OSI Model, TCP/IP Model & Wireshark Packet Analysis

PART A – OSI Model

1. OSI Layer Explanations

Layer 1 – Physical Layer

The Physical layer handles how raw data moves across a medium, using things like electric signals or light flashes instead of smart processing. It sets rules for wires, plugs, voltage levels, and pin setups - including stuff such as Ethernet cords, fiber lines, or wireless radio waves. Think of it like a highway: just as cars need roads to drive, data needs this layer to go anywhere. There's no routing or labels here - just basic bit transfer from one point to another.

Layer 2 – Data Link Layer

The Data Link layer helps data flow between devices on a single local network. Rather than just passing raw bits, it wraps them into organized frames while handling physical addresses, catching mistakes, or controlling when each device can transmit. Take Ethernet, Wi-Fi (IEEE 802.11), and address lookup - they all work at this stage. Without these rules, many gadgets could talk at once, leading to chaos. Imagine it like a bouncer at an entrance checking IDs before allowing entry.

Layer 3 – Network Layer

The Network layer sends data from one network to another. Instead it picks the most efficient route using IP addresses to guide the way. Devices like routers work right here, handling traffic just like mail centers sorting parcels. Protocols such as IPv4, ICMP, OSPF, and IPv6 run on this level without exception. Think of it like a delivery system planning how packages move between distant places. Unlike Layer 2, which stays inside local zones, Layer 3 links far-off locations together.

Layer 4 – Transport Layer

The Transport layer manages how data moves from one device to another across a network. Instead it takes care of splitting info into chunks, putting them back together, managing speed, and making sure nothing gets lost. On this level you've got TCP and UDP - TCP works like a confirmed delivery with tracking, whereas UDP skips the paperwork for quicker drops. Meanwhile ports such as 21, 53, or 443 are tied right here, helping direct traffic. Think of it like a mail runner who doesn't just drop off a package at the door but makes sure it goes to the exact room using number tags (ports).

Layer 5 – Session Layer

The Session layer handles how connections between apps begin, stay running, or close. Instead it watches conversations already in motion - like signing into an account, chatting on video, or moving files - and makes sure things don't drop or drift out of sync. Tools like remote procedure calls, NetBIOS, or digital session tags work here. Think about making a call: you dial, talk while linked, then stop once someone disconnects.

Layer 6 – Presentation Layer

The Presentation layer shifts data from app format to network form - or back again. It handles tasks such as encrypting info, unscrambling it later, squeezing files down, or turning them into readable code. Things like JPEG images, MP3 audio, PNG graphics, secure connections via SSL/TLS, plus text systems including ASCII and Unicode fit right in this space. Think of someone translating speech so folks who speak differently can actually get what’s being said. What matters here is how information looks - transmission details? Not its job.

Layer 7 – Application Layer

The Application layer lets people work with network tools up close. It handles ways to surf websites, send emails, move files around while chatting online. You’ll find stuff like HTTP, HTTPS, DNS, along with FTP, SMTP, or even DHCP living right here. Think of it like a reception area at an office - folks show up there asking for help. That doesn’t refer to mobile apps, rather the backend functions those programs depend on.

2. OSI Mnemonic

Mnemonic:

“Please Do Not Throw Sausage Pizza Away”

This phrase is a popular and easy way to remember the seven layers of the OSI (Open Systems Interconnection) model from bottom to top. Each word represents the first letter of a layer, helping students quickly recall the correct order.

P – Physical (Layer 1)

This is the lowest layer of the OSI model. The Physical Layer deals with raw data transmission as electrical, optical, or radio signals. It defines cables, connectors, voltage levels, timings, light pulses, and frequencies. Anything related to the physical hardware and actual movement of bits happens here—for example Ethernet cables, Wi-Fi radio waves, fiber optics, and network interface cards (NICs). It does not understand packets or addresses; it only moves bits (0s and 1s).

D – Data Link (Layer 2)

The Data Link Layer ensures that data transferred over the physical medium is error-free, reliable, and properly framed. It organizes bits into frames, manages MAC addresses, and handles error detection using checksums. It also decides who can send data at a time using protocols like CSMA/CD or CSMA/CA. Devices like switches operate at this layer. It is divided into two sublayers: LLC (Logical Link Control) and MAC (Media Access Control).

N – Network (Layer 3)

The Network Layer handles routing and logical addressing, meaning it decides the best path for data to travel across networks. It uses IP addresses to identify devices across different networks and performs packet forwarding, fragmentation, and traffic control. Routers work at this layer. Protocols such as IPv4, IPv6, ICMP, and ARP function here. The focus is on moving packets from source to destination across multiple networks.

T – Transport (Layer 4)

The Transport Layer ensures end-to-end communication between devices. It provides reliable or unreliable data delivery depending on the protocol. TCP ensures reliable communication through error correction, sequencing, acknowledgment, and congestion control. UDP provides faster but connectionless communication for real-time applications like gaming and VoIP. This layer breaks data into segments and ensures that the data arrives completely and correctly.

S – Session (Layer 5)

The Session Layer manages the start, control, and end of communication sessions between devices or applications. It keeps track of connections so that two applications can continue their conversation without interruption.

It also handles session checkpoints, so if a connection fails midway, communication can resume from the last saved point. Examples include online meetings, remote logins, and continuous data exchange.

P – Presentation (Layer 6)

The Presentation Layer acts as the translator of the OSI model. It makes sure the data sent from one application can be understood by another. It handles data formatting, encryption, compression, and conversion into standard formats. This is where tasks like converting text to ASCII or Unicode, encrypting data using SSL/TLS, or compressing files (ZIP, JPEG, MPEG) occur. Essentially, it prepares data for the Application Layer and vice versa.

A – Application (Layer 7)

The Application Layer is the closest to the user. It provides user interfaces and network services directly used by applications such as browsers, email clients, file transfer tools, and messaging apps. It enables activities such as web browsing, sending emails, watching videos, and downloading files. Protocols like HTTP, HTTPS, FTP, SMTP, and DNS operate here. This is where interaction between humans and applications happens.

3. OSI vs TCP/IP Model Comparison

The OSI and TCP/IP models both describe how data moves from a sender to a receiver, but they were created for different purposes. The OSI Model is a **theoretical reference model** with 7 separate layers. It was mainly designed to help people understand the flow of data and to standardize networking concepts. Each layer has a very specific job, and the OSI model separates responsibilities in a very detailed manner. Because of this, it is widely used in education and documentation.

The TCP/IP Model, in contrast, is a **practical model** developed based on the actual protocols used on the internet. It has only 4 layers, because it combines some of the OSI layers into broader, more functional layers. TCP/IP focuses on real-world communication, which is why routers, servers, and the entire internet still depend on it. While OSI is better for learning, TCP/IP is what actually runs modern networks. Both models explain the same process but at different levels of abstraction.

Mapping Table

OSI Layer	**TCP/IP Layer**
Application / Presentation / Session (L7/L6/L5)	Application
Transport (L4)	Transport
Network (L3)	Internet
Data Link / Physical (L2/L1)	Network Access

4. Protocol Data Units (PDUs)

Every layer of the OSI model has a special name for the data it processes. This name represents what kind of information the layer adds to the data. As data moves downward from the Application layer to the Physical layer, each layer adds its own header (and sometimes trailer). As the data moves upward, each layer removes its corresponding header and interprets it.

Layer 4 – Transport

At the Transport layer, the data unit is called a Segment if it is using TCP (because TCP is connection-oriented and breaks data into numbered segments). For UDP, the PDU is called a Datagram because UDP sends data in lightweight, connectionless chunks.

Layer 3 – Network

The PDU here is a Packet. This layer adds logical addressing (IP addresses) and routing information. The network layer's job is to move packets from one network to another.

Layer 2 – Data Link

Here the PDU is called a Frame. This layer adds MAC addresses and prepares data for local delivery within the same network. It also handles error detection via frame checksums.

Layer 1 – Physical

The PDU is simply Bits. These are electrical signals, radio waves, or light pulses that represent binary 1s and 0s.

PDU Table

OSI Layer	**PDU Name**
Layer 4 – Transport	Segment (TCP) / Datagram (UDP)
Layer 3 – Network	Packet
Layer 2 – Data Link	Frame
Layer 1 – Physical	Bits

5. Addressing Concepts

Addressing plays a vital role in how data is delivered across networks. Each type of address works at a different OSI layer and serves a different purpose.

MAC Address – Used at Layer 2 (Data Link Layer)

A MAC address is a unique, fixed, hardware-based address assigned to a device's network interface card (like your Wi-Fi or Ethernet adapter). It is expressed in hexadecimal format (e.g., A4-5E-60-1B-2C-7D). MAC addresses are used only within the local network, meaning your device uses them to communicate with routers, switches, or nearby devices. Layer 2 frames rely on MAC addresses for delivery on a LAN. This type of addressing does not change unless the hardware is replaced.

IP Address – Used at Layer 3 (Network Layer)

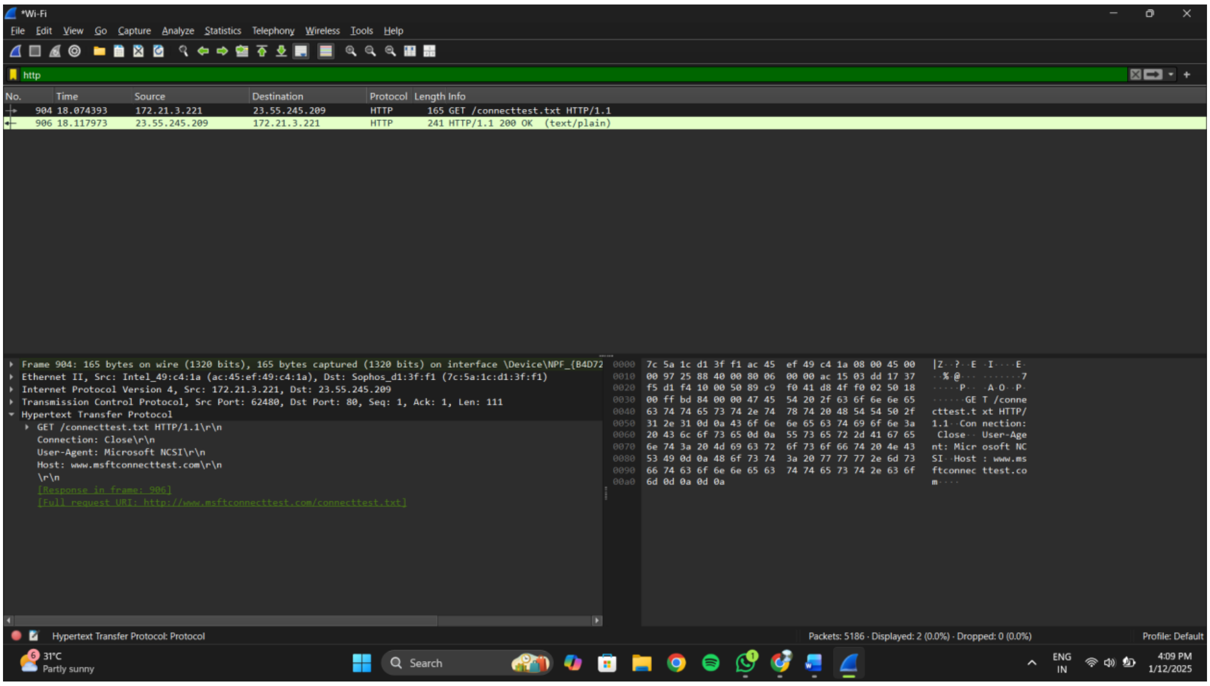
An IP address is a logical, software-assigned address that identifies a device on a global network. Unlike MAC addresses, IP addresses can change when you switch networks, restart devices, or use DHCP. IP addresses help routers make decisions about the best path to reach a destination. For example, your laptop might have 192.168.1.10 on a home network but a completely different IP when connected to campus Wi-Fi. IP addressing allows communication beyond the local network.

Port Number – Used at Layer 4 (Transport Layer)

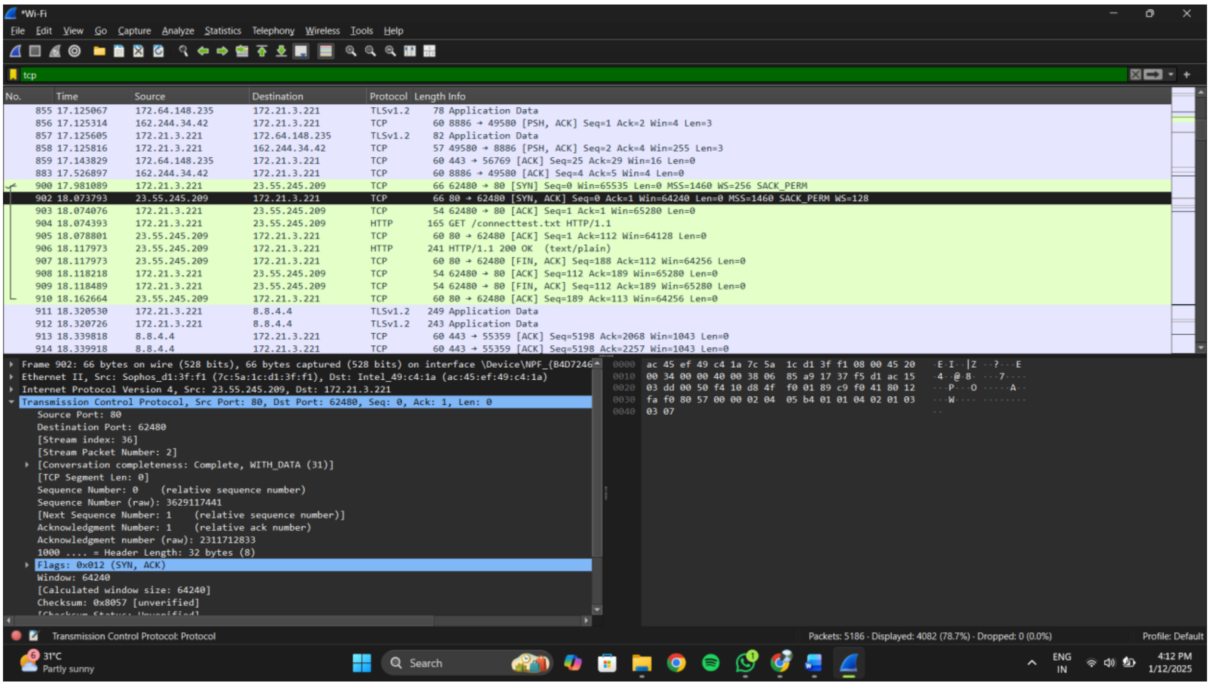
A port number identifies specific applications or services running on a device. While IP addresses identify *where* a device is, port numbers identify *what* service the device wants to access. For example, visiting a website uses TCP port 80 (HTTP) or 443 (HTTPS), while DNS uses UDP port 53. Multiple applications can run on the same device using different ports, allowing many network services to operate simultaneously. Ports, combined with IP addresses, create a socket, such as:
192.168.1.10:443

Part B – Wireshark Practical

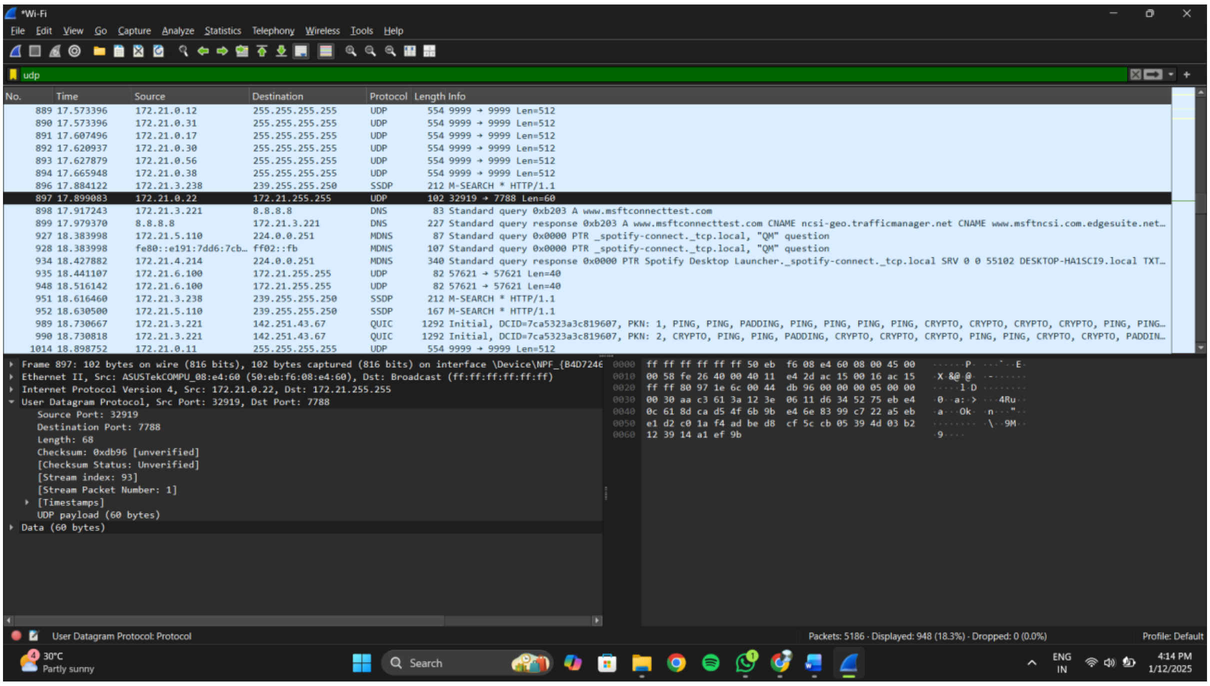
1. HTTP Traffic



2. TCP Packets

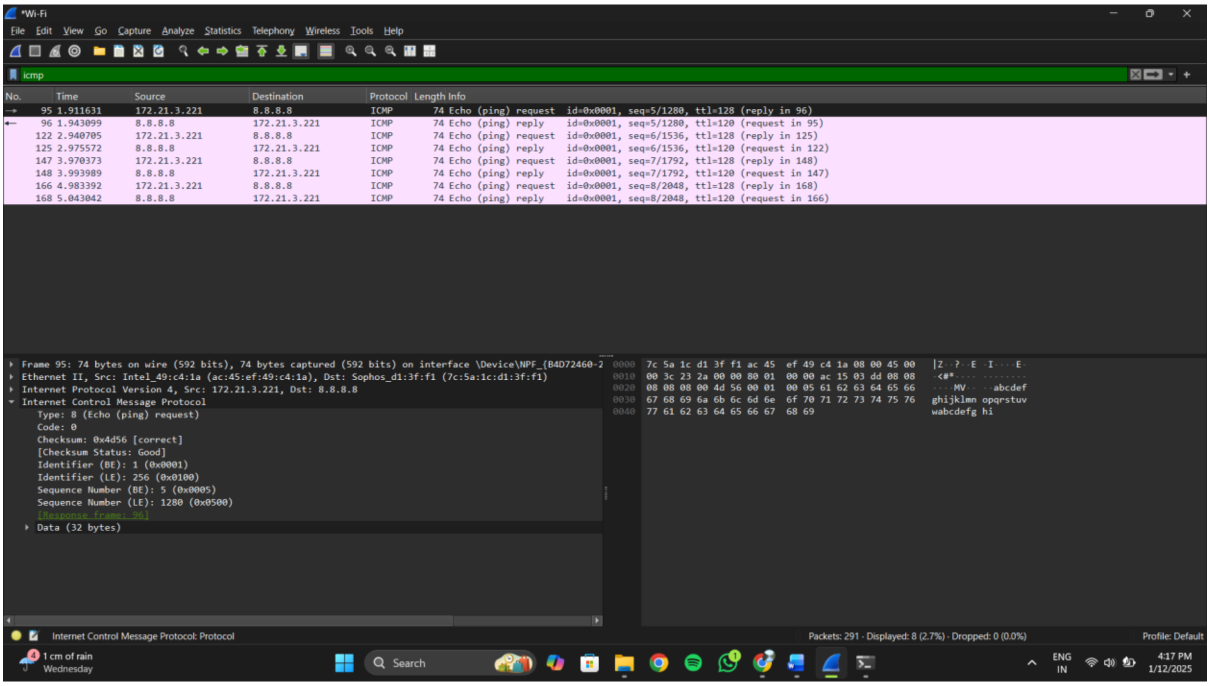


3. UDP Packets

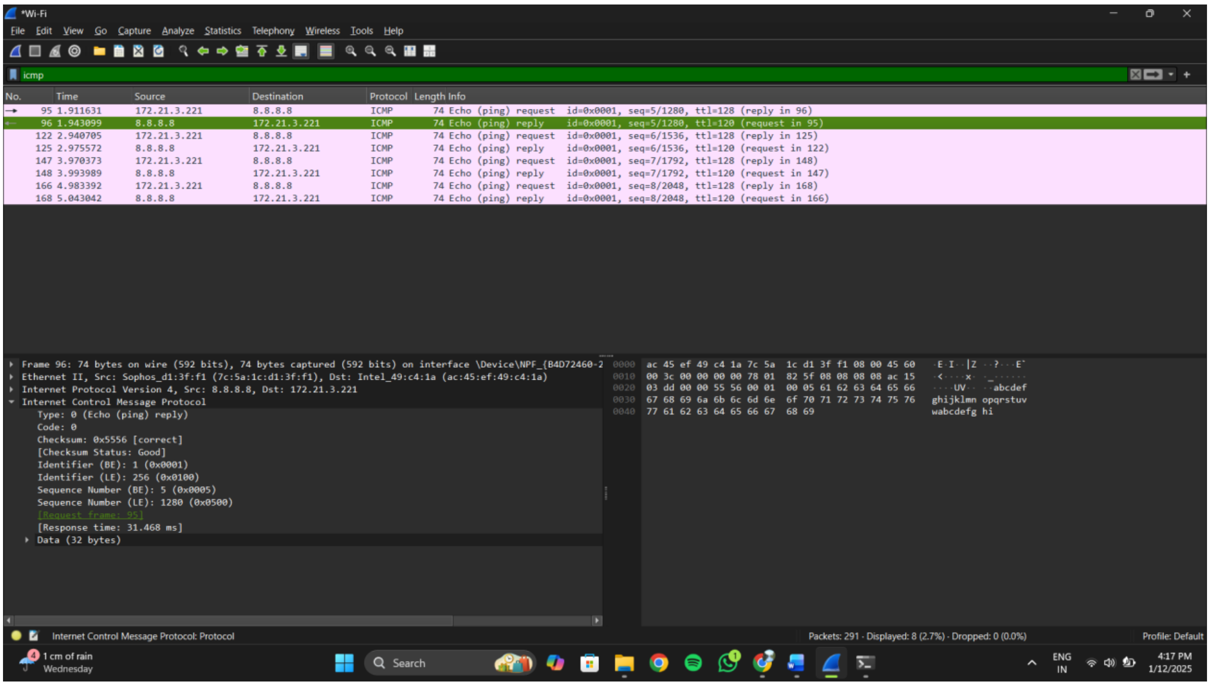


4. ICMP Packets (Ping)

(REQUEST)

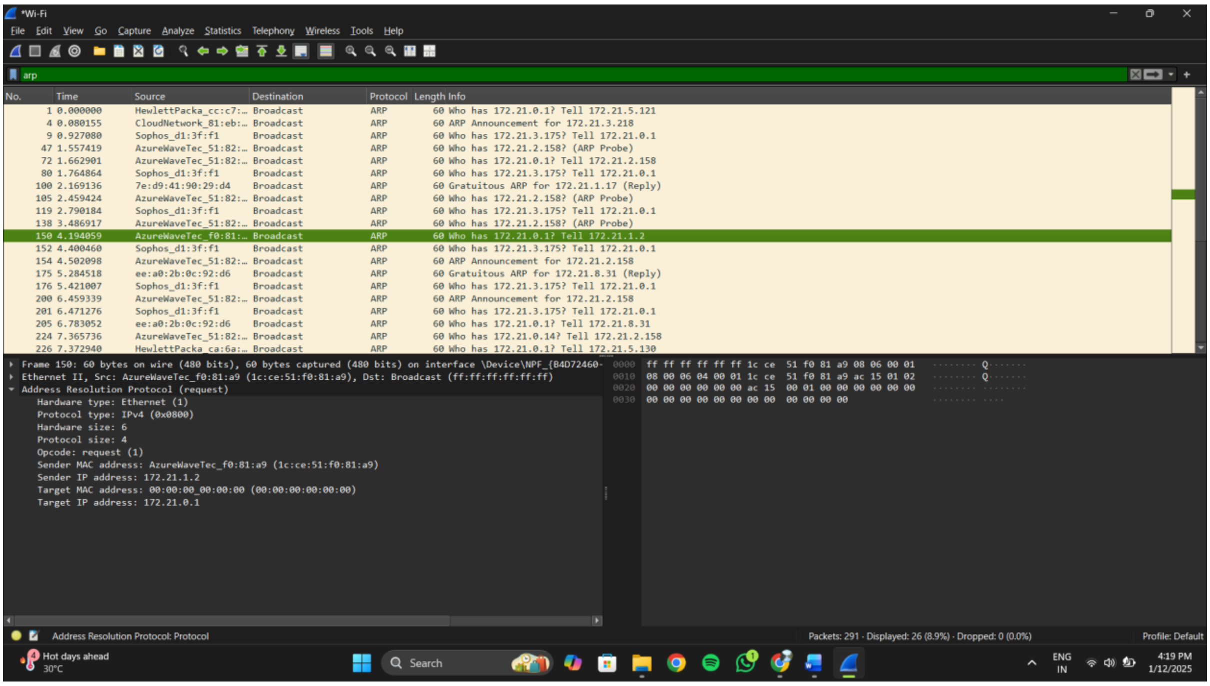


(REPLY)

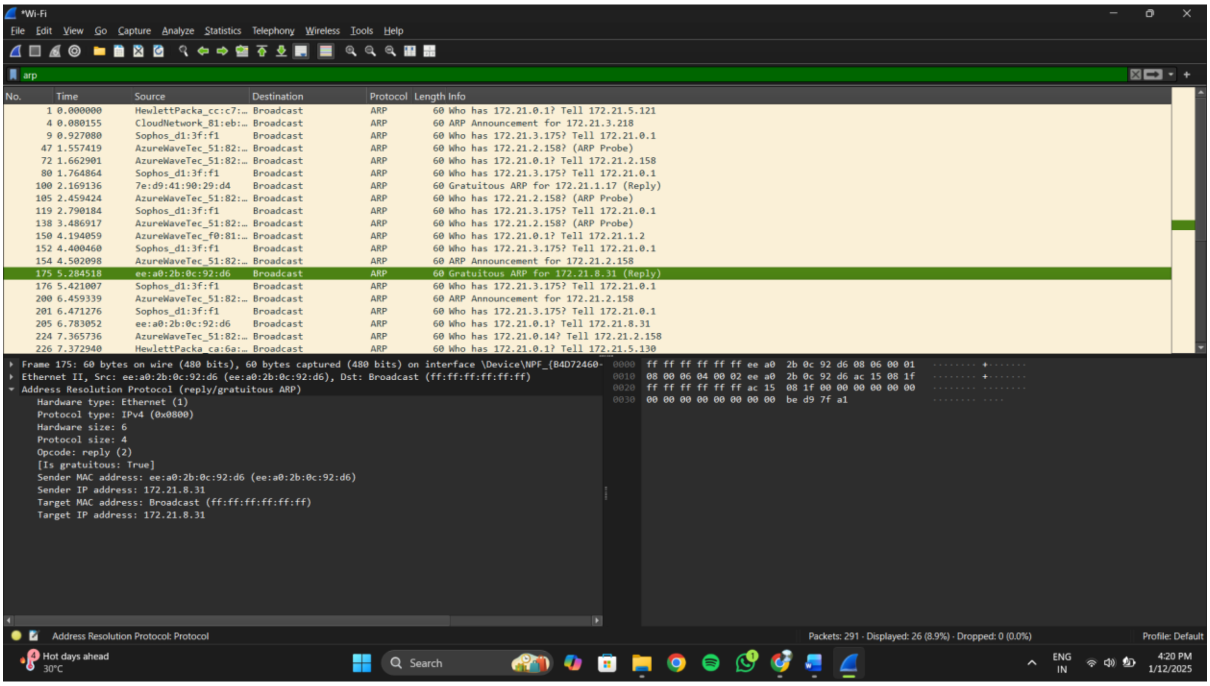


5. ARP Frames

(REQUEST)



(REPLY)


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
arp
No. Time Source Destination Protocol Length Info
1 0.000000 HewlettPacka_cc:c7:… Broadcast ARP 60 Who has 172.21.0.1? Tell 172.21.5.121
4 0.080155 CloudNetwork_81:eb:… Broadcast ARP 60 ARP Announcement for 172.21.3.218
9 0.927080 Sophos_d1:3f:f1 Broadcast ARP 60 Who has 172.21.3.175? Tell 172.21.0.1
47 1.557419 AzureWaveTec_51:82:… Broadcast ARP 60 Who has 172.21.2.158? (ARP Probe)
72 1.662901 AzureWaveTec_51:82:… Broadcast ARP 60 Who has 172.21.0.1? Tell 172.21.2.158
80 1.764864 Sophos_d1:3f:f1 Broadcast ARP 60 Who has 172.21.3.175? Tell 172.21.0.1
100 2.169136 7e:d9:41:90:29:d4 Broadcast ARP 60 Gratuitous ARP for 172.21.1.17 (Reply)
105 2.459424 AzureWaveTec_51:82:… Broadcast ARP 60 Who has 172.21.2.158? (ARP Probe)
119 2.790184 Sophos_d1:3f:f1 Broadcast ARP 60 Who has 172.21.3.175? Tell 172.21.0.1
138 3.486917 AzureWaveTec_51:82:… Broadcast ARP 60 Who has 172.21.2.158? (ARP Probe)
150 4.194059 AzureWaveTec_f0:81:… Broadcast ARP 60 Who has 172.21.0.1? Tell 172.21.1.2
152 4.400460 Sophos_d1:3f:f1 Broadcast ARP 60 Who has 172.21.3.175? Tell 172.21.0.1
154 4.502098 AzureWaveTec_51:82:… Broadcast ARP 60 ARP Announcement for 172.21.2.158
175 5.284518 ee:a0:2b:0c:92:d6 Broadcast ARP 60 Gratuitous ARP for 172.21.8.31 (Reply)
176 5.421007 Sophos_d1:3f:f1 Broadcast ARP 60 Who has 172.21.3.175? Tell 172.21.0.1
200 6.459339 AzureWaveTec_51:82:… Broadcast ARP 60 ARP Announcement for 172.21.2.158
201 6.471276 Sophos_d1:3f:f1 Broadcast ARP 60 Who has 172.21.3.175? Tell 172.21.0.1
205 6.783052 ee:a0:2b:0c:92:d6 Broadcast ARP 60 Who has 172.21.0.1? Tell 172.21.8.31
224 7.365736 AzureWaveTec_51:82:… Broadcast ARP 60 Who has 172.21.0.14? Tell 172.21.2.158
226 7.372940 HewlettPacka_ca:6a:… Broadcast ARP 60 Who has 172.21.0.1? Tell 172.21.5.130
Frame 175: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{B4D72460-
Ethernet II, Src: ee:a0:2b:0c:92:d6 (ee:a0:2b:0c:92:d6), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (reply/gratuitous ARP)
Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: reply (2)
[Is gratuitous: True]
Sender MAC address: ee:a0:2b:0c:92:d6 (ee:a0:2b:0c:92:d6)
Sender IP address: 172.21.8.31
Target MAC address: Broadcast (ff:ff:ff:ff:ff:ff)
Target IP address: 172.21.8.31
0000 ff ff ff ff ff ff ee a0 2b 0c 92 d6 08 06 00 01
0010 08 00 06 04 00 02 ee a0 2b 0c 92 d6 ac 15 08 1f
0020 ff ff ff ff ff ff ac 15 08 1f 00 00 00 00 00 00
0030 00 00 00 00 00 00 00 00 be d9 7f a1
Address Resolution Protocol: Protocol
Packets: 291 · Displayed: 26 (8.9%) · Dropped: 0 (0.0%)
Profile: Default
Hot days ahead
30°C
Search
ENG
IN
4:20 PM
1/12/2025