Shailesh_task5

Network Traffic Summary (Wireshark Analysis)

1. ICMP Traffic (Ping Requests/Replies)

Protocol: ICMP (Internet Control Message Protocol

Type: Echo (ping) Request/Reply

Communication: Between 192.168.138.61 and 8.8.8.8 (Google DNS)

Observation:

Normal ping communication with proper request and reply sequences (e.g., seq=1/256, seq=2/512, etc.)

This indicates the host is testing network connectivity or performing a diagnostic trace route.

2. HTTP Traffic

Protocol: HTTP over TCP (Port 80)

Source IPs: 184.28.173.48 and 151.101.38.172

Destination: 192.168.138.61

Observation:

Multiple large-size packets (1354 bytes) indicating HTTP continuation responses.

Likely file/data transfer or web browsing activity from remote servers to the local client.

3. ARP Traffic (Address Resolution Protocol)

Screenshot: Screenshot 2025-06-30 195301.png

Protocol: ARP

Activity:

Who has 192.168.138.61? Tell 192.168.138.42

Response: 192.168.138.61 is at b4:8c:9d:64:17:e5

Observation:

Typical ARP request and reply sequence.

Confirms MAC-to-IP resolution in the local network.

No spoofing behavior observed in this snapshot.

4. UDP and mDNS Traffic

Screenshot: Screenshot 2025-06-30 195329.png

Protocol: UDP and mDNS

UDP Communication:

Between 142.251.223.234 and 192.168.138.61

Ports: 443 → 64428 (Encrypted traffic likely via QUIC or other UDP-based service)

mDNS (Multicast DNS):

Frequent queries for service discovery in .local domain (e.g., _googlecast._tcp.local)

Devices appear to be discovering Chromecast or similar services on the LAN.

Observation:

Standard UDP and multicast service discovery.

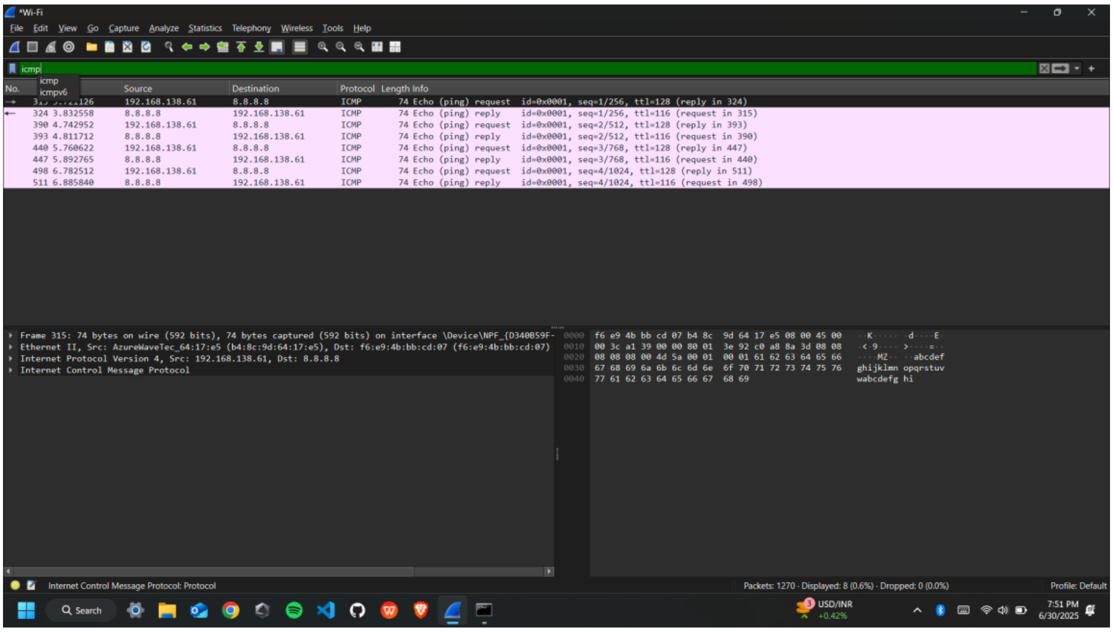
No suspicious or malformed packets.

Overall Network Activity Insights

Protocol	Purpose	Remarks
ICMP	Network diagnostics	Normal ping to Google DNS
HTTP	Web traffic	Continued HTTP responses from servers
ARP	Local network IP-MAC mapping	Normal address resolution activity

Protocol	Purpose	Remarks
UDP/mDNS	Streaming/Service discovery	Chromecast or IoT service identification

Screenshots:


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
icmp
icmpv6

```
No.          Source           Destination      Protocol Length Info
→  315 [illegible]126  192.168.138.61  8.8.8.8          ICMP     74 Echo (ping) request  id=0x0001, seq=1/256, ttl=128 (reply in 324)
←  324 3.832558  8.8.8.8          192.168.138.61   ICMP     74 Echo (ping) reply    id=0x0001, seq=1/256, ttl=116 (request in 315)
   390 4.742952  192.168.138.61   8.8.8.8          ICMP     74 Echo (ping) request  id=0x0001, seq=2/512, ttl=128 (reply in 393)
   393 4.811712  8.8.8.8          192.168.138.61   ICMP     74 Echo (ping) reply    id=0x0001, seq=2/512, ttl=116 (request in 390)
   440 5.760622  192.168.138.61   8.8.8.8          ICMP     74 Echo (ping) request  id=0x0001, seq=3/768, ttl=128 (reply in 447)
   447 5.892765  8.8.8.8          192.168.138.61   ICMP     74 Echo (ping) reply    id=0x0001, seq=3/768, ttl=116 (request in 440)
   498 6.782512  192.168.138.61   8.8.8.8          ICMP     74 Echo (ping) request  id=0x0001, seq=4/1024, ttl=128 (reply in 511)
   511 6.885840  8.8.8.8          192.168.138.61   ICMP     74 Echo (ping) reply    id=0x0001, seq=4/1024, ttl=116 (request in 498)
```

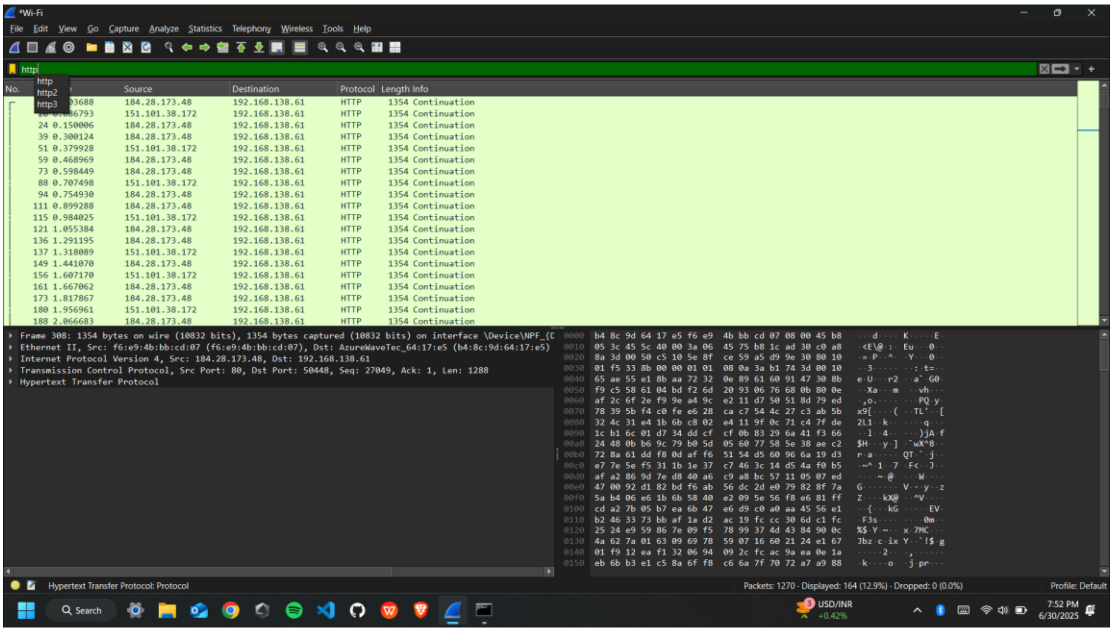
```
> Frame 315: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{D340B59F-
> Ethernet II, Src: AzureWaveTec_64:17:e5 (b4:8c:9d:64:17:e5), Dst: f6:e9:4b:bb:cd:07 (f6:e9:4b:bb:cd:07)
> Internet Protocol Version 4, Src: 192.168.138.61, Dst: 8.8.8.8
> Internet Control Message Protocol
```

```
0000  f6 e9 4b bb cd 07 b4 8c  9d 64 17 e5 08 00 45 00   ··K·····  ·d····E·
0010  00 3c a1 39 00 00 80 01  3e 92 c0 a8 8a 3d 08 08   ·<·9····  >····=··
0020  08 08 08 00 4d 5a 00 01  00 01 61 62 63 64 65 66   ····MZ··  ··abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn  opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg  hi
```

Internet Control Message Protocol: Protocol

Packets: 1270 · Displayed: 8 (0.6%) · Dropped: 0 (0.0%)

Profile: Default



*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
http
http2
http3

```
No.  Time         Source           Destination      Protocol Length Info
     ..03688      184.28.173.48    192.168.138.61   HTTP     1354 Continuation
     ..086793     151.101.38.172   192.168.138.61   HTTP     1354 Continuation
  24 0.150006     184.28.173.48    192.168.138.61   HTTP     1354 Continuation
  39 0.300124     184.28.173.48    192.168.138.61   HTTP     1354 Continuation
  51 0.379928     151.101.38.172   192.168.138.61   HTTP     1354 Continuation
  59 0.468969     184.28.173.48    192.168.138.61   HTTP     1354 Continuation
  73 0.598449     184.28.173.48    192.168.138.61   HTTP     1354 Continuation
  88 0.707498     151.101.38.172   192.168.138.61   HTTP     1354 Continuation
  94 0.754930     184.28.173.48    192.168.138.61   HTTP     1354 Continuation
 111 0.899288     184.28.173.48    192.168.138.61   HTTP     1354 Continuation
 115 0.984025     151.101.38.172   192.168.138.61   HTTP     1354 Continuation
 121 1.055384     184.28.173.48    192.168.138.61   HTTP     1354 Continuation
 136 1.291195     184.28.173.48    192.168.138.61   HTTP     1354 Continuation
 137 1.318089     151.101.38.172   192.168.138.61   HTTP     1354 Continuation
 149 1.441070     184.28.173.48    192.168.138.61   HTTP     1354 Continuation
 156 1.607170     151.101.38.172   192.168.138.61   HTTP     1354 Continuation
 161 1.667062     184.28.173.48    192.168.138.61   HTTP     1354 Continuation
 173 1.817867     184.28.173.48    192.168.138.61   HTTP     1354 Continuation
 180 1.956961     151.101.38.172   192.168.138.61   HTTP     1354 Continuation
 188 2.066683     184.28.173.48    192.168.138.61   HTTP     1354 Continuation
```

```
> Frame 308: 1354 bytes on wire (10832 bits), 1354 bytes captured (10832 bits) on interface \Device\NPF_{C
> Ethernet II, Src: f6:e9:4b:bb:cd:07 (f6:e9:4b:bb:cd:07), Dst: AzureWaveTec_64:17:e5 (b4:8c:9d:64:17:e5)
> Internet Protocol Version 4, Src: 184.28.173.48, Dst: 192.168.138.61
> Transmission Control Protocol, Src Port: 80, Dst Port: 50448, Seq: 27049, Ack: 1, Len: 1288
> Hypertext Transfer Protocol
```

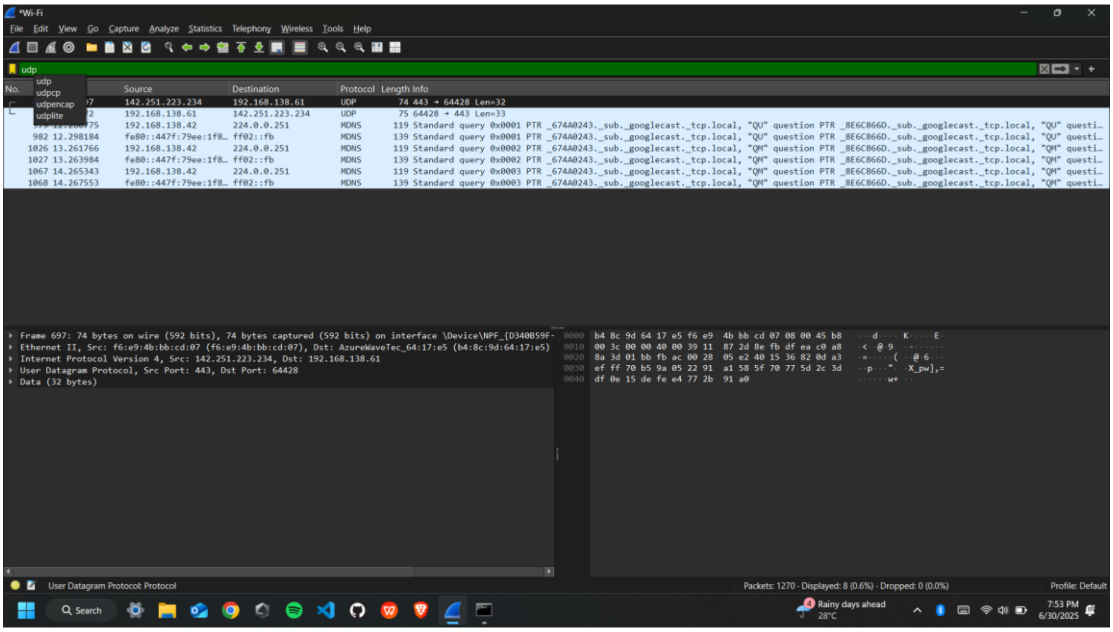
```
0000  b4 8c 9d 64 17 e5 f6 e9  4b bb cd 07 08 00 45 b8
0010  05 3c 45 5c 40 00 3a 06  45 75 b8 1c ad 30 c0 a8
0020  8a 3d 00 50 c5 10 5e 8f  ce 59 a5 d9 9e 30 80 10
0030  01 f5 33 8b 00 00 01 01  08 0a 3a b1 74 3d 00 10
0040  65 ae 55 e1 8b aa 72 32  0e 89 61 60 91 47 30 8b
0050  f9 c5 58 61 04 bd f2 6d  20 93 06 76 68 0b 80 0e
0060  af 2c 6f 2e f9 9e a4 9c  e2 11 d7 50 51 8d 79 ed
0070  78 39 5b f4 c0 fe e6 28  ca c7 54 4c 27 c3 ab 5b
0080  32 4c 31 e4 1b 6b c8 02  e4 11 9f 0c 71 c4 7f de
0090  1c b1 6c 01 d7 34 dd cf  cf 0b 83 29 6a 41 f3 66
00a0  24 48 0b b6 9c 79 b0 5d  05 60 77 58 5e 38 ae c2
00b0  72 8a 61 dd f8 0d af f6  51 54 d5 60 96 6a 19 d3
00c0  e7 7e 5e f5 31 1b 1e 37  c7 46 3c 14 d5 4a f0 b5
00d0  af a2 86 9d 7e d8 40 a6  c9 a8 bc 57 11 05 07 ed
00e0  47 00 92 d1 82 bd f6 ab  56 dc 2d e0 79 82 8f 7a
00f0  5a b4 06 e6 1b 6b 58 40  e2 09 5e 56 f8 e6 81 ff
0100  cd a2 7b 05 b7 ea 6b 47  e6 d9 c0 a0 aa 45 56 e1
0110  b2 46 33 73 bb af 1a d2  ac 19 fc cc 30 6d c1 fc
0120  25 24 e9 59 86 7e 09 f5  78 99 37 4d 43 84 90 0c
0130  4a 62 7a 01 63 09 69 78  59 07 16 60 21 24 e1 67
0140  01 f9 12 ea f1 32 06 94  09 2c fc ac 9a ea 0e 1a
0150  eb 6b b3 e1 c5 8a 6f f8  c6 6a 7f 70 72 a7 a9 88
```

Hypertext Transfer Protocol: Protocol

Packets: 1270 · Displayed: 164 (12.9%) · Dropped: 0 (0.0%)

Profile: Default

Search
3 USD/INR
+0.42%
7:52 PM
6/30/2025



*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
udp
udp
udpcp
udpencap
udplite

```
No.  Time         Source                  Destination      Protocol Length Info
     ..97         142.251.223.234         192.168.138.61   UDP        74 443 → 64428 Len=32
     ..72         192.168.138.61          142.251.223.234  UDP        75 64428 → 443 Len=33
     ..75         192.168.138.42          224.0.0.251      MDNS      119 Standard query 0x0001 PTR _674A0243._sub._googlecast._tcp.local, "QU" question PTR _8E6C866D._sub._googlecast._tcp.local, "QU" questi…
 982 12.298184    fe80::447f:79ee:1f8…    ff02::fb         MDNS      139 Standard query 0x0001 PTR _674A0243._sub._googlecast._tcp.local, "QU" question PTR _8E6C866D._sub._googlecast._tcp.local, "QU" questi…
1026 13.261766    192.168.138.42          224.0.0.251      MDNS      119 Standard query 0x0002 PTR _674A0243._sub._googlecast._tcp.local, "QM" question PTR _8E6C866D._sub._googlecast._tcp.local, "QM" questi…
1027 13.263984    fe80::447f:79ee:1f8…    ff02::fb         MDNS      139 Standard query 0x0002 PTR _674A0243._sub._googlecast._tcp.local, "QM" question PTR _8E6C866D._sub._googlecast._tcp.local, "QM" questi…
1067 14.265343    192.168.138.42          224.0.0.251      MDNS      119 Standard query 0x0003 PTR _674A0243._sub._googlecast._tcp.local, "QM" question PTR _8E6C866D._sub._googlecast._tcp.local, "QM" questi…
1068 14.267553    fe80::447f:79ee:1f8…    ff02::fb         MDNS      139 Standard query 0x0003 PTR _674A0243._sub._googlecast._tcp.local, "QM" question PTR _8E6C866D._sub._googlecast._tcp.local, "QM" questi…
```

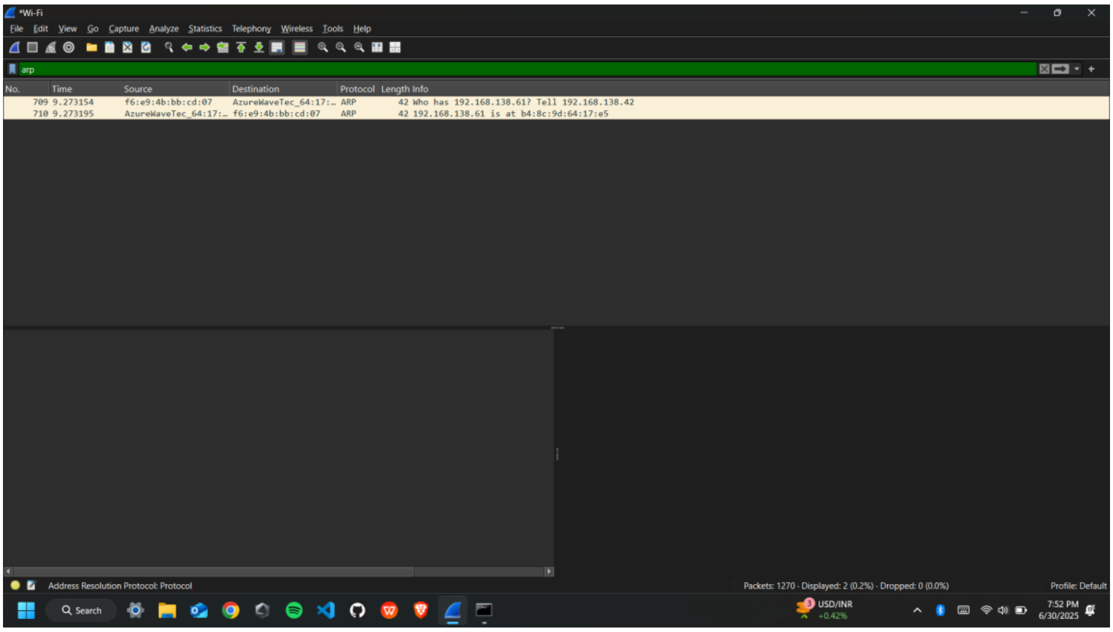
```
> Frame 697: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{D340B59F-
> Ethernet II, Src: f6:e9:4b:bb:cd:07 (f6:e9:4b:bb:cd:07), Dst: AzureWaveTec_64:17:e5 (b4:8c:9d:64:17:e5)
> Internet Protocol Version 4, Src: 142.251.223.234, Dst: 192.168.138.61
> User Datagram Protocol, Src Port: 443, Dst Port: 64428
> Data (32 bytes)
```

```
0000  b4 8c 9d 64 17 e5 f6 e9  4b bb cd 07 08 00 45 b8
0010  00 3c 00 00 40 00 39 11  87 2d 8e fb df ea c0 a8
0020  8a 3d 01 bb fb ac 00 28  05 e2 40 15 36 82 0d a3
0030  ef ff 70 b5 9a 05 22 91  a1 58 5f 70 77 5d 2c 3d
0040  df 0e 15 de fe e4 77 2b  91 a0
```

User Datagram Protocol: Protocol

Packets: 1270 · Displayed: 8 (0.6%) · Dropped: 0 (0.0%)

Profile: Default



*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

arp

```
No.   Time      Source                 Destination            Protocol Length Info
  709 9.273154  f6:e9:4b:bb:cd:07      AzureWaveTec_64:17:…   ARP         42 Who has 192.168.138.61? Tell 192.168.138.42
  710 9.273195  AzureWaveTec_64:17:…   f6:e9:4b:bb:cd:07      ARP         42 192.168.138.61 is at b4:8c:9d:64:17:e5
```

```
Address Resolution Protocol: Protocol          Packets: 1270 · Displayed: 2 (0.2%) · Dropped: 0 (0.0%)          Profile: Default
```

Search
3
USD/INR
+0.42%
7:52 PM
6/30/2025