**Task 5: Capture and Analyze Network Traffic Using Wireshark.**

1. **Install Wireshark and tshark (if not already)**

* $sudo apt upgrade
* A computer screen shot of a program

  AI-generated content may be incorrect.$sudo apt install -y wireshark tshark

Add your user to the wireshark group (so you can run captures without sudo):

* $sudo usermod -aG wireshark $USER

# Apply group immediately for current shell:

* A screenshot of a computer

  AI-generated content may be incorrect.$getent group wireshark

1. **Identify your active interface**

List interfaces:

* $ ip link show # lists all interfaces or with tshark
* $tshark -D

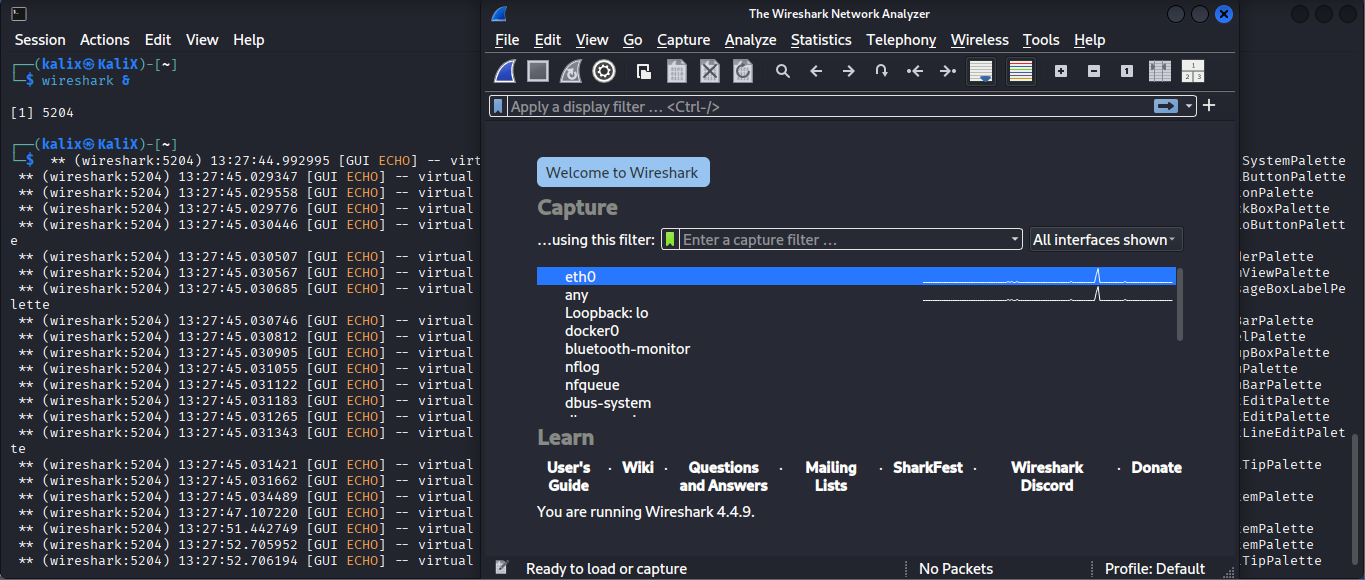
A screenshot of a computer

AI-generated content may be incorrect.

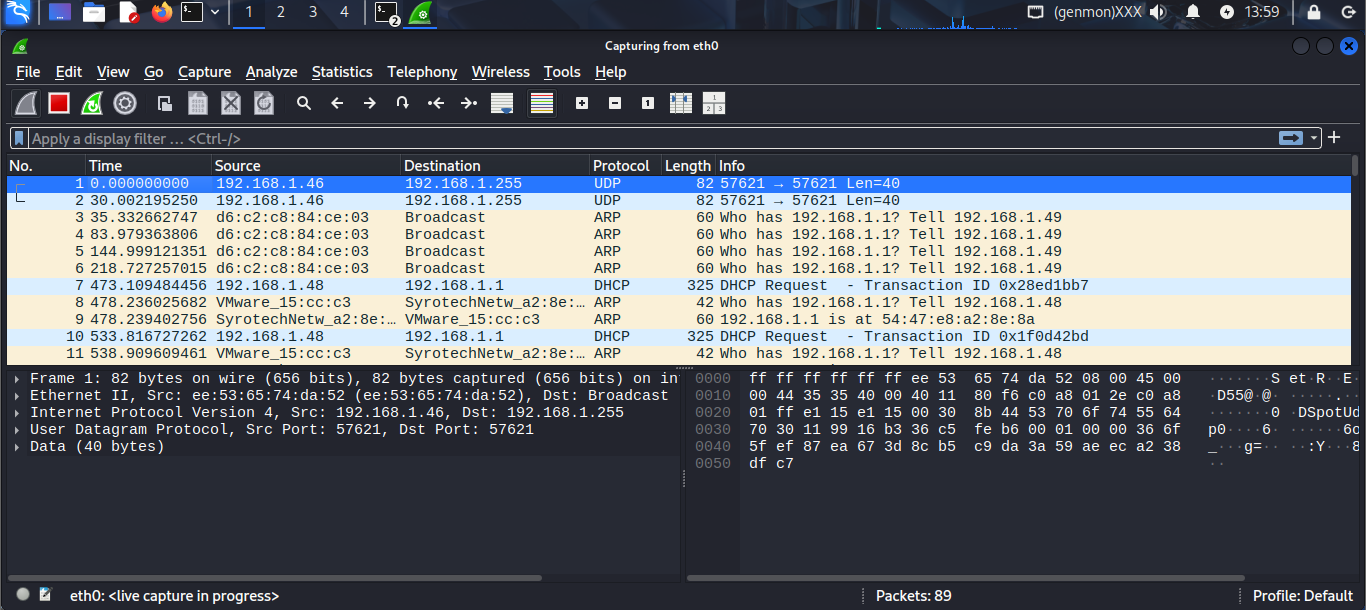
Common names: eth0, ens33, wlan0, wlp3s0.

1. **GUI capture with Wireshark**

* Start Wireshark

$wireshark &

* Select the interface (e.g., wlan0 or eth0) and click the blue shark-fin to **Start** capturing.
* (Optional) Set a **capture filter** to limit what is recorded (see below).



* Generate traffic (see step 4).
* Click the red square to **Stop** capture.
* Save capture: File → Save As... → choose capture.pcap or capture.pcapng, save to ~/wireshark-task/captures/capture.pcap.

1. **Generate traffic to create packets**

Open another terminal while capturing, run a few commands to generate different protocols:

# 1. DNS lookup (UDP)

$dig @8.8.8.8 example.com

# 2. Ping (ICMP)

$ping -c 5 8.8.8.8

# 3. HTTP request (un-encrypted)

$curl -I http://example.com

# 4. HTTPS request (TLS)

$curl -I https://example.com

# 5. SSH attempt (TCP) - optional if you have a host

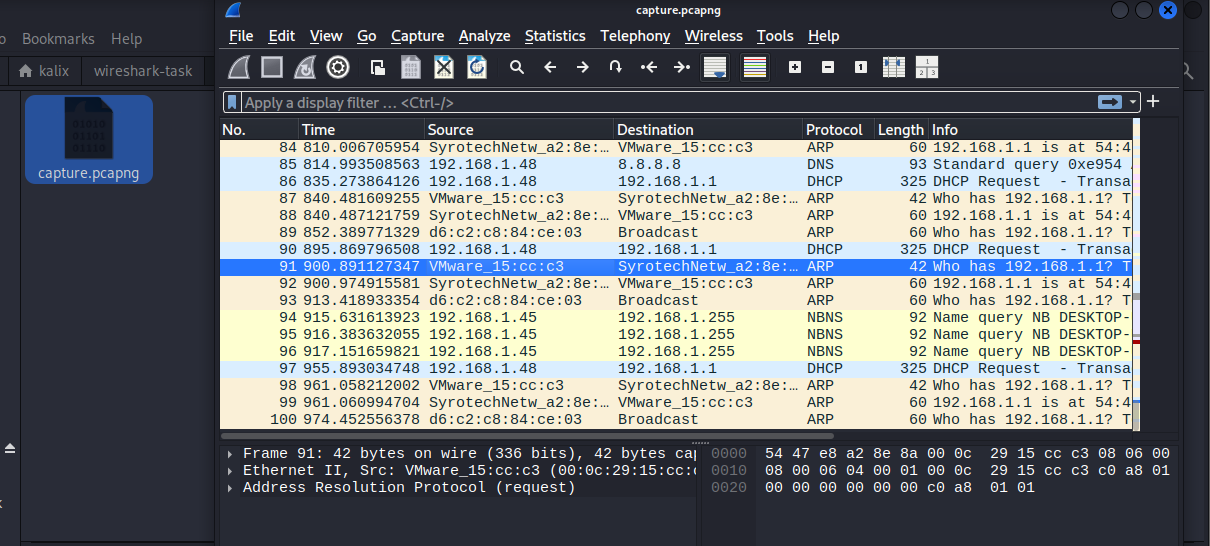
$ssh -o BatchMode=yes user@remote-host true

# 6. Simple apt update to create TLS + HTTP traffic (will generate DNS and TLS)

$sudo apt update -y

* Run a few of these (mix them) while the capture is running for ~1 minute

1. **Stop capture and save pcapng / pcap**

If using GUI — click Stop and File → Save As....  
If using CLI — capture will stop automatically if you used -a duration or press Ctrl+C to stop tshark/dumpcap.