

INDEX

NAME : P. Karsibalan STD : CSE SEC : B ROLL NO : 220701121

[illegible]

Practical - 5.

AIM:

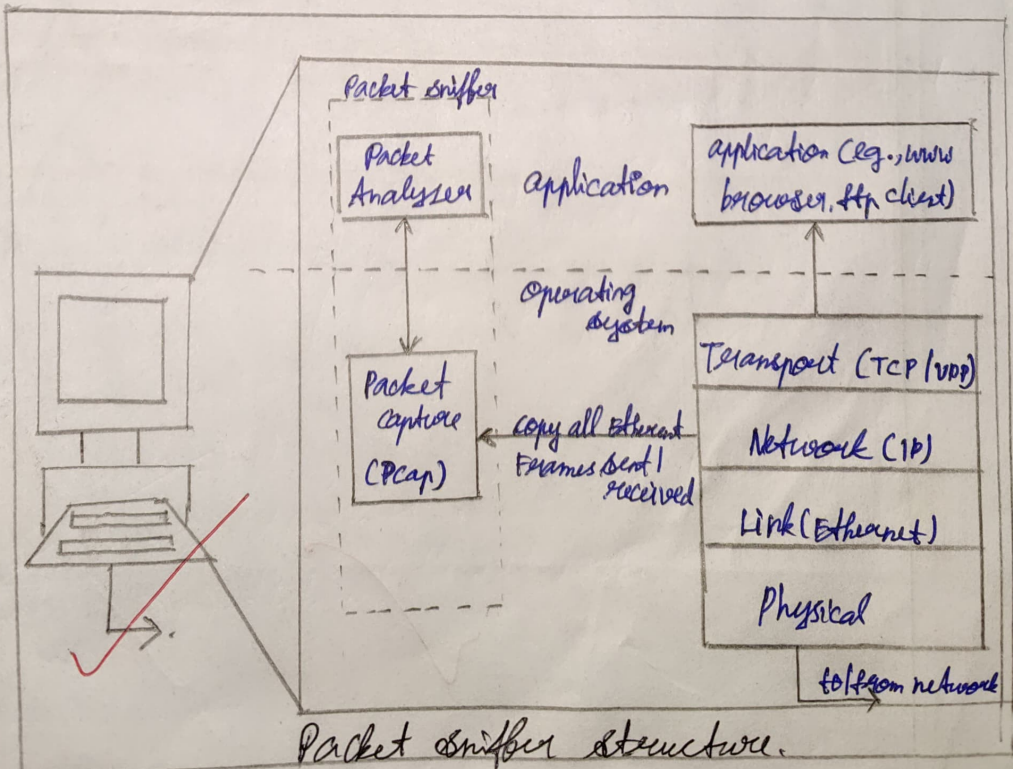
Experiments on packet capture tools: Wireshark.

Packet Sniffer:

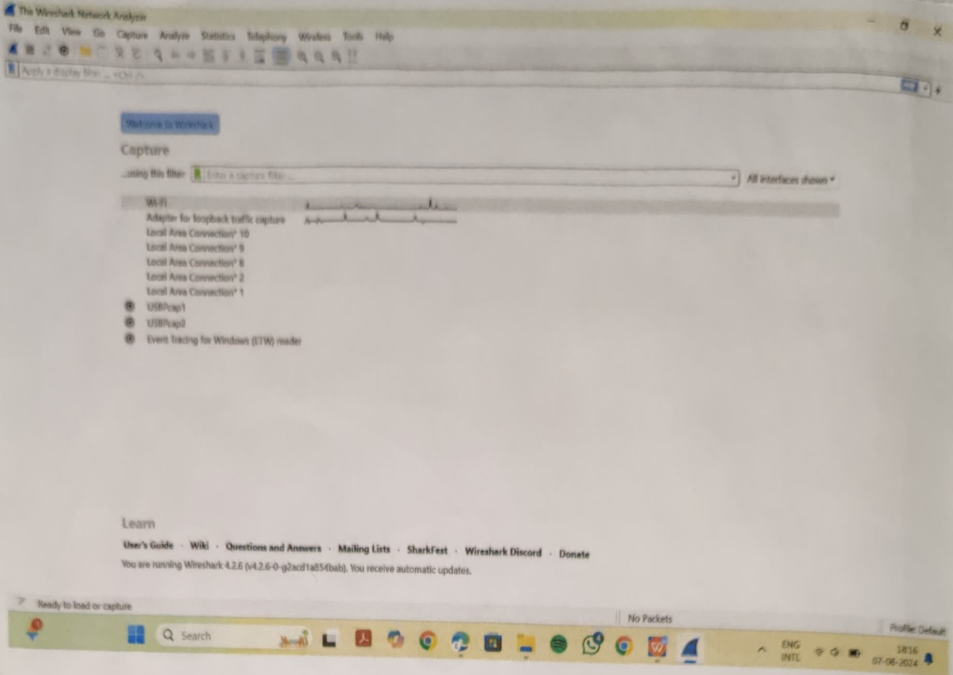
- sniffs messages being sent / received from / by your computer.
- store and display the contents of the various protocol fields in the message.
- Passive Program
 - never sends packets itself
 - no packets addressed to it
 - receives a copy of packets (sent/received)

Packet Sniffer Structure Diagnostic Tools.

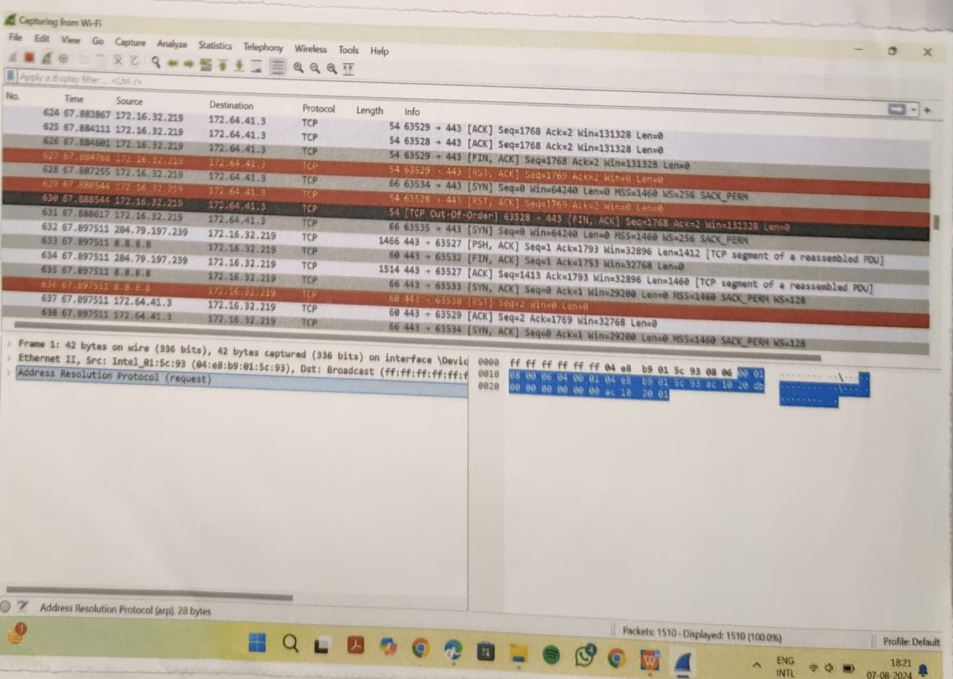
- Tcpdump
 - Eg. Acpdump - ex host 10.129.41.2 - W
 - ex 3. out.
- Wireshark.
 - Wireshark - Y ex 3. out



CAPTURING PACKETS?



PACKETS LISTS, DETAILS AND BYTES:




[illegible]

The screenshot displays the Wireshark network protocol analyzer interface. The main window shows a packet capture list on the left, with packets 1 through 20 visible. The selected packet (1) is an ICMP Echo (ping) request from 192.168.1.1 to 192.168.1.1. The packet details pane on the right shows the structure of the ICMP Echo request, including the type, code, and identifier. The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.

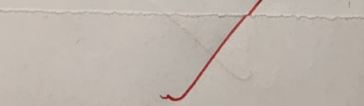
Overlaid on the interface is the 'Wireshark - Coloring Rules Default' dialog box. This dialog allows users to define or modify the display filter for a specific packet. The 'Filter' field contains the following rule: `tcp.analysis.flags & 0x10 & tcp.analysis.window_update & 0x10 & tcp.analysis.keep_alive & 0x10 & tcp.analysis.keep_alive_ack`. The 'Apply a display filter...' button is highlighted in the top left corner of the dialog.

Below the dialog box, the 'Frame 1366: 54 bytes on wire (432 bits) capture length 54 bytes (432 bits)' is visible. The packet details for this frame show it is an Ethernet II, Type II, Protocol II, and TCP Reset (RST) packet. The packet bytes pane shows the raw data in hexadecimal and ASCII.

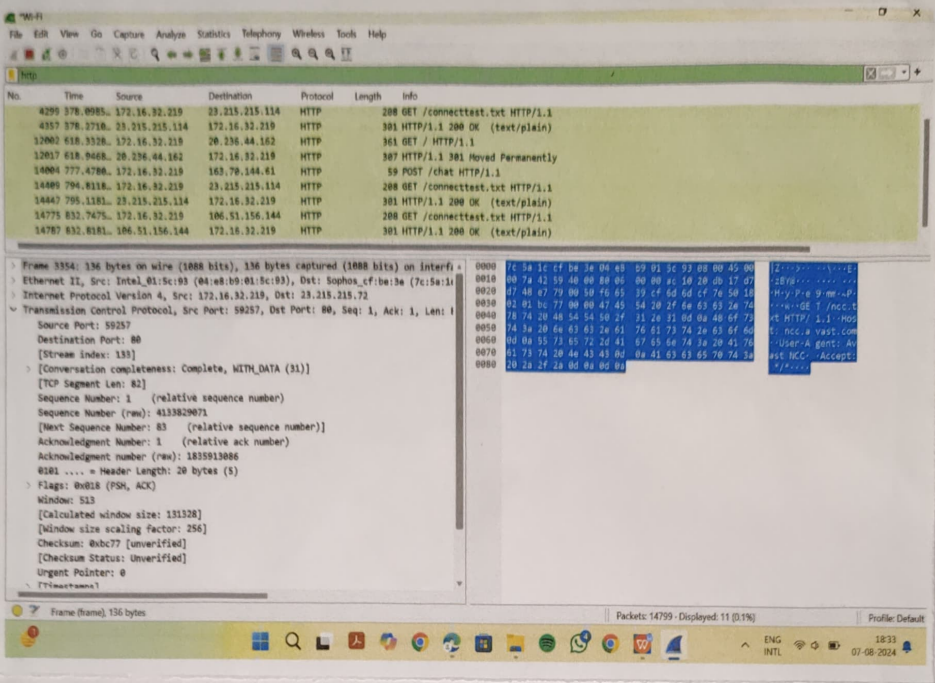
At the bottom of the screenshot, the status bar indicates 'Packets: 15967 - Displayed: 15967 (100.0%) - Dropped: 0 (0.0%) - Profile: Default'. The system tray shows the date and time as '18:42 07-08-2024'.



✓ COLORING RULES



DISPLAYING HTTP PACKETS:-

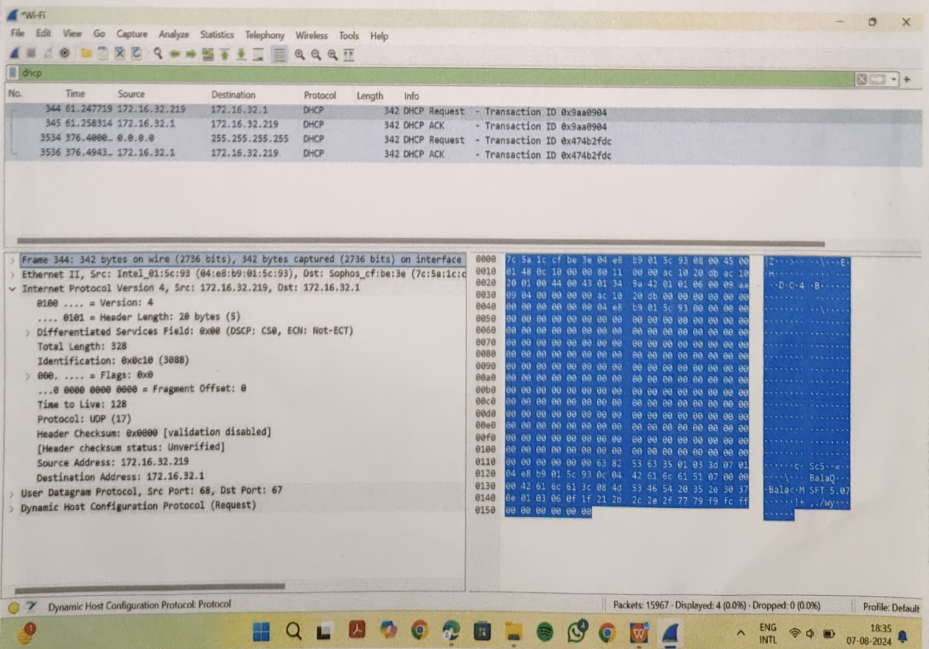


The image shows a Wireshark network traffic capture of HTTP packets. The top pane displays a list of captured packets, with packet 14787 selected. The middle pane shows the details of this packet, which is an HTTP GET request for '/connecttest.txt' from 172.16.32.219 to 106.51.156.144. The bottom pane shows the raw packet data in hexadecimal and ASCII. The status bar at the bottom indicates that 14799 packets are displayed, with 11 dropped.

No.	Time	Source	Destination	Protocol	Length	Info
4299	378.0985	172.16.32.219	172.16.32.219	HTTP	208	GET /connecttest.txt HTTP/1.1
4357	378.2710	172.16.32.219	172.16.32.219	HTTP	301	HTTP/1.1 200 OK (text/plain)
12001	618.3128	172.16.32.219	20.236.44.162	HTTP	361	GET / HTTP/1.1
12057	618.9468	20.236.44.162	172.16.32.219	HTTP	387	HTTP/1.1 301 Moved Permanently
14004	777.4786	172.16.32.219	163.79.144.41	HTTP	59	POST /chat HTTP/1.1
14480	794.8318	172.16.32.219	23.215.215.114	HTTP	208	GET /connecttest.txt HTTP/1.1
14447	795.1181	23.215.215.114	172.16.32.219	HTTP	301	HTTP/1.1 200 OK (text/plain)
14775	832.7475	172.16.32.219	106.51.156.144	HTTP	208	GET /connecttest.txt HTTP/1.1
14787	832.8181	106.51.156.144	172.16.32.219	HTTP	301	HTTP/1.1 200 OK (text/plain)

Frame 14787: 136 bytes on wire (1088 bits), 136 bytes captured (1088 bits) on interface 0
Ethernet II, Src: Intel_01:5c:93 (08:00:b0:01:5c:93), Dst: Sophos_cf:be:3e (7c:5a:11:7c:5a:11)
Internet Protocol Version 4, Src: 172.16.32.219, Dst: 106.51.156.144
Transmission Control Protocol, Src Port: 59257, Dst Port: 80, Seq: 1, Ack: 1, Len: 1
Source Port: 59257
Destination Port: 80
[Stream index: 133]
[Conversation completeness: Complete, WITH DATA (31)]
[TCP Segment Len: 82]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 4133829071
Next Sequence Number: 83 (relative sequence number)
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 1835913086
0101 = Header Length: 20 bytes (5)
Flags: 0x018 (PSH, ACK)
Window: 513
[Calculated window size: 131328]
[Window size scaling factor: 256]
Checksum: 0xb77 [unverified]
Checksum status: Unverified
Urgent Pointer: 0
[Timestamp: 0]

DISPLAY DHCP PACKETS:-



The image shows a Wireshark network traffic capture of DHCP packets. The top pane displays a list of captured packets, with packet 344 selected. The middle pane shows the details of this packet, which is a DHCP Request from 172.16.32.219 to 255.255.255.255. The bottom pane shows the raw packet data in hexadecimal and ASCII. The status bar at the bottom indicates that 15967 packets are displayed, with 4 dropped and 0.00% dropped.

No.	Time	Source	Destination	Protocol	Length	Info
344	61.247759	172.16.32.219	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x3aa9904
345	61.258514	172.16.32.219	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x3aa9904
3534	376.4600	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x47ab2fde
3536	376.4943	172.16.32.1	172.16.32.219	DHCP	342	DHCP ACK - Transaction ID 0x47ab2fde

Frame 344: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
Ethernet II, Src: Intel_01:5c:93 (08:00:b0:01:5c:93), Dst: Sophos_cf:be:3e (7c:5a:11:7c:5a:11)
Internet Protocol Version 4, Src: 172.16.32.219, Dst: 255.255.255.255
DHCP
0100 = Version: 4
... 0000 0000 0000 = Fragment Offset: 0
Time to Live: 128
Protocol: UDP (17)
Header Checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source Address: 172.16.32.1
Destination Address: 255.255.255.255
User Datagram Protocol, Src Port: 68, Dst Port: 67
Dynamic Host Configuration Protocol (Request)

Student's observation:-

- 1] what is Promiscuous mode?
Promiscuous mode is a network interface card (NIC) setting that allows card to intercept and read all network packets on network segment.
- 2] Does ARP Packets has transport layer header? Explain.
NO, ARP Packets do not have transport layer header.
- 3] which transport layer protocol is used by DNS?
DNS (Domain name system) primarily uses UDP for its transport layer protocol.
- 4] what is the port number used http Protocol?
HTTP Protocol uses port number 80 by default.
- 5] what is broadcast IP address?
It is a broadcast IP address which is used to send packets to all devices on a specific network segment.

9/8/24

Result:-

Thus, the experiments on packet capture tool Wireshark is studied and observed.