassembled in 169]
164	0.631681	150.171.27.11	10.12.101.6	TCP	1514	443 → 50003 [ACK] Seq=1 Ack=1793 Win=199936 Len=1460 [TCP PDU reassembled in 169]
163	0.618064	150.171.27.11	10.12.101.6	TCP	60	443 → 50003 [ACK] Seq=1 Ack=1793 Win=199936 Len=0
162	0.616502	150.171.27.11	10.12.101.6	TCP	60	443 → 50003 [ACK] Seq=1 Ack=1441 Win=199936 Len=0
161	0.588655	10.12.101.6	52.107.252.2	TCP	54	49979 → 443 [ACK] Seq=5332 Ack=6366 Win=255 Len=0
160	0.588616	10.12.101.6	20.44.220.42	TCP	54	50001 → 443 [ACK] Seq=2060 Ack=52943 Win=253 Len=0
159	0.588512	20.44.220.42	10.12.101.6	TCP	60	443 → 50001 [FIN, ACK] Seq=52942 Ack=2060 Win=64128 Len=0
156	0.588512	52.107.252.2	10.12.101.6	TCP	1514	443 → 49979 [ACK] Seq=4293 Ack=5332 Win=781 Len=1460 [TCP PDU reassembled in 157]
155	0.588512	52.107.252.2	10.12.101.6	TCP	1514	443 → 49979 [ACK] Seq=2833 Ack=5332 Win=781 Len=1460 [TCP PDU reassembled in 157]
154	0.576983	10.12.101.6	20.189.173.18	TCP	54	49998 → 443 [ACK] Seq=2278 Ack=7046 Win=1021 Len=0
150	0.574114	10.12.101.6	150.171.27.11	TCP	54	50003 → 443 [ACK] Seq=1 Ack=1 Win=65280 Len=0
149	0.574052	10.12.101.6	20.189.173.18	TCP	54	49998 → 443 [ACK] Seq=2278 Ack=6557 Win=1023 Len=0
148	0.573698	150.171.27.11	10.12.101.6	TCP	66	443 → 50003 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
146	0.573698	20.189.173.18	10.12.101.6	TCP	60	443 → 49998 [ACK] Seq=6510 Ack=2278 Win=781 Len=0
144	0.533307	10.12.101.6	20.44.220.42	TCP	66	50004 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
143	0.496576	52.107.252.2	10.12.101.6	TCP	60	443 → 49979 [ACK] Seq=2833 Ack=5332 Win=781 Len=0
142	0.487012	10.12.101.6	20.44.220.42	TCP	54	50001 → 443 [FIN, ACK] Seq=2059 Ack=52942 Win=253 Len=0
140	0.483666	10.12.101.6	20.44.220.42	TCP	54	50001 → 443 [ACK] Seq=2059 Ack=52293 Win=255 Len=0
138	0.483175	20.44.220.42	10.12.101.6	TCP	1514	443 → 50001 [ACK] Seq=49373 Ack=2059 Win=64128 Len=1460 [TCP PDU reassembled in 139]
137	0.476708	10.12.101.6	150.171.27.11	TCP	66	50003 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
129	0.441294	52.107.252.2	10.12.101.6	TCP	60	443 → 49979 [ACK] Seq=2833 Ack=4833 Win=781 Len=0
128	0.441213	10.12.101.6	20.44.220.42	TCP	54	50001 → 443 [ACK] Seq=2059 Ack=49373 Win=255 Len=0
127	0.441087	10.12.101.6	49.44.133.33	TCP	54	49995 → 443 [RST, ACK] Seq=2 Ack=25 Win=0 Len=0
126	0.440863	49.44.133.33	10.12.101.6	TCP	60	443 → 49995 [FIN, ACK] Seq=25 Ack=2 Win=80 Len=0
124	0.440863	20.44.220.42	10.12.101.6	TCP	1514	443 → 50001 [PSH, ACK] Seq=47913 Ack=2059 Win=64128 Len=1460 [TCP PDU reassembled in 139]
122	0.440863	20.44.220.42	10.12.101.6	TCP	1514	443 → 50001 [PSH, ACK] Seq=44993 Ack=2059 Win=64128 Len=1460 [TCP PDU reassembled in 123]
121	0.438564	20.44.220.42	10.12.101.6	TCP	1514	443 → 50001 [ACK] Seq=43533 Ack=2059 Win=64128 Len=1460 [TCP PDU reassembled in 123]
120	0.436237	10.12.101.6	20.44.220.42	TCP	54	50001 → 443 [ACK] Seq=2059 Ack=43533 Win=255 Len=0
118	0.436179	20.44.220.42	10.12.101.6	TCP	1514	443 → 50001 [ACK] Seq=40613 Ack=2059 Win=64128 Len=1460 [TCP PDU reassembled in 119]
117	0.436179	20.44.220.42	10.12.101.6	TCP	1514	443 → 50001 [PSH, ACK] Seq=39153 Ack=2059 Win=64128 Len=1460 [TCP PDU reassembled in 119]
115	0.432151	10.12.101.6	20.44.220.42	TCP	54	50001 → 443 [ACK] Seq=2059 Ack=37693 Win=255 Len=0
114	0.432088	20.44.220.42	10.12.101.6	TCP	1514	443 → 50001 [PSH, ACK] Seq=36233 Ack=2059 Win=64128 Len=1460 [TCP PDU reassembled in 116]
113	0.430781	20.44.220.42	10.12.101.6	TCP	1514	443 → 50001 [ACK] Seq=34773 Ack=2059 Win=64128 Len=1460 [TCP PDU reassembled in 116]
112	0.429039	10.12.101.6	20.44.220.42	TCP	54	50001 → 443 [ACK] Seq=2059 Ack=34773 Win=255 Len=0
110	0.424643	20.44.220.42	10.12.101.6	TCP	1514	443 → 50001 [ACK] Seq=31853 Ack=2059 Win=64128 Len=1460 [TCP PDU reassembled in 111]
109	0.423013	10.12.101.6	20.44.220.42	TCP	54	50001 → 443 [ACK] Seq=2059 Ack=31853 Win=255 Len=0
108	0.422972	20.44.220.42	10.12.101.6	TCP	1514	443 → 50001 [PSH, ACK] Seq=30393 Ack=2059 Win=64128 Len=1460 [TCP PDU reassembled in 111]
106	0.420888	10.12.101.6	20.44.220.42	TCP	54	50001 → 443 [ACK] Seq=2059 Ack=28933 Win=255 Len=0
105	0.420798	20.44.220.42	10.12.101.6	TCP	1514	443 → 50001 [PSH, ACK] Seq=27473 Ack=2059 Win=64128 Len=1460 [TCP PDU reassembled in 107]

Frame 164: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF\_{D054C65F-A2FD-4628-B252-71895C63F40F}, id 0  
Packets: 1136 · Displayed: 981 (86.4%) · Dropped: 0 (0.0%)  
Profile: Default

6)

There are various protocol based packets that have been captured as can be seen above such as DNS, TCP, HTTP and also packets of TLS and ARP are also observed in the log

8)

After capturing network traffic using Wireshark for one minute I identified multiple protocols including TCP, DNS, and HTTP DNS was used to resolve domain names when browsing websites TCP managed the reliable transmission of packets and HTTP handled the actual website data transfer The capture confirmed active communication between my system and web servers and I saved the data as a TASK-5.pcap file for further analysis.