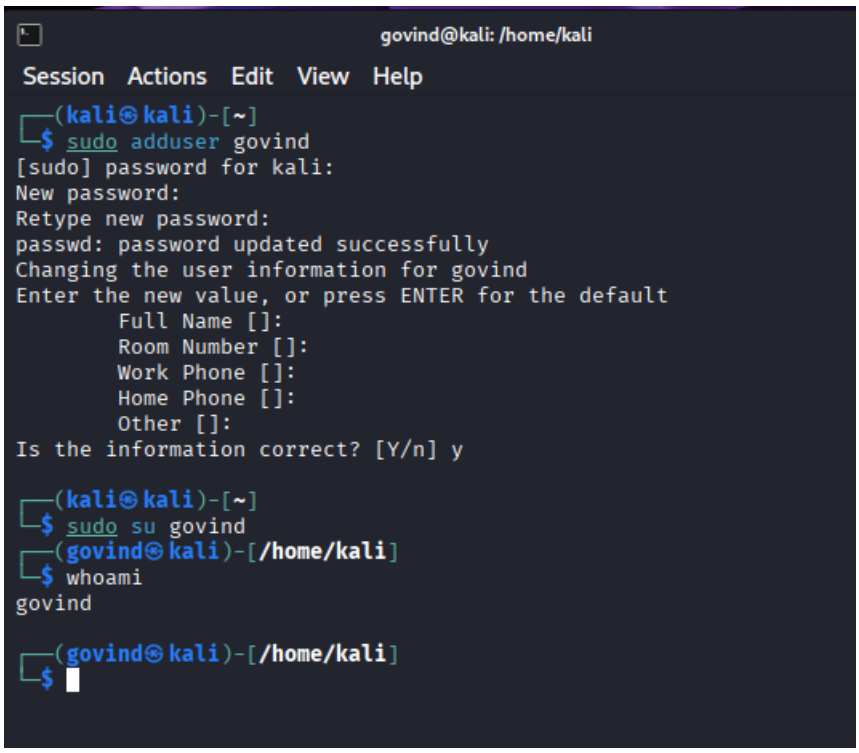
Project-2: Comparative Analysis of Telnet and SSH Using Wireshark -

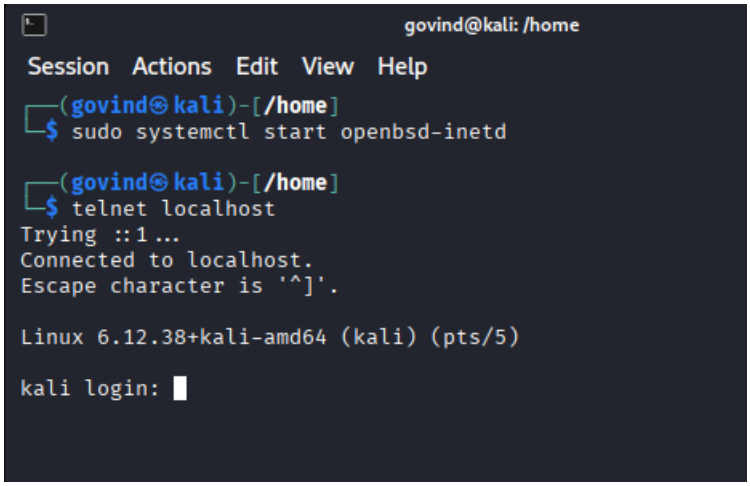
1. Kali Linux Hostname / User Configuration:

A new user (Govind) was created and user switching was tested to simulate real-world non-root access.



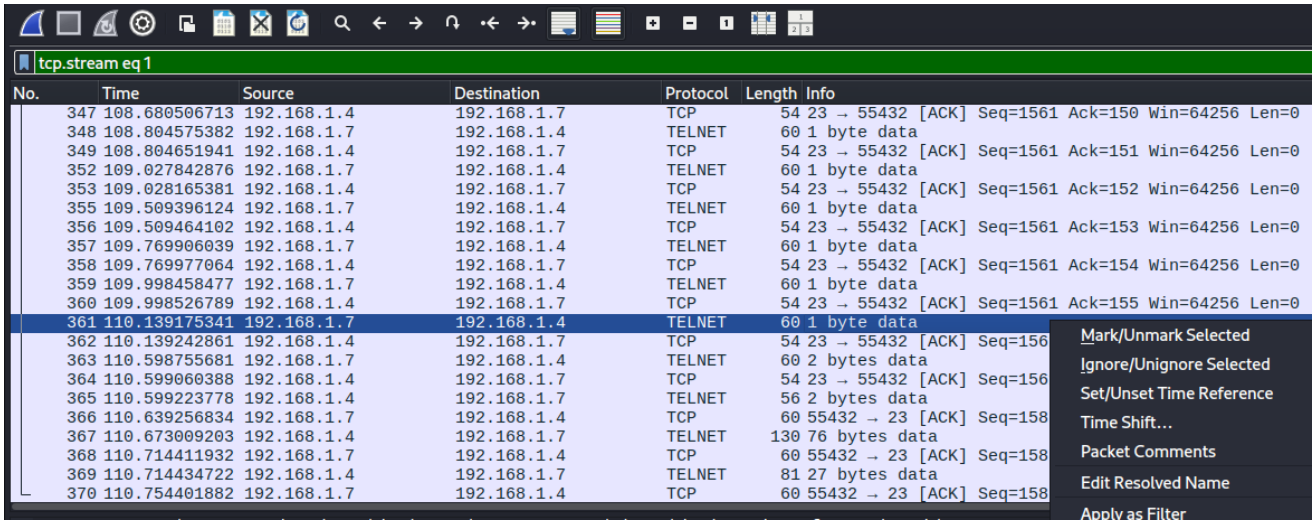
2. Telnet Service Configuration and Activation:

Telnet service was enabled using openbsd-inetd to demonstrate insecure plaintext communication.



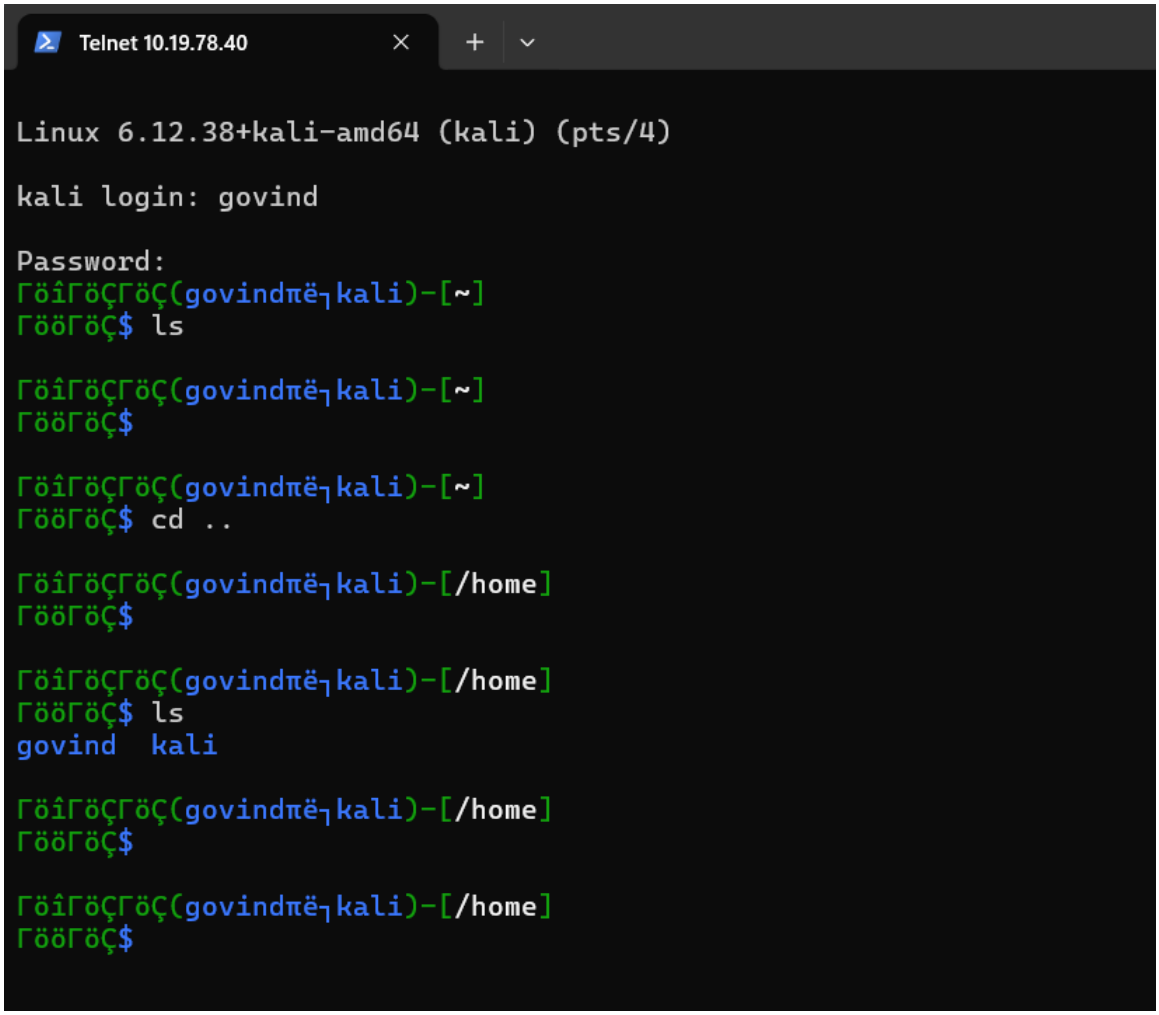
3.Wireshark Capturing Telnet Traffic:

Wireshark was used on Kali Linux to capture Telnet packets on TCP port 23.



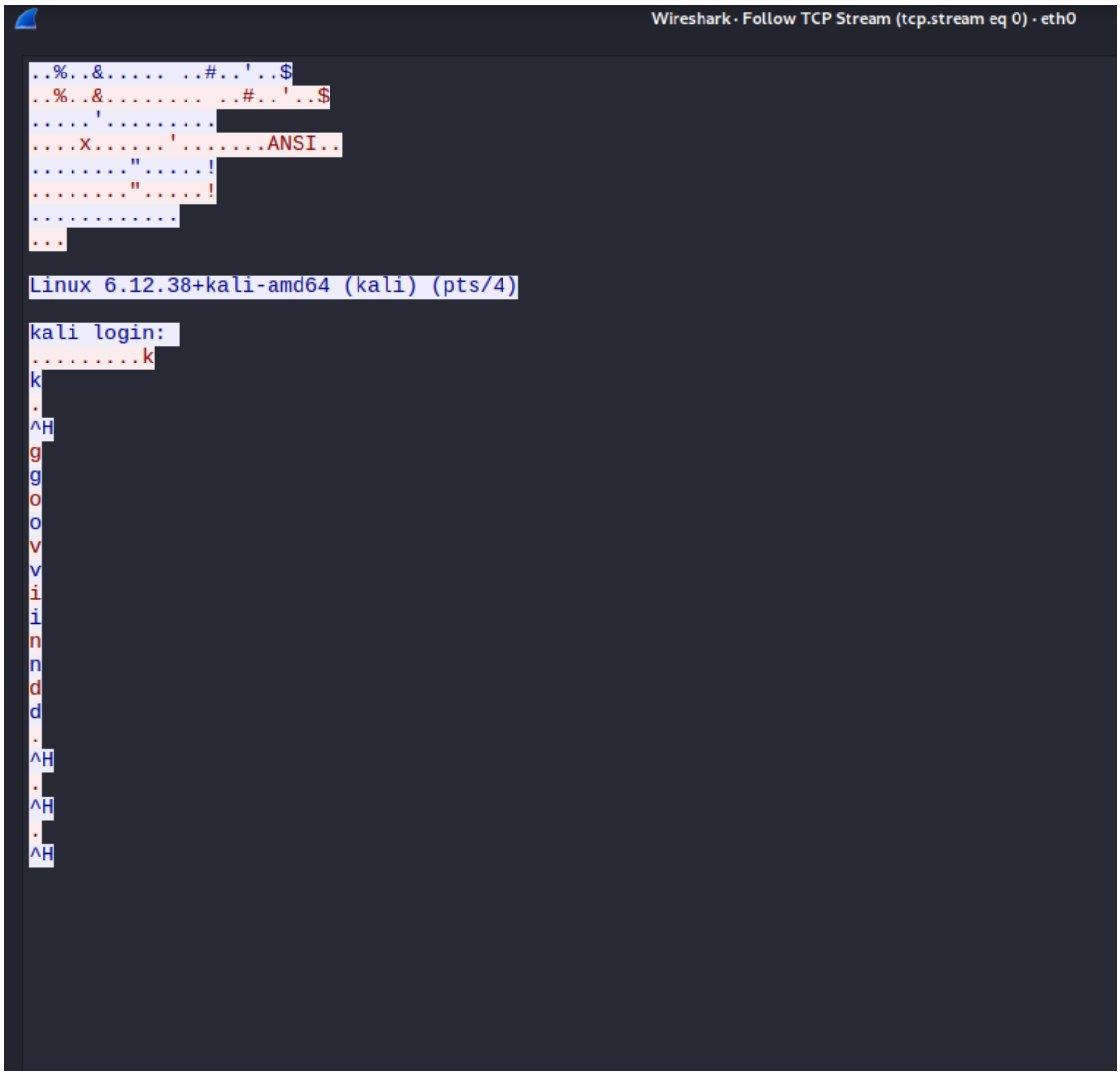
4. Telnet Login and Command Execution:

Telnet login was performed from Windows and commands were executed.



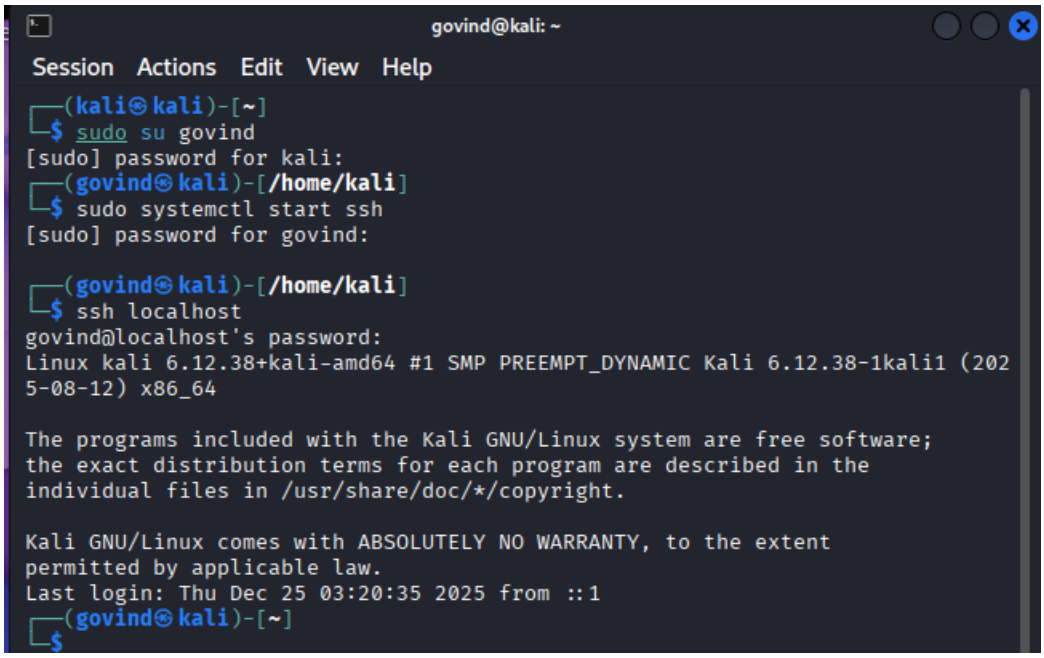
5. Plain-text Credentials Visible in Packets:

Telnet TCP stream shows username and password in plaintext.



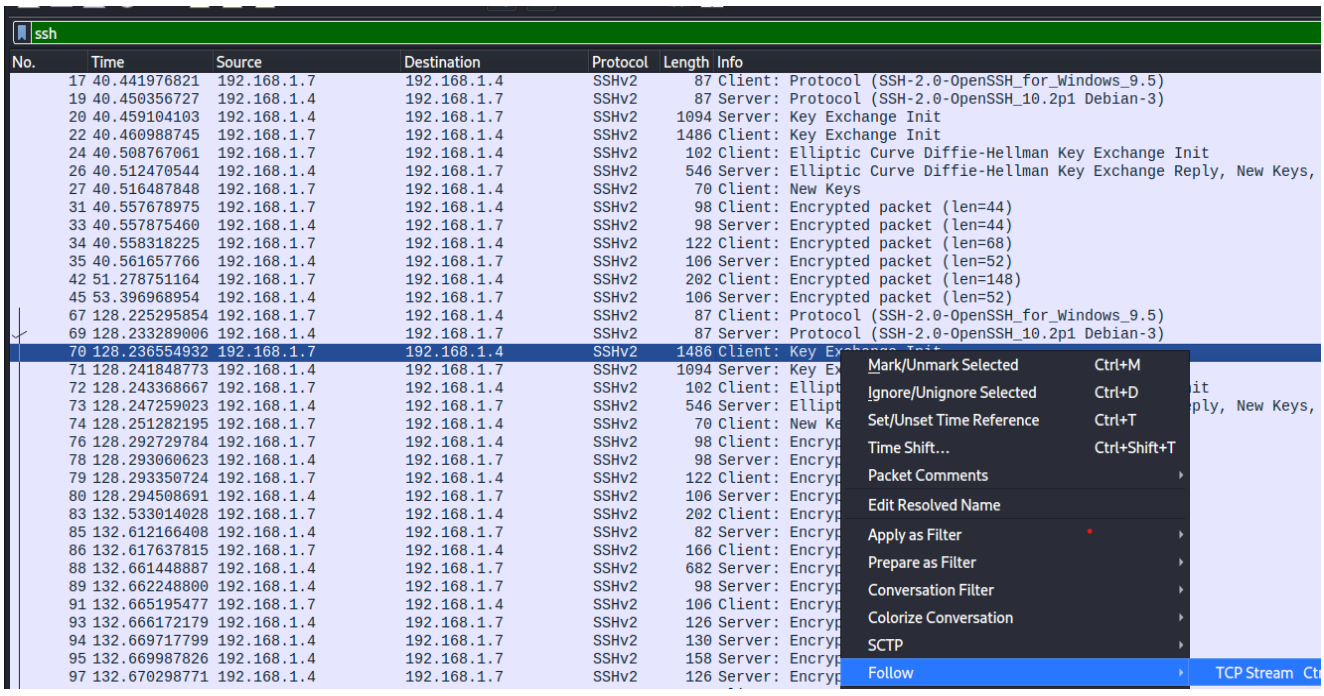
6. SSH Service Configuration and Activation:

SSH service was verified and started on Kali Linux.



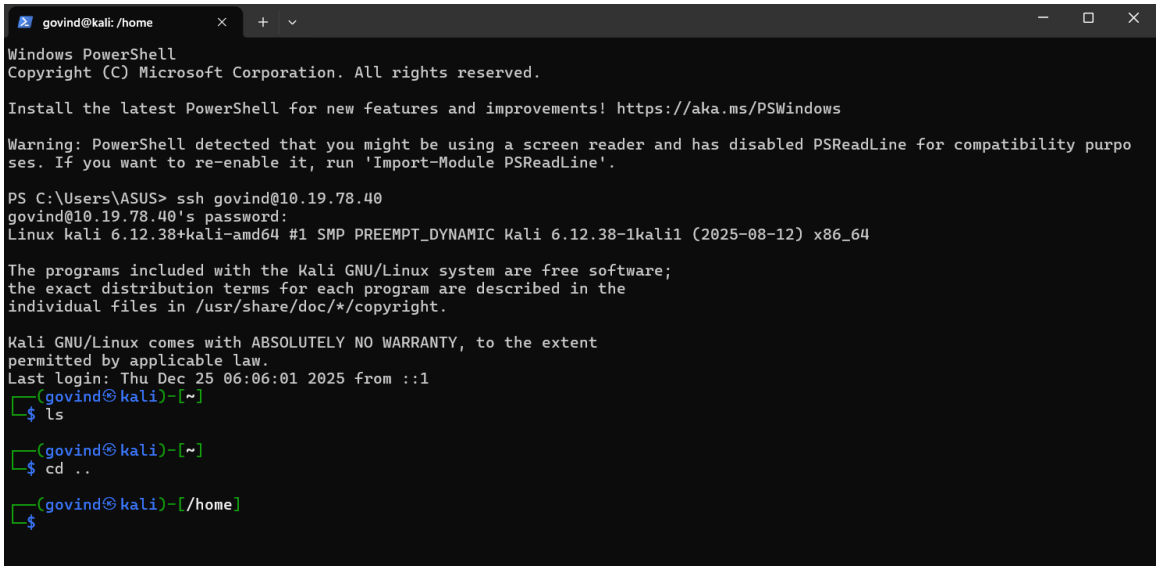
7. Wireshark Capturing SSH Traffic:

Wireshark captured SSH traffic on TCP port 22.



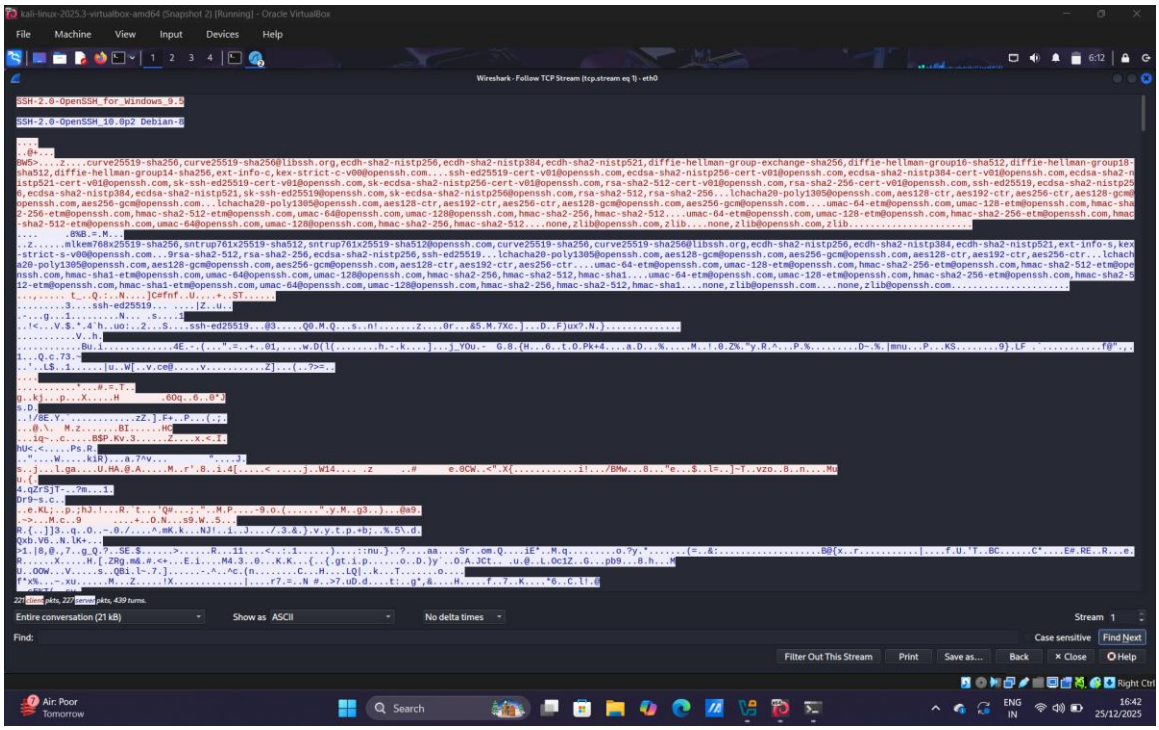
8. SSH Login and Command Execution:

SSH login from Windows to Kali was successful.



9. Encrypted SSH Packets (Unreadable Payload)

SSH TCP stream shows encrypted unreadable payload.



Final Comparison Summary

Telnet transmits credentials in plaintext and is insecure, whereas SSH encrypts all communication, making it safe against packet sniffing attacks.

Telnet runs over TCP port 23 and does not encrypt data. Enabling it intentionally creates an insecure service to demonstrate real-world risks in legacy systems.

Wireshark captures packets at the network interface level. By filtering Telnet traffic, we can clearly observe how data travels without encryption.

User credentials and commands are transmitted directly over the network. This simulates how attackers can sniff sensitive data on unsecured networks.

The visibility of usernames and passwords proves Telnet is insecure. This is a critical vulnerability that violates basic security principles.

SSH replaces Telnet by providing encrypted remote access. It is the industry standard for secure system administration.

Although packets are captured, their content is unreadable. This demonstrates the effectiveness of cryptographic protection.

Even login credentials and commands remain encrypted. This protects users against packet sniffing and man-in-the-middle attacks.

The payload appears as random data due to encryption algorithms. This ensures confidentiality even if traffic is intercepted.

Telnet should never be used in modern networks. SSH is secure, reliable, and resistant to passive network attacks.