Batch: A1	Roll No.: 16010120015
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:

CO: Study about the function of the wireshark analyser tool such as

Deep inspection of hundreds of protocols, with more being added all the time

- Live capture and offline analysis
- Multi-platform: Runs on Windows, Linux, macOS, Solaris, FreeBSD, NetBSD, and many others
- The most powerful display filters in the industry

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

Wireshark is an open-source packet analyzer, 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 as a sniffer, network protocol analyzer, and network analyzer.
- It is also used by network security engineers to examine security problems.

It is often called as 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:

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

Features of Wireshark

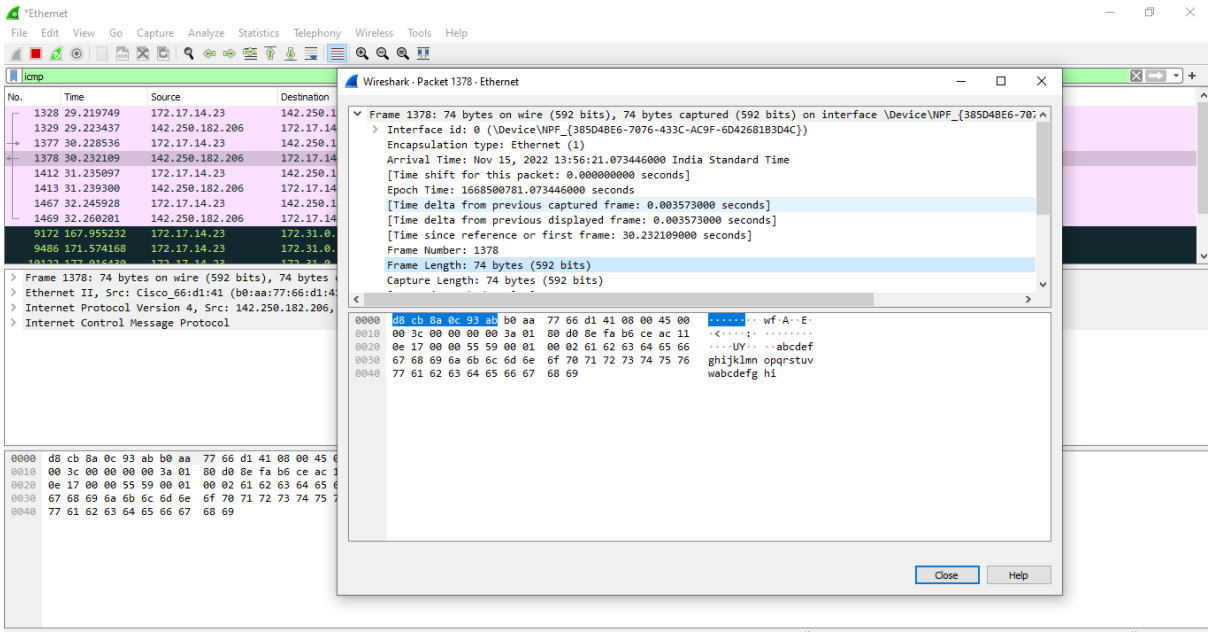
- It is multi-platform software, i.e., it can run on Linux, Windows, OS X, FreeBSD, NetBSD, etc.
- It is a standard three-pane packet browser.
- It performs deep inspection of the hundreds of protocols.
- It often involves live analysis, i.e., from the different types of the network like the Ethernet, loopback, etc., we can read live data.

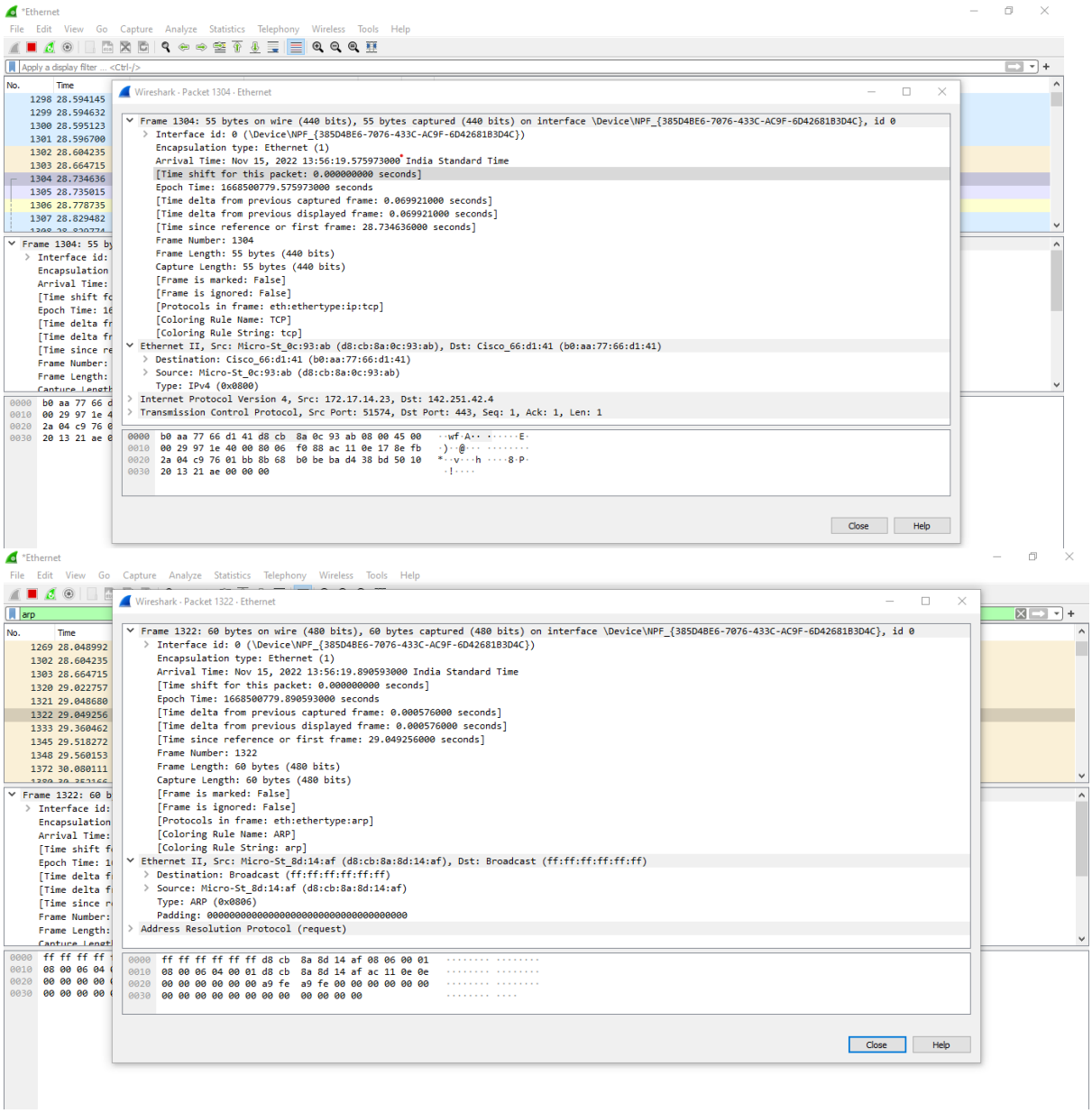
- It has sort and filter options which makes ease to the user to view the data.
- It is also useful in VoIP analysis.

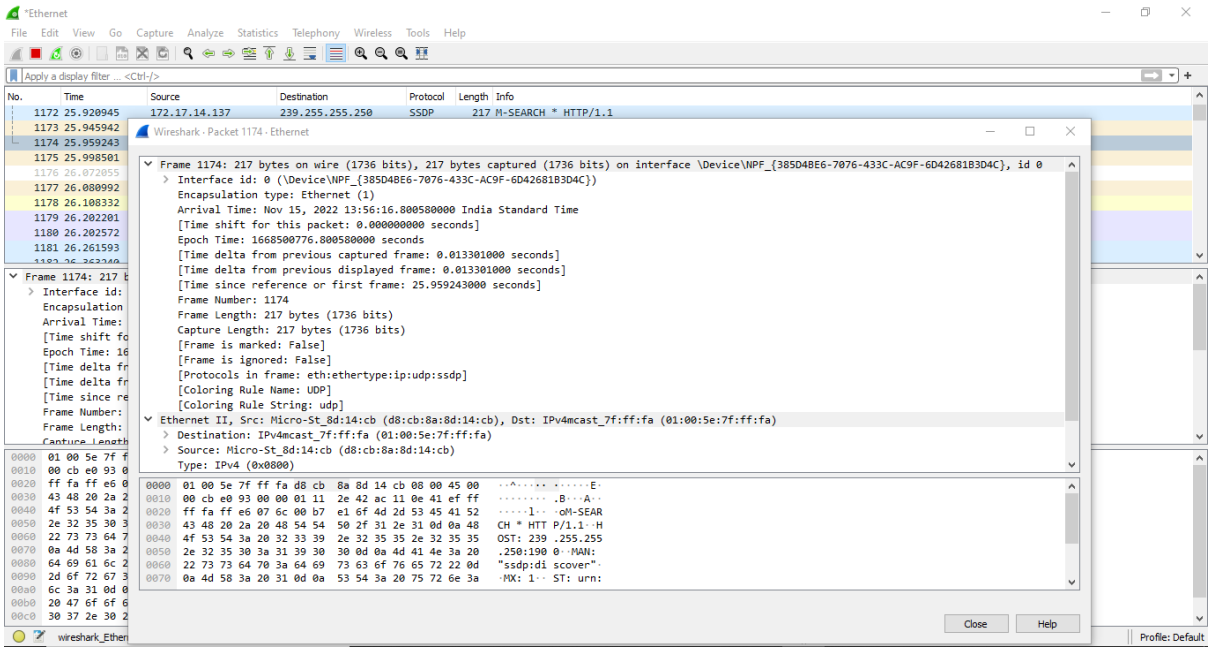
Wireshark does three things:

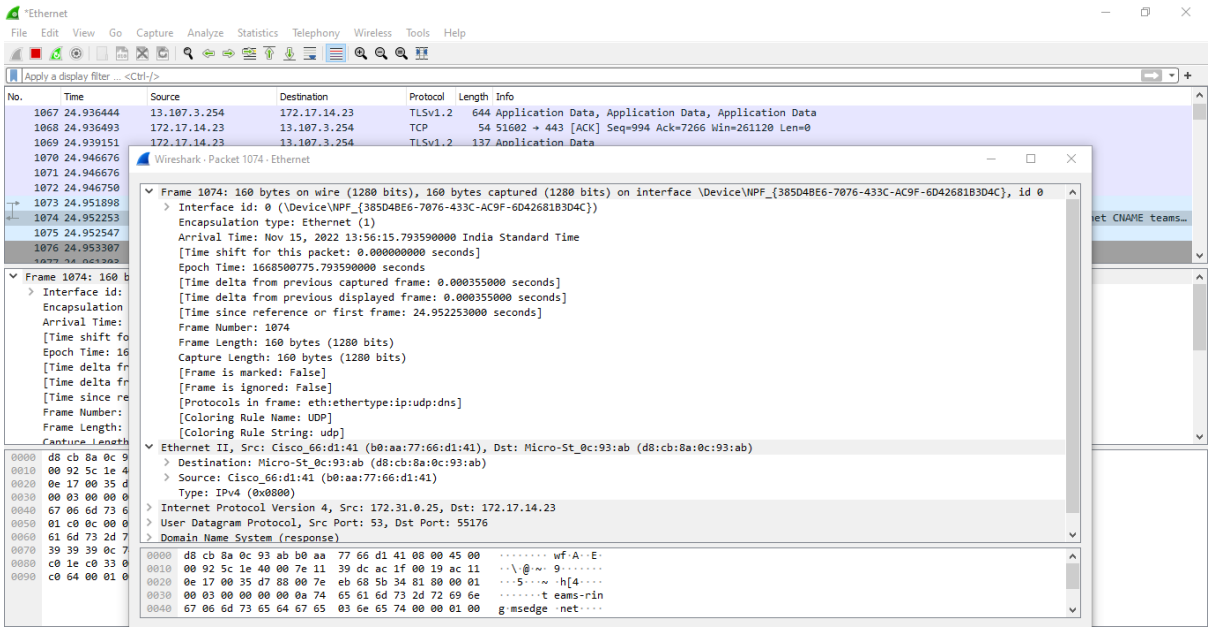
1. **Packet Capture:** Wireshark listens to a network connection in real time and then grabs entire streams of traffic – quite possibly tens of thousands of packets at a time.
2. **Filtering:** Wireshark is capable of slicing and dicing all of this random live data using filters. By applying a filter, you can obtain just the information you need to see.
3. **Visualization:** Wireshark, like any good packet sniffer, allows you to dive right into the very middle of a network packet. It also allows you to visualize entire conversations and network streams.

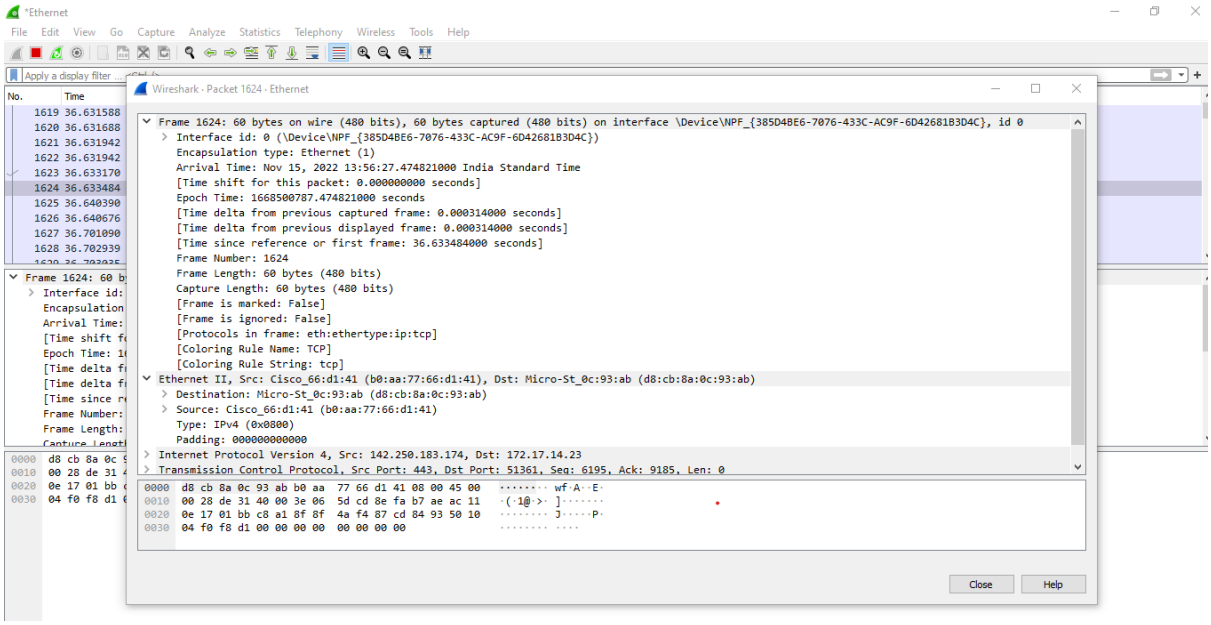
IMPLEMENTATION:

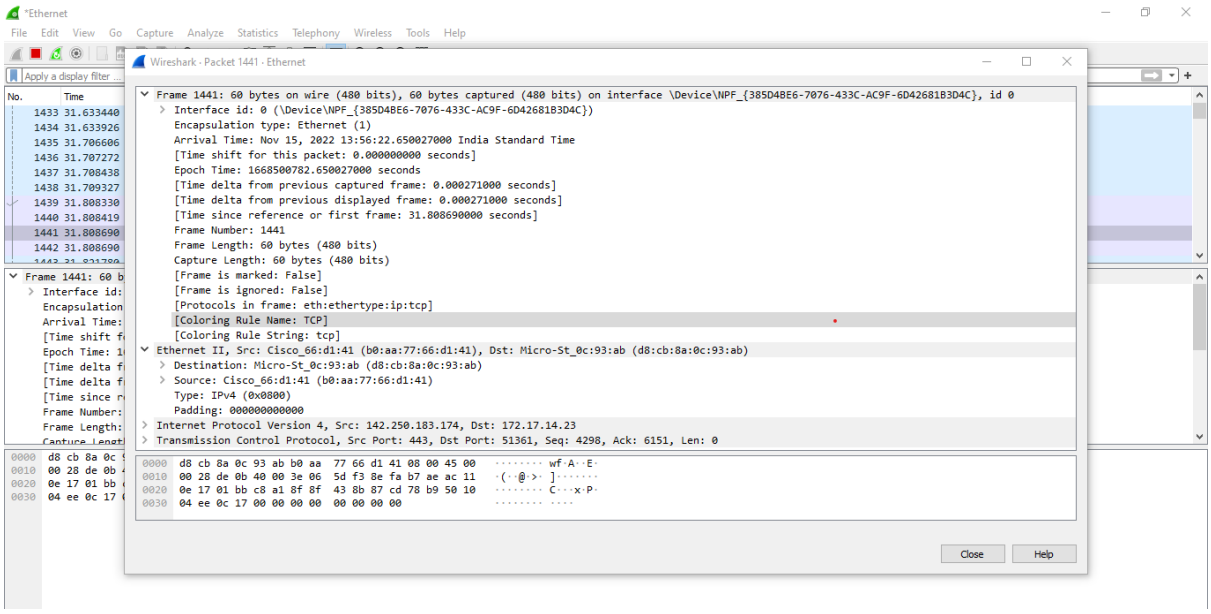



Wireshark · Packet 1304 · Ethernet
Frame 1304: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface \Device\NPF_{385D4BE6-7076-433C-AC9F-6D42681B3D4C}, id 0
Interface id: 0 (\Device\NPF_{385D4BE6-7076-433C-AC9F-6D42681B3D4C})
Encapsulation type: Ethernet (1)
Arrival Time: Nov 15, 2022 13:56:19.575973000 India Standard Time
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1668500779.575973000 seconds
[Time delta from previous captured frame: 0.069921000 seconds]
[Time delta from previous displayed frame: 0.069921000 seconds]
[Time since reference or first frame: 28.734636000 seconds]
Frame Number: 1304
Frame Length: 55 bytes (440 bits)
Capture Length: 55 bytes (440 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:tcp]
[Coloring Rule Name: TCP]
[Coloring Rule String: tcp]
Ethernet II, Src: Micro-St_0c:93:ab (d8:cb:8a:0c:93:ab), Dst: Cisco_66:d1:41 (b0:aa:77:66:d1:41)
Destination: Cisco_66:d1:41 (b0:aa:77:66:d1:41)
Source: Micro-St_0c:93:ab (d8:cb:8a:0c:93:ab)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 172.17.14.23, Dst: 142.251.42.4
Transmission Control Protocol, Src Port: 51574, Dst Port: 443, Seq: 1, Ack: 1, Len: 1
0000 b0 aa 77 66 d1 41 d8 cb 8a 0c 93 ab 08 00 45 00
0010 00 29 97 1e 40 00 80 06 f0 88 ac 11 0e 17 8e fb
0020 2a 04 c9 76 01 bb 8b 68 b0 be ba d4 38 bd 50 10
0030 20 13 21 ae 00 00 00
Close
Help
Wireshark · Packet 1322 · Ethernet
Frame 1322: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{385D4BE6-7076-433C-AC9F-6D42681B3D4C}, id 0
Interface id: 0 (\Device\NPF_{385D4BE6-7076-433C-AC9F-6D42681B3D4C})
Encapsulation type: Ethernet (1)
Arrival Time: Nov 15, 2022 13:56:19.890593000 India Standard Time
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1668500779.890593000 seconds
[Time delta from previous captured frame: 0.000576000 seconds]
[Time delta from previous displayed frame: 0.000576000 seconds]
[Time since reference or first frame: 29.049256000 seconds]
Frame Number: 1322
Frame Length: 60 bytes (480 bits)
Capture Length: 60 bytes (480 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:arp]
[Coloring Rule Name: ARP]
[Coloring Rule String: arp]
Ethernet II, Src: Micro-St_8d:14:af (d8:cb:8a:8d:14:af), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Destination: Broadcast (ff:ff:ff:ff:ff:ff)
Source: Micro-St_8d:14:af (d8:cb:8a:8d:14:af)
Type: ARP (0x0806)
Padding: 000000000000000000000000000000000000
Address Resolution Protocol (request)
0000 ff ff ff ff ff ff d8 cb 8a 8d 14 af 08 06 00 01
0010 08 00 06 04 00 01 d8 cb 8a 8d 14 af ac 11 0e 0e
0020 00 00 00 00 00 00 a9 fe a9 fe 00 00 00 00 00 00
0030 00 00 00 00 00 00 00 00 00 00 00 00
Close
Help


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1172 25.920945 172.17.14.137 239.255.255.250 SSDP 217 M-SEARCH * HTTP/1.1
1173 25.945942
1174 25.959243
1175 25.998501
1176 26.072055
1177 26.080992
1178 26.108332
1179 26.202201
1180 26.202572
1181 26.261593
Wireshark · Packet 1174 · Ethernet
Frame 1174: 217 bytes on wire (1736 bits), 217 bytes captured (1736 bits) on interface \Device\NPF_{385D4BE6-7076-433C-AC9F-6D42681B3D4C}, id 0
Interface id: 0 (\Device\NPF_{385D4BE6-7076-433C-AC9F-6D42681B3D4C})
Encapsulation type: Ethernet (1)
Arrival Time: Nov 15, 2022 13:56:16.800580000 India Standard Time
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1668500776.800580000 seconds
[Time delta from previous captured frame: 0.013301000 seconds]
[Time delta from previous displayed frame: 0.013301000 seconds]
[Time since reference or first frame: 25.959243000 seconds]
Frame Number: 1174
Frame Length: 217 bytes (1736 bits)
Capture Length: 217 bytes (1736 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:udp:ssdp]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: Micro-St_8d:14:cb (d8:cb:8a:8d:14:cb), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
Destination: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
Source: Micro-St_8d:14:cb (d8:cb:8a:8d:14:cb)
Type: IPv4 (0x0800)
0000 01 00 5e 7f ff fa d8 cb 8a 8d 14 cb 08 00 45 00
0010 00 cb e0 93 00 00 01 11 2e 42 ac 11 0e 41 ef ff
0020 ff fa ff e6 07 6c 00 b7 e1 6f 4d 2d 53 45 41 52
0030 43 48 20 2a 20 48 54 54 50 2f 31 2e 31 0d 0a 48
0040 4f 53 54 3a 20 32 33 39 2e 32 35 35 2e 32 35 35
0050 2e 32 35 30 3a 31 39 30 30 0d 0a 4d 41 4e 3a 20
0060 22 73 73 64 70 3a 64 69 73 63 6f 76 65 72 22 0d
0070 0a 4d 58 3a 20 31 0d 0a 53 54 3a 20 75 72 6e 3a
Close
Help
Profile: Default


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1067 24.936444 13.107.3.254 172.17.14.23 TLSv1.2 644 Application Data, Application Data, Application Data
1068 24.936493 172.17.14.23 13.107.3.254 TCP 54 51602 → 443 [ACK] Seq=994 Ack=7266 Win=261120 Len=0
1069 24.939151 172.17.14.23 13.107.3.254 TLSv1.2 137 Application Data
1070 24.946676
1071 24.946676
1072 24.946750
1073 24.951898
1074 24.952253
1075 24.952547
1076 24.953307
Wireshark · Packet 1074 · Ethernet
Frame 1074: 160 bytes on wire (1280 bits), 160 bytes captured (1280 bits) on interface \Device\NPF_{385D4BE6-7076-433C-AC9F-6D42681B3D4C}, id 0
Interface id: 0 (\Device\NPF_{385D4BE6-7076-433C-AC9F-6D42681B3D4C})
Encapsulation type: Ethernet (1)
Arrival Time: Nov 15, 2022 13:56:15.793590000 India Standard Time
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1668500775.793590000 seconds
[Time delta from previous captured frame: 0.000355000 seconds]
[Time delta from previous displayed frame: 0.000355000 seconds]
[Time since reference or first frame: 24.952253000 seconds]
Frame Number: 1074
Frame Length: 160 bytes (1280 bits)
Capture Length: 160 bytes (1280 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: Cisco_66:d1:41 (b0:aa:77:66:d1:41), Dst: Micro-St_0c:93:ab (d8:cb:8a:0c:93:ab)
Destination: Micro-St_0c:93:ab (d8:cb:8a:0c:93:ab)
Source: Cisco_66:d1:41 (b0:aa:77:66:d1:41)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 172.31.0.25, Dst: 172.17.14.23
User Datagram Protocol, Src Port: 53, Dst Port: 55176
Domain Name System (response)
0000 d8 cb 8a 0c 93 ab b0 aa 77 66 d1 41 08 00 45 00
0010 00 92 5c 1e 40 00 7e 11 39 dc ac 1f 00 19 ac 11
0020 0e 17 00 35 d7 88 00 7e eb 68 5b 34 81 80 00 01
0030 00 03 00 00 00 00 0a 74 65 61 6d 73 2d 72 69 6e
0040 67 06 6d 73 65 64 67 65 03 6e 65 74 00 00 01 00


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
No. Time
1619 36.631588
1620 36.631688
1621 36.631942
1622 36.631942
1623 36.633170
1624 36.633484
1625 36.640390
1626 36.640676
1627 36.701090
1628 36.702939
Wireshark · Packet 1624 · Ethernet
Frame 1624: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{385D4BE6-7076-433C-AC9F-6D42681B3D4C}, id 0
Interface id: 0 (\Device\NPF_{385D4BE6-7076-433C-AC9F-6D42681B3D4C})
Encapsulation type: Ethernet (1)
Arrival Time: Nov 15, 2022 13:56:27.474821000 India Standard Time
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1668500787.474821000 seconds
[Time delta from previous captured frame: 0.000314000 seconds]
[Time delta from previous displayed frame: 0.000314000 seconds]
[Time since reference or first frame: 36.633484000 seconds]
Frame Number: 1624
Frame Length: 60 bytes (480 bits)
Capture Length: 60 bytes (480 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:tcp]
[Coloring Rule Name: TCP]
[Coloring Rule String: tcp]
Ethernet II, Src: Cisco_66:d1:41 (b0:aa:77:66:d1:41), Dst: Micro-St_0c:93:ab (d8:cb:8a:0c:93:ab)
Destination: Micro-St_0c:93:ab (d8:cb:8a:0c:93:ab)
Source: Cisco_66:d1:41 (b0:aa:77:66:d1:41)
Type: IPv4 (0x0800)
Padding: 000000000000
Internet Protocol Version 4, Src: 142.250.183.174, Dst: 172.17.14.23
Transmission Control Protocol, Src Port: 443, Dst Port: 51361, Seq: 6195, Ack: 9185, Len: 0
0000 d8 cb 8a 0c 93 ab b0 aa 77 66 d1 41 08 00 45 00
0010 00 28 de 31 40 00 3e 06 5d cd 8e fa b7 ae ac 11
0020 0e 17 01 bb c8 a1 8f 8f 4a f4 87 cd 84 93 50 10
0030 04 f0 f8 d1 00 00 00 00 00 00 00 00
Close
Help



CONCLUSION:

Hence we have implemented and successfully studied about Wireshark

Wireshark basically Which captures packets from a network connection, such as from your computer to your home office or the internet.. Wireshark is the most often-used packet sniffer

Post Lab Questions:

Date: ___15/11/2022____ **Signature of faculty in-charge**