Batch: A1	**Roll No.: 16010123012**
Experiment / assignment / tutorial No. 10	
Grade: AA / AB / BB / BC / CC / CD /DD	
Signature of the Staff In-charge with date	

Experiment No.:10

TITLE: Study of Packet Analyzer tool: Wireshark

AIM: To study and analyse various Protocols using Packet Analyzer tool: Wireshark

Expected Outcome of Experiment:

Books/ Journals/ Websites referred:

1. A. S. Tanenbaum, "Computer Networks", Pearson Education, Fourth Edition
2. B. A. Forouzan, "Data Communications and Networking", TMH, Fourth Edition

Pre Lab/ Prior Concepts:

IPv4 Addressing, Subnetting, Link State Protocol, Router configuration Commands

New Concepts to be learned: Packet Analyzer tool: Wireshark.

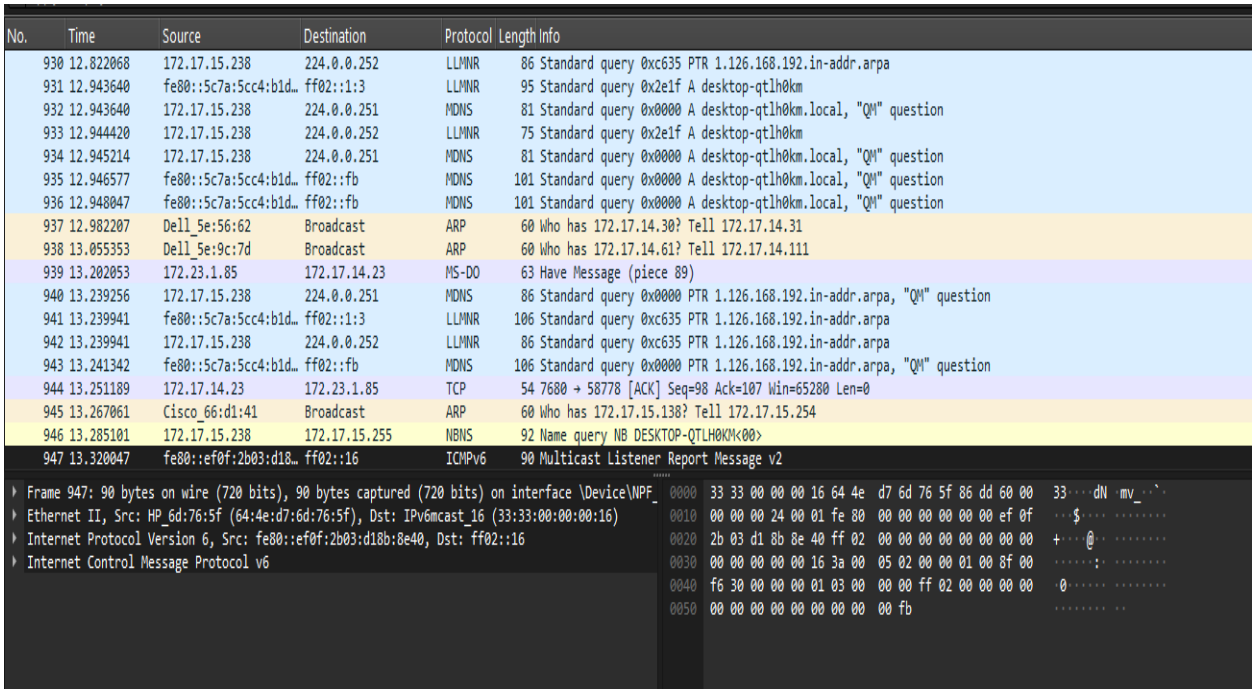
THEORY:

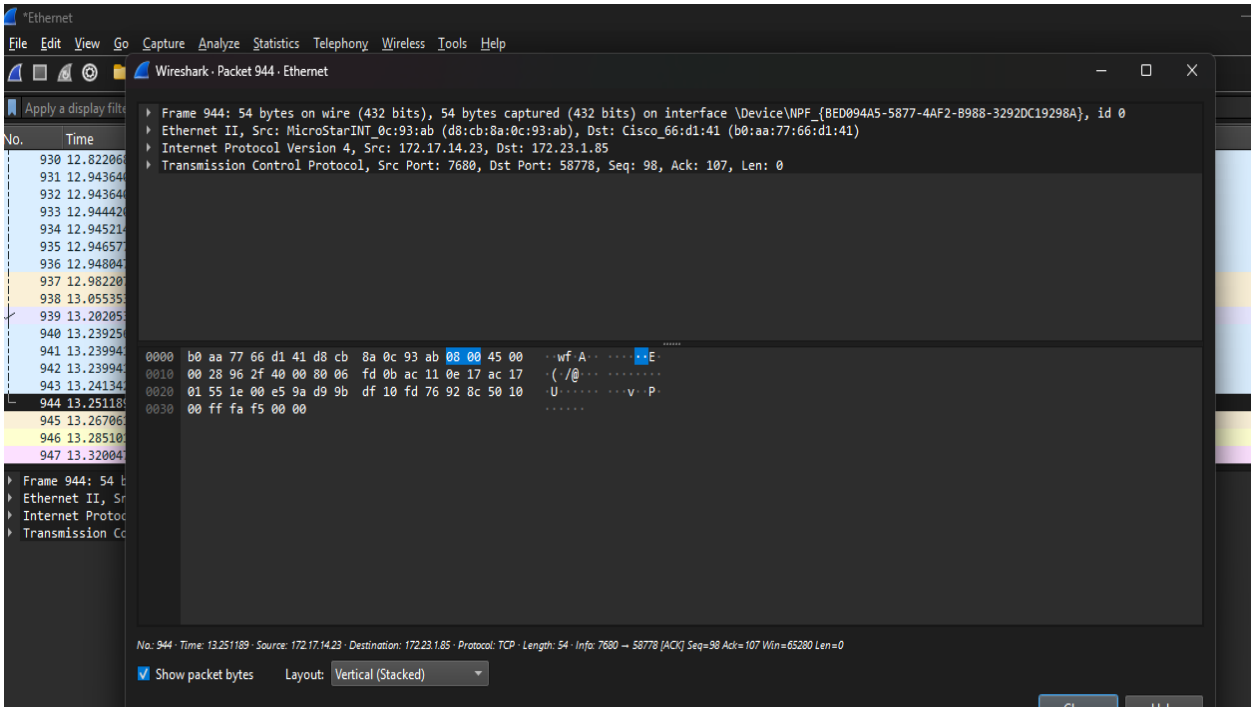
Wireshark is an open-source packet analyser, which is used for education, analysis, software development, communication protocol development, and network troubleshooting. It is used to track the packets so that each one is filtered to meet our specific needs. It is commonly called a sniffer, network protocol analyser, and network analyser. It is also used by network security engineers to examine security problems. Wireshark is a free to use application which is used to apprehend the data back and forth. It is often called a free packet sniffer computer application. It puts the network card into an unselective mode, i.e., to accept all the packets which it receives

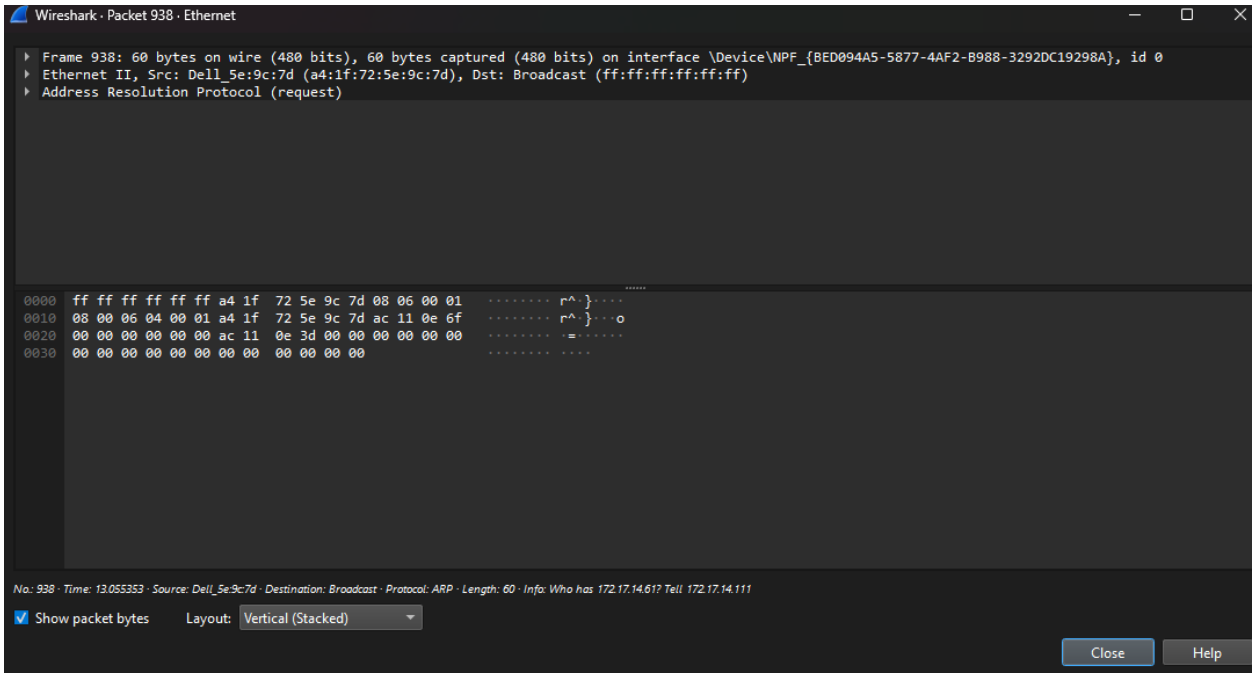
Uses of Wireshark

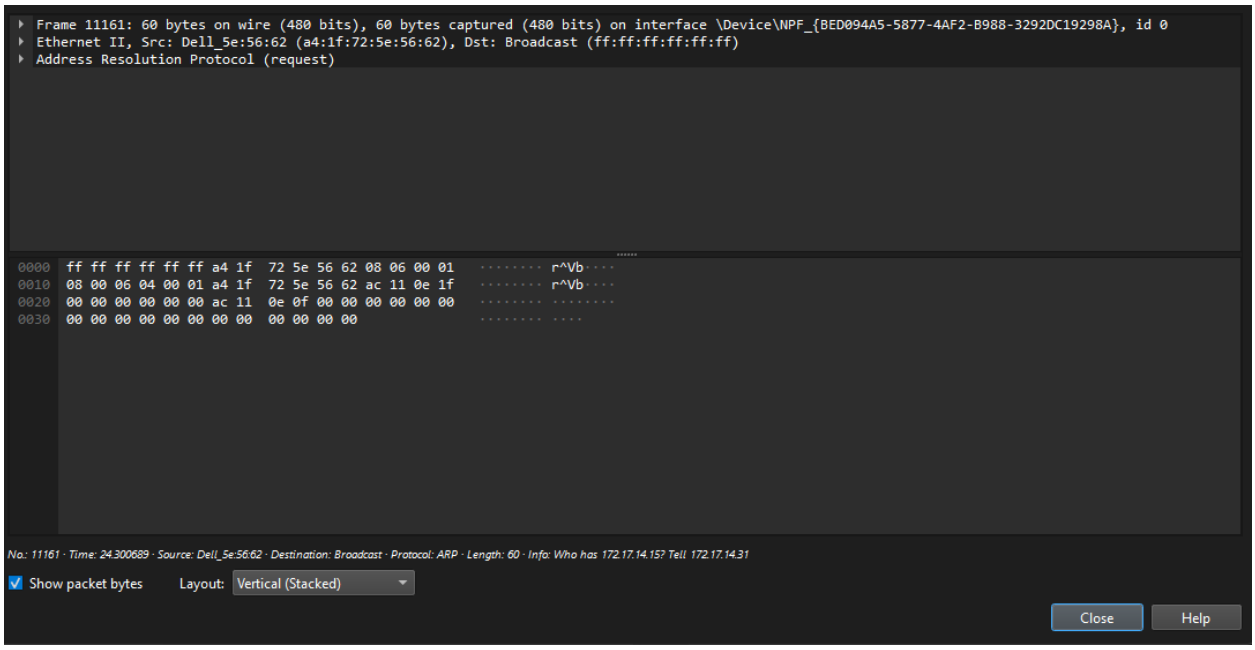
1. It is used by network security engineers to examine security problems.
2. It allows the users to watch all the traffic being passed over the network.
3. It is used by network engineers to troubleshoot network issues.
4. It also helps to troubleshoot latency issues and malicious activities on your network.
5. It can also analyze dropped packets.

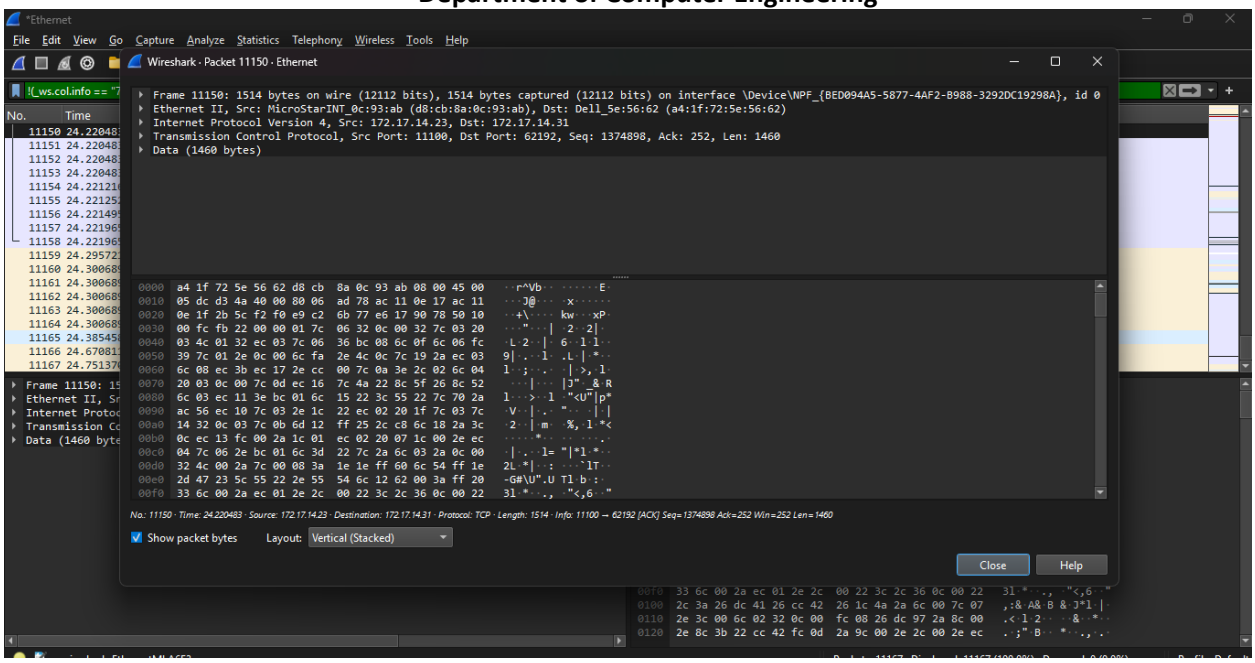
IMPLEMENTATION:



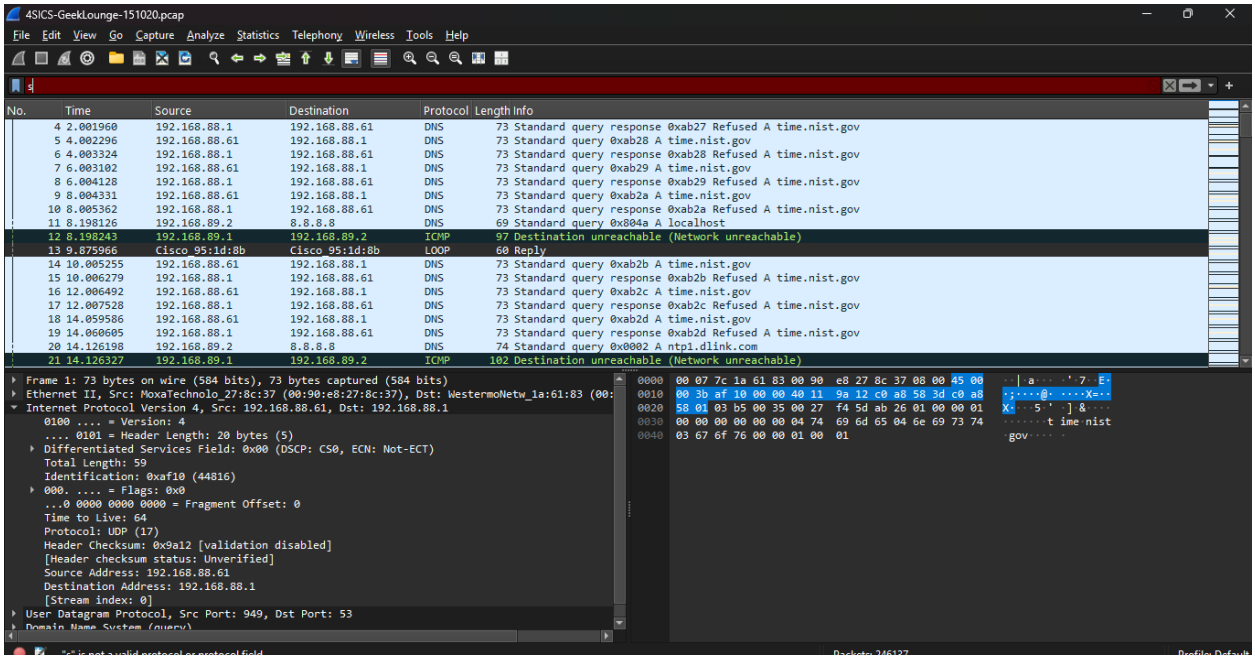


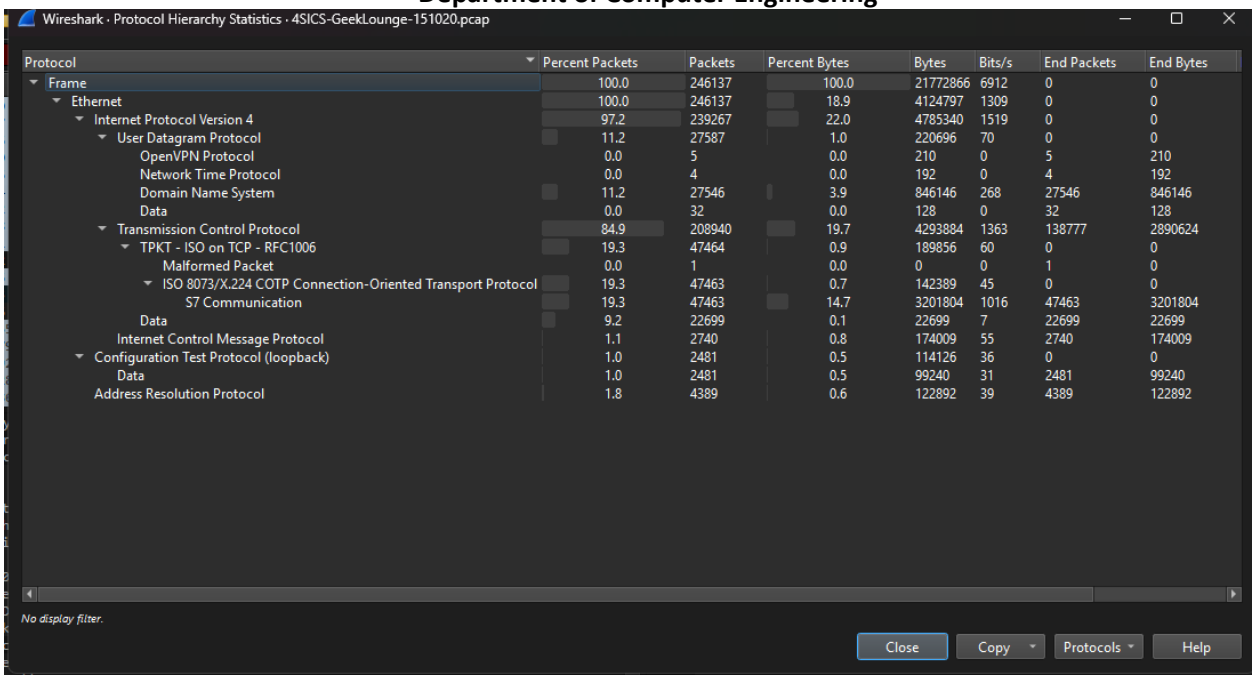

Wireshark · Packet 938 · Ethernet
Frame 938: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{BED094A5-5877-4AF2-B988-3292DC19298A}, id 0
Ethernet II, Src: Dell_5e:9c:7d (a4:1f:72:5e:9c:7d), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)
0000 ff ff ff ff ff ff a4 1f 72 5e 9c 7d 08 06 00 01
0010 08 00 06 04 00 01 a4 1f 72 5e 9c 7d ac 11 0e 6f
0020 00 00 00 00 00 00 ac 11 0e 3d 00 00 00 00 00 00
0030 00 00 00 00 00 00 00 00 00 00 00 00
No.: 938 · Time: 13.055353 · Source: Dell_5e:9c:7d · Destination: Broadcast · Protocol: ARP · Length: 60 · Info: Who has 172.17.14.61? Tell 172.17.14.111
Show packet bytes
Layout: Vertical (Stacked)
Close
Help

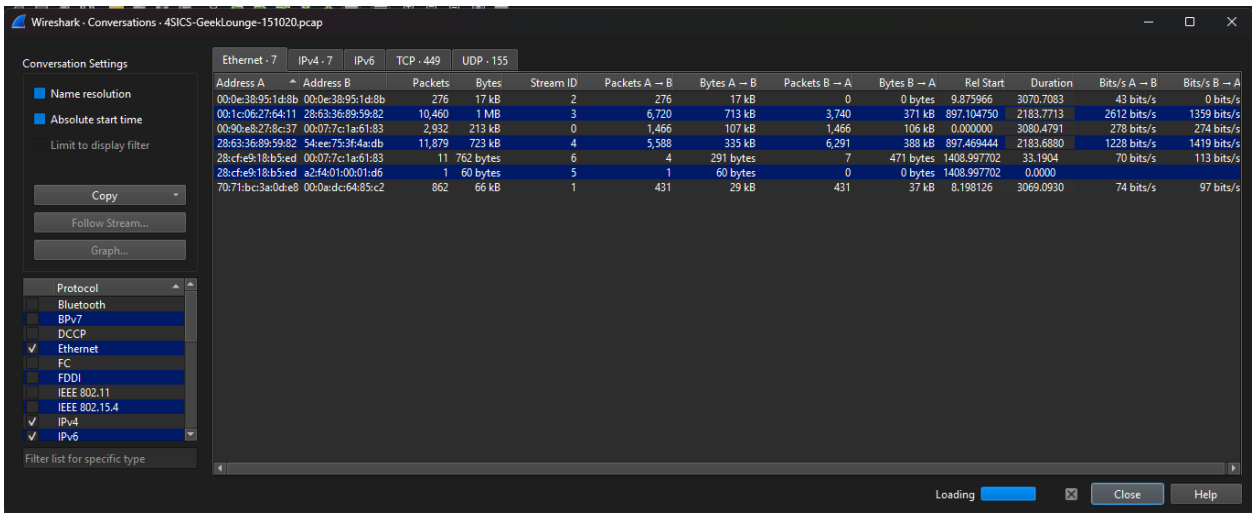

Frame 11161: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{BED094A5-5877-4AF2-B988-3292DC19298A}, id 0
Ethernet II, Src: Dell_5e:56:62 (a4:1f:72:5e:56:62), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)
0000 ff ff ff ff ff ff a4 1f 72 5e 56 62 08 06 00 01
0010 08 00 06 04 00 01 a4 1f 72 5e 56 62 ac 11 0e 1f
0020 00 00 00 00 00 00 ac 11 0e 0f 00 00 00 00 00 00
0030 00 00 00 00 00 00 00 00 00 00 00 00
No.: 11161 · Time: 24.300689 · Source: Dell_5e:56:62 · Destination: Broadcast · Protocol: ARP · Length: 60 · Info: Who has 172.17.14.15? Tell 172.17.14.31
Show packet bytes
Layout: Vertical (Stacked)
Close
Help

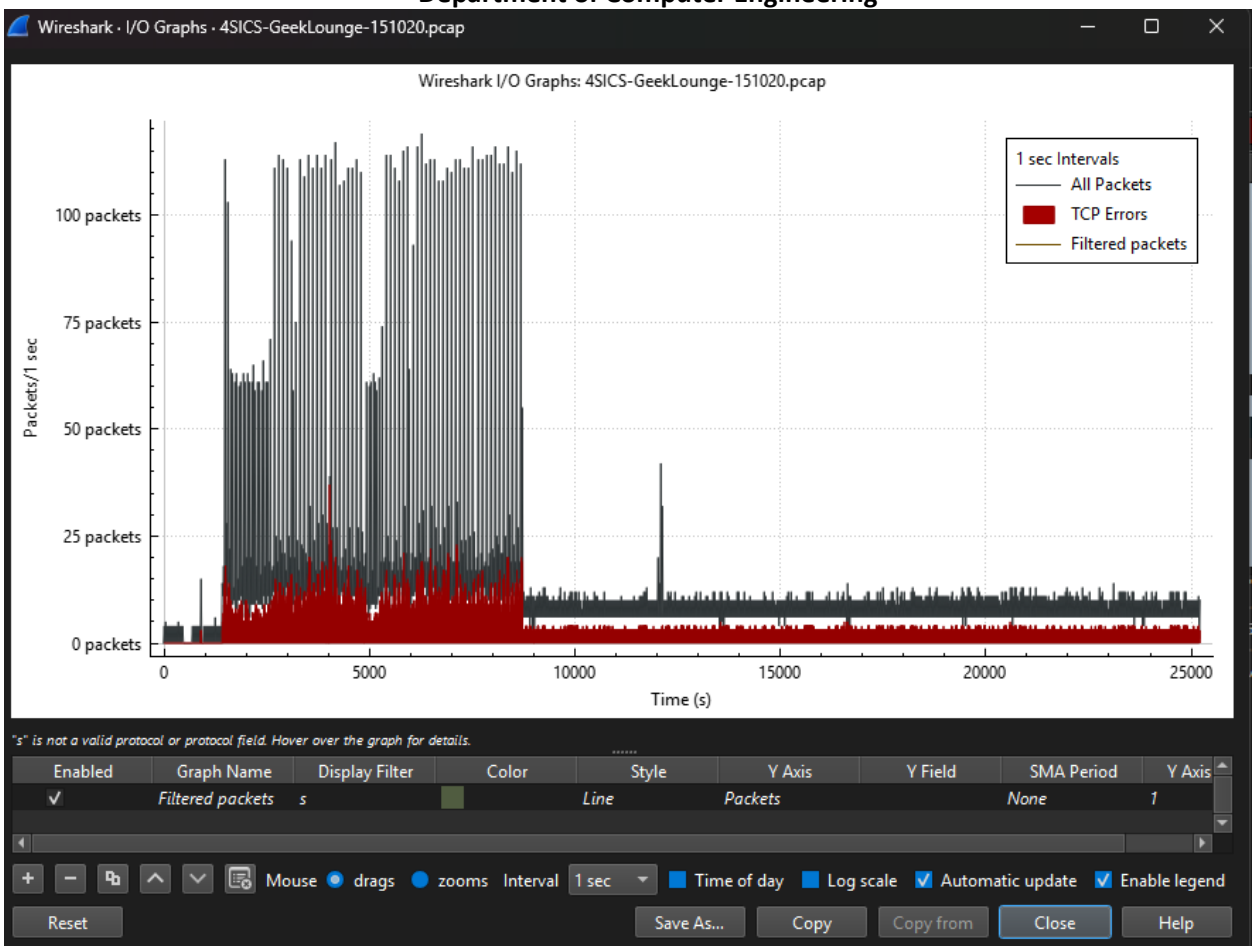

Wireshark · Packet 11150 · Ethernet
Frame 11150: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF_{BED094A5-5877-4AF2-B988-3292DC19298A}, id 0
Ethernet II, Src: MicroStarINT_0c:93:ab (d8:cb:8a:0c:93:ab), Dst: Dell_5e:56:62 (a4:1f:72:5e:56:62)
Internet Protocol Version 4, Src: 172.17.14.23, Dst: 172.17.14.31
Transmission Control Protocol, Src Port: 11100, Dst Port: 62192, Seq: 1374898, Ack: 252, Len: 1460
Data (1460 bytes)
Show packet bytes
Layout: Vertical (Stacked)
Close
Help

PCAP FILE


4SICS-GeekLounge-151020.pcap
No. Time Source Destination Protocol Length Info
4 2.001960 192.168.88.1 192.168.88.61 DNS 73 Standard query response 0xab27 Refused A time.nist.gov
5 4.002296 192.168.88.61 192.168.88.1 DNS 73 Standard query 0xab28 A time.nist.gov
6 4.003324 192.168.88.1 192.168.88.61 DNS 73 Standard query response 0xab28 Refused A time.nist.gov
7 6.003102 192.168.88.61 192.168.88.1 DNS 73 Standard query 0xab29 A time.nist.gov
8 6.004128 192.168.88.1 192.168.88.61 DNS 73 Standard query response 0xab29 Refused A time.nist.gov
9 8.004331 192.168.88.61 192.168.88.1 DNS 73 Standard query 0xab2a A time.nist.gov
10 8.005362 192.168.88.1 192.168.88.61 DNS 73 Standard query response 0xab2a Refused A time.nist.gov
11 8.198126 192.168.89.2 8.8.8.8 DNS 69 Standard query 0x804a A localhost
12 8.198243 192.168.89.1 192.168.89.2 ICMP 97 Destination unreachable (Network unreachable)
13 9.875966 Cisco_95:1d:8b Cisco_95:1d:8b LOOP 60 Reply
14 10.005255 192.168.88.61 192.168.88.1 DNS 73 Standard query 0xab2b A time.nist.gov
15 10.006279 192.168.88.1 192.168.88.61 DNS 73 Standard query response 0xab2b Refused A time.nist.gov
16 12.006492 192.168.88.61 192.168.88.1 DNS 73 Standard query 0xab2c A time.nist.gov
17 12.007528 192.168.88.1 192.168.88.61 DNS 73 Standard query response 0xab2c Refused A time.nist.gov
18 14.059586 192.168.88.61 192.168.88.1 DNS 73 Standard query 0xab2d A time.nist.gov
19 14.060605 192.168.88.1 192.168.88.61 DNS 73 Standard query response 0xab2d Refused A time.nist.gov
20 14.126198 192.168.89.2 8.8.8.8 DNS 74 Standard query 0x0002 A ntp1.dlink.com
21 14.126327 192.168.89.1 192.168.89.2 ICMP 102 Destination unreachable (Network unreachable)
Frame 1: 73 bytes on wire (584 bits), 73 bytes captured (584 bits)
Ethernet II, Src: MoxaTechnolo_27:8c:37 (00:90:e8:27:8c:37), Dst: WestermoNetw_1a:61:83 (00:
Internet Protocol Version 4, Src: 192.168.88.61, Dst: 192.168.88.1
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 59
Identification: 0xaf10 (44816)
000. .... = Flags: 0x0
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 64
Protocol: UDP (17)
Header Checksum: 0x9a12 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.88.61
Destination Address: 192.168.88.1
[Stream index: 0]
User Datagram Protocol, Src Port: 949, Dst Port: 53
Domain Name System (query)


Wireshark · Protocol Hierarchy Statistics · 4SICS-GeekLounge-151020.pcap
Protocol | Percent Packets | Packets | Percent Bytes | Bytes | Bits/s | End Packets | End Bytes
Frame | 100.0 | 246137 | 100.0 | 21772866 | 6912 | 0 | 0
Ethernet | 100.0 | 246137 | 18.9 | 4124797 | 1309 | 0 | 0
Internet Protocol Version 4 | 97.2 | 239267 | 22.0 | 4785340 | 1519 | 0 | 0
User Datagram Protocol | 11.2 | 27587 | 1.0 | 220696 | 70 | 0 | 0
OpenVPN Protocol | 0.0 | 5 | 0.0 | 210 | 0 | 5 | 210
Network Time Protocol | 0.0 | 4 | 0.0 | 192 | 0 | 4 | 192
Domain Name System | 11.2 | 27546 | 3.9 | 846146 | 268 | 27546 | 846146
Data | 0.0 | 32 | 0.0 | 128 | 0 | 32 | 128
Transmission Control Protocol | 84.9 | 208940 | 19.7 | 4293884 | 1363 | 138777 | 2890624
TPKT - ISO on TCP - RFC1006 | 19.3 | 47464 | 0.9 | 189856 | 60 | 0 | 0
Malformed Packet | 0.0 | 1 | 0.0 | 0 | 0 | 1 | 0
ISO 8073/X.224 COTP Connection-Oriented Transport Protocol | 19.3 | 47463 | 0.7 | 142389 | 45 | 0 | 0
S7 Communication | 19.3 | 47463 | 14.7 | 3201804 | 1016 | 47463 | 3201804
Data | 9.2 | 22699 | 0.1 | 22699 | 7 | 22699 | 22699
Internet Control Message Protocol | 1.1 | 2740 | 0.8 | 174009 | 55 | 2740 | 174009
Configuration Test Protocol (loopback) | 1.0 | 2481 | 0.5 | 114126 | 36 | 0 | 0
Data | 1.0 | 2481 | 0.5 | 99240 | 31 | 2481 | 99240
Address Resolution Protocol | 1.8 | 4389 | 0.6 | 122892 | 39 | 4389 | 122892
No display filter.
Close
Copy
Protocols
Help


Wireshark · Conversations · 4SICS-GeekLounge-151020.pcap
Conversation Settings
Name resolution
Absolute start time
Limit to display filter
Copy
Follow Stream...
Graph...
Protocol
Bluetooth
BPv7
DCCP
Ethernet
FC
FDDI
IEEE 802.11
IEEE 802.15.4
IPv4
IPv6
Filter list for specific type
Ethernet · 7
IPv4 · 7
IPv6
TCP · 449
UDP · 155
Address A | Address B | Packets | Bytes | Stream ID | Packets A → B | Bytes A → B | Packets B → A | Bytes B → A | Rel Start | Duration | Bits/s A → B | Bits/s B → A
00:0e:38:95:1d:8b | 00:0e:38:95:1d:8b | 276 | 17 kB | 2 | 276 | 17 kB | 0 | 0 bytes | 9.875966 | 3070.7083 | 43 bits/s | 0 bits/s
00:1c:06:27:64:11 | 28:63:36:89:59:82 | 10,460 | 1 MB | 3 | 6,720 | 713 kB | 3,740 | 371 kB | 897.104750 | 2183.7713 | 2612 bits/s | 1359 bits/s
00:90:e8:27:8c:37 | 00:07:7c:1a:61:83 | 2,932 | 213 kB | 0 | 1,466 | 107 kB | 1,466 | 106 kB | 0.000000 | 3080.4791 | 278 bits/s | 274 bits/s
28:63:36:89:59:82 | 54:ee:75:3f:4a:db | 11,879 | 723 kB | 4 | 5,588 | 335 kB | 6,291 | 388 kB | 897.469444 | 2183.6880 | 1228 bits/s | 1419 bits/s
28:cf:e9:18:b5:ed | 00:07:7c:1a:61:83 | 11 | 762 bytes | 6 | 4 | 291 bytes | 7 | 471 bytes | 1408.997702 | 33.1904 | 70 bits/s | 113 bits/s
28:cf:e9:18:b5:ed | a2:f4:01:00:01:d6 | 1 | 60 bytes | 5 | 1 | 60 bytes | 0 | 0 bytes | 1408.997702 | 0.0000
70:71:bc:3a:0d:e8 | 00:0a:dc:64:85:c2 | 862 | 66 kB | 1 | 431 | 29 kB | 431 | 37 kB | 8.198126 | 3069.0930 | 74 bits/s | 97 bits/s
Loading
Close
Help



CONCLUSION:

In this experiment, we studied the Wireshark packet analyzer tool and learned how to capture and analyse network packets. We observed different protocol headers such as IPv4, TCP, UDP, and ICMP, and understood how data is transmitted across a network. This experiment helped us gain practical knowledge of network monitoring, troubleshooting, and protocol analysis.

Date: 30/10/25 **Signature of faculty in-charge**