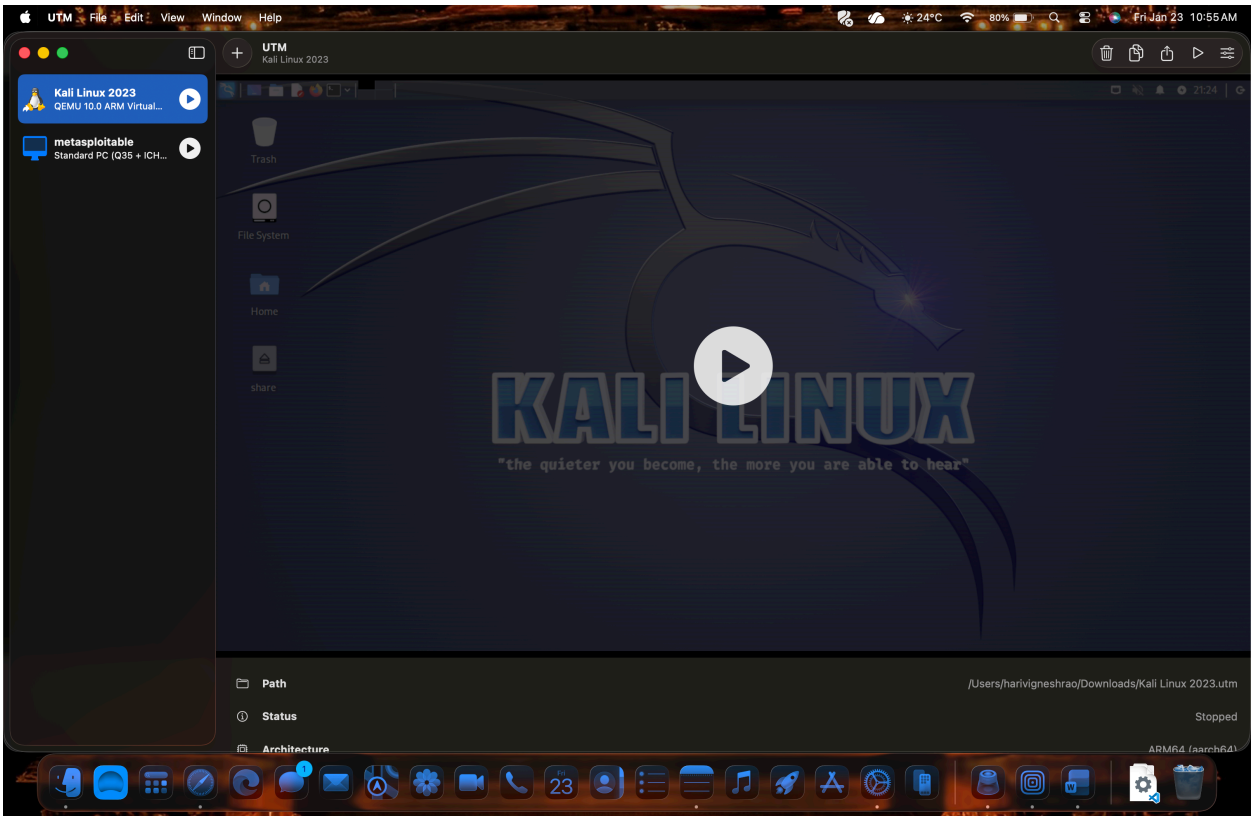
CYBER SECURITY LAB-4 PACKET SNIFFING AND NETWORK TRAFFIC ANALYSIS

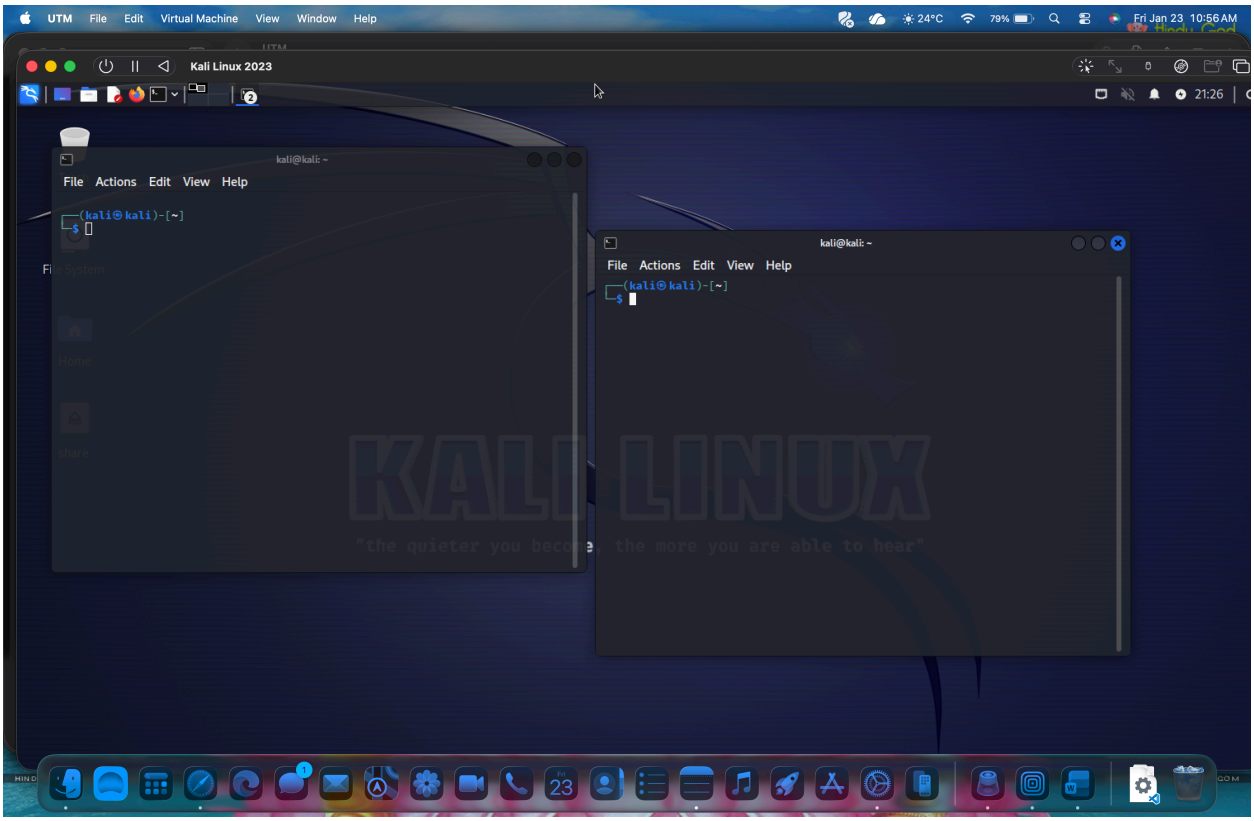
HARI VIGNESH RAO 23BD1A05Q

Procedure:

Step 1: Open Kali Linux.



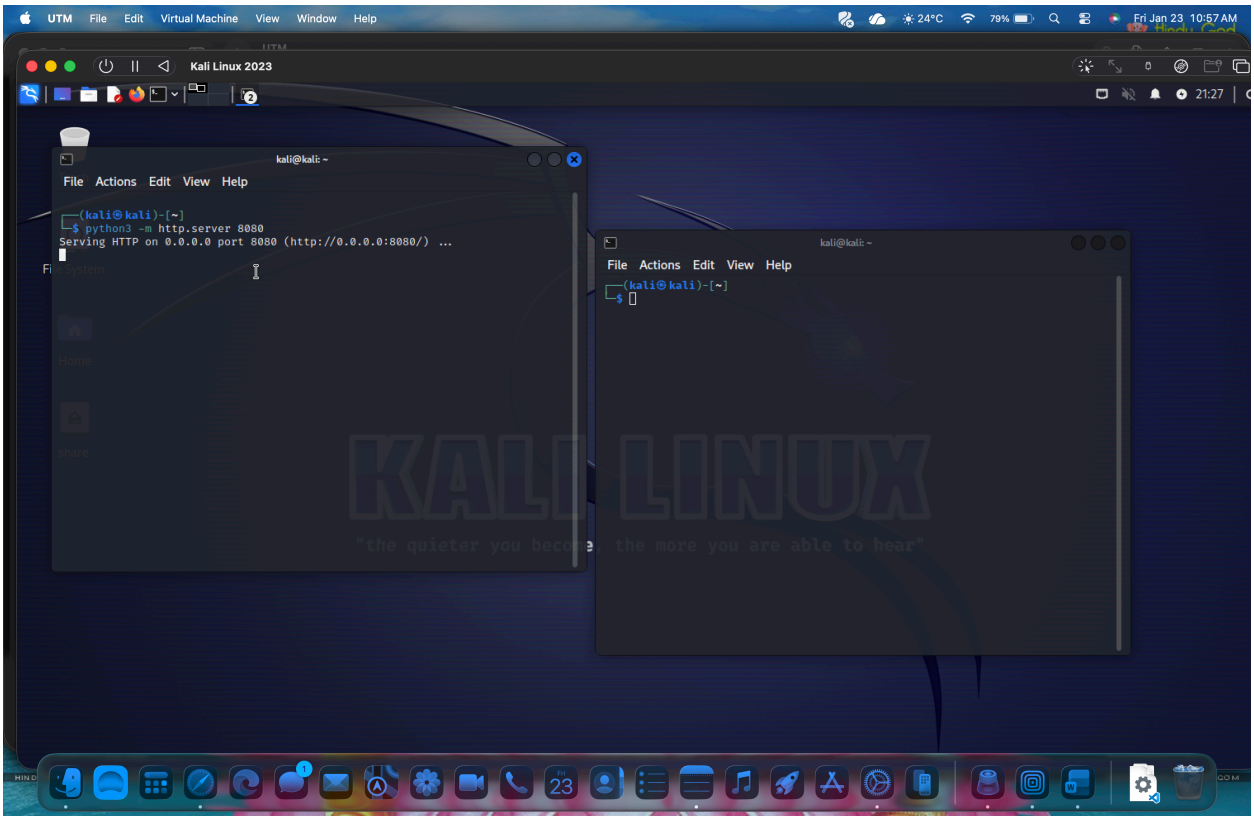
Step 2: Open Terminal in Kali Linux.



Step 3:

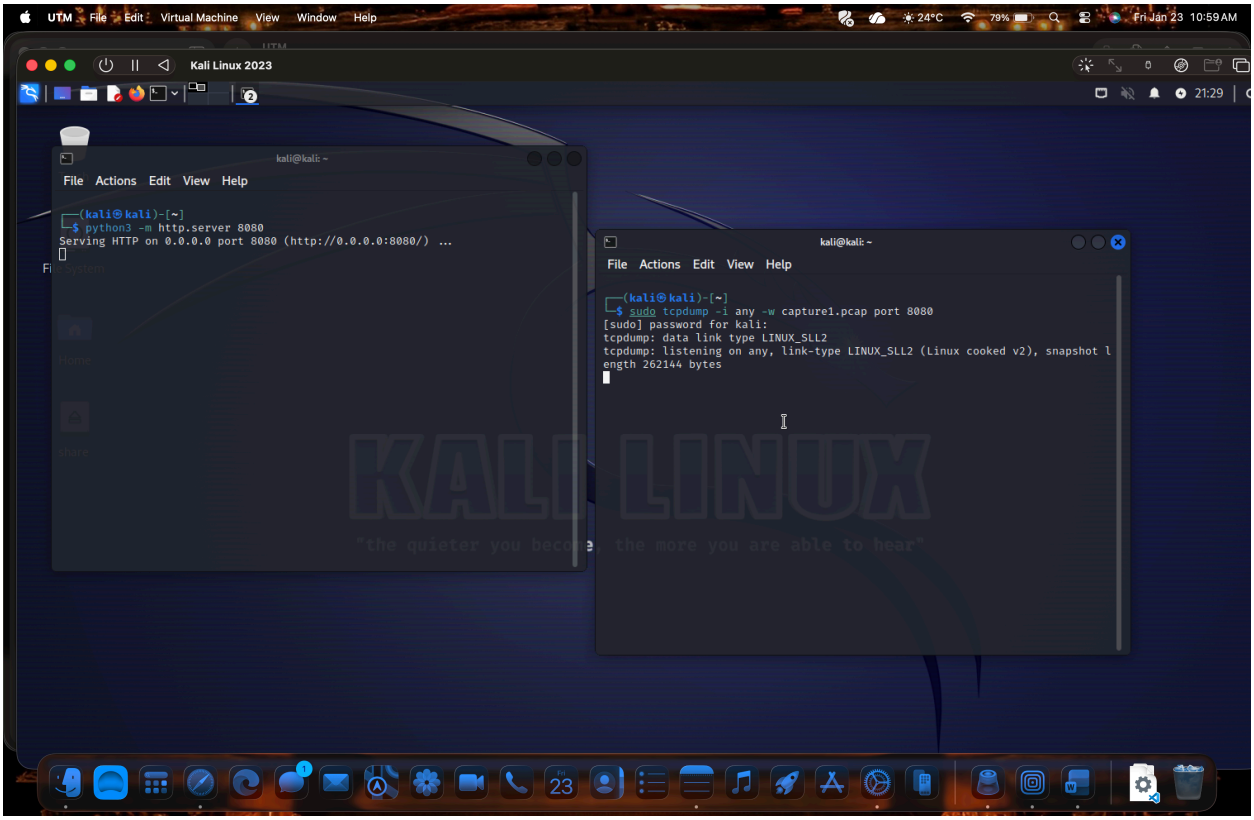
Start a local HTTP server on port 8080 using :

python3 -m http.server 8080



Step 4: In another new terminal start packet capture:

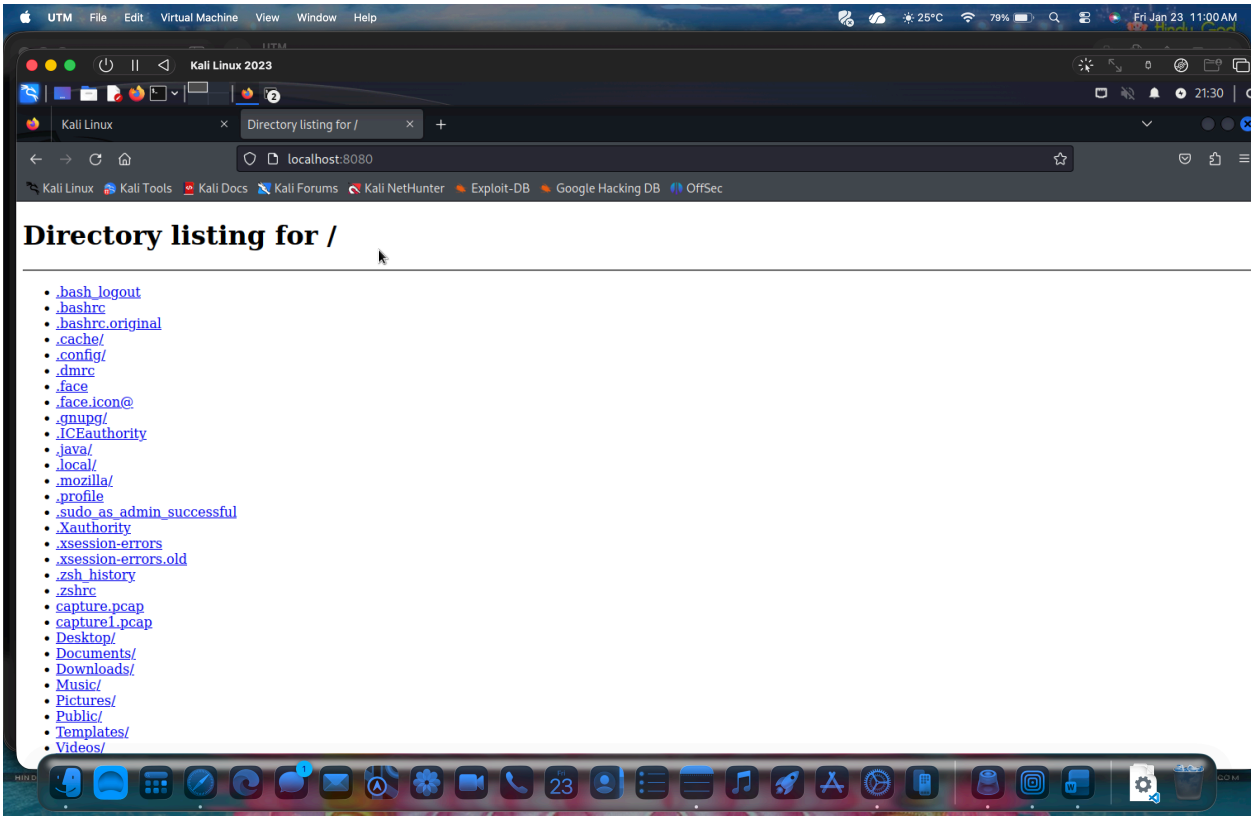
sudo tcpdump -i any -w capture.pcap port 8080



Step 5: Open Firefox in kali Linux and go to:

http://localhost:8080

Refresh the page to generate traffic.



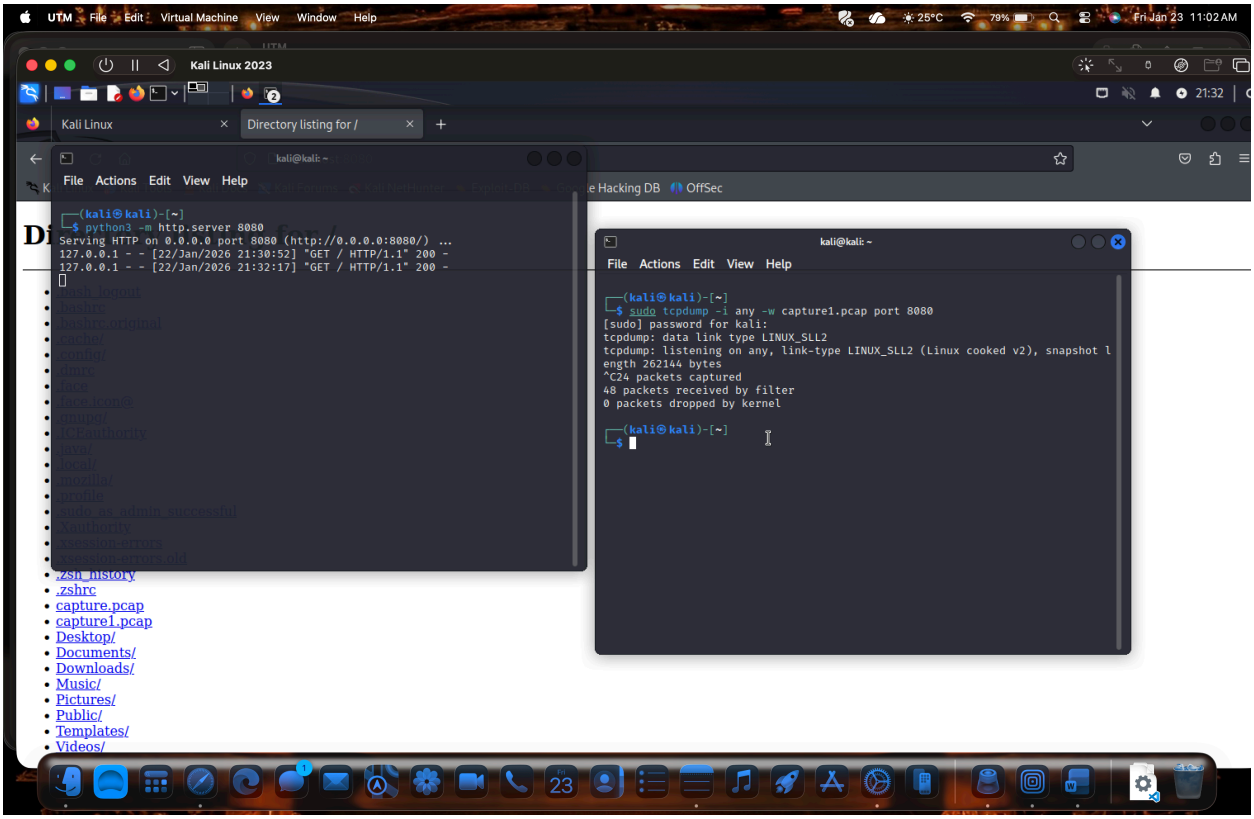
Step 6:

Go back to tcpdump terminal.

Stop packet capturing by using Ctrl + C.

It will stop and show how many packets were captured

The packets are saved as capture.pcap.



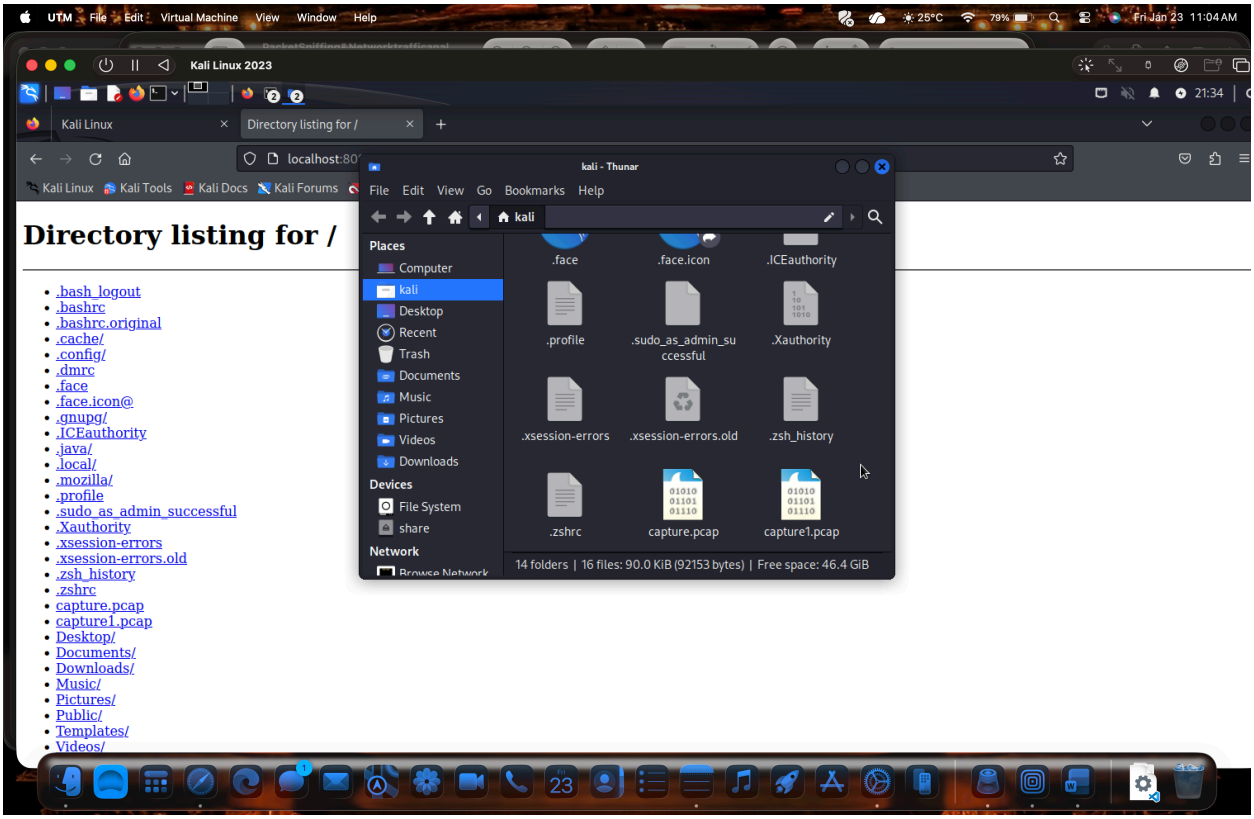
Step 7:

• Click the Kali Linux dragon icon (top left).

• Type: File Manager and open it.

• Your Home folder will open.

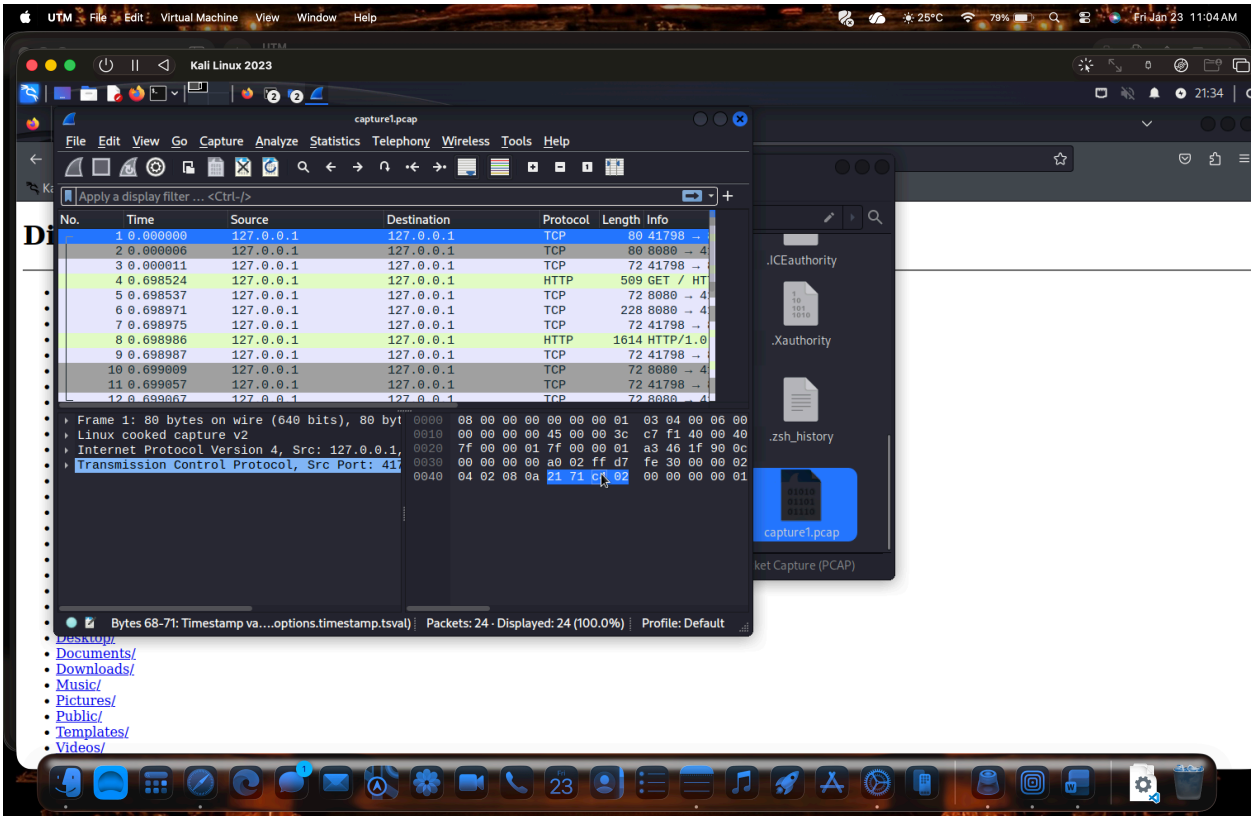
• You will see the file: capture1.pcap.



Step 8:-

• Since Wireshark is pre-installed in Kali, just double-click capture1.pcap.

• The file will open directly in Wireshark for analysis.



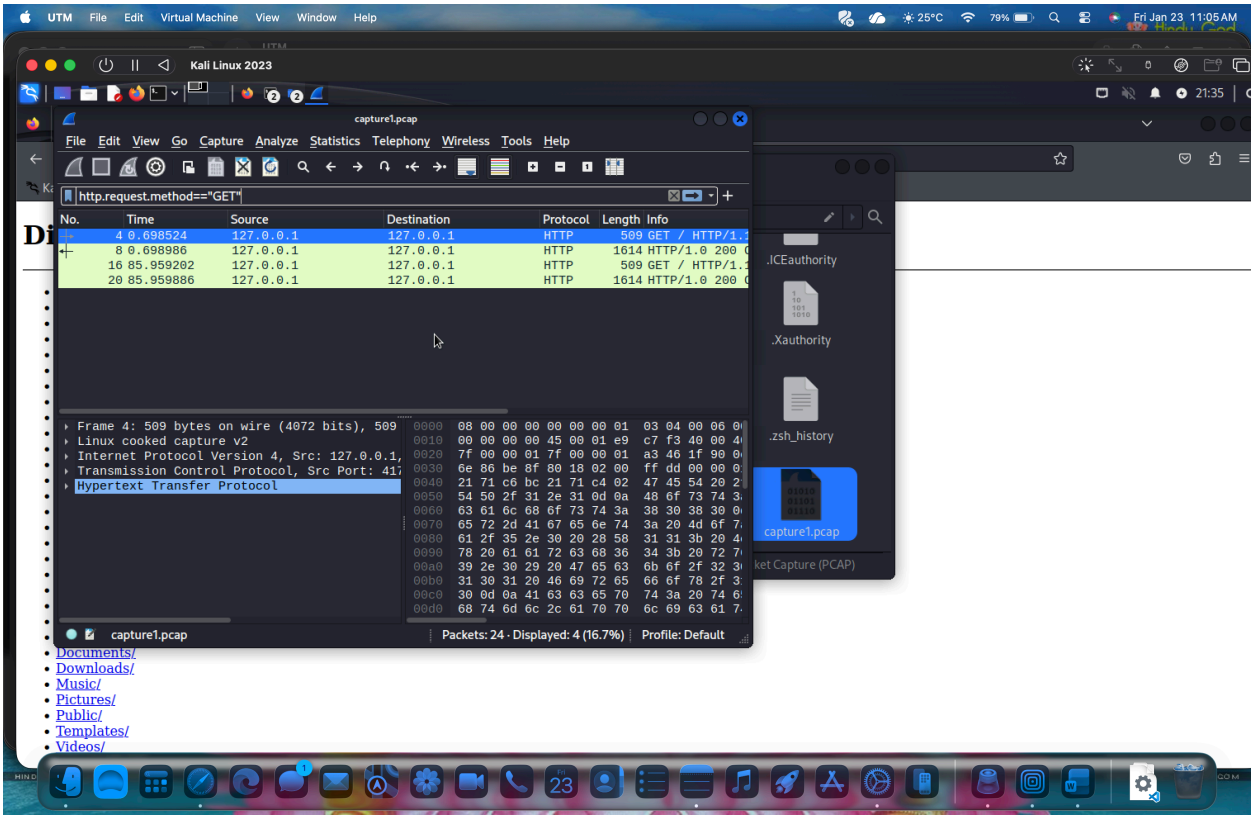
Step 9:-

Filter Login Packets

In Wireshark filter bar, type: http.request.method == "GET"

Press Enter.

Now only important packets will show.



Step 10:-

Click on any one of the packet and the following data is displayed.

Browser details such as OS, browser version, language, and visited URLs are visible.If a form is submitted, username and password can be seen in plain text.This proves HTTP is insecure.