Task 3: Networking Basics for Cyber Security

1. Introduction

This report is prepared as part of **Task 3: Networking Basics for Cyber Security**.
The objective of this task is to understand basic networking concepts and analyze live network traffic using packet sniffing tools.

2. Tool Used

- **Wireshark** – A network packet analyzer used to capture and inspect network traffic in real time.

3. Objective of the Task

- To capture live network traffic
- To analyze DNS, TCP, HTTP, and HTTPS packets
- To understand the difference between plain-text and encrypted communication
- To observe the TCP three-way handshake

4. Methodology

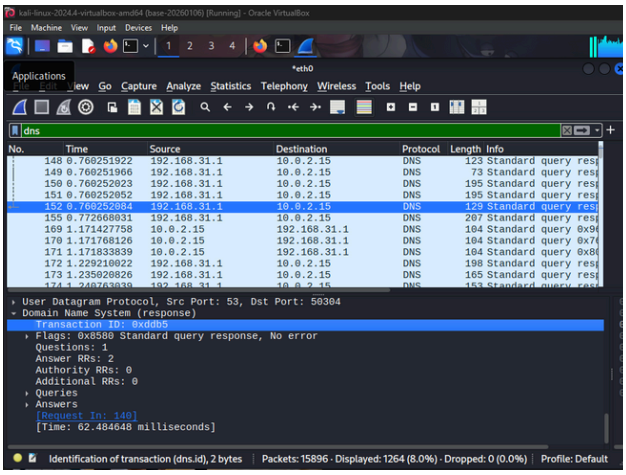
The following steps were performed to complete the task:

1. Installed Wireshark on the system
2. Selected the active network interface and started packet capture
3. Generated network traffic by visiting HTTP and HTTPS websites
4. Applied protocol filters such as HTTP, DNS, TCP, and TLS
5. Observed packet details and communication behavior
6. Saved the captured packets for further analysis

5. Observations

5.1 DNS Traffic Analysis

DNS packets were captured when websites were accessed.
The DNS protocol was used to resolve domain names into IP addresses.

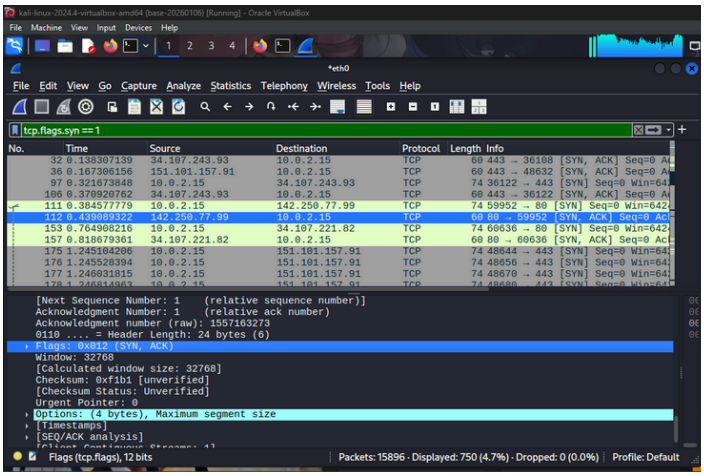


5.2 TCP Three-Way Handshake

The TCP three-way handshake was observed during communication setup.
The handshake consists of:

- SYN
- SYN-ACK
- ACK

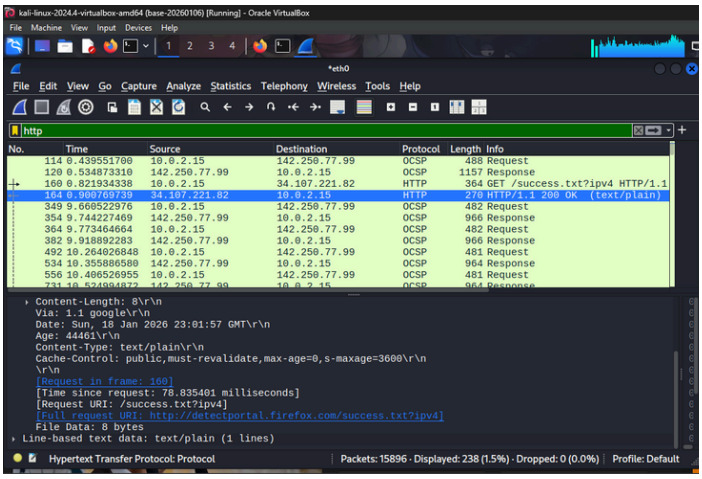
This process ensures a reliable connection between the client and server.



5.3 Plain-Text Traffic (HTTP)

When accessing an HTTP website, packet contents were visible in readable format.
Details such as request method, host name, and user-agent were clearly visible.

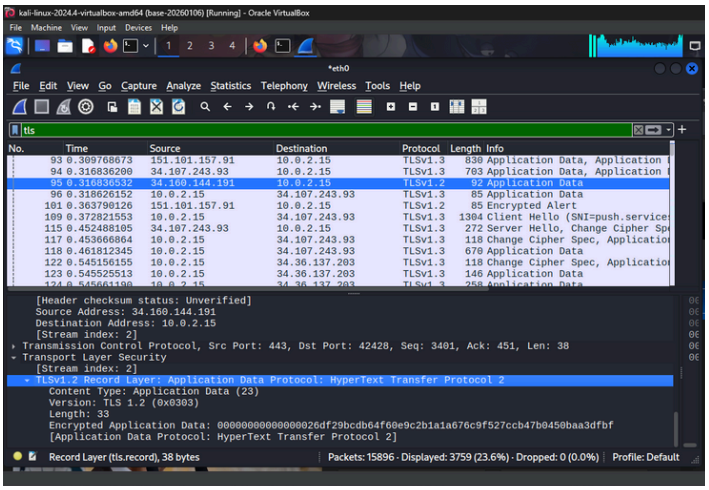
This shows that HTTP traffic is **not secure** and can be easily read by attackers.



5.4 Encrypted Traffic (HTTPS)

When accessing HTTPS websites, the captured packets were encrypted using TLS.
The packet contents were not readable and appeared as encrypted application data.

This demonstrates that HTTPS provides secure communication.



6. Difference Between HTTP and HTTPS

HTTP	HTTPS
Data is plain text	Data is encrypted
Not secure	Secure
Easily readable	Not readable
Vulnerable to attacks	Protected using TLS

7. Learning Outcome

Through this task, I learned how to capture and analyze network traffic using Wireshark.
I gained practical understanding of packet sniffing, TCP communication, DNS resolution, and the importance of encrypted communication in cyber security.

8. Conclusion

This task helped in developing foundational skills in network traffic analysis, which is an essential part of cyber security and network monitoring.