Task 5: Capture and Analyze Network Traffic Using Wireshark

Name: Pulak Jindal
Internship/Organization: Elevate Labs
Date: 27th October, 2025

Objective

To capture live network traffic using Wireshark and identify different network protocols and traffic types.

Tools Used

- Wireshark
- Operating System: Kali Linux

Procedure

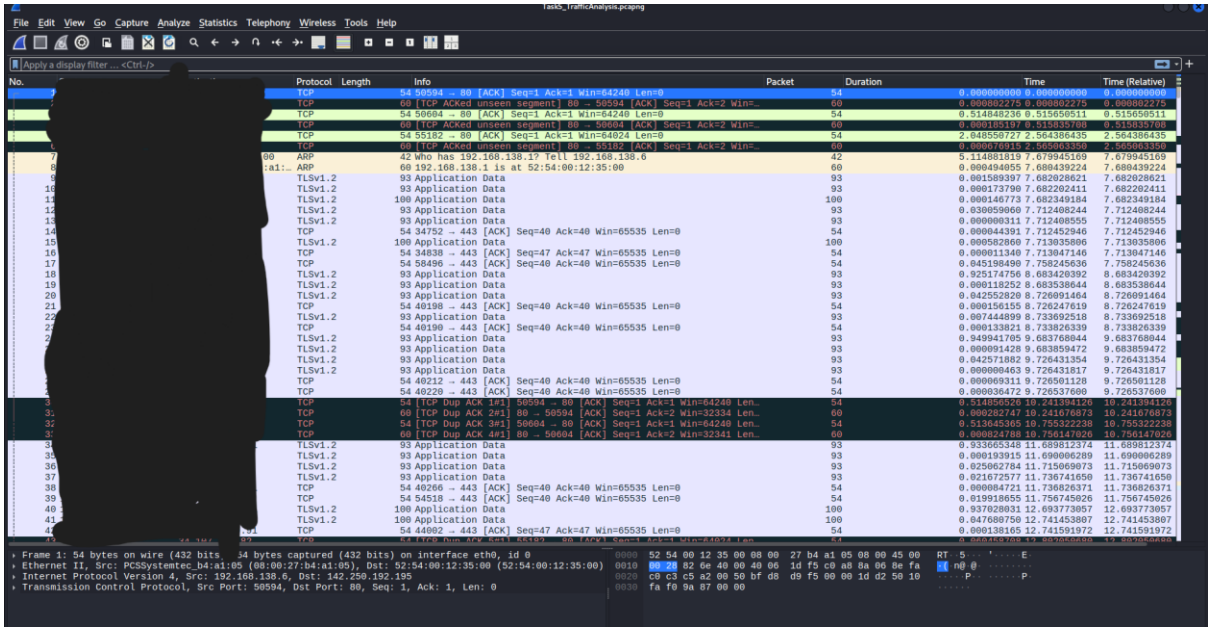
1. Launched Wireshark.
2. Selected active network interface (eth0).
3. Started live capture and browsed websites + pinged a server.
4. Captured data for ~1 minute.
5. Applied protocol filters (HTTP, DNS, ICMP, etc.).
6. Stopped capture and saved as Task5_TrafficAnalysis.pcap.

Analysis Summary

- **Total Packets Captured:** 1219
- **Top 3 Protocols by Count:** ARP, TCP, TLSv1.2
- **Key Insights:**
    - ARP used for local network address resolution.
    - TLSv1.2 for encryption of data over network.

Conclusion

Wireshark successfully captured and displayed live network packets. Multiple protocols were identified, enhancing understanding of how devices communicate across layers of the network. This task improved my practical knowledge of packet analysis and protocol structures.


Tasks_TrafficAnalysis.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Protocol Length Info Packet Duration Time Time (Relative)
TCP 54 50594 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0 54 0.000000000 0.000000000
TCP 60 [TCP ACKed unseen segment] 80 → 50594 [ACK] Seq=1 Ack=2 Win=… 60 0.000082275 0.000082275
TCP 54 50604 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0 54 0.514848236 0.515650511
TCP 60 [TCP ACKed unseen segment] 80 → 50604 [ACK] Seq=1 Ack=2 Win=… 60 0.000185197 0.515835708
TCP 54 55182 → 80 [ACK] Seq=1 Ack=1 Win=64024 Len=0 54 2.048550727 2.564386435
TCP 60 [TCP ACKed unseen segment] 80 → 55182 [ACK] Seq=1 Ack=2 Win=… 60 0.000070915 2.564063350
ARP 42 Who has 192.168.138.1? Tell 192.168.138.6 42 5.114881819 7.679945169
ARP 60 192.168.138.1 is at 52:54:00:12:35:00 60 0.000494055 7.680439224
TLSv1.2 93 Application Data 93 0.001589397 7.682028621
TLSv1.2 93 Application Data 93 0.000173790 7.682202411
TLSv1.2 100 Application Data 100 0.000146773 7.682349184
TLSv1.2 93 Application Data 93 0.030059060 7.712408244
TLSv1.2 93 Application Data 93 0.000000311 7.712408555
TCP 54 34752 → 443 [ACK] Seq=40 Ack=40 Win=65535 Len=0 54 0.000044391 7.712452946
TLSv1.2 100 Application Data 100 0.000582860 7.713035806
TCP 54 34838 → 443 [ACK] Seq=47 Ack=47 Win=65535 Len=0 54 0.000011340 7.713047146
TCP 54 58496 → 443 [ACK] Seq=40 Ack=40 Win=65535 Len=0 54 0.045198490 7.758245636
TLSv1.2 93 Application Data 93 0.925174756 8.683420392
TLSv1.2 93 Application Data 93 0.000118252 8.683538644
TLSv1.2 93 Application Data 93 0.042552820 8.726091464
TCP 54 40198 → 443 [ACK] Seq=40 Ack=40 Win=65535 Len=0 54 0.000156155 8.726247619
TLSv1.2 93 Application Data 93 0.007444899 8.733692518
TCP 54 40199 → 443 [ACK] Seq=40 Ack=40 Win=65535 Len=0 54 0.000133821 8.733826339
TLSv1.2 93 Application Data 93 0.949941705 9.683768044
TLSv1.2 93 Application Data 93 0.000091428 9.683859472
TLSv1.2 93 Application Data 93 0.042571882 9.726431354
TLSv1.2 93 Application Data 93 0.000000463 9.726431817
TCP 54 40212 → 443 [ACK] Seq=40 Ack=40 Win=65535 Len=0 54 0.000069311 9.726501128
TCP 54 40220 → 443 [ACK] Seq=40 Ack=40 Win=65535 Len=0 54 0.000036472 9.726537600
TCP 54 [TCP Dup ACK 1#1] 50594 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len… 54 0.514856526 10.241394126
TCP 60 [TCP Dup ACK 2#1] 80 → 50594 [ACK] Seq=1 Ack=2 Win=32334 Len… 60 0.000282747 10.241676873
TCP 54 [TCP Dup ACK 3#1] 50604 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len… 54 0.513645365 10.755322238
TCP 60 [TCP Dup ACK 4#1] 80 → 50604 [ACK] Seq=1 Ack=2 Win=32341 Len… 60 0.000247788 10.756147026
TLSv1.2 93 Application Data 93 0.933665348 11.689812374
TLSv1.2 93 Application Data 93 0.000193915 11.690006289
TLSv1.2 93 Application Data 93 0.025062784 11.715069073
TLSv1.2 93 Application Data 93 0.021672577 11.736741650
TCP 54 40266 → 443 [ACK] Seq=40 Ack=40 Win=65535 Len=0 54 0.000084721 11.736826371
TCP 54 54518 → 443 [ACK] Seq=40 Ack=40 Win=65535 Len=0 54 0.019918655 11.756745026
TLSv1.2 100 Application Data 100 0.937028031 12.693773057
TLSv1.2 100 Application Data 100 0.047680750 12.741453807
TCP 54 44002 → 443 [ACK] Seq=47 Ack=47 Win=65535 Len=0 54 0.000138165 12.741591972
Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id 0
Ethernet II, Src: PCSSystemtec_b4:a1:05 (08:00:27:b4:a1:05), Dst: 52:54:00:12:35:00 (52:54:00:12:35:00)
Internet Protocol Version 4, Src: 192.168.138.6, Dst: 142.250.192.195
Transmission Control Protocol, Src Port: 50594, Dst Port: 80, Seq: 1, Ack: 1, Len: 0
0000 52 54 00 12 35 00 08 00 27 b4 a1 05 08 00 45 00
0010 00 28 82 6e 40 00 40 06 1d f5 c0 a8 8a 06 8e fa
0020 c0 c3 c5 a2 00 50 bf d8 d9 f5 00 00 1d d2 50 10
0030 fa f0 9a 87 00 00