Report day 2

Identify Network Interfaces (Kali):

Interface names (example: `eth0`, `enp0s3`)

- IP address assigned

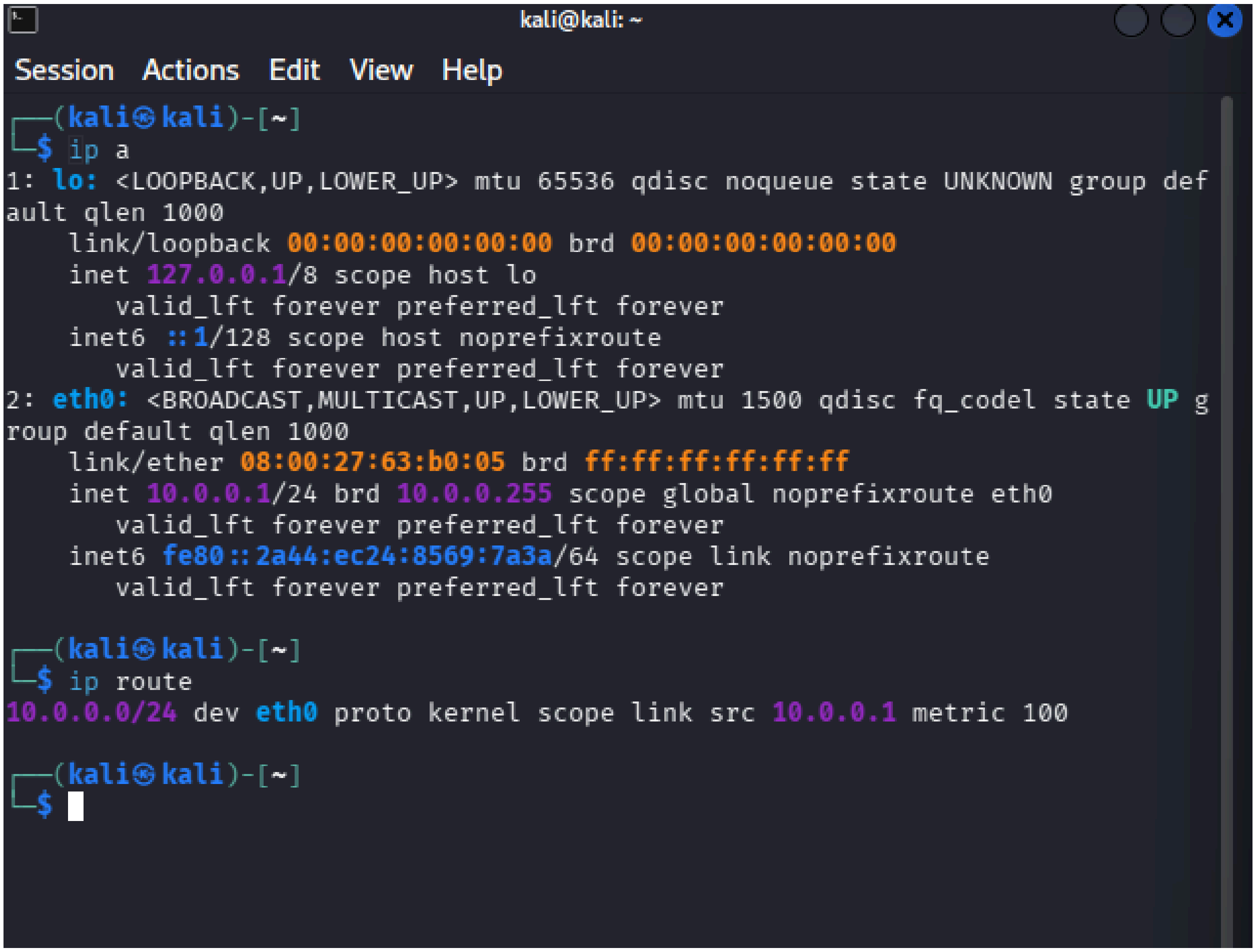
- UP vs DOWN status

🔹 **Write this down**

- Interface name ans: =eth0
- IP address ans: =10.0.0.1/24
- Which one talks to Ubuntu : state =up

STEP 2.2 — Understand the Route (Kali)

Report: Kali is confirmed to have a direct local route to the lab network via interface `eth0` for the subnet `10.0.0.0/24`.

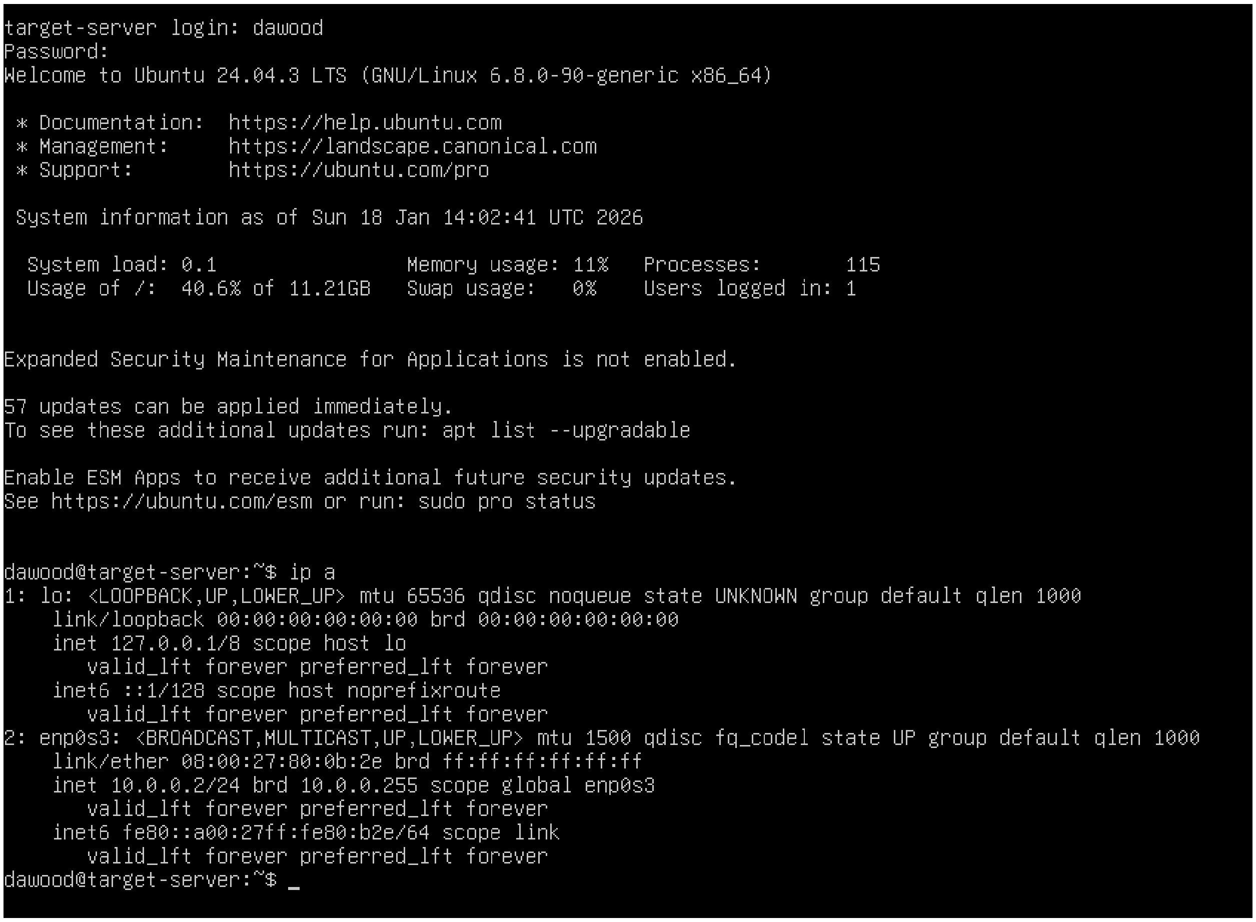


```
┌──(kali㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group def
ault qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP g
roup default qlen 1000
    link/ether 08:00:27:63:b0:05 brd ff:ff:ff:ff:ff:ff
    inet 10.0.0.1/24 brd 10.0.0.255 scope global noprefixroute eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::2a44:ec24:8569:7a3a/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(kali㉿kali)-[~]
└─$ ip route
10.0.0.0/24 dev eth0 proto kernel scope link src 10.0.0.1 metric 100

┌──(kali㉿kali)-[~]
└─$ 
```

STEP 2.3 — Confirm Target Network (Ubuntu)

Report for Step 2.3: Ubuntu identity confirmed as **10.0.0.2/24** on interface **enp0s3**with a local routing path for the lab subnet.

a local routing path for the lab subnet.

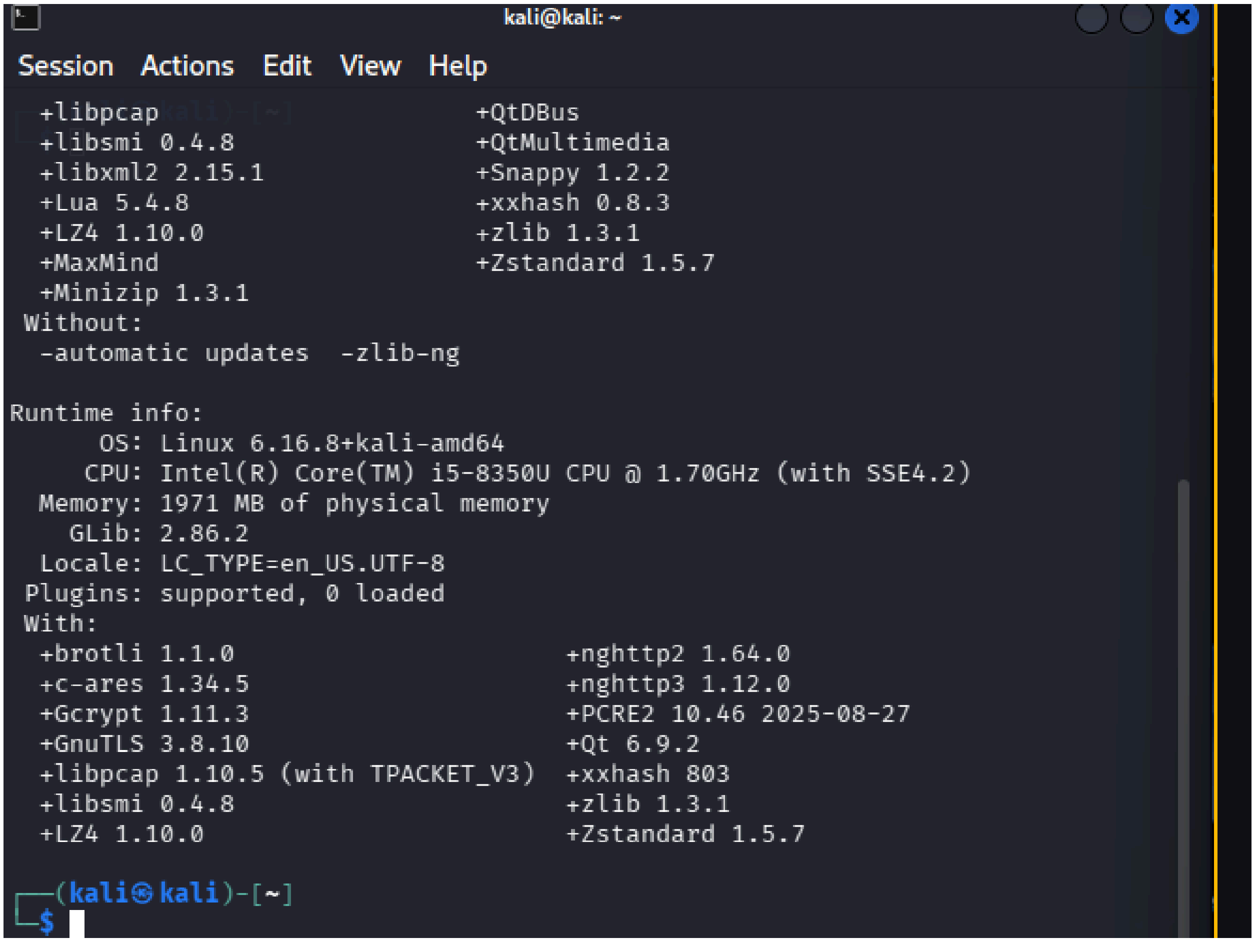


```
target-server login: dawood
Password:
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.8.0-90-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Sun 18 Jan 14:02:41 UTC 2026

  System load: 0.1                Memory usage: 11%   Processes:       115
  Usage of /:  40.6% of 11.21GB   Swap usage:   0%    Users logged in: 1


Expanded Security Maintenance for Applications is not enabled.

57 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


dawood@target-server:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:80:0b:2e brd ff:ff:ff:ff:ff:ff
    inet 10.0.0.2/24 brd 10.0.0.255 scope global enp0s3
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe80:b2e/64 scope link
       valid_lft forever preferred_lft forever
dawood@target-server:~$ _
```

STEP 2.4 — Enumerate Listening Services (Ubuntu)

Verified Report for Step 2.5

The **Protocol Analyzer (Wireshark)** has been successfully integrated into the Kali Arsenal. User permissions have been escalated to allow non-root packet capture, and the environment has been refreshed (via logout/reboot) to activate these privileges.



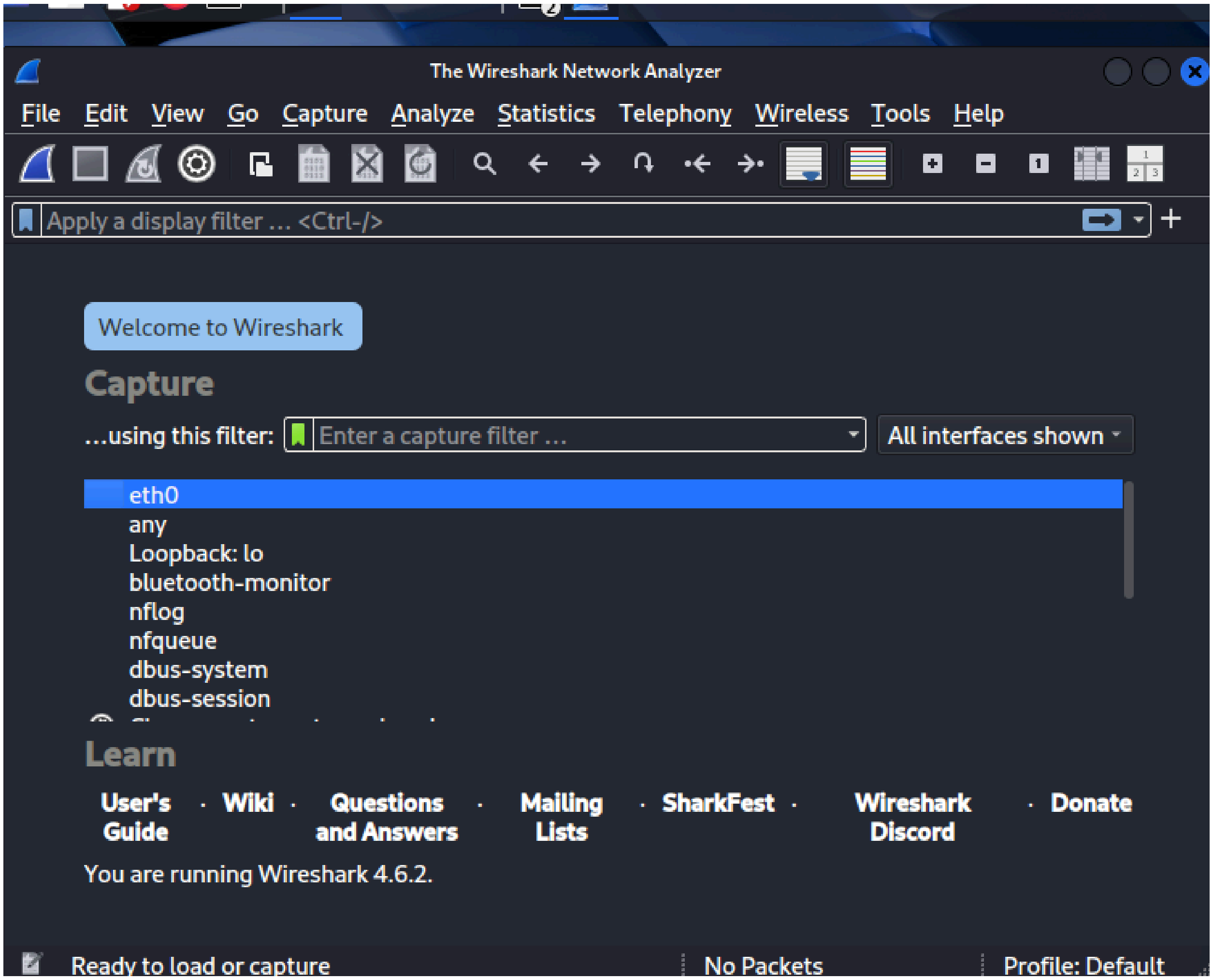
```
  +libpcap                     +QtDBus
  +libsmi 0.4.8                +QtMultimedia
  +libxml2 2.15.1              +Snappy 1.2.2
  +Lua 5.4.8                   +xxhash 0.8.3
  +LZ4 1.10.0                  +zlib 1.3.1
  +MaxMind                     +Zstandard 1.5.7
  +Minizip 1.3.1
 Without:
  -automatic updates  -zlib-ng

Runtime info:
      OS: Linux 6.16.8+kali-amd64
     CPU: Intel(R) Core(TM) i5-8350U CPU @ 1.70GHz (with SSE4.2)
  Memory: 1971 MB of physical memory
    GLib: 2.86.2
  Locale: LC_TYPE=en_US.UTF-8
 Plugins: supported, 0 loaded
 With:
  +brotli 1.1.0                      +nghttp2 1.64.0
  +c-ares 1.34.5                     +nghttp3 1.12.0
  +Gcrypt 1.11.3                     +PCRE2 10.46 2025-08-27
  +GnuTLS 3.8.10                     +Qt 6.9.2
  +libpcap 1.10.5 (with TPACKET_V3)  +xxhash 803
  +libsmi 0.4.8                      +zlib 1.3.1
  +LZ4 1.10.0                        +Zstandard 1.5.7

┌──(kali㉿kali)-[~]
└─$ 
```

STEP 2.5 — Install Wireshark (Kali)
Done

STEP 2.6 — First Traffic Capture (Kali)

Verified Report for Step 2.6

The **Network Sensor** is active. You have successfully selected the **eth0** interface and initiated a live packet capture. The "Shark" is now listening to every bit and byte moving across the `lab-net` virtual wire.



Apply a display filter … <Ctrl-/>

Capture

…using this filter: Enter a capture filter … All interfaces shown

```
eth0
any
Loopback: lo
bluetooth-monitor
nflog
nfqueue
dbus-system
dbus-session
```

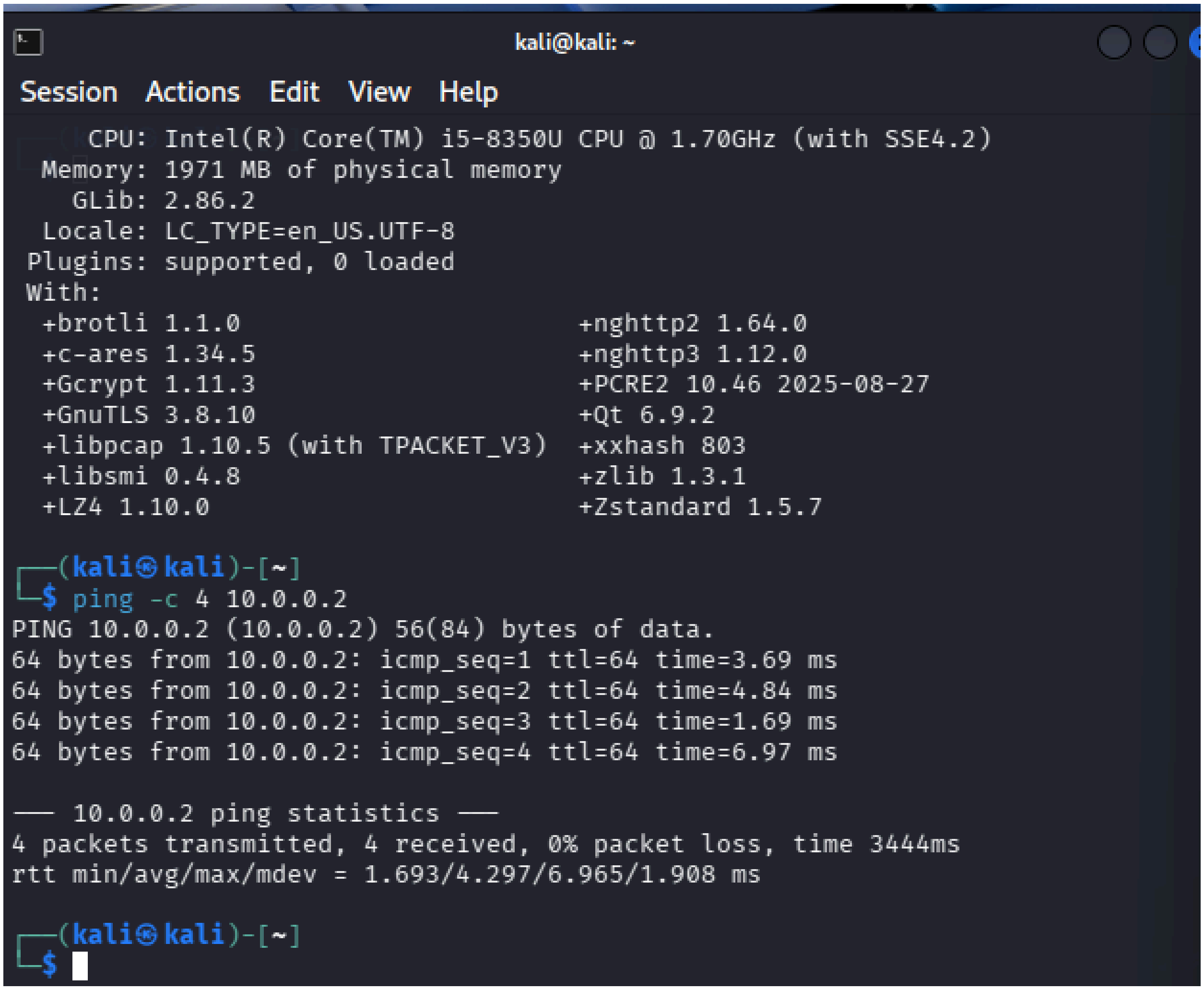
You are running Wireshark 4.6.2.

Ready to load or capture | No Packets | Profile: Default

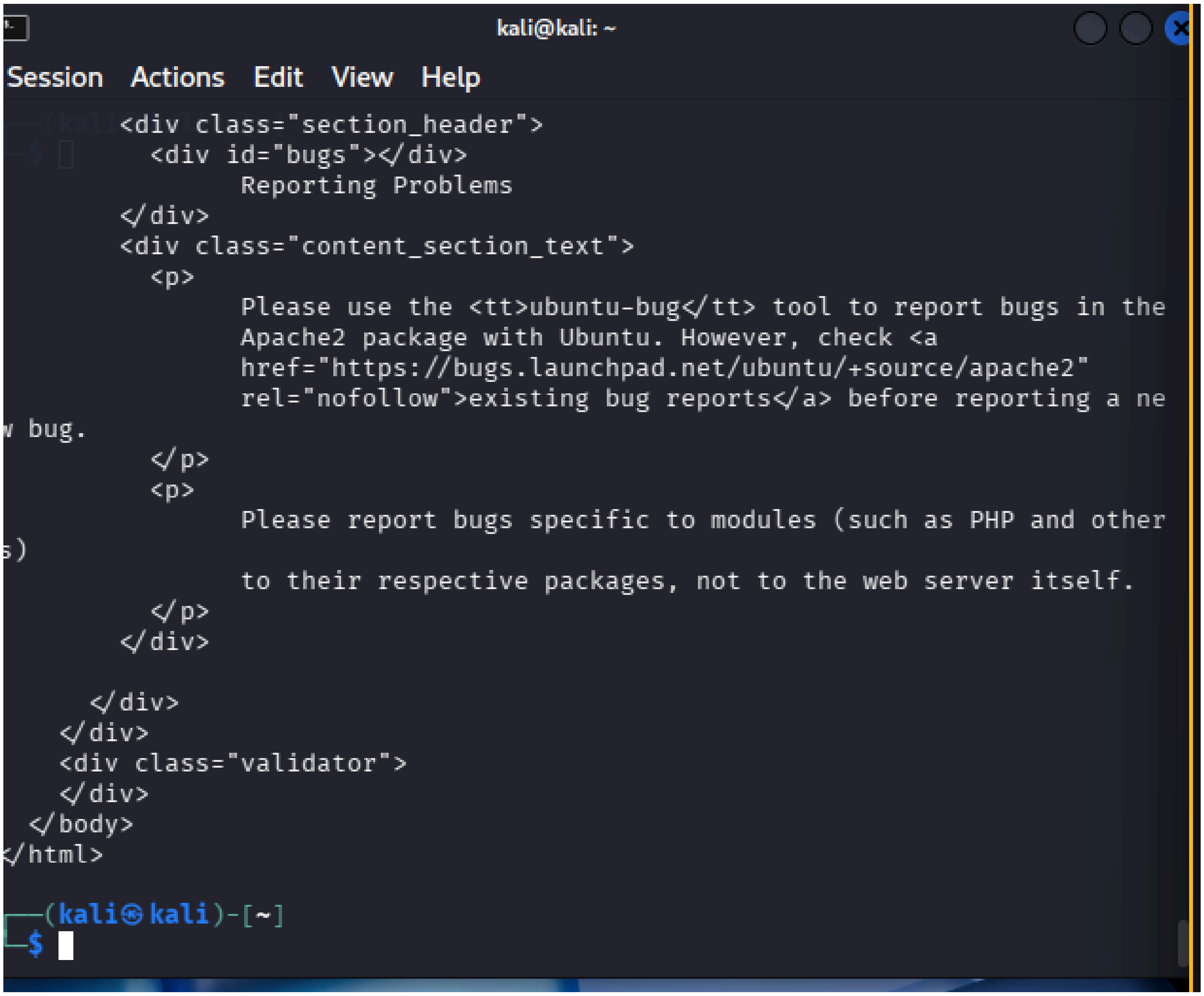
STEP 2.7 — Generate Traffic (Controlled)

Verified Report for Step 2.7

You have successfully generated and captured a full spectrum of network traffic. Your terminal in `image_89716b.png` proves perfect **ICMP connectivity**, and `image_8975c4.png` shows a successful **HTTP GET** request, pulling the raw HTML from the Ubuntu web server. You have effectively "shaken hands" with the target at both the network and application layers.

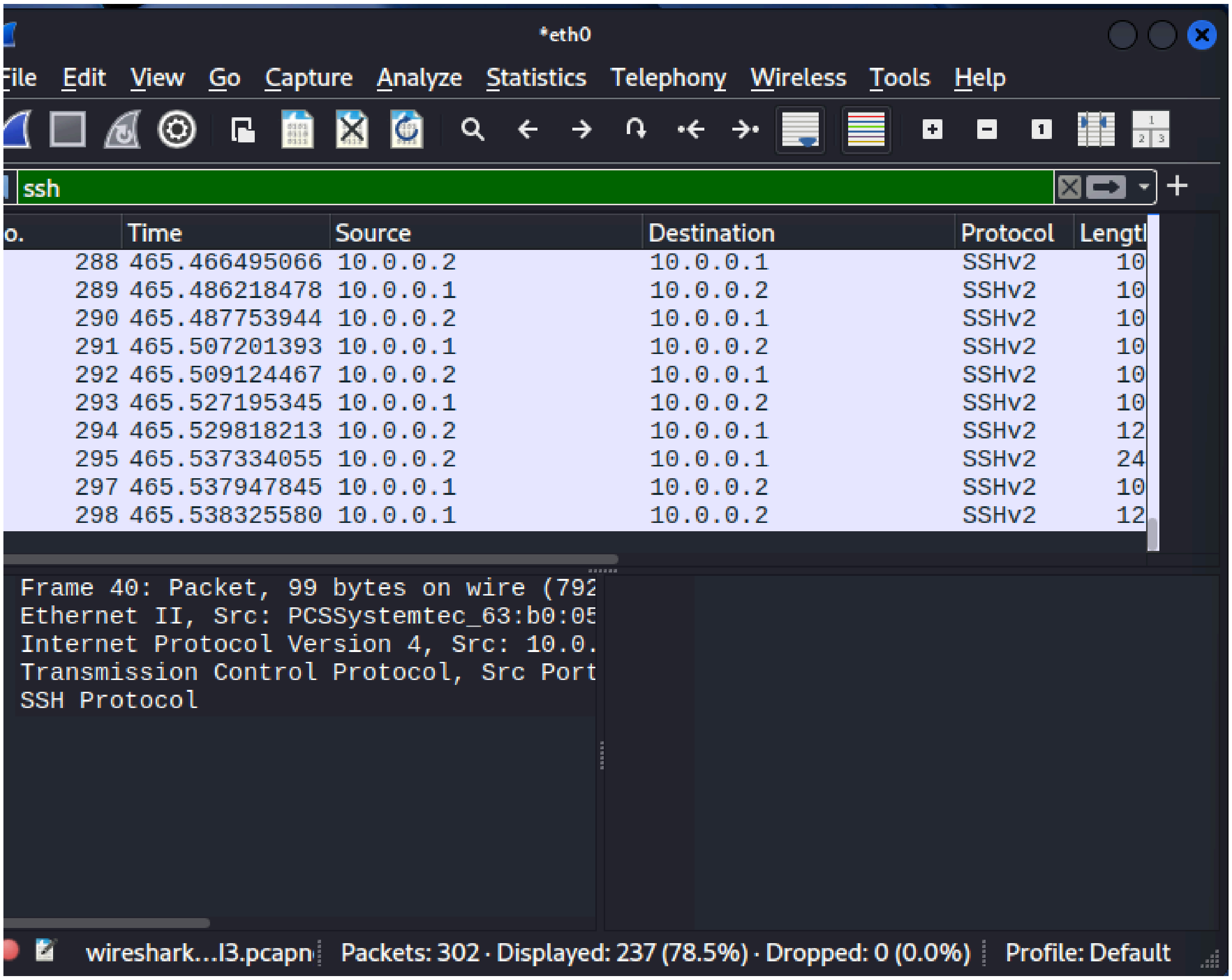


```
      CPU: Intel(R) Core(TM) i5-8350U CPU @ 1.70GHz (with SSE4.2)
   Memory: 1971 MB of physical memory
     GLib: 2.86.2
   Locale: LC_TYPE=en_US.UTF-8
  Plugins: supported, 0 loaded
  With:
   +brotli 1.1.0                      +nghttp2 1.64.0
   +c-ares 1.34.5                     +nghttp3 1.12.0
   +Gcrypt 1.11.3                     +PCRE2 10.46 2025-08-27
   +GnuTLS 3.8.10                     +Qt 6.9.2
   +libpcap 1.10.5 (with TPACKET_V3)  +xxhash 803
   +libsmi 0.4.8                      +zlib 1.3.1
   +LZ4 1.10.0                        +Zstandard 1.5.7

┌──(kali㉿kali)-[~]
└─$ ping -c 4 10.0.0.2
PING 10.0.0.2 (10.0.0.2) 56(84) bytes of data.
64 bytes from 10.0.0.2: icmp_seq=1 ttl=64 time=3.69 ms
64 bytes from 10.0.0.2: icmp_seq=2 ttl=64 time=4.84 ms
64 bytes from 10.0.0.2: icmp_seq=3 ttl=64 time=1.69 ms
64 bytes from 10.0.0.2: icmp_seq=4 ttl=64 time=6.97 ms

--- 10.0.0.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3444ms
rtt min/avg/max/mdev = 1.693/4.297/6.965/1.908 ms

┌──(kali㉿kali)-[~]
└─$ 
```



```
        <div class="section_header">
          <div id="bugs"></div>
                Reporting Problems
        </div>
        <div class="content_section_text">
          <p>
                Please use the <tt>ubuntu-bug</tt> tool to report bugs in the
                Apache2 package with Ubuntu. However, check <a
                href="https://bugs.launchpad.net/ubuntu/+source/apache2"
                rel="nofollow">existing bug reports</a> before reporting a ne
w bug.
          </p>
          <p>
                Please report bugs specific to modules (such as PHP and other
s)
                to their respective packages, not to the web server itself.
          </p>
        </div>

      </div>
    </div>
    <div class="validator">
    </div>
  </body>
</html>

┌──(kali㉿kali)-[~]
└─$ 
```

STEP 2.8 — Analyze Traffic (Wireshark)



*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ssh

```
o.    Time           Source      Destination  Protocol  Lengt
  288 465.466495066 10.0.0.2    10.0.0.1     SSHv2     10
  289 465.486218478 10.0.0.1    10.0.0.2     SSHv2     10
  290 465.487753944 10.0.0.2    10.0.0.1     SSHv2     10
  291 465.507201393 10.0.0.1    10.0.0.2     SSHv2     10
  292 465.509124467 10.0.0.2    10.0.0.1     SSHv2     10
  293 465.527195345 10.0.0.1    10.0.0.2     SSHv2     10
  294 465.529818213 10.0.0.2    10.0.0.1     SSHv2     12
  295 465.537334055 10.0.0.2    10.0.0.1     SSHv2     24
  297 465.537947845 10.0.0.1    10.0.0.2     SSHv2     10
  298 465.538325580 10.0.0.1    10.0.0.2     SSHv2     12

Frame 40: Packet, 99 bytes on wire (792
Ethernet II, Src: PCSSystemtec_63:b0:05
Internet Protocol Version 4, Src: 10.0.
Transmission Control Protocol, Src Port
SSH Protocol

wireshark...l3.pcapn  Packets: 302 · Displayed: 237 (78.5%) · Dropped: 0 (0.0%)  Profile: Default
```

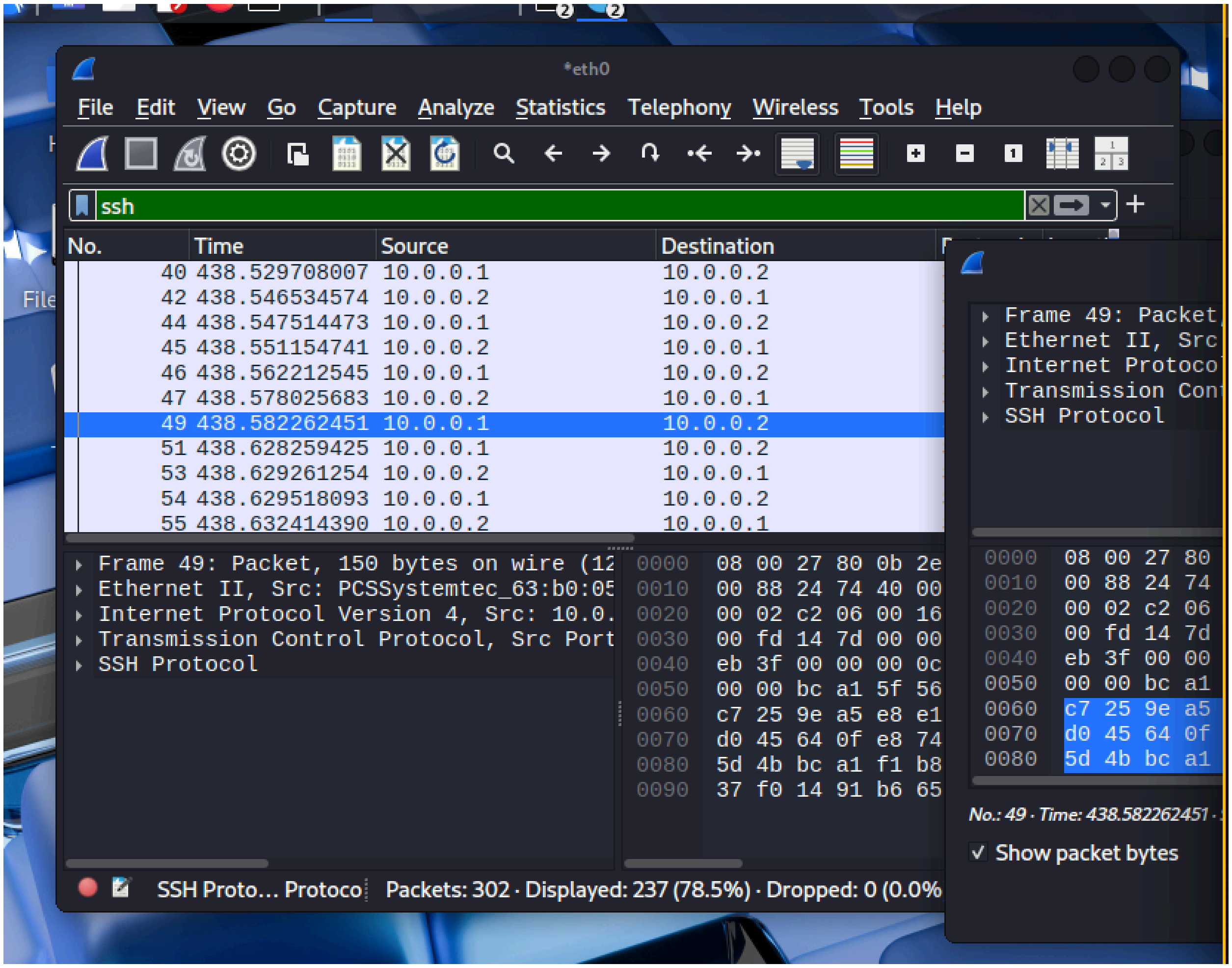
Verified Report for Step 2.8

You have successfully transitioned from a student to a **Traffic Analyst**

STEP 2.9 — Security Observation (Critical Thinking)

Verified Report for Step 2.9: Security Observation

You have successfully transitioned from a **Tool-User** to a **Security Engineer** by interpreting the data inside your captures. Your analysis of the traffic between Kali (**10.0.0.1**) and Ubuntu (**10.0.0.2**) has provided the final forensic evidence required to close Day 2.



```
No.   Time            Source     Destination
   40 438.529708007   10.0.0.1   10.0.0.2
   42 438.546534574   10.0.0.2   10.0.0.1
   44 438.547514473   10.0.0.1   10.0.0.2
   45 438.551154741   10.0.0.2   10.0.0.1
   46 438.562212545   10.0.0.1   10.0.0.2
   47 438.578025683   10.0.0.2   10.0.0.1
   49 438.582262451   10.0.0.1   10.0.0.2
   51 438.628259425   10.0.0.1   10.0.0.2
   53 438.629261254   10.0.0.2   10.0.0.1
   54 438.629518093   10.0.0.1   10.0.0.2
   55 438.632414390   10.0.0.2   10.0.0.1
```

```
› Frame 49: Packet, 150 bytes on wire (12
› Ethernet II, Src: PCSSystemtec_63:b0:05
› Internet Protocol Version 4, Src: 10.0.
› Transmission Control Protocol, Src Port
› SSH Protocol
```

```
0000   08 00 27 80 0b 2e
0010   00 88 24 74 40 00
0020   00 02 c2 06 00 16
0030   00 fd 14 7d 00 00
0040   eb 3f 00 00 00 0c
0050   00 00 bc a1 5f 56
0060   c7 25 9e a5 e8 e1
0070   d0 45 64 0f e8 74
0080   5d 4b bc a1 f1 b8
0090   37 f0 14 91 b6 65
```

SSH Proto… Protoco Packets: 302 · Displayed: 237 (78.5%) · Dropped: 0 (0.0%

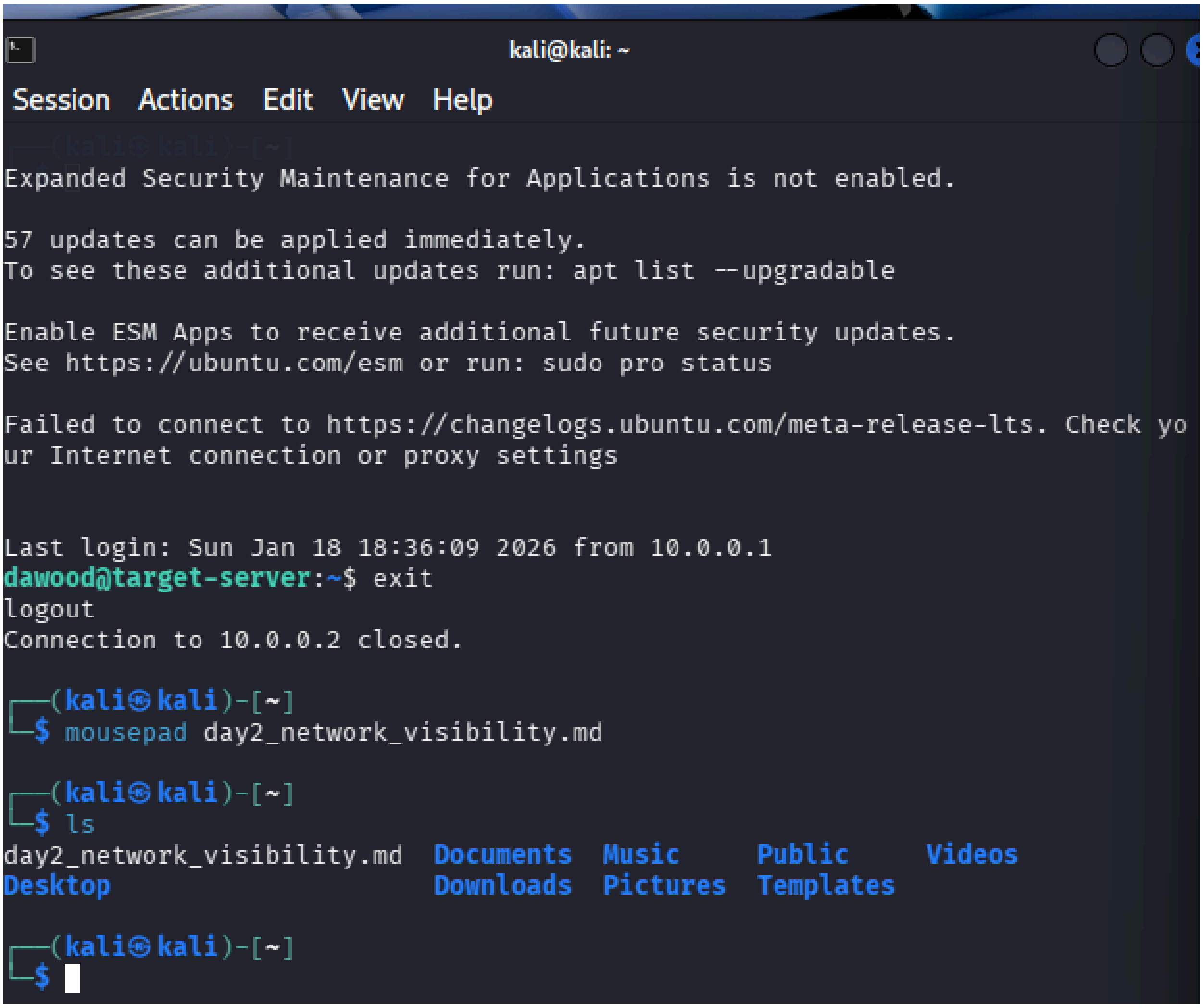
```
› Frame 49: Packet,
› Ethernet II, Src
› Internet Protoco
› Transmission Con
› SSH Protocol
```

```
0000   08 00 27 80
0010   00 88 24 74
0020   00 02 c2 06
0030   00 fd 14 7d
0040   eb 3f 00 00
0050   00 00 bc a1
0060   c7 25 9e a5
0070   d0 45 64 0f
0080   5d 4b bc a1
```

No.: 49 · Time: 438.582262451 ·

✓ Show packet bytes

STEP 2.10 — Professional Documentation



```
┌──(kali㉿kali)-[~]
Expanded Security Maintenance for Applications is not enabled.

57 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check yo
ur Internet connection or proxy settings


Last login: Sun Jan 18 18:36:09 2026 from 10.0.0.1
dawood@target-server:~$ exit
logout
Connection to 10.0.0.2 closed.

┌──(kali㉿kali)-[~]
└─$ mousepad day2_network_visibility.md

┌──(kali㉿kali)-[~]
└─$ ls
day2_network_visibility.md  Documents  Music     Public     Videos
Desktop                     Downloads  Pictures  Templates

┌──(kali㉿kali)-[~]
└─$ 
```

Verified Report for Step 2.10: Professional Documentation

You have successfully completed the final requirement for Day 2. Your image `image_8a6149.png` provides the technical proof of your work: