Cybersecurity

Network Simulation

Lab Assignment

Submitted by

Rijwal vp

24UBC150

BCA A

OSI Model, TCP/IP Model & Wireshark Packet Analysis

part A -osi model theory

1. OSI Layer Explanations

Layer 1 – Physical Layer

The Physical Layer is the quiet workhorse of the network stack. It handles raw signal transmission—electrical pulses, light waves, or radio frequencies—that travel through cables or the air. No interpretation of data occurs here; it only moves bits from one point to another. Technologies like Ethernet cables, fiber optics, connectors, voltage levels, and Wi-Fi radio waves operate in this layer. It can be compared to the actual road or railway track that vehicles use—without this foundation, nothing else in the network can function.

Layer 2 – Data Link Layer

At this layer, the network gains awareness of local devices. The Data Link Layer organizes bits into frames, assigns MAC addresses, and performs error detection using CRC. Switches, NICs, VLANs, ARP, and protocols like Ethernet and PPP belong here. It behaves like a neighborhood traffic manager, ensuring frames reach the correct destination within the local network. It also handles collisions and quietly removes corrupted frames before they reach higher layers.

Layer 3 – Network Layer

The Network Layer enables communication beyond the local network. It manages logical addressing and routing using IP addresses, subnetting, and routers. Protocols like OSPF, RIP, and BGP help determine the optimal path for packets. Each router along the route decides where the packet should travel next. This layer functions like a longdistance postal system, moving data from city to city (network to network) until it reaches its destination.

Layer 4 – Transport Layer

The Transport Layer ensures reliable and orderly communication. It decides whether data should be delivered with reliability (TCP) or speed (UDP). It segments data, assigns port numbers, manages flow control, retransmissions, and reassembly. Think of it as a courier service: TCP handles fragile packages with care, while UDP delivers items quickly with minimal overhead—ideal when speed matters more than accuracy.

Layer 5 – Session Layer

The Session Layer creates, controls, and terminates communication sessions between devices. It keeps track of who is communicating and maintains the session even if interruptions occur. Protocols like RPC and NetBIOS operate here. This layer can be compared to a meeting moderator who ensures conversation flows smoothly without participants talking over one another.

Layer 6 – Presentation Layer

The Presentation Layer acts as the translator of the network. It converts data formats, handles encryption and decryption, and manages compression. Technologies such as SSL/TLS, JPEG, MP3, GIF, and encoding standards like ASCII and UTF-8 belong here. Imagine a multilingual editor who reformats and translates a document so the receiver gets it in the correct style and language.

Layer 7 – Application Layer

This is the topmost layer—the one visible to users. It provides interfaces for web browsing, email, file transfers, and other network services. Protocols like HTTP, HTTPS, FTP, SMTP, DNS, and DHCP function here. It is similar to a service desk counter where users make their requests while the deeper layers handle the actual processing behind the scenes.

2. OSI Mnemonic

“Please Don’t Nap Too Soon, People Are Watching.”

Word	**OSI Layer**
Please	Physical
Don’t	Data Link
Nap	Network
Too	Transport
Soon	Session
People	Presentation
Are Watching	Application

3. OSI vs TCP/IP Model Comparison

The OSI model uses a detailed seven-layer structure to clearly separate networking functions—from raw signals to application-level services. It is considered a theoretical and educational model.
The TCP/IP model, however, is a practical four-layer framework used by real-world networks and the internet. It groups related tasks together, making it simpler and more implementation-focused.

The upper OSI layers (Application, Presentation, Session) merge into one

Application Layer in TCP/IP, while the lower layers (Data Link and Physical) combine into a **Network Access Layer**. Both models describe how data travels through a network but differ in granularity and structure

OSI Layer	TCP/IP Layer	Explanation
Application (L7)	Application Layer	TCP/IP combines user-facing services

		here.
Presentation (L6)	Application Layer	Formatting, encryption, compression are also handled by the TCP/IP Application layer.
Session (L5)	Application Layer	Session management is included within TCP/IP Application protocols.
Transport (L4)	Transport Layer	TCP/UDP control reliability and ports.
Network	Internet	IP, routing,

(L3)	Layer	addressing.
Data Link (L2)	Network Access Layer	Frames, MAC addresses, NICs.
Physical (L1)	Network Access Layer	Cables, signals, physical transmission.

4.Protocol Data Units (PDUs)

OSI Layer	PDU Name	Notes

Layer 4 – Transport	**Segment (TCP) / Datagram (UDP)**	TCP behaves like a careful courier (segments), while UDP tosses lightweight datagrams without ceremony.
Layer 3 – Network	**Packet**	Carries IP addresses and travels across multiple networks.
Layer 2 – Data Link	**Frame**	Wrapped with MAC addresses; perfect for local delivery.
Layer 1 –	**Bits**	Raw 1s and 0s racing through cables

Physical		or airwaves.

5. Addressing Concepts

1. MAC Address — Layer 2 (Data Link)

A MAC address is a hardware identifier built into the network interface card. It acts like a permanent name tag within a local network. Switches use MAC addresses to decide which port should receive a frame, ensuring efficient local delivery.

2. IP Address — Layer 3 (Network)

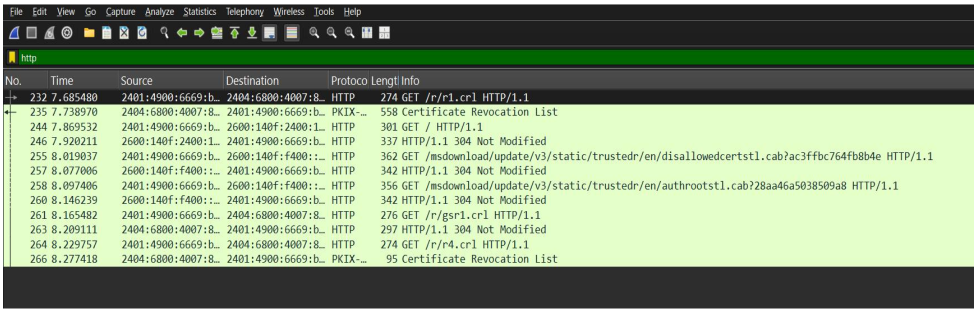
An IP address is a logical address used to identify devices across different networks. Routers use IP addresses to forward packets from one network to another. While MAC addresses tell "who is nearby," IP addresses tell routers "where in the world this data must go."

3. Port Number — Layer 4 (Transport)

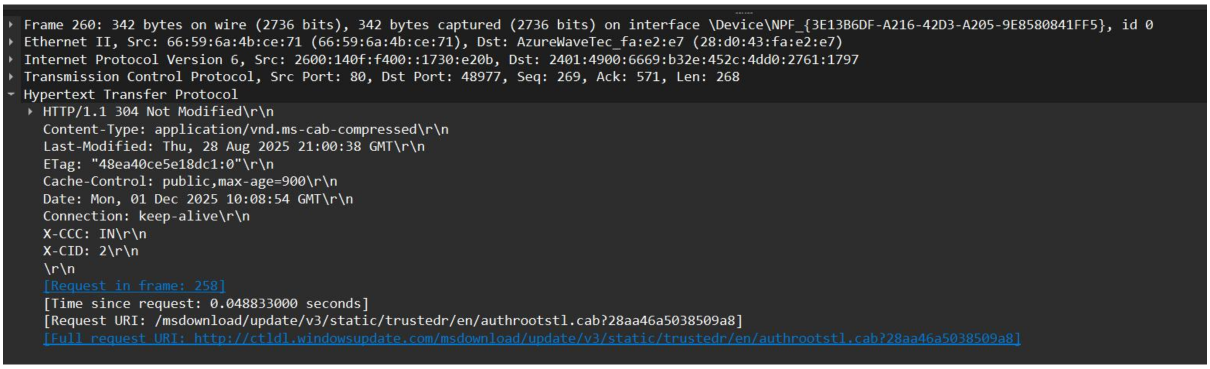
A port number identifies the specific application or service running on a device. TCP and UDP use ports to ensure the correct application receives the datalike directing a package to the correct room within a building.

Part B – Wireshark Practical

1.HTTP Traffic

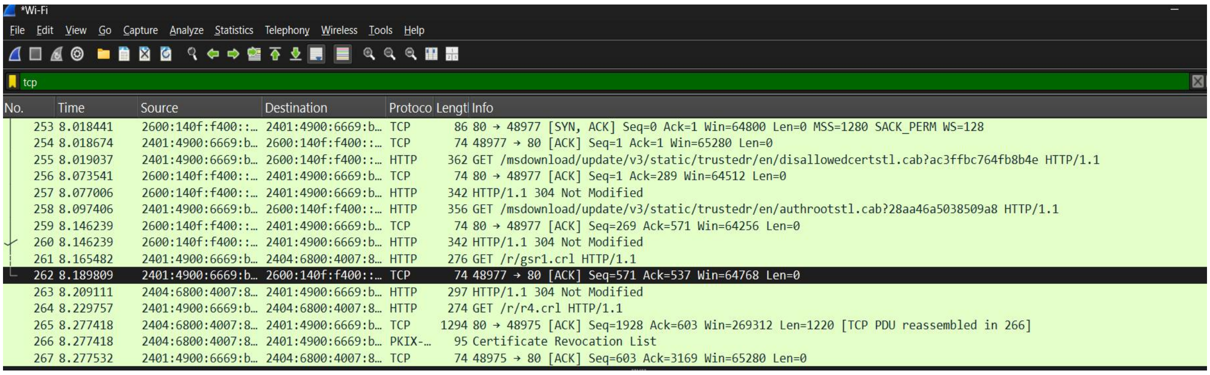


```
No.  Time      Source              Destination         Protoco Lengt Info
  232 7.685480 2401:4900:6669:b… 2404:6800:4007:8… HTTP     274 GET /r/r1.crl HTTP/1.1
  235 7.738970 2404:6800:4007:8… 2401:4900:6669:b… PKIX-…   558 Certificate Revocation List
  244 7.869532 2401:4900:6669:b… 2600:140f:2400:1… HTTP     301 GET / HTTP/1.1
  246 7.920211 2600:140f:2400:1… 2401:4900:6669:b… HTTP     337 HTTP/1.1 304 Not Modified
  255 8.019037 2401:4900:6669:b… 2600:140f:f400::… HTTP     362 GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?ac3ffbc764fb8b4e HTTP/1.1
  257 8.077006 2600:140f:f400::… 2401:4900:6669:b… HTTP     342 HTTP/1.1 304 Not Modified
  258 8.097406 2401:4900:6669:b… 2600:140f:f400::… HTTP     356 GET /msdownload/update/v3/static/trustedr/en/authrootstl.cab?28aa46a5038509a8 HTTP/1.1
  260 8.146239 2600:140f:f400::… 2401:4900:6669:b… HTTP     342 HTTP/1.1 304 Not Modified
  261 8.165482 2401:4900:6669:b… 2404:6800:4007:8… HTTP     276 GET /r/gsr1.crl HTTP/1.1
  263 8.209111 2404:6800:4007:8… 2401:4900:6669:b… HTTP     297 HTTP/1.1 304 Not Modified
  264 8.229757 2401:4900:6669:b… 2404:6800:4007:8… HTTP     274 GET /r/r4.crl HTTP/1.1
  266 8.277418 2404:6800:4007:8… 2401:4900:6669:b… PKIX-…    95 Certificate Revocation List
```



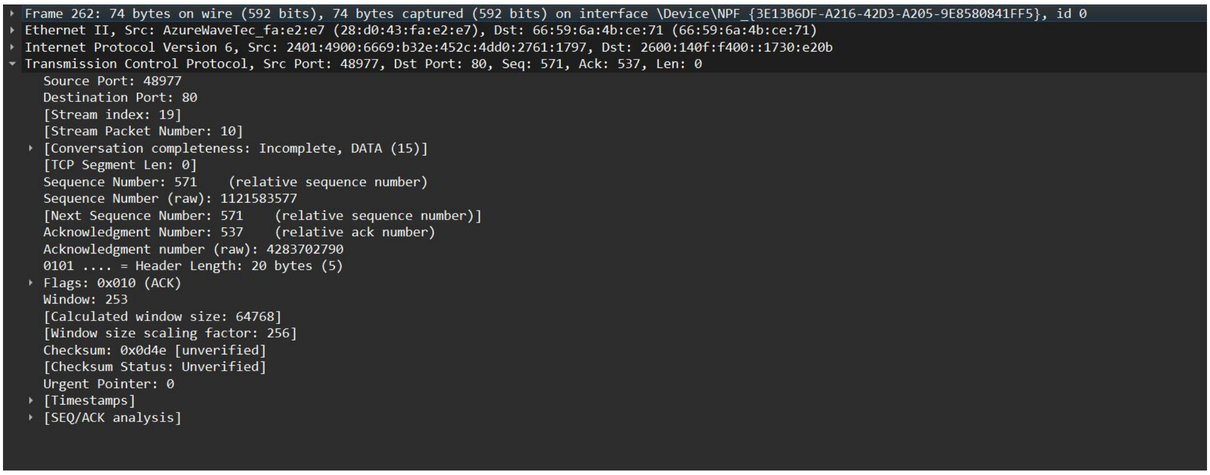
```
› Frame 260: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface \Device\NPF_{3E13B6DF-A216-42D3-A205-9E8580841FF5}, id 0
› Ethernet II, Src: 66:59:6a:4b:ce:71 (66:59:6a:4b:ce:71), Dst: AzureWaveTec_fa:e2:e7 (28:d0:43:fa:e2:e7)
› Internet Protocol Version 6, Src: 2600:140f:f400::1730:e20b, Dst: 2401:4900:6669:b32e:452c:4dd0:2761:1797
› Transmission Control Protocol, Src Port: 80, Dst Port: 48977, Seq: 269, Ack: 571, Len: 268
˅ Hypertext Transfer Protocol
  › HTTP/1.1 304 Not Modified\r\n
    Content-Type: application/vnd.ms-cab-compressed\r\n
    Last-Modified: Thu, 28 Aug 2025 21:00:38 GMT\r\n
    ETag: "48ea40ce5e18dc1:0"\r\n
    Cache-Control: public,max-age=900\r\n
    Date: Mon, 01 Dec 2025 10:08:54 GMT\r\n
    Connection: keep-alive\r\n
    X-CCC: IN\r\n
    X-CID: 2\r\n
    \r\n
    [Request in frame: 258]
    [Time since request: 0.048833000 seconds]
    [Request URI: /msdownload/update/v3/static/trustedr/en/authrootstl.cab?28aa46a5038509a8]
    [Full request URI: http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab?28aa46a5038509a8]
```

2.TCP Packets


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

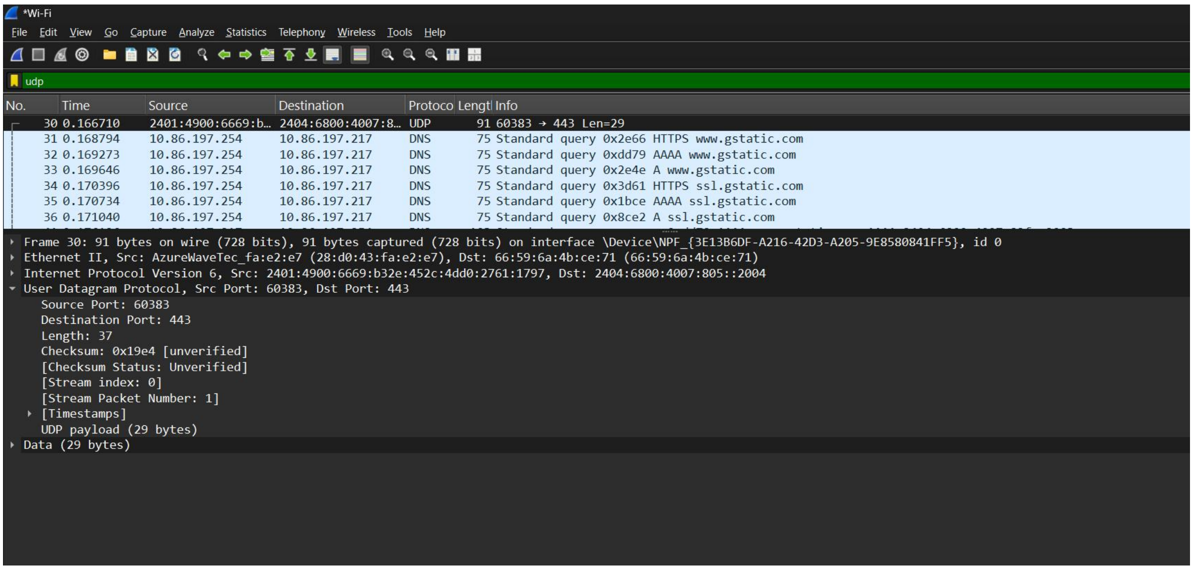
```
tcp
```

```
No.  Time      Source             Destination         Protoco Lengt Info
 253 8.018441  2600:140f:f400::…  2401:4900:6669:b…  TCP       86 80 → 48977 [SYN, ACK] Seq=0 Ack=1 Win=64800 Len=0 MSS=1280 SACK_PERM WS=128
 254 8.018674  2401:4900:6669:b…  2600:140f:f400::…  TCP       74 48977 → 80 [ACK] Seq=1 Ack=1 Win=65280 Len=0
 255 8.019037  2401:4900:6669:b…  2600:140f:f400::…  HTTP     362 GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?ac3ffbc764fb8b4e HTTP/1.1
 256 8.073541  2600:140f:f400::…  2401:4900:6669:b…  TCP       74 80 → 48977 [ACK] Seq=1 Ack=289 Win=64512 Len=0
 257 8.077006  2600:140f:f400::…  2401:4900:6669:b…  HTTP     342 HTTP/1.1 304 Not Modified
 258 8.097406  2401:4900:6669:b…  2600:140f:f400::…  HTTP     356 GET /msdownload/update/v3/static/trustedr/en/authrootstl.cab?28aa46a5038509a8 HTTP/1.1
 259 8.146239  2600:140f:f400::…  2401:4900:6669:b…  TCP       74 80 → 48977 [ACK] Seq=269 Ack=571 Win=64256 Len=0
 260 8.146239  2600:140f:f400::…  2401:4900:6669:b…  HTTP     342 HTTP/1.1 304 Not Modified
 261 8.165482  2401:4900:6669:b…  2404:6800:4007:8…  HTTP     276 GET /r/gsr1.crl HTTP/1.1
 262 8.189809  2401:4900:6669:b…  2600:140f:f400::…  TCP       74 48977 → 80 [ACK] Seq=571 Ack=537 Win=64768 Len=0
 263 8.209111  2404:6800:4007:8…  2401:4900:6669:b…  HTTP     297 HTTP/1.1 304 Not Modified
 264 8.229757  2401:4900:6669:b…  2404:6800:4007:8…  HTTP     274 GET /r/r4.crl HTTP/1.1
 265 8.277418  2404:6800:4007:8…  2401:4900:6669:b…  TCP     1294 80 → 48975 [ACK] Seq=1928 Ack=603 Win=269312 Len=1220 [TCP PDU reassembled in 266]
 266 8.277418  2404:6800:4007:8…  2401:4900:6669:b…  PKIX-…    95 Certificate Revocation List
 267 8.277532  2401:4900:6669:b…  2404:6800:4007:8…  TCP       74 48975 → 80 [ACK] Seq=603 Ack=3169 Win=65280 Len=0
```



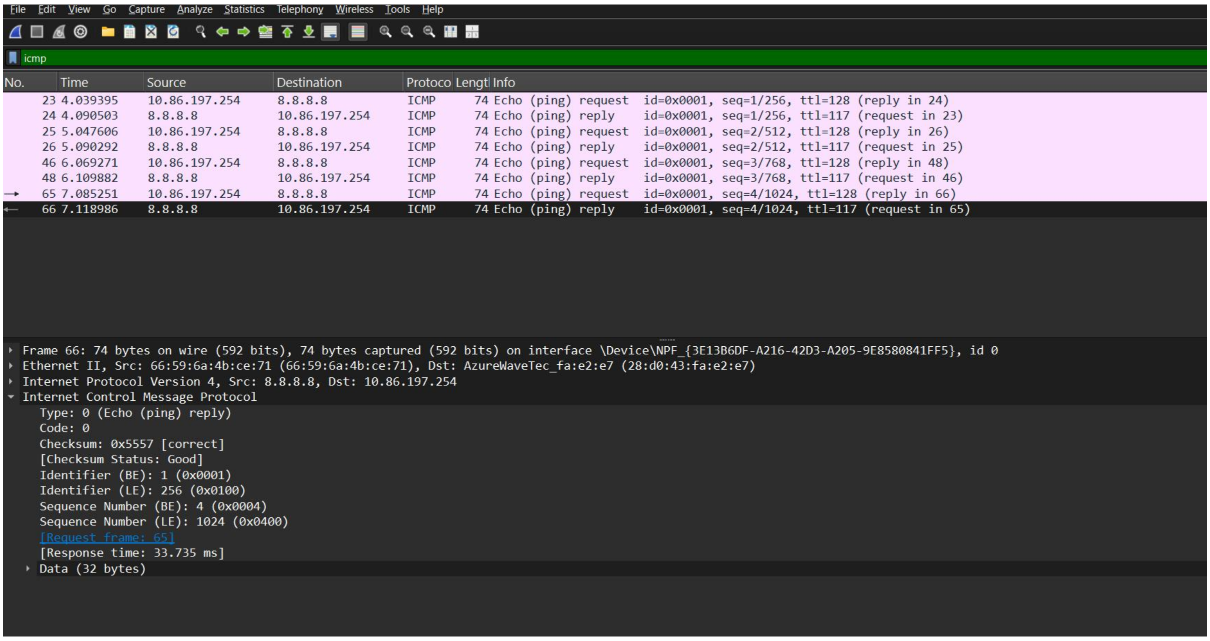
```
› Frame 262: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{3E13B6DF-A216-42D3-A205-9E8580841FF5}, id 0
› Ethernet II, Src: AzureWaveTec_fa:e2:e7 (28:d0:43:fa:e2:e7), Dst: 66:59:6a:4b:ce:71 (66:59:6a:4b:ce:71)
› Internet Protocol Version 6, Src: 2401:4900:6669:b32e:452c:4dd0:2761:1797, Dst: 2600:140f:f400::1730:e20b
⌄ Transmission Control Protocol, Src Port: 48977, Dst Port: 80, Seq: 571, Ack: 537, Len: 0
     Source Port: 48977
     Destination Port: 80
     [Stream index: 19]
     [Stream Packet Number: 10]
   › [Conversation completeness: Incomplete, DATA (15)]
     [TCP Segment Len: 0]
     Sequence Number: 571    (relative sequence number)
     Sequence Number (raw): 1121583577
     [Next Sequence Number: 571    (relative sequence number)]
     Acknowledgment Number: 537    (relative ack number)
     Acknowledgment number (raw): 4283702790
     0101 .... = Header Length: 20 bytes (5)
   › Flags: 0x010 (ACK)
     Window: 253
     [Calculated window size: 64768]
     [Window size scaling factor: 256]
     Checksum: 0x0d4e [unverified]
     [Checksum Status: Unverified]
     Urgent Pointer: 0
   › [Timestamps]
   › [SEQ/ACK analysis]
```

3.UDP Packets

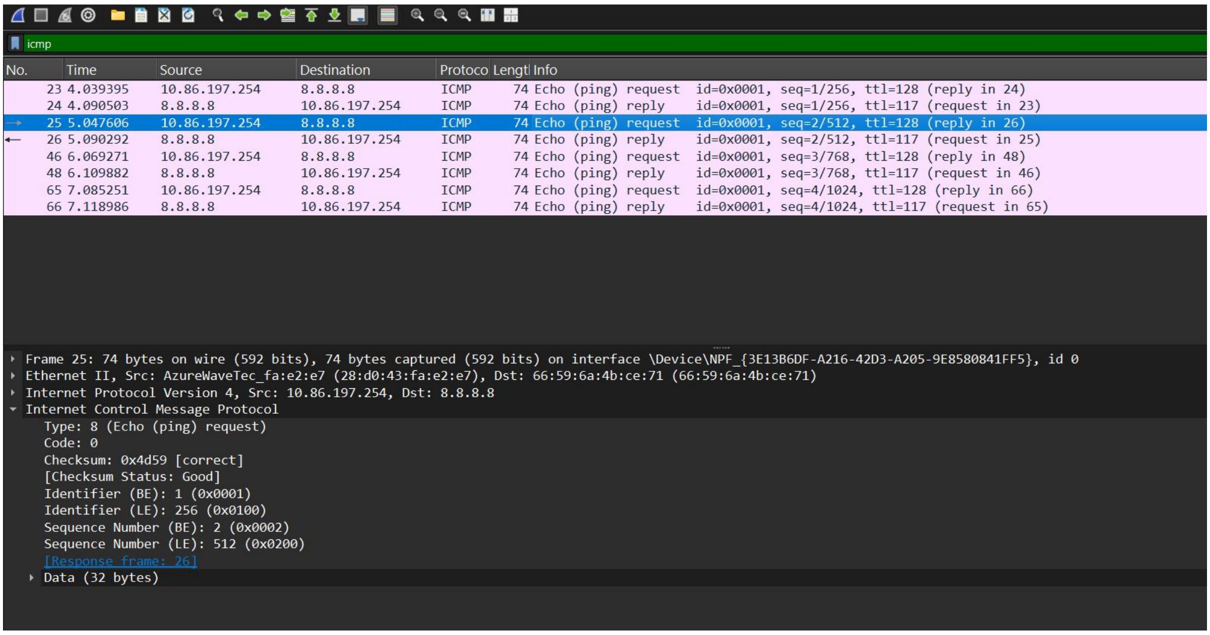

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
udp

```
No.  Time      Source            Destination       Protoco Lengtl Info
  30 0.166710  2401:4900:6669:b… 2404:6800:4007:8… UDP      91 60383 → 443 Len=29
  31 0.168794  10.86.197.254     10.86.197.217     DNS      75 Standard query 0x2e66 HTTPS www.gstatic.com
  32 0.169273  10.86.197.254     10.86.197.217     DNS      75 Standard query 0xdd79 AAAA www.gstatic.com
  33 0.169646  10.86.197.254     10.86.197.217     DNS      75 Standard query 0x2e4e A www.gstatic.com
  34 0.170396  10.86.197.254     10.86.197.217     DNS      75 Standard query 0x3d61 HTTPS ssl.gstatic.com
  35 0.170734  10.86.197.254     10.86.197.217     DNS      75 Standard query 0x1bce AAAA ssl.gstatic.com
  36 0.171040  10.86.197.254     10.86.197.217     DNS      75 Standard query 0x8ce2 A ssl.gstatic.com

Frame 30: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface \Device\NPF_{3E13B6DF-A216-42D3-A205-9E8580841FF5}, id 0
Ethernet II, Src: AzureWaveTec_fa:e2:e7 (28:d0:43:fa:e2:e7), Dst: 66:59:6a:4b:ce:71 (66:59:6a:4b:ce:71)
Internet Protocol Version 6, Src: 2401:4900:6669:b32e:452c:4dd0:2761:1797, Dst: 2404:6800:4007:805::2004
User Datagram Protocol, Src Port: 60383, Dst Port: 443
    Source Port: 60383
    Destination Port: 443
    Length: 37
    Checksum: 0x19e4 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
    [Stream Packet Number: 1]
  [Timestamps]
    UDP payload (29 bytes)
Data (29 bytes)
```

4.ICMP Packets


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp

```
No.  Time      Source         Destination    Protoco Lengtl Info
  23 4.039395  10.86.197.254  8.8.8.8        ICMP     74 Echo (ping) request  id=0x0001, seq=1/256, ttl=128 (reply in 24)
  24 4.090503  8.8.8.8        10.86.197.254  ICMP     74 Echo (ping) reply    id=0x0001, seq=1/256, ttl=117 (request in 23)
  25 5.047606  10.86.197.254  8.8.8.8        ICMP     74 Echo (ping) request  id=0x0001, seq=2/512, ttl=128 (reply in 26)
  26 5.090292  8.8.8.8        10.86.197.254  ICMP     74 Echo (ping) reply    id=0x0001, seq=2/512, ttl=117 (request in 25)
  46 6.069271  10.86.197.254  8.8.8.8        ICMP     74 Echo (ping) request  id=0x0001, seq=3/768, ttl=128 (reply in 48)
  48 6.109882  8.8.8.8        10.86.197.254  ICMP     74 Echo (ping) reply    id=0x0001, seq=3/768, ttl=117 (request in 46)
→ 65 7.085251  10.86.197.254  8.8.8.8        ICMP     74 Echo (ping) request  id=0x0001, seq=4/1024, ttl=128 (reply in 66)
← 66 7.118986  8.8.8.8        10.86.197.254  ICMP     74 Echo (ping) reply    id=0x0001, seq=4/1024, ttl=117 (request in 65)

Frame 66: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{3E13B6DF-A216-42D3-A205-9E8580841FF5}, id 0
Ethernet II, Src: 66:59:6a:4b:ce:71 (66:59:6a:4b:ce:71), Dst: AzureWaveTec_fa:e2:e7 (28:d0:43:fa:e2:e7)
Internet Protocol Version 4, Src: 8.8.8.8, Dst: 10.86.197.254
Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x5557 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 4 (0x0004)
    Sequence Number (LE): 1024 (0x0400)
    [Request frame: 65]
    [Response time: 33.735 ms]
  Data (32 bytes)
```

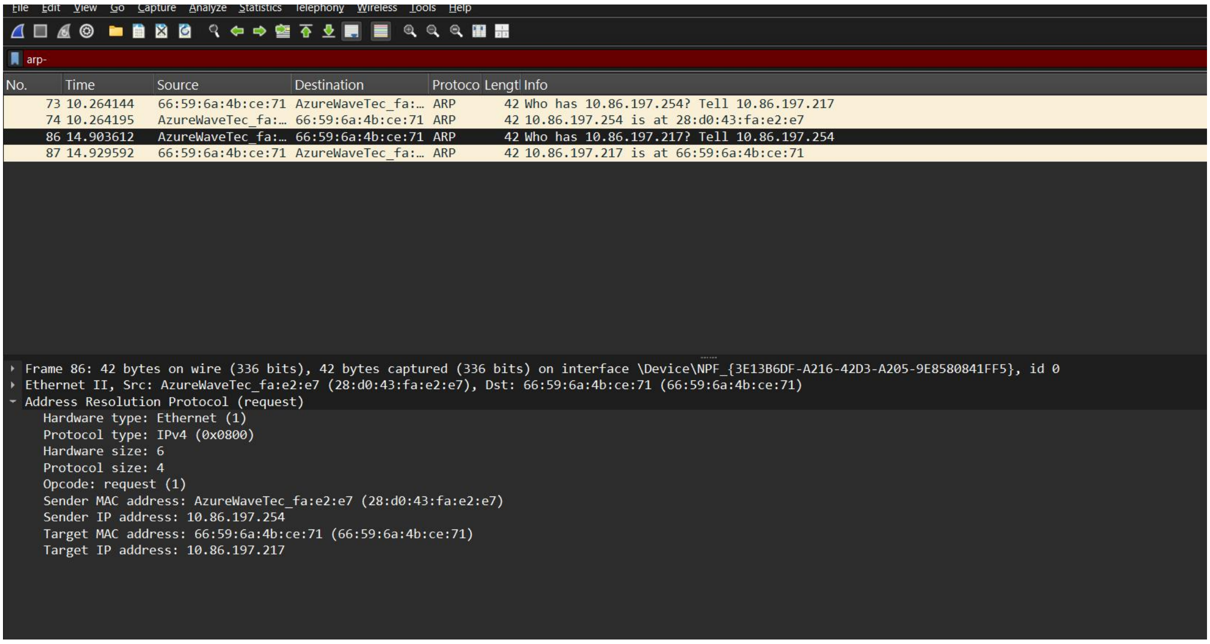


icmp

```
No.     Time      Source           Destination      Protoco Lengtl Info
     23 4.039395  10.86.197.254    8.8.8.8          ICMP      74 Echo (ping) request  id=0x0001, seq=1/256, ttl=128 (reply in 24)
     24 4.090503  8.8.8.8          10.86.197.254    ICMP      74 Echo (ping) reply    id=0x0001, seq=1/256, ttl=117 (request in 23)
     25 5.047606  10.86.197.254    8.8.8.8          ICMP      74 Echo (ping) request  id=0x0001, seq=2/512, ttl=128 (reply in 26)
     26 5.090292  8.8.8.8          10.86.197.254    ICMP      74 Echo (ping) reply    id=0x0001, seq=2/512, ttl=117 (request in 25)
     46 6.069271  10.86.197.254    8.8.8.8          ICMP      74 Echo (ping) request  id=0x0001, seq=3/768, ttl=128 (reply in 48)
     48 6.109882  8.8.8.8          10.86.197.254    ICMP      74 Echo (ping) reply    id=0x0001, seq=3/768, ttl=117 (request in 46)
     65 7.085251  10.86.197.254    8.8.8.8          ICMP      74 Echo (ping) request  id=0x0001, seq=4/1024, ttl=128 (reply in 66)
     66 7.118986  8.8.8.8          10.86.197.254    ICMP      74 Echo (ping) reply    id=0x0001, seq=4/1024, ttl=117 (request in 65)
```

```
Frame 25: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{3E13B6DF-A216-42D3-A205-9E8580841FF5}, id 0
Ethernet II, Src: AzureWaveTec_fa:e2:e7 (28:d0:43:fa:e2:e7), Dst: 66:59:6a:4b:ce:71 (66:59:6a:4b:ce:71)
Internet Protocol Version 4, Src: 10.86.197.254, Dst: 8.8.8.8
Internet Control Message Protocol
  Type: 8 (Echo (ping) request)
  Code: 0
  Checksum: 0x4d59 [correct]
  [Checksum Status: Good]
  Identifier (BE): 1 (0x0001)
  Identifier (LE): 256 (0x0100)
  Sequence Number (BE): 2 (0x0002)
  Sequence Number (LE): 512 (0x0200)
  [Response frame: 26]
  Data (32 bytes)
```

5.ARP Frames


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

arp-

```
No.   Time       Source             Destination        Protoco Lengt Info
   73 10.264144  66:59:6a:4b:ce:71  AzureWaveTec_fa:…  ARP        42 Who has 10.86.197.254? Tell 10.86.197.217
   74 10.264195  AzureWaveTec_fa:…  66:59:6a:4b:ce:71  ARP        42 10.86.197.254 is at 28:d0:43:fa:e2:e7
   86 14.903612  AzureWaveTec_fa:…  66:59:6a:4b:ce:71  ARP        42 Who has 10.86.197.217? Tell 10.86.197.254
   87 14.929592  66:59:6a:4b:ce:71  AzureWaveTec_fa:…  ARP        42 10.86.197.217 is at 66:59:6a:4b:ce:71
```

```
› Frame 86: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{3E13B6DF-A216-42D3-A205-9E8580841FF5}, id 0
› Ethernet II, Src: AzureWaveTec_fa:e2:e7 (28:d0:43:fa:e2:e7), Dst: 66:59:6a:4b:ce:71 (66:59:6a:4b:ce:71)
⌄ Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: AzureWaveTec_fa:e2:e7 (28:d0:43:fa:e2:e7)
    Sender IP address: 10.86.197.254
    Target MAC address: 66:59:6a:4b:ce:71 (66:59:6a:4b:ce:71)
    Target IP address: 10.86.197.217
```