Task 5 : Capture and Analyze Network Traffic Using Wireshark

1.Installation & Setup

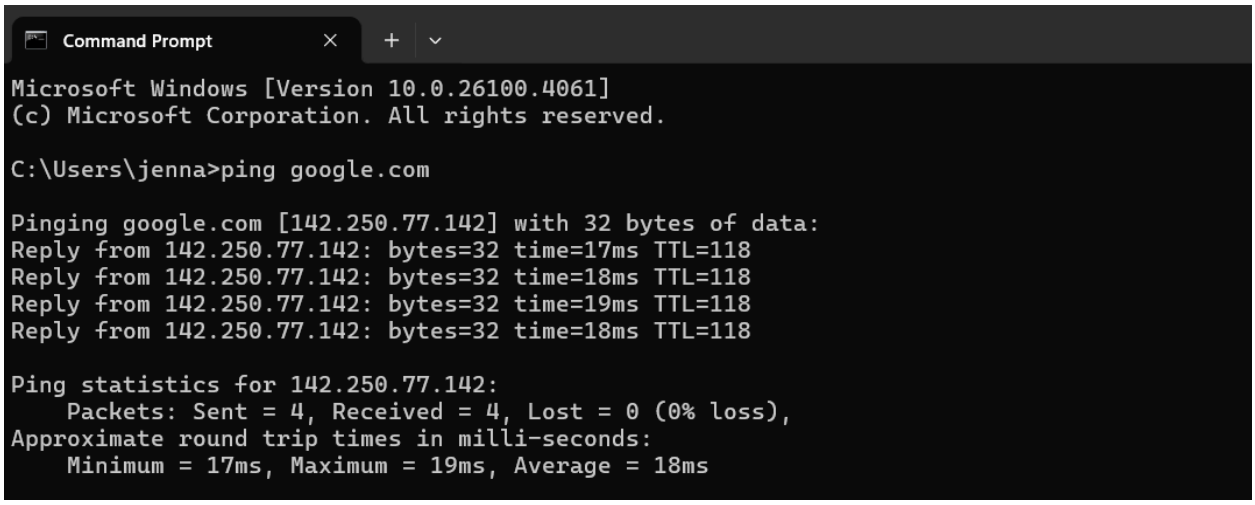
- Wireshark was downloaded and installed from the official website.

- The capture was started on the active Wi-Fi interface.

2.Traffic Generation

- A website was browsed to simulate typical user behavior.

- The `ping` command was used to generate ICMP traffic (`ping google.com`).



```
Command Prompt

Microsoft Windows [Version 10.0.26100.4061]
(c) Microsoft Corporation. All rights reserved.

C:\Users\jenna>ping google.com

Pinging google.com [142.250.77.142] with 32 bytes of data:
Reply from 142.250.77.142: bytes=32 time=17ms TTL=118
Reply from 142.250.77.142: bytes=32 time=18ms TTL=118
Reply from 142.250.77.142: bytes=32 time=19ms TTL=118
Reply from 142.250.77.142: bytes=32 time=18ms TTL=118

Ping statistics for 142.250.77.142:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 17ms, Maximum = 19ms, Average = 18ms
```

3.Capture Duration

- Network capture was allowed to run for approximately 60 seconds.
-

4.Protocol Findings Summary

During the packet capture and analysis, several key network protocols were identified using specific Wireshark filters.

1. HTTP (Unencrypted Web Traffic)

Using the `http` filter, unencrypted HTTP communications were observed. A sample GET request was sent to the server with IP address `132.196.154.22`, and the server responded with `HTTP/1.1 200 OK`. This traffic contained software telemetry and basic service requests. Since HTTP is plaintext, all transmitted data was visible and could be intercepted or read during transit.

2. TLS (Encrypted HTTPS Traffic)

Applying the `tls` filter revealed encrypted traffic between the system and Microsoft servers. A

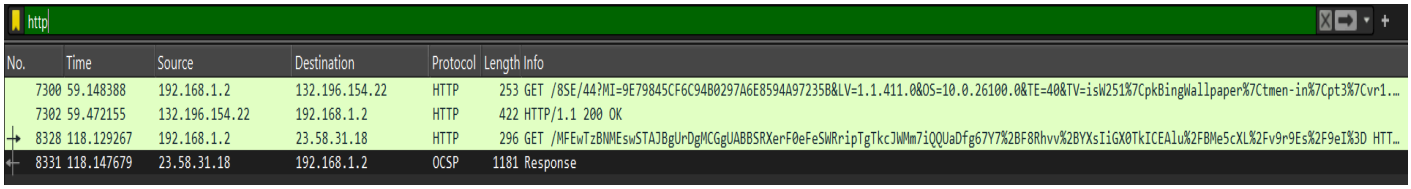
typical "Client Hello" message was sent to `static.edge.microsoftapp.net`, followed by encrypted application data exchanges with the IP address `13.107.246.58`. The TLS handshakes were conducted using TLSv1.2 and TLSv1.3 protocols, confirming that secure communication was established for browser or system services.

3. QUIC (Encrypted Traffic over HTTP/3)

Using the `quic` filter, initial QUIC packets were captured, including CRYPTO and PING frames sent to `142.251.221.197`, associated with Google services. Additional traffic was seen with the IP `103.165.166.40`, also using QUIC. These indicate the use of HTTP/3 for fast and encrypted web traffic, typically seen in services like Google Search or YouTube.

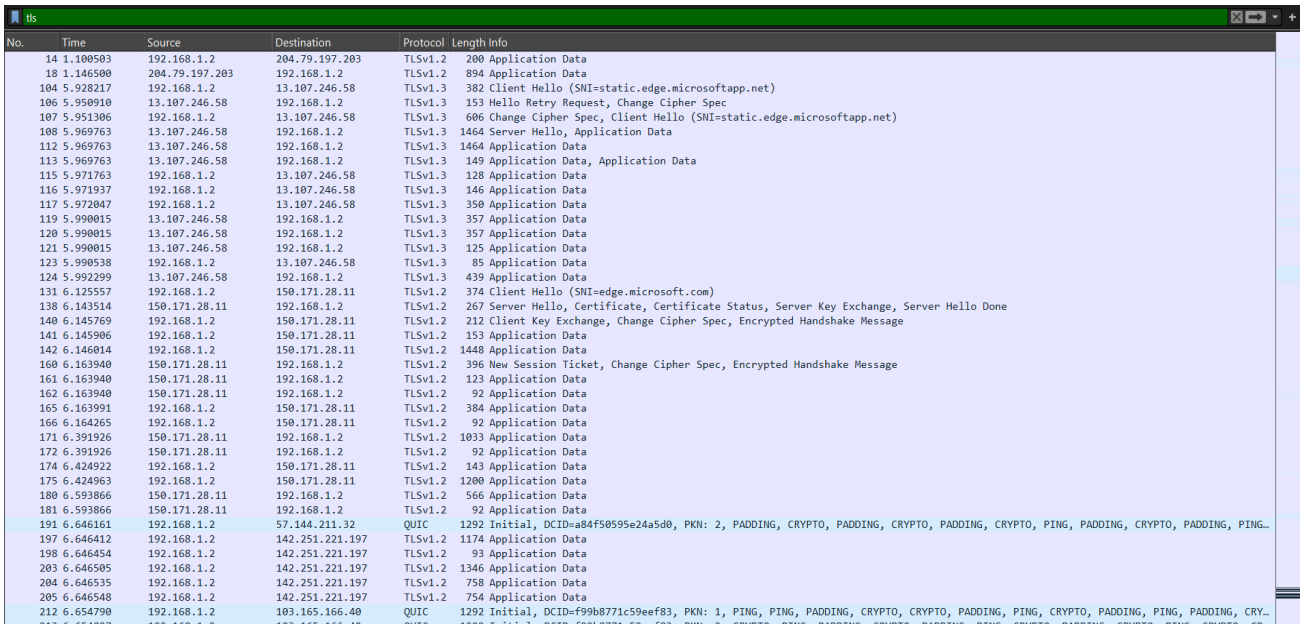
Other Observed Protocols:

- **DNS** was used to resolve domain names such as `edge.microsoft.com` to their respective IP addresses.
- **TCP** served as the underlying transport protocol for most HTTP and TLS communications.
- **ICMP** packets were observed when ping commands were executed to test basic network connectivity.



http

No.	Time	Source	Destination	Protocol	Length	Info
7300	59.148388	192.168.1.2	132.196.154.22	HTTP	253	GET /8SE/44?MI=9E79845CF6C94B0297A6E8594A97235B&LV=1.1.411.0&OS=10.0.26100.0&TE=40&TV=isW251%7CpkBingWallpaper%7Ctmen-in%7Cpt3%7Cvr1.…
7302	59.472155	132.196.154.22	192.168.1.2	HTTP	422	HTTP/1.1 200 OK
8328	118.129267	192.168.1.2	23.58.31.18	HTTP	296	GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBSRXerF0eFeSWRripTgTkcJWMm7iQQUaDfg67Y7%2BF8Rhvv%2BYXsIiGX0TkICEAlu%2FBMe5cXL%2Fv9r9Es%2F9eI%3D HTT…
8331	118.147679	23.58.31.18	192.168.1.2	OCSP	1181	Response



tls

No.	Time	Source	Destination	Protocol	Length	Info
14	1.100503	192.168.1.2	204.79.197.203	TLSv1.2	200	Application Data
18	1.146500	204.79.197.203	192.168.1.2	TLSv1.2	894	Application Data
104	5.928217	192.168.1.2	13.107.246.58	TLSv1.3	382	Client Hello (SNI=static.edge.microsoftapp.net)
106	5.950910	13.107.246.58	192.168.1.2	TLSv1.3	153	Hello Retry Request, Change Cipher Spec
107	5.951306	192.168.1.2	13.107.246.58	TLSv1.3	606	Change Cipher Spec, Client Hello (SNI=static.edge.microsoftapp.net)
108	5.969763	13.107.246.58	192.168.1.2	TLSv1.3	1464	Server Hello, Application Data
112	5.969763	13.107.246.58	192.168.1.2	TLSv1.3	1464	Application Data
113	5.969763	13.107.246.58	192.168.1.2	TLSv1.3	149	Application Data, Application Data
115	5.971763	192.168.1.2	13.107.246.58	TLSv1.3	128	Application Data
116	5.971937	192.168.1.2	13.107.246.58	TLSv1.3	146	Application Data
117	5.972047	192.168.1.2	13.107.246.58	TLSv1.3	350	Application Data
119	5.990015	13.107.246.58	192.168.1.2	TLSv1.3	357	Application Data
120	5.990015	13.107.246.58	192.168.1.2	TLSv1.3	357	Application Data
121	5.990015	13.107.246.58	192.168.1.2	TLSv1.3	125	Application Data
123	5.990538	192.168.1.2	13.107.246.58	TLSv1.3	85	Application Data
124	5.992299	13.107.246.58	192.168.1.2	TLSv1.3	439	Application Data
131	6.125557	192.168.1.2	150.171.28.11	TLSv1.2	374	Client Hello (SNI=edge.microsoft.com)
138	6.143514	150.171.28.11	192.168.1.2	TLSv1.2	267	Server Hello, Certificate, Certificate Status, Server Key Exchange, Server Hello Done
140	6.145769	192.168.1.2	150.171.28.11	TLSv1.2	212	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
141	6.145906	192.168.1.2	150.171.28.11	TLSv1.2	153	Application Data
142	6.146014	192.168.1.2	150.171.28.11	TLSv1.2	1448	Application Data
160	6.163940	150.171.28.11	192.168.1.2	TLSv1.2	396	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
161	6.163940	150.171.28.11	192.168.1.2	TLSv1.2	123	Application Data
162	6.163940	150.171.28.11	192.168.1.2	TLSv1.2	92	Application Data
165	6.163991	192.168.1.2	150.171.28.11	TLSv1.2	384	Application Data
166	6.164265	192.168.1.2	150.171.28.11	TLSv1.2	92	Application Data
171	6.391926	150.171.28.11	192.168.1.2	TLSv1.2	1033	Application Data
172	6.391926	150.171.28.11	192.168.1.2	TLSv1.2	92	Application Data
174	6.424922	192.168.1.2	150.171.28.11	TLSv1.2	143	Application Data
175	6.424963	192.168.1.2	150.171.28.11	TLSv1.2	1200	Application Data
180	6.593866	150.171.28.11	192.168.1.2	TLSv1.2	566	Application Data
181	6.593866	150.171.28.11	192.168.1.2	TLSv1.2	92	Application Data
191	6.646161	192.168.1.2	57.144.211.32	QUIC	1292	Initial, DCID=a84f50595e24a5d0, PKN: 2, PADDING, CRYPTO, PADDING, CRYPTO, PADDING, CRYPTO, PING, PADDING, CRYPTO, PADDING, PING…
197	6.646412	192.168.1.2	142.251.221.197	TLSv1.2	1174	Application Data
198	6.646454	192.168.1.2	142.251.221.197	TLSv1.2	93	Application Data
203	6.646505	192.168.1.2	142.251.221.197	TLSv1.2	1346	Application Data
204	6.646535	192.168.1.2	142.251.221.197	TLSv1.2	758	Application Data
205	6.646548	192.168.1.2	142.251.221.197	TLSv1.2	754	Application Data
212	6.654790	192.168.1.2	103.165.166.40	QUIC	1292	Initial, DCID=f99b8771c59eef83, PKN: 1, PING, PING, PADDING, CRYPTO, CRYPTO, PADDING, PING, CRYPTO, PADDING, PING, PADDING, CRY…

dns

No.	Time	Source	Destination	Protocol	Length	Info
95	5.899208	192.168.1.2	103.160.195.230	DNS	88	Standard query 0x9cc6 A static.edge.microsoftapp.net
96	5.899362	192.168.1.2	103.160.195.230	DNS	88	Standard query 0x8c59 HTTPS static.edge.microsoftapp.net
98	5.907718	103.160.195.230	192.168.1.2	DNS	425	Standard query response 0x8c59 HTTPS static.edge.microsoftapp.net CNAME edge-cloud-resource-static.azureedge.net CNAME edge-clo…
99	5.907718	103.160.195.230	192.168.1.2	DNS	369	Standard query response 0x9cc6 A static.edge.microsoftapp.net CNAME edge-cloud-resource-static.azureedge.net CNAME edge-cloud-r…
179	6.590593	192.168.1.2	103.160.195.230	DNS	74	Standard query 0x5137 A assets.msn.com
183	6.598455	103.160.195.230	192.168.1.2	DNS	247	Standard query response 0x5137 A assets.msn.com CNAME assets-msn-com-world-atm-default.trafficmanager.net CNAME assets.msn.com.…
184	6.644000	192.168.1.2	103.199.160.80	DNS	79	Standard query 0x21bc A aefd.nelreports.net
185	6.644125	192.168.1.2	103.199.160.80	DNS	79	Standard query 0x7863 HTTPS aefd.nelreports.net
186	6.644478	192.168.1.2	103.199.160.80	DNS	80	Standard query 0xba9f A a.nel.cloudflare.com
187	6.644576	192.168.1.2	103.199.160.80	DNS	80	Standard query 0x57b9 HTTPS a.nel.cloudflare.com
188	6.645300	192.168.1.2	103.199.160.80	DNS	79	Standard query 0x1d13 A deff.nelreports.net
189	6.645393	192.168.1.2	103.199.160.80	DNS	79	Standard query 0xcd1e HTTPS deff.nelreports.net
206	6.653872	103.199.160.80	192.168.1.2	DNS	237	Standard query response 0x7863 HTTPS aefd.nelreports.net CNAME aefd.nelreports.net.akamaized.net CNAME a1851.dscg2.akamai.net S…
207	6.653872	103.199.160.80	192.168.1.2	DNS	194	Standard query response 0x21bc A aefd.nelreports.net CNAME aefd.nelreports.net.akamaized.net CNAME a1851.dscg2.akamai.net A 103…
208	6.653872	103.199.160.80	192.168.1.2	DNS	96	Standard query response 0xba9f A a.nel.cloudflare.com A 35.190.80.1
209	6.653872	103.199.160.80	192.168.1.2	DNS	235	Standard query response 0xcd1e HTTPS deff.nelreports.net CNAME deff.nelreports.net.akamaized.net CNAME a1858.dscd.akamai.net SO…
210	6.653872	103.199.160.80	192.168.1.2	DNS	159	Standard query response 0x57b9 HTTPS a.nel.cloudflare.com SOA coleman.ns.cloudflare.com
211	6.653872	103.199.160.80	192.168.1.2	DNS	193	Standard query response 0x1d13 A deff.nelreports.net CNAME deff.nelreports.net.akamaized.net CNAME a1858.dscd.akamai.net A 103.…
463	11.036019	192.168.1.2	103.199.160.80	DNS	72	Standard query 0xbc4d A www.bing.com
464	11.036108	192.168.1.2	103.199.160.80	DNS	72	Standard query 0x2771 HTTPS www.bing.com
465	11.046580	103.199.160.80	192.168.1.2	DNS	343	Standard query response 0xbc4d A www.bing.com CNAME www-www.bing.com.trafficmanager.net CNAME www.bing.com.edgekey.net CNAME e8…
466	11.046580	103.199.160.80	192.168.1.2	DNS	277	Standard query response 0x2771 HTTPS www.bing.com CNAME www-www.bing.com.trafficmanager.net CNAME www.bing.com.edgekey.net CNAM…
496	13.100543	192.168.1.2	103.199.160.80	DNS	78	Standard query 0xc4aa A studio.youtube.com
497	13.100675	192.168.1.2	103.199.160.80	DNS	78	Standard query 0xf7eb HTTPS studio.youtube.com
498	13.101278	192.168.1.2	103.199.160.80	DNS	78	Standard query 0xa9b3 A studio.youtube.com
499	13.101398	192.168.1.2	103.199.160.80	DNS	75	Standard query 0x84f6 A www.youtube.com
500	13.111441	103.199.160.80	192.168.1.2	DNS	371	Standard query response 0xa9b3 A studio.youtube.com CNAME youtube-ui.l.google.com A 142.250.77.142 A 142.250.205.14 A 142.251.4…
501	13.111441	103.199.160.80	192.168.1.2	DNS	371	Standard query response 0xc4aa A studio.youtube.com CNAME youtube-ui.l.google.com A 142.250.206.14 A 142.251.221.142 A 142.251.…
502	13.111441	103.199.160.80	192.168.1.2	DNS	130	Standard query response 0xf7eb HTTPS studio.youtube.com CNAME youtube-ui.l.google.com HTTPS
503	13.111441	103.199.160.80	192.168.1.2	DNS	368	Standard query response 0x84f6 A www.youtube.com CNAME youtube-ui.l.google.com A 142.251.43.238 A 142.251.221.174 A 142.251.221…
546	15.835767	192.168.1.2	103.160.195.230	DNS	80	Standard query 0xde13 A oauth-auth.oc.hp.com
547	15.844125	103.160.195.230	192.168.1.2	DNS	189	Standard query response 0xde13 A oauth-auth.oc.hp.com CNAME hpcorp-prod-columbia.apigee.net CNAME hpcorp-prod-columbia.dn.apige…
569	16.863123	192.168.1.2	103.160.195.230	DNS	91	Standard query 0xc415 A geoip-integrations.us.oc.hp.com
570	16.870591	103.160.195.230	192.168.1.2	DNS	200	Standard query response 0xc415 A geoip-integrations.us.oc.hp.com CNAME hpcorp-prod-columbia.apigee.net CNAME hpcorp-prod-columb…
669	21.859936	192.168.1.2	103.199.160.80	DNS	78	Standard query 0x1281 A edge.microsoft.com
670	21.860149	192.168.1.2	103.199.160.80	DNS	78	Standard query 0x9bed HTTPS edge.microsoft.com
671	21.870245	103.199.160.80	192.168.1.2	DNS	178	Standard query response 0x1281 A edge.microsoft.com CNAME edge-microsoft-com.ax-0002.ax-msedge.net CNAME ax-0002.ax-msedge.net …
672	21.870245	103.199.160.80	192.168.1.2	DNS	192	Standard query response 0x9bed HTTPS edge.microsoft.com CNAME edge-microsoft-com.ax-0002.ax-msedge.net SOA ns1.ax-msedge.net
723	23.622219	192.168.1.2	103.160.195.230	DNS	79	Standard query 0x2561 A default.exp-tas.com

icmp

No.	Time	Source	Destination	Protocol	Length	Info
→ 8954	122.113011	192.168.1.2	142.250.77.142	ICMP	74	Echo (ping) request id=0x0001, seq=1/256, ttl=128 (reply in 8957)
← 8957	122.130279	142.250.77.142	192.168.1.2	ICMP	74	Echo (ping) reply id=0x0001, seq=1/256, ttl=118 (request in 8954)
8961	123.119440	192.168.1.2	142.250.77.142	ICMP	74	Echo (ping) request id=0x0001, seq=2/512, ttl=128 (reply in 8962)
8962	123.137498	142.250.77.142	192.168.1.2	ICMP	74	Echo (ping) reply id=0x0001, seq=2/512, ttl=118 (request in 8961)
8977	124.133283	192.168.1.2	142.250.77.142	ICMP	74	Echo (ping) request id=0x0001, seq=3/768, ttl=128 (reply in 8978)
8978	124.152829	142.250.77.142	192.168.1.2	ICMP	74	Echo (ping) reply id=0x0001, seq=3/768, ttl=118 (request in 8977)
9003	125.165121	192.168.1.2	142.250.77.142	ICMP	74	Echo (ping) request id=0x0001, seq=4/1024, ttl=128 (reply in 9004)
9004	125.183168	142.250.77.142	192.168.1.2	ICMP	74	Echo (ping) reply id=0x0001, seq=4/1024, ttl=118 (request in 9003)