EXPERIMENT-3

◇ Wireshark

Aim

To capture, analyze, and troubleshoot network traffic using Wireshark for network monitoring and forensic investigation.

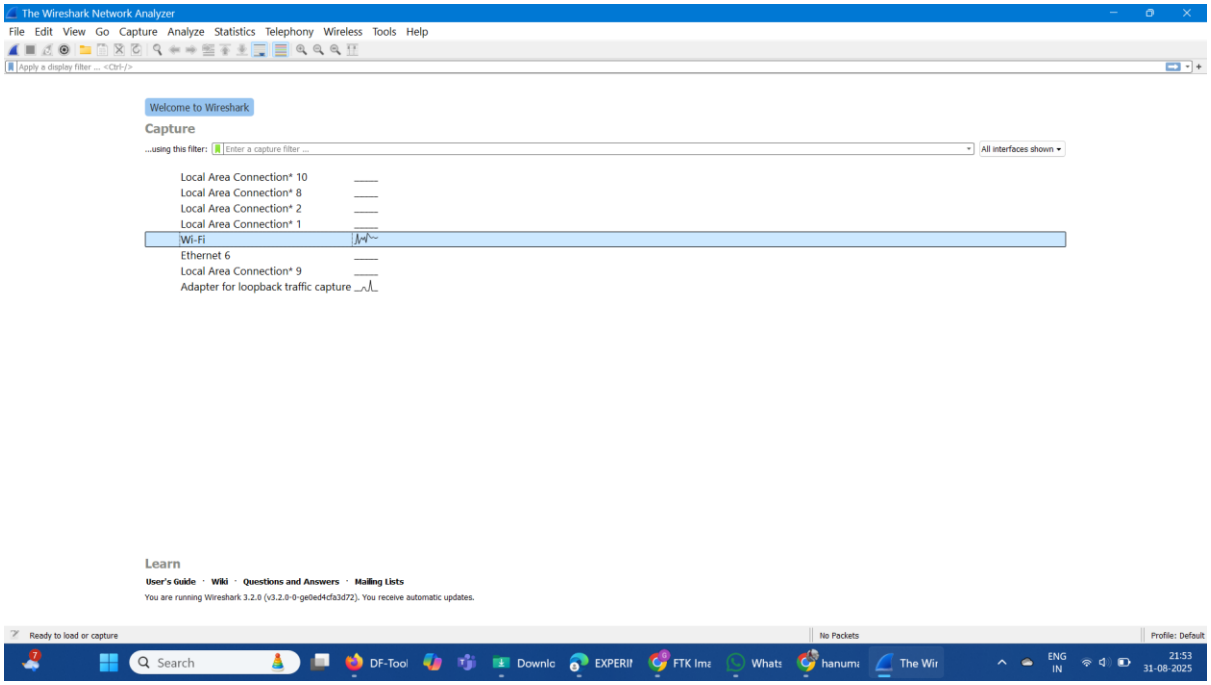
Tools / Features

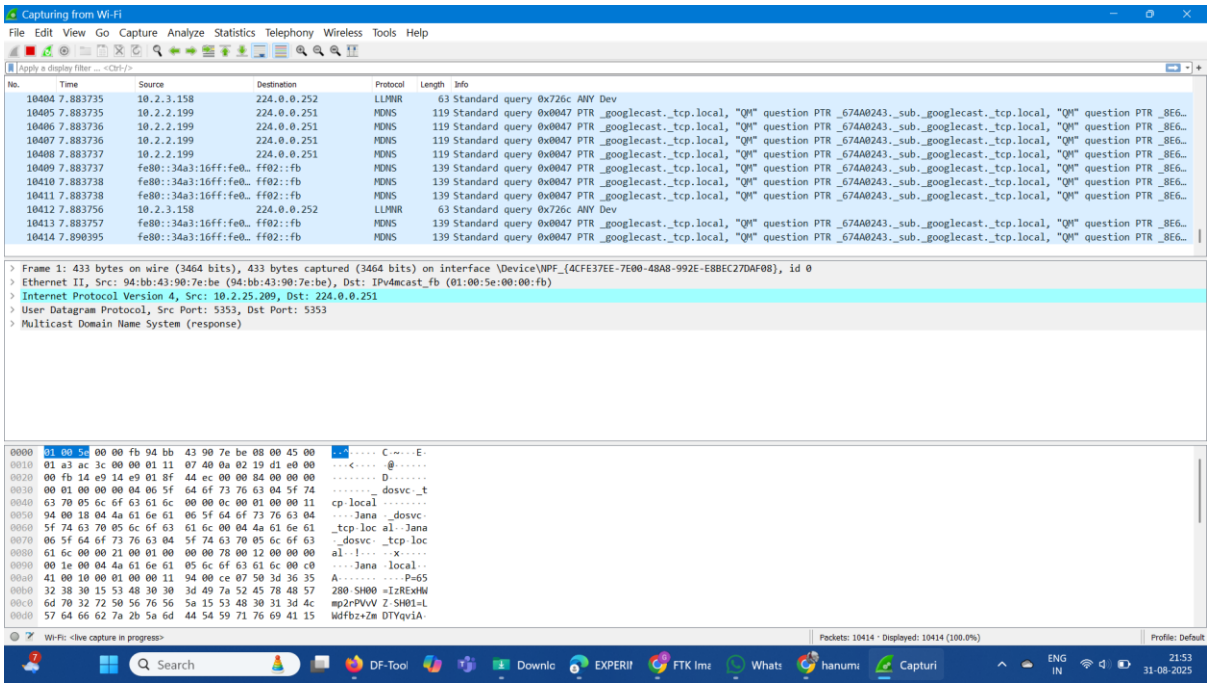
- **Packet Capture** – Captures live traffic from interfaces (Ethernet, Wi-Fi, etc.).
- **Protocol Analysis** – Supports 2000+ protocols (TCP, UDP, HTTP, DNS, SSL, etc.).
- **Filters** – Apply capture filters and display filters for specific traffic.
- **Packet Dissection** – Shows details like source/destination IP, ports, flags.
- **Stream Follow** – Reconstructs TCP/UDP streams for analysis.
- **Export Data** – Save captured packets in `.pcap` format for later use.
- **Statistics** – Provides I/O graphs, flow diagrams, and protocol hierarchy.

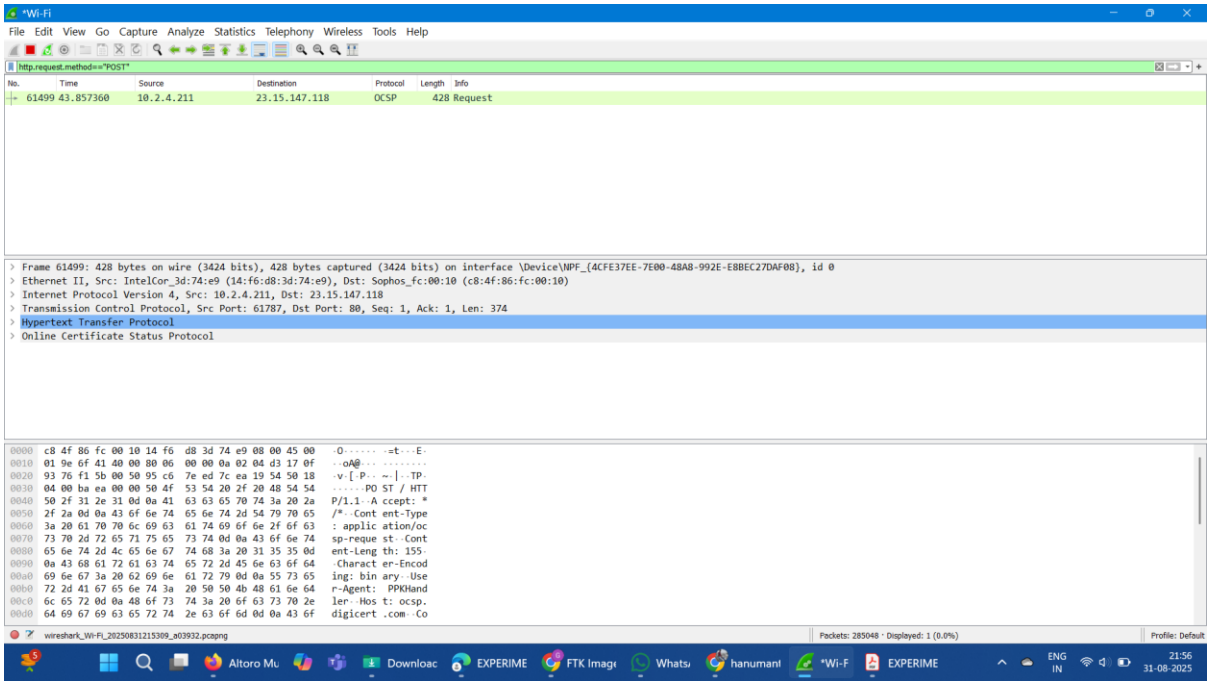
Procedure

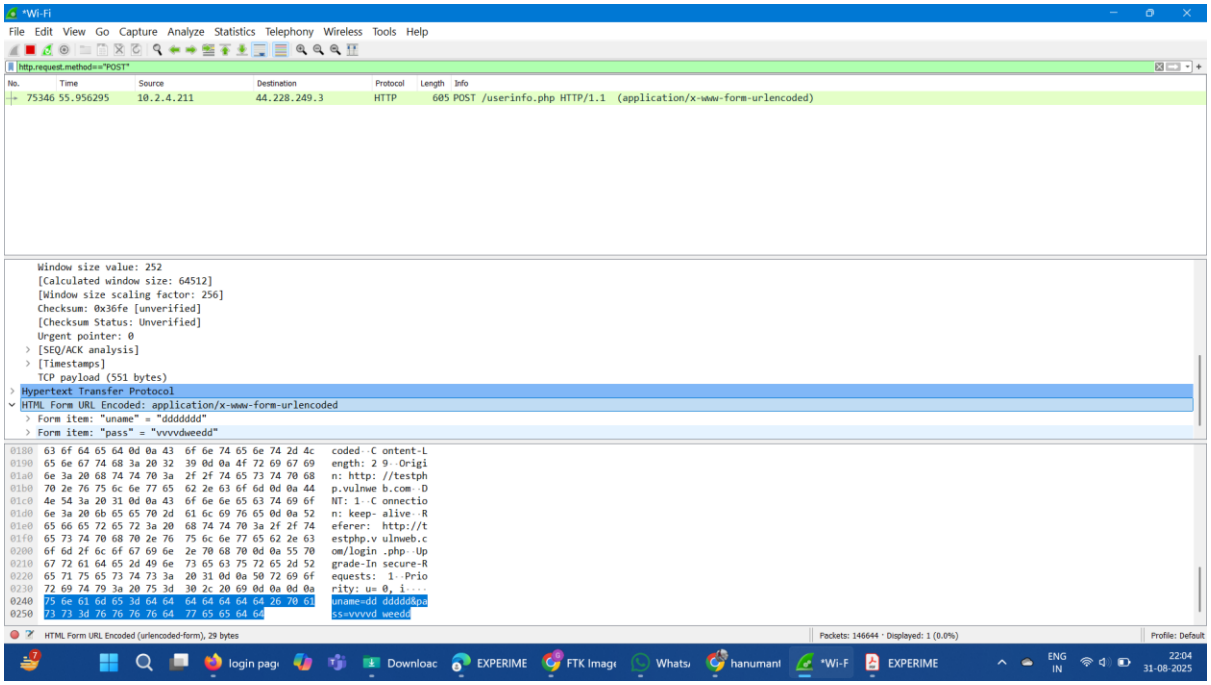
1. **Launch Wireshark** → Open the tool with administrator rights.
2. **Select Interface** → Choose the network adapter (Wi-Fi, Ethernet, etc.).
3. **Start Capture** → Click the blue shark icon (start capturing packets).
4. **Apply Filters** → Use filters (e.g., `http`, `ip.addr == 192.168.1.1`, `tcp.port == 80`) to focus on traffic.
5. **Analyze Packets** → Select a packet to view details in three panes (summary, details, raw data).
6. **Follow Stream** → Right-click → Follow → TCP Stream (to see conversation).
7. **Save Capture** → Stop capture and save as `.pcap` for reporting.

OUTPUT:


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Capture
...using this filter: Enter a capture filter ...
All interfaces shown
Local Area Connection* 10
Local Area Connection* 8
Local Area Connection* 2
Local Area Connection* 1
Wi-Fi
Ethernet 6
Local Area Connection* 9
Adapter for loopback traffic capture
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
You are running Wireshark 3.2.0 (v3.2.0-0-ge0ed4cfa3d72). You receive automatic updates.
Ready to load or capture
No Packets
Profile: Default
Search
DF-Tool
Downlo
EXPERIT
FTK Ima
Whats
hanuma
The Wir
ENG
IN
21:53
31-08-2025


Capturing from 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
10404 7.883735 10.2.3.158 224.0.0.252 LLMNR 63 Standard query 0x726c ANY Dev
10405 7.883735 10.2.2.199 224.0.0.251 MDNS 119 Standard query 0x0047 PTR _googlecast._tcp.local, "QM" question PTR _674A0243._sub._googlecast._tcp.local, "QM" question PTR _8E6…
10406 7.883736 10.2.2.199 224.0.0.251 MDNS 119 Standard query 0x0047 PTR _googlecast._tcp.local, "QM" question PTR _674A0243._sub._googlecast._tcp.local, "QM" question PTR _8E6…
10407 7.883736 10.2.2.199 224.0.0.251 MDNS 119 Standard query 0x0047 PTR _googlecast._tcp.local, "QM" question PTR _674A0243._sub._googlecast._tcp.local, "QM" question PTR _8E6…
10408 7.883737 10.2.2.199 224.0.0.251 MDNS 119 Standard query 0x0047 PTR _googlecast._tcp.local, "QM" question PTR _674A0243._sub._googlecast._tcp.local, "QM" question PTR _8E6…
10409 7.883737 fe80::34a3:16ff:fe0… ff02::fb MDNS 139 Standard query 0x0047 PTR _googlecast._tcp.local, "QM" question PTR _674A0243._sub._googlecast._tcp.local, "QM" question PTR _8E6…
10410 7.883738 fe80::34a3:16ff:fe0… ff02::fb MDNS 139 Standard query 0x0047 PTR _googlecast._tcp.local, "QM" question PTR _674A0243._sub._googlecast._tcp.local, "QM" question PTR _8E6…
10411 7.883738 fe80::34a3:16ff:fe0… ff02::fb MDNS 139 Standard query 0x0047 PTR _googlecast._tcp.local, "QM" question PTR _674A0243._sub._googlecast._tcp.local, "QM" question PTR _8E6…
10412 7.883756 10.2.3.158 224.0.0.252 LLMNR 63 Standard query 0x726c ANY Dev
10413 7.883757 fe80::34a3:16ff:fe0… ff02::fb MDNS 139 Standard query 0x0047 PTR _googlecast._tcp.local, "QM" question PTR _674A0243._sub._googlecast._tcp.local, "QM" question PTR _8E6…
10414 7.890395 fe80::34a3:16ff:fe0… ff02::fb MDNS 139 Standard query 0x0047 PTR _googlecast._tcp.local, "QM" question PTR _674A0243._sub._googlecast._tcp.local, "QM" question PTR _8E6…
Frame 1: 433 bytes on wire (3464 bits), 433 bytes captured (3464 bits) on interface \Device\NPF_{4CFE37EE-7E00-48A8-992E-E8BEC27DAF08}, id 0
Ethernet II, Src: 94:bb:43:90:7e:be (94:bb:43:90:7e:be), Dst: IPv4mcast_fb (01:00:5e:00:00:fb)
Internet Protocol Version 4, Src: 10.2.25.209, Dst: 224.0.0.251
User Datagram Protocol, Src Port: 5353, Dst Port: 5353
Multicast Domain Name System (response)
0000 01 00 5e 00 00 fb 94 bb 43 90 7e be 08 00 45 00
0010 01 a3 ac 3c 00 00 01 11 07 40 0a 02 19 d1 e0 00
0020 00 fb 14 e9 14 e9 01 8f 44 ec 00 00 84 00 00 00
0030 00 01 00 00 00 04 06 5f 64 6f 73 76 63 04 5f 74
0040 63 70 05 6c 6f 63 61 6c 00 00 0c 00 01 00 00 11
0050 94 00 18 04 4a 61 6e 61 06 5f 64 6f 73 76 63 04
0060 5f 74 63 70 05 6c 6f 63 61 6c 00 04 4a 61 6e 61
0070 06 5f 64 6f 73 76 63 04 5f 74 63 70 05 6c 6f 63
0080 61 6c 00 00 21 00 01 00 00 00 78 00 12 00 00 00
0090 00 1e 00 04 4a 61 6e 61 05 6c 6f 63 61 6c 00 c0
00a0 41 00 10 00 01 00 00 11 94 00 ce 07 50 3d 36 35
00b0 32 38 30 15 53 48 30 30 3d 49 7a 52 45 78 48 57
00c0 6d 70 32 72 50 56 76 56 5a 15 53 48 30 31 3d 4c
00d0 57 64 66 62 7a 2b 5a 6d 44 54 59 71 76 69 41 15
Wi-Fi: <live capture in progress>
Packets: 10414 · Displayed: 10414 (100.0%)
Profile: Default
Search
DF-Tool
Downlo
EXPERIT
FTK Ima
Whats
hanuma
Capturi
ENG
IN
21:53
31-08-2025





Result:

Network packets were successfully captured and analyzed using **Wireshark**.
The tool provided detailed insights into protocols, IP addresses, and communication flows, which can be used for troubleshooting and forensic investigation.