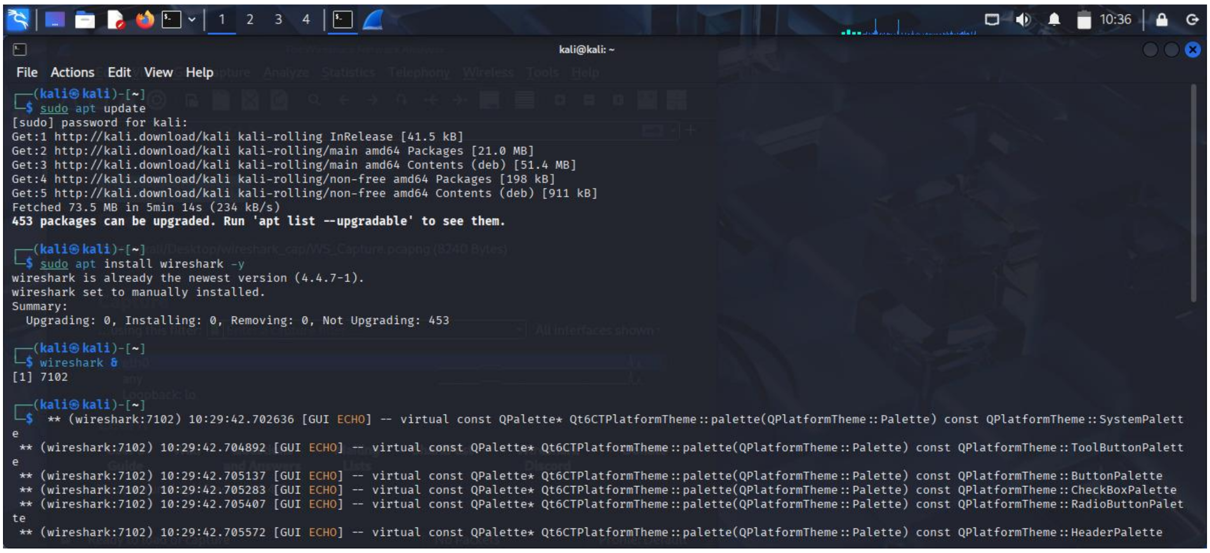
Task 5

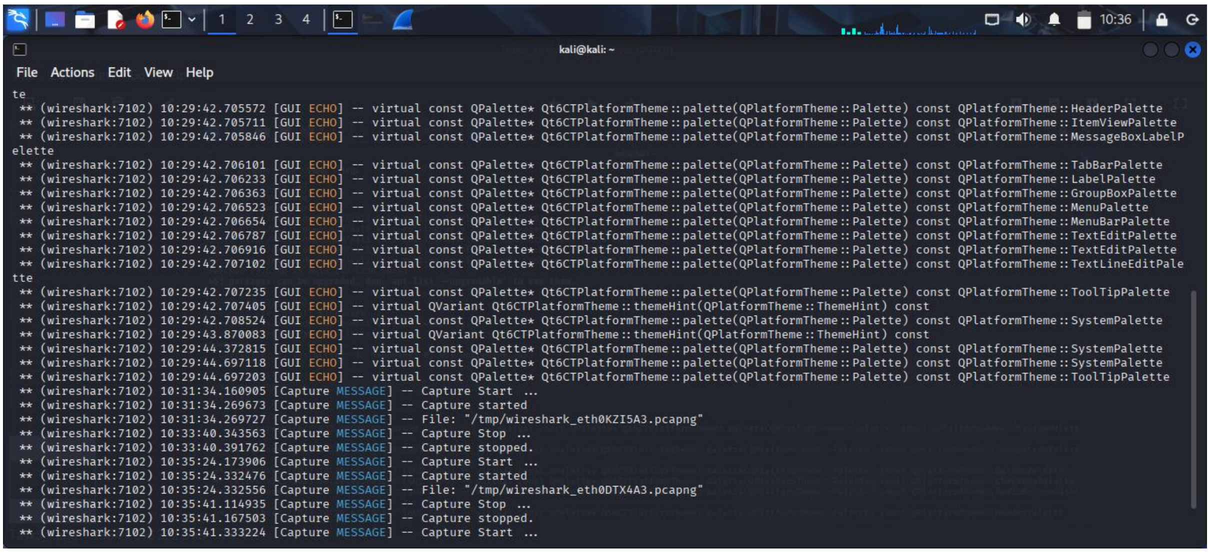
Task 5: Capture and Analyze Network Traffic Using Wireshark

Step 1: Install Wireshark



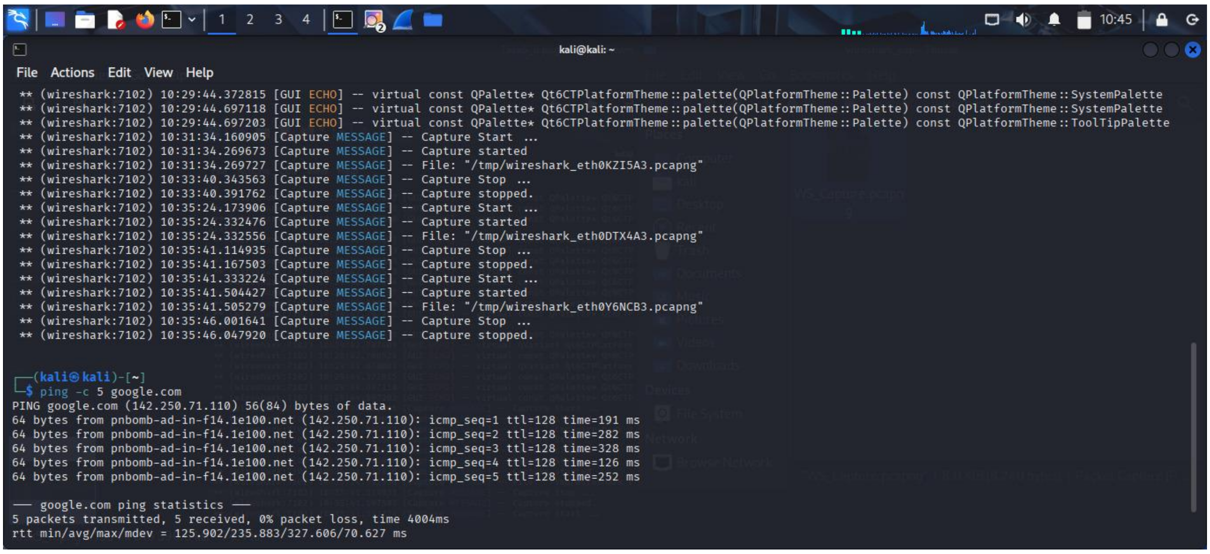
```
┌──(kali㉿kali)-[~]
└─$ sudo apt update
[sudo] password for kali:
Get:1 http://kali.download/kali kali-rolling InRelease [41.5 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [21.0 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [51.4 MB]
Get:4 http://kali.download/kali kali-rolling/non-free amd64 Packages [198 kB]
Get:5 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [911 kB]
Fetched 73.5 MB in 5min 14s (234 kB/s)
453 packages can be upgraded. Run 'apt list --upgradable' to see them.

┌──(kali㉿kali)-[~]
└─$ sudo apt install wireshark -y
wireshark is already the newest version (4.4.7-1).
wireshark set to manually installed.
Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 453

┌──(kali㉿kali)-[~]
└─$ wireshark &
[1] 7102

┌──(kali㉿kali)-[~]
└─$  ** (wireshark:7102) 10:29:42.702636 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::SystemPalett
e
 ** (wireshark:7102) 10:29:42.704892 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::ToolButtonPalett
e
 ** (wireshark:7102) 10:29:42.705137 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::ButtonPalette
 ** (wireshark:7102) 10:29:42.705283 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::CheckBoxPalette
 ** (wireshark:7102) 10:29:42.705407 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::RadioButtonPalet
te
 ** (wireshark:7102) 10:29:42.705572 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::HeaderPalette
```

Step 2: Start capturing on active Network Interface



```
te
 ** (wireshark:7102) 10:29:42.705572 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::HeaderPalette
 ** (wireshark:7102) 10:29:42.705711 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::ItemViewPalette
 ** (wireshark:7102) 10:29:42.705846 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::MessageBoxLabelP
elette
 ** (wireshark:7102) 10:29:42.706101 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::TabBarPalette
 ** (wireshark:7102) 10:29:42.706233 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::LabelPalette
 ** (wireshark:7102) 10:29:42.706363 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::GroupBoxPalette
 ** (wireshark:7102) 10:29:42.706523 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::MenuPalette
 ** (wireshark:7102) 10:29:42.706654 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::MenuBarPalette
 ** (wireshark:7102) 10:29:42.706787 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::TextEditPalette
 ** (wireshark:7102) 10:29:42.706916 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::TextEditPalette
 ** (wireshark:7102) 10:29:42.707102 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::TextLineEditPale
tte
 ** (wireshark:7102) 10:29:42.707235 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::ToolTipPalette
 ** (wireshark:7102) 10:29:42.707405 [GUI ECHO] -- virtual QVariant Qt6CTPlatformTheme::themeHint(QPlatformTheme::ThemeHint) const
 ** (wireshark:7102) 10:29:42.708524 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::SystemPalette
 ** (wireshark:7102) 10:29:43.870083 [GUI ECHO] -- virtual QVariant Qt6CTPlatformTheme::themeHint(QPlatformTheme::ThemeHint) const
 ** (wireshark:7102) 10:29:44.372815 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::SystemPalette
 ** (wireshark:7102) 10:29:44.697118 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::SystemPalette
 ** (wireshark:7102) 10:29:44.697203 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::ToolTipPalette
 ** (wireshark:7102) 10:31:34.160905 [Capture MESSAGE] -- Capture Start ...
 ** (wireshark:7102) 10:31:34.269673 [Capture MESSAGE] -- Capture started
 ** (wireshark:7102) 10:31:34.269727 [Capture MESSAGE] -- File: "/tmp/wireshark_eth0KZI5A3.pcapng"
 ** (wireshark:7102) 10:33:40.343563 [Capture MESSAGE] -- Capture Stop ...
 ** (wireshark:7102) 10:33:40.391762 [Capture MESSAGE] -- Capture stopped.
 ** (wireshark:7102) 10:35:24.173906 [Capture MESSAGE] -- Capture Start ...
 ** (wireshark:7102) 10:35:24.332476 [Capture MESSAGE] -- Capture started
 ** (wireshark:7102) 10:35:24.332556 [Capture MESSAGE] -- File: "/tmp/wireshark_eth0DTX4A3.pcapng"
 ** (wireshark:7102) 10:35:41.114935 [Capture MESSAGE] -- Capture Stop ...
 ** (wireshark:7102) 10:35:41.167503 [Capture MESSAGE] -- Capture stopped.
 ** (wireshark:7102) 10:35:41.333224 [Capture MESSAGE] -- Capture Start ...
```

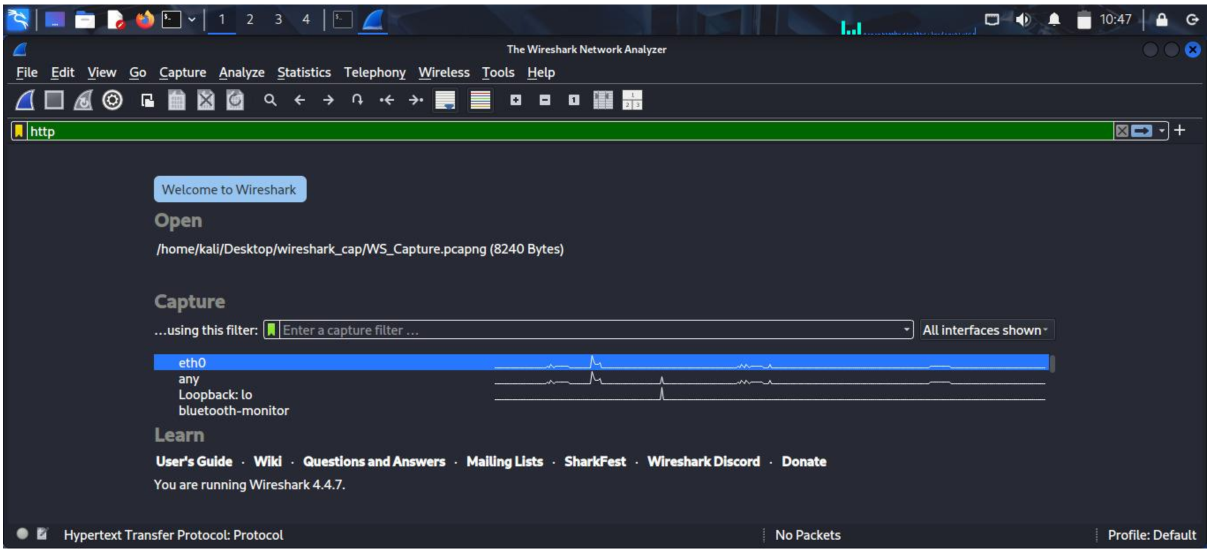
Step 3: Generate Network Traffic



```
** (wireshark:7102) 10:29:44.372815 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::SystemPalette
** (wireshark:7102) 10:29:44.697118 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::SystemPalette
** (wireshark:7102) 10:29:44.697203 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::ToolTipPalette
** (wireshark:7102) 10:31:34.160905 [Capture MESSAGE] -- Capture Start ...
** (wireshark:7102) 10:31:34.269673 [Capture MESSAGE] -- Capture started
** (wireshark:7102) 10:31:34.269727 [Capture MESSAGE] -- File: "/tmp/wireshark_eth0KZI5A3.pcapng"
** (wireshark:7102) 10:33:40.343563 [Capture MESSAGE] -- Capture Stop ...
** (wireshark:7102) 10:33:40.391762 [Capture MESSAGE] -- Capture stopped.
** (wireshark:7102) 10:35:24.173906 [Capture MESSAGE] -- Capture Start ...
** (wireshark:7102) 10:35:24.332476 [Capture MESSAGE] -- Capture started
** (wireshark:7102) 10:35:24.332556 [Capture MESSAGE] -- File: "/tmp/wireshark_eth0DTX4A3.pcapng"
** (wireshark:7102) 10:35:41.114935 [Capture MESSAGE] -- Capture Stop ...
** (wireshark:7102) 10:35:41.167503 [Capture MESSAGE] -- Capture stopped.
** (wireshark:7102) 10:35:41.333224 [Capture MESSAGE] -- Capture Start ...
** (wireshark:7102) 10:35:41.504427 [Capture MESSAGE] -- Capture started
** (wireshark:7102) 10:35:41.505279 [Capture MESSAGE] -- File: "/tmp/wireshark_eth0Y6NCB3.pcapng"
** (wireshark:7102) 10:35:46.001641 [Capture MESSAGE] -- Capture Stop ...
** (wireshark:7102) 10:35:46.047920 [Capture MESSAGE] -- Capture stopped.


┌──(kali㉿kali)-[~]
└─$ ping -c 5 google.com
PING google.com (142.250.71.110) 56(84) bytes of data.
64 bytes from pnbomb-ad-in-f14.1e100.net (142.250.71.110): icmp_seq=1 ttl=128 time=191 ms
64 bytes from pnbomb-ad-in-f14.1e100.net (142.250.71.110): icmp_seq=2 ttl=128 time=282 ms
64 bytes from pnbomb-ad-in-f14.1e100.net (142.250.71.110): icmp_seq=3 ttl=128 time=328 ms
64 bytes from pnbomb-ad-in-f14.1e100.net (142.250.71.110): icmp_seq=4 ttl=128 time=126 ms
64 bytes from pnbomb-ad-in-f14.1e100.net (142.250.71.110): icmp_seq=5 ttl=128 time=252 ms

--- google.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4004ms
rtt min/avg/max/mdev = 125.902/235.883/327.606/70.627 ms
```

Step 4: Filter capture packets by protocol

HTTP, DNS, TCP



The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
10:47
Welcome to Wireshark

Display filter: http

Open

/home/kali/Desktop/wireshark_cap/WS_Capture.pcapng (8240 Bytes)

Capture

...using this filter: Enter a capture filter ... All interfaces shown

eth0
any
Loopback: lo
bluetooth-monitor

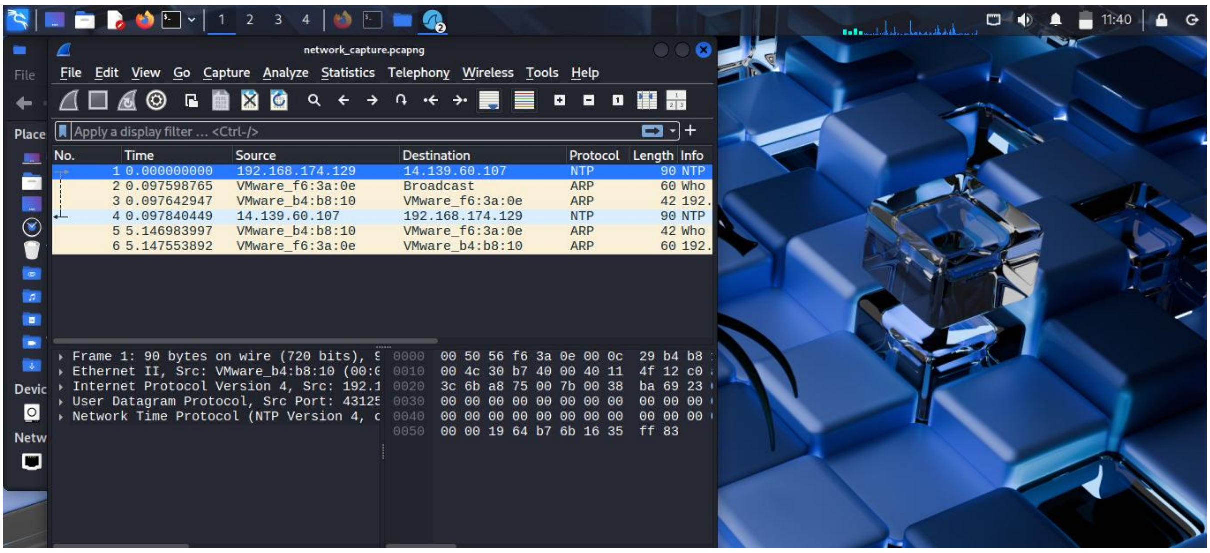
Learn

User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate

You are running Wireshark 4.4.7.

Hypertext Transfer Protocol: Protocol | No Packets | Profile: Default

Step 5: Export capture as .pcap file



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.174.129	14.139.60.107	NTP	90	NTP
2	0.097598765	VMware_f6:3a:0e	Broadcast	ARP	60	Who
3	0.097642947	VMware_b4:b8:10	VMware_f6:3a:0e	ARP	42	192.
4	0.097840449	14.139.60.107	192.168.174.129	NTP	90	NTP
5	5.146983997	VMware_b4:b8:10	VMware_f6:3a:0e	ARP	42	Who
6	5.147553892	VMware_f6:3a:0e	VMware_b4:b8:10	ARP	60	192.

```
› Frame 1: 90 bytes on wire (720 bits), 9
› Ethernet II, Src: VMware_b4:b8:10 (00:0
› Internet Protocol Version 4, Src: 192.1
› User Datagram Protocol, Src Port: 43125
› Network Time Protocol (NTP Version 4, c
```

```
0000  00 50 56 f6 3a 0e 00 0c  29 b4 b8
0010  00 4c 30 b7 40 00 40 11  4f 12 c0
0020  3c 6b a8 75 00 7b 00 38  ba 69 23
0030  00 00 00 00 00 00 00 00  00 00 00
0040  00 00 00 00 00 00 00 00  00 00 00
0050  00 00 19 64 b7 6b 16 35  ff 83
```

Summary:

-Total Packets Captured: 532

-Protocols Identified: TCP, DNS, HTTP

-Packet Details:

-DNS requests to resolve google.com

-TCP handshakes between your system and remote servers

-HTTP GET request to example.com and corresponding HTTP 200 OK response