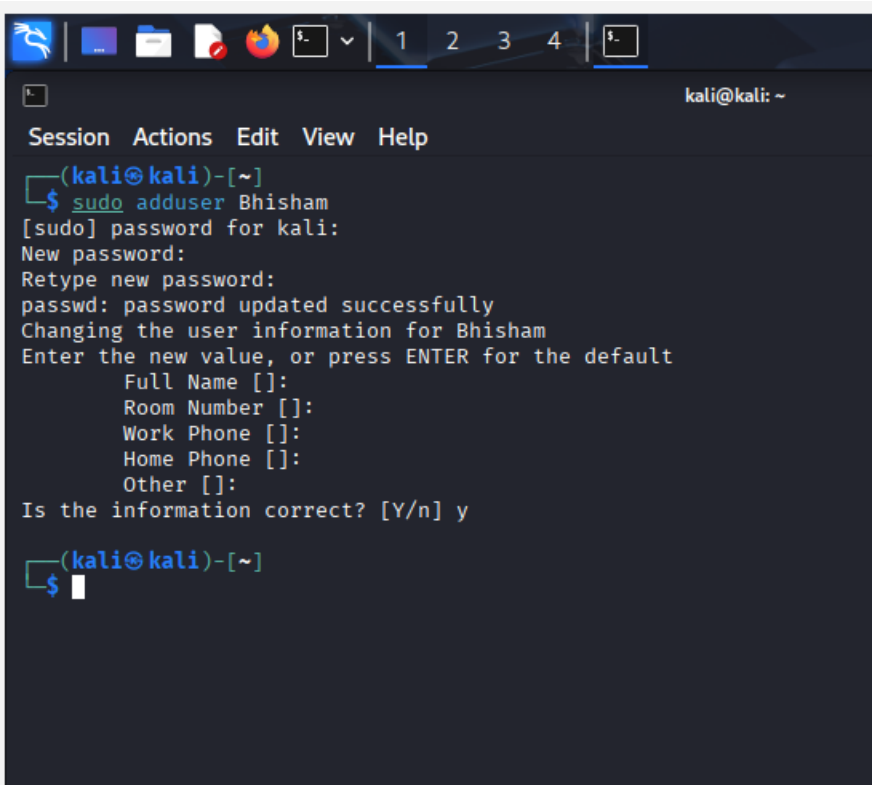
# Project-2: Comparative Analysis of Telnet and SSH Using Wireshark –

*By: Bhisham Sahu*

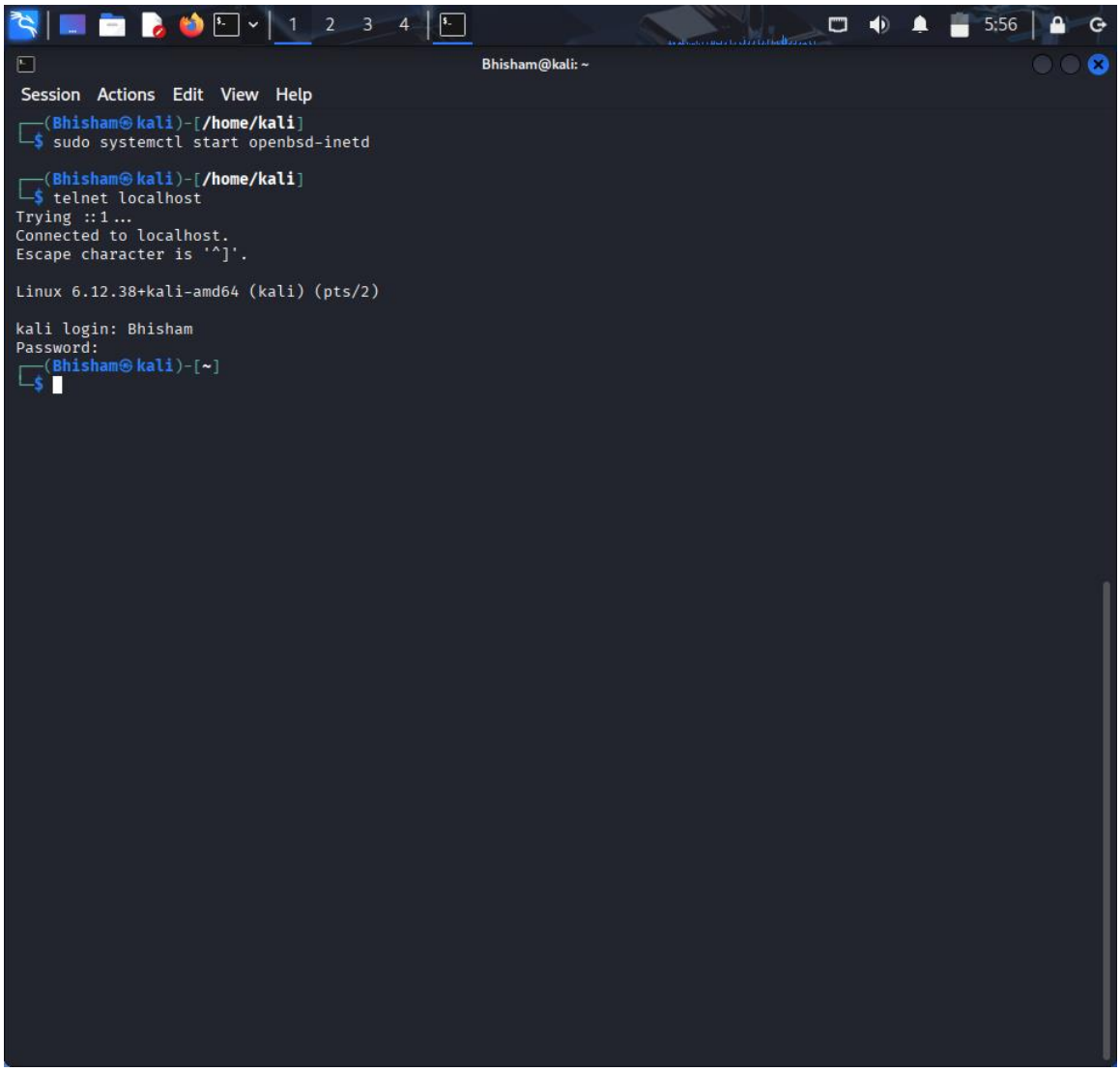
## 1. Kali Linux Hostname / User Configuration:

A non-root user (Bhisham) was created on Kali Linux and user switching was successfully performed to simulate a real-world multi-user operating environment.



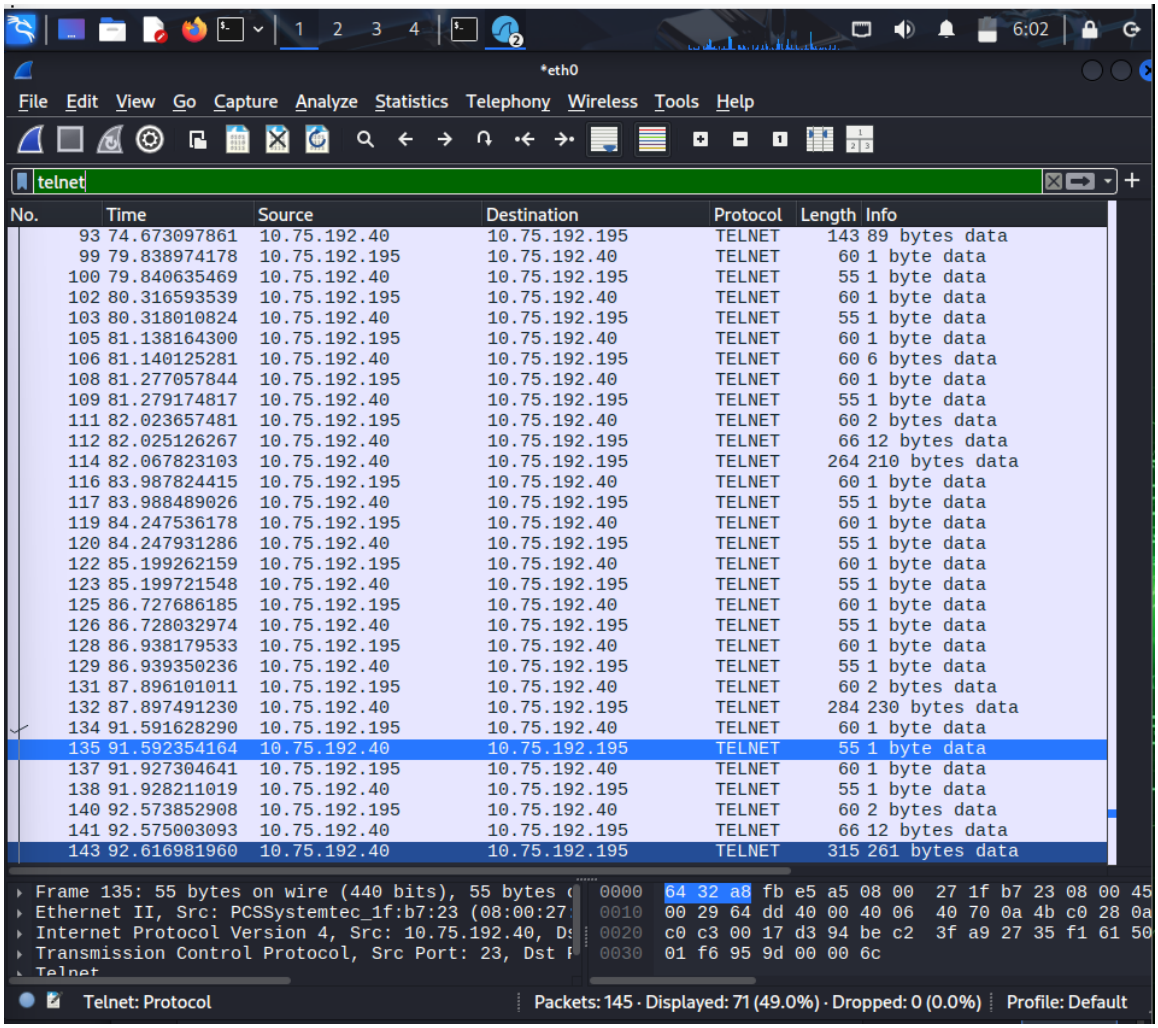
## 2. Telnet Service Configuration and Activation:

The Telnet service was enabled using openbsd-inetd, allowing plaintext communication for demonstrating protocol-level security weaknesses.



## 3.Wireshark Capturing Telnet Traffic:

Wireshark was used to capture Telnet network traffic on TCP port 23, enabling packet-level inspection of unencrypted data.

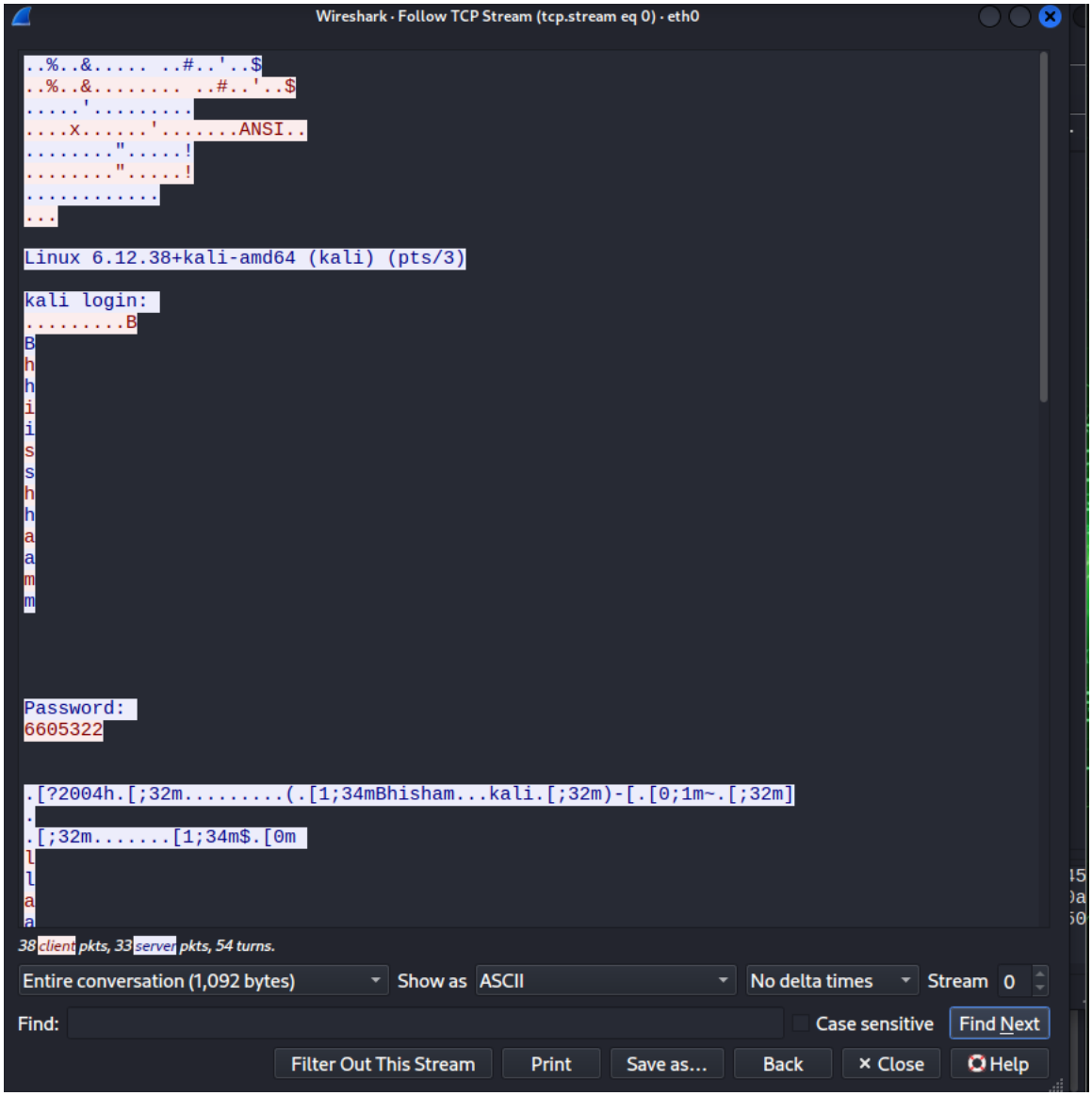


## 4. Telnet Login and Command Execution:

A successful Telnet login was performed from a Windows client, and commands were executed on the Kali Linux server.

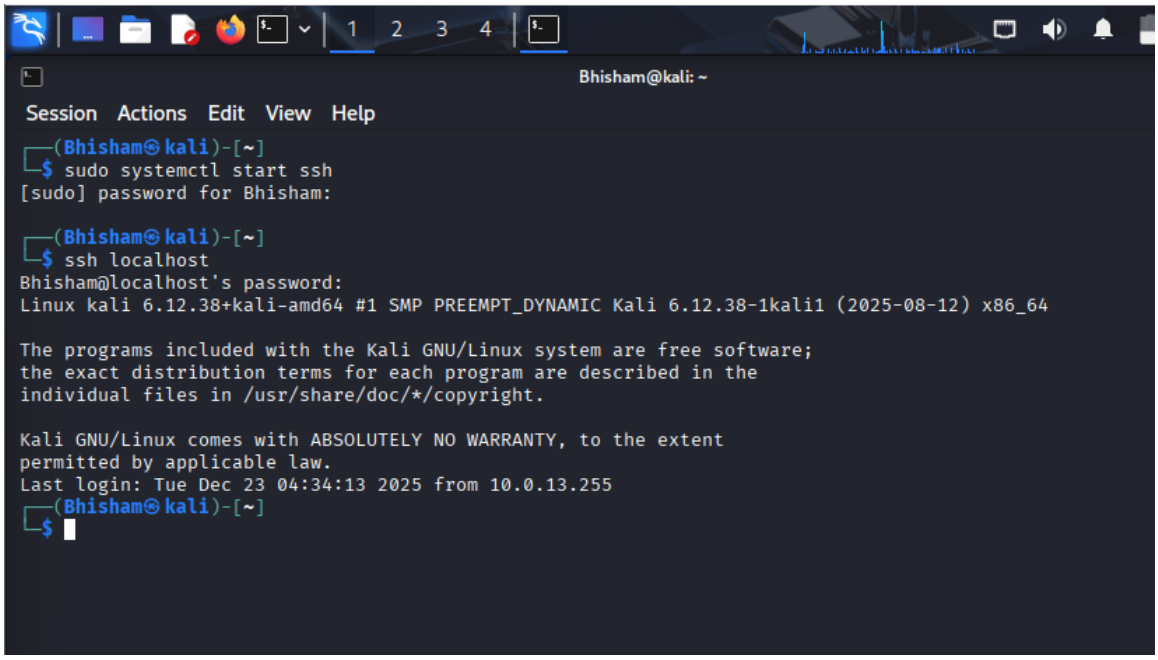

## 5. Plain-text Credentials Visible in Packets:

Usernames, passwords, and commands were observed in readable plaintext within the Telnet TCP stream, confirming the insecure nature of Telnet.



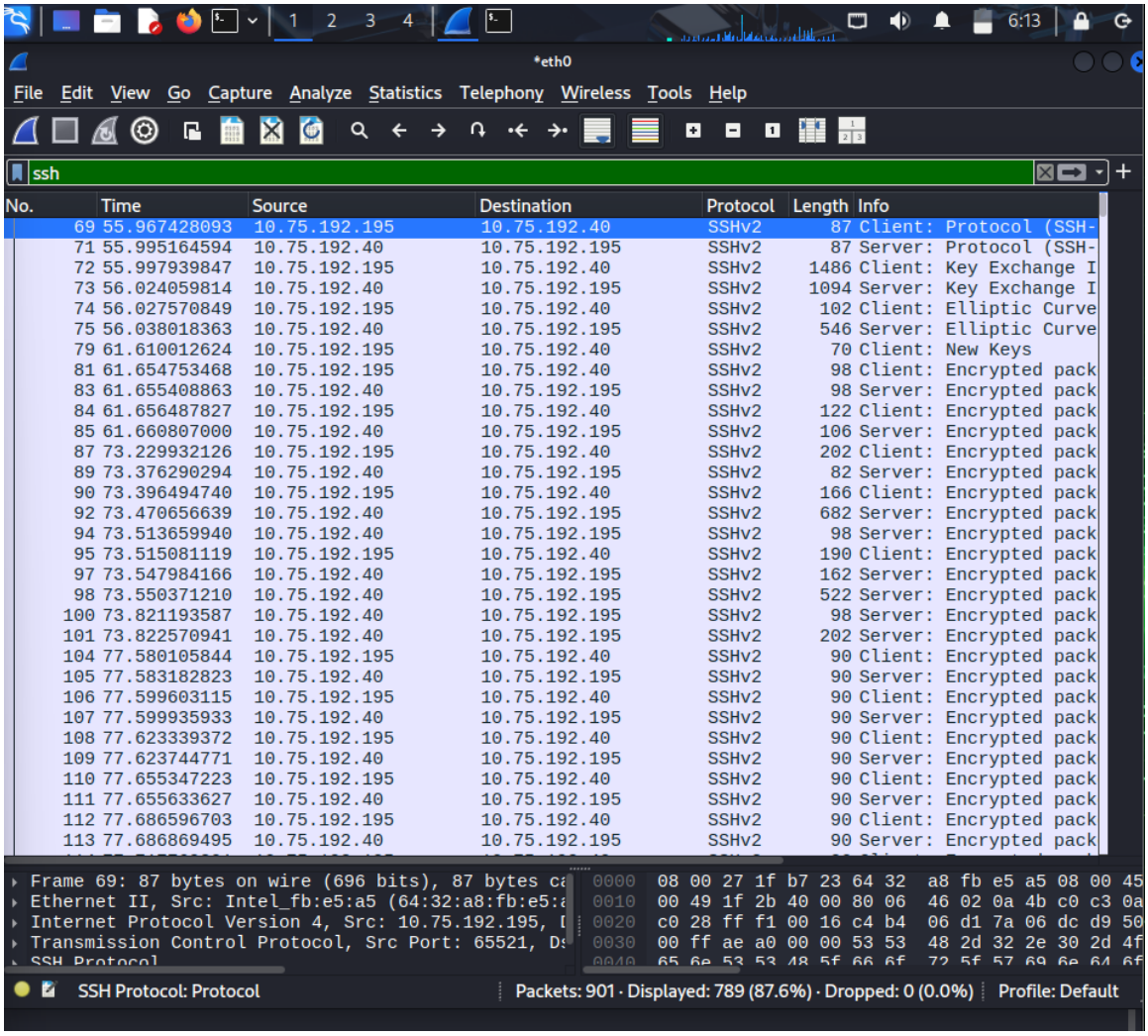

## 6. SSH Service Configuration and Activation:

The SSH service was verified to be active, enabling secure and encrypted remote access.



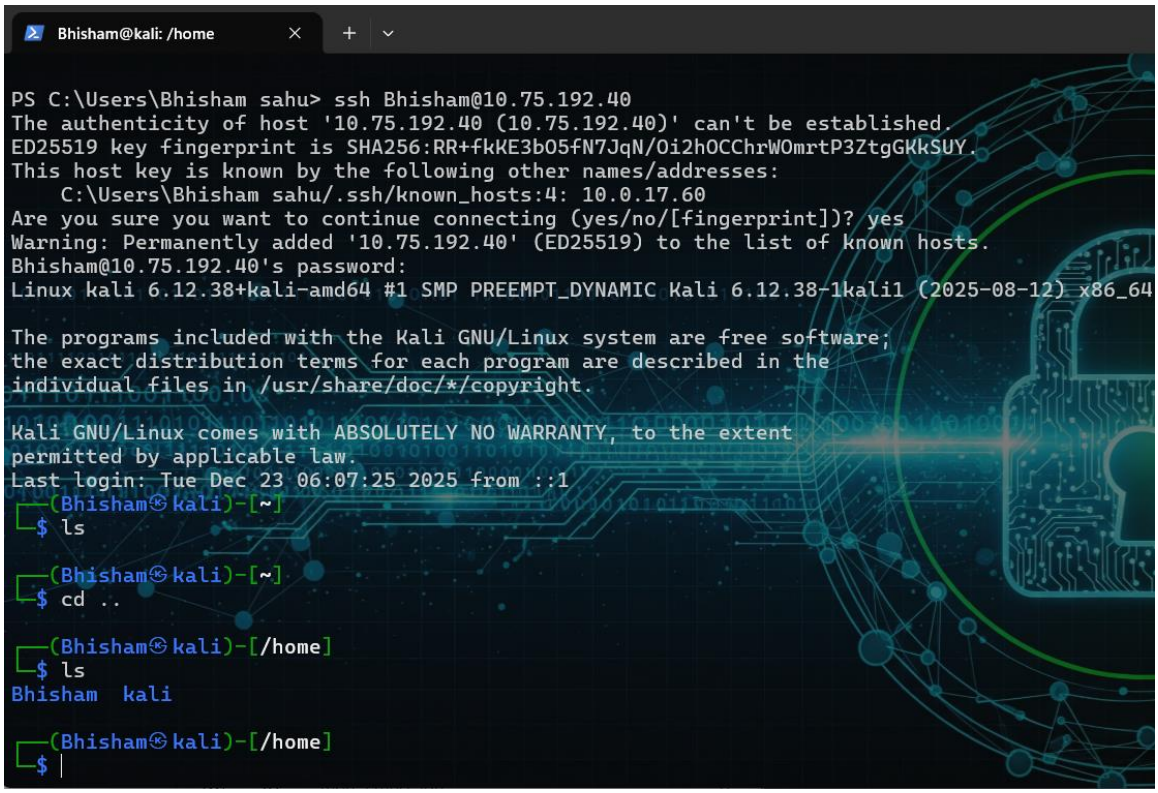

## 7. Wireshark Capturing SSH Traffic:

SSH network traffic was captured on TCP port 22, allowing analysis of encrypted communication.



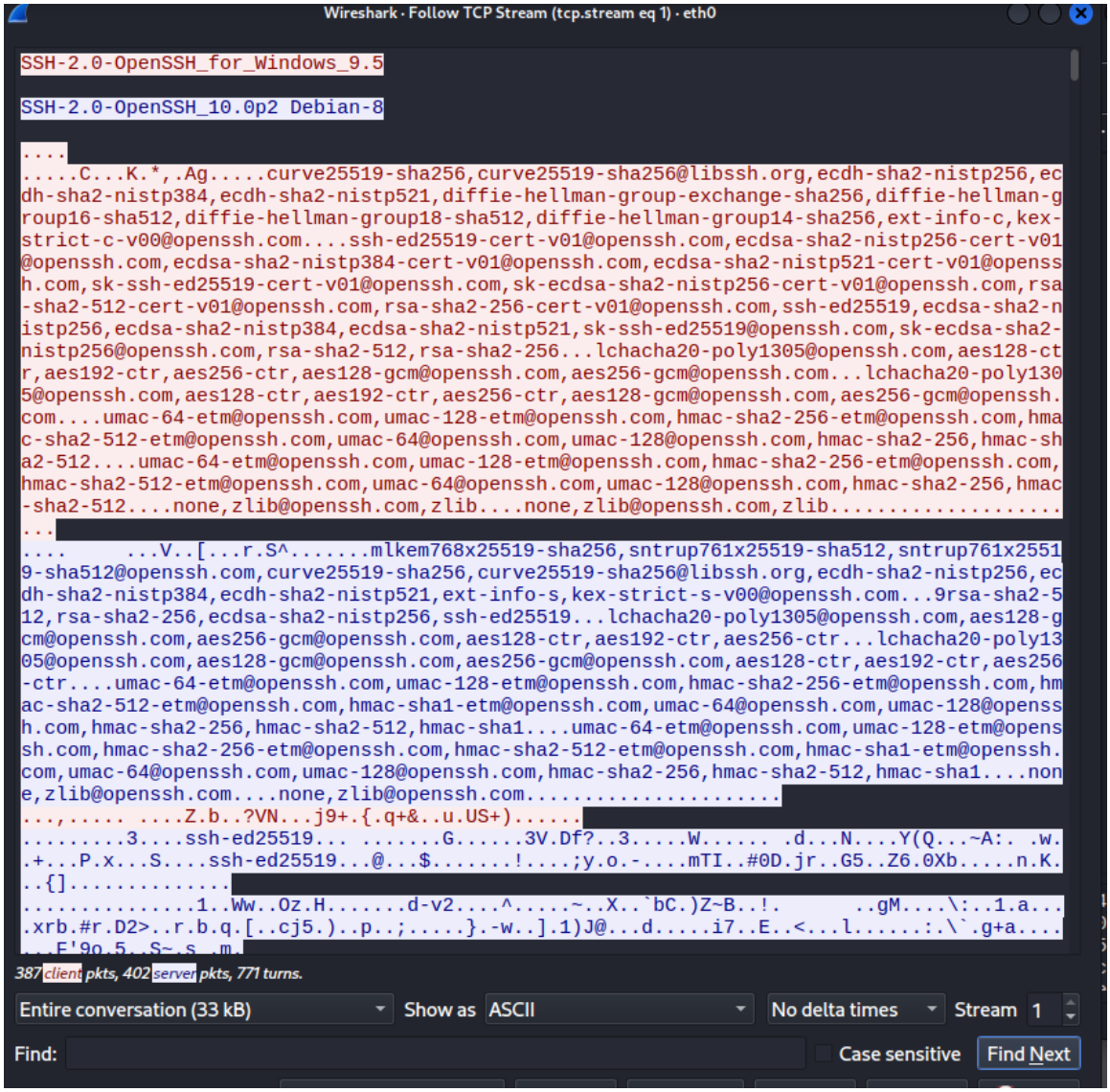

## 8. SSH Login and Command Execution:

Secure authentication and remote command execution were successfully performed using the SSH protocol.




## 9. Encrypted SSH Packets (Unreadable Payload):

The SSH TCP stream payload appeared encrypted and unreadable, demonstrating effective cryptographic protection of data.




## 10. Final Comparison Summary:

This project presents a comparative security analysis of Telnet and SSH using real-time network traffic capture with Wireshark. Telnet was intentionally configured to demonstrate its insecure design, as it transmits usernames, passwords, and commands in plaintext, making it highly vulnerable to packet sniffing attacks. In

contrast, SSH was implemented to provide encrypted communication, ensuring confidentiality and integrity of data even when network traffic is intercepted. The captured packets clearly highlight the difference between unencrypted and encrypted protocols.

Based on the observed results, the project concludes that Telnet should not be used in modern networks, whereas SSH is the secure and industry-standard protocol for remote system administration.