EX:NO:5
31.7.25

Experiment on packet capture tool wireshark.

AIM:

Experiments on packet capture tool .wireshark.

Packet Sniffer:

* Sniffs messages being sent/received from/by your computer.
* Store and display the contents of the various protocol field in the message.
* Passive program.
  - never sends packet itself
  - no packets addressed to it.
  - receiver a copy of all packets (sent/received)

Packet Sniffer Structure, Diagnostic Tools:

* Tcpdump
  - E.g. tcpdump -enx host 10.129.41.2 -w
* wireshark
  - wireshark -r exe3.out.

Wireshark:

Wireshark, a network-analysis tool formerly known as Ethereal, captures packets in real time and display them in human readable format.

What we can do with wireshark:

* Capture network traffic
* Decode packet protocols using dissectors.
* Watch smart statistics.
* Analyze problems.

Wireshark used For:

* Network administration : troubleshoot network problems
* Developers : debug protocol implementations.
* People : learn network protocol internals.

Getting Wireshark:

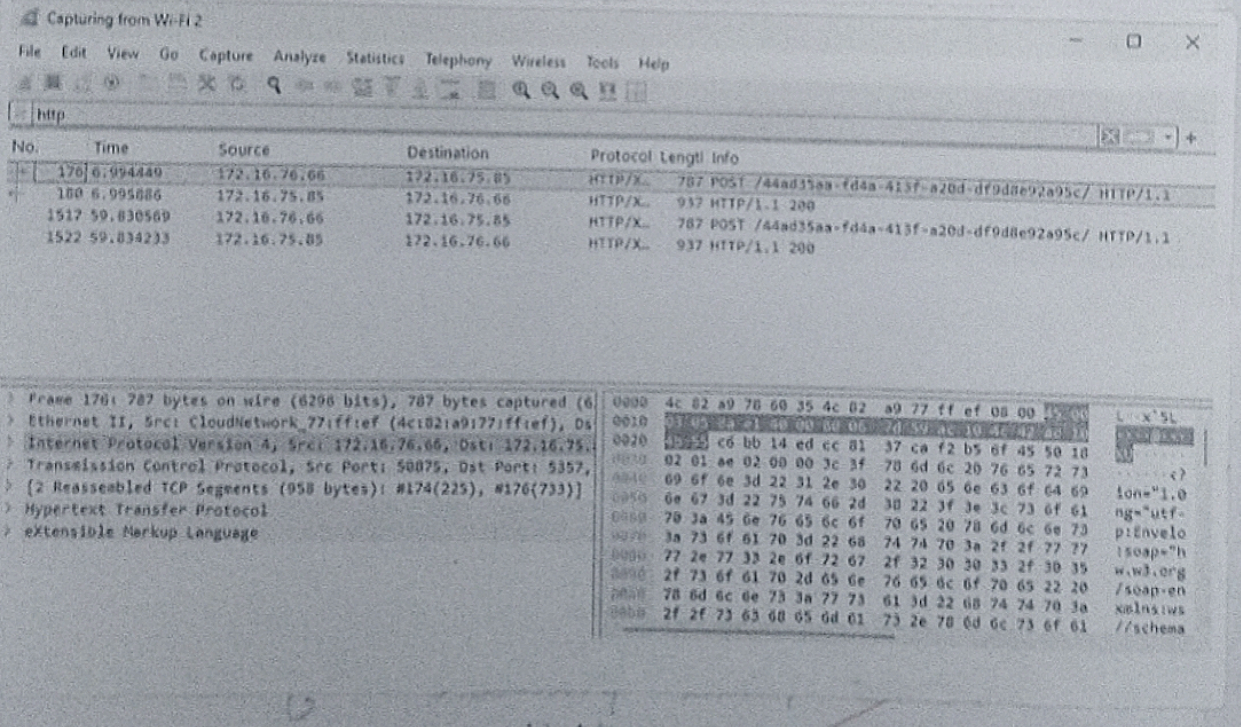
Wireshark can be downloaded for window or macOS from its official website.

Capturing Packets.

After downloading and installing Wireshark, launch it and double-click the name of a network interface under Capture to start capturing packets on that interface.

Sample Captures:

If there's nothing interesting on your own network to inspect, Wireshark's wiki has you covered.

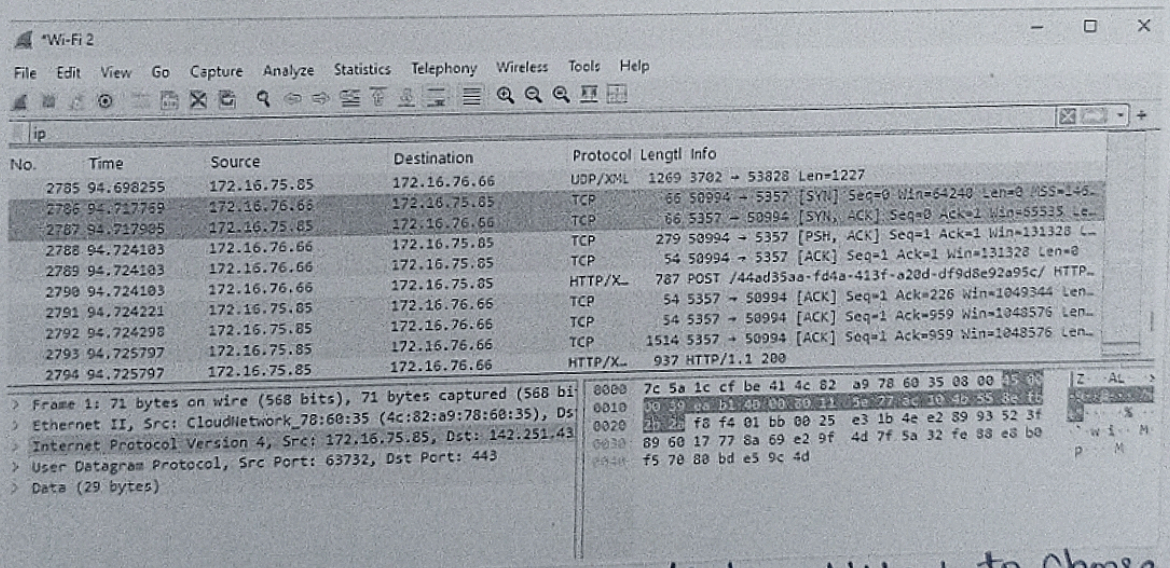


The "Packet Bytes" Pane:

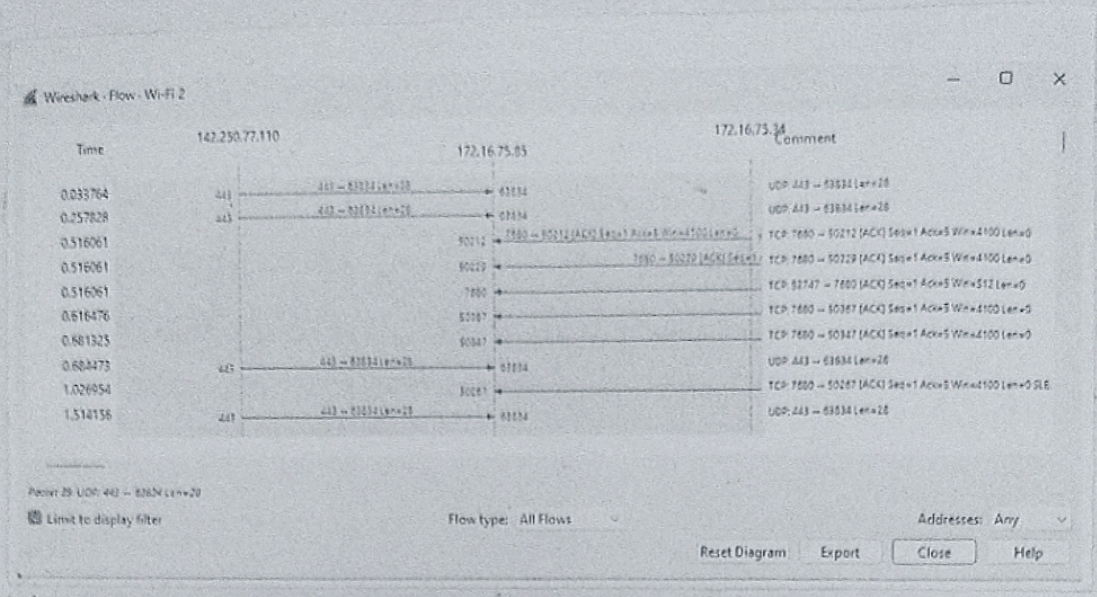
The packet bytes pane shows the data of the current packet (selected in the "packet list" pane) in a hexdump style.

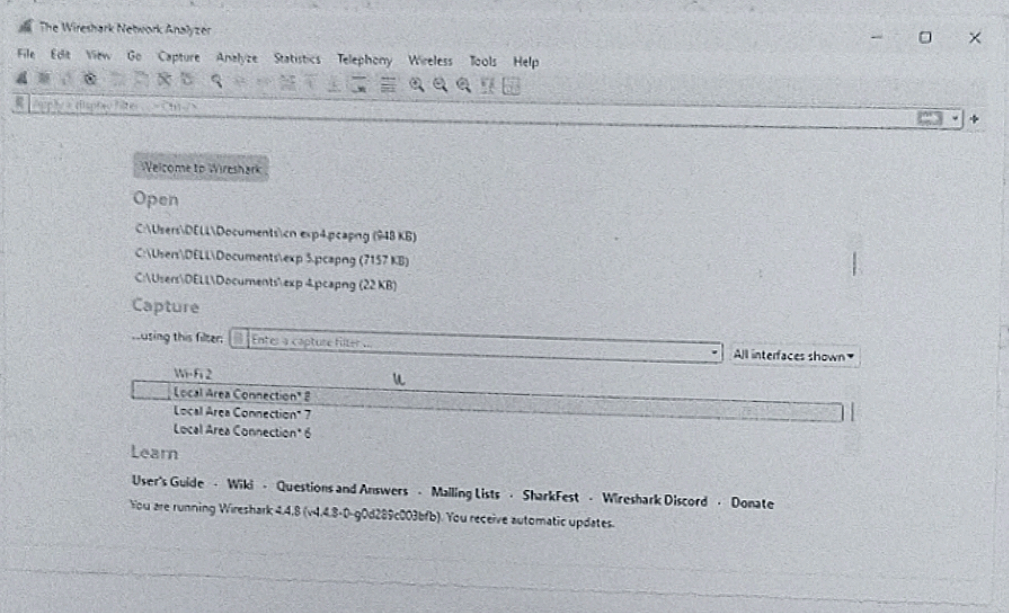
Filtering Packets:

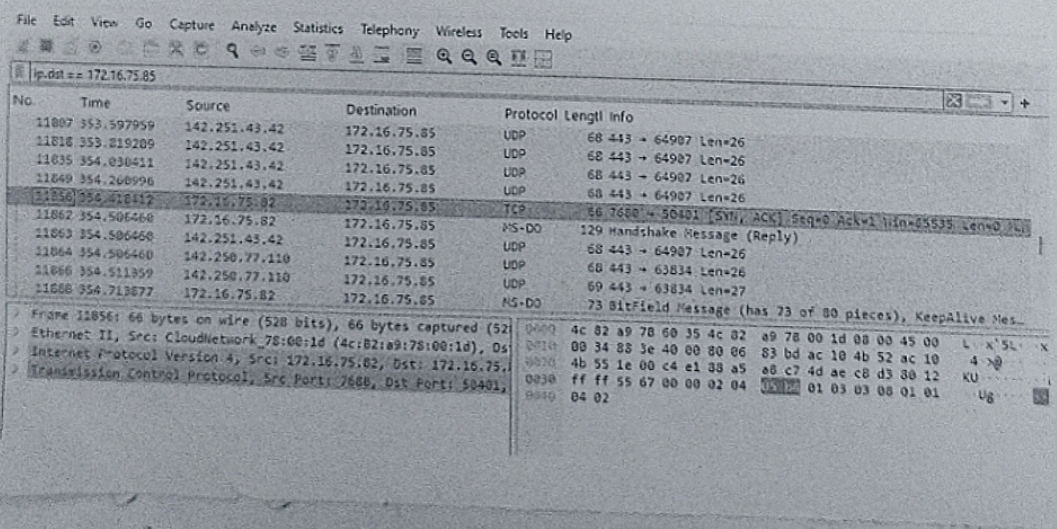
If you're trying to inspect something specific, such as the traffic a program send when phoning home, it helps to close down all other applications using network so you can narrow down the traffic. Still, you'll likely have a large amount of packets to sift through. That's where wireshark's filters come in.

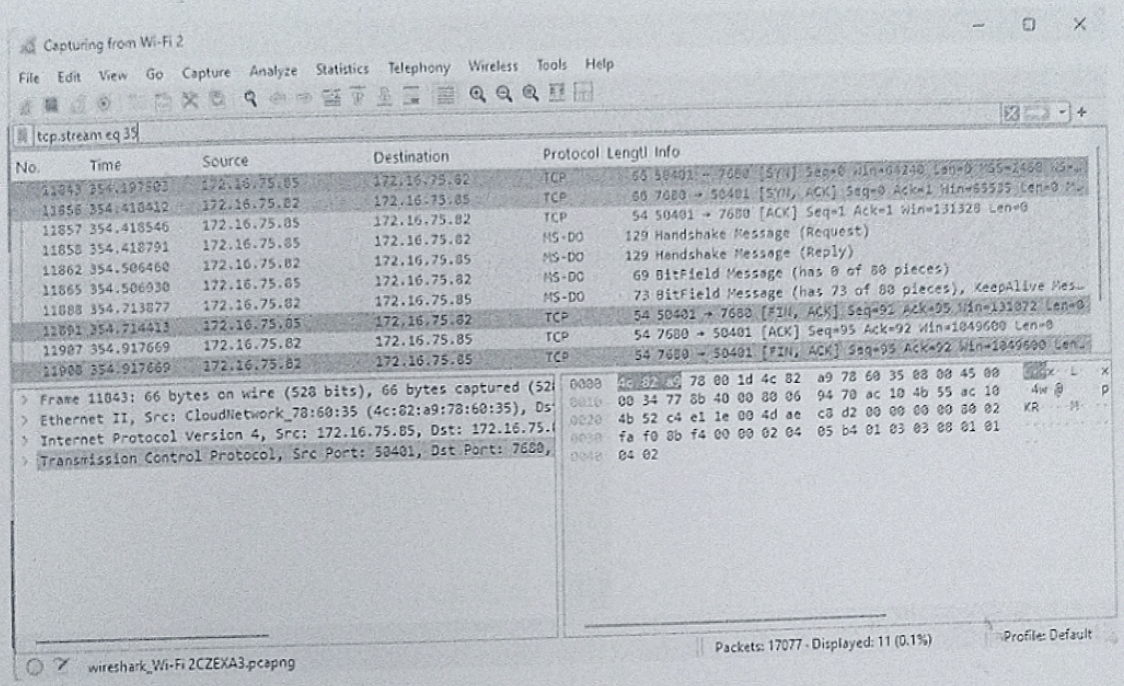


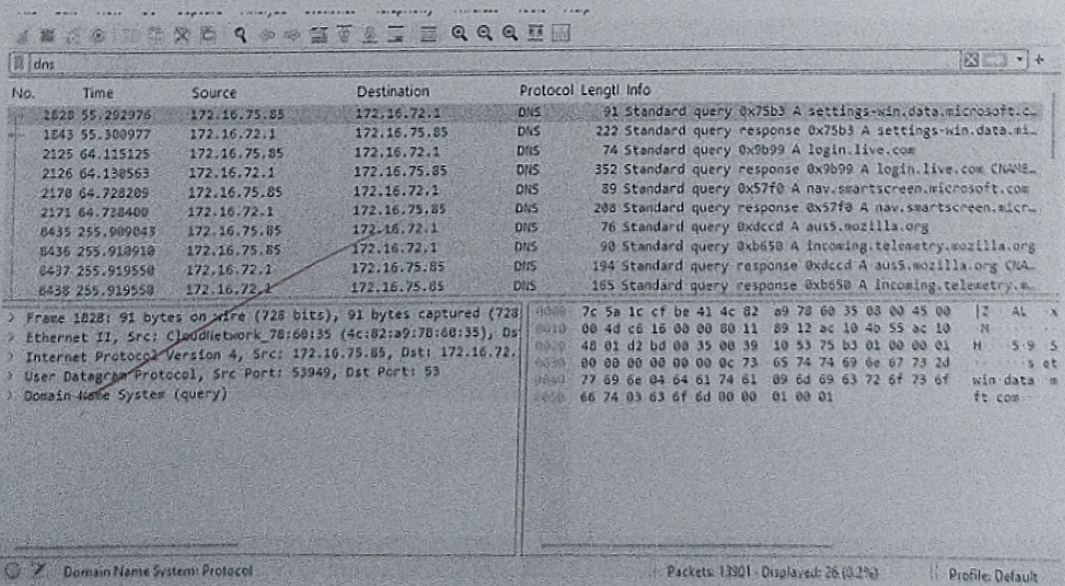
You can also click Analze > Display filters to choose a filter from among the default filter included in wireshark. close the window and you'll find a filter has been applied automatically. wireshark is showing you the packet that make up the conversion.

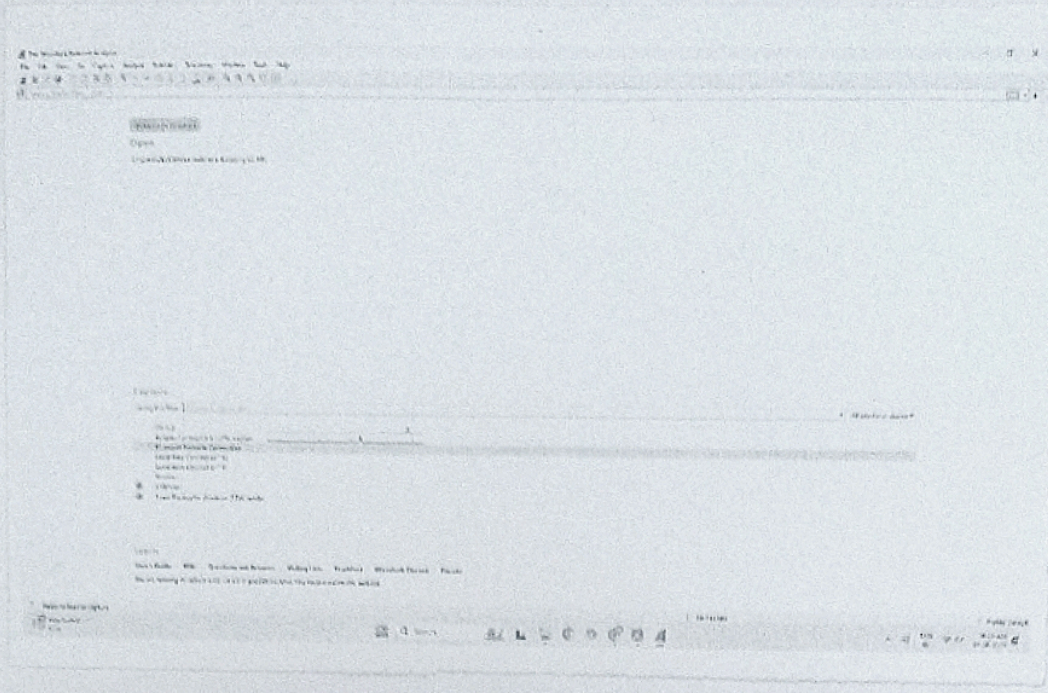

Wireshark · Flow · Wi-Fi 2
Time
142.250.77.110
172.16.75.85
172.16.75.34
Comment
0.033764
0.257828
0.516061
0.516061
0.516061
0.616476
0.681325
0.684473
1.026954
1.314136
UDP: 443 → 63834 Len=28
UDP: 443 → 63834 Len=28
TCP: 7680 → 50212 [ACK] Seq=1 Ack=5 Win=4100 Len=0
TCP: 7680 → 50229 [ACK] Seq=1 Ack=5 Win=4100 Len=0
TCP: 52747 → 7680 [ACK] Seq=1 Ack=5 Win=512 Len=0
TCP: 7680 → 50367 [ACK] Seq=1 Ack=5 Win=4100 Len=0
TCP: 7680 → 50347 [ACK] Seq=1 Ack=5 Win=4100 Len=0
UDP: 443 → 63834 Len=28
TCP: 7680 → 50267 [ACK] Seq=1 Ack=5 Win=4100 Len=0 SLE
UDP: 443 → 63834 Len=28
Limit to display filter
Flow type: All Flows
Addresses: Any
Reset Diagram
Export
Close
Help


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Welcome to Wireshark
Open
C:\Users\DELL\Documents\cn exp4.pcapng (948 KB)
C:\Users\DELL\Documents\exp 5.pcapng (7157 KB)
C:\Users\DELL\Documents\exp 4.pcapng (22 KB)
Capture
...using this filter:
Enter a capture filter ...
All interfaces shown
Wi-Fi 2
Local Area Connection* 8
Local Area Connection* 7
Local Area Connection* 6
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate
You are running Wireshark 4.4.8 (v4.4.8-0-g0d289c003bfb). You receive automatic updates.


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.dst == 172.16.75.85
No. Time Source Destination Protocol Lengtl Info
11807 353.597959 142.251.43.42 172.16.75.85 UDP 68 443 → 64907 Len=26
11818 353.819209 142.251.43.42 172.16.75.85 UDP 68 443 → 64907 Len=26
11835 354.030411 142.251.43.42 172.16.75.85 UDP 68 443 → 64907 Len=26
11849 354.260996 142.251.43.42 172.16.75.85 UDP 68 443 → 64907 Len=26
11856 354.418412 172.16.75.82 172.16.75.85 TCP 66 7680 → 50401 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 ML
11862 354.506460 172.16.75.82 172.16.75.85 MS-DO 129 Handshake Message (Reply)
11863 354.506460 142.251.43.42 172.16.75.85 UDP 68 443 → 64907 Len=26
11864 354.506460 142.250.77.110 172.16.75.85 UDP 68 443 → 63834 Len=26
11866 354.511859 142.250.77.110 172.16.75.85 UDP 69 443 → 63834 Len=27
11868 354.713877 172.16.75.82 172.16.75.85 MS-DO 73 BitField Message (has 73 of 80 pieces), KeepAlive Mes
Frame 11856: 66 bytes on wire (528 bits), 66 bytes captured (52
Ethernet II, Src: CloudNetwork_78:00:1d (4c:82:a9:78:00:1d), Ds
Internet Protocol Version 4, Src: 172.16.75.82, Dst: 172.16.75.
Transmission Control Protocol, Src Port: 7680, Dst Port: 50401,
0000 4c 82 a9 78 00 1d 4c 82 a9 78 00 1d 08 00 45 00
0010 00 34 88 3e 40 00 80 06 83 bd ac 10 4b 52 ac 10
0020 4b 55 1e 00 c4 e1 38 a5 a8 c7 4d ae c8 d3 30 12
0030 ff ff 55 67 00 00 02 04 05 b4 01 03 03 08 01 01
0040 04 02

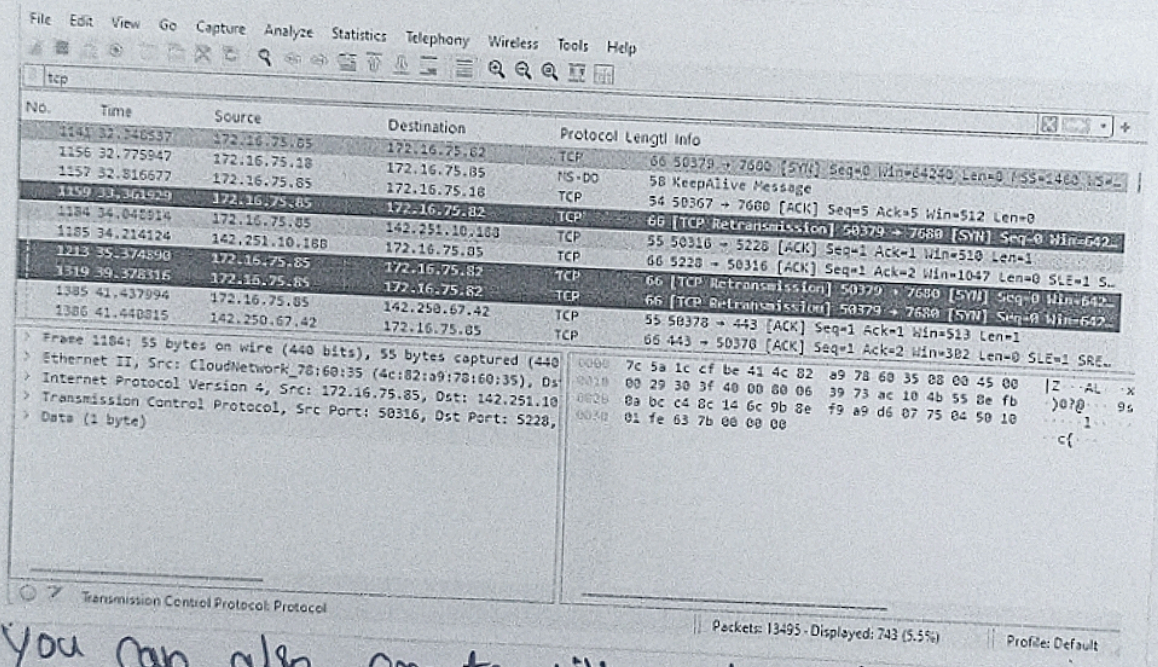

Capturing from Wi-Fi 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.stream eq 35
No. Time Source Destination Protocol Lengtl Info
11843 354.197503 172.16.75.85 172.16.75.82 TCP 66 50401 → 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=…
11856 354.418412 172.16.75.82 172.16.75.85 TCP 66 7680 → 50401 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MS…
11857 354.418546 172.16.75.85 172.16.75.82 TCP 54 50401 → 7680 [ACK] Seq=1 Ack=1 Win=131328 Len=0
11858 354.418791 172.16.75.85 172.16.75.82 MS-DO 129 Handshake Message (Request)
11862 354.506460 172.16.75.82 172.16.75.85 MS-DO 129 Handshake Message (Reply)
11865 354.506930 172.16.75.85 172.16.75.82 MS-DO 69 BitField Message (has 0 of 80 pieces)
11888 354.713877 172.16.75.82 172.16.75.85 MS-DO 73 BitField Message (has 73 of 80 pieces), KeepAlive Mes…
11891 354.714413 172.16.75.85 172.16.75.82 TCP 54 50401 → 7680 [FIN, ACK] Seq=92 Ack=95 Win=131072 Len=0
11907 354.917669 172.16.75.82 172.16.75.85 TCP 54 7680 → 50401 [ACK] Seq=95 Ack=92 Win=1049600 Len=0
11908 354.917669 172.16.75.82 172.16.75.85 TCP 54 7680 → 50401 [FIN, ACK] Seq=95 Ack=92 Win=1049600 Len…
Frame 11043: 66 bytes on wire (528 bits), 66 bytes captured (52
Ethernet II, Src: CloudNetwork_78:60:35 (4c:82:a9:78:60:35), Ds
Internet Protocol Version 4, Src: 172.16.75.85, Dst: 172.16.75.
Transmission Control Protocol, Src Port: 50401, Dst Port: 7680,
0000 4c 82 a9 78 60 35 88 08 45 00
0010 00 34 77 8b 40 00 80 06 94 70 ac 10 4b 55 ac 10
0020 4b 52 c4 e1 1e 00 4d ae c8 d2 00 00 00 00 80 02
0030 fa f0 8b f4 00 00 02 04 05 b4 01 03 03 08 01 01
0040 04 02
wireshark_Wi-Fi 2CZEXA3.pcapng
Packets: 17077 · Displayed: 11 (0.1%)
Profile: Default


dns
No. Time Source Destination Protocol Lengtl Info
1828 55.292976 172.16.75.85 172.16.72.1 DNS 91 Standard query 0x75b3 A settings-win.data.microsoft.c…
1843 55.300977 172.16.72.1 172.16.75.85 DNS 222 Standard query response 0x75b3 A settings-win.data.mi…
2125 64.115125 172.16.75.85 172.16.72.1 DNS 74 Standard query 0x9b99 A login.live.com
2126 64.130563 172.16.72.1 172.16.75.85 DNS 352 Standard query response 0x9b99 A login.live.com CNAME…
2170 64.728289 172.16.75.85 172.16.72.1 DNS 89 Standard query 0x57f0 A nav.smartscreen.microsoft.com
2171 64.728400 172.16.72.1 172.16.75.85 DNS 208 Standard query response 0x57f0 A nav.smartscreen.micr…
8435 255.909043 172.16.75.85 172.16.72.1 DNS 76 Standard query 0xdccd A aus5.mozilla.org
8436 255.910910 172.16.75.85 172.16.72.1 DNS 90 Standard query 0xb650 A incoming.telemetry.mozilla.org
8437 255.919550 172.16.72.1 172.16.75.85 DNS 194 Standard query response 0xdccd A aus5.mozilla.org CNA…
8438 255.919550 172.16.72.1 172.16.75.85 DNS 165 Standard query response 0xb650 A incoming.telemetry.m…
Frame 1828: 91 bytes on wire (728 bits), 91 bytes captured (728
Ethernet II, Src: CloudNetwork_78:60:35 (4c:82:a9:78:60:35), Ds
Internet Protocol Version 4, Src: 172.16.75.85, Dst: 172.16.72.
User Datagram Protocol, Src Port: 53949, Dst Port: 53
Domain Name System (query)
0000 7c 5a 1c cf be 41 4c 82 a9 78 60 35 08 00 45 00
0010 00 4d c6 16 00 00 80 11 89 12 ac 10 4b 55 ac 10
0020 48 01 d2 bd 00 35 00 39 10 53 75 b3 01 00 00 01
0030 00 00 00 00 00 00 0c 73 65 74 74 69 6e 67 73 2d
0040 77 69 6e 04 64 61 74 61 09 6d 69 63 72 6f 73 6f
0050 66 74 03 63 6f 6d 00 00 01 00 01
Domain Name System (protocol
Packets: 13901 · Displayed: 26 (0.2%)
Profile: Default



Inspecting Packet:

Click a packet to select it and you can dig down to view its details.



You can also create filters from here. Just right-cli one of the details and use the Apply as filter submenu to create a filter based on it.

Flow Graph: Gives a better understanding of what we see.

Capturing and Analysis Packets using wireshark Tool:

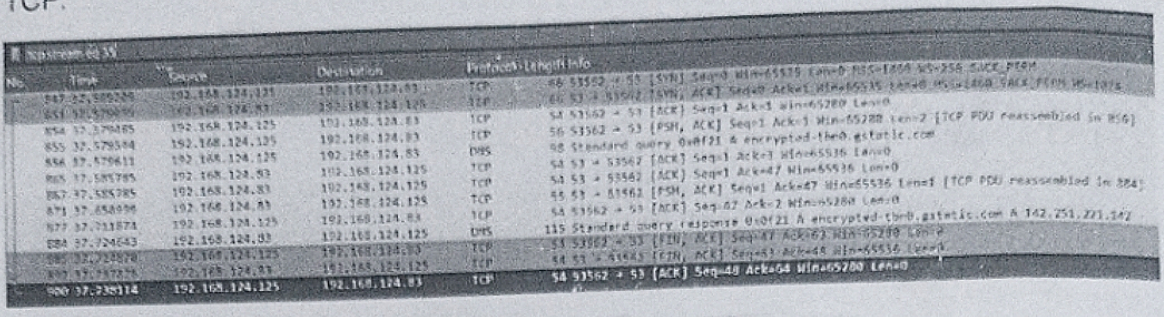
To filter, capture, view, Packets in wireshark Tool, capture 100 packet from the Ethernet: IEEE 802.3, LAN Interface and Save it.

Procedure:

* Select local Area Connection in wireshark.
* Go to Capture → option.
* Select Stop capture automatically after 100 packets
* Then Click Start capture & Save the packets.

1. Create a filter to display only TCP/UDP Packets, inspect the packets and provide the flow graph.
2. Create a filter to display only ARP packets and inspect the packets.
3. Create a Filter to display only DNS Packets and Provide the flow graph.
   * Go to capture -> option.
   * Select Stop capture auto matically after 100 Packets.
   * Then Click Start capture.
   * Search DNS Packets in search bar.
   * To see flow graph click Statistics → Flowgraph.
   * Save the packets.

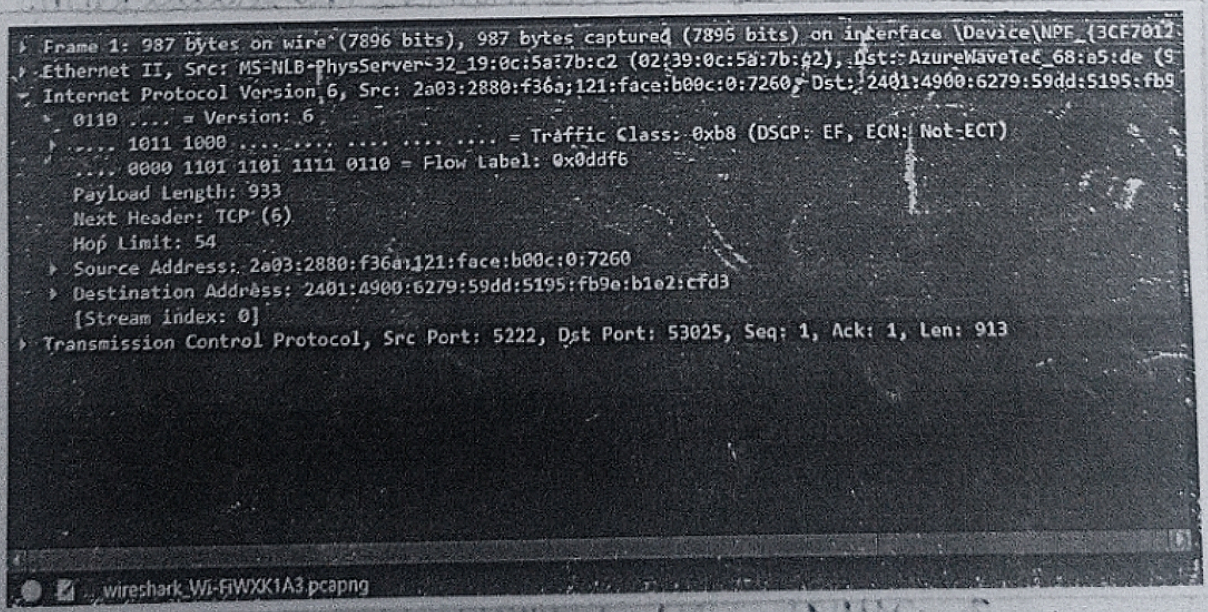
TCP:



4. Create a filter to display only HTTP packets and inspect the packets

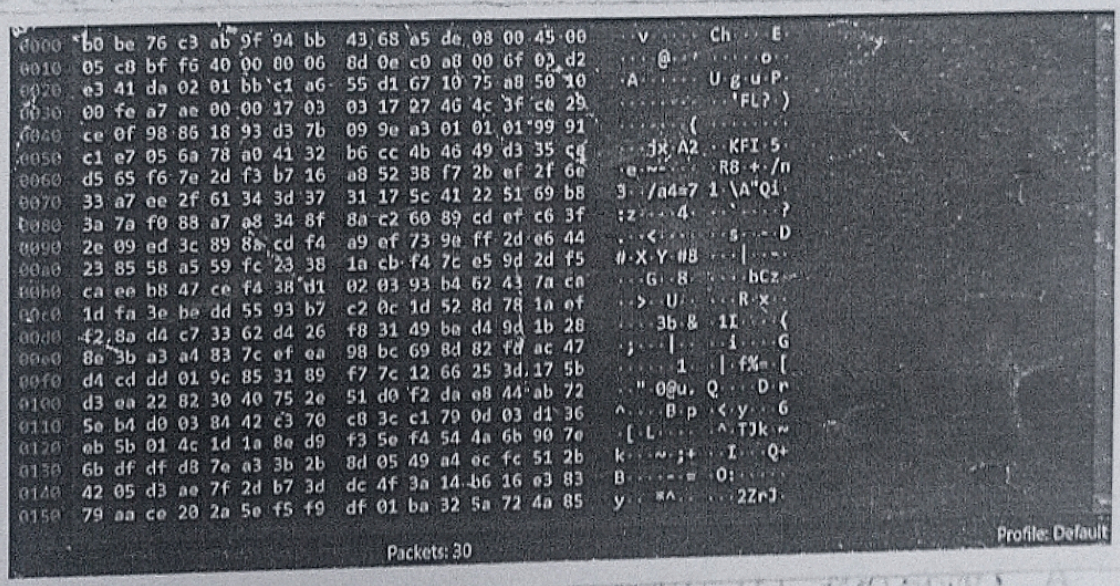
Procedure:

* Select local Area Connection in wireshark.
* Go to Capture → option.
* Select Stop capture automatically after 100 packets
* Then click start capture.
* Search HTTP packets and save packets.



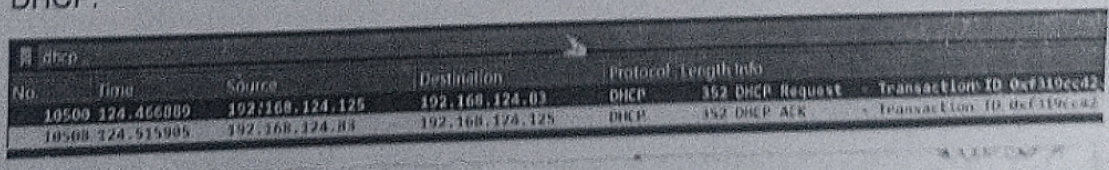
5. Create a filter to display only IP/ICMP Packet's inspect the packets.

* Select Local Area connection in Wireshark.
* Go to Capture ⇒ option.
* Select Stop capture automatically after two packets.
* Then click Start capture.
* Search ICMP/IP packet in search bar.
* Save the packets.



6. Create a filter to display only DHCP packets and inspect the packets.

DHCP:



Student observation:

1. What is promiscuous mode?

Promiscuous mode is a setting for a network interface card (NIC) where it captures all network packet that pass through it, not just those addressed to it. It is used in packet sniffing and network monitoring.

2. Does ARP packets have transport layer header? Exp

NO. ARP (Address Resolution Protocol) packets do not have a transport layer header. ARP works at Data Link layer to map an IP address to a MAC address.

3. Which transport layer protocol is used by DNS?

DNS can use: UDP on port 53 for most queries (Factor) TCP on port 53 for tasks like zone tranfer or responses exceeding 512 bytes.

4. What is a broadcast IP address?

A broadcast IP address is an address used to send data to all hosts in a network simultaneously. In IPV4, it's highest address in a subnet.

Eg. For network 192.168.1.0/24, the broadcast address is 192.168.1.255.

5. What is the port number used by HTTP protocol?

HTTP uses port 80 (TCP). For secure HTTP (HTTPS), the port is 443 (TCP).

Results

Experiments on packet capture tool. Wireshark was successfully studied.