

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

Step 1: Install Wireshark

```
sudo apt update
```

```
sudo apt install wireshark -y
```

```
sudo usermod -aG wireshark $USER
```

Log out and log back in for changes to take effect.

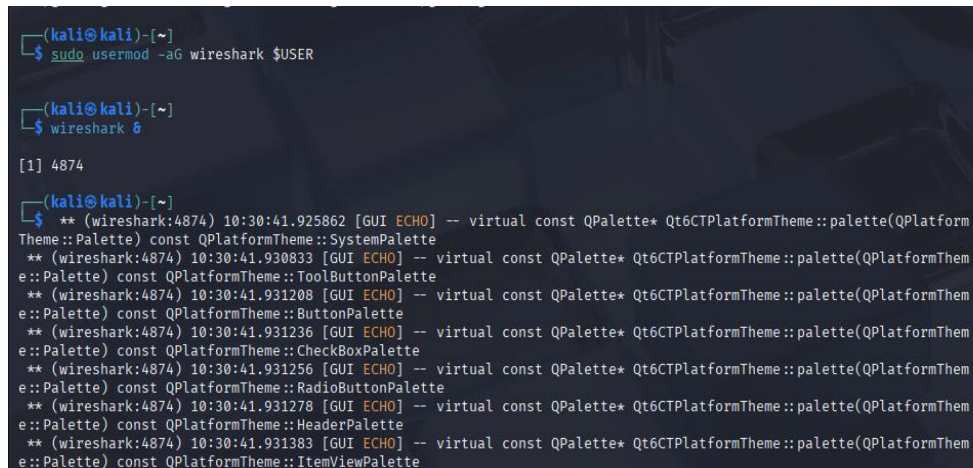
```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ sudo apt update  
sudo apt install wireshark -y  
[sudo] password for kali:  
Sorry, try again.  
[sudo] password for kali:  
Hit:1 https://packages.wazuh.com/4.x/apt stable InRelease  
Get:2 http://kali.download/kali kali-rolling InRelease [41.5 kB]  
Hit:3 https://repo.mongodb.org/apt/debian bullseye/mongodb-org/6.0 InRelease  
Get:4 http://kali.download/kali kali-rolling/main amd64 Packages [21.0 MB]  
Hit:5 https://repo.mongodb.org/apt/debian bullseye/mongodb-org/7.0 InRelease  
Get:6 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [51.4 MB]  
Get:7 http://kali.download/kali kali-rolling/non-free-firmware amd64 Packages [10.6 kB]  
Fetched 72.4 MB in 27s (2,661 kB/s)  
264 packages can be upgraded. Run 'apt list --upgradable' to see them.  
Warning: https://repo.mongodb.org/apt/debian/dists/bullseye/mongodb-org/6.0/InRelease: Policy will reject signature within a year, see --audit for details  
Warning: https://repo.mongodb.org/apt/debian/dists/bullseye/mongodb-org/7.0/InRelease: Policy will reject signature within a year, see --audit for details  
wireshark is already the newest version (4.4.7-1).  
Summary:  
Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 264  
(kali@kali)-[~]  
$ sudo usermod -aG wireshark $USER
```

```
(kali@kali)-[~]  
$ sudo usermod -aG wireshark $USER  
  
(kali@kali)-[~]  
$ wireshark &  
[1] 4874  
  
(kali@kali)-[~]  
$ ** (wireshark:4874) 10:30:41.925862 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::SystemPalette  
** (wireshark:4874) 10:30:41.930833 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::ToolButtonPalette  
** (wireshark:4874) 10:30:41.931208 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::ButtonPalette  
** (wireshark:4874) 10:30:41.931236 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::CheckBoxPalette  
** (wireshark:4874) 10:30:41.931256 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::RadioButtonPalette  
** (wireshark:4874) 10:30:41.931278 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::HeaderPalette  
** (wireshark:4874) 10:30:41.931383 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::ItemViewPalette
```

## Step 2: Launch Wireshark and Select Interface

wireshark &

- Open Wireshark GUI.
- Select the **active interface** (e.g., eth0 or wlan0).
- Click **Start Capturing**.

A terminal window on a Kali Linux system. The prompt is (kali@kali)-[~]. The user enters 'sudo usermod -aG wireshark \$USER'. The prompt changes to (kali@kali)-[~] and the user enters 'wireshark &'. The prompt changes to [1] 4874. The user then enters a long command to install Qt6CTPlatformTheme and Qt6CTPlatformTheme::palette. The output shows several lines of C++ code being installed, including virtual const QPalette\* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::SystemPalette, virtual const QPalette\* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::ToolButtonPalette, virtual const QPalette\* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::ButtonPalette, virtual const QPalette\* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::CheckBoxPalette, virtual const QPalette\* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::RadioButtonPalette, virtual const QPalette\* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::HeaderPalette, and virtual const QPalette\* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::ItemViewPalette.

```
(kali@kali)-[~]  
$ sudo usermod -aG wireshark $USER  
  
(kali@kali)-[~]  
$ wireshark &  
  
[1] 4874  
  
(kali@kali)-[~]  
$ ** (wireshark:4874) 10:30:41.925862 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::SystemPalette  
** (wireshark:4874) 10:30:41.930833 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::ToolButtonPalette  
** (wireshark:4874) 10:30:41.931208 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::ButtonPalette  
** (wireshark:4874) 10:30:41.931236 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::CheckBoxPalette  
** (wireshark:4874) 10:30:41.931256 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::RadioButtonPalette  
** (wireshark:4874) 10:30:41.931278 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::HeaderPalette  
** (wireshark:4874) 10:30:41.931383 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::ItemViewPalette
```

## Step 3: Generate Traffic

Open a terminal and run:

ping google.com

- Also, open Firefox and visit a website such as example.com.

## Step 4: Stop Capture

- After 1 minute, click the **red square Stop button** in Wireshark.

## Step 5: Apply Protocol Filters

Use the filter bar in Wireshark to analyze specific protocols:

- dns
- tcp
- icmp

## Step 6: Screenshots of Captured Packets

- DNS Traffic

Captured DNS queries and responses.

No.	Time	Source	Destination	Protocol	Length	Info
35	88.173834656	192.168.254.139	192.168.254.2	DNS	70	Standard query 0xee99 A google.com
36	88.174899926	192.168.254.139	192.168.254.2	DNS	70	Standard query 0xb0e7 AAAA google.com
37	88.189992493	192.168.254.2	192.168.254.139	DNS	86	Standard query response 0xee99 A google.com A 142.250.192.110
38	88.189993784	192.168.254.2	192.168.254.139	DNS	154	Standard query response 0xb0e7 AAAA google.com AAAA 2484:6800:4007:838::200e AAAA 2484:6800:4007:82a::200e AAAA 2484:6800:4007:836::200e
41	88.254455861	192.168.254.139	192.168.254.2	DNS	88	Standard query 0x32ea PTR 119.192.250.142.in-addr.arpa
42	88.260580553	192.168.254.2	192.168.254.139	DNS	510	Standard query response 0x32ea PTR 119.192.250.142.in-addr.arpa PTR bow12s17-in-f14.1e100.net OPT

Domain Name System: Protocol

Packets: 269 - Displayed: 6 (2.2%) - Dropped: 0 (0.0%)

Profile: Default

- TCP Traffic

Shows TCP SYN, retransmissions, RST/ACK, etc.

No.	Time	Source	Destination	Protocol	Length	Info
4	2.668778814	192.168.254.139	192.168.1.100	TCP	74	41789 → 1515 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3164866690 TSecr=0 WS=128
13	11.754241987	192.168.254.139	192.168.1.100	TCP	74	[TCP Retransmission] 41789 → 1515 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3164874882 TSecr=0 WS=128
15	12.692875899	192.168.1.100	192.168.254.139	TCP	60	1515 → 41789 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
16	31.697752171	192.168.254.139	192.168.1.100	TCP	74	57329 → 1515 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3164908026 TSecr=0 WS=128
17	38.738426319	192.168.254.139	192.168.1.100	TCP	74	[TCP Retransmission] 57329 → 1515 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3164908188 TSecr=0 WS=128
18	39.754410137	192.168.254.139	192.168.1.100	TCP	74	[TCP Retransmission] 57329 → 1515 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3164902882 TSecr=0 WS=128
19	40.779188838	192.168.254.139	192.168.1.100	TCP	74	[TCP Retransmission] 57329 → 1515 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3164903907 TSecr=0 WS=128
20	41.801919633	192.168.254.139	192.168.1.100	TCP	74	[TCP Retransmission] 57329 → 1515 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3164904630 TSecr=0 WS=128
25	43.694093854	192.168.254.139	192.168.1.100	TCP	74	[TCP Retransmission] 57329 → 1515 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3164905954 TSecr=0 WS=128
26	45.710447309	192.168.254.139	192.168.1.100	TCP	74	[TCP Retransmission] 57329 → 1515 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3164907078 TSecr=0 WS=128
27	46.742559260	192.168.254.139	192.168.1.100	TCP	74	[TCP Retransmission] 57329 → 1515 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3164912082 TSecr=0 WS=128
28	57.934511190	192.168.254.139	192.168.1.100	TCP	74	[TCP Retransmission] 57329 → 1515 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3164920194 TSecr=0 WS=128
30	59.679501083	192.168.1.100	192.168.254.139	TCP	60	1515 → 57329 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
43	59.832659125	192.168.254.139	192.168.1.100	TCP	74	39487 → 1515 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3164951344 TSecr=0 WS=128
48	59.926832326	192.168.254.139	192.168.1.100	TCP	74	[TCP Retransmission] 39487 → 1515 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3164952354 TSecr=0 WS=128
51	51.951278832	192.168.254.139	192.168.1.100	TCP	74	[TCP Retransmission] 39487 → 1515 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3164953378 TSecr=0 WS=128
54	52.975391771	192.168.254.139	192.168.1.100	TCP	74	[TCP Retransmission] 39487 → 1515 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3164954402 TSecr=0 WS=128
59	59.989333354	192.168.254.139	192.168.1.100	TCP	74	[TCP Retransmission] 39487 → 1515 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3164955426 TSecr=0 WS=128
62	55.822931883	192.168.254.139	192.168.1.100	TCP	74	[TCP Retransmission] 39487 → 1515 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3164956450 TSecr=0 WS=128

Frame 4: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth0, id 0

Ethernet II, Src: VMware\_d2:ea:ff (08:0c:29:d2:ea:ff), Dst: VMware\_f6:cc:9f (08:50:56:f6:cc:9f)

Internet Protocol Version 4, Src: 192.168.254.139, Dst: 192.168.1.100

Transmission Control Protocol, Src Port: 41789, Dst Port: 1515, Seq: 0, Len: 0

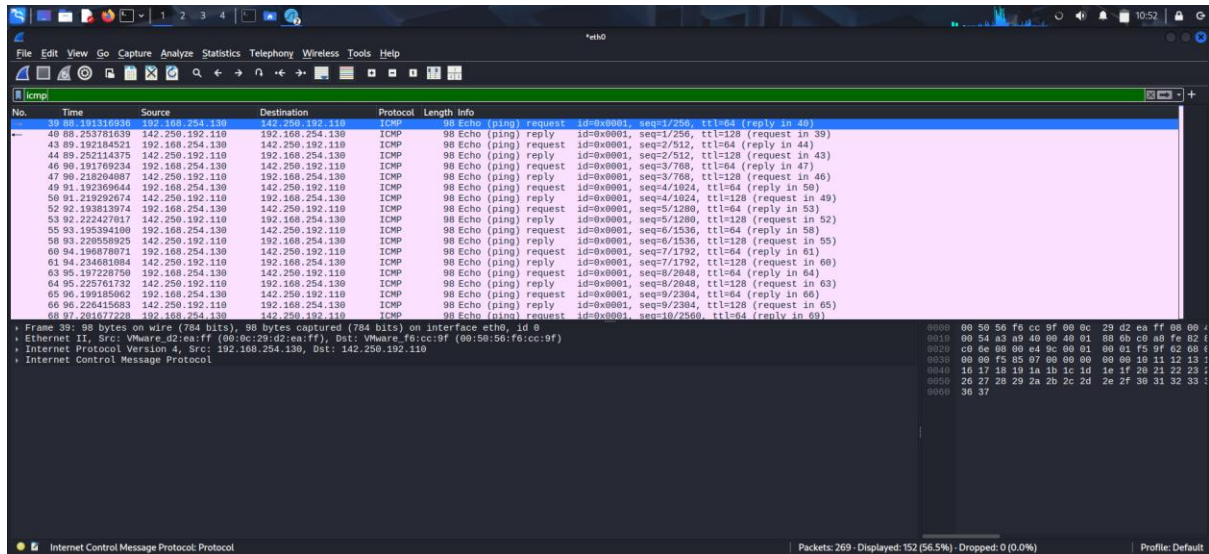
Transmission Control Protocol: Protocol

Packets: 269 - Displayed: 31 (11.5%) - Dropped: 0 (0.0%)

Profile: Default

- ICMP Traffic

Echo request and reply packets generated by ping.



## Step 7: Export the Capture

Go to File → Export Specified Packets.

Save as network - capture.pcap.