TASK -5

Capture and Analyze Network Traffic Using Wireshark

JUNE 3, 2025

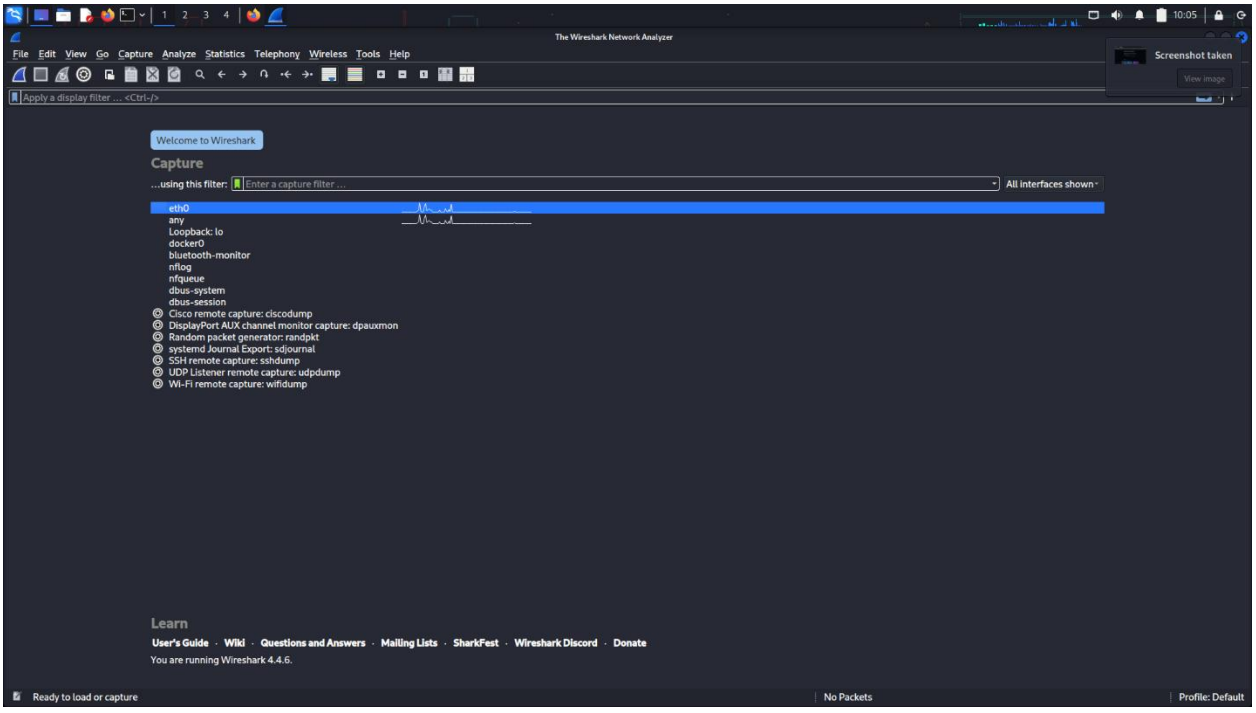
PRADEEP U S

Capture and Analyze Network Traffic Using Wireshark

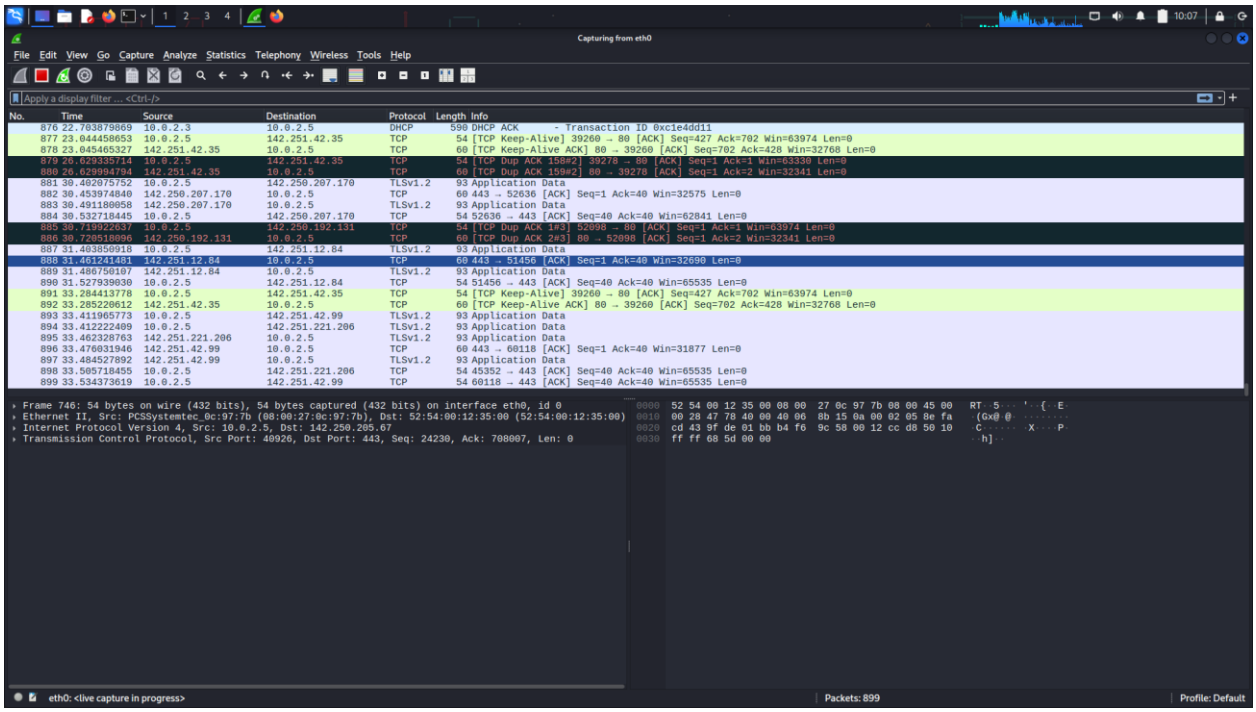
The goal of this task is to capture live network packets, identify basic protocols, and analyze traffic types using **Wireshark**.

Steps

- Installed and launched Wireshark.
- Selected the active network interface (**Wi-Fi/Ethernet**).
- Started packet capture while browsing websites and pinging a server



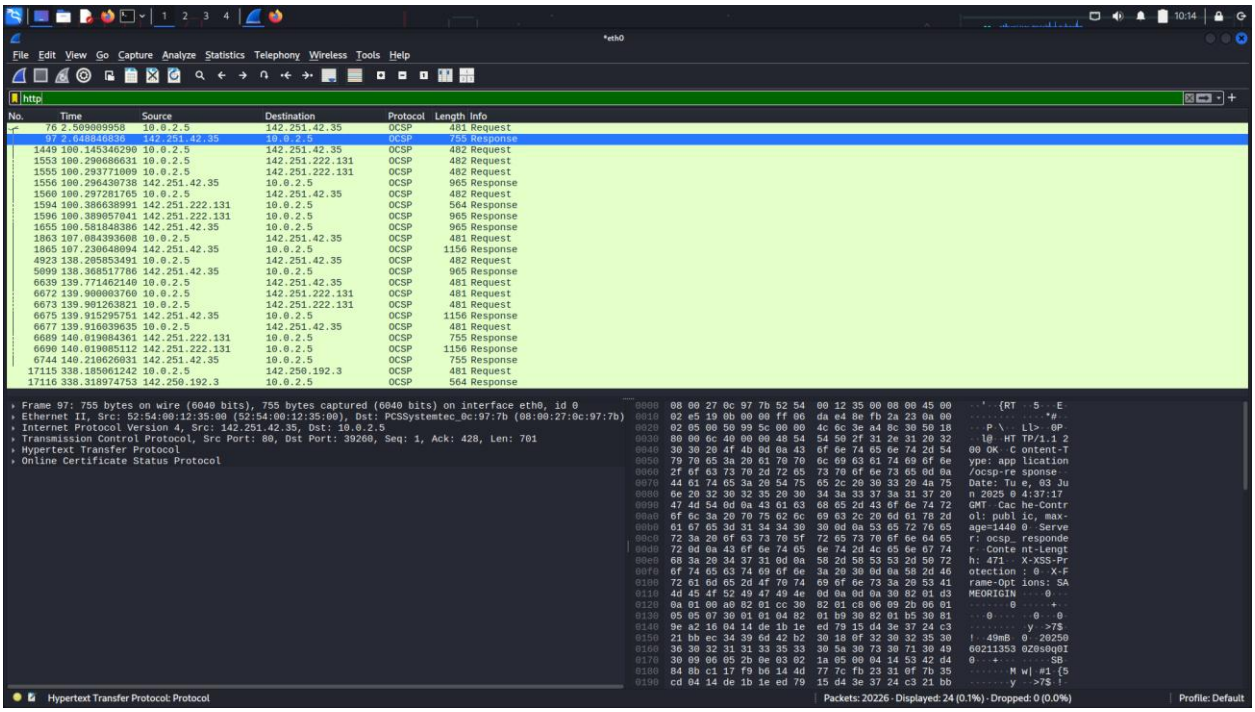
- I capture the traffic from eth0



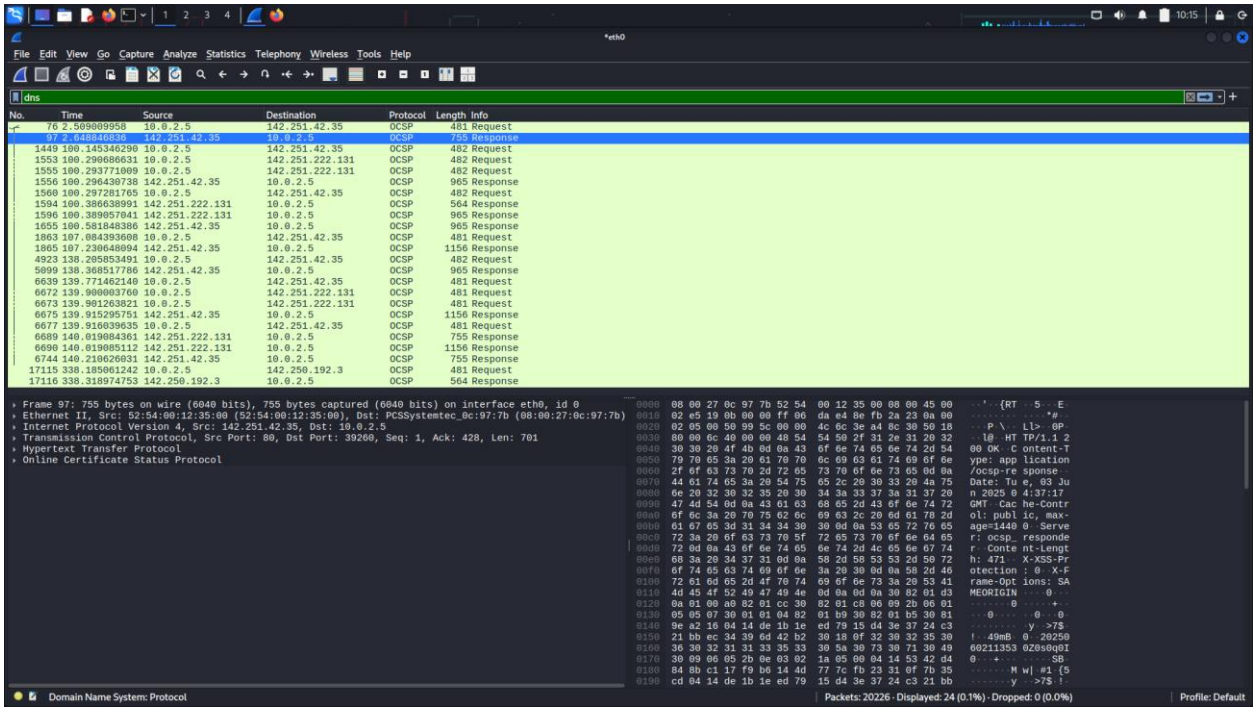
After running the capture for about **1 minute**, packet analysis began by applying filters:

- **HTTP** (http) → Displayed web browsing traffic.
- **DNS** (dns) → Revealed domain name resolution queries.
- **TCP** (tcp) → Showed connection-based data exchanges

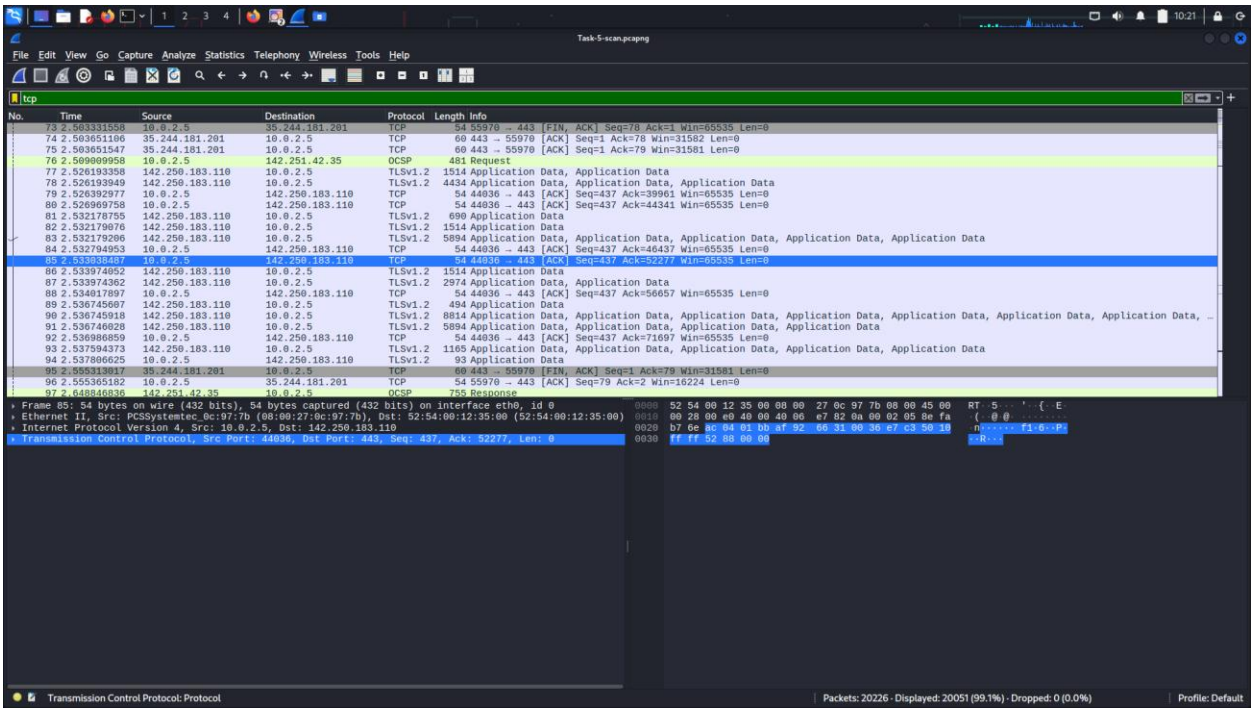
HTTP



DNS


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
No. Time Source Destination Protocol Length Info
76 2.509009958 10.0.2.5 142.251.42.35 OCSP 481 Request
97 2.648846836 142.251.42.35 10.0.2.5 OCSP 755 Response
1449 100.145346290 10.0.2.5 142.251.42.35 OCSP 482 Request
1553 100.290686631 10.0.2.5 142.251.222.131 OCSP 482 Request
1555 100.293771009 10.0.2.5 142.251.222.131 OCSP 482 Request
1556 100.296430738 142.251.42.35 10.0.2.5 OCSP 965 Response
1560 100.297281765 10.0.2.5 142.251.42.35 OCSP 482 Request
1594 100.386638991 142.251.222.131 10.0.2.5 OCSP 564 Response
1596 100.389057041 142.251.222.131 10.0.2.5 OCSP 965 Response
1655 100.581848386 142.251.42.35 10.0.2.5 OCSP 965 Response
1863 107.084393608 10.0.2.5 142.251.42.35 OCSP 481 Request
1865 107.230648094 142.251.42.35 10.0.2.5 OCSP 1156 Response
4923 138.205853491 10.0.2.5 142.251.42.35 OCSP 482 Request
5099 138.368517786 142.251.42.35 10.0.2.5 OCSP 965 Response
6639 139.771462140 10.0.2.5 142.251.42.35 OCSP 481 Request
6672 139.900003760 10.0.2.5 142.251.222.131 OCSP 481 Request
6673 139.901263821 10.0.2.5 142.251.222.131 OCSP 481 Request
6675 139.915295751 142.251.42.35 10.0.2.5 OCSP 1156 Response
6677 139.916039635 10.0.2.5 142.251.42.35 OCSP 481 Request
6689 140.019084361 142.251.222.131 10.0.2.5 OCSP 755 Response
6690 140.019085112 142.251.222.131 10.0.2.5 OCSP 1156 Response
6744 140.210626031 142.251.42.35 10.0.2.5 OCSP 755 Response
17115 338.185061242 10.0.2.5 142.250.192.3 OCSP 481 Request
17116 338.318974753 142.250.192.3 10.0.2.5 OCSP 564 Response
Frame 97: 755 bytes on wire (6040 bits), 755 bytes captured (6040 bits) on interface eth0, id 0
Ethernet II, Src: 52:54:00:12:35:00 (52:54:00:12:35:00), Dst: PCSSystemtec_0c:97:7b (08:00:27:0c:97:7b)
Internet Protocol Version 4, Src: 142.251.42.35, Dst: 10.0.2.5
Transmission Control Protocol, Src Port: 80, Dst Port: 39260, Seq: 1, Ack: 428, Len: 701
Hypertext Transfer Protocol
Online Certificate Status Protocol
Domain Name System: Protocol
Packets: 20226 · Displayed: 24 (0.1%) · Dropped: 0 (0.0%)
Profile: Default

TCP


Task-5-scan.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp
No. Time Source Destination Protocol Length Info
73 2.503331558 10.0.2.5 35.244.181.201 TCP 54 55970 → 443 [FIN, ACK] Seq=78 Ack=1 Win=65535 Len=0
74 2.503651106 35.244.181.201 10.0.2.5 TCP 60 443 → 55970 [ACK] Seq=1 Ack=78 Win=31582 Len=0
75 2.503651547 35.244.181.201 10.0.2.5 TCP 60 443 → 55970 [ACK] Seq=1 Ack=79 Win=31581 Len=0
76 2.509009958 10.0.2.5 142.251.42.35 OCSP 481 Request
77 2.526193358 142.250.183.110 10.0.2.5 TLSv1.2 1514 Application Data, Application Data
78 2.526193949 142.250.183.110 10.0.2.5 TLSv1.2 4434 Application Data, Application Data, Application Data
79 2.526392977 10.0.2.5 142.250.183.110 TCP 54 44036 → 443 [ACK] Seq=437 Ack=39961 Win=65535 Len=0
80 2.526969758 10.0.2.5 142.250.183.110 TCP 54 44036 → 443 [ACK] Seq=437 Ack=44341 Win=65535 Len=0
81 2.532178755 142.250.183.110 10.0.2.5 TLSv1.2 690 Application Data
82 2.532179076 142.250.183.110 10.0.2.5 TLSv1.2 1514 Application Data
83 2.532179206 142.250.183.110 10.0.2.5 TLSv1.2 5894 Application Data, Application Data, Application Data, Application Data
84 2.532794953 10.0.2.5 142.250.183.110 TCP 54 44036 → 443 [ACK] Seq=437 Ack=46437 Win=65535 Len=0
85 2.533038487 10.0.2.5 142.250.183.110 TCP 54 44036 → 443 [ACK] Seq=437 Ack=52277 Win=65535 Len=0
86 2.533974052 142.250.183.110 10.0.2.5 TLSv1.2 1514 Application Data
87 2.533974362 142.250.183.110 10.0.2.5 TLSv1.2 2974 Application Data, Application Data
88 2.534017897 10.0.2.5 142.250.183.110 TCP 54 44036 → 443 [ACK] Seq=437 Ack=56657 Win=65535 Len=0
89 2.536745607 142.250.183.110 10.0.2.5 TLSv1.2 494 Application Data
90 2.536745918 142.250.183.110 10.0.2.5 TLSv1.2 8814 Application Data, Application Data, Application Data, Application Data, Application Data, Application Data, …
91 2.536746028 142.250.183.110 10.0.2.5 TLSv1.2 5894 Application Data, Application Data, Application Data, Application Data
92 2.536986859 10.0.2.5 142.250.183.110 TCP 54 44036 → 443 [ACK] Seq=437 Ack=71697 Win=65535 Len=0
93 2.537594373 142.250.183.110 10.0.2.5 TLSv1.2 1165 Application Data, Application Data, Application Data, Application Data
94 2.537806625 10.0.2.5 142.250.183.110 TLSv1.2 93 Application Data
95 2.555313017 35.244.181.201 10.0.2.5 TCP 60 443 → 55970 [FIN, ACK] Seq=1 Ack=79 Win=31581 Len=0
96 2.555365182 10.0.2.5 35.244.181.201 TCP 54 55970 → 443 [ACK] Seq=79 Ack=2 Win=16224 Len=0
97 2.648846836 142.251.42.35 10.0.2.5 OCSP 755 Response
Frame 85: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id 0
Ethernet II, Src: PCSSystemtec_0c:97:7b (08:00:27:0c:97:7b), Dst: 52:54:00:12:35:00 (52:54:00:12:35:00)
Internet Protocol Version 4, Src: 10.0.2.5, Dst: 142.250.183.110
Transmission Control Protocol, Src Port: 44036, Dst Port: 443, Seq: 437, Ack: 52277, Len: 0
Transmission Control Protocol: Protocol
Packets: 20226 · Displayed: 20051 (99.1%) · Dropped: 0 (0.0%)
Profile: Default

Observations & Insights

- **Web traffic behavior**: HTTP requests indicated website interaction.
- **DNS resolution**: Queries showed hostname-to-IP translations.
- **TCP handshake & communication**: Tracked reliable data exchange.

Conclusion

By performing this **packet capture and protocol analysis**, insights into real-world network communication were gained. This exercise enhanced practical networking skills and improved understanding of data flow across the internet.