

Name :- Manav Pahilwani

Roll No :- 37

Class :- D11AD

CSS Exp 1

Output :-

## 1. ICMP

The screenshot shows a Wireshark packet capture on the 'Ethernet' interface. The packet list on the left shows several ICMP Echo (ping) requests and replies. The selected packet (No. 36798) is an ICMP Echo (ping) request from 192.168.32.1 to 8.8.8.8. The packet details pane on the right shows the 'Internet Control Message Protocol' section, indicating it's a request with ID 0x0001, sequence 480/57345, and TTL 255. The packet bytes pane on the right shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
29748	61.541498	192.168.47.220	192.168.39.163	ICMP	74	Echo (ping) request id=0x0001, seq=381/32001, ttl=128 (reply in 29752)
29752	61.541684	192.168.39.163	192.168.47.220	ICMP	74	Echo (ping) reply id=0x0001, seq=381/32001, ttl=128 (request in 29748)
30837	64.142468	192.168.39.163	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=476/56321, ttl=255 (no response found!)
34590	72.109623	192.168.32.1	192.168.39.163	ICMP	94	Destination unreachable (Host unreachable)
34591	72.109623	192.168.32.1	192.168.39.163	ICMP	94	Destination unreachable (Host unreachable)
35299	74.139977	192.168.39.163	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=476/56833, ttl=255 (no response found!)
35946	75.469451	192.168.32.1	192.168.39.163	ICMP	94	Destination unreachable (Host unreachable)
36798	77.453084	192.168.32.1	192.168.39.163	ICMP	94	Destination unreachable (Host unreachable)
36799	77.453084	192.168.32.1	192.168.39.163	ICMP	94	Destination unreachable (Host unreachable)
40435	78.572978	192.168.32.1	192.168.39.163	ICMP	94	Destination unreachable (Host unreachable)
42642	80.720799	192.168.32.1	192.168.39.163	ICMP	94	Destination unreachable (Host unreachable)
44519	84.162991	192.168.39.163	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=480/57345, ttl=255 (no response found!)
44953	85.068719	192.168.32.1	192.168.39.163	ICMP	94	Destination unreachable (Host unreachable)
47370	88.204913	192.168.32.1	192.168.39.163	ICMP	94	Destination unreachable (Host unreachable)
49384	93.516304	192.168.32.1	192.168.39.163	ICMP	94	Destination unreachable (Host unreachable)
49518	94.125397	192.168.39.163	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=482/57857, ttl=255 (no response found!)

> Frame 36798: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface \Device\NPF\_{9F42AF25-417B-4B24-8528-7FD43B570961}, id 0000 f4 6b 8c 86 48 5a c8 4f 86 fc 00 05 08 00 45 c0  
> Ethernet II, Src: Sophos\_fc:00:05 (c8:4f:86:fc:00:05), Dst: HonHaiPr\_86:48:5a (f4:6b:8c:86:48:5a)  
> Internet Protocol Version 4, Src: 192.168.32.1, Dst: 192.168.39.163  
> Internet Control Message Protocol  
0010 00 50 ef cb 00 00 40 01 c1 2c c0 a8 20 01 c0 a8  
0020 27 a3 03 01 f6 00 00 00 00 00 45 00 00 34 cc 75  
0030 40 00 7f 06 36 73 c0 a8 27 a3 0a 03 06 8d c5 06  
0040 07 6c 73 e3 ee bc 00 00 00 00 02 fa f0 4c 31  
0050 00 00 02 04 05 b4 01 03 03 08 01 01 04 02

## 2. IP address

The screenshot shows a Wireshark packet capture on the 'Ethernet' interface. The packet list on the left shows various network protocols including DNS, ARP, TCP, and UDP. The selected packet (No. 192.168.39.163) is a DNS query from 192.168.33.31 to 224.0.0.251. The packet details pane on the right shows the 'Internet Protocol Version 4' section, indicating it's a query from 192.168.33.31 to 224.0.0.251. The packet bytes pane on the right shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
1313..	227.590897	192.168.33.31	224.0.0.251	NDNS	60	Standard query response 0x0000
1313..	227.590897	Pegatron_76:72:e9	Broadcast	ARP	60	Who has 192.168.32.20? Tell 192.168.32.208
1313..	227.593059	192.168.43.106	224.0.0.251	NDNS	60	Standard query response 0x0000
1313..	227.599127	Dell_bc:b6:3e	Broadcast	ARP	60	Who has 192.168.43.119? Tell 192.168.46.72
1313..	227.607137	142.250.183.142	192.168.39.163	TLSv1.3	447	[TCP Previous segment not captured], Application Data
1313..	227.607165	192.168.39.163	142.250.183.142	TCP	66	[TCP Dup ACK 131362#1] 50518 + 443 [ACK] Seq=1270307 Ack=56541 Win=262400 Len=0 SLE=57070 SRE=57463
1313..	227.608556	142.250.199.164	192.168.39.163	TLSv1.3	889	Application Data, Application Data
1313..	227.609728	142.250.183.142	192.168.39.163	TLSv1.3	284	Application Data
1313..	227.609728	142.250.183.142	192.168.39.163	TLSv1.3	93	Application Data
1313..	227.609757	192.168.39.163	142.250.183.142	TCP	66	[TCP Dup ACK 131362#2] 50518 + 443 [ACK] Seq=1270307 Ack=56541 Win=262400 Len=0 SLE=57070 SRE=57693
1313..	227.609756	192.168.39.163	142.250.199.164	TLSv1.3	89	Application Data
1313..	227.609769	192.168.39.163	142.250.183.142	TCP	66	[TCP Dup ACK 131362#3] 50518 + 443 [ACK] Seq=1270307 Ack=56541 Win=262400 Len=0 SLE=57070 SRE=57732
1313..	227.610004	142.250.183.142	192.168.39.163	TLSv1.3	593	[TCP Fast Retransmission], Application Data
1313..	227.611230	142.250.199.164	192.168.39.163	TLSv1.3	160	Application Data, Application Data
1313..	227.611292	192.168.39.163	142.250.183.142	TLSv1.3	128	Application Data, Application Data
1313..	227.612028	192.168.39.163	142.250.199.164	TLSv1.3	93	Application Data
1313..	227.612054	192.168.45.228	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1

> Frame 1: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface \Device\NPF\_{9F42AF25-417B-4B24-8528-7FD43B570961}, id 0000 33 33 00 01 00 03 10 78 d2 44 30 a0 86 dd 60 00  
> Ethernet II, Src: ElitegPro\_44:30:a9 (10:78:d2:44:30:a9), Dst: IPv6mcast\_01:00:03 (33:33:00:01:00:03)  
> Internet Protocol Version 6, Src: fe80::e16b:7a32:408e:b9d, Dst: ff02::1:3  
> User Datagram Protocol, Src Port: 56840, Dst Port: 5355  
> Link-Local Multicast Name Resolution (query)  
0010 00 00 00 23 11 01 fe 80 00 00 00 00 00 e1 6b  
0020 7a 32 40 8e 0b 9d ff 02 00 00 00 00 00 00 00  
0030 00 00 00 01 00 03 de 08 14 eb 00 23 44 91 1e a5  
0040 00 00 00 01 00 00 00 00 00 00 09 43 44 50 4e 33  
0050 30 33 2d 32 00 00 01 00 01

### 3. HTTP

[illegible]

The screenshot displays the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The top toolbar contains icons for various functions like opening files, saving, and capturing. The main window is divided into three panes:

- Packet List:** Shows a list of captured packets. Packet 2669 is a GET request to /http. Packet 2675 is a POST request to /index.php, which is highlighted in green. The details of packet 2675 are expanded, showing the form data.
- Packet Details:** Provides a hierarchical view of the selected packet's structure. For the POST request, it shows the Content-Type as 'application/x-www-form-urlencoded' and the form data as 'email=ManavP@gmail.com' and 'password=ManavPahilwani'.
- Packet Bytes:** Displays the raw data of the selected packet in hexadecimal and ASCII format.

The status bar at the bottom indicates the current capture file is 'wireshark\_WiFi9K0ZY1.pcapng', the packet count is 26832, and the display filter is '(0.0%)'. The system clock shows 15:40 on 19-Jan-2023.

# HTTPS

For HTTPS we use tcp.port == 443

The image shows a Wireshark network capture of an HTTPS connection. The top pane displays a list of network packets. The second pane shows the details of a selected TCP packet (No. 2726), highlighting the Transmission Control Protocol (TCP) segment. The third pane shows the raw data of the packet, which is a TLS record. The details pane for the TCP segment shows the source port as 50624 and the destination port as 443. The details pane for the TLS record shows the TLS version as 1.2 and the application data as a sequence of bytes.

No.	Time	Source	Destination	Protocol	Length	Info
2726	513.231726	192.168.1.11	45.77.147.178	TCP	54	[TCP Retransmission] 50755 → 443 [FIN, ACK] Seq=582 Ack=349 Win=131584 Len=0
2726	513.232771	192.168.1.11	45.77.147.178	TCP	55	[TCP Spurious Retransmission] 50755 → 443 [ACK] Seq=581 Ack=349 Win=131584 Len=1
2726	515.811908	192.168.1.11	5.9.71.92	TCP	55	[TCP Keep-Alive] 49679 → 443 [ACK] Seq=1 Ack=1 Win=515 Len=1
2726	516.037110	5.9.71.92	192.168.1.11	TCP	54	[TCP Keep-Alive] 443 → 49679 [ACK] Seq=0 Ack=2 Win=501 Len=0
2726	516.037110	5.9.71.92	192.168.1.11	TCP	66	[TCP Keep-Alive ACK] 443 → 49679 [ACK] Seq=1 Ack=2 Win=501 Len=0 SLE=1 SRE=2
2726	516.037145	192.168.1.11	5.9.71.92	TCP	54	[TCP Dup ACK 105386] 49679 → 443 [ACK] Seq=2 Ack=1 Win=515 Len=0
2726	517.195322	192.168.1.11	54.68.110.139	TLSv1.2	166	Application Data
2726	517.195517	192.168.1.11	54.68.110.139	TLSv1.2	100	Application Data
2726	517.195600	192.168.1.11	54.68.110.139	TLSv1.2	308	Application Data
2726	517.471616	54.68.110.139	192.168.1.11	TCP	54	443 → 50247 [ACK] Seq=9160 Ack=6350 Win=44032 Len=0
2726	517.471616	54.68.110.139	192.168.1.11	TCP	54	443 → 50247 [ACK] Seq=9160 Ack=6404 Win=44032 Len=0
2726	517.471616	54.68.110.139	192.168.1.11	TCP	54	443 → 50247 [ACK] Seq=9160 Ack=6658 Win=45312 Len=0
2726	517.471616	54.68.110.139	192.168.1.11	TLSv1.2	100	Application Data
2726	517.471616	54.68.110.139	192.168.1.11	TLSv1.2	286	Application Data
2726	517.471616	54.68.110.139	192.168.1.11	TLSv1.2	92	Application Data
2726	517.471778	192.168.1.11	54.68.110.139	TLSv1.2	54	50247 → 443 [ACK] Seq=6658 Ack=9476 Win=131072 Len=0
2726	517.473455	192.168.1.11	54.68.110.139	TLSv1.2	96	Application Data
2726	517.844154	192.168.1.11	54.68.110.139	TCP	96	[TCP Retransmission] 50247 → 443 [PSH, ACK] Seq=6658 Ack=9476 Win=131072 Len=42
2726	517.847348	54.68.110.139	192.168.1.11	TCP	54	443 → 50247 [ACK] Seq=9476 Ack=6700 Win=45312 Len=0

Frame 266987: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF{...} Ethernet II, Src: IntelCor\_87:80:11 (a8:7e:ea:87:80:11), Dst: PPCBroad\_7b:c8:56 (64:fb:92:7b:c8:56) Internet Protocol Version 4, Src: 192.168.1.11, Dst: 74.214.196.131 Transmission Control Protocol, Src Port: 50624, Dst Port: 443, Seq: 582, Ack: 4486, Len: 0

Source Port: 50624  
Destination Port: 443  
[Stream index: 803]  
[Conversation completeness: Complete, WITH\_DATA (63)]  
[TCP Segment Len: 0]  
Sequence Number: 582 (relative sequence number)  
Sequence Number (raw): 4276641955  
[Next Sequence Number: 583 (relative sequence number)]  
Acknowledgment Number: 4486 (relative ack number)  
Acknowledgment number (raw): 984846202  
0101 .... = Header Length: 20 bytes (5)  
Flags: 0x011 (FIN, ACK)  
Window: 512  
[Calculated window size: 131072]  
[Window size scaling factor: 256]

# UDP

The image shows a Wireshark network capture of a UDP connection. The top pane displays a list of network packets. The second pane shows the details of a selected UDP packet (No. 2758), highlighting the User Datagram Protocol (UDP) segment. The third pane shows the raw data of the packet, which is a DNS query. The details pane for the UDP segment shows the source port as 52392 and the destination port as 53. The details pane for the DNS query shows the query type as A and the query data as a sequence of bytes.

No.	Time	Source	Destination	Protocol	Length	Info
2758	602.586421	142.250.199.142	192.168.1.11	QUIC	290	Protected Payload (KP0)
2758	602.586778	192.168.1.11	142.250.199.142	QUIC	81	Protected Payload (KP0), DCID=e09d4d6eb9ce56d0
2758	602.587063	192.168.1.11	142.250.199.142	QUIC	75	Protected Payload (KP0), DCID=e09d4d6eb9ce56d0
2758	602.601532	142.250.199.142	192.168.1.11	QUIC	67	Protected Payload (KP0)
2758	611.324135	192.168.1.11	142.250.183.195	QUIC	1292	Initial, DCID=b919e3c7a9bb02e7, PKN: 1, PING, CRYPTO, PADDING, PING, PADDING, CRYPTO, CRYPTO, PING
2758	611.324548	192.168.1.11	142.250.183.195	QUIC	120	0-RTT, DCID=b919e3c7a9bb02e7
2758	611.325050	192.168.1.11	142.250.183.195	QUIC	464	0-RTT, DCID=b919e3c7a9bb02e7
2758	611.357614	142.250.183.195	192.168.1.11	QUIC	1292	Initial, SCID=f919e3c7a9bb02e7, PKN: 1, ACK, PADDING
2758	611.392065	142.250.183.195	192.168.1.11	QUIC	1292	Protected Payload (KP0)
2759	611.392065	142.250.183.195	192.168.1.11	QUIC	840	Protected Payload (KP0)
2759	611.392065	142.250.183.195	192.168.1.11	QUIC	210	Protected Payload (KP0)
2759	611.392065	142.250.183.195	192.168.1.11	QUIC	67	Protected Payload (KP0)
2759	611.392065	142.250.183.195	192.168.1.11	QUIC	67	Protected Payload (KP0)
2759	611.393290	192.168.1.11	142.250.183.195	QUIC	121	Handshake, DCID=f919e3c7a9bb02e7
2759	611.393560	192.168.1.11	142.250.183.195	QUIC	75	Protected Payload (KP0), DCID=f919e3c7a9bb02e7
2759	611.393839	192.168.1.11	142.250.183.195	QUIC	75	Protected Payload (KP0), DCID=f919e3c7a9bb02e7
2759	611.398680	142.250.183.195	192.168.1.11	QUIC	162	Protected Payload (KP0)
2759	611.429421	192.168.1.11	142.250.183.195	QUIC	75	Protected Payload (KP0), DCID=f919e3c7a9bb02e7

Frame 1: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface \Device\NPF{...} Ethernet II, Src: IntelCor\_87:80:11 (a8:7e:ea:87:80:11), Dst: PPCBroad\_7b:c8:56 (64:fb:92:7b:c8:56) Internet Protocol Version 4, Src: 192.168.1.11, Dst: 103.170.80.3 User Datagram Protocol, Src Port: 52392, Dst Port: 53

Source Port: 52392  
Destination Port: 53  
Length: 39  
Checksum: 0x7999 [unverified]  
[Checksum Status: Unverified]  
[Stream index: 0]  
[Timestamps]  
UDP payload (31 bytes)  
Domain Name System (query)