

## practical - 5

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 fields in the messages.

\* passive program

- never sends packets itself
- no packets addressed to it
- receives a copy of all packets (sent/received).

## Packet Sniffer Structure Diagnostic tools

\* Tcp dump

- Eg: tcpdump -e -e host

10.129.41.2 - w.exe 3.out

\* wire shark

- wireshark -r.exe 3.out

# CAPTURING AND ANALYSING PACKETS USING WIRESHARK TOOL

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
129	13.898106	fe80::5577:584:933b...	ff02::fb	MDNS	134	Standard query resp
130	13.898106	172.16.10.219	224.0.0.251	MDNS	114	Standard query resp
131	13.898106	172.16.10.219	224.0.0.251	MDNS	114	Standard query resp
132	14.101206	52.168.117.169	172.16.9.230	TLSv1.2	105	Change Cipher Spec,
133	14.101315	172.16.9.230	52.168.117.169	TCP	54	65096 → 443 [ACK] S
134	14.102389	172.16.9.230	52.168.117.169	TLSv1.2	512	Application Data
135	14.102505	172.16.9.230	52.168.117.169	TLSv1.2	772	Application Data
136	14.105521	52.168.117.169	172.16.9.230	TCP	60	443 → 65096 [ACK] S
137	14.105521	52.168.117.169	172.16.9.230	TCP	60	443 → 65096 [ACK] S
138	14.120123	GigaByteTech_0c:b4:...	Broadcast	ARP	60	Who has 172.16.8.68
139	14.261981	172.16.9.230	172.16.11.255	UDP	186	58377 → 51007 Len=1

Frame 1: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface 0

Ethernet II, Src: Intel\_84:28:58 (94:e7:0b:84:28:58), Dst: 01:00:00:00:00:00

Internet Protocol Version 4, Src: 172.16.9.230, Dst: 172.16.11.255

Transmission Control Protocol, Src Port: 50261, Dst Port: 51007

Transport Layer Security

0000 7c 5a 1c cf be 45 94 e7 0b 84 28 58 08 00 45

0010 00 4b 77 91 40 00 80 06 00 00 ac 10 09 e6 14

0020 2c 4e c4 55 01 bb 42 3f 86 60 9c ac 9a dd 50

0030 02 00 f7 41 00 00 17 83 03 00 1e 00 00 00

0040 00 00 b0 3e 3d 73 29 bf 90 b7 2a 7f 3b fb 80

0050 06 bd a6 f2 eb 6d af a5 38

wireshark\_Wi-FiFLV3R2.pcapng

Packets: 139 · Displayed: 139 (100.0%) · Dropped: 0 (0.0%) Profile: Default

Create a Filter to display only TCP/UDP packets, inspect the packets and provide the flow graph

Wi-Fi

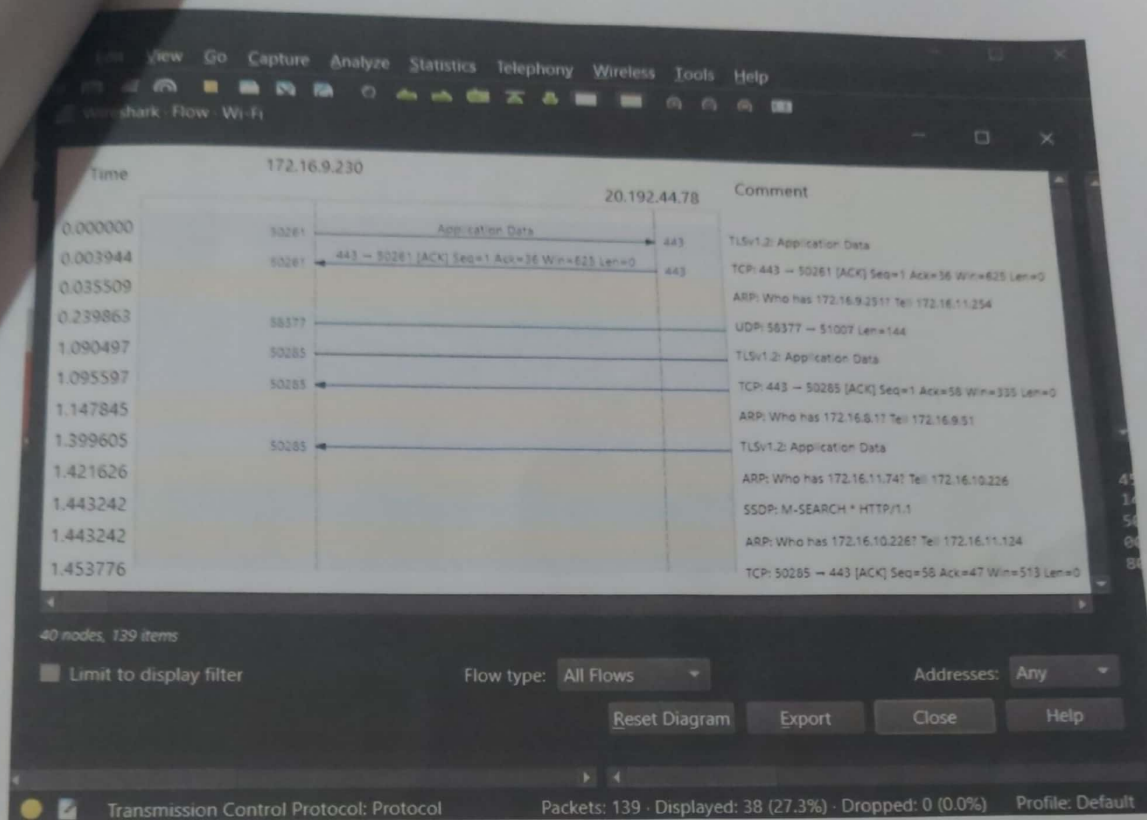
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.16.9.230	20.192.44.78	TLSv1.2	89	Application Data
2	0.003944	20.192.44.78	172.16.9.230	TCP	60	443 → 50261 [ACK] S
5	1.090497	172.16.9.230	4.195.14.14	TLSv1.2	111	Application Data
6	1.095597	4.195.14.14	172.16.9.230	TCP	60	443 → 50285 [ACK] S
8	1.399605	4.195.14.14	172.16.9.230	TLSv1.2	100	Application Data
12	1.453776	172.16.9.230	4.195.14.14	TCP	54	50285 → 443 [ACK] S
16	3.381788	172.16.9.230	40.99.9.34	TCP	54	50536 → 443 [FIN, A
22	5.044442	172.16.9.230	23.223.244.137	TCP	54	50523 → 443 [FIN, A
25	5.299095	172.16.9.230	23.223.244.137	TCP	54	50531 → 443 [RST, A
26	5.299112	172.16.9.230	13.107.6.254	TCP	54	50540 → 443 [RST, A
27	5.299112	172.16.9.230	204.79.197.254	TCP	54	50541 → 443 [RST, A
28	5.299231	172.16.9.230	23.223.244.137	TCP	54	50534 → 443 [RST, A

▶ Frame 1: 89 bytes on wire (712 bits), 89 bytes captured on interface (712 bits) on 0:00:00:00:00:00  
▶ Ethernet II, Src: Intel\_84:28:58 (94:e7:0b:84:28:58), Dst: 00:00:00:00:00:00  
▶ Internet Protocol Version 4, Src: 172.16.9.230, Dst: 20.192.44.78  
▶ Transmission Control Protocol, Src Port: 50261, Dst Port: 443, Seq: 172169230, Win: 0, Len: 89  
▶ Transport Layer Security  
0000 7c 5a 1c cf be 45 94 e7 0b 84 28 58 08 00 45  
0010 00 4b 77 91 40 00 80 06 00 00 ac 10 09 e6 14  
0020 2c 4e c4 55 01 bb 42 3f 86 60 9c ac 9a dd 50  
0030 02 00 f7 41 00 00 17 03 03 00 1e 00 00 00 00  
0040 00 00 b0 3e 3d 73 29 bf 90 b7 2a 7f 3b fb 80  
0050 06 bd a6 f2 eb 6d af a5 38

Transmission Control Protocol: Protocol Packets: 139 · Displayed: 38 (27.3%) · Dropped: 0 (0.0%) Profile: Default







The image shows a Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons for file operations, navigation, and analysis.

The main window displays a list of captured packets. The first column shows the packet number (No.), followed by time, source IP, destination IP, protocol, length, and a brief information snippet. The selected packet is #62, which is an HTTP GET request from 172.16.9.230 to 34.104.35.123.

No.	Time	Source	Destination	Protocol	Length	Info
62	1.333759	172.16.9.230	34.104.35.123	HTTP	520	GET /edgedl/diffgen
85	1.587342	34.104.35.123	172.16.9.230	HTTP	692	HTTP/1.1 416 Request
89	1.589990	172.16.9.230	34.104.35.123	HTTP	500	HEAD /edgedl/diffgen
103	1.681359	34.104.35.123	172.16.9.230	HTTP	707	HTTP/1.1 200 OK
115	1.735861	172.16.9.230	34.104.35.123	HTTP	520	GET /edgedl/diffgen
146	2.610929	34.104.35.123	172.16.9.230	HTTP	692	HTTP/1.1 416 Request
155	2.613199	172.16.9.230	34.104.35.123	HTTP	500	HEAD /edgedl/diffgen
166	2.928873	34.104.35.123	172.16.9.230	HTTP	707	HTTP/1.1 200 OK
184	2.992602	172.16.9.230	34.104.35.123	HTTP	520	GET /edgedl/diffgen
208	4.051452	34.104.35.123	172.16.9.230	HTTP	692	HTTP/1.1 416 Request
212	4.053466	172.16.9.230	34.104.35.123	HTTP	500	HEAD /edgedl/diffgen
217	4.252037	34.104.35.123	172.16.9.230	HTTP	668	HTTP/1.1 200 OK

Below the packet list, the details pane for the selected packet (Frame 62) is expanded, showing the following layers:

- Ethernet II, Src: Intel\_84:28:58 (94:e7:0b:84:28:58), Dst: 34:104:35:123
- Internet Protocol Version 4, Src: 172.16.9.230, Dst: 34.104.35.123
- Transmission Control Protocol, Src Port: 65107, Dst Port: 80
- Hypertext Transfer Protocol

The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII format. The first few bytes are 7c 5a 1c cf be 45 94 e7 0b 84 28 58 00 00, which correspond to the Ethernet II header fields.

At the bottom right, summary statistics are displayed: Packets: 791 · Displayed: 24 (3.0%) · Dropped: 0 (0.0%). The profile is set to Default.

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 main packet list pane shows a list of captured packets. Packet 62 is selected, which is an HTTP GET request to /edged1/diffgen. The packet details pane on the right shows the structure of the selected packet, including Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol. The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
43	0.829429	172.16.11.92	224.0.0.251	MDNS	443	Standard query 0x00
47	0.968831	172.16.9.230	172.16.11.255	UDP	186	58377 → 51007 Len=1
49	1.034289	172.16.11.118	224.0.0.251	MDNS	188	Standard query resp
54	1.034289	172.16.8.218	224.0.0.251	MDNS	200	Standard query resp
56	1.129812	172.16.11.92	224.0.0.251	MDNS	450	Standard query 0x00
61	1.331880	172.16.11.92	224.0.0.251	MDNS	450	Standard query 0x00
62	1.333759	172.16.9.230	34.104.35.123	HTTP	520	GET /edged1/diffgen
68	1.539068	172.16.8.218	224.0.0.251	MDNS	266	Standard query resp
71	1.539068	172.16.11.92	224.0.0.251	MDNS	450	Standard query 0x00
72	1.553103	172.16.11.92	224.0.0.251	MDNS	258	Standard query resp
74	1.587342	20.198.119.143	172.16.9.230	TCP	60	443 → 65184 [ACK] S
75	1.587342	20.198.119.143	172.16.9.230	TLSv1.2	105	Change Cipher Spec

Frame 62: 520 bytes on wire (4160 bits), 520 byte captured [0] (4160 bits) on interface 0  
 Ethernet II, Src: Intel\_84:28:58 (94:e7:0b:84:28:58), Dst: 01:00:0c:00:00:00  
 Internet Protocol Version 4, Src: 172.16.9.230, Dst: 34.104.35.123  
 Transmission Control Protocol, Src Port: 65107, Dst Port: 80  
 Hypertext Transfer Protocol

0000 7c 5a 1c cf be 45 94 e7 0b 84 28 58 08 00  
 0010 01 fa 90 bb 40 00 80 06 00 00 ac 10 09 e6  
 0020 23 7b fe 53 00 00 cf 42 57 fe 87 35 12 eb  
 0030 01 fe fd c5 00 00 47 45 54 20 2f 65 64 67  
 0040 6c 2f 64 69 66 66 67 65 6e 2d 70 75 66 68  
 0050 2f 68 66 6e 6b 70 69 6d 6c 68 68 67 69 65  
 0060 64 67 66 65 6d 6a 68 6f 66 6d 66 62 6c 6d  
 0070 62 2f 31 2e 62 31 37 36 61 30 63 33 61 31  
 0080 64 62 63 30 62 34 63 38 65 33 38 34 64 66  
 0090 38 31 33 36 63 32 39 32 65 63 38 61 38 63  
 00a0 35 38 30 31 34 61 38 32 62 37 39 37 64 30  
 00b0 39 38 33 38 2f 31 2e 64 36 38 66 31 66 64  
 00c0 30 65 64 32 64 66 37 34 61 64 31 33 30 37  
 00d0 65 39 64 34 36 35 30 37 35 62 65 33 38 65

Packets: 791 · Displayed: 591 (74.7%) · Dropped: 0 (0.0%) Profile: Default

Result:

Thus the experiment is successfully executed and output is verified

*Done*  
17/8/24