Cyber Security Internship – Task 5 Report

Task Title: Capture and Analyze Network Traffic Using Wireshark
Name: *Gitika Khira*
Date: *11-08-2025*

---

1. Objective

The objective of this task is to:

- Capture live network packets using Wireshark.
- Identify at least three different protocols.
- Analyze packet details and understand protocol interactions.

---

2. Tools & Environment

- **Software:** Wireshark (latest version)
- **Operating System:** *Linux*
- **Network Interface:** *Ethernet (eth0)*

---

3. Procedure

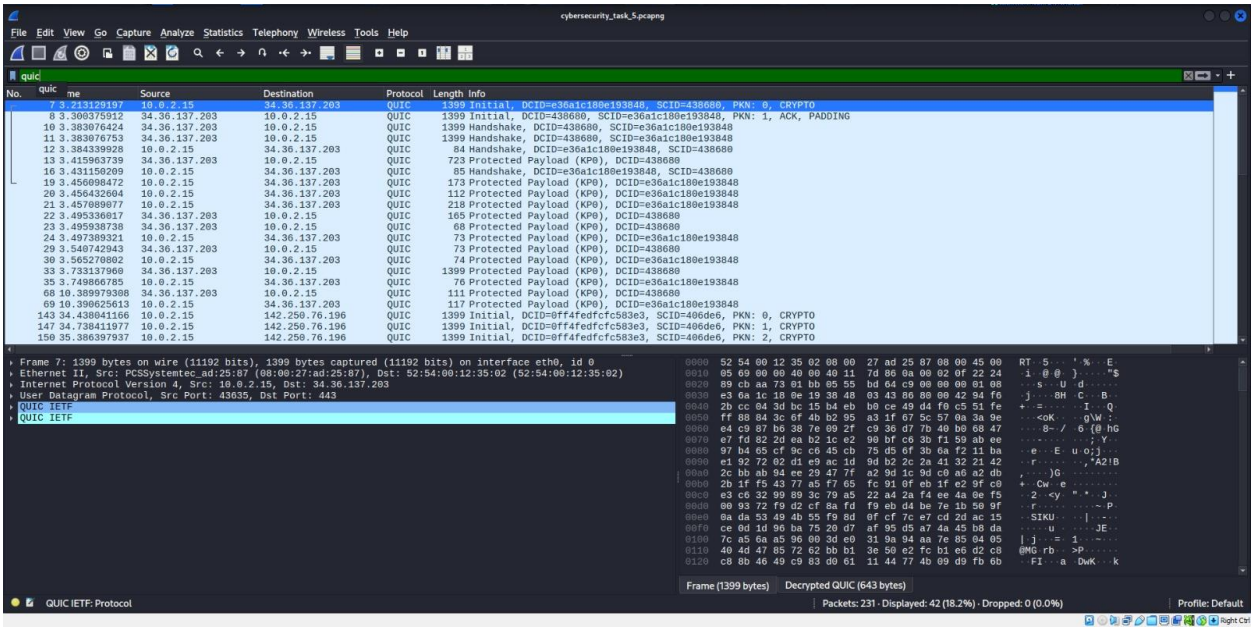
3.1 Installation

- Wireshark came pre-installed with Kali-Linux, so no installation was required.

3.2 Packet Capture

- Selected the active network interface [Etherner(eth0)].
- Started live capture.
- Generated network traffic by:
  - Visiting websites in the browser.
  - Pinging `google.com` from terminal/command prompt.
- Stopped the capture after ~1 minute.

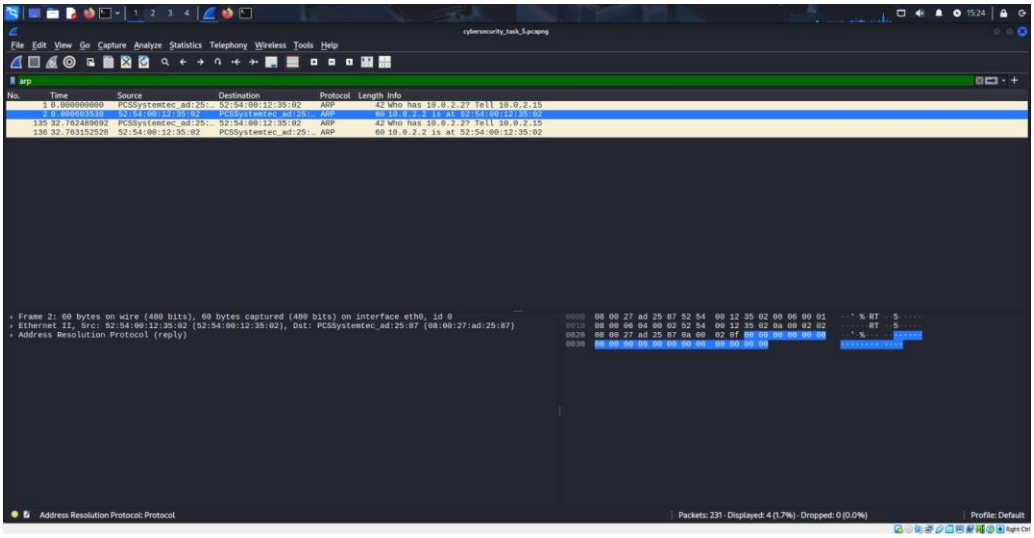
📷 Screenshot 1:



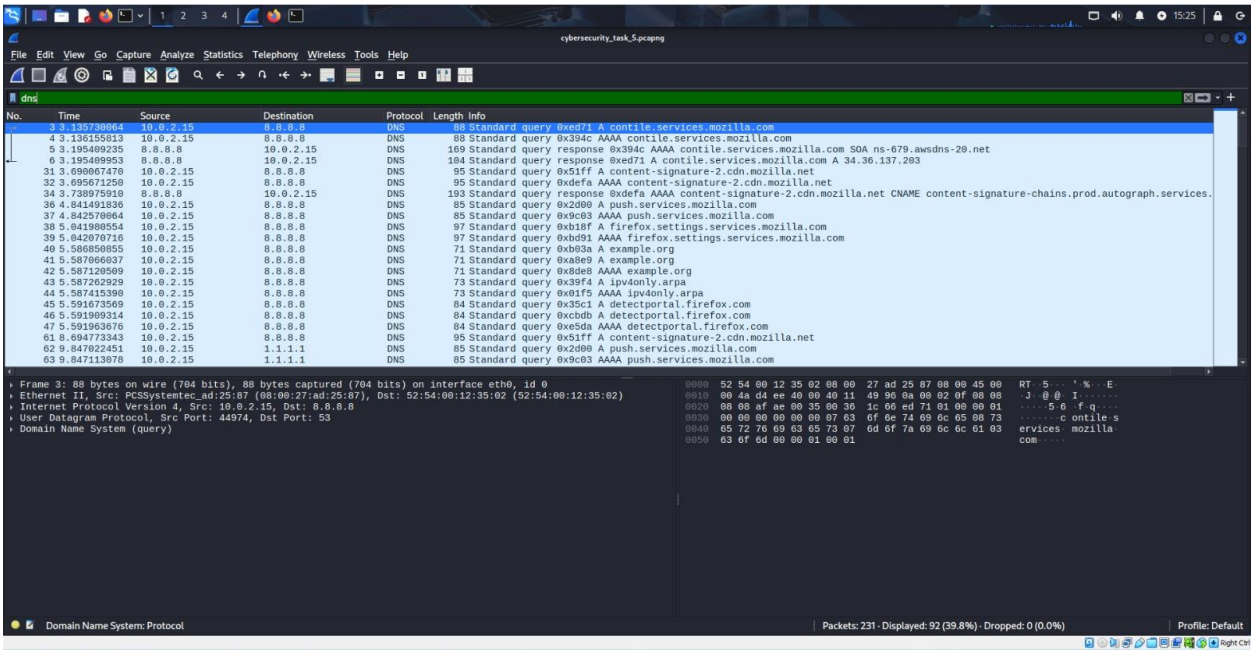
3.3 Filtering and Analysis

- Applied protocol filters:
  - QUIC → `quic`
  - DNS → `dns`
  - ARP → `arp`
- Checked source/destination IPs, ports, and packet info.

📷 Screenshot 2:



📸 Screenshot 3:



3.4 Exporting Data

- Saved the captured traffic as `cybersecurity_task_5.pcapng`.

---

4. Observations

Protocol	Purpose	Example Observation
QUIC	Multiplexed transport over UDP, used for HTTP/3	QUIC Initial and Handshake packets exchanged between 10.0.2.15 and 34.36.137.203
ARP	Maps IP addresses to MAC addresses	Reply: 10.0.2.2 is at 52:54:00:12:35:02
DNS	Resolves domain names to IP addresses	Query for example.org sent to 8.8.8.8

Additional Notes:

- QUIC traffic was encrypted, so only handshake and packet metadata were visible, not the actual payload.
- ARP packets were exchanged within the local network before any communication with external servers.
- DNS queries preceded QUIC traffic, indicating that domain name resolution happens before establishing encrypted connections.

---

5. Conclusion

This task provided practical exposure to packet capturing and protocol analysis.
I successfully identified DNS, HTTP, and TCP protocols, and understood their sequence in typical web communication.

---

6. Deliverables

- **Packet Capture File:** `task5_capture.pcap`
- **GitHub Repository:** *https://github.com/gitikakhira69/CyberSecurity_Task_5.git*