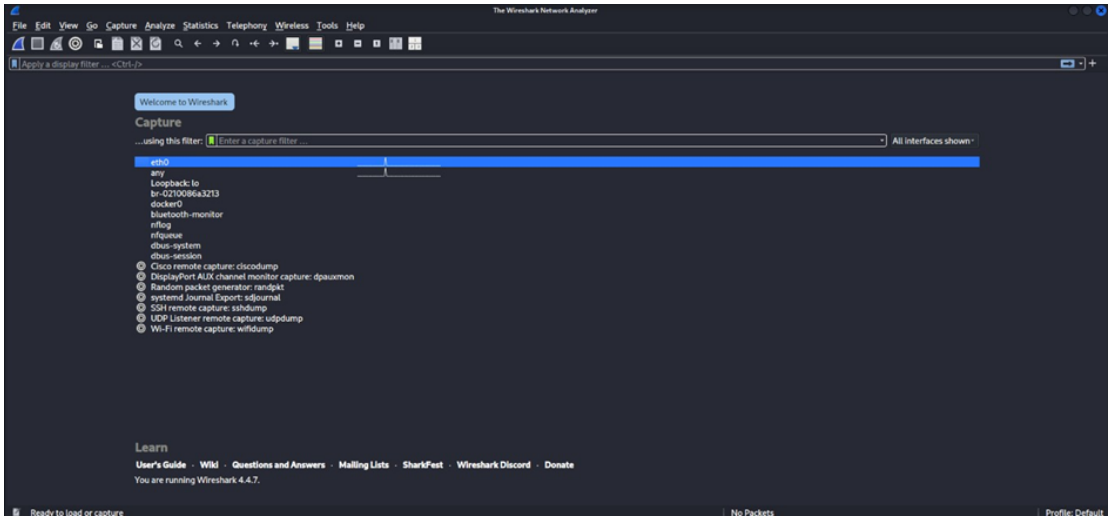
Task 3: Networking Basics for Cyber Security

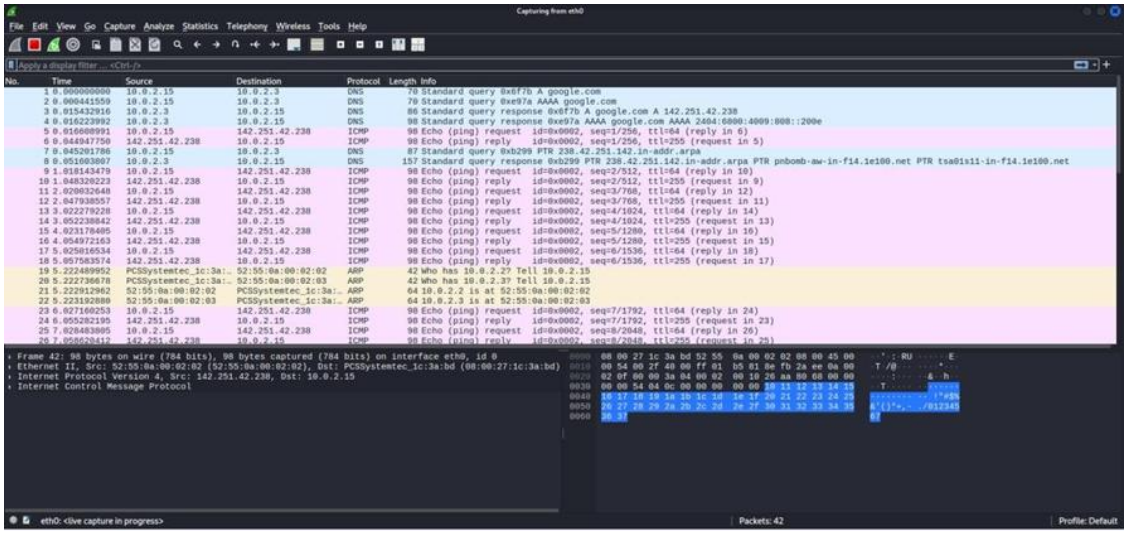
Wireshark is a free and open-source network protocol analyzer used for capturing and analyzing network traffic in real time. It helps users see what's happening on their network at a very granular level, making it an essential tool for network troubleshooting, security analysis, protocol development, and education.

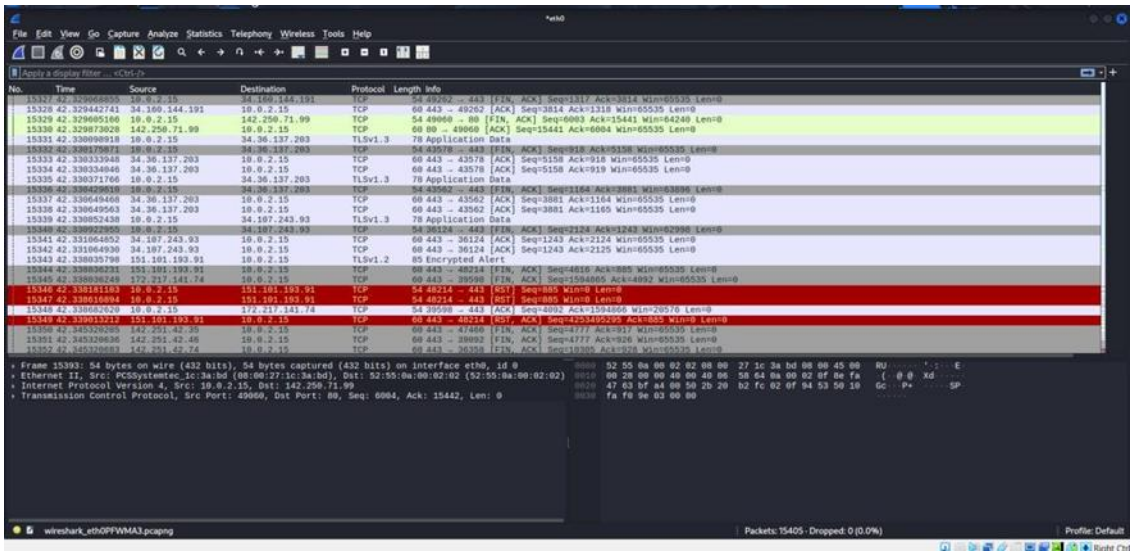
- Launch Wireshark as Administrator/root.
- Select a network interface (e.g., eth0, wlan0).
- Go to Capture Options.
- Enable Promiscuous Mode and start the capture:
  - Observe that you can see all network packets, even those not addressed to your machine.
- Stop capture.
- Now disable Promiscuous Mode and start capture again.
  - You will now see only packets addressed to your machine (mostly ARP, DNS, TCP/UDP for your IP).
- Compare both captures to observe the difference.

sudo Wireshark:

Wireshark home screen showing network interfaces.



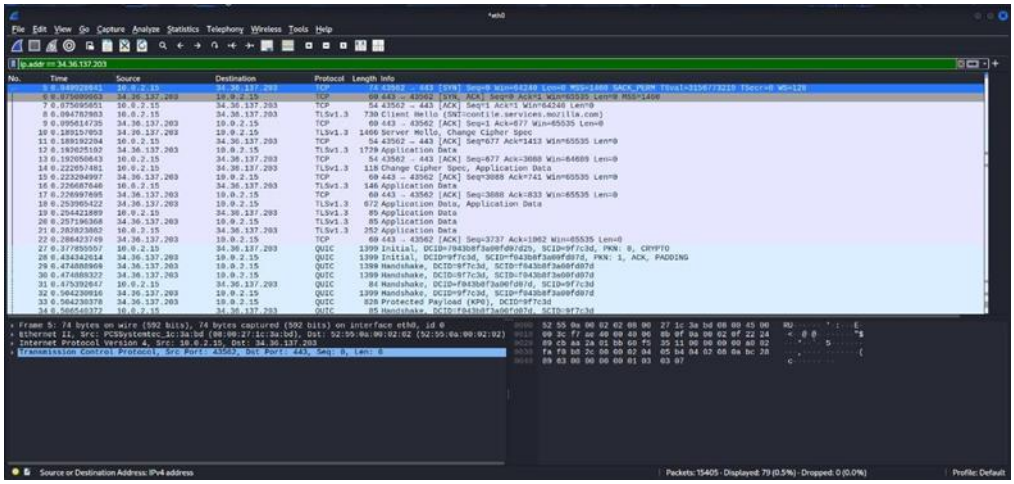




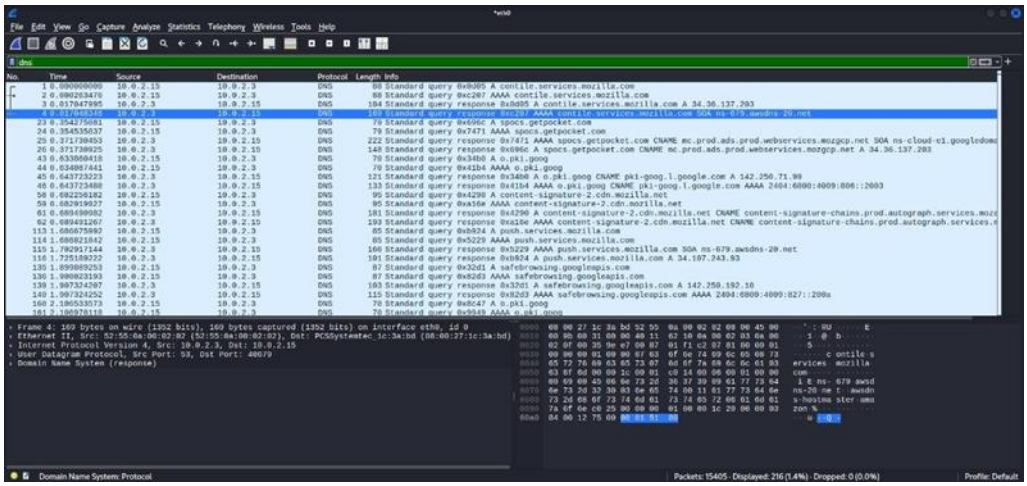
Packets can be traced based on different filters.

1. Start a new capture.
2. Apply different display filters in Wireshark:
    - ip.addr == 34.36.137.203 → Shows packets from/to a specific IP.
    - tcp.port == 80 → Captures HTTP traffic.
    - udp → Captures only UDP packets.
    - http.request.method == "GET" → Shows HTTP GET requests.
    - dns → Filters DNS query packets.
3. Analyze the packets based on protocol, source/destination, length, info.
4. Optionally, save captured data as .pcap file for later analysis.

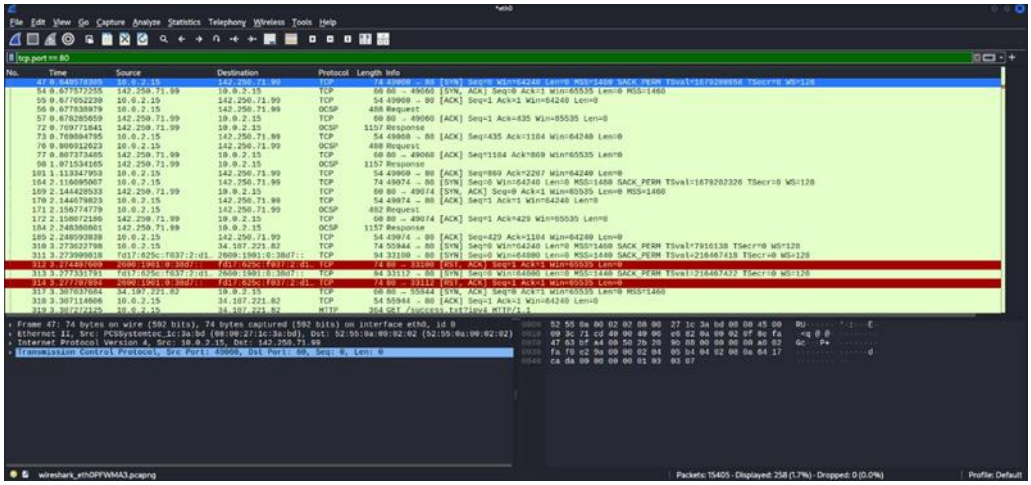
- **ip.addr == 34.36.137.203**



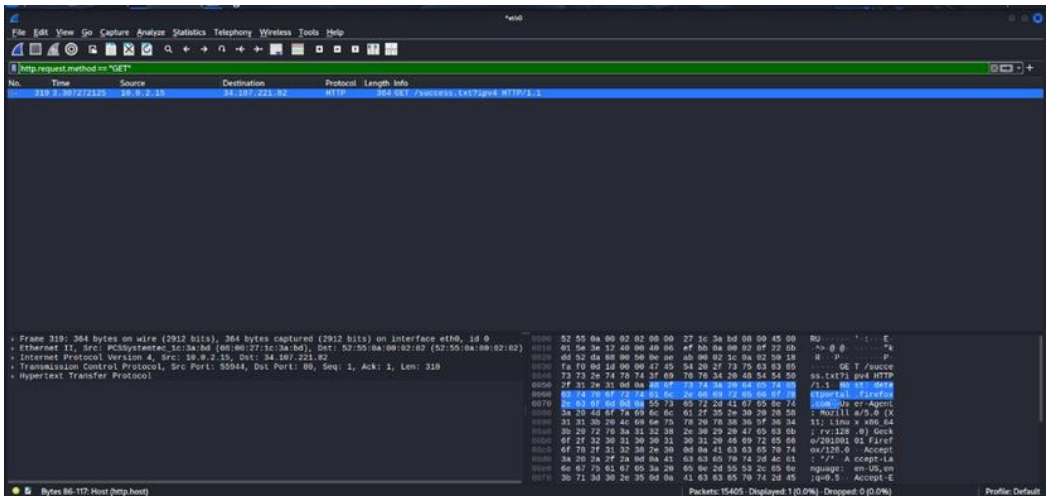
- **Dns**



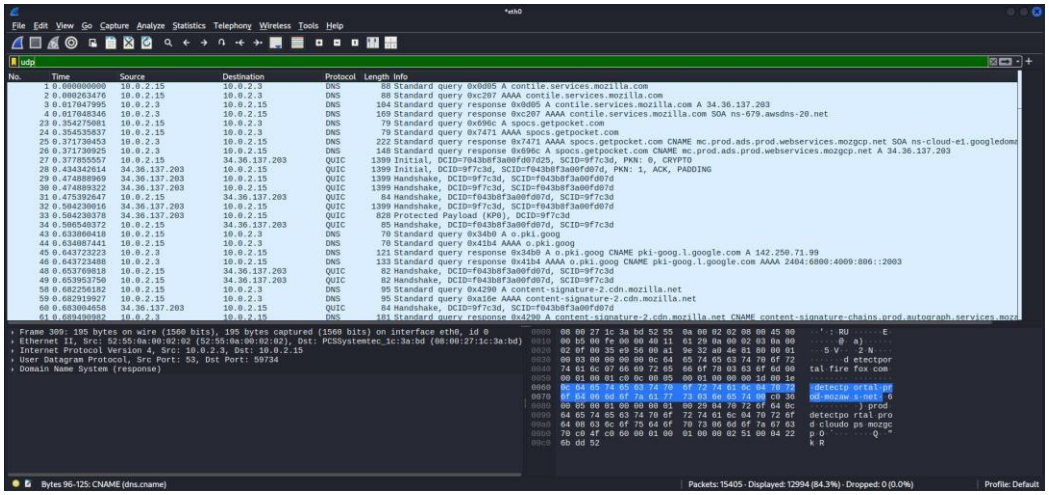
- **tcp.port == 80**



- **http.request.method == "GET"**



- **Udp**



- **tcp.flags.syn == 1**