

Ex: No: 5

31.7.25

Experiment on packet capture tool
KiteShark.

AIM:

Experiments on Packet capture tool, KiteShark.

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.
 - receives 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 -> 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 wire shark:

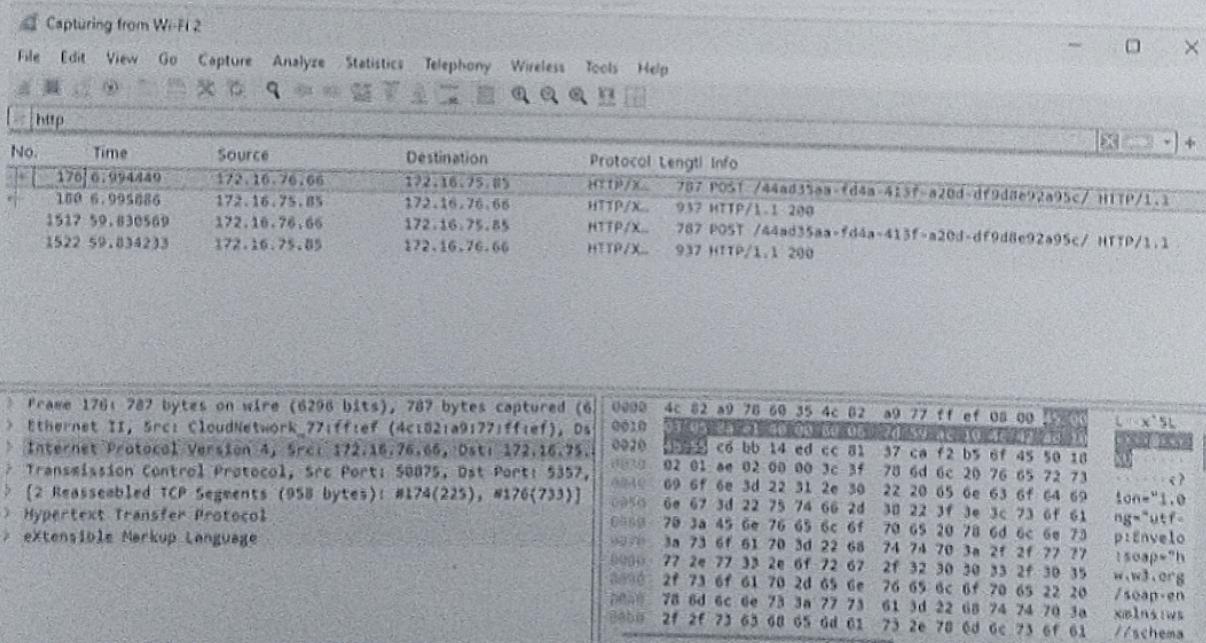
Boire8hank can be downloaded for windows or macos from its official website.

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.

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

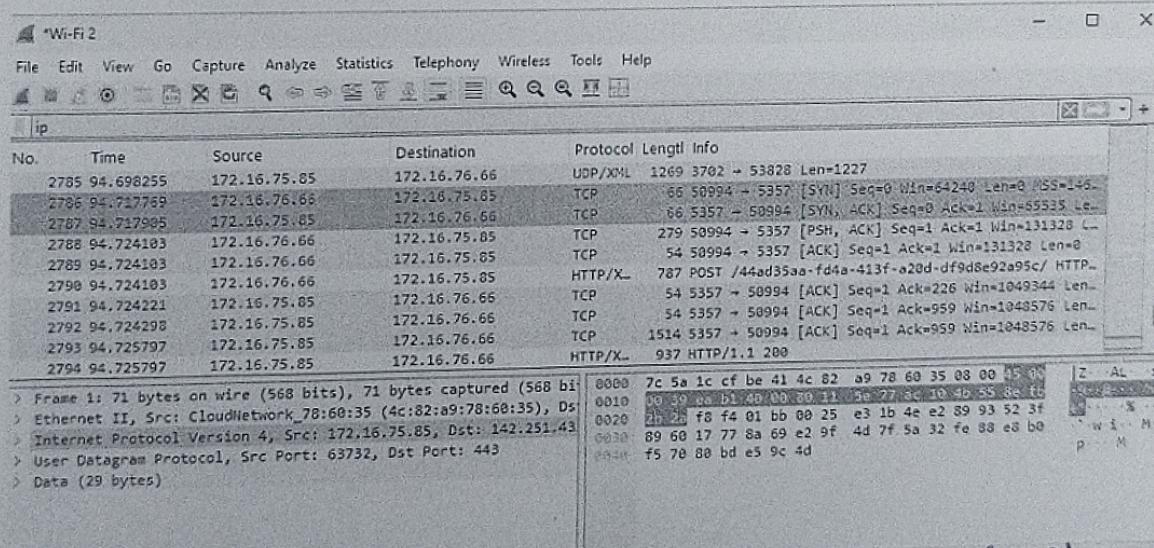


The "Packet Bytes" pane:

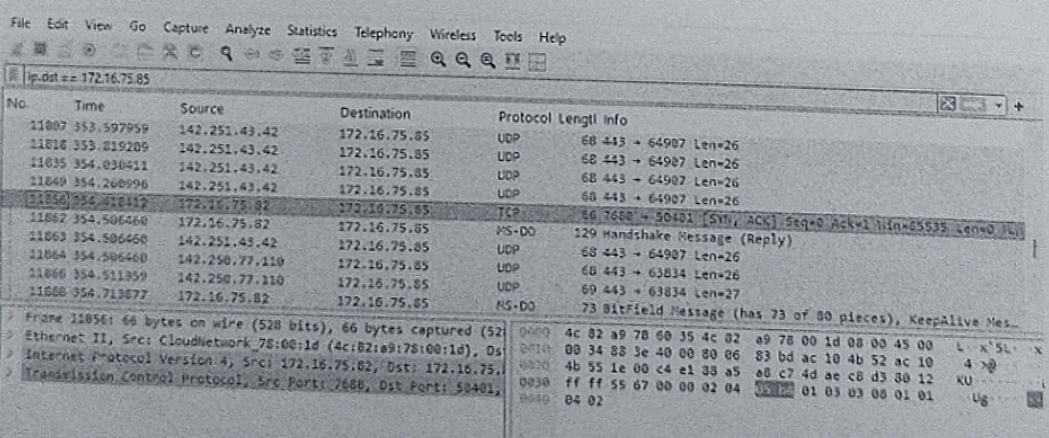
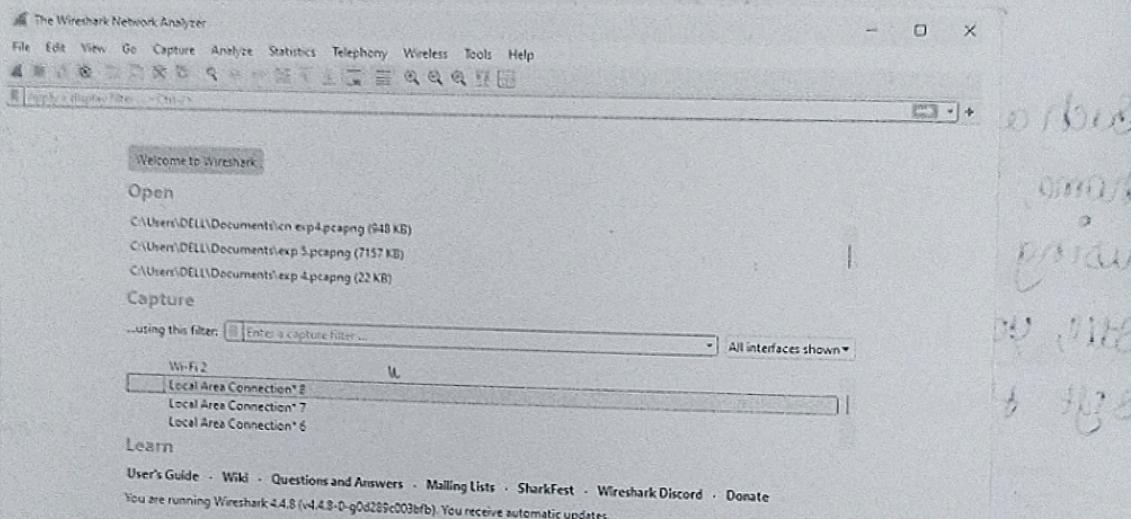
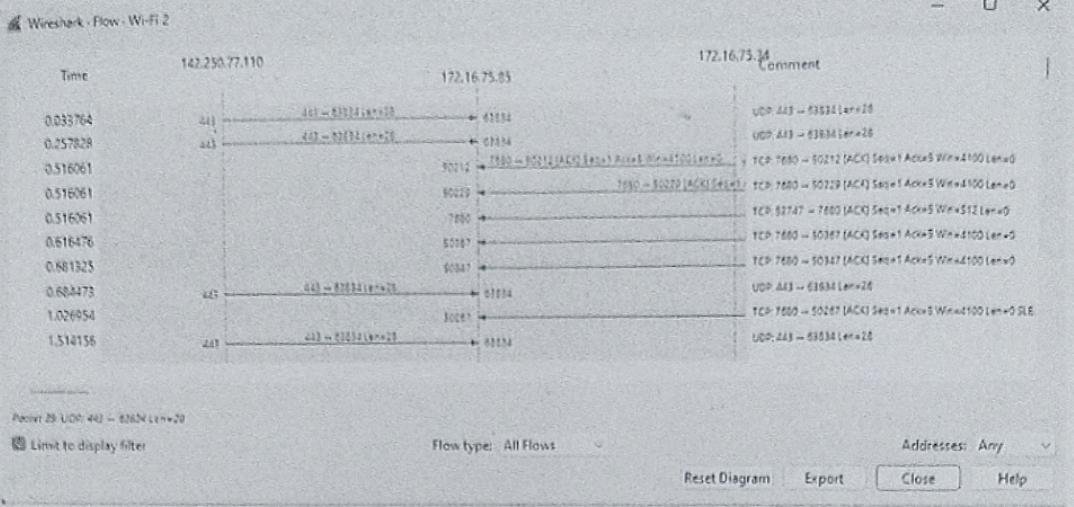
The packet bytes pane shows the data of the current packet (selected in the "packet list" pane) in a hexdump style.

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 Analyze > 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 packets that make up the conversion.



Capturing from Wi-Fi 2

tcpstream eq 35

No.	Time	Source	Destination	Protocol	Length	Info
11043	354.197582	172.16.75.85	172.16.75.82	TCP	65	50401 → 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=2460 KSYN
11056	354.418412	172.16.75.82	172.16.75.85	TCP	65	7680 → 50401 [SYN, ACK] Seq=0 Ack=1 Win=55535 Len=0 KSYN
11057	354.418546	172.16.75.85	172.16.75.82	TCP	54	50401 → 7680 [ACK] Seq=1 Ack=1 Win=131328 Len=0
11058	354.418791	172.16.75.85	172.16.75.82	MS-DO	129	Handshake Message (Request)
11062	354.506468	172.16.75.82	172.16.75.85	MS-DO	129	Handshake Message (Reply)
11065	354.506930	172.16.75.85	172.16.75.82	MS-DO	69	BitField Message (has 0 of 80 pieces)
11088	354.713877	172.16.75.82	172.16.75.85	MS-DO	73	BitField Message (has 73 of 80 pieces), KeepAlive Mes
11091	354.714411	172.16.75.85	172.16.75.82	TCP	54	50401 → 7680 [FIN, ACK] Seq=92 Ack=95 Win=131372 Len=0
11097	354.917669	172.16.75.82	172.16.75.85	TCP	54	7680 → 50401 [ACK] Seq=95 Ack=92 Win=1849600 Len=0
11098	354.917669	172.16.75.82	172.16.75.85	TCP	54	7680 → 50401 [FIN, ACK] Seq=95 Ack=92 Win=1849600 Len=0
> Frame 11043: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface CloudNetwork_78:60:35 (4c:82:a9:78:60:35), Dst: 172.16.75.82 (172.16.75.82), Src: CloudNetwork_78:60:35 (4c:82:a9:78:60:35), Dst: 172.16.75.82 (172.16.75.82), Transmission Control Protocol, Src Port: 50401, Dst Port: 7680						
0000					46	52 46 78 00 1d 4c 82 a9 78 60 35 00 00 45 00
0010					00	34 77 88 40 00 88 00 94 78 ac 10 40 55 ac 10
0020					00	4b 52 c4 e1 1e 00 4d ac c8 d2 00 00 00 00 00 02
0030					00	fa f0 8b f4 00 00 02 04 05 b4 01 03 03 08 01 01
0040					00	04 02

Packets: 17077 - Displayed: 11 (0.1%)

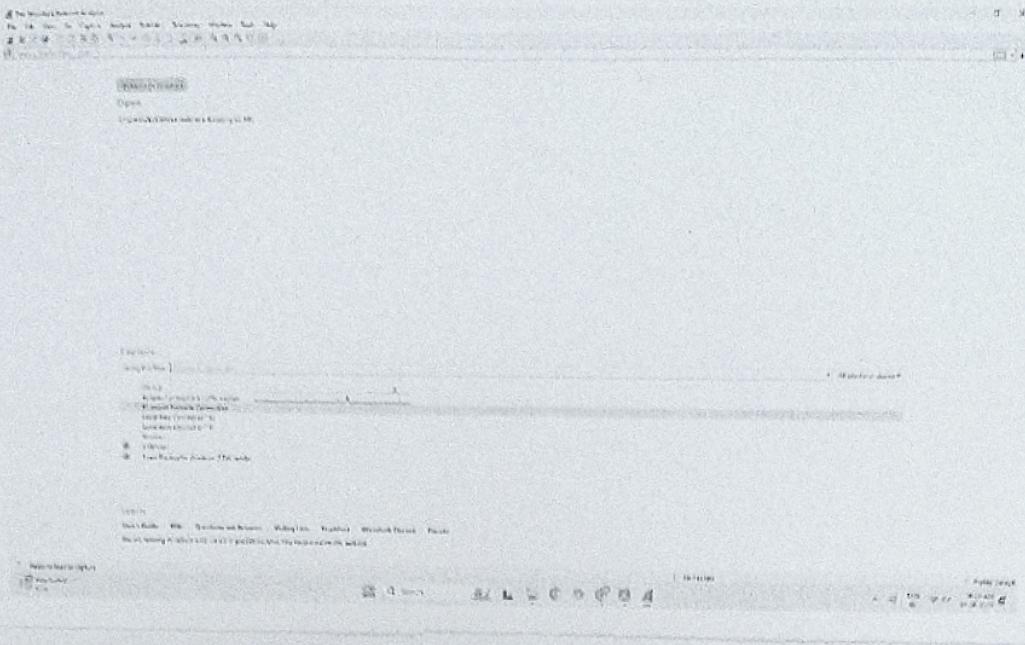
Profile: Default

dns

No.	Time	Source	Destination	Protocol	Length	Info
1628	55.292976	172.16.75.85	172.16.72.1	DNS	91	Standard query 0x75b3 A settings-win.data.microsoft.com
1843	55.300977	172.16.72.1	172.16.75.85	DNS	222	Standard query response 0x75b3 A settings-win.data.microsoft.com
2125	64.115125	172.16.75.85	172.16.72.1	DNS	74	Standard query 0xb99 A login.live.com
2126	64.138563	172.16.72.1	172.16.75.85	DNS	352	Standard query response 0xb99 A login.live.com CHNAME
2170	64.728209	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.microsoft.com
8435	255.009043	172.16.75.85	172.16.72.1	DNS	76	Standard query 0xdccc A auss.mozilla.org
8436	255.918910	172.16.75.85	172.16.72.1	DNS	90	Standard query 0xb580 A incoming.telemetry.mozilla.org
8437	255.919550	172.16.72.1	172.16.75.85	DNS	194	Standard query response 0x4ccc A auss.mozilla.org CNAME
8438	255.919550	172.16.72.1	172.16.75.85	DNS	165	Standard query response 0xb580 A incoming.telemetry.mozilla.org
> Frame 18281: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface CloudNetwork_78:60:35 (4c:82:a9:78:60:35), Dst: 172.16.72.1 (172.16.72.1), Src: User Datagram Protocol, Src Port: 53949, Dst Port: 53						
0000					7c	5a 1c cf be 41 4c 82 a9 78 60 35 03 00 45 00
0010					00	4d c6 16 00 00 80 11 89 12 ac 10 40 55 ac 10
0020					00	4b 01 d2 bd 00 35 00 39 10 53 75 b3 01 00 00 01
0030					00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0040					00	77 b9 6e 04 64 61 74 61 89 6d 69 63 72 6f 73 0f
0050					00	66 74 03 03 0f 6d 00 00 01 00 00 01

Packets: 13801 - Displayed: 26 (0.1%)

Profile: Default



Inspecting Packets:

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

tcp						
No.	Time	Source	Destination	Protocol	Length	Info
1141	32.34.6537	172.16.75.85	172.16.75.62	TCP	66	50379 → 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SRE=1
1156	32.775947	172.16.75.18	172.16.75.85	MS-DO	58	KeepAlive Message
1157	32.816677	172.16.75.85	172.16.75.18	TCP	54	50367 → 7680 [ACK] Seq=5 Ack=5 Win=512 Len=0
1159	33.361929	172.16.75.85	172.16.75.82	TCP	66	[TCP Retransmission] 50379 → 7680 [SYN] Seq=0 Win=642
1184	34.048814	172.16.75.85	142.251.10.188	TCP	55	50316 → 5228 [ACK] Seq=1 Ack=1 Win=512 Len=1
1185	34.211424	142.251.10.188	172.16.75.85	TCP	66	5228 → 50316 [ACK] Seq=1 Ack=2 Win=512 Len=1
1213	35.374890	172.16.75.85	172.16.75.82	TCP	66	[TCP Retransmission] 50379 → 7680 [SYN] Seq=0 Win=642 SRE=1
1319	39.328316	172.16.75.85	172.16.75.82	TCP	66	[TCP Retransmission] 50379 → 7680 [SYN] Seq=0 Win=642
1385	41.437994	172.16.75.85	142.250.67.42	TCP	55	50378 → 443 [ACK] Seq=1 Ack=1 Win=512 Len=1
1386	41.440815	142.250.67.42	172.16.75.85	TCP	66	443 → 50378 [ACK] Seq=1 Ack=2 Win=382 Len=0 SRE=1
> Frame 1184: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface eth0, Src: CloudNetwork_78:60:35 (4c:82:a9:78:60:35), Dst: 172.16.75.85 (172.16.75.85), Length: 440 bytes on wire (352 bits), 440 bytes captured (352 bits) on interface eth0						
> Ethernet II, Src: CloudNetwork_78:60:35 (4c:82:a9:78:60:35), Dst: 172.16.75.85 (172.16.75.85), Type: Internet Protocol Version 4 (TCP) (0x0800)						
> Internet Protocol Version 4, Src: 172.16.75.85 (172.16.75.85), Dst: 142.251.10.188 (142.251.10.188), Length: 64 bytes						
> Transmission Control Protocol, Src Port: 50316 (50316), Dst Port: 5228 (5228), Length: 52 bytes						
> Data (1 byte)						

You can also create filters from here. Just right-click 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 \rightarrow 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 \rightarrow option.
 - * Select Stop capture automatically after 100 packets.
 - * Then click Start Capture.
 - * Search DNS Packets in search bar.
 - * To see flow graph click Statistics \rightarrow Flowgraph.
 - * Save the packets.

TCP:

No.	Time	Source	Destination	Protocol	Length	Info
547	2023-03-23 10:55:23	192.168.124.121	192.168.124.83	TCP	64	53562 - 53 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM
548	2023-03-23 10:55:23	192.168.124.121	192.168.124.125	TCP	64	54 53562 - 53 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM
554	2023-03-23 10:55:23	192.168.124.125	192.168.124.83	TCP	54	54 53562 - 53 [ACK] Seq=1 Ack=1 Win=65280 Len=0
655	2023-03-23 10:55:24	192.168.124.125	192.168.124.83	TCP	56	54 53562 - 53 [PSH, ACK] Seq=1 Ack=1 Win=65280 Len=2 [TCP PDU reassembled in R50]
656	2023-03-23 10:55:24	192.168.124.125	192.168.124.83	TCP	96	Standard query 0x0f21 A encrypted-0x0f20.gastnic.com
665	2023-03-23 10:55:24	192.168.124.125	192.168.124.83	TCP	54	53 53562 [ACK] Seq=1 Ack=7 Win=65536 Len=0
667	2023-03-23 10:55:25	192.168.124.83	192.168.124.125	TCP	54	53 53562 [ACK] Seq=1 Ack=7 Win=65536 Len=0
671	2023-03-23 10:55:25	192.168.124.83	192.168.124.125	TCP	55	53 53562 [ACK] Seq=1 Ack=7 Win=65536 Len=0
677	2023-03-23 10:55:27	192.168.124.125	192.168.124.83	TCP	54	54 53562 - 53 [ACK] Seq=0z2 Ack=7 Win=65280 Len=0
684	2023-03-23 10:55:27	192.168.124.83	192.168.124.125	TCP	119	Standard query response 0x0f21 A encrypted-0x0f20.gastnic.com A 142.251.221.347
685	2023-03-23 10:55:27	192.168.124.125	192.168.124.83	TCP	54	54 53562 - 53 [FIN, ACK] Seq=47 Ack=48 Win=65536 Len=0
686	2023-03-23 10:55:27	192.168.124.83	192.168.124.125	TCP	54	53 53562 [FIN, ACK] Seq=47 Ack=48 Win=65536 Len=0
690	2023-03-23 10:55:28	192.168.124.125	192.168.124.83	TCP	54	54 53562 - 53 [ACK] Seq=48 Ack=49 Win=65280 Len=0

Stomach contents of the *Stephanolepis* larvae

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

Procedure: Tie the two strips of 10×10 cm.

* Select Local Area Connection in wireShark.

• Go to, Capture → option. local table r.

* Select Stop capture automatically after 100 packet

* Then click Start Capture.

* Search HTTP packets and save packets.

AC regular who works at refills & story

1885-1886. The first of the new species of the genus *Leptodora* was described by Dr. G. M. Allen in 1886.

Frame 1: 987 bytes on wire (7896 bits), 987 bytes captured (7896 bits) on interface \Device\NPF_{3CE701}

Frame 1: 98 bytes on wire (7856 bits), 98 bytes captured (7856 bits) on interface Intel PRO/100 MT Desktop
Ethernet II, Src: MS-NLB-PhysServer~32.19:0c:5a:7b:c2 (02:39:0c:5a:7b:c2), Dst: AzureWaveTec_68:a5:de (00:0c:68:a5:de:62)
Internet Protocol Version 6, Src: 2a03:2880:f36a:121:face:b00c:0:7260, Dst: 2401:4900:6279:59dd:5195:fb:0:110
Version: 6

0110 = Version: 6
1011 1000 = Traffic Class: 0xb8 (DSCP: EF, ECN: Not-ECT)
0000 1101 1101 1111 0110 = Flow Label: 0x0ddfb
Payload Length: 933

Payload Length: 933
Next Header: TCP (6)
Hop Limit: 54
Source Address: 2a03:2880:f36a:121:face:b00c:0:7260

► Source Address: 2a03:2880:f36a:121:face:b00c:0:7260
► Destination Address: 2401:4900:6279:59dd:5195:fb9e:b1e2:cf3
[Stream index: 0]
[Port: 5322, Dst Port: 53025, Seq: 1, Arki: 1, Len: 913]

[Stream Index: 0]
Transmission Control Protocol, Src Port: 5222, Dst Port: 53025, Seq: 1, Ack: 1, Len: 913

Wireshark Wi-Fi WXK1A3.pcapng

Wireshark_Wi-FiXX1As pcapng

Wrote all the file doing only one at a time.

1980-03-01 ✓

5. Create a filter to display only IP/ICMP Packets and inspect the packets.

- * Select Local Area Connection in Network.
 - * 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.

Packet#	Source IP	Dest IP	Protocol	Length	Time	Sequence	Data
0000	60 be 76 c3 ab 9f 94 bb	43 68 e5 de 08 00 45 00	v	Ch	E		
0010	05 c8 bf f6 40 00 a0 00	8d 0e c0 a8 00 6f 02 d2	@		o		
0020	e3 41 da 02 01 bb c1 a6	55 d1 67 10 75 a8 50 10	A		U g u P		
0030	00 fe a7 ee 00 00 17 03	03 17 27 46 4c 3f cd 25			'FLP')		
0040	ce 0f 98 85 18 93 d3 7b	09 9e a3 01 01 01 99 91			(
0050	c1 e7 05 6a 78 a0 41 32	b6 cc 4b 46 49 d3 35 c6			JK A2 KFI 5		
0060	d5 65 f6 7e 2d f3 b7 16	a8 52 38 f7 2b ef 2f 6e			R8 + /n		
0070	33 a7 ee 2f 61 34 3d 37	31 17 5c 41 22 51 69 b8			3 - /a=7 1 \A"Q1		
0080	3a 7a fa 88 a7 a8 34 8f	8a c2 60 89 cd ef c6 3f			:z - 4. ?		
0090	2e 09 ed 3c 89 8b cd f4	a9 ef 73 9e ff 2d 66 44			< - 5 - D		
00a0	23 85 58 a5 59 fc 23 38	1a cb f4 7c e5 9d 2d f5			# X - Y - # - -		
00b0	ca ee b8 47 ce f4 38 d1	02 03 93 b4 62 43 7a ca			- G - 8 - bCz -		
00c0	1d fa 3e be dd 55 93 b7	c2 0c 1d 52 8d 78 1a ef			> - U - R - x		
00d0	f2 8a d4 c7 33 62 d4 26	f8 31 49 be d4 9d 1b 28			3b & 11 - (
00e0	8e 3b a3 a4 83 7c ef ea	98 bc 69 8d 82 fd ac 47			; - - 1 - G		
00f0	d4 cd dd 01 9c 85 31 89	f7 7c 12 66 25 3d 17 5b			1. f% - [
0100	d3 ea 22 82 30 40 75 26	51 d0 f2 da e8 44 "ab 72			" Ogu. Q - D r		
0110	5e b4 d0 03 84 42 c3 70	c8 3c c1 79 0d 03 d1 36			^ - B - p < y 6		
0120	eb 5b 01 4c 1d 1a 8e d9	f3 5e f4 54 4a 6b 90 7e			[L - ^ - Tjk - ^		
0130	6b df df d8 7e a3 3b 2b	8d 05 49 a4 ec fc 51 2b			k - - + - I - Q		
0140	42 05 d3 ae 7f 2d b7 3d	dc 4f 3a 14 - b6 16 e3 83			B - - = O -		
0150	79 aa ce 20 2a 5e f5 f9	df 01 ba 32 5a 72 4a 85			y - ^ - 22rJ		

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

the packets

DHCP

dhcp						
No.	Time	Source	Destination	Protocol	Length	Info
10500	124.466880	192.168.124.125	192.168.124.03	DHCP	362	DHCP Request
10508	124.515995	192.168.124.03	192.168.124.125	DHCP	362	DHCP ACK

Student Observation: (who will be able to answer)

1. What is Promiscuous mode?
Promiscuous mode is a setting for a network interface card (NIC) where it captures all network packets that pass through it, not just the ones addressed to it. It is used in packet sniffing and network monitoring.
2. Does ARP packets have transport layer header? Explain.
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 transfer 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.