



CYBER SECURITY

Protecting the Digital World

Made by:

ADITYA KUMAR SRIVASTAVA

SEMESTER = 3

ERP = 6606491

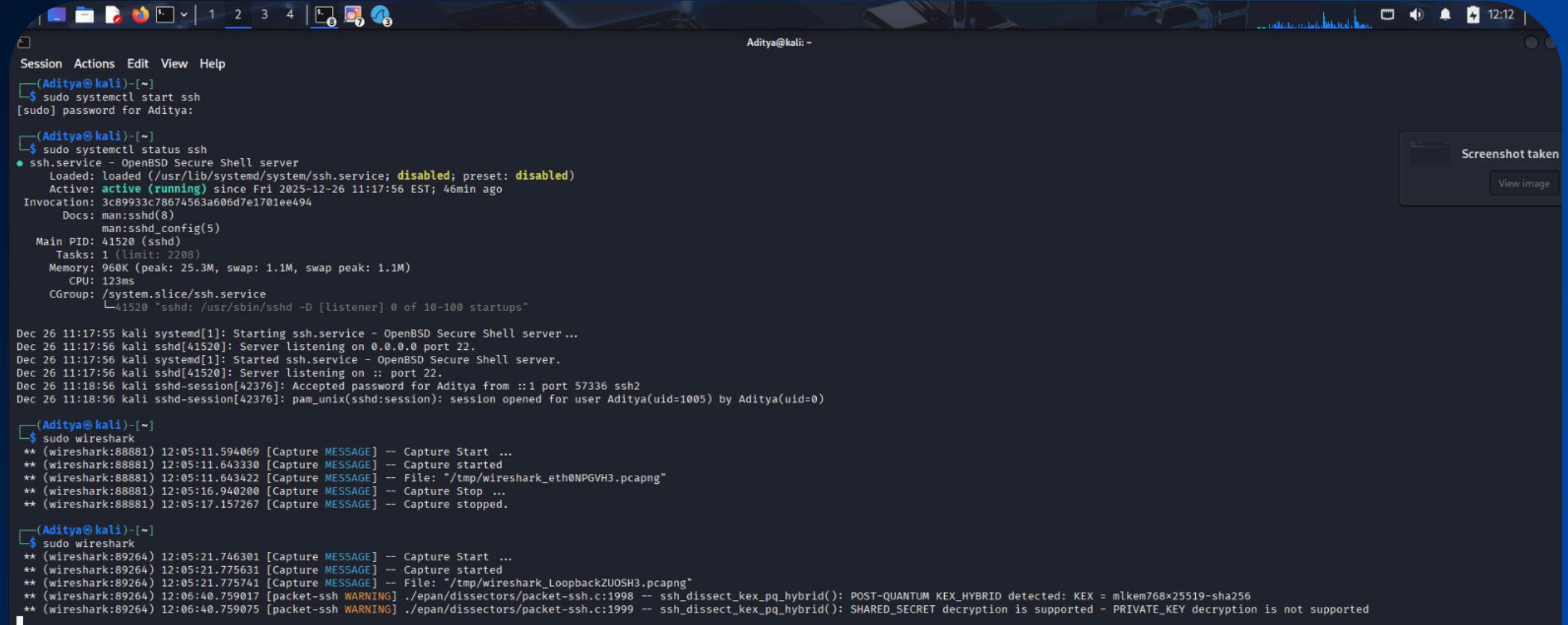
MINOR 1 PROJECT

GROUP G4

KALI LINUX ENVIRONMENT SETUP

The Foundation of Digital Protection

- Kali Linux system initialized successfully.
- Terminal environment ready for network testing.
- Used as attacker machine for experiment.



A screenshot of a Kali Linux desktop environment showing a terminal window. The terminal output shows the following steps:

```
(Aditya㉿kali)-[~]
$ sudo systemctl start ssh
[sudo] password for Aditya:
(Aditya㉿kali)-[~]
$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
  Loaded: loaded (/usr/lib/systemd/system/ssh.service; disabled; preset: disabled)
  Active: active (running) since Fri 2025-12-26 11:17:56 EST; 46min ago
  Invocation: 3c89933c78674563a006d7e1701ee494
    Docs: man:sshd(8)
          man:sshd_config(5)
  Main PID: 41520 (sshd)
    Tasks: 1 (limit: 2208)
   Memory: 960K (peak: 25.3M, swap: 1.1M, swap peak: 1.1M)
     CPU: 123ms
    CGroup: /system.slice/ssh.service
            └─41520 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Dec 26 11:17:55 kali systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
Dec 26 11:17:56 kali sshd[41520]: Server listening on 0.0.0.0 port 22.
Dec 26 11:17:56 kali systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
Dec 26 11:17:56 kali sshd[41520]: Server listening on :: port 22.
Dec 26 11:18:56 kali sshd-session[42376]: Accepted password for Aditya from ::1 port 57336 ssh2
Dec 26 11:18:56 kali sshd-session[42376]: pam_unix(sshd:session): session opened for user Aditya(uid=1005) by Aditya(uid=0)

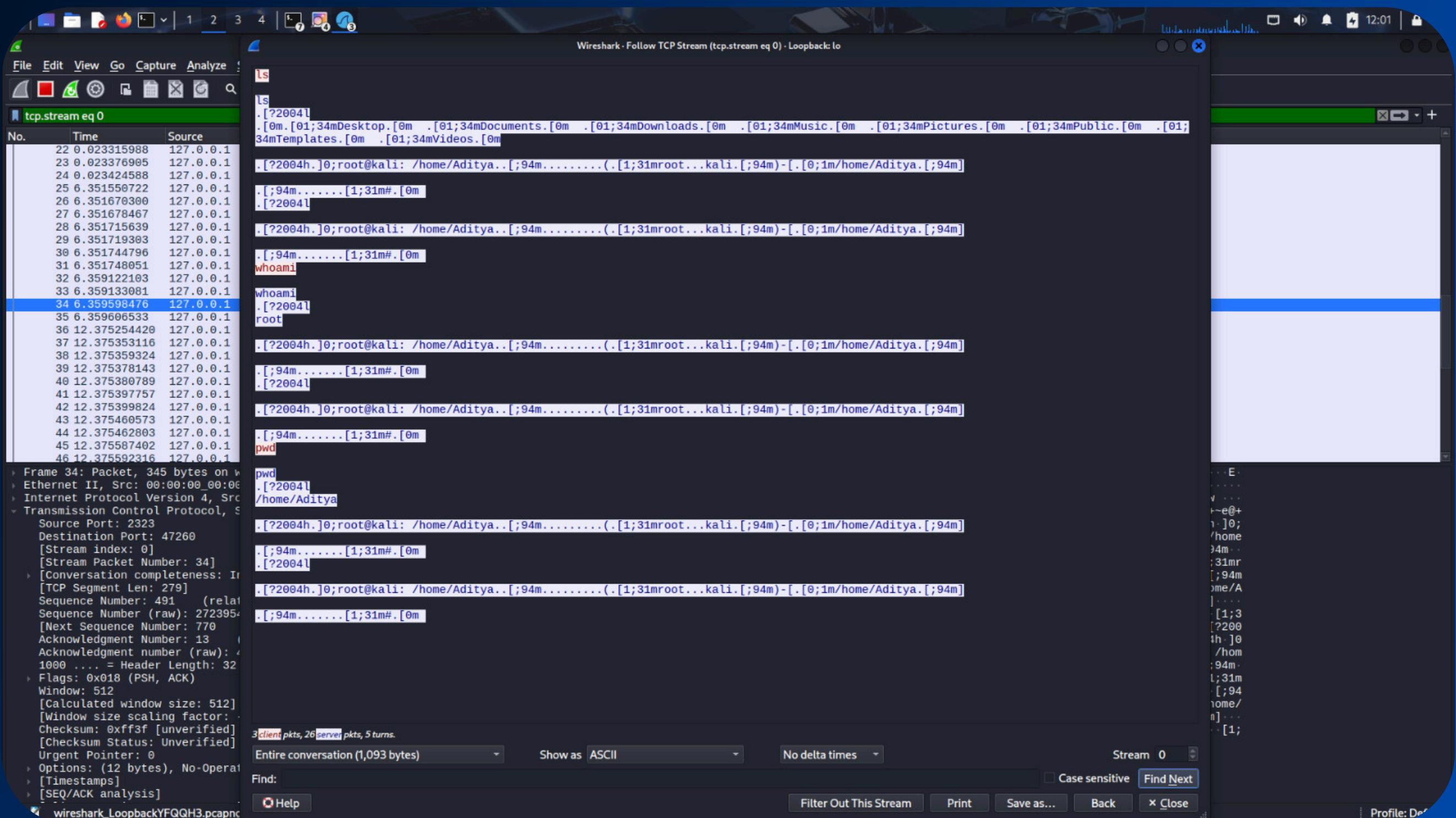
(Aditya㉿kali)-[~]
$ sudo wireshark
** (wireshark:88881) 12:05:11.594069 [Capture MESSAGE] -- Capture Start ...
** (wireshark:88881) 12:05:11.643330 [Capture MESSAGE] -- Capture started
** (wireshark:88881) 12:05:11.643422 [Capture MESSAGE] -- File: "/tmp/wireshark_eth0NPGVH3.pcapng"
** (wireshark:88881) 12:05:16.940200 [Capture MESSAGE] -- Capture Stop ...
** (wireshark:88881) 12:05:17.157267 [Capture MESSAGE] -- Capture stopped.

(Aditya㉿kali)-[~]
$ sudo wireshark
** (wireshark:89264) 12:05:21.746301 [Capture MESSAGE] -- Capture Start ...
** (wireshark:89264) 12:05:21.775631 [Capture MESSAGE] -- Capture started
** (wireshark:89264) 12:05:21.775741 [Capture MESSAGE] -- File: "/tmp/wireshark_LoopbackZUOSH3.pcapng"
** (wireshark:89264) 12:06:40.759017 [packet-ssh WARNING] ./epan/dissectors/packet-ssh.c:1998 -- ssh_dissect_kex_pq_hybrid(): POST-QUANTUM KEX_HYBRID detected: KEX = mlkem768x25519-sha256
** (wireshark:89264) 12:06:40.759075 [packet-ssh WARNING] ./epan/dissectors/packet-ssh.c:1999 -- ssh_dissect_kex_pq_hybrid(): SHARED_SECRET decryption is supported - PRIVATE_KEY decryption is not supported
```

A small tooltip in the top right corner of the terminal window says "Screenshot taken".

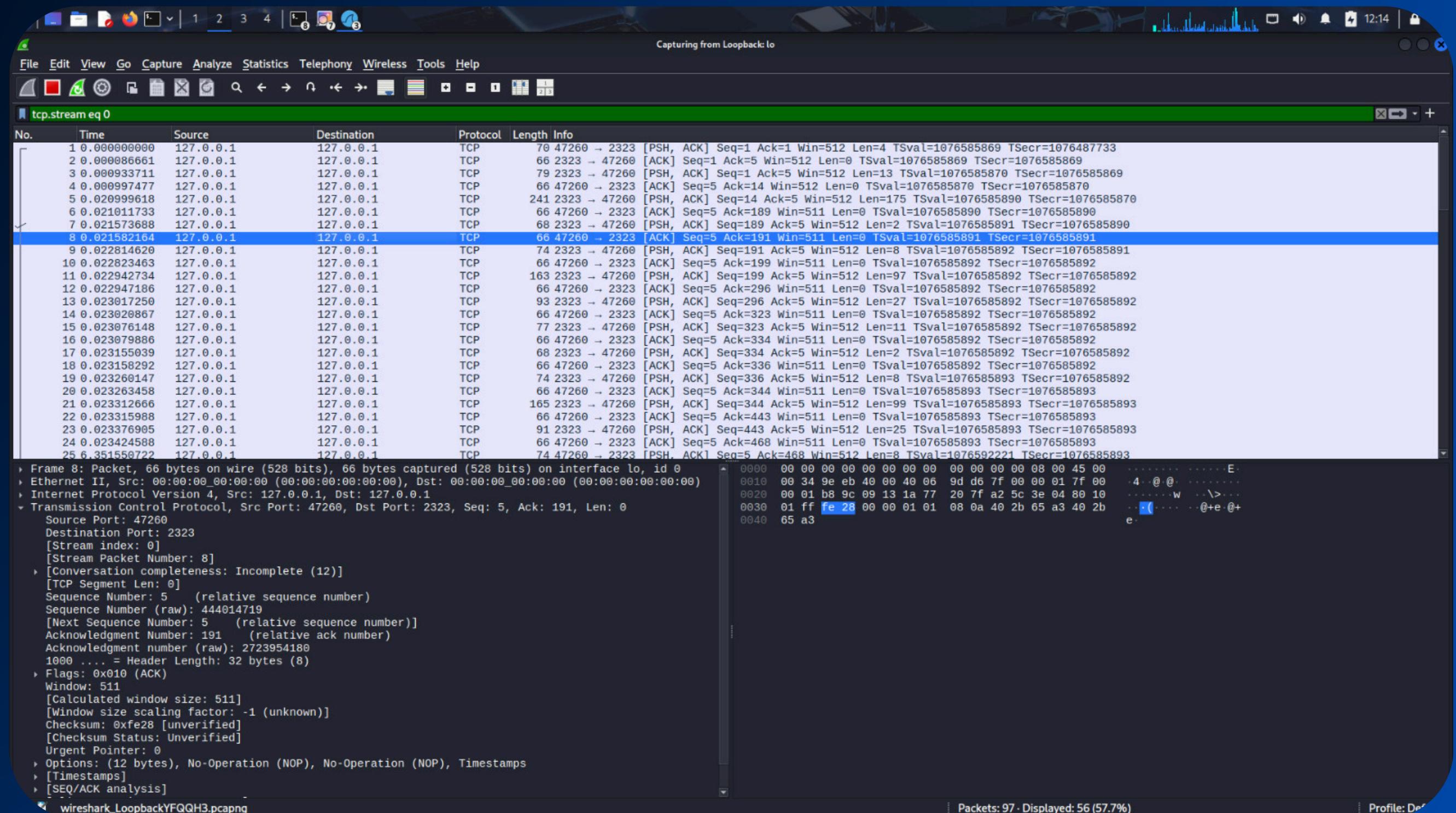
TELNET SERVICE CONFIGURATION

- Telnet service installed using system package manager.
 - Service verified and running successfully.
 - System ready to accept Telnet connections.



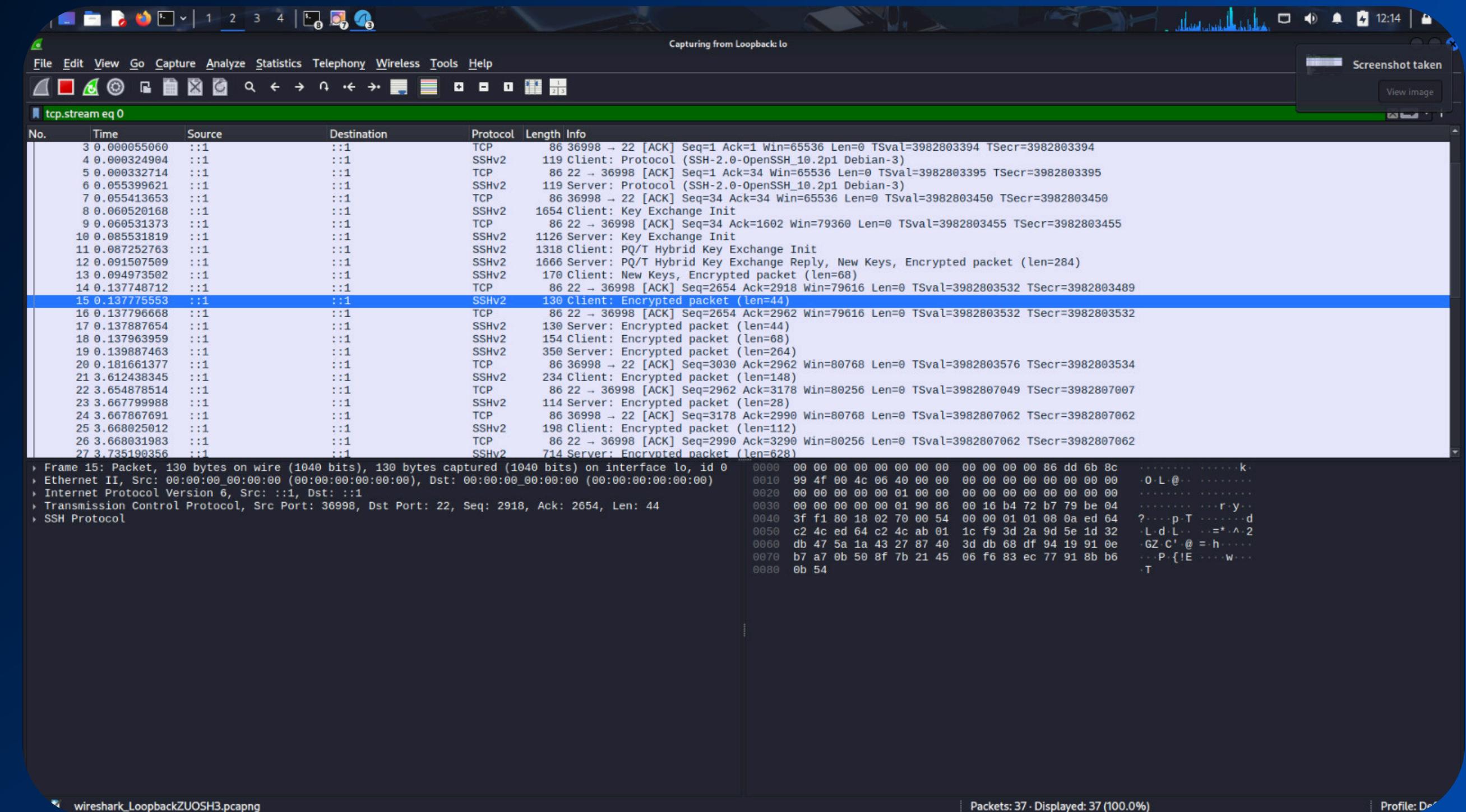
TELNET COMMAND EXECUTION

- Commands executed through Telnet.
 - Output visible in clear text.
 - Confirms lack of encryption in Telnet.



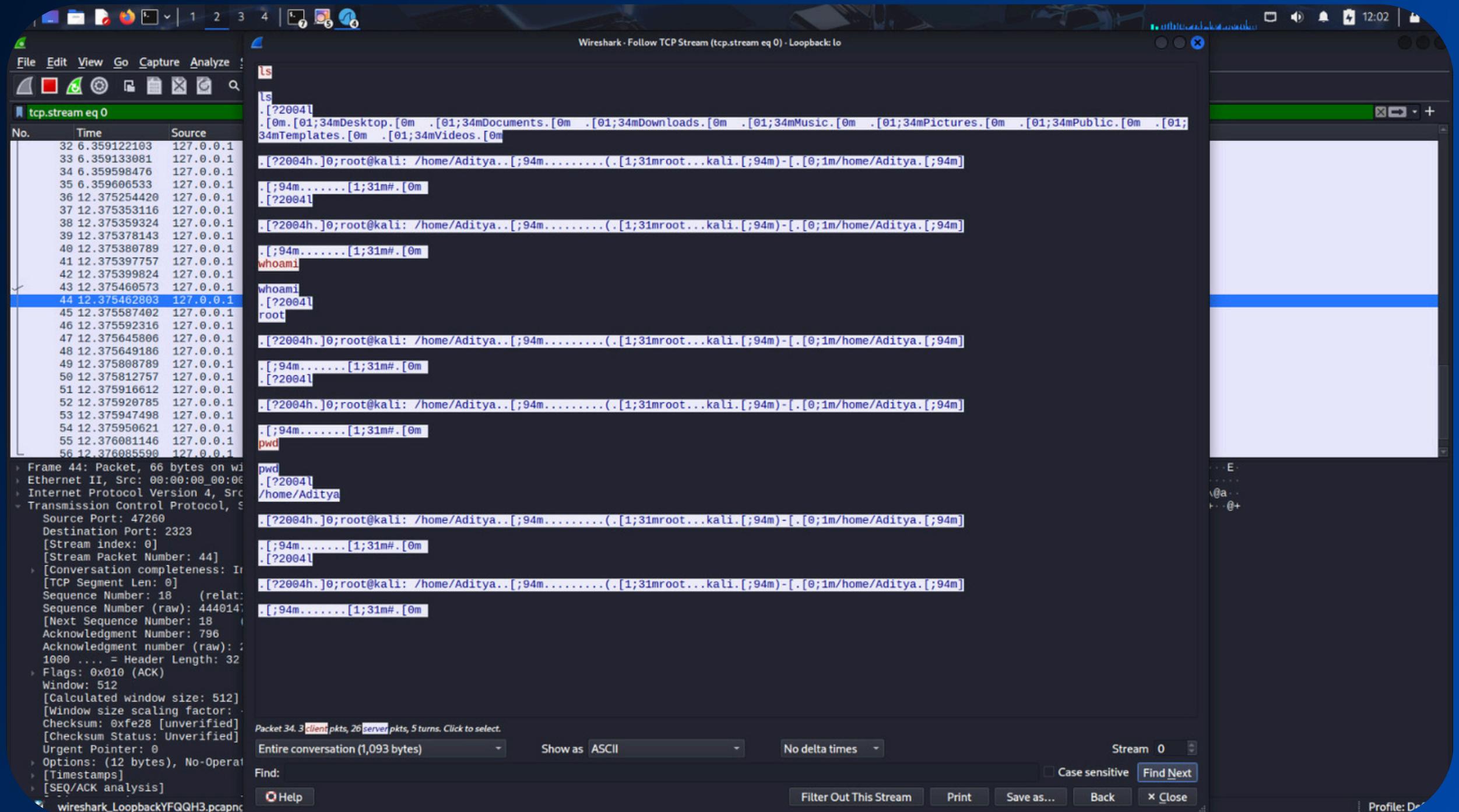
WIRESHARK CAPTURING TELNET TRAFFIC

- Network packets captured on loopback interface.
- Traffic recorded during Telnet session.
- Packet inspection enabled.



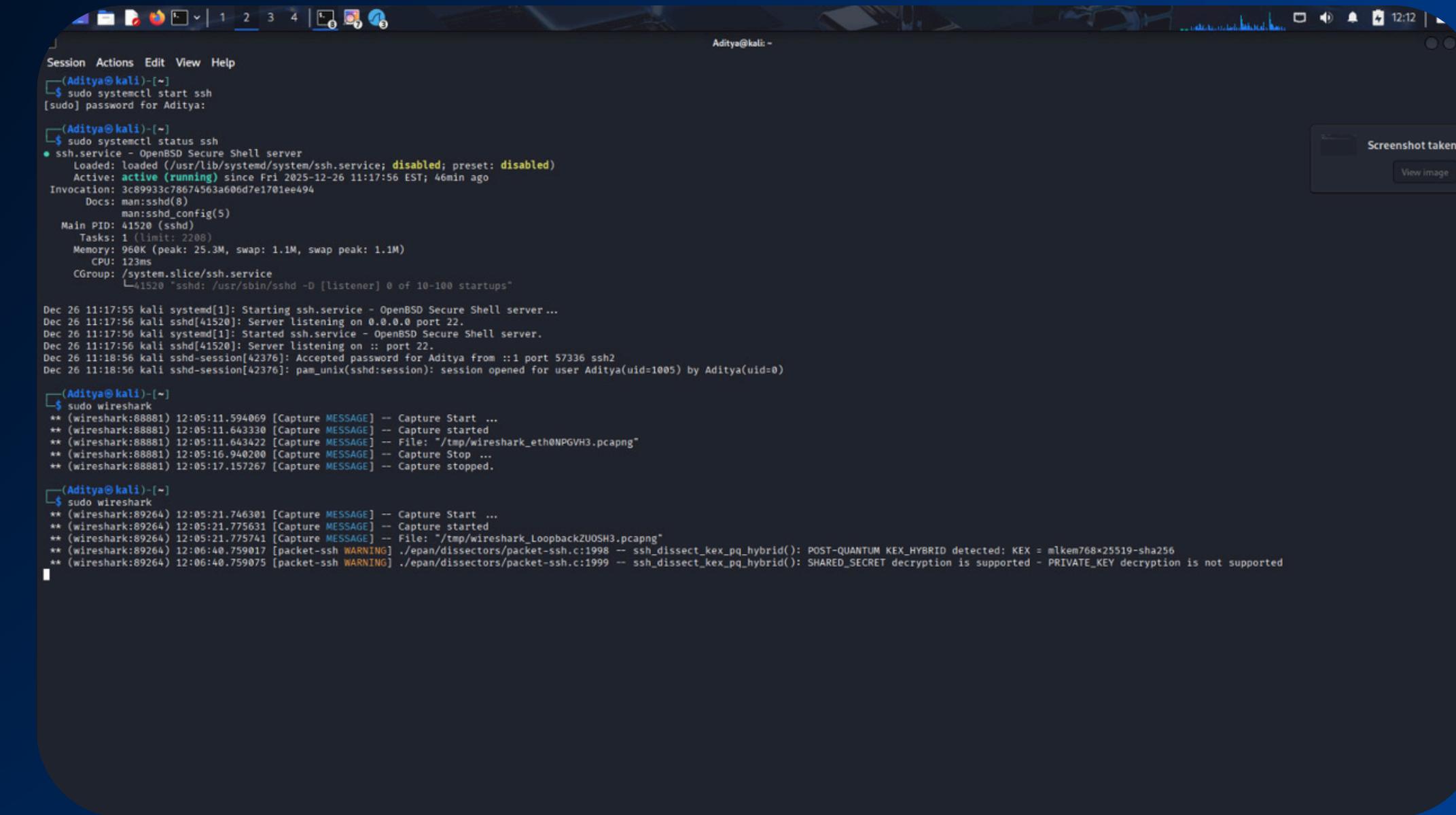
PLAIN-TEXT CREDENTIAL EXPOSURE

- User credentials visible in packet data.
- Commands readable in ASCII format.
- Demonstrates Telnet security weakness.



SSH SERVICE CONFIGURATION

- User credentials visible in packet data.
- Commands readable in ASCII format.
- Demonstrates Telnet security weakness.



The screenshot shows a terminal window on a Kali Linux desktop environment. The terminal output is as follows:

```
Session Actions Edit View Help
(Aditya㉿kali) [~]
$ sudo systemctl start ssh
[sudo] password for Aditya:

(Aditya㉿kali) [~]
$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
  Loaded: loaded (/usr/lib/systemd/system/ssh.service; disabled; preset: disabled)
  Active: active (running) since Fri 2025-12-26 11:17:56 EST; 46min ago
    Invocation: 3c89933c78674563a606d7e1701ee494
      Docs: man:sshd(8)
             man:sshd_config(5)
    Main PID: 41520 (sshd)
      Tasks: 1 (limit: 2208)
     Memory: 960K (peak: 25.3M, swap: 1.1M, swap peak: 1.1M)
       CPU: 123ms
      CGroup: /system.slice/ssh.service
              └─41520 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups

Dec 26 11:17:55 kali systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
Dec 26 11:17:56 kali sshd[41520]: Server listening on 0.0.0.0 port 22.
Dec 26 11:17:56 kali systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
Dec 26 11:17:56 kali sshd[41520]: Server listening on :: port 22.
Dec 26 11:18:56 kali sshd-session[42376]: Accepted password for Aditya from ::1 port 57336 ssh2
Dec 26 11:18:56 kali sshd-session[42376]: pam_unix(sshd:session): session opened for user Aditya(uid=1005) by Aditya(uid=0)

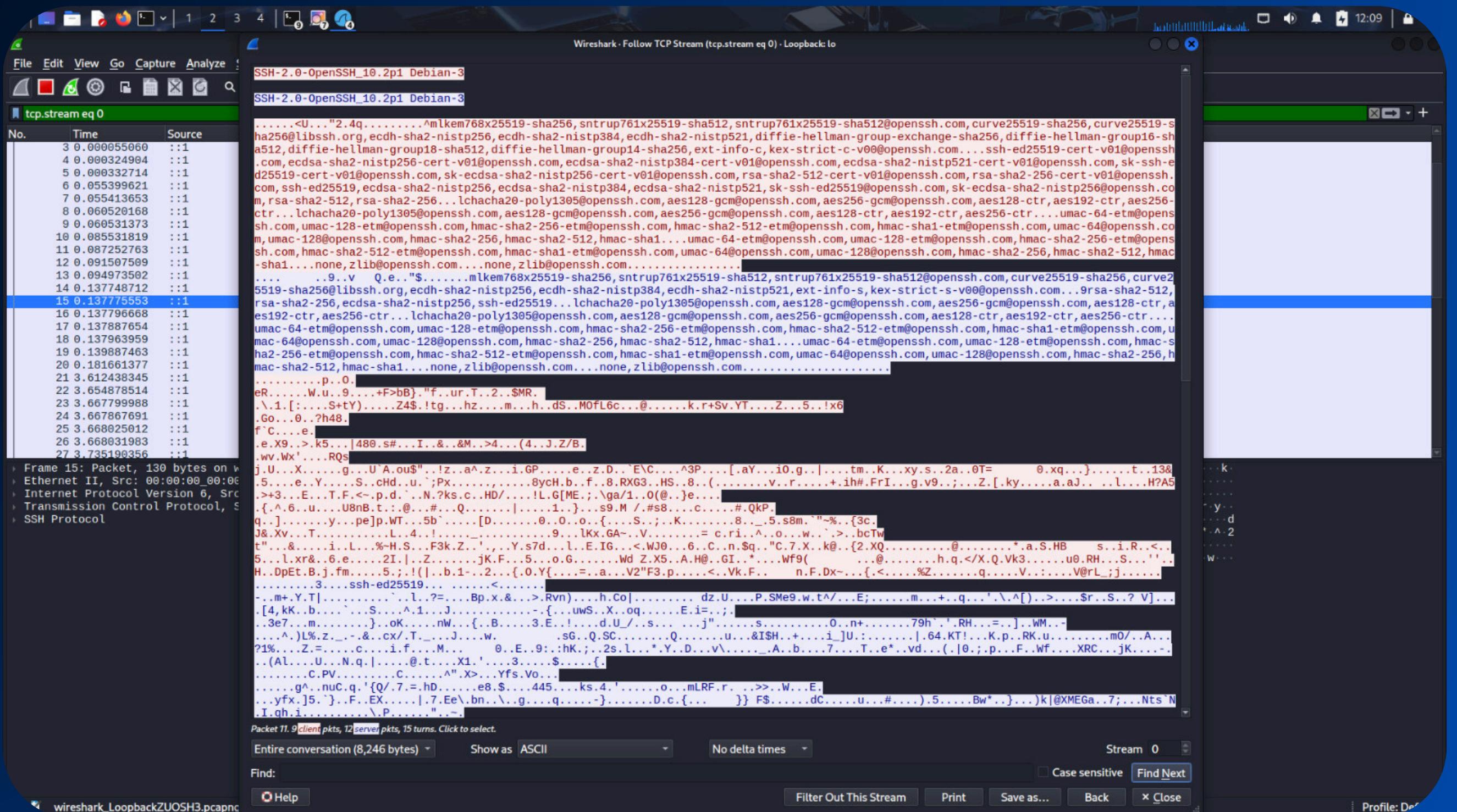
(Aditya㉿kali) [~]
$ sudo wireshark
** (wireshark:8888) 12:05:11.594069 [Capture MESSAGE] -- Capture Start ...
** (wireshark:8888) 12:05:11.643330 [Capture MESSAGE] -- Capture started
** (wireshark:8888) 12:05:11.643422 [Capture MESSAGE] -- File: "/tmp/wireshark_eth0NPGVH3.pcapng"
** (wireshark:8888) 12:05:16.940200 [Capture MESSAGE] -- Capture Stop ...
** (wireshark:8888) 12:05:17.157267 [Capture MESSAGE] -- Capture stopped.

(Aditya㉿kali) [~]
$ sudo wireshark
** (wireshark:89264) 12:05:21.746301 [Capture MESSAGE] -- Capture Start ...
** (wireshark:89264) 12:05:21.755631 [Capture MESSAGE] -- Capture started
** (wireshark:89264) 12:05:21.775741 [Capture MESSAGE] -- File: "/tmp/wireshark_LoopbackZUOSH3.pcapng"
** (wireshark:89264) 12:06:40.759017 [packet-ssh WARNING] ./epan/dissectors/packet-ssh.c:1998 -- ssh_dissect_kex_pqHybrid(): POST-QUANTUM KEX_HYBRID detected: KEX = m1kem768x25519-sha256
** (wireshark:89264) 12:06:40.759075 [packet-ssh WARNING] ./epan/dissectors/packet-ssh.c:1999 -- ssh_dissect_kex_pqHybrid(): SHARED_SECRET decryption is supported - PRIVATE_KEY decryption is not supported
```

A tooltip in the top right corner of the terminal window says "Screenshot taken" and "View image".

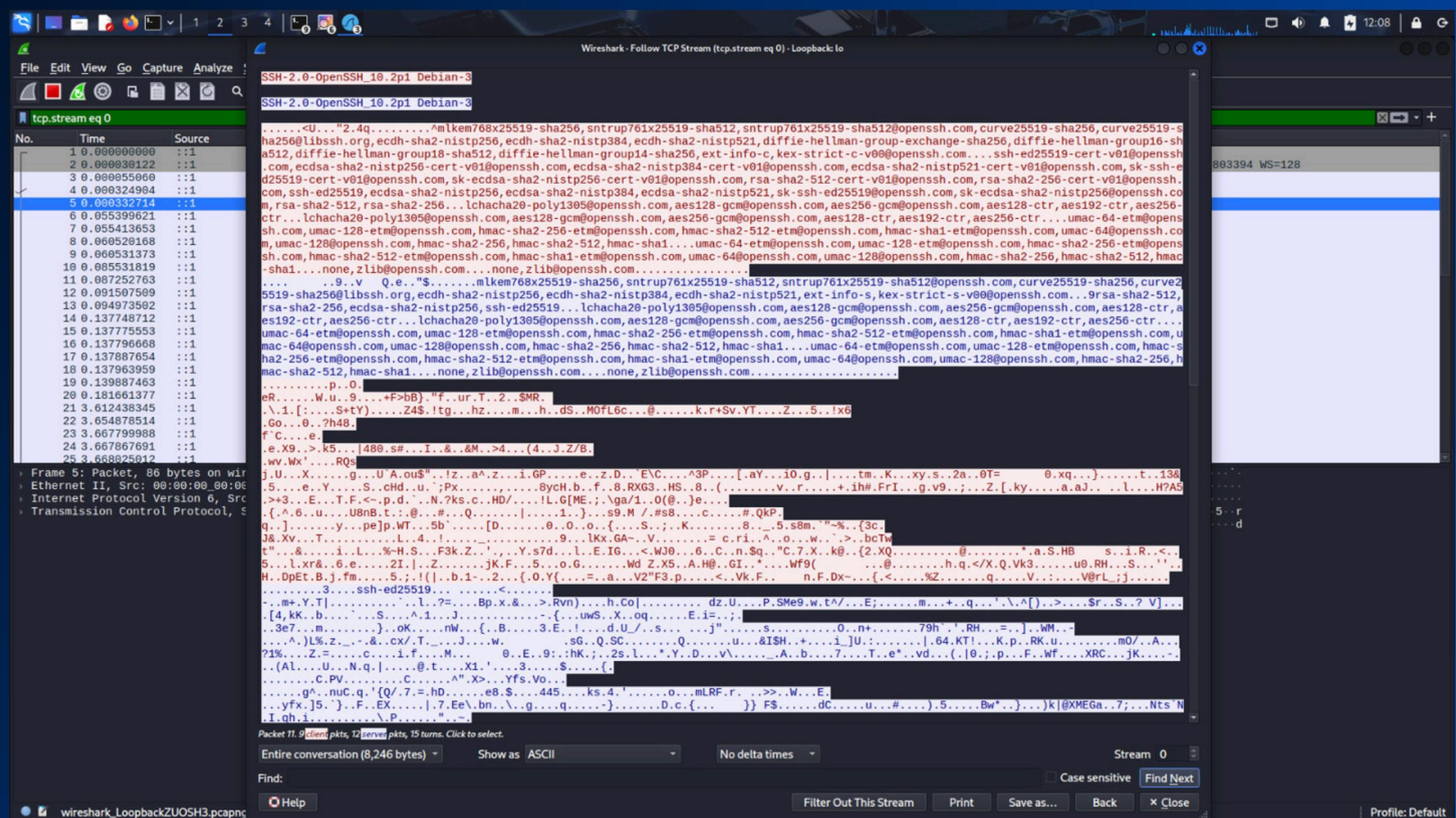
SSH CONNECTION ESTABLISHMENT

- User authenticated using SSH.
- Encrypted connection established.
- Secure remote access achieved.



ENCRYPTED SSH TRAFFIC IN WIRESHARK

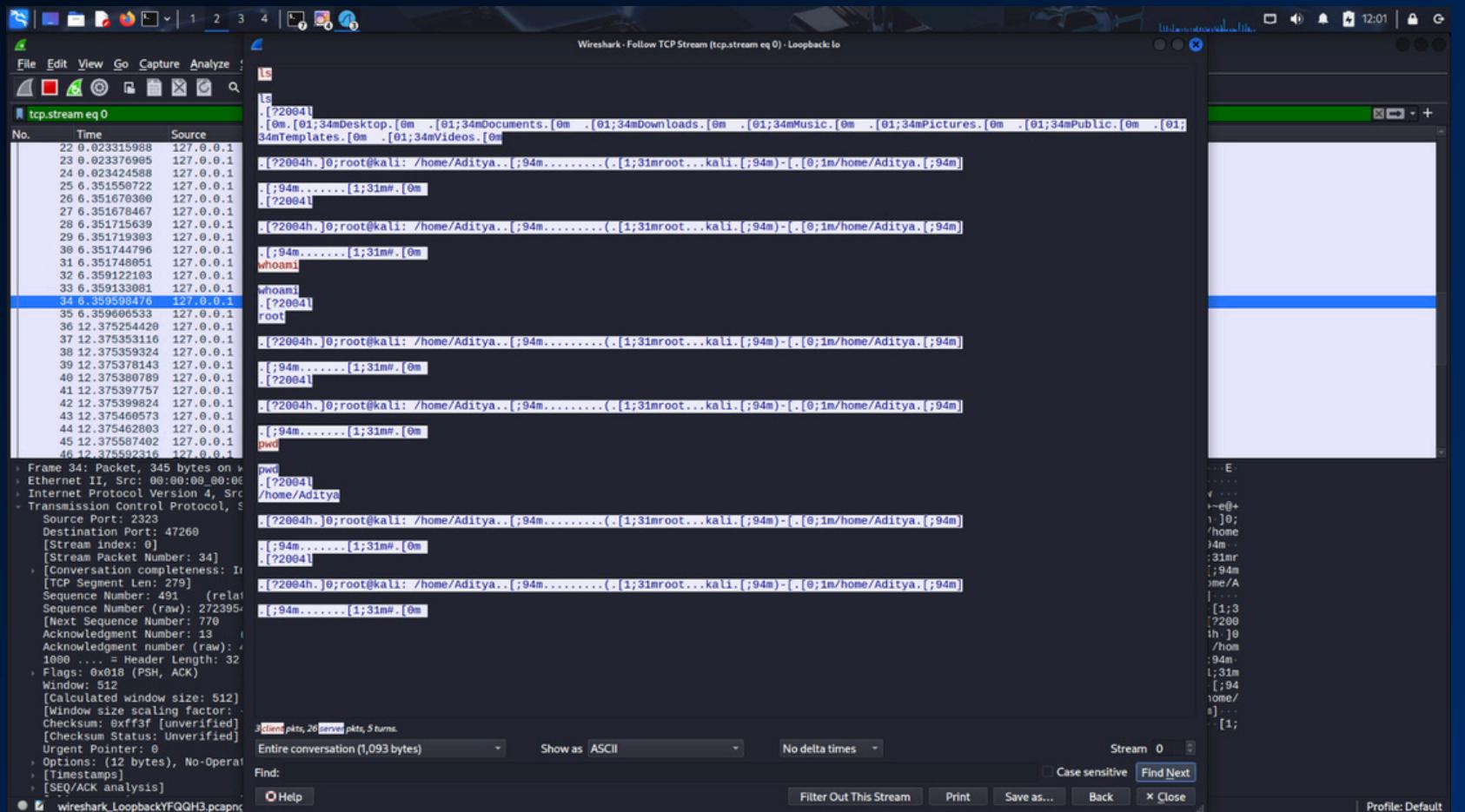
- Packet payload appears unreadable.
- Strong encryption applied.
- Confirms SSH security mechanism.



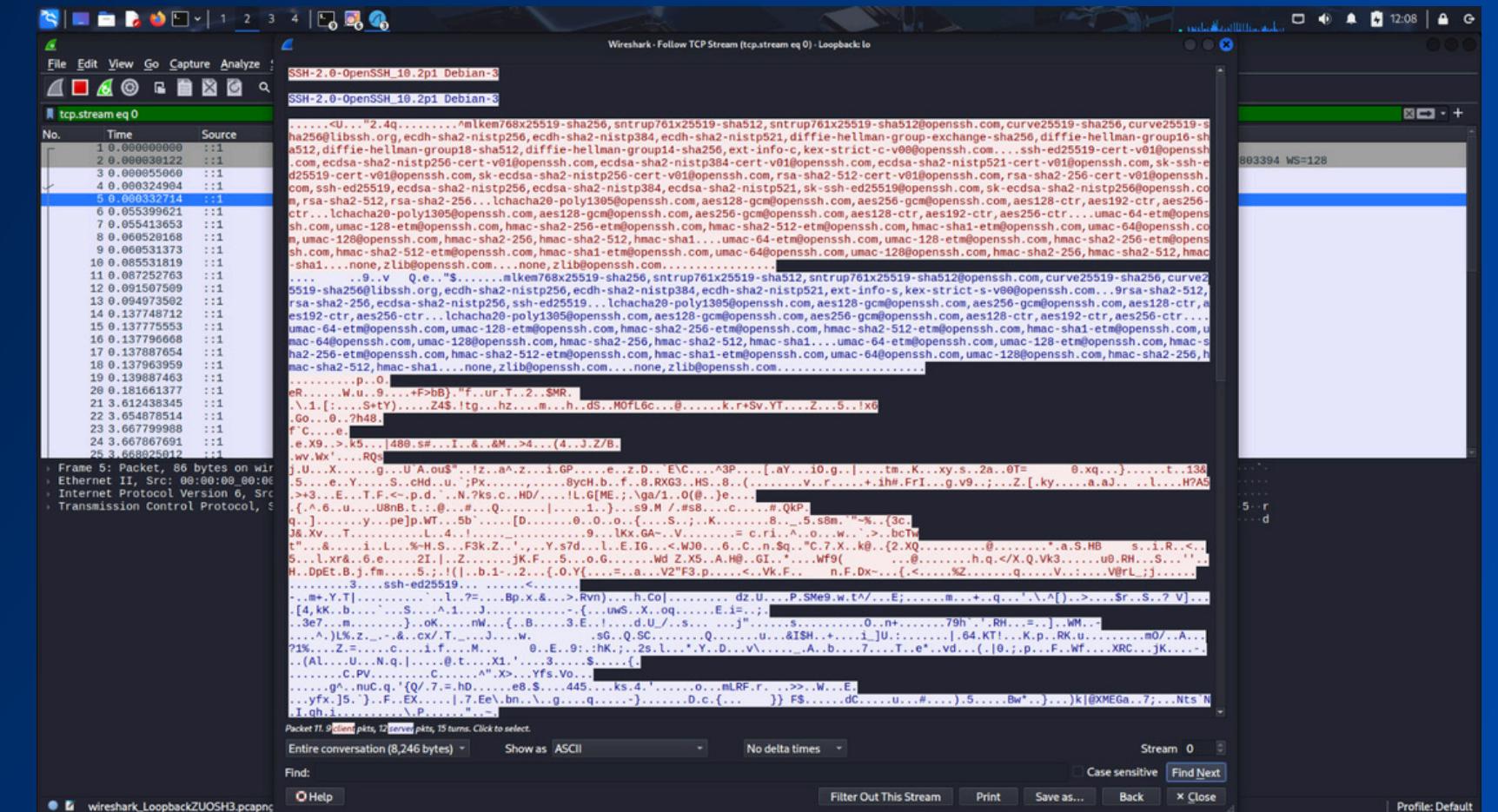
TELNET VS SSH

- Telnet transmits data in plain text.
- SSH encrypts all communication.
- SSH is recommended for secure access.

TELNET



SSH





THANK YOU

Secure Your Digital Life Today