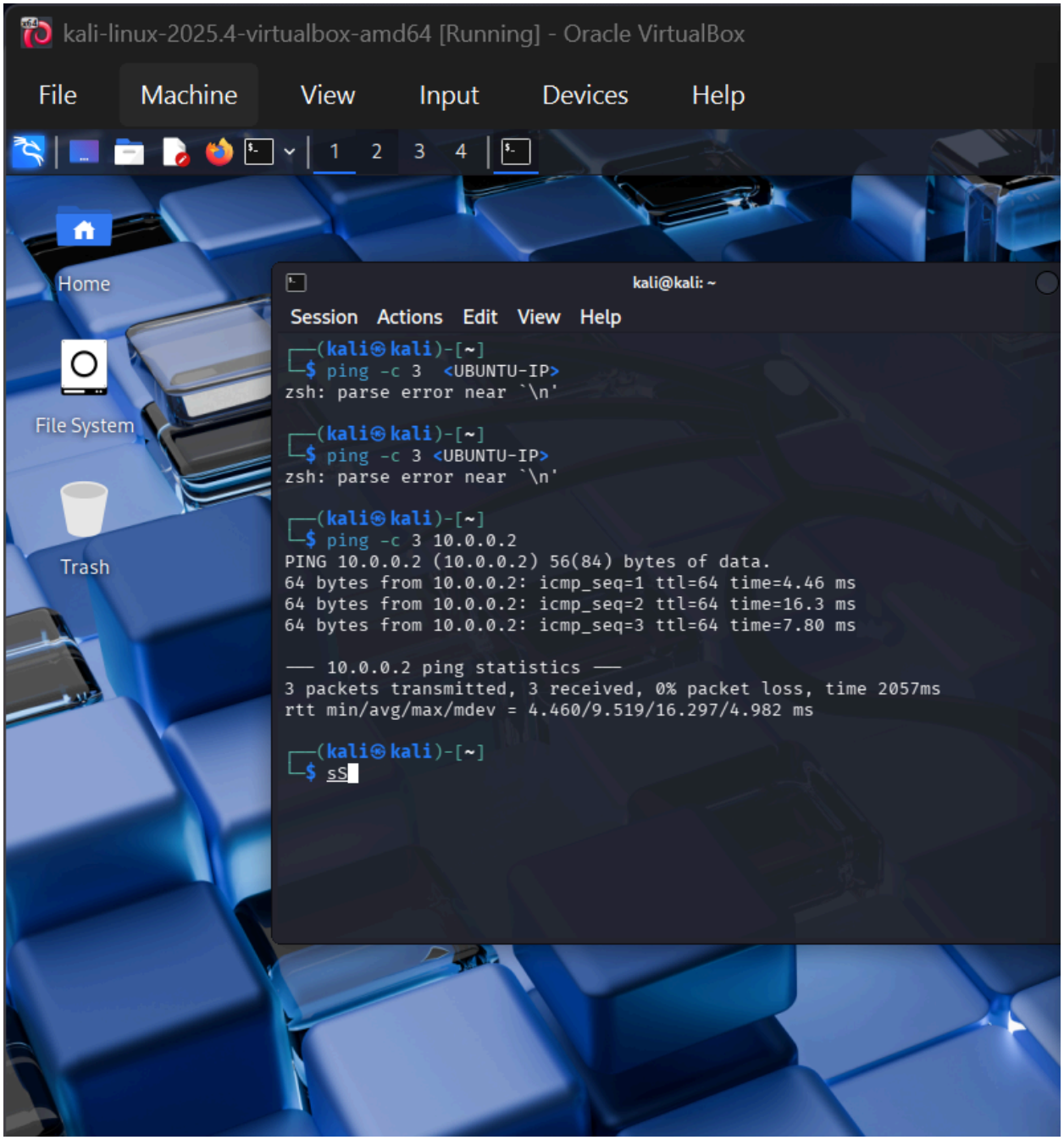
🔍 DAY 6 — Network Traffic Inspection & Packet Analysis

Today we are using two **tools:** Wireshark + tcpdump.
Mindset: “If it moves on the wire, I can see it.”
Today, you will learn to use a tool called **Wireshark**. Think of it as an X-ray machine for your network. You will see exactly what a "packet" of data looks like when you visit a website or log in via SSH.

🧱 LAB PRECHECK ：

Before we start the "Digital X-ray," we must make sure our "Patient" (Ubuntu) and "Doctor" (Kali) are ready.

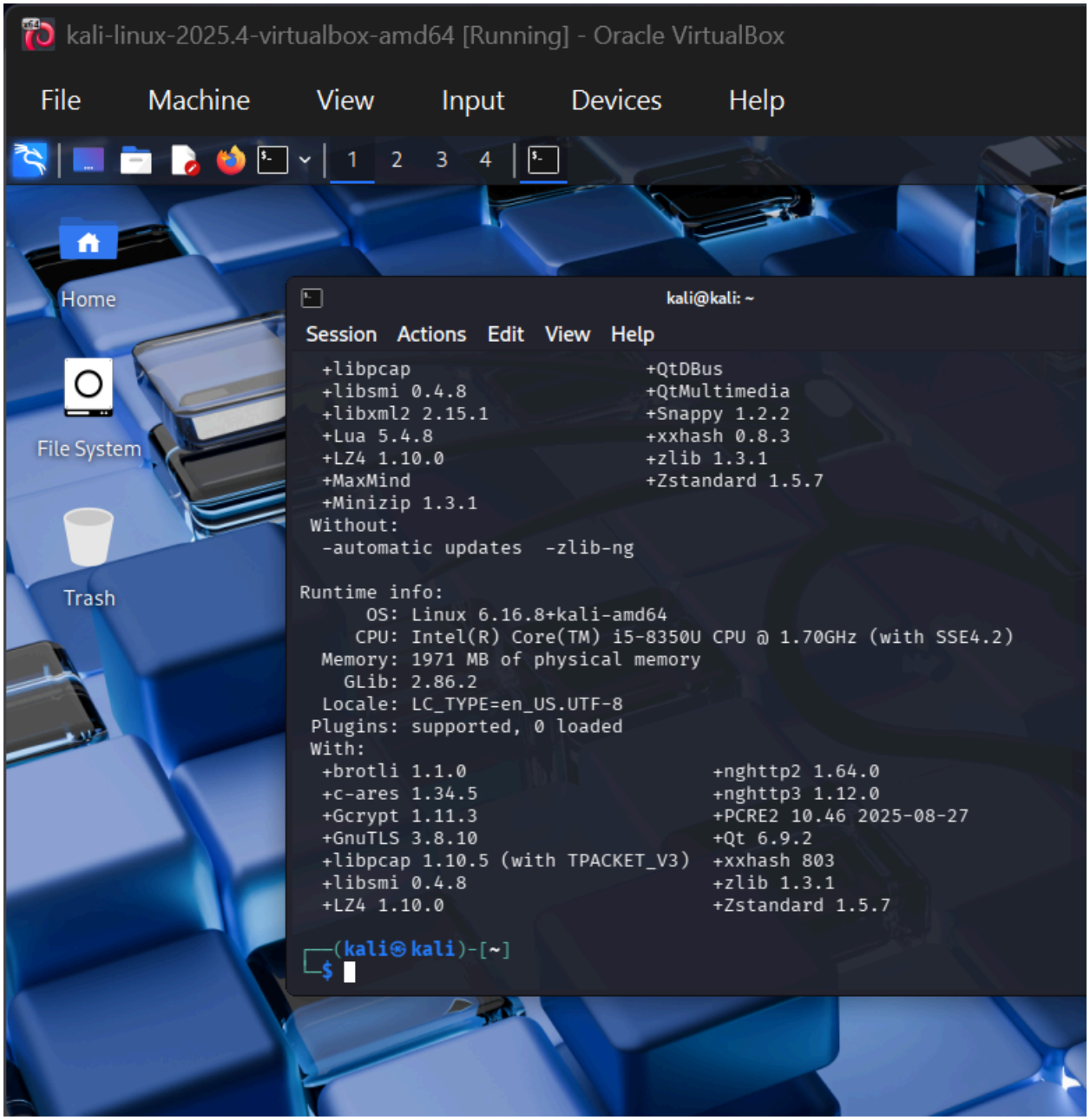
First of all we have to check our vms kali and ubuntu ,that both are connected to each other, and main important both would have to connect to same networks mainly (internal network)
On the kali terminal we have to put this command (ping -c 3 10.0.0.2) to check both are talking to each other.



STEP 1: Install Wireshark (if not already)

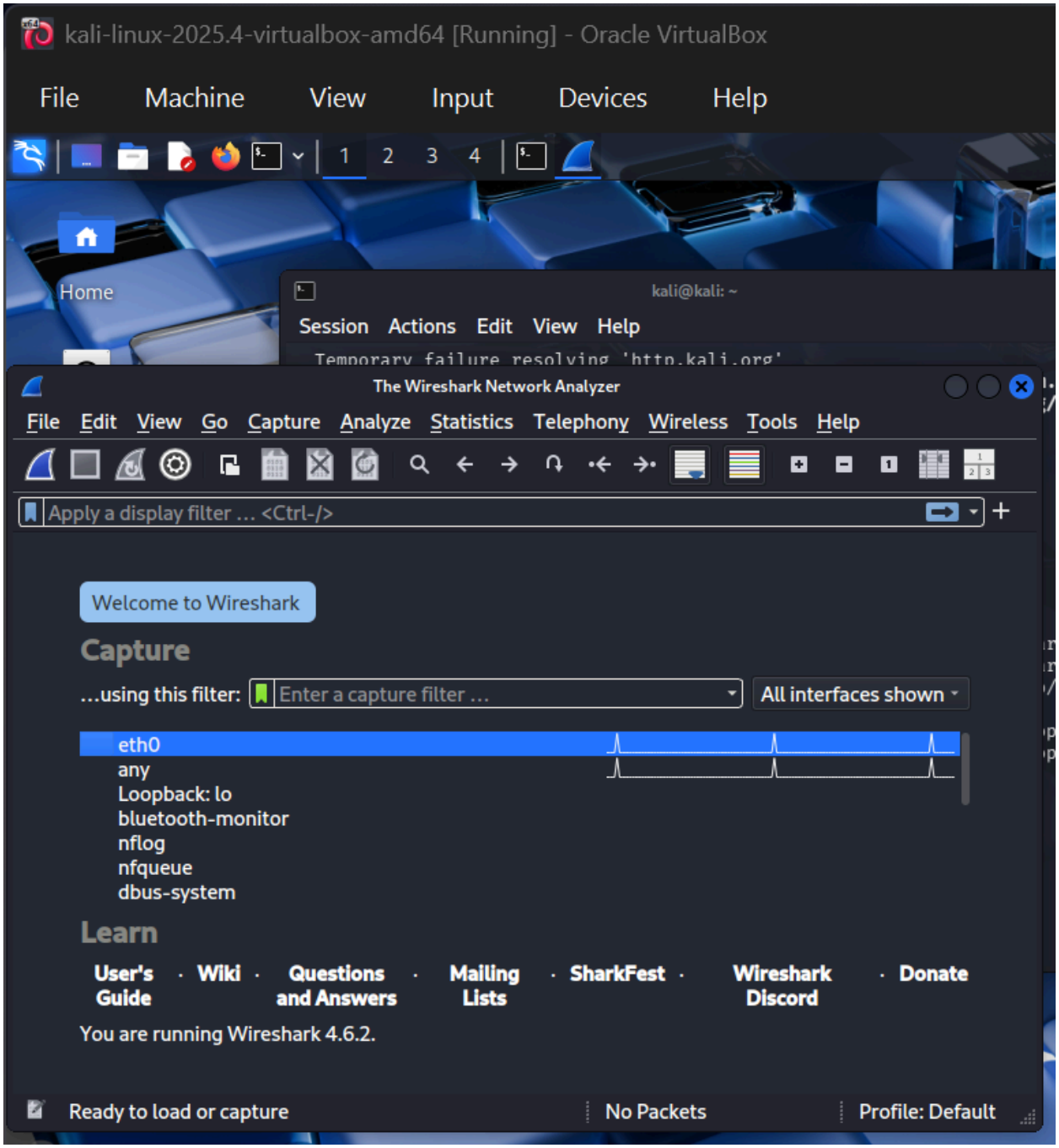
In this step we have to install wireshark on linux .first if linux is on (internal network) we have to provide linux to access of internet ,we will convert internal network to NAT Then we have to enter this command to update (sudo apt update) after that we have install wireshark using this command (sudo apt install wireshark -y) inbetwwen installation we have to allow to capture root by typing (Yes) if they ask only .after that we have to logout by (ctrl+c) and we will check the status by giving command

(wireshark –version) and if have to open wireshark we can use this command (wireshark&).



STEP 2: Identify the Correct Interface

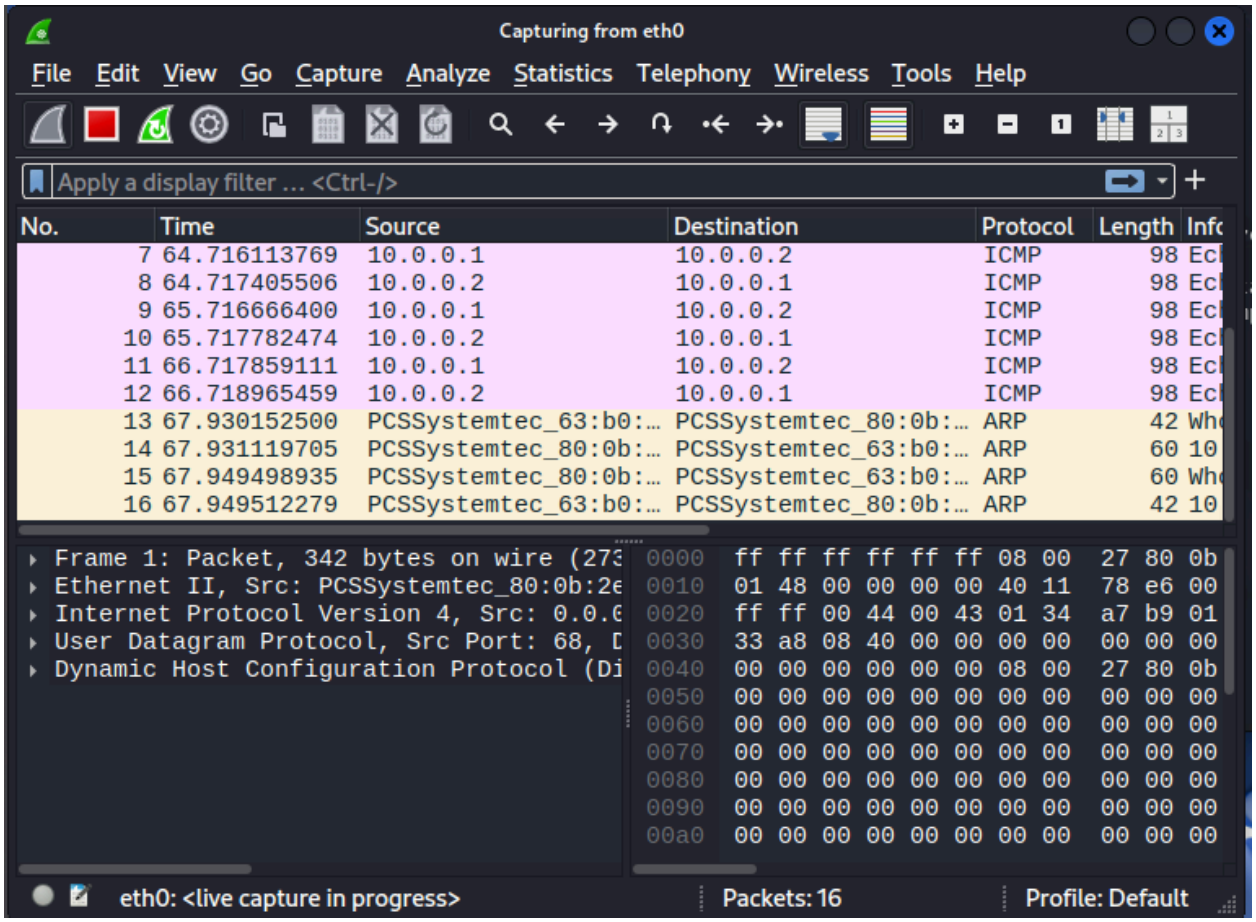
After opening wireshark we have to watch active interface inform of (eth0)or (any)
Both packets would be moving like heartbeats up and down we have to amin chose eth0



STEP 3: Capture ICMP (Ping Test)

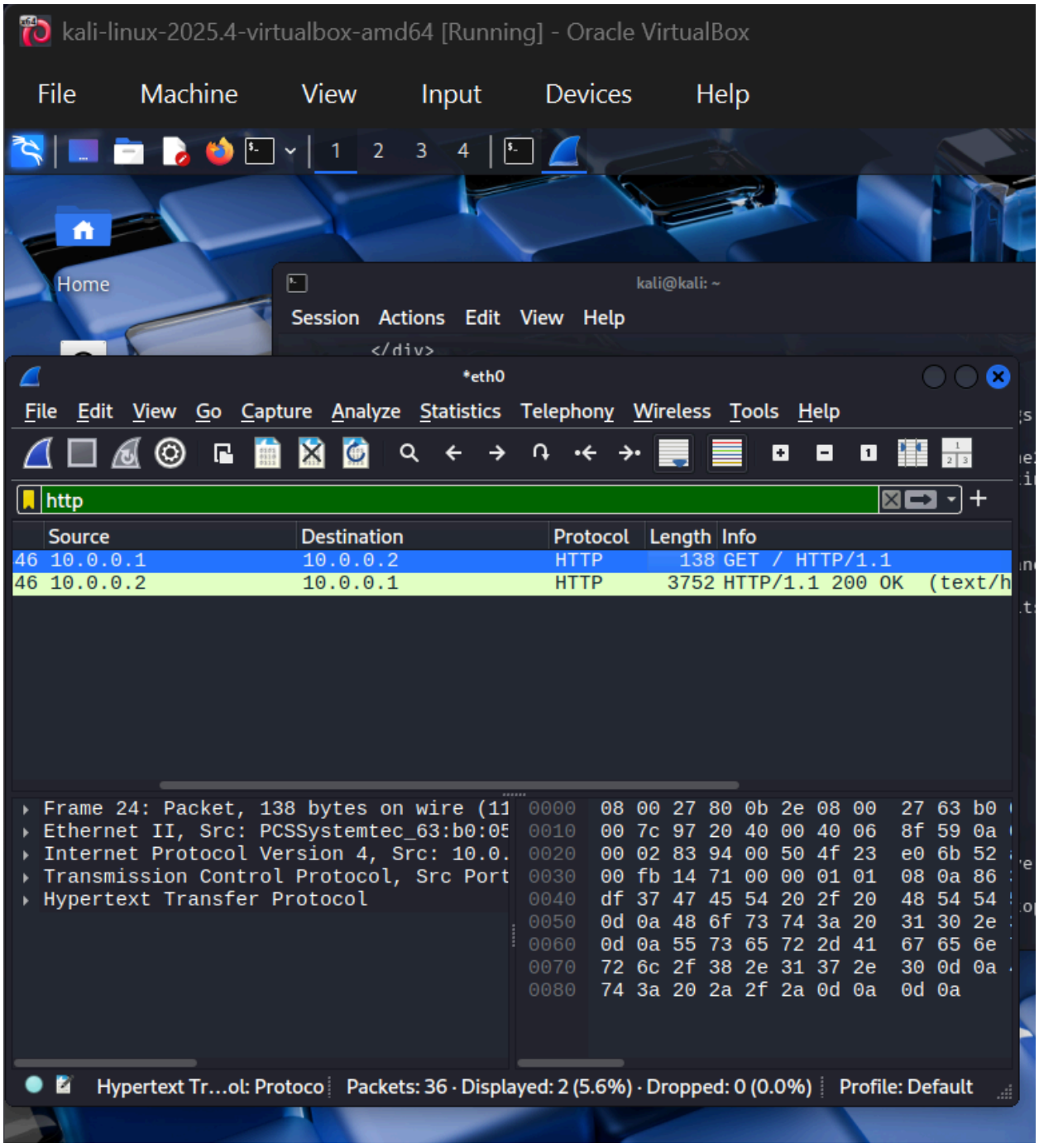
Now we can see two terminal is open one is kali terminal and other is wireshark terminal .now we have to move to to kali terminal and type this command (ping 10.0.0.2) for ping testing

After command we have to move to wireshark terminal and on the above searchbar we have to type icmp now the result we can see in layers .In Wireshark, make sure **eth0** is highlighted. **Go Live**: Click the **Blue Shark Fin** icon in the top-left corner.**Stop the Recording**: Go back to Wireshark and click the **Red Square** icon (next to the shark fin).



STEP 4: Capture HTTP Traffic (Plaintext)

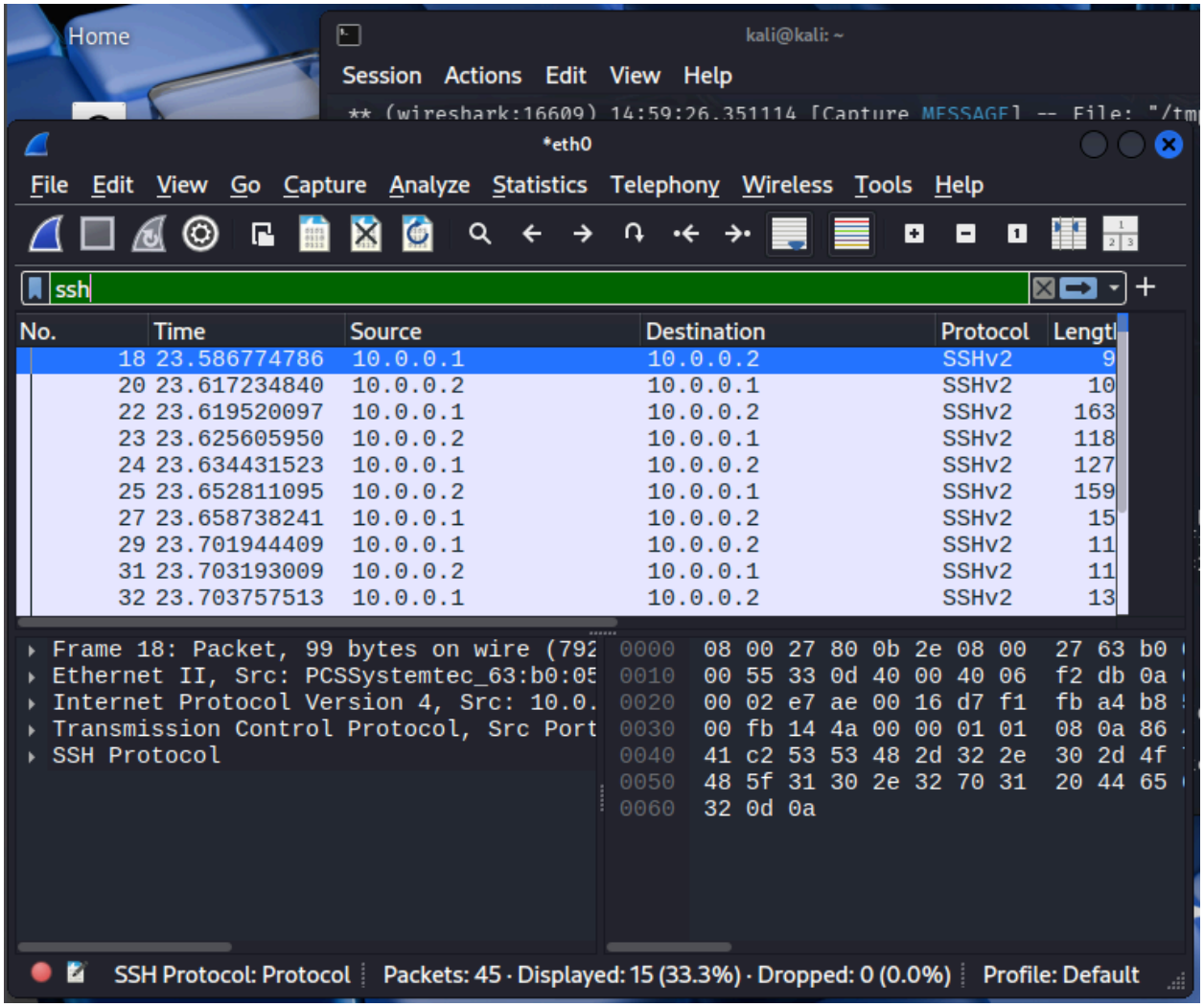
Now we have capture http(hyper text transfer protocol) traffic .on the kali terminal we have to type (curl http://10.0.0.2) after this command we have to go back to wireshark terminal , search http then it will show everything .**Stop the Recording**: Go back to Wireshark and click the **Red Square** icon (next to the shark fin).then type http



STEP 5: Capture SSH Traffic (Encrypted)

Now we to do same thing that we have done on http but the command will be change , on the kali terminal we will put (ssh testuser@10.0.0.2) after this we have to put wrong or any password for encrypted action appears then have to go back to wireshark terminal and **Stop the**

Recording: Go back to Wireshark and click the **Red Square** icon (next to the shark fin). Then in the search bar type ssh we will see many layers of encrypted ,that is the wrong password we enterend .



STEP 6: Compare & Think (MOST IMPORTANT STEP)

Answer these in your notes:

- Why can I read HTTP but not SSH?
- What layer is encryption applied?

- Why does packet visibility still matter even when encrypted?

1ans : why i can read http(port80) but not ssh(port22) becz the first thing the command we have entered ,it is to see website html and on that time we have not entered in ubuntu terminal

2ans: in which layer I have put an incorrect or correct password that layer is encrypted.

3ans: packet still matters while encrypted ,if anyone (attacker)is doing something with our os ,server ,like attacking we can see that by the wireshark tool.|

STEP 7: (Optional but Powerful) Use tcpdump

See to install tspdump we have to use same procedure that we have done before for wireshark
Just the command to install we will type (sudo apt install tcpdump -y) but it should be install in ubuntu terminal not kali.
Now we are doing (The Terminal Sniffer) on ubuntu ,we are going to prepare the Ubuntu "Listener" the command we are using in this is (sudo tcpdump -i any port 22 or port 80)
Explanation: `-i any` means listen on every wire; `port 22` is SSH; `port 80` is HTTP.

Press Enter. The terminal will say: `tcpdump: listening on any...`. It is now waiting for a signal.Trigger from Kali (The "Sender")**Go to your Kali Linux VM**.

Trigger HTTP: Type `curl http://10.0.0.2` and press Enter.

Trigger SSH: Type `ssh 10.0.0.2` and press Enter (you don't even need to log in, just start the connection).

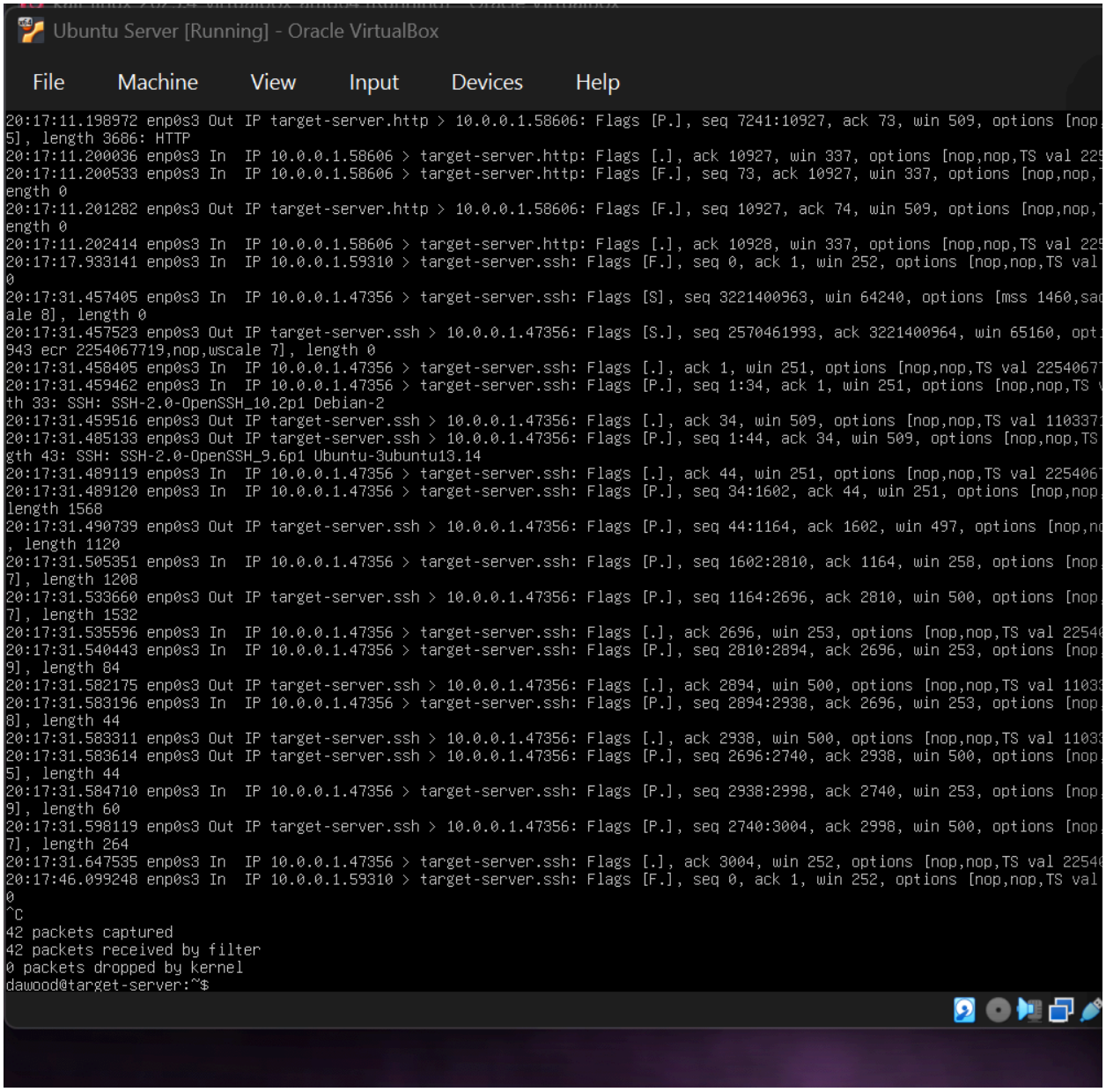
Go back to Ubuntu. You will see lines of text flying across the screen!

Stop it: Press Ctrl + C on your keyboard to stop the capture.

Look for the names:

- Look for lines containing `.http` or `.80`.

- Look for lines containing `.ssh` or `.22`.



. Connectivity & Troubleshooting

Command	Where to Type	What it Does

ping -c 4 10.0.0.2	**Kali**	Checks if the "bridge" to Ubuntu is open.
nc -zv 10.0.0.2 22	**Kali**	Checks if the SSH "door" (Port 22) is open.
sudo systemctl restart ssh	**Ubuntu**	Wakes up the SSH service if it's sleeping.
sudo ufw allow 22/tcp	**Ubuntu**	Tells the firewall to let SSH traffic pass through.

2. Generating Traffic

Command	Where to Type	What it Does
curl http://10.0.0.2	**Kali**	Grabs the website data (creates HTTP traffic).
ssh testuser@10.0.0.2	**Kali**	Starts a secure connection (creates SSH traffic).

3. Packet Capturing (CLI)

Command	Where to Type	What it Does
sudo tcpdump -i any	**Ubuntu**	Starts sniffing all traffic on the server.
sudo tcpdump -i any port 80	**Ubuntu**	Sniffs ONLY website (HTTP) traffic.

"Golden" Command Sheet

Action	Command	Result
Test	ping -c 4 10.0.0.2	Confirms connection.
Sniff (GUI)	wireshark	Visualizes the packets.
Trigger HTTP	curl http://10.0.0.2	Generates insecure traffic.
Trigger SSH	ssh 10.0.0.2	Generates secure traffic.
Sniff (CLI)	sudo tcpdump -i any	Professional server-side capture.