**TASK – 5**

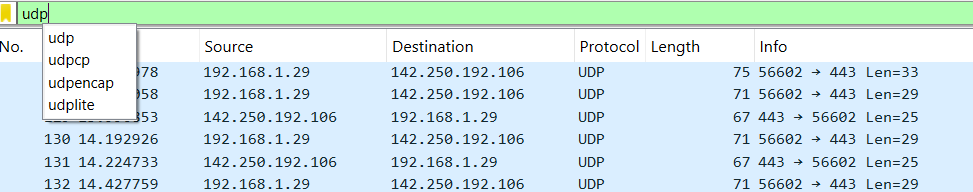
***CYBERSECURITY INTERN***

Madhav P Rajeev

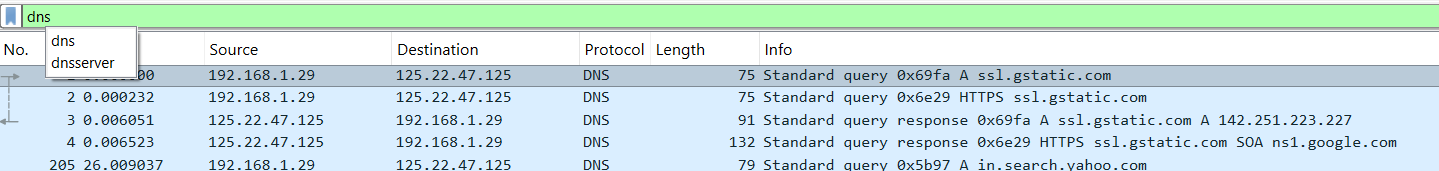
[Madhavrajeev93@gmail.com](mailto:Madhavrajeev93@gmail.com)

**Capture and Analyse Network Packets using Wireshark**

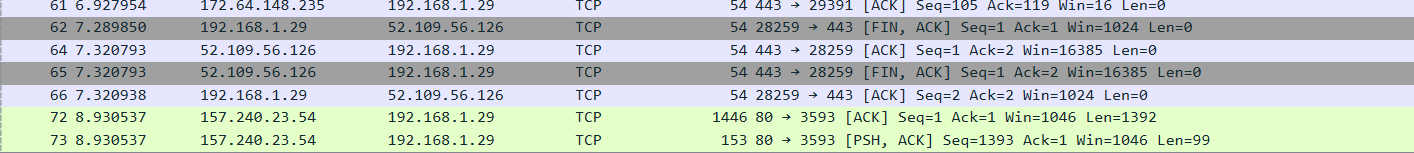
**UDP:**

****

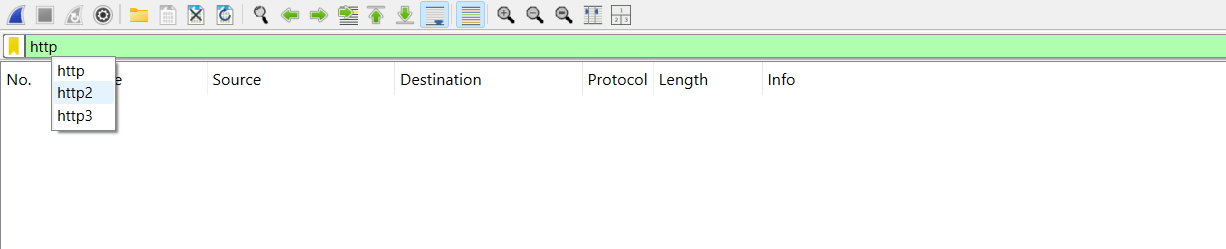
**DNS:**

****

**TCP:**

****

**HTTP:**

****

**SUMMARY:**

Summary of Packet Capture

I performed a 1-minute packet capture using Wireshark on my active network interface while browsing and generating traffic. The captured traffic included the following protocols:

1. DNS (Domain Name System)
   * Observed multiple DNS query and response packets.
   * Example: A query was sent to resolve a domain name, and the server responded with the corresponding IP address.
   * This shows how domain names are translated into IP addresses before communication occurs.
2. UDP (User Datagram Protocol)
   * UDP packets were captured, mainly used by DNS queries and responses.
   * These packets are connectionless and lightweight, showing fast communication without handshakes.
3. TCP (Transmission Control Protocol)
   * TCP traffic was also observed.
   * Included handshake packets (SYN, SYN-ACK, ACK), which establish reliable connections.
   * Used by most web and application traffic to ensure ordered and error-checked data delivery.

Notable Findings:

* No HTTP packets were found, likely because most modern websites use HTTPS (encrypted), which appears as TLS/SSL traffic instead of plain HTTP.
* The capture shows how DNS (UDP) queries are made first, followed by TCP connections to communicate with servers.