

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

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

- `$sudo apt upgrade`
- `$sudo apt install -y wireshark tshark`

```
Session Actions Edit View Help
(kalix@Kalix)-[~]
$ sudo apt install -y wireshark tshark
[sudo] password for kalix:
wireshark is already the newest version (4.4.9-1).
tshark is already the newest version (4.4.9-1).
tshark set to manually installed.
The following package was automatically installed and is no longer required:
  libjs-jquery-ui
Use 'sudo apt autoremove' to remove it.

Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 0
(kalix@Kalix)-[~]
$
```

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

- `$sudo usermod -aG wireshark $USER`  
# Apply group immediately for current shell:
- `$getent group wireshark`

```
Session Actions Edit View Help
-l, --login NEW_LOGIN      new value of the login name
-L, --lock                 lock the user account
-m, --move-home            move contents of the home directory to the
                           new location (use only with -d)
-o, --non-unique           allow using duplicate (non-unique) UID
-p, --password PASSWORD    use encrypted password for the new password
-P, --prefix PREFIX_DIR    prefix directory where are located the /etc/* files
-r, --remove               remove the user from only the supplemental GROUPS
                           mentioned by the -G option without removing
                           the user from other groups
-R, --root CHROOT_DIR      directory to chroot into
-s, --shell SHELL          new login shell for the user account
-u, --uid UID              new UID for the user account
-U, --unlock               unlock the user account
-v, --add-subuids FIRST-LAST add range of subordinate uids
-V, --del-subuids FIRST-LAST remove range of subordinate uids
-w, --add-subgids FIRST-LAST add range of subordinate gids
-W, --del-subgids FIRST-LAST remove range of subordinate gids
-Z, --selinux-user SEUSER   new SELinux user mapping for the user account
    --selinux-range SERANGE new SELinux MLS range for the user account

(kalix@Kalix)-[~]
$ getent group wireshark
wireshark:x:124:kalix,root

(kalix@Kalix)-[~]
$ getent group wireshark
wireshark:x:124:kalix,root

(kalix@Kalix)-[~]
$
```

## 2. Identify your active interface

List interfaces:

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

```
(kalix@Kalix)-[~]
$ ip link show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT group default qlen 1000
   link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP mode DEFAULT group default qlen 1000
   link/ether 00:0c:29:15:cc:c3 brd ff:ff:ff:ff:ff:ff
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN mode DEFAULT group default
   link/ether 02:42:00:c2:62:d8 brd ff:ff:ff:ff:ff:ff

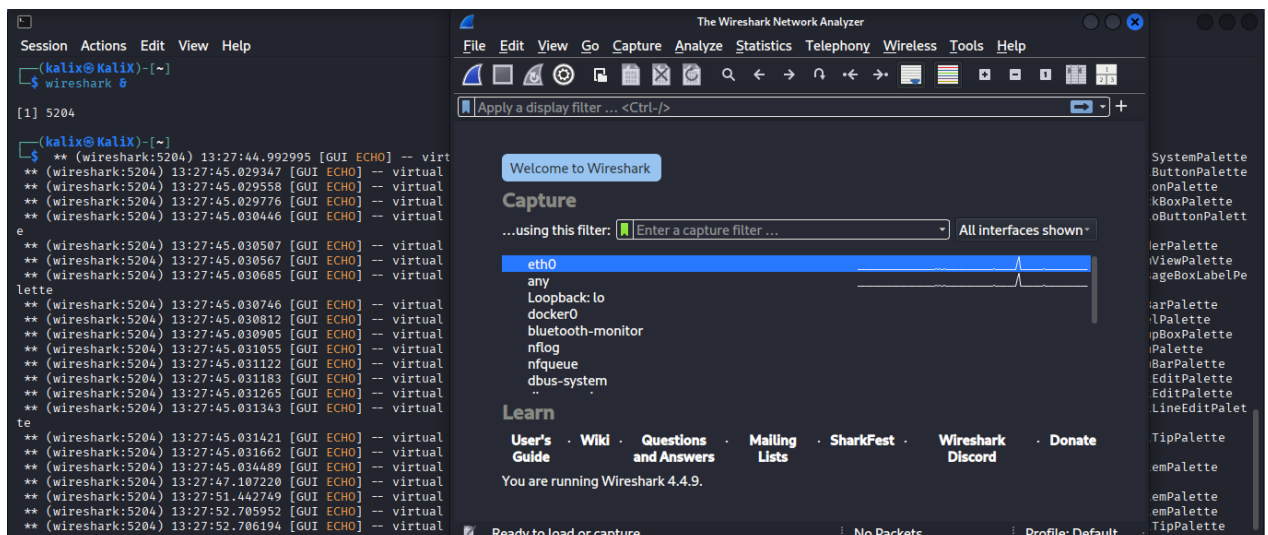
(kalix@Kalix)-[~]
$ tshark -D
1. eth0
2. any
3. lo (Loopback)
4. docker0
5. bluetooth-monitor
6. nflog
7. nfqueue
8. dbus-system
9. dbus-session
10. ciscodump (Cisco remote capture)
11. dpaukmon (DisplayPort AUX channel monitor capture)
12. randpkt (Random packet generator)
13. sdjournal (systemd Journal Export)
14. sshdump (SSH remote capture)
15. udpdump (UDP Listener remote capture)
16. wifidump (Wi-Fi remote capture)

(kalix@Kalix)-[~]
$
```

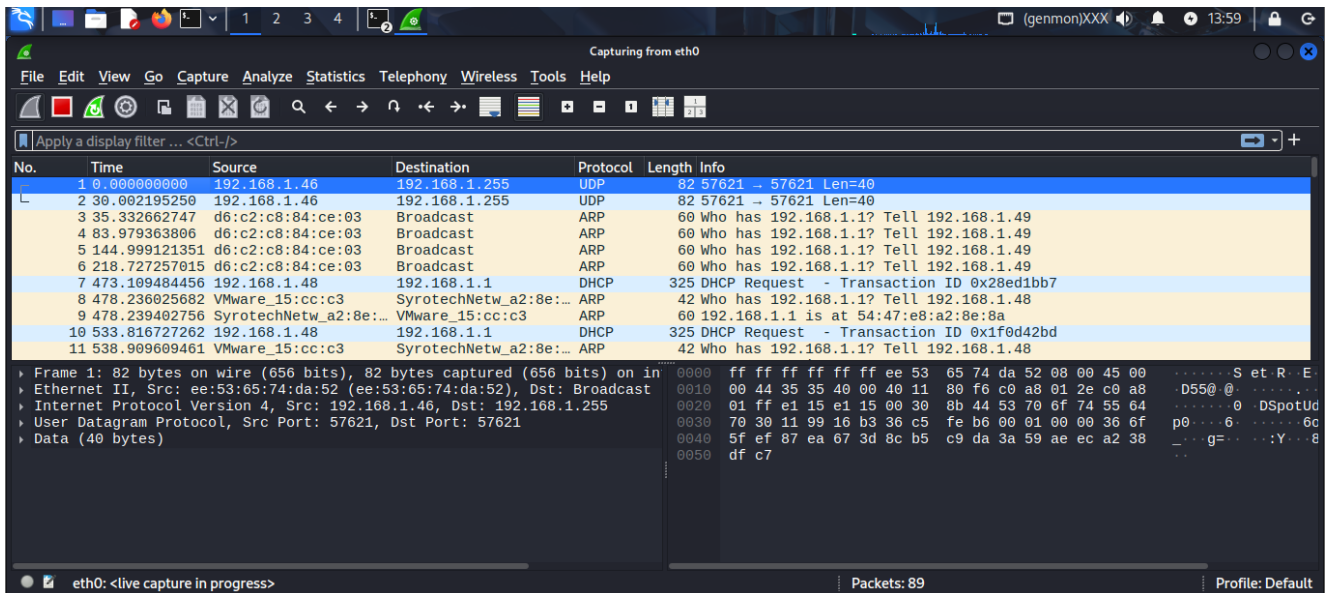
Common names: eth0, ens33, wlan0, wlp3s0.

## 3. 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`.

#### 4. 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.

## 5. 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`.

