Mahavir Education Trust's

SHAH & ANCHOR KUTCHHI ENGINEERING COLLEGE

Chembur, Mumbai - 400 088

UG Program in Information Technology

Experiment No: 05				
Date of Performance:	07/10/2024			
Date of Submission:	14/10/2024			
Program Formation/ Execution/ Correction (06)	**Timely Submission (01)**	**Viva (03)**	**Experiment Marks (10)**	**Teacher Signature with date**

EXPERIMENT - 05

Aim: Study of packet sniffer tools wireshark.

Theory:

Wireshark is an open-source network protocol analyzer that allows users to capture and examine data packets moving through a network in real time. It supports numerous protocols and provides in-depth packet details, making it valuable for network diagnostics, security analysis, and troubleshooting.

Key Concepts:

1. Packet Sniffing: The process of intercepting and logging traffic passing over a digital network or part of a network.
2. Protocols: Wireshark supports a wide range of protocols, such as TCP, UDP, HTTP, FTP, and more.
3. Packet Capture: Wireshark captures raw network traffic, allowing analysis of headers and payloads.
4. Network Analysis: Wireshark helps in identifying latency, connection issues, security breaches, and network misconfigurations.

Applications of Wireshark:

1. Network Troubleshooting: Detects network performance issues.
2. Security Analysis: Identifies malicious activities like unauthorized access, Distributed Denial of Service (DDoS) attacks, and other forms of cyber-attacks.
3. Protocol Development: Useful for developing and testing new network protocols.

Procedure

Requirements:

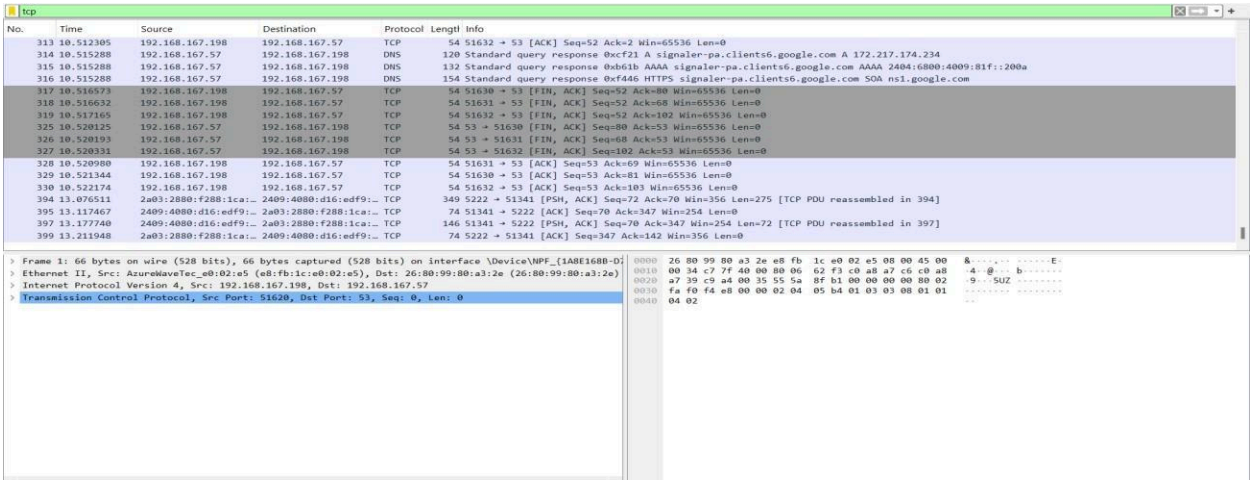
- A computer with an active internet connection.
- Wireshark installed on the system (available for Windows, macOS, and Linux).

Steps:

1. Install Wireshark:
    - Download Wireshark from the official website and install it.
    - Ensure the installation of supporting libraries for packet capture, such as WinPcap (for Windows) or libpcap (for Linux/Mac).

2. Launch Wireshark:
    - Open the Wireshark application.
    - Select the network interface you want to monitor (e.g., Ethernet, Wi-Fi).
3. Start Capturing Packets:
    - Click on the network interface and press the Start button to begin packet capture.
    - Wireshark will display packets in real-time as they are captured, showing details such as source/destination IP addresses, protocol used, packet size, and more.
4. Filter Traffic:
    - Use Wireshark's filtering options to narrow down the packets you wish to analyze.
    - For example, to view only HTTP traffic, use the filter http.
5. Analyze Packets:
    - Click on individual packets to view detailed breakdowns of each packet, including layer-specific information (Ethernet, IP, TCP/UDP, Application layer data).
    - Look for packet anomalies, such as retransmissions, duplicate packets, or security vulnerabilities like suspicious traffic from unknown sources.
6. Stop the Capture:
    - After enough packets have been captured, press the Stop button.
    - You can save the captured data for future analysis in various formats (e.g., .pcap).
7. Save & Export Data:
    - Wireshark allows users to save the captured session, export packet details, and generate reports.

Output:




udp
No. Time Source Destination Protocol Lengtl Info
5657 64.820929 2404:6800:4009:81e:... 2409:4080:d16:edf9:... QUIC 1292 Initial, SCID=e597f0a8de891657, PKN: 3, CRYPTO, PADDING
5658 64.822807 2404:6800:4009:81e:... 2409:4080:d16:edf9:... QUIC 367 Protected Payload (KP0)
5659 64.822807 2404:6800:4009:81e:... 2409:4080:d16:edf9:... QUIC 987 Protected Payload (KP0)
5660 64.822807 2404:6800:4009:81e:... 2409:4080:d16:edf9:... QUIC 106 Protected Payload (KP0)
5661 64.822807 2404:6800:4009:81e:... 2409:4080:d16:edf9:... QUIC 86 Protected Payload (KP0)
5662 64.823633 2409:4080:d16:edf9:... 2404:6800:4009:81e:... QUIC 1292 Handshake, DCID=e597f0a8de891657
5663 64.823788 2409:4080:d16:edf9:... 2404:6800:4009:81e:... QUIC 93 Protected Payload (KP0), DCID=e597f0a8de891657
5664 64.824174 2409:4080:d16:edf9:... 2404:6800:4009:81e:... QUIC 618 Protected Payload (KP0), DCID=e597f0a8de891657
5669 64.860507 2409:4080:d16:edf9:... 2404:6800:4009:801:... UDP 91 63539 → 443 Len=29
5670 64.959544 2404:6800:4009:801:... 2409:4080:d16:edf9:... UDP 87 443 → 63539 Len=25
5671 64.959544 2404:6800:4009:81e:... 2409:4080:d16:edf9:... QUIC 182 Protected Payload (KP0)
5672 64.959544 2404:6800:4009:81e:... 2409:4080:d16:edf9:... QUIC 91 Protected Payload (KP0)
5673 64.960222 2409:4080:d16:edf9:... 2404:6800:4009:81e:... QUIC 94 Protected Payload (KP0), DCID=e597f0a8de891657
5674 65.060131 2404:6800:4009:81e:... 2409:4080:d16:edf9:... QUIC 652 Protected Payload (KP0)
5675 65.060131 2404:6800:4009:81e:... 2409:4080:d16:edf9:... QUIC 83 Protected Payload (KP0)
5676 65.060880 2409:4080:d16:edf9:... 2404:6800:4009:81e:... QUIC 97 Protected Payload (KP0), DCID=e597f0a8de891657
5698 65.160888 2404:6800:4009:81e:... 2409:4080:d16:edf9:... QUIC 86 Protected Payload (KP0)
Frame 5517: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface \Device\NPF_{1A8E168
Ethernet II, Src: AzureWaveTec_e0:02:e5 (e8:fb:1c:e0:02:e5), Dst: 26:80:99:80:a3:2e (26:80:99:80:a3:2e)
Internet Protocol Version 6, Src: 2409:4080:d16:edf9:7102:a45c:e5d1:c466, Dst: 2404:6800:4009:81e::200a
User Datagram Protocol, Src Port: 51285, Dst Port: 443
Data (29 bytes)
0000 26 80 99 80 a3 2e e8 fb 1c e0 02 e5 86 dd 60 0b
0010 c0 0a 00 25 11 fe 24 09 40 80 0d 16 ed f9 71 02
0020 a4 5c e5 d1 c4 66 24 04 68 00 40 09 08 1e 00 00
0030 00 00 00 00 20 0a c8 55 01 bb 00 25 34 61 57 e3
0040 18 1d 66 d9 06 26 de 84 77 6a 83 c3 aa 3a a6 4a
0050 6c f9 0c 75 bb ed 5c 22 ab 18 aa
http
No. Time Source Destination Protocol Lengtl Info
4583 34.054426 2409:4080:d16:edf9:... 2405:200:1602::312c... HTTP 258 HEAD /pr/492350f6-3a01-4f97-b9c0-c7c6ddf67d60/Office/Data/16.0.18025.20140/s641033.cab HTTP/1.1
4586 34.105638 2405:200:1602::312c... 2409:4080:d16:edf9:... HTTP 592 HTTP/1.1 200 OK
4587 34.117830 2409:4080:d16:edf9:... 2405:200:1602::312c... HTTP 258 HEAD /pr/492350f6-3a01-4f97-b9c0-c7c6ddf67d60/Office/Data/16.0.18025.20140/s641033.cab HTTP/1.1
4588 34.157735 2405:200:1602::312c... 2409:4080:d16:edf9:... HTTP 592 HTTP/1.1 200 OK
4671 34.810550 2409:4080:d16:edf9:... 64:ff9b::6f77:f82 HTTP 396 GET /pr/492350f6-3a01-4f97-b9c0-c7c6ddf67d60/Office/Data/16.0.18025.20140/s641033.cab HTTP/1.1
4673 34.860122 64:ff9b::6f77:f82 2409:4080:d16:edf9:... HTTP 697 HTTP/1.1 206 Partial Content
4692 34.983478 192.168.167.198 74.225.225.201 HTTP 379 GET /pr/492350f6-3a01-4f97-b9c0-c7c6ddf67d60/Office/Data/16.0.18025.20140/s641033.cab?cacheHostOrigin=f.c2r.ts.cdn.office.net HTTP/...
5108 47.915193 2409:4080:d16:edf9:... 64:ff9b::312c:320a HTTP 185 GET /connecttest.txt HTTP/1.1
5110 48.029273 64:ff9b::312c:320a 2409:4080:d16:edf9:... HTTP 261 HTTP/1.1 200 OK (text/plain)
6494 77.929711 2409:4080:d16:edf9:... 64:ff9b::312c:320a HTTP 185 GET /connecttest.txt HTTP/1.1
6496 77.964473 64:ff9b::312c:320a 2409:4080:d16:edf9:... HTTP 261 HTTP/1.1 200 OK (text/plain)
6767 86.480786 2409:4080:d16:edf9:... 64:ff9b::6f77:f82 HTTP 368 GET /pr/492350f6-3a01-4f97-b9c0-c7c6ddf67d60/Office/Data/16.0.18025.20140/s641033.cab HTTP/1.1
6840 86.636751 64:ff9b::6f77:f82 2409:4080:d16:edf9:... HTTP 89 HTTP/1.1 206 Partial Content
6900 87.197356 2409:4080:d16:edf9:... 2405:200:1602::312c... HTTP 396 GET /pr/492350f6-3a01-4f97-b9c0-c7c6ddf67d60/Office/Data/16.0.18025.20140/s641033.cab HTTP/1.1
6902 87.240591 2405:200:1602::312c... 2409:4080:d16:edf9:... HTTP 635 HTTP/1.1 206 Partial Content
6907 87.360843 192.168.167.198 74.225.225.201 HTTP 380 GET /pr/492350f6-3a01-4f97-b9c0-c7c6ddf67d60/Office/Data/16.0.18025.20140/s641033.cab?cacheHostOrigin=f.c2r.ts.cdn.office.net HTTP/...
6913 87.867532 192.168.167.198 74.225.225.201 HTTP 385 GET /pr/492350f6-3a01-4f97-b9c0-c7c6ddf67d60/Office/Data/16.0.18025.20140/s641033.cab?cacheHostOrigin=f.c2r.ts.cdn.office.net HTTP/...
6918 88.353629 192.168.167.198 74.225.225.201 HTTP 385 GET /pr/492350f6-3a01-4f97-b9c0-c7c6ddf67d60/Office/Data/16.0.18025.20140/s641033.cab?cacheHostOrigin=f.c2r.ts.cdn.office.net HTTP/...
Frame 5110: 261 bytes on wire (2088 bits), 261 bytes captured (2088 bits) on interface \Device\NPF_{1A8E
Ethernet II, Src: 26:80:99:80:a3:2e (26:80:99:80:a3:2e), Dst: AzureWaveTec_e0:02:e5 (e8:fb:1c:e0:02:e5)
Internet Protocol Version 6, Src: 64:ff9b::312c:320a, Dst: 2409:4080:d16:edf9:7102:a45c:e5d1:c466
Transmission Control Protocol, Src Port: 80, Dst Port: 51402, Seq: 1, Ack: 112, Len: 187
Hypertext Transfer Protocol
Line-based text data: text/plain (1 lines)
0000 e8 fb 1c e0 02 e5 26 80 99 80 a3 2e 86 dd 62 80
0010 00 00 00 cf 06 39 00 64 ff 9b 00 00 00 00 00 00
0020 00 00 31 2c 32 0a 24 09 40 80 0d 16 ed f9 71 02
0030 a4 5c e5 d1 c4 66 00 50 c8 ca 9f 46 6c 4c 0a f6
0040 f1 ee 50 18 01 f6 aa e8 00 00 48 54 54 50 2f 31
0050 2e 31 20 32 30 30 20 4f 4b 0d 0a 43 6f 6e 74 65
0060 6e 74 2d 4c 65 6e 67 74 68 3a 20 32 32 0d 0a 44
0070 61 74 65 3a 20 4d 6f 6e 2c 20 31 34 20 4f 63 74
0080 20 32 30 32 34 20 31 34 3a 31 31 3a 35 36 20 47
0090 4d 54 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20
00a0 63 6c 6f 73 65 0d 0a 43 6f 6e 74 65 6e 74 2d 54
00b0 79 70 65 3a 20 74 65 78 74 2f 70 6c 61 69 6e 0d
00c0 0a 43 61 63 68 65 2d 43 6f 6e 74 72 6f 6c 3a 20
00d0 6d 61 78 2d 61 67 65 3d 33 30 2c 20 6d 75 73 74
00e0 2d 72 65 76 61 6c 69 64 61 74 65 0d 0a 0d 0a 4d
00f0 69 63 72 6f 73 6f 66 74 20 43 6f 6e 6e 65 63 74
0100 20 54 65 73 74
quic
No. Time Source Destination Protocol Lengtl Info
14962 220.664523 2404:6800:4009:825:... 2409:4080:d16:edf9:... QUIC 369 Protected Payload (KP0)
14963 220.664885 2409:4080:d16:edf9:... 2404:6800:4009:825:... QUIC 175 Protected Payload (KP0), DCID=f05f64733972dbd3
14965 220.708826 2404:6800:4009:825:... 2409:4080:d16:edf9:... QUIC 182 Protected Payload (KP0)
14966 220.709142 2409:4080:d16:edf9:... 2404:6800:4009:825:... QUIC 95 Protected Payload (KP0), DCID=f05f64733972dbd3
14969 220.883526 2404:6800:4009:825:... 2409:4080:d16:edf9:... QUIC 261 Protected Payload (KP0)
14970 220.883526 2404:6800:4009:825:... 2409:4080:d16:edf9:... QUIC 83 Protected Payload (KP0)
14972 220.884197 2409:4080:d16:edf9:... 2404:6800:4009:825:... QUIC 99 Protected Payload (KP0), DCID=f05f64733972dbd3
14973 220.884392 2409:4080:d16:edf9:... 2404:6800:4009:825:... QUIC 95 Protected Payload (KP0), DCID=f05f64733972dbd3
14975 220.979880 2404:6800:4009:825:... 2409:4080:d16:edf9:... QUIC 89 Protected Payload (KP0)
15024 224.345073 2404:6800:4009:825:... 2409:4080:d16:edf9:... QUIC 347 Protected Payload (KP0), DCID=f05f64733972dbd3
15026 224.415560 2404:6800:4009:825:... 2409:4080:d16:edf9:... QUIC 94 Protected Payload (KP0)
15027 224.442801 2409:4080:d16:edf9:... 2404:6800:4009:825:... QUIC 94 Protected Payload (KP0), DCID=f05f64733972dbd3
15030 224.616928 2404:6800:4009:825:... 2409:4080:d16:edf9:... QUIC 148 Protected Payload (KP0)
15031 224.617649 2404:6800:4009:825:... 2409:4080:d16:edf9:... QUIC 83 Protected Payload (KP0)
15032 224.617699 2409:4080:d16:edf9:... 2404:6800:4009:825:... QUIC 99 Protected Payload (KP0), DCID=f05f64733972dbd3
15034 224.652311 2409:4080:d16:edf9:... 2404:6800:4009:825:... QUIC 94 Protected Payload (KP0), DCID=f05f64733972dbd3
15036 224.689006 2404:6800:4009:825:... 2409:4080:d16:edf9:... QUIC 86 Protected Payload (KP0)
Frame 1468: 1292 bytes on wire (10336 bits), 1292 bytes captured (10336 bits) on interface \Device\NPF_{
Ethernet II, Src: AzureWaveTec_e0:02:e5 (e8:fb:1c:e0:02:e5), Dst: 26:80:99:80:a3:2e (26:80:99:80:a3:2e)
Internet Protocol Version 6, Src: 2409:4080:d16:edf9:7102:a45c:e5d1:c466, Dst: 2404:6800:4009:802::2003
User Datagram Protocol, Src Port: 49293, Dst Port: 443
QUIC IETF
0000 26 80 99 80 a3 2e e8 fb 1c e0 02 e5 86 dd 60 03
0010 1e b9 04 d6 11 fe 24 09 40 80 0d 16 ed f9 71 02
0020 a4 5c e5 d1 c4 66 24 04 68 00 40 09 08 02 00 00
0030 00 00 00 00 20 03 c0 8d 01 bb 04 d6 7b 27 c4 00
0040 00 00 01 08 1a ca fe 90 bb 99 2d 2a 00 40 46 00
0050 18 e5 42 40 26 d8 c5 14 3d 5b 55 06 c6 70 37 1f
0060 a3 35 fc af 60 65 2a 85 ba d9 dc 10 f2 8c b8 98
0070 b8 43 a2 c5 d9 6b 31 f9 6c 88 2a 9a bf b1 b5 8c
0080 4b 84 2f 60 82 66 a9 13 30 49 a1 8e b6 92 b1 d3
0090 f3 d6 41 13 90 44 75 10 9d 42 f4 83 3d 7c 16 24
00a0 28 57 44 1c 2e 23 00 e0 28 c3 11 77 5a c8 a9 e5
00b0 ae 39 cc fb 9b ec 8e 0e 75 6b a8 cb 73 eb 94 51
00c0 cf ac 83 f7 01 0b 36 b2 64 b9 56 c5 00 a7 20 13
00d0 8b df 68 82 92 68 e7 d9 6a a5 1c 16 ed fa f2 19
00e0 bb 5e 3f f3 65 06 0f 40 d7 90 70 8b b8 cc 30 6b
00f0 66 fb fc a5 be 69 5c 37 7a ec cc 91 ed 12 0e e5
0100 7a 76 e6 00 07 3c 32 59 bd 57 76 d8 59 eb 81 d3
0110 a0 65 11 c4 16 0f 85 16 6c f1 41 72 bb a8 52 e5
0120 85 12 24 72 18 95 39 5c 23 79 2b 78 86 10 81 2b
0130 c1 b9 2a 31 91 a1 a5 df 51 96 e2 d8 54 80 c8 21
0140 18 e1 37 04 40 f7 5b 4a 95 ac 0f d6 ec d2 03 d9
Frame (1292 bytes) Decrypted QUIC (1124 bytes)

Conclusion :

By using Wireshark, users can effectively troubleshoot network problems, monitor performance, and safeguard networks from malicious activities. This hands-on study helps in building foundational knowledge of packet analysis and network security.