Task-5

Date: 29-09-2025

Task 5: Capture and Analyze Network Traffic Using Wireshark.

Objective: Capture live network packets and identify basic protocols and traffic types.

Tools Used: Wireshark

What is Wireshark?

It's like a CCTV camera for your network – it watches all the data (packets) going in and out of your computer or network, and shows you what's happening behind the scenes.

What we can see in Wireshark:

- See which devices are talking to each other.
- Check what kind of data is being sent (web, email, video, etc.).
- Troubleshoot network problems.
- Learn how network protocols work.

Steps to capture packets in Wireshark:

Step1: Install Wireshark

Step2: Open terminal and enter Wireshark to open Wireshark GUI application

Step3: Click on start capturing button on top-left

Step4: Now browse a website or ping a server to generate traffic

Step5: Stop capture after a minute. (located at top-left)

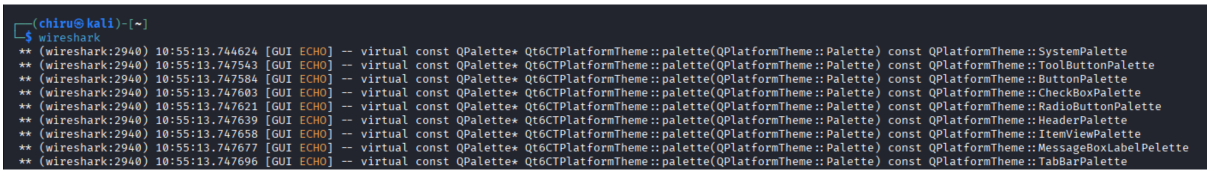
Step6: Filter captured packets by protocol (e.g., HTTP, DNS, TCP)

Step7: Identify at least 3 different protocols in the capture.

(To identify the protocols, click CTRL+F to find the protocol name)

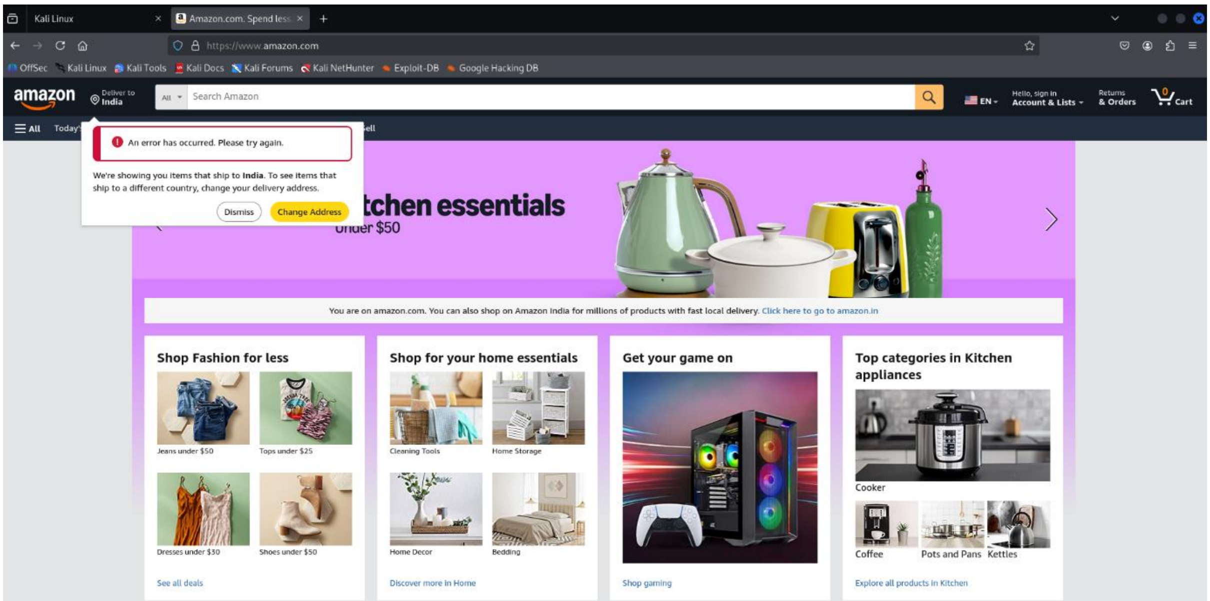
Step8: Export the capture as a .pcap file.

To open Wireshark:



```
┌──(chiru㉿kali)-[~]
└─$ wireshark
** (wireshark:2940) 10:55:13.744624 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::SystemPalette
** (wireshark:2940) 10:55:13.747543 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::ToolButtonPalette
** (wireshark:2940) 10:55:13.747584 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::ButtonPalette
** (wireshark:2940) 10:55:13.747603 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::CheckBoxPalette
** (wireshark:2940) 10:55:13.747621 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::RadioButtonPalette
** (wireshark:2940) 10:55:13.747639 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::HeaderPalette
** (wireshark:2940) 10:55:13.747658 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::ItemViewPalette
** (wireshark:2940) 10:55:13.747677 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::MessageBoxLabelPelette
** (wireshark:2940) 10:55:13.747696 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::TabBarPalette
```

To capture the packets in Wireshark open any browser and search any website:



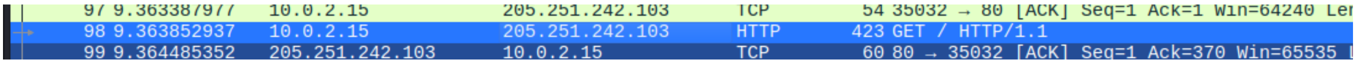
https://www.amazon.com

An error has occurred. Please try again.

We're showing you items that ship to **India**. To see items that ship to a different country, change your delivery address.

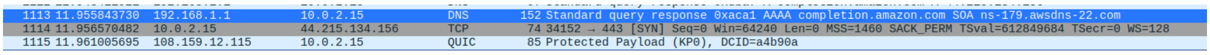
You are on amazon.com. You can also shop on Amazon India for millions of products with fast local delivery. Click here to go to amazon.in

HTTP Packet:



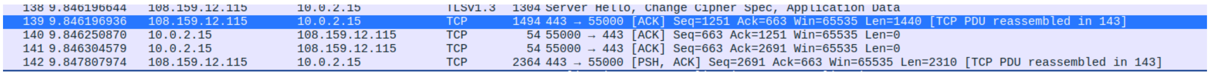
```
 97 9.363387977   10.0.2.15         205.251.242.103   TCP      54 35032 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len
 98 9.363852937   10.0.2.15         205.251.242.103   HTTP    423 GET / HTTP/1.1
 99 9.364485352   205.251.242.103   10.0.2.15         TCP      60 80 → 35032 [ACK] Seq=1 Ack=370 Win=65535 L
```

DNS Packet:



```
1113 11.955843730  192.168.1.1     10.0.2.15        DNS   152 Standard query response 0xaca1 AAAA completion.amazon.com SOA ns-179.awsdns-22.com
1114 11.956570482  10.0.2.15       44.215.134.156   TCP    74 34152 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=612849684 TSecr=0 WS=128
1115 11.961005695  108.159.12.115  10.0.2.15        QUIC   85 Protected Payload (KP0), DCID=a4b90a
```

TCP Packet:



```
138 9.846196644   108.159.12.115    10.0.2.15         TLSv1.3  1304 Server Hello, Change Cipher Spec, Application Data
139 9.846196936   108.159.12.115    10.0.2.15         TCP      1494 443 → 55000 [ACK] Seq=1251 Ack=663 Win=65535 Len=1440 [TCP PDU reassembled in 143]
140 9.846250870   10.0.2.15         108.159.12.115    TCP        54 55000 → 443 [ACK] Seq=663 Ack=1251 Win=65535 Len=0
141 9.846304579   10.0.2.15         108.159.12.115    TCP        54 55000 → 443 [ACK] Seq=663 Ack=2691 Win=65535 Len=0
142 9.847807974   108.159.12.115    10.0.2.15         TCP      2364 443 → 55000 [PSH, ACK] Seq=2691 Ack=663 Win=65535 Len=2310 [TCP PDU reassembled in 143]
```

So we can see in HTTP Packet it was connect to ip address: 205.251.242.103 default ip address of amazon.com