

Date: 26/08/2024

Lab Practical #08:

Study Packet capture and header analysis by Wireshark (HTTP, TCP, UDP, IP, etc.)

Practical Assignment #08:

1. Explain usage of Wireshark tool.

- **Capture Traffic:** Start capturing network traffic by selecting the appropriate network interface. **Apply Filters:** Use capture filters (before capturing) or display filters (after capturing) to focus on specific traffic, like http for HTTP traffic or ip.addr == 192.168.1.1 for traffic to/from a specific IP.
- **Analyze Packets:** Examine packet details, including protocol layers, headers, and payloads. Expand sections for in-depth analysis.
- **Follow Streams:** Use the "Follow TCP/UDP Stream" feature to view continuous data exchanges between endpoints.
- **Identify Issues:** Spot anomalies, such as retransmissions, duplicate packets, or protocol errors, to diagnose network problems.
- **Export Data:** Save captured data in various formats, or export specific packets for further analysis.
- **Use Statistics:** Access tools like "Protocol Hierarchy," "Conversations," and "Endpoint" statistics for summary views of the traffic.
- **Customize Views:** Colorize packets and customize columns to highlight important information for easier analysis.
- **Decrypt SSL/TLS Traffic:** If you have the right keys, decrypt SSL/TLS traffic for deeper inspection. **Automate Tasks:** Use command-line tools like T-shark for automated packet capturing and analysis.

2. Packet capture and header analysis by Wireshark (HTTP, TCP, UDP, IP, etc.)

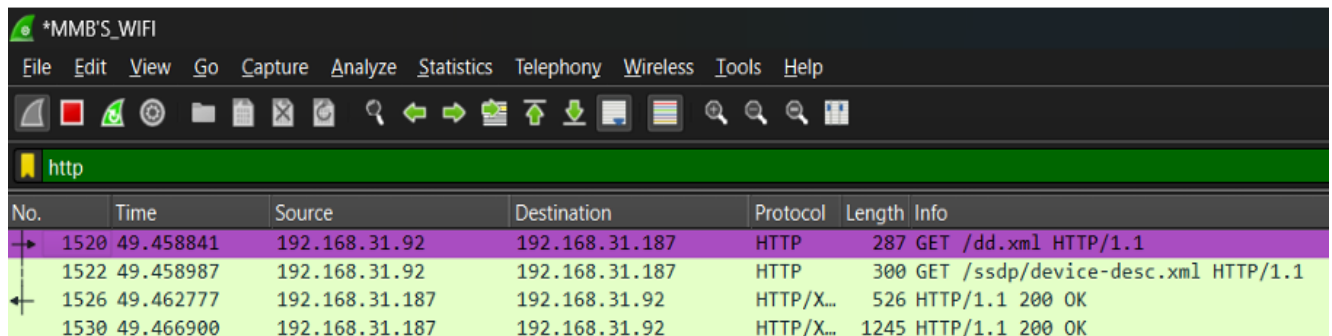
⇒ Steps Of Packet capture and header analysis by Wireshark:

- Install and Launch Wireshark
 - Download and Install: Get Wireshark from its official website. Launch Wireshark: Open the application after installation.
- Start Packet Capture
 - Select Network Interface: Choose the network interface you want to monitor (e.g., Wi-Fi, Ethernet). You will see a list of interfaces with activity graphs.
 - Begin Capturing: Click the "Start Capturing Packets" button (the shark fin icon) to begin capturing packets.
- Generate Network Traffic
 - While Wireshark is capturing, generate some network traffic related to the protocols you're interested in (e.g., visit a website for HTTP traffic, use a network application for TCP/UDP traffic).
- Stop Capture
 - Once you've captured enough packets, click the red stop button to stop capturing.
- Filter Packets
 - Apply Protocol Filters: Use the filter bar at the top to focus on specific protocols. For example: HTTP: Type http in the filter bar.
 - TCP: Type tcp.

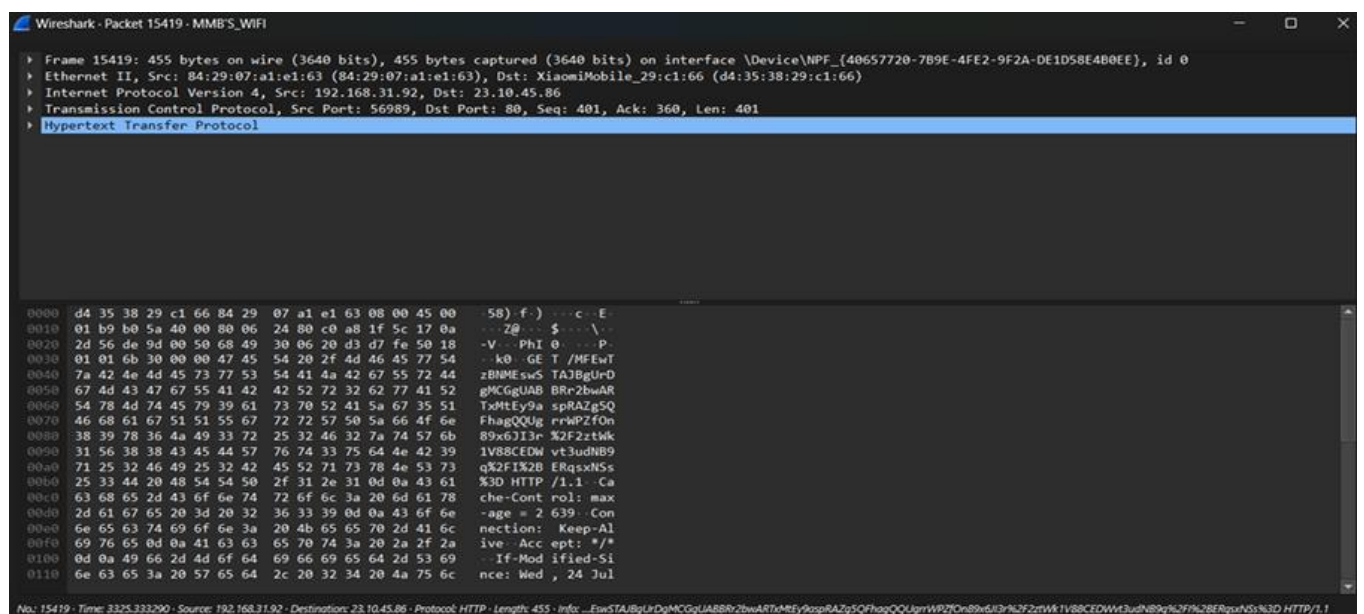
Date: 26/08/2024

- DP: Type udp.
- IP: Type ip.
- Apply Filter: Press Enter after typing the filter to view only the relevant packets. ➤
- 6. Select and Analyze Packets
- Packet List Pane: This pane shows a summary of captured packets, including time, source, destination, protocol, and length.
- Packet Details Pane: Click on a packet in the list to see its details in the middle pane. This pane displays a hierarchical view of the packet's headers.

HTTP:



No.	Time	Source	Destination	Protocol	Length	Info
1520	49.458841	192.168.31.92	192.168.31.187	HTTP	287	GET /dd.xml HTTP/1.1
1522	49.458987	192.168.31.92	192.168.31.187	HTTP	300	GET /ssdp/device-desc.xml HTTP/1.1
1526	49.462777	192.168.31.187	192.168.31.92	HTTP/X...	526	HTTP/1.1 200 OK
1530	49.466900	192.168.31.187	192.168.31.92	HTTP/X...	1245	HTTP/1.1 200 OK



Wireshark - Packet 15419 - MMB'S_WIFI

Frame 15419: 455 bytes on wire (3640 bits), 455 bytes captured (3640 bits) on interface \Device\NPF_{40657720-7B9E-4FE2-9F2A-DE1D58E4B0EE}, id 0

Ethernet II, Src: 84:29:07:a1:e1:63 (84:29:07:a1:e1:63), Dst: XiaomiMobile_29:c1:66 (d4:35:38:29:c1:66)

Internet Protocol Version 4, Src: 192.168.31.92, Dst: 23.10.45.86

Transmission Control Protocol, Src Port: 56989, Dst Port: 80, Seq: 401, Ack: 360, Len: 401

Hypertext Transfer Protocol

```

0000  d4 35 38 29 c1 66 84 29 07 a1 e1 63 08 00 45 00  (S) f) ... c E
0010  01 b9 b0 5a 40 00 80 06 24 80 c0 a8 1f 5c 17 0a  ...Z@... $ ... \
0020  2d 56 de 9d 00 50 68 49 30 06 20 d3 d7 fe 50 18  -V...PHI 0...P
0030  01 01 6b 30 00 00 47 45 54 20 2f 4d 46 45 77 54  -k0-GE T /MFEwT
0040  7a 42 4e 4d 45 73 77 53 54 41 4a 42 67 55 72 44  zBNMeswS TAjBgUrD
0050  67 4d 43 47 67 55 41 42 42 52 72 32 62 77 41 52  gMCGGUAB BRr2bwAR
0060  54 78 4d 74 45 79 39 61 73 70 52 41 5a 67 35 51  TxMTEy9a spRAZgSQ
0070  46 68 61 67 51 51 55 67 72 72 57 50 5a 66 4f 6e  FhagQQUg rrwPZFOn
0080  38 39 78 36 4a 49 33 72 25 32 46 32 7a 74 57 6b  89x6JI3r %2F2ztWk
0090  31 56 38 38 43 45 44 57 76 74 33 75 64 4e 42 39  1V88CEDW vt3udNB9
00a0  71 25 32 46 49 25 32 42 45 52 71 73 78 4e 53 73  q%2F1K2B ERqpxNSs
00b0  25 33 44 20 48 54 54 50 2f 31 2e 31 0d 0a 43 61  %3D HTTP /1.1 -Ca
00c0  63 68 65 2d 43 6f 6e 74 72 6f 6c 3a 20 6d 61 78  che-Cont rol: max
00d0  2d 61 67 65 20 3d 20 32 36 33 39 0d 0a 43 6f 6e  -age = 2 639: Con
00e0  6e 65 63 74 69 6f 6e 3a 20 4b 65 65 70 2d 41 6c  nection: Keep-Al
00f0  69 76 65 0d 0a 41 63 63 65 70 74 3a 20 2a 2f 2a  ive-Acc ept: /*
0100  0d 0a 49 66 2d 4d 6f 64 69 66 69 65 64 2d 53 69  -If-Mod ified-Si
0110  6e 63 65 3a 20 57 65 64 2c 20 32 34 20 4a 75 6c  nce: Wed , 24 Jul
  
```

No.: 15419 - Time: 23.25.32290 - Source: 192.168.31.92 - Destination: 23.10.45.86 - Protocol: HTTP - Length: 455 - Info: ...EwSTAjBgUrDgMCGGUABBRr2bwARtMEy9spRAZgSQFhagQQUgrrwPZFOn89x6JI3r%2F2ztWk1V88CEDWvt3udNB9q%2F1K2BERqpxNS%3D HTTP/1.1



DARSHAN INSTITUTE OF ENGINEERING & TECHNOLOGY

Semester 5th | Practical Assignment | Computer Networks (2101CS501)

Date: 26/08/2024

TCP:

*MMB'S_WIFI							
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help							
tcp							
No.	Time	Source	Destination	Protocol	Length	Info	
15403	3325.324671	57.128.101.79	192.168.31.92	TCP	54	443 → 56985 [ACK] Seq=1328 Ack=1461 Win=63452 Len=0	
15404	3325.324671	57.128.101.79	192.168.31.92	TLSv1.2	868	Application Data	
15405	3325.324671	101.33.47.206	192.168.31.92	TCP	58	8081 → 56993 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1424	
15406	3325.324899	192.168.31.92	101.33.47.206	TCP	1185	56992 → 8081 [PSH, ACK] Seq=1 Ack=1 Win=65535 Len=1131	
15407	3325.324909	192.168.31.92	101.33.47.206	TCP	1249	56991 → 8081 [PSH, ACK] Seq=1 Ack=1 Win=65535 Len=1195	
15408	3325.324919	192.168.31.92	101.33.47.206	TCP	54	56993 → 8081 [ACK] Seq=1 Ack=1 Win=65535 Len=0	
15409	3325.324951	192.168.31.92	101.33.47.206	TCP	1249	56993 → 8081 [PSH, ACK] Seq=1 Ack=1 Win=65535 Len=1195	
15410	3325.324957	192.168.31.92	101.33.47.206	TCP	54	56991 → 8081 [FIN, ACK] Seq=1196 Ack=1 Win=65535 Len=0	
15411	3325.324957	192.168.31.92	101.33.47.206	TCP	54	56992 → 8081 [FIN, ACK] Seq=1132 Ack=1 Win=65535 Len=0	
15412	3325.324980	192.168.31.92	101.33.47.206	TCP	54	56993 → 8081 [FIN, ACK] Seq=1196 Ack=1 Win=65535 Len=0	
15413	3325.325507	192.168.31.92	57.128.101.79	TCP	54	56985 → 443 [FIN, ACK] Seq=1461 Ack=2142 Win=63895 Len=0	
15415	3325.329001	101.33.47.206	192.168.31.92	TCP	58	8081 → 56990 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1424	

Wireshark - Packet 15407 - MMB'S_WIFI

▶ Frame 15407: 1249 bytes on wire (9992 bits), 1249 bytes captured (9992 bits) on interface \Device\NPF_{40657720-7B9E-4FE2-9F2A-DE1D58E480EE}, id 0

▶ Ethernet II, Src: 84:29:07:a1:e1:63 (84:29:07:a1:e1:63), Dst: XiaomiMobile_29:c1:66 (d4:35:38:29:c1:66)

▶ Internet Protocol Version 4, Src: 192.168.31.92, Dst: 101.33.47.206

▶ Transmission Control Protocol, Src Port: 56991, Dst Port: 8081, Seq: 1, Ack: 1, Len: 1195

▶ Data (1195 bytes)

0000	d4 35 38 29 c1 66 84 29 07 a1 e1 63 08 00 45 00	58) f)	...c...E-
0010	04 d3 28 dd 40 00 80 06 58 54 c0 a8 1f 5c 65 21	..(@	...XT...e!
0020	2f ce de 9f 1f 91 5a 39 a8 5d 4a 8e d7 a4 50 18	/-----Z9	..]J...P-
0030	ff ff 79 d6 00 00 04 ab 08 00 04 06 0b 77 75 70	..y	-----wup
0040	5f 76 65 72 73 69 6f 6e 16 03 33 2e 30 06 0d 54	_version	...3.0...T
0050	59 50 45 5f 43 4f 4d 50 52 45 53 53 16 01 32 06	YPE_COMP	RESS..2-
0060	09 65 6e 63 72 5f 74 79 70 65 16 07 72 73 61 70	en	cr_ty pe rsap
0070	6f 73 74 06 07 62 65 61 5f 6b 65 79 16 ac 6e 44	ost	bea key nd
0080	4a 59 4c 51 64 4e 31 55 67 34 35 59 6c 6c 6a 5a	JYLDnIU	g45Y1ljZ
0090	2b 64 6b 64 4e 78 56 67 78 36 50 66 6d 32 4c 48	+dkdNxVg	x6Pfm2LH
00a0	6a 42 57 72 48 64 32 6d 49 69 48 68 6b 59 56 2b	jBwHd2m	IiHhkYV+
00b0	32 6b 49 42 6e 31 2f 6a 77 55 73 36 45 30 32 61	2kIBn1/j	wUs6E02a
00c0	4e 54 4b 4a 6d 7a 74 72 32 6f 2b 4c 56 6b 70 45	NTKJmztr	2o+LVkpE
00d0	2b 69 33 48 4f 52 6a 6f 4e 69 32 6d 65 6e 67 63	+i3HORjo	Ni2mengc
00e0	47 73 52 56 74 75 4c 64 64 57 30 51 6c 6d 36 4f	GsRVtulD	dW0Qlm60
00f0	78 6a 6c 70 58 64 77 6a 30 2b 35 6f 64 4b 37 4e	xjlpXdwj	0+5odK7N
0100	51 79 6f 70 56 76 6f 4b 48 45 4d 68 4d 4d 4f 57	QyopVvoK	HEMhMWOW
0110	57 65 76 6f 36 31 78 35 63 72 6a 4e 4f 77 71 63	Wevo61xS	crjNOwqc