

Capture and Analyze Network Traffic Using Wireshark

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

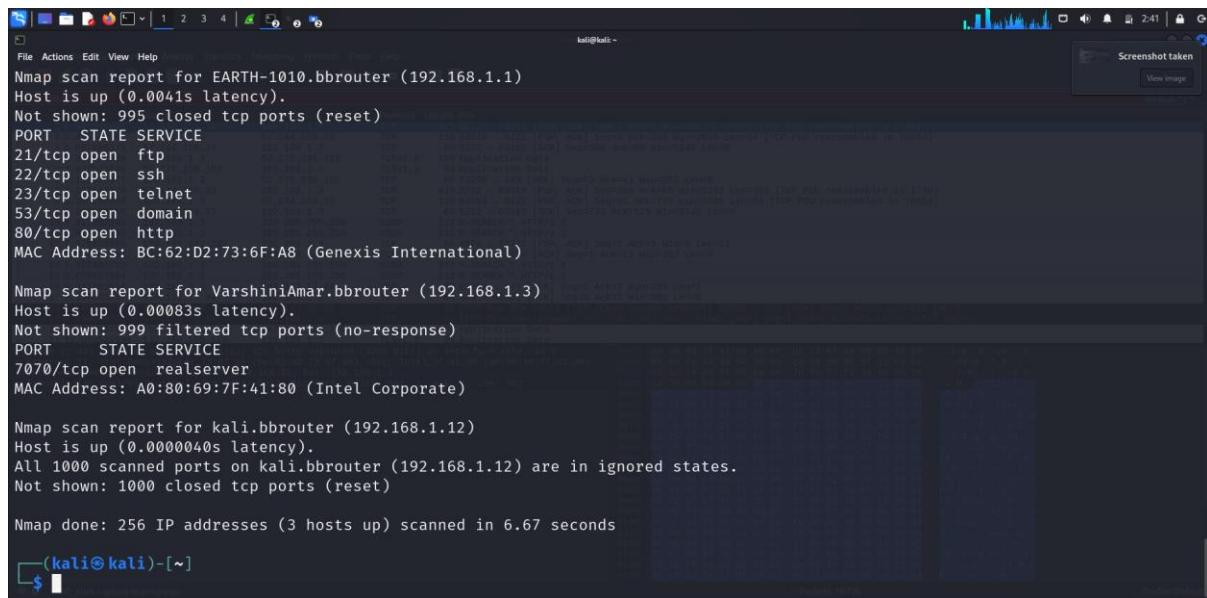
Tools: Wireshark

Deliverables: A packet capture (.pcap) file and a short report of protocols identified

STEP 01 - Install Wireshark

I have used **kali linux** for (wireshark)

STEP 02 - Start capturing on your active network interface

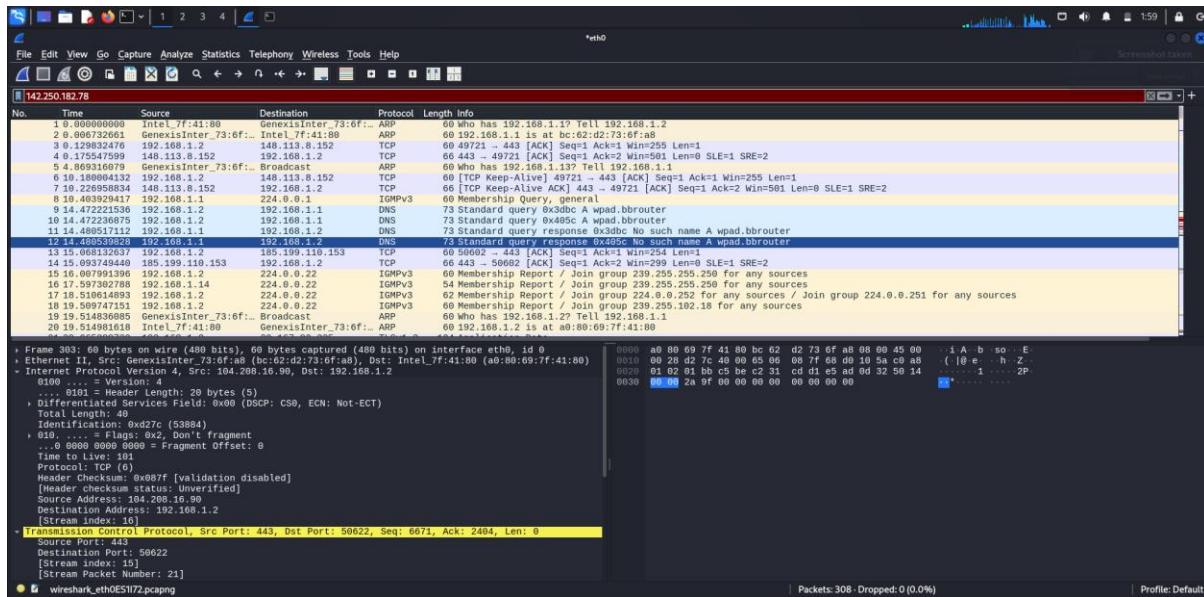


```
Nmap scan report for EARTH-1010.bbrouter (192.168.1.1)
Host is up (0.004s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
53/tcp    open  domain
80/tcp    open  http
MAC Address: BC:62:D2:73:6F:A8 (Genexis International)

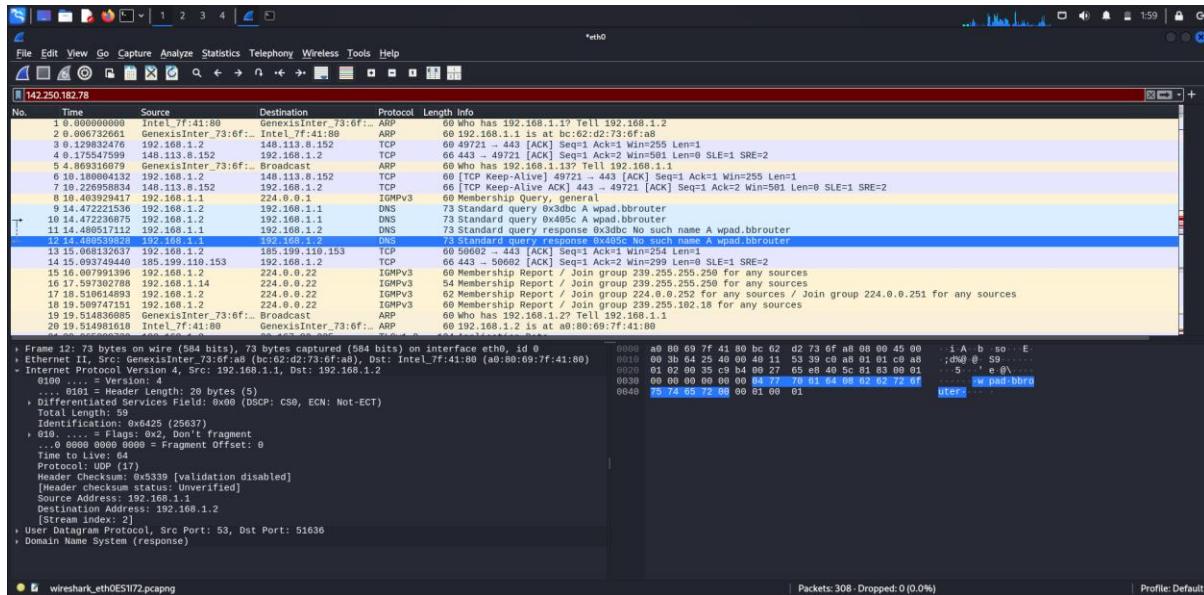
Nmap scan report for VarshiniAmar.bbrouter (192.168.1.3)
Host is up (0.00083s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE
7070/tcp  open  realserver
MAC Address: A0:80:69:7F:41:80 (Intel Corporate)

Nmap scan report for kali.bbrouter (192.168.1.12)
Host is up (0.0000040s latency).
All 1000 scanned ports on kali.bbrouter (192.168.1.12) are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (3 hosts up) scanned in 6.67 seconds
```

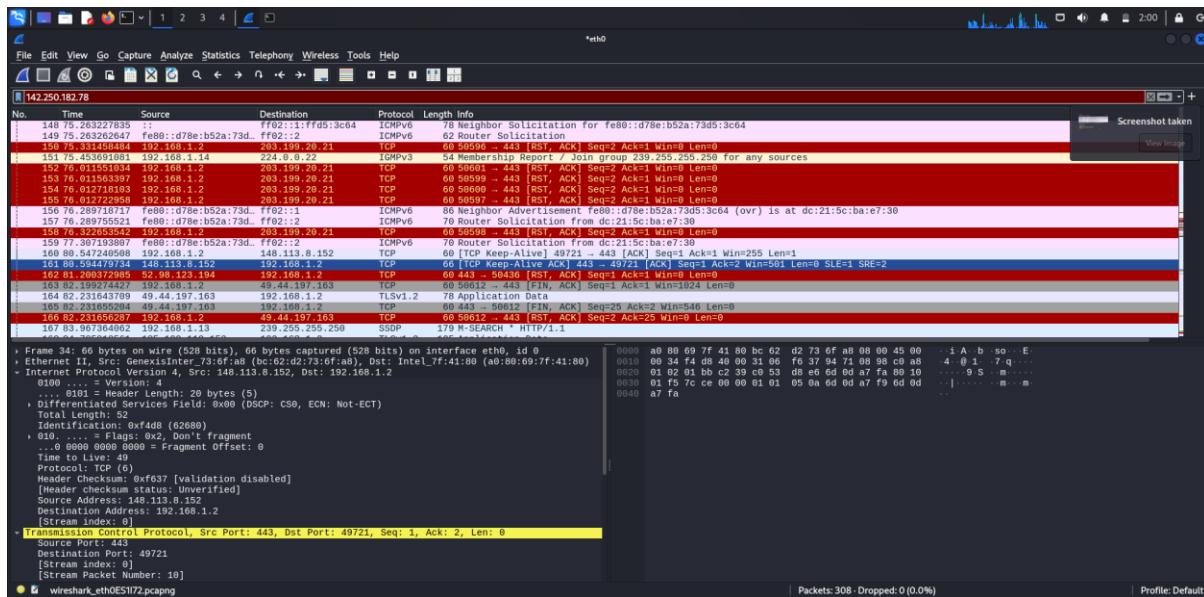
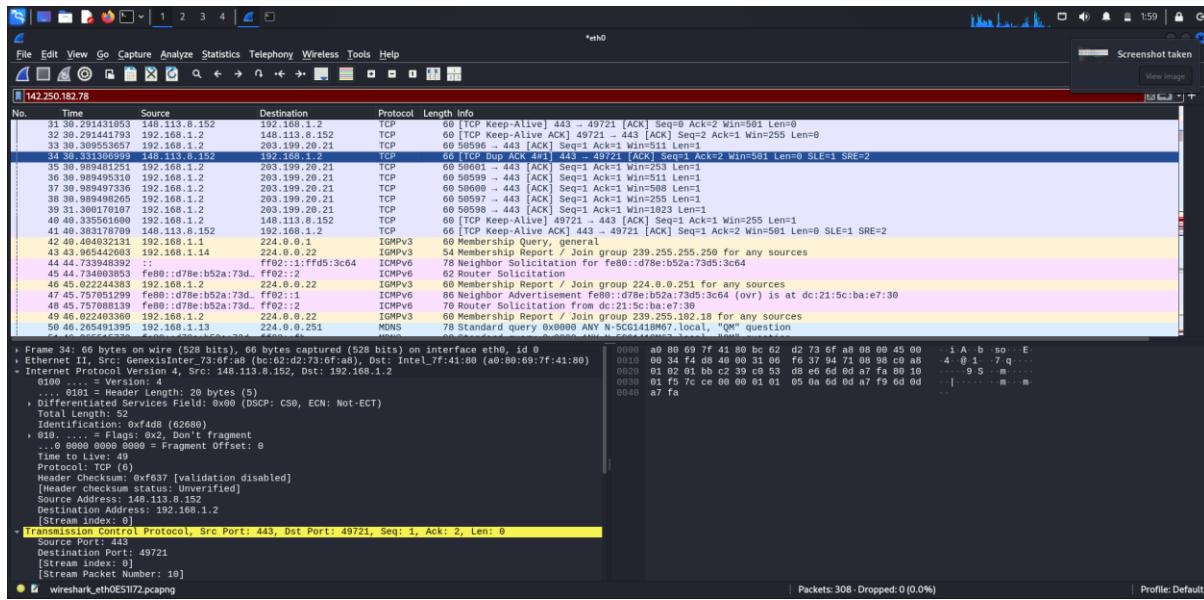


STEP 03 - Browse a website or ping a server to generate traffic

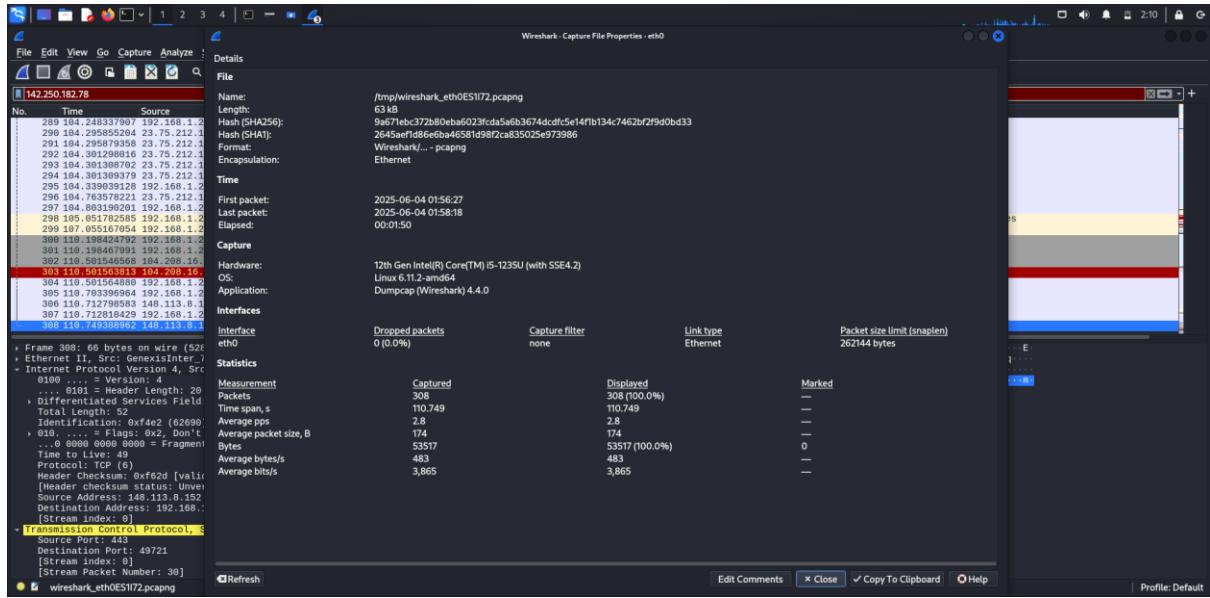


PING google.com

STEP 04 - Filter captured packets by protocol (e.g., HTTP, DNS, TCP)



STEP 05 - Export the capture as a .pcap file.



STEP 06 - Summarize your findings and packet details.

Wireshark Packet Capture Summary Report

File Name: wireshark_eth0E5172.pcapng

Capture Date: 2025-06-04

Duration: 50.51seconds

Interface: eth0(Ethernet)

System Hardware: 12th Gen Intel(R) Core(TM) i5-1235U

Packet Size Limit: 262,144 bytes

Capture Software: Dumpcap (Wireshark) 4.0.4

Capture Statistics

- Total Packets Captured:** 308
- Displayed Packets:** 308 (100%)
- Dropped Packets:** 0

- **Average Packet Size:** 174 bytes
- **Total Data Captured:** 53,517 bytes
- **Average Bandwidth:** 8,865 bits/sec

Protocols Identified in the Capture

1. TCP (Transmission Control Protocol)

- **Observed in Packet #308**
- **Source IP:** 142.250.180.78
- **Source Port:** 443 (HTTPS)
- **Destination Port:** 49721
- **Stream index:** 1
- Used for encrypted web communication (HTTPS).

2. TLS (Transport Layer Security)

- TLS traffic is likely seen in the stream from port 443.
- TLS secures HTTP traffic, indicating secure browsing or access to websites like Google.

3. HTTP/2 or HTTPS (Encrypted)

- The port and flow suggest the usage of encrypted web communication with Google servers.
- The detailed protocol may be seen as **TLS**, **QUIC**, or **HTTP2** if expanded in packet details.

Key Insights

- Device communicated with 142.250.180.78 — an IP address belonging to **Google**.
- All 308 packets were successfully captured and displayed with no packet loss.
- The network interface used was Ethernet (eth0) with a high capture size limit (good for deep inspection).
- The presence of TCP over port 443 strongly indicates encrypted HTTPS traffic.
- The capture shows only a **single stream (Stream index: 1)** — possibly one secure browsing session or ping interaction with Google servers.

Outcome:

- Successfully captured a live network session.
- Identified key Internet protocols: **TCP**, **TLS**, and likely **HTTPS**.
- Analyzed communication between your local system and an external IP (Google).
- Gained hands-on experience in using Wireshark for basic protocol analysis.