OSI & Wireshark Lab Assignment Report

Submitted By,

Jacob Tom

24UBC133

II BCA A

Part A – OSI Model Theory

1. OSI Layer Explanations

Layer 1 – Physical

The Physical layer deals with the actual movement of electrical, optical, or radio signals across a medium. It is responsible for cables, connectors, voltage levels, frequencies, and the raw transmission of 0s and 1s. Examples include Ethernet cables, fiber optics, Wi-Fi radio signals, and hubs. A real-world analogy: it is like the road on which vehicles travel—it doesn't matter what the vehicles carry; the job of the road is simply to allow movement.

Layer 2 – Data Link

This layer is responsible for node-to-node communication on the same network segment. It organizes raw bits into frames, attaches MAC addresses, and ensures reliable delivery within the local network. Technologies like Ethernet, Wi-Fi (802.11), ARP, and switches operate here. A real-world analogy: it acts like numbering mailboxes in an apartment building—each frame knows which mailbox (MAC address) it must reach.

Layer 3 – Network

The Network layer handles logical addressing and routing across networks. It decides the best path for packets to travel from source to destination across multiple hops. IP (IPv4/IPv6) and routers operate here. Real-world analogy: it is like a postal system that uses pin codes to route letters across cities and states.

Layer 4 – Transport

The Transport layer ensures end-to-end communication between applications. It manages segmentation, flow control, reliability, and port numbers. TCP provides reliable delivery, while UDP provides faster, connectionless communication. Real-world analogy: a courier service that decides whether to deliver with tracking (TCP) or without tracking (UDP).

Layer 5 – Session

This layer establishes, manages, and terminates communication sessions. It keeps track of ongoing dialogues between systems, such as login sessions or continuous data stream sessions. A real-world analogy: it is like a meeting manager ensuring two parties stay connected during a conversation.

Layer 6 – Presentation

The Presentation layer translates data into a format the receiving application understands. It handles data encryption, compression, and encoding (e.g., SSL/TLS, JPEG, MP3). Real-world analogy: a translator who converts one language to another so both parties can understand.

Layer 7 – Application

This layer interacts directly with end users and applications. It provides services like HTTP, FTP, SMTP, DNS, and interfaces for communication. Real-world analogy: it is like a restaurant menu—users select what they want, and the system handles the details behind the scenes.

2. OSI Mnemonic

Mnemonic:
"Please Do Not Throw Sausage Pizza Away"

This maps as:

Mnemonic Word	OSI Layer
Please	**Physical (L1)**
Do	**Data Link (L2)**
Not	**Network (L3)**
Throw	**Transport (L4)**
Sausage	**Session (L5)**
Pizza	**Presentation (L6)**
Away	**Application (L7)**

3. OSI vs TCP/IP Model Comparison

The OSI Model is a conceptual 7-layer framework that explains how data travels across networks, with each layer having a specific role. The TCP/IP Model is a practical 4-layer model used in real networking today. TCP/IP combines certain OSI layers for simplicity and focuses directly on delivery, transport, and application services. While OSI is mainly theoretical, TCP/IP defines actual protocols used on the Internet.

Mapping Table

OSI Layer(s)	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)

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

MAC Address – Layer 2 (Data Link)

A MAC address is a unique physical hardware identifier assigned to a network interface card. It is used for communication within the same LAN. Switches use MAC addresses to forward frames to the correct device.

IP Address – Layer 3 (Network)

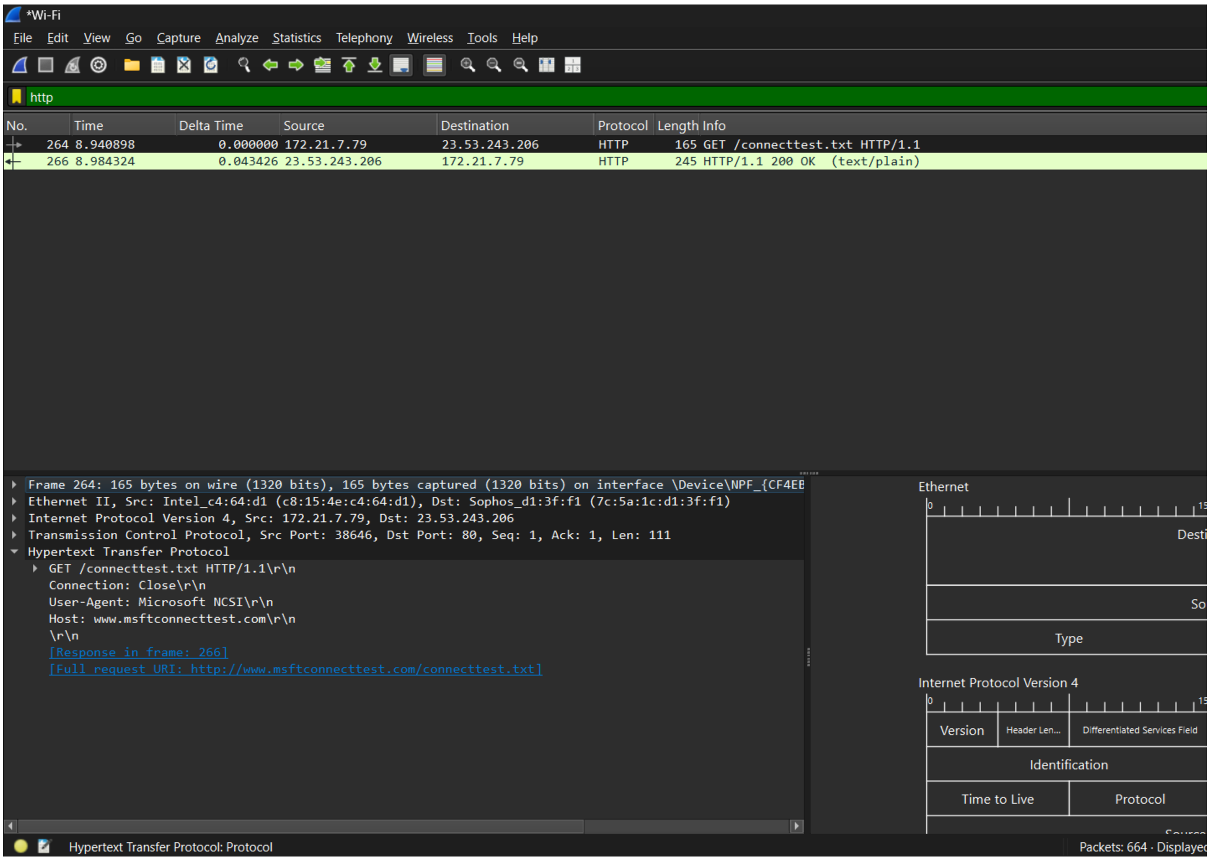
An IP address represents a logical address that identifies a device across networks. Routers use IP addresses to forward packets to the correct network destination.

Port Number – Layer 4 (Transport)

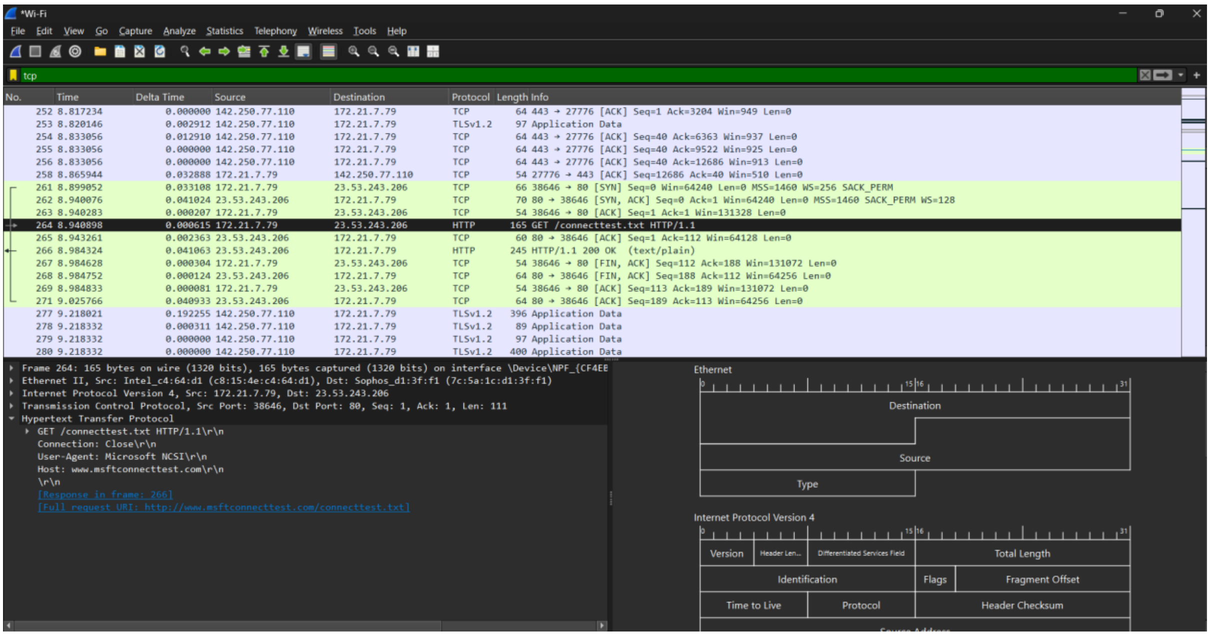
A port number identifies a specific application or service running on a device (e.g., port 80 for HTTP, port 53 for DNS). It ensures that data arriving at a device is delivered to the correct software process.

Part B – Wireshark Practical

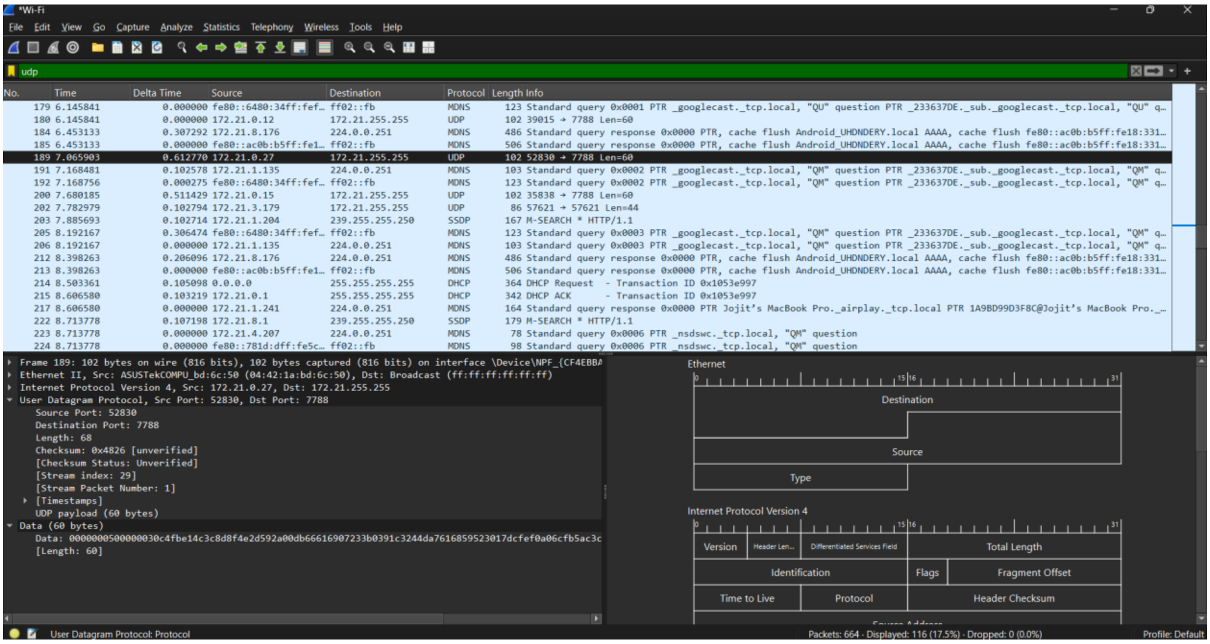
1.HTTP Traffic (TCP + Application Layer)



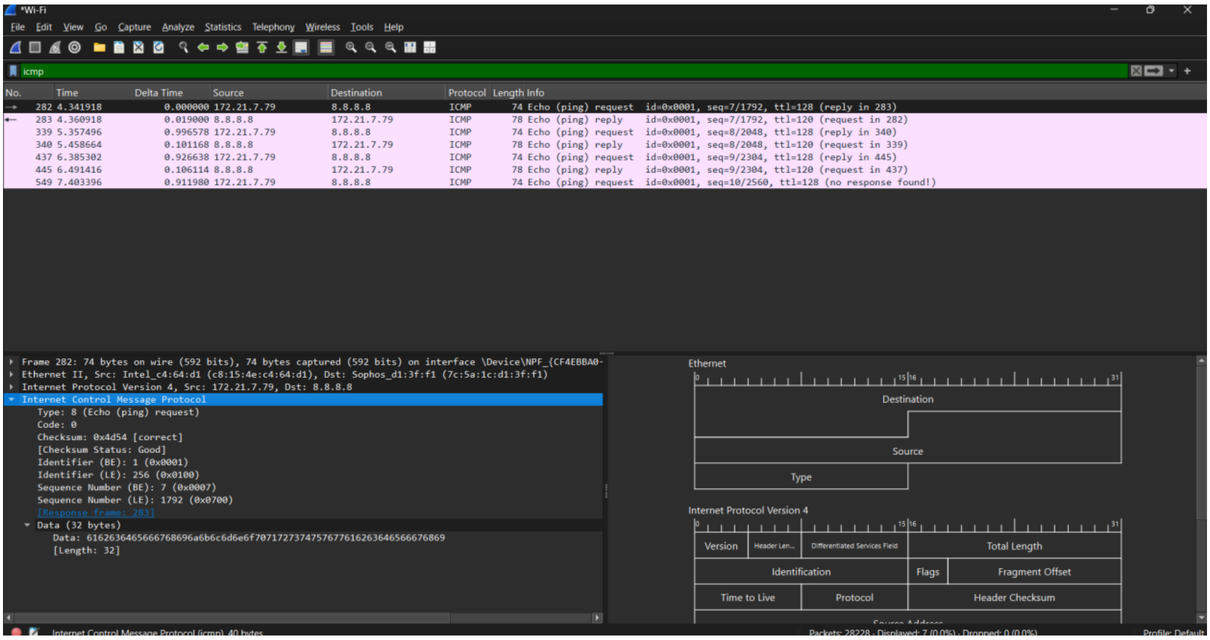
2.TCP Packet Analysis

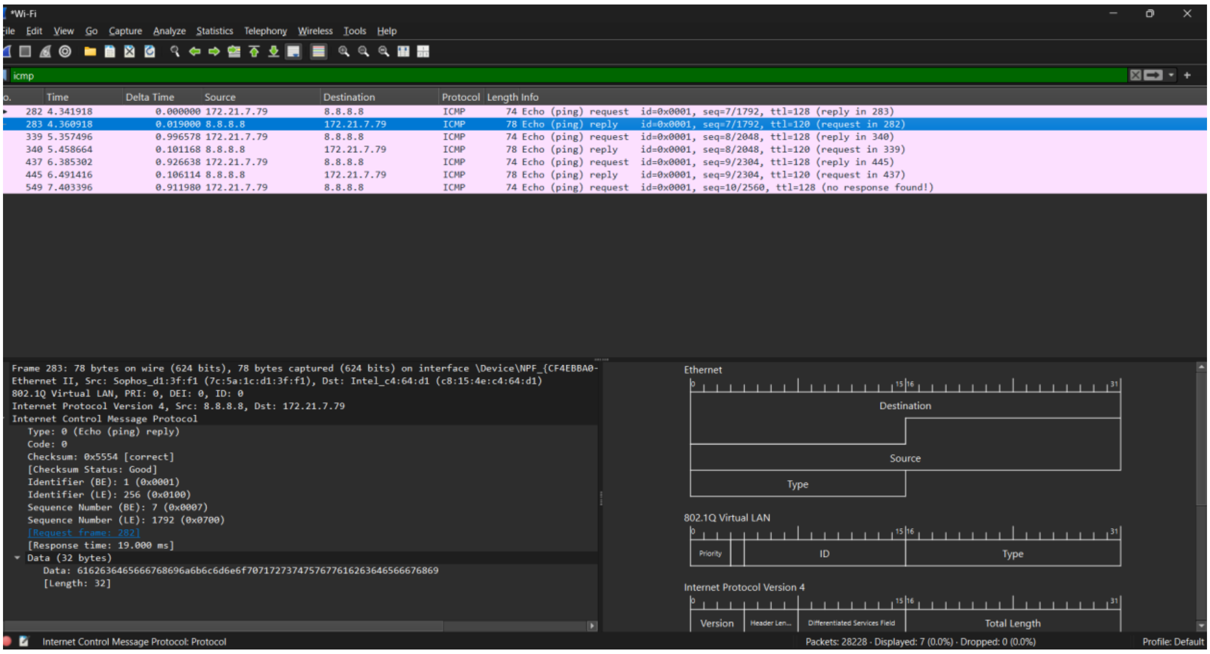


3. UDP Packet Analysis

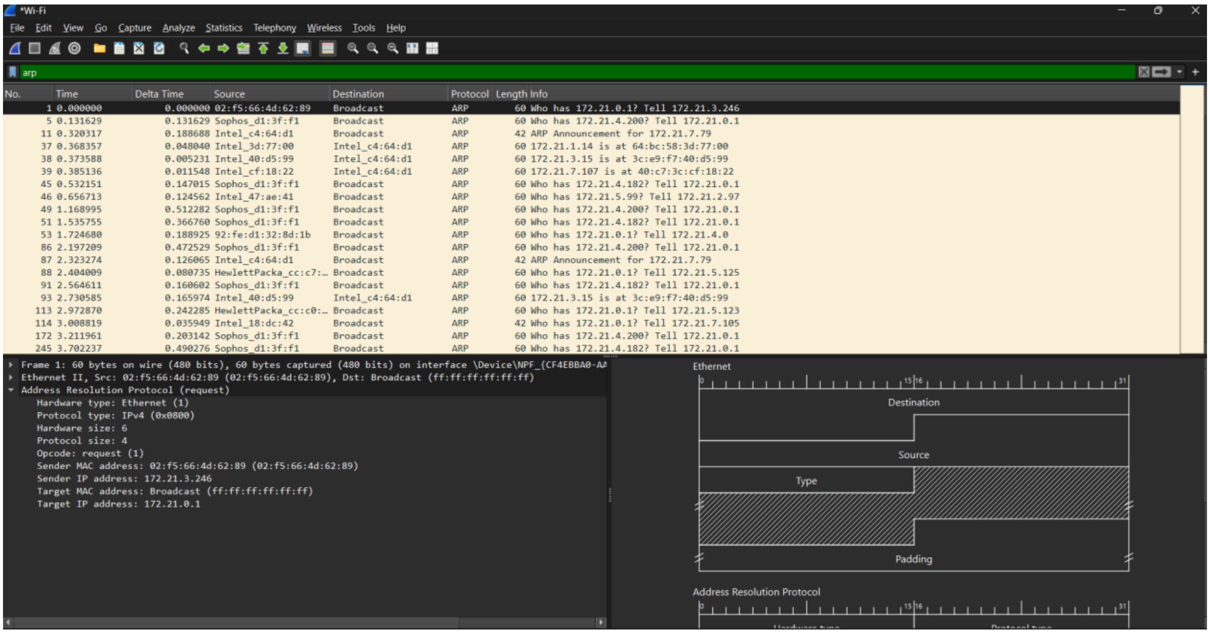

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
udp
No. Time Delta Time Source Destination Protocol Length Info
179 6.145841 0.000000 fe80::6480:34ff:fef… ff02::fb MDNS 123 Standard query 0x0001 PTR _googlecast._tcp.local, "QU" question PTR _233637DE._sub._googlecast._tcp.local, "QU" q…
180 6.145841 0.000000 172.21.0.12 172.21.255.255 UDP 102 39015 → 7788 Len=60
184 6.453133 0.307292 172.21.8.176 224.0.0.251 MDNS 486 Standard query response 0x0000 PTR, cache flush Android_UHDNDERY.local AAAA, cache flush fe80::ac0b:b5ff:fe18:331…
185 6.453133 0.000000 fe80::ac0b:b5ff:fe1… ff02::fb MDNS 506 Standard query response 0x0000 PTR, cache flush Android_UHDNDERY.local AAAA, cache flush fe80::ac0b:b5ff:fe18:331…
189 7.065903 0.612770 172.21.0.27 172.21.255.255 UDP 102 52830 → 7788 Len=60
191 7.168481 0.102578 172.21.1.135 224.0.0.251 MDNS 103 Standard query 0x0002 PTR _googlecast._tcp.local, "QM" question PTR _233637DE._sub._googlecast._tcp.local, "QM" q…
192 7.168756 0.000275 fe80::6480:34ff:fef… ff02::fb MDNS 123 Standard query 0x0002 PTR _googlecast._tcp.local, "QM" question PTR _233637DE._sub._googlecast._tcp.local, "QM" q…
200 7.680185 0.511429 172.21.0.15 172.21.255.255 UDP 102 35838 → 7788 Len=60
202 7.782979 0.102794 172.21.3.179 172.21.255.255 UDP 86 57621 → 57621 Len=44
203 7.885693 0.102714 172.21.1.204 239.255.255.250 SSDP 167 M-SEARCH * HTTP/1.1
205 8.192167 0.306474 fe80::6480:34ff:fef… ff02::fb MDNS 123 Standard query 0x0003 PTR _googlecast._tcp.local, "QM" question PTR _233637DE._sub._googlecast._tcp.local, "QM" q…
206 8.192167 0.000000 172.21.1.135 224.0.0.251 MDNS 103 Standard query 0x0003 PTR _googlecast._tcp.local, "QM" question PTR _233637DE._sub._googlecast._tcp.local, "QM" q…
212 8.398263 0.206096 172.21.8.176 224.0.0.251 MDNS 486 Standard query response 0x0000 PTR, cache flush Android_UHDNDERY.local AAAA, cache flush fe80::ac0b:b5ff:fe18:331…
213 8.398263 0.000000 fe80::ac0b:b5ff:fe1… ff02::fb MDNS 506 Standard query response 0x0000 PTR, cache flush Android_UHDNDERY.local AAAA, cache flush fe80::ac0b:b5ff:fe18:331…
214 8.503361 0.105098 0.0.0.0 255.255.255.255 DHCP 364 DHCP Request - Transaction ID 0x1053e997
215 8.606580 0.103219 172.21.0.1 255.255.255.255 DHCP 342 DHCP ACK - Transaction ID 0x1053e997
217 8.606580 0.000000 172.21.1.241 224.0.0.251 MDNS 164 Standard query response 0x0000 PTR Jojit's MacBook Pro._airplay._tcp.local PTR 1A9BD99D3F8C@Jojit's MacBook Pro._…
222 8.713778 0.107198 172.21.8.1 239.255.255.250 SSDP 179 M-SEARCH * HTTP/1.1
223 8.713778 0.000000 172.21.4.207 224.0.0.251 MDNS 78 Standard query 0x0006 PTR _nsdswc._tcp.local, "QM" question
224 8.713778 0.000000 fe80::781d:dff:fe5c… ff02::fb MDNS 98 Standard query 0x0006 PTR _nsdswc._tcp.local, "QM" question
Frame 189: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface \Device\NPF_{CF4EBBA
Ethernet II, Src: ASUSTekCOMPU_bd:6c:50 (04:42:1a:bd:6c:50), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 172.21.0.27, Dst: 172.21.255.255
User Datagram Protocol, Src Port: 52830, Dst Port: 7788
Source Port: 52830
Destination Port: 7788
Length: 68
Checksum: 0x4826 [unverified]
[Checksum Status: Unverified]
[Stream index: 29]
[Stream Packet Number: 1]
[Timestamps]
UDP payload (60 bytes)
Data (60 bytes)
Data: 0000000500000030c4fbe14c3c8d8f4e2d592a00db66616907233b0391c3244da7616859523017dcfef0a06cfb5ac3c
[Length: 60]
Ethernet
Destination
Source
Type
Internet Protocol Version 4
Version
Header Len…
Differentiated Services Field
Total Length
Identification
Flags
Fragment Offset
Time to Live
Protocol
Header Checksum
User Datagram Protocol: Protocol
Packets: 664 · Displayed: 116 (17.5%) · Dropped: 0 (0.0%)
Profile: Default

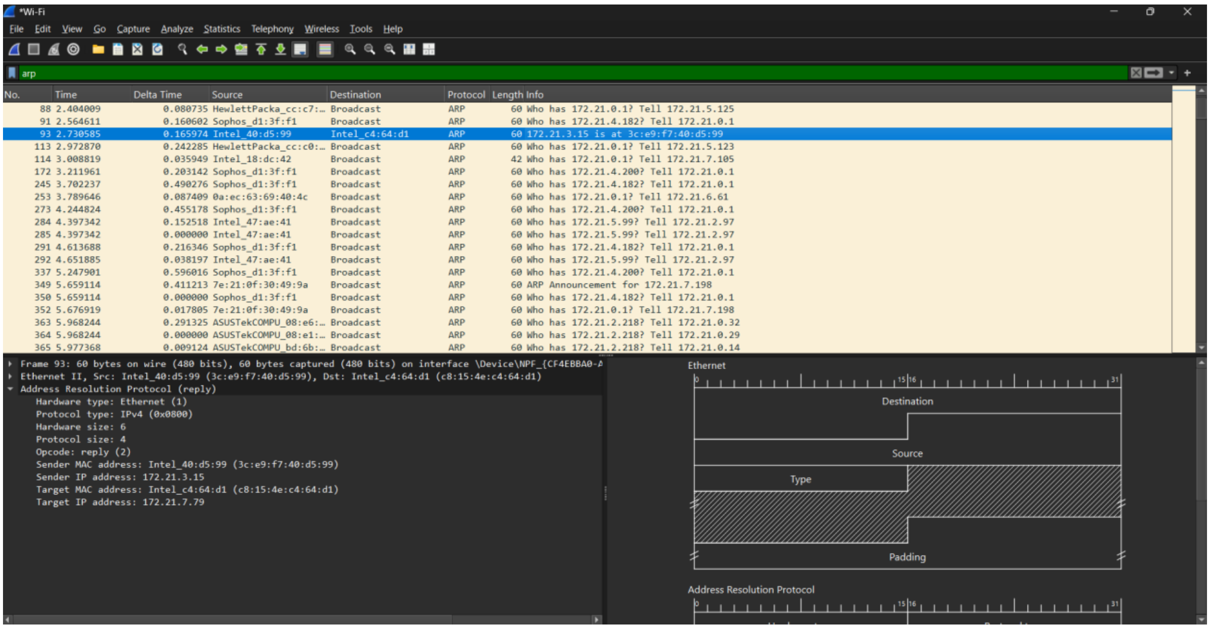
4. ICMP (Ping)


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
No. Time Delta Time Source Destination Protocol Length Info
282 4.341918 0.000000 172.21.7.79 8.8.8.8 ICMP 74 Echo (ping) request id=0x0001, seq=7/1792, ttl=128 (reply in 283)
283 4.360918 0.019000 8.8.8.8 172.21.7.79 ICMP 78 Echo (ping) reply id=0x0001, seq=7/1792, ttl=120 (request in 282)
339 5.357496 0.996578 172.21.7.79 8.8.8.8 ICMP 74 Echo (ping) request id=0x0001, seq=8/2048, ttl=128 (reply in 340)
340 5.458664 0.101168 8.8.8.8 172.21.7.79 ICMP 78 Echo (ping) reply id=0x0001, seq=8/2048, ttl=120 (request in 339)
437 6.385302 0.926638 172.21.7.79 8.8.8.8 ICMP 74 Echo (ping) request id=0x0001, seq=9/2304, ttl=128 (reply in 445)
445 6.491416 0.106114 8.8.8.8 172.21.7.79 ICMP 78 Echo (ping) reply id=0x0001, seq=9/2304, ttl=120 (request in 437)
549 7.403396 0.911980 172.21.7.79 8.8.8.8 ICMP 74 Echo (ping) request id=0x0001, seq=10/2560, ttl=128 (no response found!)
Frame 282: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{CF4EBBA0-
Ethernet II, Src: Intel_c4:64:d1 (c8:15:4e:c4:64:d1), Dst: Sophos_d1:3f:f1 (7c:5a:1c:d1:3f:f1)
Internet Protocol Version 4, Src: 172.21.7.79, Dst: 8.8.8.8
Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0x4d54 [correct]
[Checksum Status: Good]
Identifier (BE): 1 (0x0001)
Identifier (LE): 256 (0x0100)
Sequence Number (BE): 7 (0x0007)
Sequence Number (LE): 1792 (0x0700)
[Response frame: 283]
Data (32 bytes)
Data: 6162636465666768696a6b6c6d6e6f7071727374757677616263646566676869
[Length: 32]
Ethernet
Destination
Source
Type
Internet Protocol Version 4
Version
Header Len…
Differentiated Services Field
Total Length
Identification
Flags
Fragment Offset
Time to Live
Protocol
Header Checksum
Internet Control Message Protocol (icmp), 40 bytes
Packets: 28228 · Displayed: 7 (0.0%) · Dropped: 0 (0.0%)
Profile: Default


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
No. Time Delta Time Source Destination Protocol Length Info
282 4.341918 0.000000 172.21.7.79 8.8.8.8 ICMP 74 Echo (ping) request id=0x0001, seq=7/1792, ttl=128 (reply in 283)
283 4.360918 0.019000 8.8.8.8 172.21.7.79 ICMP 78 Echo (ping) reply id=0x0001, seq=7/1792, ttl=120 (request in 282)
339 5.357496 0.996578 172.21.7.79 8.8.8.8 ICMP 74 Echo (ping) request id=0x0001, seq=8/2048, ttl=128 (reply in 340)
340 5.458664 0.101168 8.8.8.8 172.21.7.79 ICMP 78 Echo (ping) reply id=0x0001, seq=8/2048, ttl=120 (request in 339)
437 6.385302 0.926638 172.21.7.79 8.8.8.8 ICMP 74 Echo (ping) request id=0x0001, seq=9/2304, ttl=128 (reply in 445)
445 6.491416 0.106114 8.8.8.8 172.21.7.79 ICMP 78 Echo (ping) reply id=0x0001, seq=9/2304, ttl=120 (request in 437)
549 7.403396 0.911980 172.21.7.79 8.8.8.8 ICMP 74 Echo (ping) request id=0x0001, seq=10/2560, ttl=128 (no response found!)
Frame 283: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface \Device\NPF_{CF4EBBA0-
Ethernet II, Src: Sophos_d1:3f:f1 (7c:5a:1c:d1:3f:f1), Dst: Intel_c4:64:d1 (c8:15:4e:c4:64:d1)
802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 0
Internet Protocol Version 4, Src: 8.8.8.8, Dst: 172.21.7.79
Internet Control Message Protocol
Type: 0 (Echo (ping) reply)
Code: 0
Checksum: 0x5554 [correct]
[Checksum Status: Good]
Identifier (BE): 1 (0x0001)
Identifier (LE): 256 (0x0100)
Sequence Number (BE): 7 (0x0007)
Sequence Number (LE): 1792 (0x0700)
[Request frame: 282]
[Response time: 19.000 ms]
Data (32 bytes)
Data: 6162636465666768696a6b6c6d6e6f7071727374757677616263646566676869
[Length: 32]
Ethernet
Destination
Source
Type
802.1Q Virtual LAN
Priority
ID
Type
Internet Protocol Version 4
Version
Differentiated Services Field
Total Length
Internet Control Message Protocol: Protocol
Packets: 28228 · Displayed: 7 (0.0%) · Dropped: 0 (0.0%)
Profile: Default

5. ARP Frames


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
arp
No. Time Delta Time Source Destination Protocol Length Info
1 0.000000 0.000000 02:f5:66:4d:62:89 Broadcast ARP 60 Who has 172.21.0.1? Tell 172.21.3.246
5 0.131629 0.131629 Sophos_d1:3f:f1 Broadcast ARP 60 Who has 172.21.4.200? Tell 172.21.0.1
11 0.320317 0.188688 Intel_c4:64:d1 Broadcast ARP 42 ARP Announcement for 172.21.7.79
37 0.368357 0.048040 Intel_3d:77:00 Intel_c4:64:d1 ARP 60 172.21.1.14 is at 64:bc:58:3d:77:00
38 0.373588 0.005231 Intel_40:d5:99 Intel_c4:64:d1 ARP 60 172.21.3.15 is at 3c:e9:f7:40:d5:99
39 0.385136 0.011548 Intel_cf:18:22 Intel_c4:64:d1 ARP 60 172.21.7.107 is at 40:c7:3c:cf:18:22
45 0.532151 0.147015 Sophos_d1:3f:f1 Broadcast ARP 60 Who has 172.21.4.182? Tell 172.21.0.1
46 0.656713 0.124562 Intel_47:ae:41 Broadcast ARP 60 Who has 172.21.5.99? Tell 172.21.2.97
49 1.168995 0.512282 Sophos_d1:3f:f1 Broadcast ARP 60 Who has 172.21.4.200? Tell 172.21.0.1
51 1.535755 0.366760 Sophos_d1:3f:f1 Broadcast ARP 60 Who has 172.21.4.182? Tell 172.21.0.1
53 1.724680 0.188925 92:fe:d1:32:8d:1b Broadcast ARP 60 Who has 172.21.0.1? Tell 172.21.4.0
86 2.197209 0.472529 Sophos_d1:3f:f1 Broadcast ARP 60 Who has 172.21.4.200? Tell 172.21.0.1
87 2.323274 0.126065 Intel_c4:64:d1 Broadcast ARP 42 ARP Announcement for 172.21.7.79
88 2.404009 0.080735 HewlettPacka_cc:c7:… Broadcast ARP 60 Who has 172.21.0.1? Tell 172.21.5.125
91 2.564611 0.160602 Sophos_d1:3f:f1 Broadcast ARP 60 Who has 172.21.4.182? Tell 172.21.0.1
93 2.730585 0.165974 Intel_40:d5:99 Intel_c4:64:d1 ARP 60 172.21.3.15 is at 3c:e9:f7:40:d5:99
113 2.972870 0.242285 HewlettPacka_cc:c0:… Broadcast ARP 60 Who has 172.21.0.1? Tell 172.21.5.123
114 3.008819 0.035949 Intel_18:dc:42 Broadcast ARP 42 Who has 172.21.0.1? Tell 172.21.7.105
172 3.211961 0.203142 Sophos_d1:3f:f1 Broadcast ARP 60 Who has 172.21.4.200? Tell 172.21.0.1
245 3.702237 0.490276 Sophos_d1:3f:f1 Broadcast ARP 60 Who has 172.21.4.182? Tell 172.21.0.1
Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{CF4EBBA0-A
Ethernet II, Src: 02:f5:66:4d:62:89 (02:f5:66:4d:62:89), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)
Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: request (1)
Sender MAC address: 02:f5:66:4d:62:89 (02:f5:66:4d:62:89)
Sender IP address: 172.21.3.246
Target MAC address: Broadcast (ff:ff:ff:ff:ff:ff)
Target IP address: 172.21.0.1
Ethernet
Destination
Source
Type
Padding
Address Resolution Protocol



Part C – Conclusion

What I Learned from This Activity

Through this assignment, I gained a detailed understanding of how the OSI and TCP/IP models structure network communication. I learned how PDUs change across layers and how MAC, IP, and port numbers play different roles in delivering data. Using Wireshark helped me visualize actual packet structures and understand how protocols like HTTP, TCP, UDP, ICMP, and ARP work in real time. This activity improved both my theoretical knowledge and practical skills in network analysis.