Task 5 – Capture and Analyze Network Traffic Using Wireshark

1. Objective

The objective of this task was to capture live network packets using Wireshark and analyze them to identify basic protocols (DNS, HTTP, TCP) and their traffic characteristics.

2. Tools Used

- Wireshark (Network Protocol Analyzer)
- Operating System: [Your OS, e.g., Kali Linux/Windows]

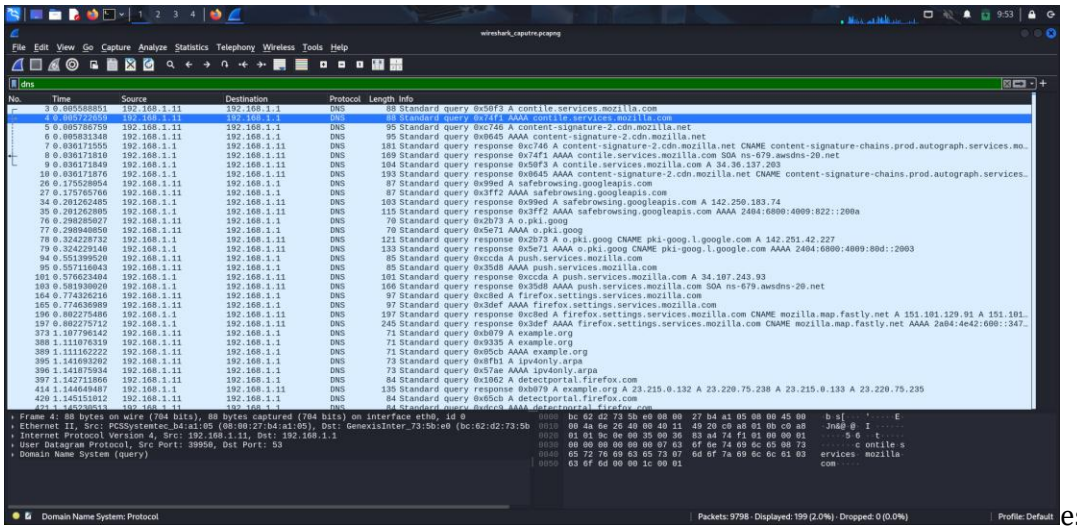
3. Methodology

1. Installed Wireshark and started capture on active interface.
2. Generated traffic by browsing websites and pinging servers.
3. Stopped capture after 1–2 minutes.
4. Applied filters (dns, http, tcp) to analyze specific protocols.
5. Saved capture as wireshark_capture.pcap.
6. Exported screenshots of findings.

4. Findings

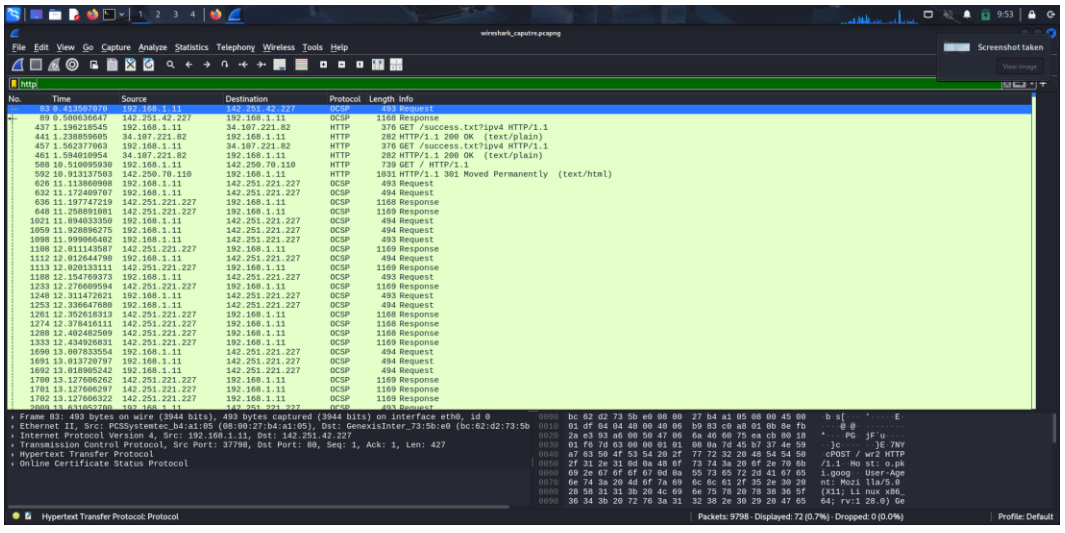
a) DNS (Domain Name System)

DNS queries and responses were captured.
Example: Query for contile.services.mozilla.com.
This shows how the system resolve domain names into IP addresses.


es

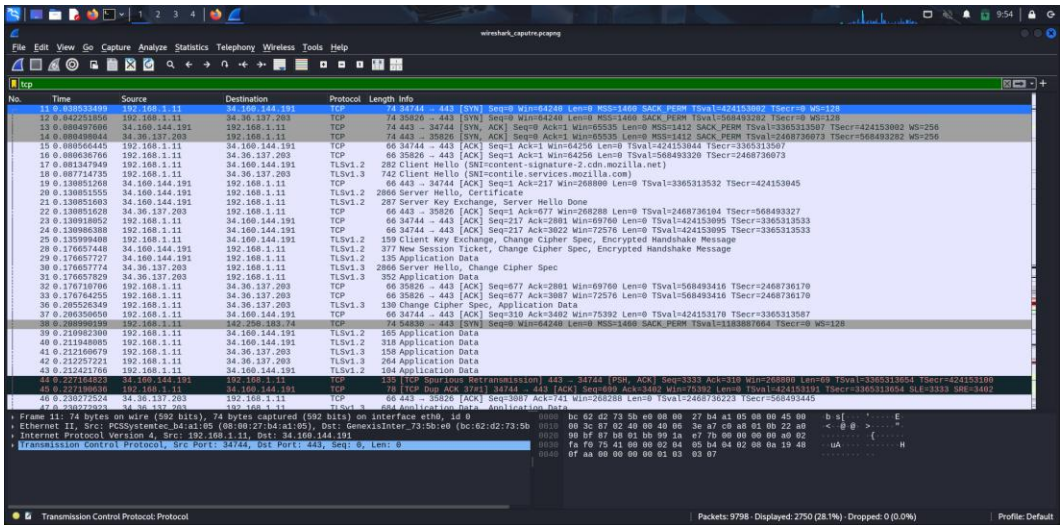
b) HTTP (Hypertext Transfer Protocol)

HTTP GET requests and responses were observed.
Example: GET /success.txt?ipv4 HTTP/1.1 request, responded with 200 OK.
This confirms successful client-server communication.



c) TCP (Transmission Control Protocol)

TCP handshake packets (SYN, SYN-ACK, ACK) were captured.
Example: Connection to 34.160.144.191 using port 443 (HTTPS).
Also observed TLS handshake packets, showing encrypted traffic.



5. Conclusion

Through this task, I gained practical experience in:

- Capturing live packets with Wireshark.
- Applying filters to focus on specific protocols.
- Understanding how DNS resolves domains, how HTTP transmits data, and how TCP establishes connections.

This strengthened my protocol analysis and troubleshooting skills.