Wireshark Packet Capture Report

Task 5 - Capture and Analyze Network Traffic

Objective:

Capture live network packets and identify basic protocols and traffic types using Wireshark.

Tools Used:

* Wireshark (v4.4.7)

Steps Followed:

1. Installed Wireshark and launched it.

2. Started packet capture on the active Wi-Fi interface.

3. Opened a browser and accessed common websites to generate network traffic.

4. Stopped the capture after approximately one minute.

5. Applied filters for common protocols such as:

   - HTTP

   - DNS

   - TCP

   - TLSv1.2

   - MDNS

6. Identified the presence of at least three different protocols in the capture.

7. Exported the captured packets as a `.pcapng` file.

8. Summarized key packet insights (see below).

Protocols Identified:

* TCP: Used for reliable data transmission, seen initiating encrypted sessions on port 443.

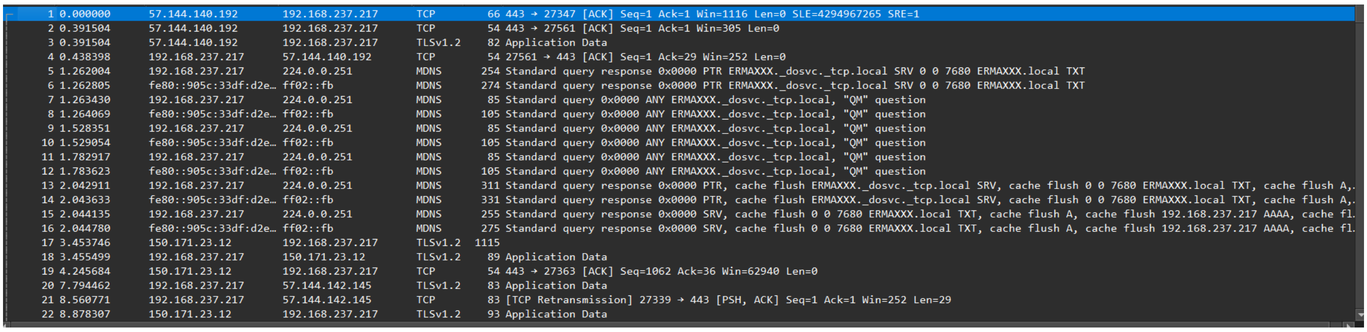
* TLSv1.2: Encrypts application layer traffic like HTTPS, ensuring privacy and integrity.

* MDNS: Enables device discovery on the local network without external DNS.

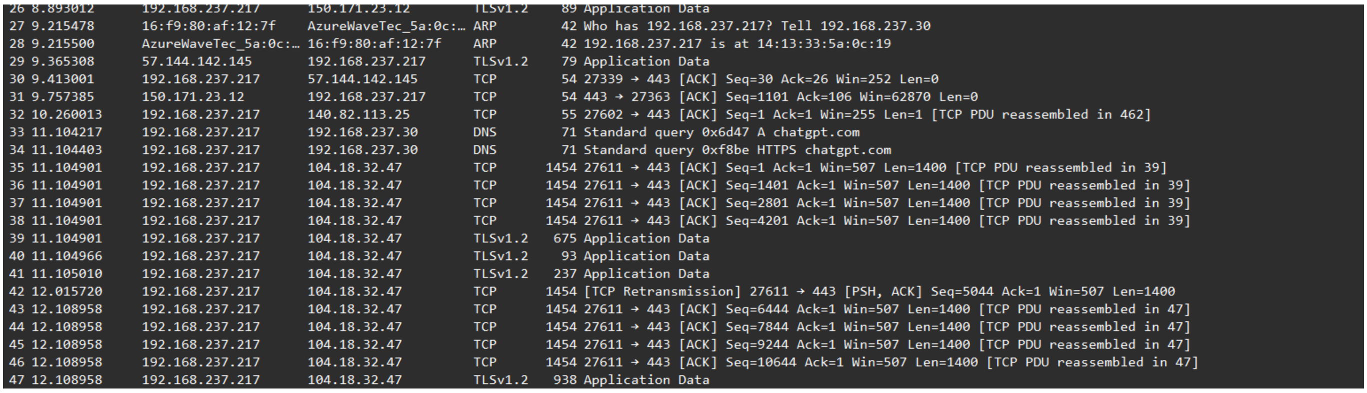
* DNS: Translates domain names (e.g., chatgpt.com) to IP addresses.

* ARP: Resolves IP addresses to MAC addresses inside the local network.

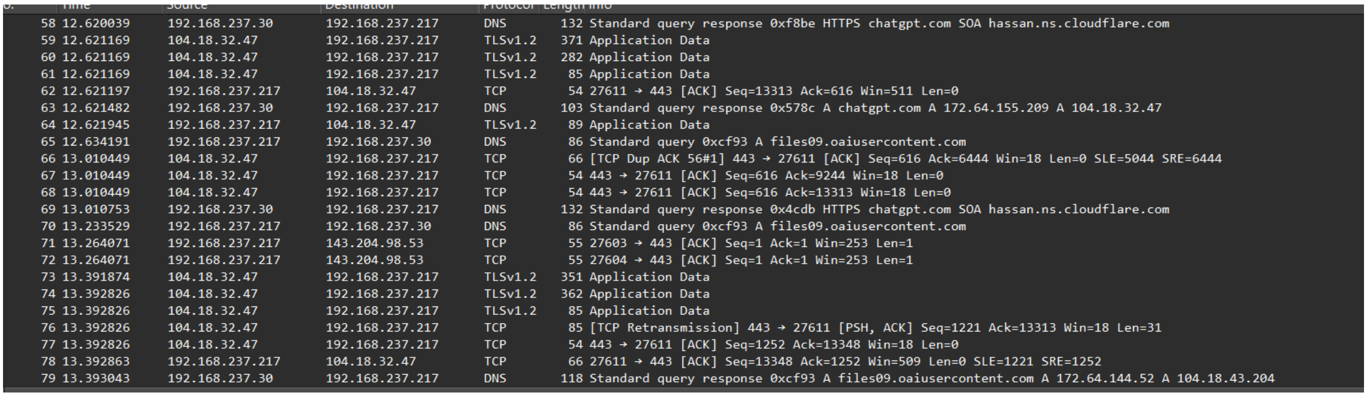
Screenshots of Capture:



```
    1 0.000000     57.144.140.192      192.168.237.217     TCP        66 443 → 27347 [ACK] Seq=1 Ack=1 Win=1116 Len=0 SLE=4294967265 SRE=1
    2 0.391504     57.144.140.192      192.168.237.217     TCP        54 443 → 27561 [ACK] Seq=1 Ack=1 Win=305 Len=0
    3 0.391504     57.144.140.192      192.168.237.217     TLSv1.2    82 Application Data
    4 0.438398     192.168.237.217     57.144.140.192      TCP        54 27561 → 443 [ACK] Seq=1 Ack=29 Win=252 Len=0
    5 1.262004     192.168.237.217     224.0.0.251         MDNS      254 Standard query response 0x0000 PTR ERMAXXX._dosvc._tcp.local SRV 0 0 7680 ERMAXXX.local TXT
    6 1.262805     fe80::905c:33df:d2e… ff02::fb           MDNS      274 Standard query response 0x0000 PTR ERMAXXX._dosvc._tcp.local SRV 0 0 7680 ERMAXXX.local TXT
    7 1.263430     192.168.237.217     224.0.0.251         MDNS       85 Standard query 0x0000 ANY ERMAXXX._dosvc._tcp.local, "QM" question
    8 1.264069     fe80::905c:33df:d2e… ff02::fb           MDNS      105 Standard query 0x0000 ANY ERMAXXX._dosvc._tcp.local, "QM" question
    9 1.528351     192.168.237.217     224.0.0.251         MDNS       85 Standard query 0x0000 ANY ERMAXXX._dosvc._tcp.local, "QM" question
   10 1.529054     fe80::905c:33df:d2e… ff02::fb           MDNS      105 Standard query 0x0000 ANY ERMAXXX._dosvc._tcp.local, "QM" question
   11 1.782917     192.168.237.217     224.0.0.251         MDNS       85 Standard query 0x0000 ANY ERMAXXX._dosvc._tcp.local, "QM" question
   12 1.783623     fe80::905c:33df:d2e… ff02::fb           MDNS      105 Standard query 0x0000 ANY ERMAXXX._dosvc._tcp.local, "QM" question
   13 2.042911     192.168.237.217     224.0.0.251         MDNS      311 Standard query response 0x0000 PTR, cache flush ERMAXXX._dosvc._tcp.local SRV, cache flush 0 0 7680 ERMAXXX.local TXT, cache flush A,…
   14 2.043633     fe80::905c:33df:d2e… ff02::fb           MDNS      331 Standard query response 0x0000 PTR, cache flush ERMAXXX._dosvc._tcp.local SRV, cache flush 0 0 7680 ERMAXXX.local TXT, cache flush A,…
   15 2.044135     192.168.237.217     224.0.0.251         MDNS      255 Standard query response 0x0000 SRV, cache flush 0 0 7680 ERMAXXX.local TXT, cache flush A, cache flush 192.168.237.217 AAAA, cache fl…
   16 2.044780     fe80::905c:33df:d2e… ff02::fb           MDNS      275 Standard query response 0x0000 SRV, cache flush 0 0 7680 ERMAXXX.local TXT, cache flush A, cache flush 192.168.237.217 AAAA, cache fl…
   17 3.453746     150.171.23.12       192.168.237.217     TLSv1.2  1115
   18 3.455499     192.168.237.217     150.171.23.12       TLSv1.2    89 Application Data
   19 4.245684     150.171.23.12       192.168.237.217     TCP        54 443 → 27363 [ACK] Seq=1062 Ack=36 Win=62940 Len=0
   20 7.794462     192.168.237.217     57.144.142.145      TLSv1.2    83 Application Data
   21 8.560771     192.168.237.217     57.144.142.145      TCP        83 [TCP Retransmission] 27339 → 443 [PSH, ACK] Seq=1 Ack=1 Win=252 Len=29
   22 8.878307     150.171.23.12       192.168.237.217     TLSv1.2    93 Application Data
```



```
26 8.893012      192.168.237.217      150.171.23.12        TLSv1.2     89 Application Data
27 9.215478      16:f9:80:af:12:7f    AzureWaveTec_5a:0c:… ARP         42 Who has 192.168.237.217? Tell 192.168.237.30
28 9.215500      AzureWaveTec_5a:0c:… 16:f9:80:af:12:7f    ARP         42 192.168.237.217 is at 14:13:33:5a:0c:19
29 9.365308      57.144.142.145       192.168.237.217      TLSv1.2     79 Application Data
30 9.413001      192.168.237.217      57.144.142.145       TCP         54 27339 → 443 [ACK] Seq=30 Ack=26 Win=252 Len=0
31 9.757385      150.171.23.12        192.168.237.217      TCP         54 443 → 27363 [ACK] Seq=1101 Ack=106 Win=62870 Len=0
32 10.260013     192.168.237.217      140.82.113.25        TCP         55 27602 → 443 [ACK] Seq=1 Ack=1 Win=255 Len=1 [TCP PDU reassembled in 462]
33 11.104217     192.168.237.217      192.168.237.30       DNS         71 Standard query 0x6d47 A chatgpt.com
34 11.104403     192.168.237.217      192.168.237.30       DNS         71 Standard query 0xf8be HTTPS chatgpt.com
35 11.104901     192.168.237.217      104.18.32.47         TCP       1454 27611 → 443 [ACK] Seq=1 Ack=1 Win=507 Len=1400 [TCP PDU reassembled in 39]
36 11.104901     192.168.237.217      104.18.32.47         TCP       1454 27611 → 443 [ACK] Seq=1401 Ack=1 Win=507 Len=1400 [TCP PDU reassembled in 39]
37 11.104901     192.168.237.217      104.18.32.47         TCP       1454 27611 → 443 [ACK] Seq=2801 Ack=1 Win=507 Len=1400 [TCP PDU reassembled in 39]
38 11.104901     192.168.237.217      104.18.32.47         TCP       1454 27611 → 443 [ACK] Seq=4201 Ack=1 Win=507 Len=1400 [TCP PDU reassembled in 39]
39 11.104901     192.168.237.217      104.18.32.47         TLSv1.2    675 Application Data
40 11.104966     192.168.237.217      104.18.32.47         TLSv1.2     93 Application Data
41 11.105010     192.168.237.217      104.18.32.47         TLSv1.2    237 Application Data
42 12.015720     192.168.237.217      104.18.32.47         TCP       1454 [TCP Retransmission] 27611 → 443 [PSH, ACK] Seq=5044 Ack=1 Win=507 Len=1400
43 12.108958     192.168.237.217      104.18.32.47         TCP       1454 27611 → 443 [ACK] Seq=6444 Ack=1 Win=507 Len=1400 [TCP PDU reassembled in 47]
44 12.108958     192.168.237.217      104.18.32.47         TCP       1454 27611 → 443 [ACK] Seq=7844 Ack=1 Win=507 Len=1400 [TCP PDU reassembled in 47]
45 12.108958     192.168.237.217      104.18.32.47         TCP       1454 27611 → 443 [ACK] Seq=9244 Ack=1 Win=507 Len=1400 [TCP PDU reassembled in 47]
46 12.108958     192.168.237.217      104.18.32.47         TCP       1454 27611 → 443 [ACK] Seq=10644 Ack=1 Win=507 Len=1400 [TCP PDU reassembled in 47]
47 12.108958     192.168.237.217      104.18.32.47         TLSv1.2    938 Application Data
```



```
o.      Time         Source               Destination          Protocol Length Info
    58 12.620039     192.168.237.30       192.168.237.217      DNS        132 Standard query response 0xf8be HTTPS chatgpt.com SOA hassan.ns.cloudflare.com
    59 12.621169     104.18.32.47         192.168.237.217      TLSv1.2    371 Application Data
    60 12.621169     104.18.32.47         192.168.237.217      TLSv1.2    282 Application Data
    61 12.621169     104.18.32.47         192.168.237.217      TLSv1.2     85 Application Data
    62 12.621197     192.168.237.217      104.18.32.47         TCP         54 27611 → 443 [ACK] Seq=13313 Ack=616 Win=511 Len=0
    63 12.621482     192.168.237.30       192.168.237.217      DNS        103 Standard query response 0x578c A chatgpt.com A 172.64.155.209 A 104.18.32.47
    64 12.621945     192.168.237.217      104.18.32.47         TLSv1.2     89 Application Data
    65 12.634191     192.168.237.217      192.168.237.30       DNS         86 Standard query 0xcf93 A files09.oaiusercontent.com
    66 13.010449     104.18.32.47         192.168.237.217      TCP         66 [TCP Dup ACK 56#1] 443 → 27611 [ACK] Seq=616 Ack=6444 Win=18 Len=0 SLE=5044 SRE=6444
    67 13.010449     104.18.32.47         192.168.237.217      TCP         54 443 → 27611 [ACK] Seq=616 Ack=9244 Win=18 Len=0
    68 13.010449     104.18.32.47         192.168.237.217      TCP         54 443 → 27611 [ACK] Seq=616 Ack=13313 Win=18 Len=0
    69 13.010753     192.168.237.30       192.168.237.217      DNS        132 Standard query response 0x4cdb HTTPS chatgpt.com SOA hassan.ns.cloudflare.com
    70 13.233529     192.168.237.217      192.168.237.30       DNS         86 Standard query 0xcf93 A files09.oaiusercontent.com
    71 13.264071     192.168.237.217      143.204.98.53        TCP         55 27603 → 443 [ACK] Seq=1 Ack=1 Win=253 Len=1
    72 13.264071     192.168.237.217      143.204.98.53        TCP         55 27604 → 443 [ACK] Seq=1 Ack=1 Win=253 Len=1
    73 13.391874     104.18.32.47         192.168.237.217      TLSv1.2    351 Application Data
    74 13.392826     104.18.32.47         192.168.237.217      TLSv1.2    362 Application Data
    75 13.392826     104.18.32.47         192.168.237.217      TLSv1.2     85 Application Data
    76 13.392826     104.18.32.47         192.168.237.217      TCP         85 [TCP Retransmission] 443 → 27611 [PSH, ACK] Seq=1221 Ack=13313 Win=18 Len=31
    77 13.392826     104.18.32.47         192.168.237.217      TCP         54 443 → 27611 [ACK] Seq=1252 Ack=13348 Win=18 Len=0
    78 13.392863     192.168.237.217      104.18.32.47         TCP         66 27611 → 443 [ACK] Seq=13348 Ack=1252 Win=509 Len=0 SLE=1221 SRE=1252
    79 13.393043     192.168.237.30       192.168.237.217      DNS        118 Standard query response 0xcf93 A files09.oaiusercontent.com A 172.64.144.52 A 104.18.43.204
```

## Outcome

This hands-on activity successfully captured live traffic and revealed multiple real-world protocols in action. The process improved understanding of Wireshark usage and enhanced protocol analysis skills.