National Forensic Sciences University
Knowledge | Wisdom | Fulfilment
An Institution of National Importance
(Ministry of Home Affairs, Government of India)

Mathematical and Computational Foundation for Artificial Intelligence

TA 2 Assignment

College Name: National Forensic Sciences University, Gandhinagar

Subject Code: CTMTAIDS SI P1

Subject Name: Mathematical and Computational Foundation for Artificial Intelligence

Course: M.Tech. Artificial Intelligence and Data Science
(Specialization in Cyber Security)

Session: 2024-25

Semester: 1st Sem

Topic: Mean, Variance, Moment, Covariance and Correlation

Submitted To:-

Dr. Vijeta Khare

Submitted By:-

Pratham Badge
(240103007003)

Step-by-Step Practical

Materials Required:

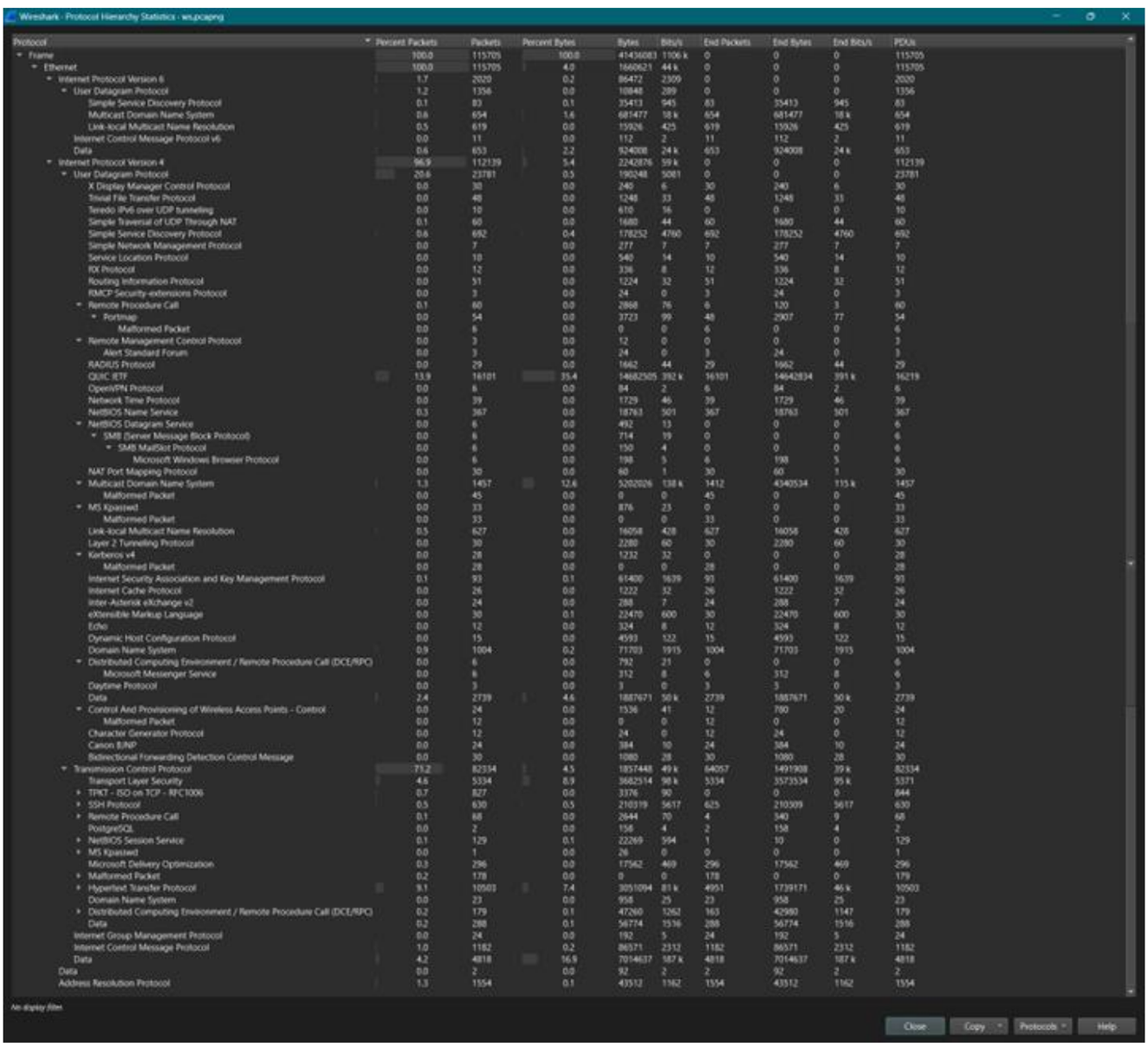
- **Wireshark** installed on student machines
- Pre-captured PCAP file
- Internet access

Step 1: Analysis Tasks

Students should complete the following **tasks** by using Wireshark's filtering tools, statistical reports, and packet details.

Task 1: Identify Basic Traffic Information

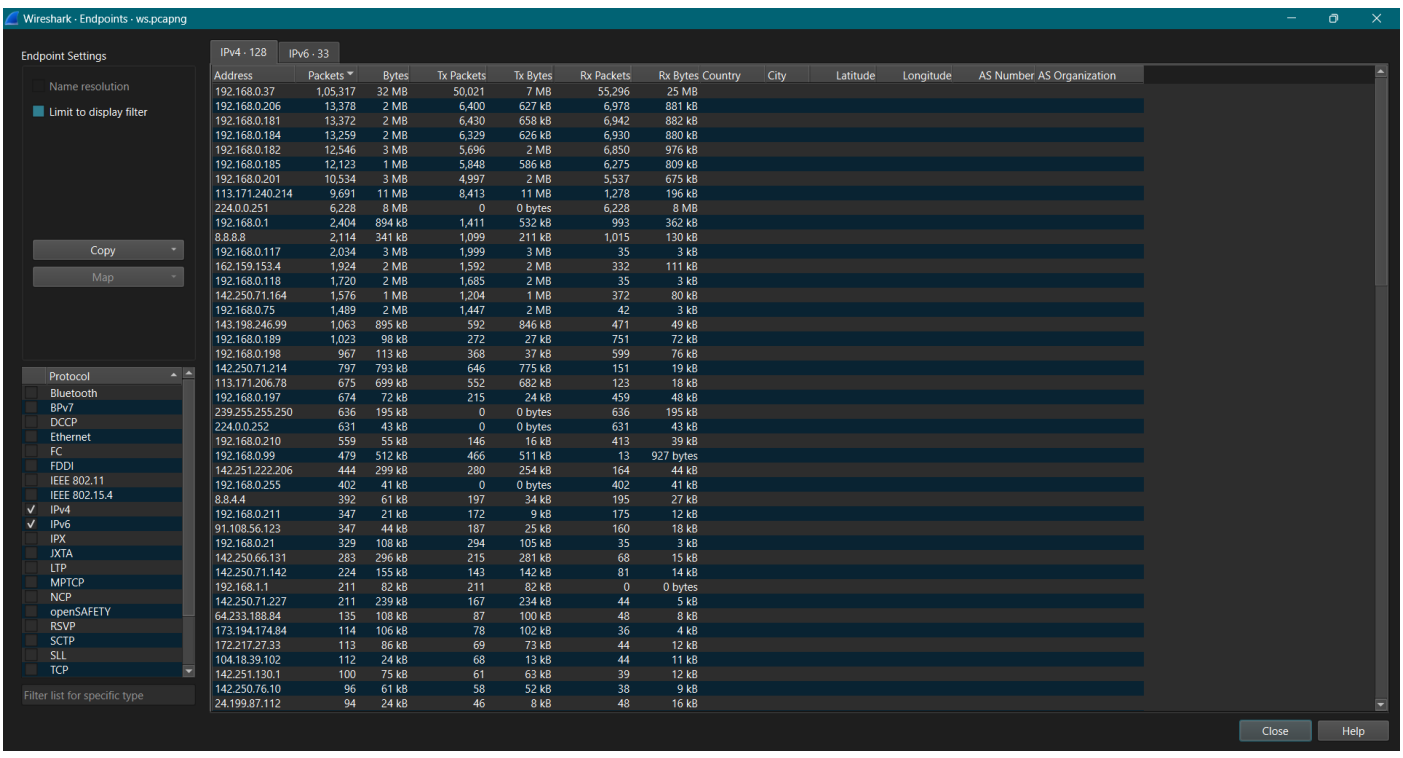
- **Protocol Breakdown**: What protocols are being used in this capture?
- **Ans)** nbdgm,remact,classicstun,rip,_ws.malformed,cotp,kpasswd,amf,tls,nat-pmp,mailslot,portmap,pgsql,asf,data,chargen,bfd,messenger,frame,icp,quic,radius,samr,xml,tftp,teredo,eth,ipv6,rmcp,isystemactivator,xdmcp,mdns,capwap,udp,echo,smb,icmp,smb2,arp,snmp,msdo,igmp,rpc,dcerpc,daytime,_ws.unreassembled,bjnp,llmnr,tpkt,dhcp,srvloc,rsp,krb4,openvpn,dns,ocsp,l2tp,rx,rdp,nbns,nbss,data-text lines, iax2, http, ssdp, ip, ntp, icmpv6, isakmp, urlencoded-form, ssh ,tcp, t125, browser
- **Steps:**
  i) Open Wireshark, open the captured file
  ii) In Menu bar, Statistics > Protocol Hierarchy

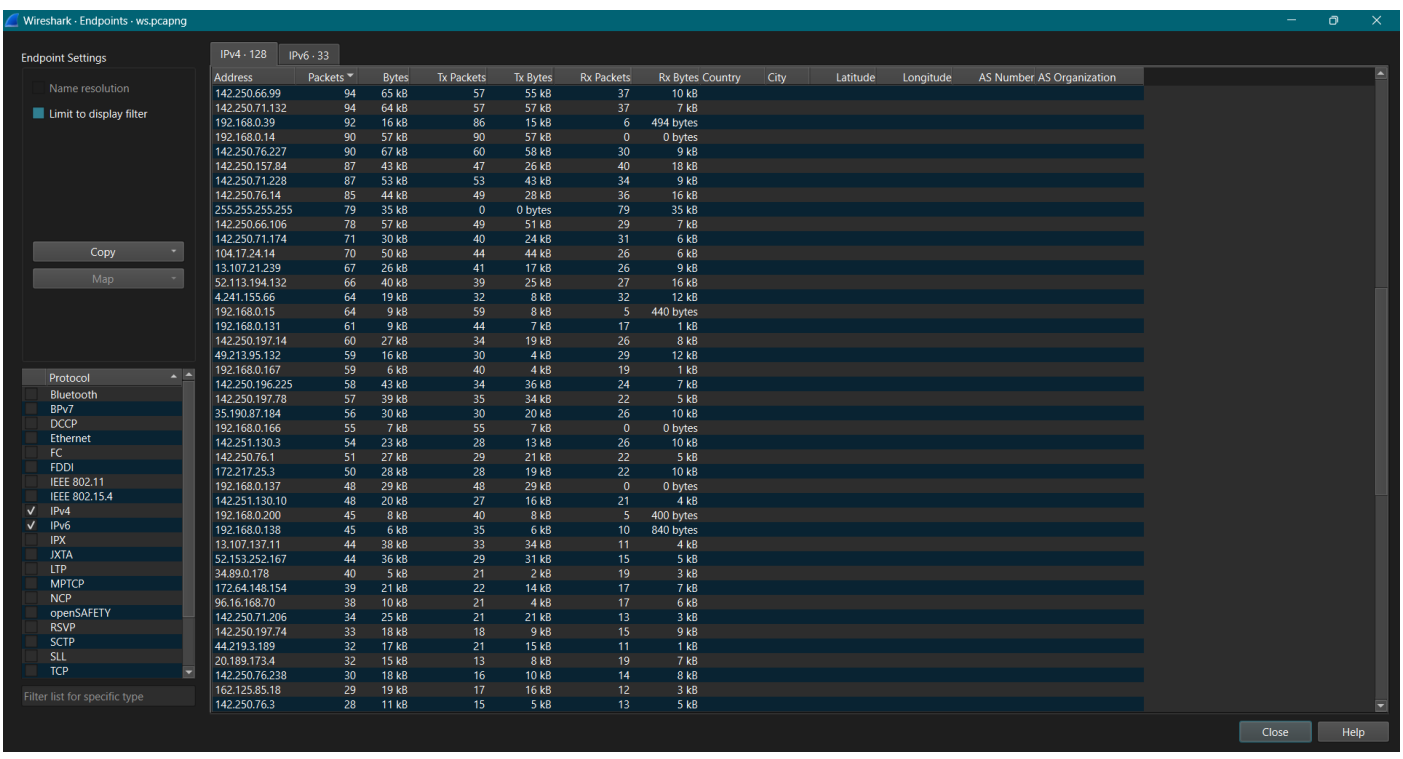


- **Traffic Volume**: Identify the **top talker IP addresses** that generate the most traffic.
- **Ans)** We get a total of 128 IPv4 Addresses, but more than 1,000 packets

Address	Packets
192.168.0.37	105317
192.168.0.206	13378
192.168.0.181	13372
192.168.0.184	13259
192.168.0.182	12546
192.168.0.185	12123
192.168.0.201	10534
113.171.240.214	9691
224.0.0.251	6228
192.168.0.1	2404
8.8.8.8	2114
192.168.0.117	2034
162.159.153.4	1924
192.168.0.118	1720
142.250.71.164	1576
192.168.0.75	1489
143.198.246.99	1063
192.168.0.189	1023

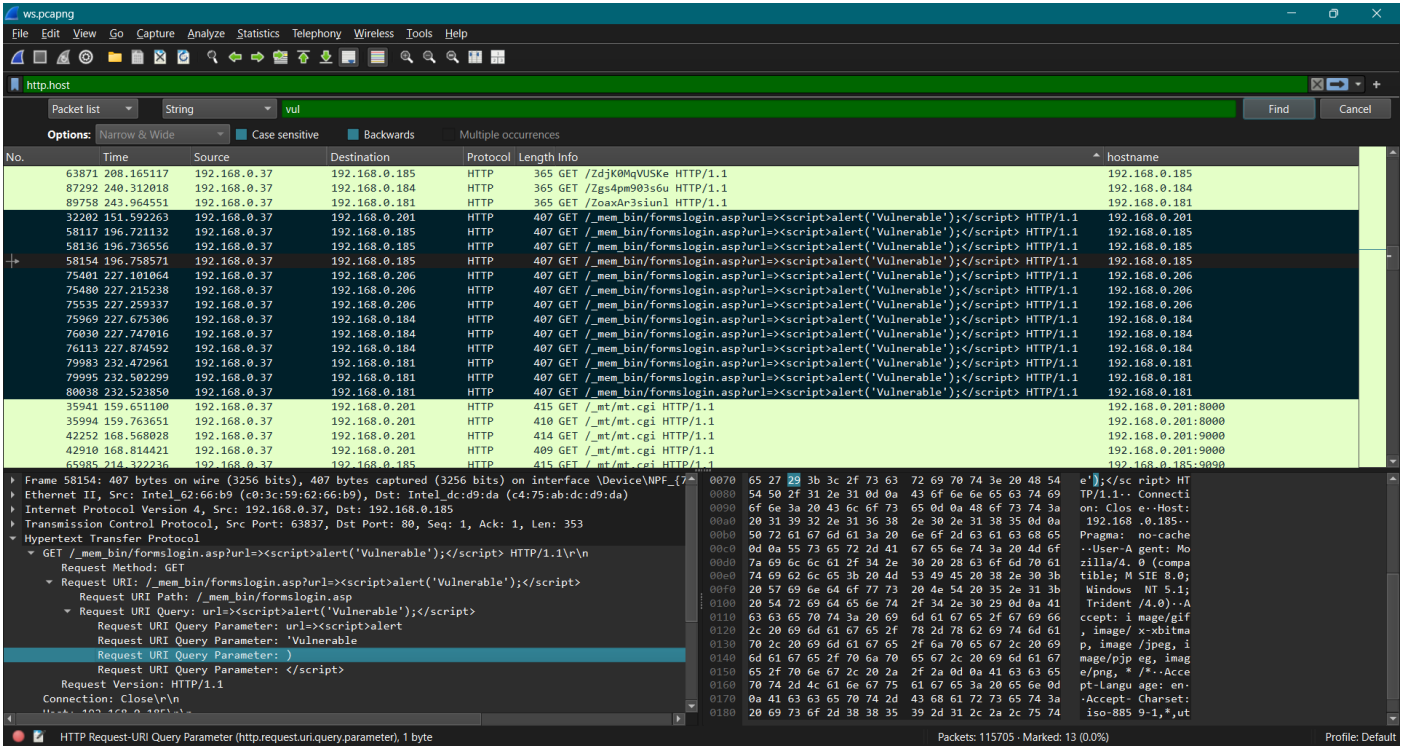
- **Steps:**
  - i) Open Wireshark, open the captured file
  - ii) In Menu bar, Statistics > Endpoints – IPv4
  - iii) Then sort IPs by packets or bytes



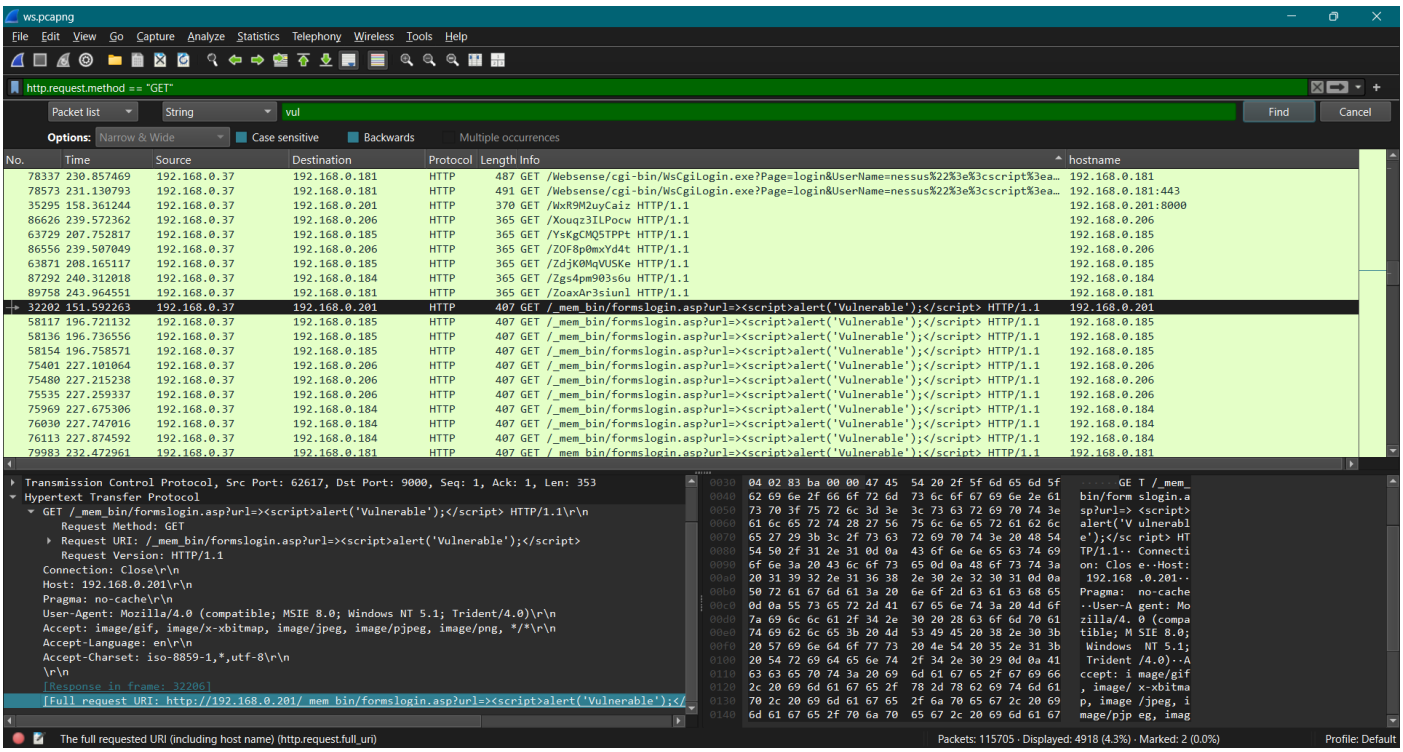


Task 2: Detect HTTP Communications

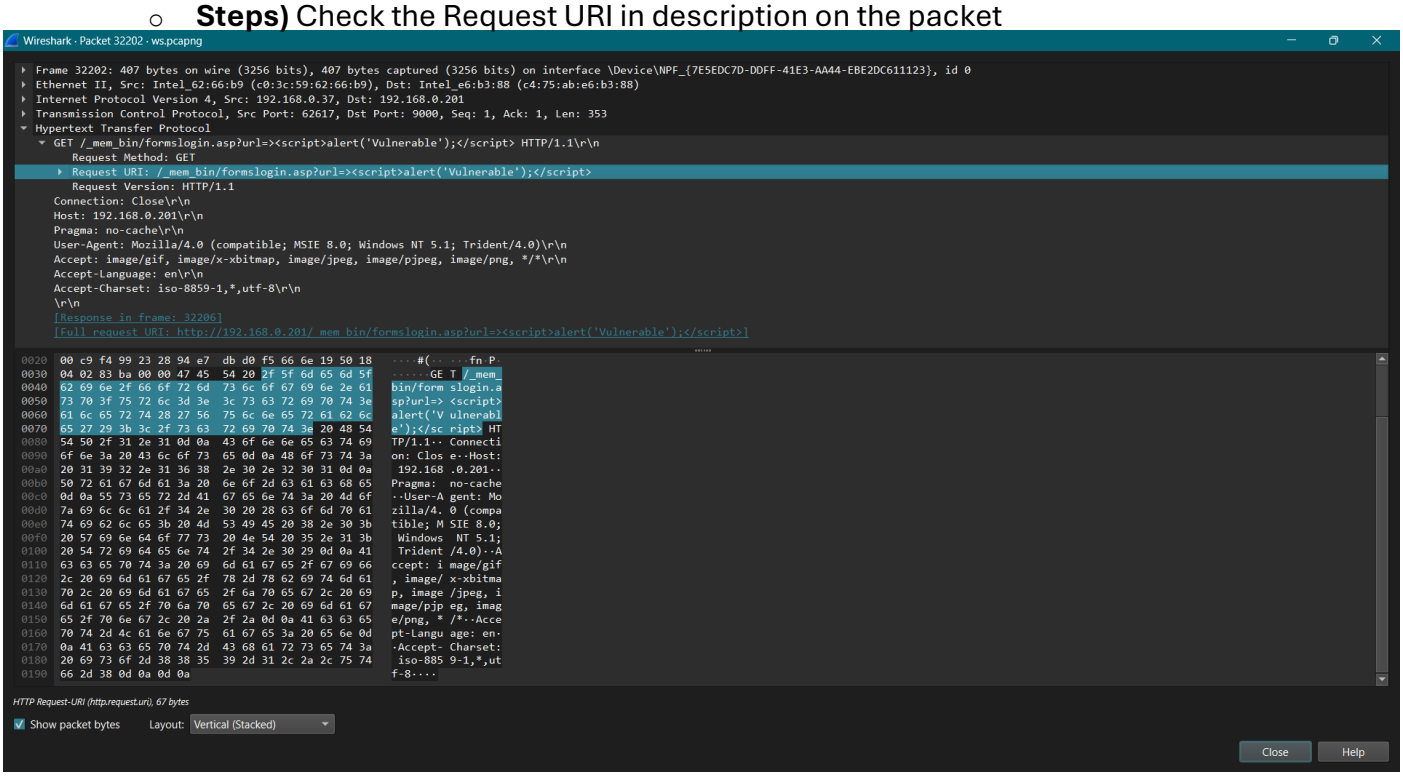
- **HTTP Analysis**: Are there any HTTP requests to suspicious websites?
- **Ans)** Yes, Vulnerable
- **Steps:**
  - i) Open Wireshark, open the captured file
  - ii) In the Filter bar apply http filter, type `http` and press **Enter**.
  - iii) Then check for suspicious websites



- **Inspect a GET Request**: Locate an HTTP GET request and identify:
  - **Hostname of the website.**
  - **Ans)** 192.168.0.201
  - **Steps)** filter “http.host”



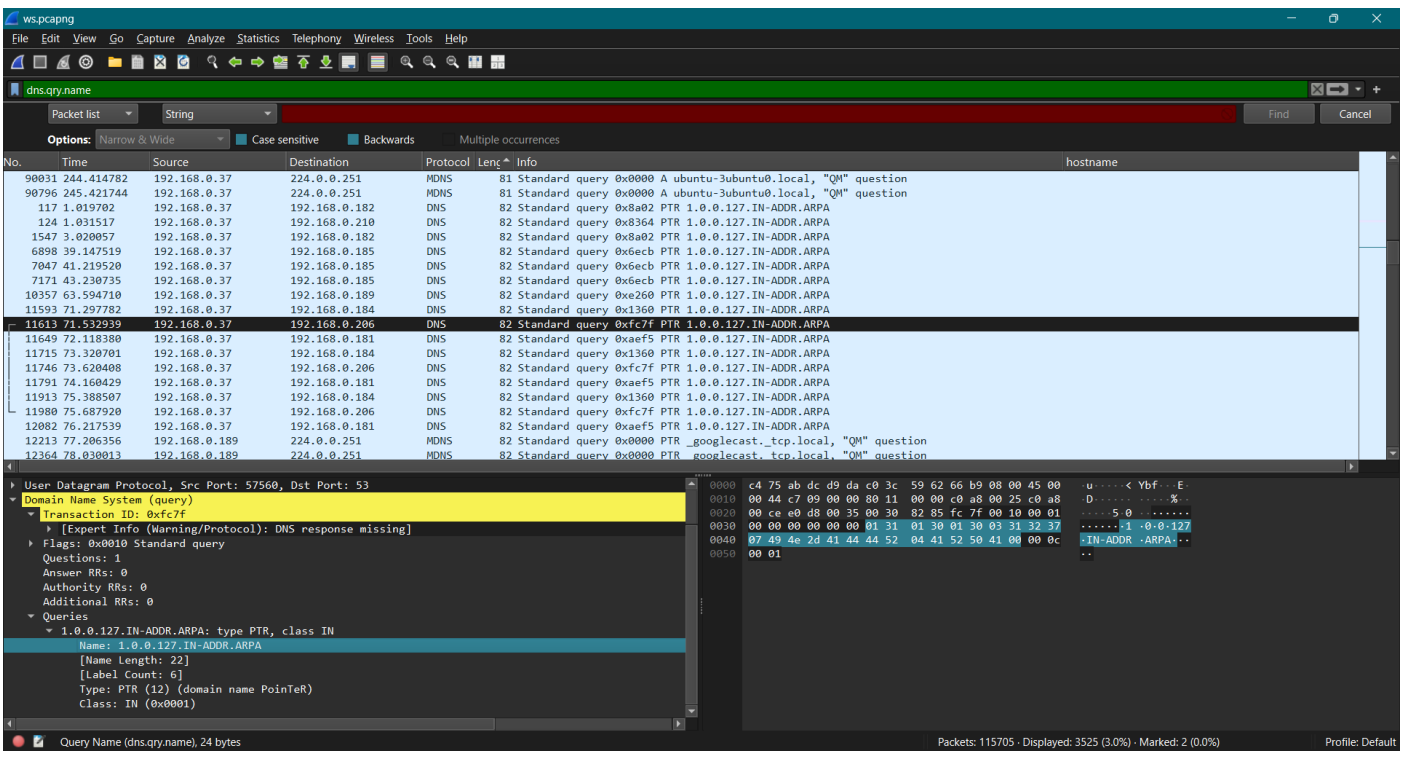
  - **Type of data being requested.**
  - **Ans)** /_mem_bin/formslogin.asp?url=><script>alert('Vulnerable');</script>
  - **Steps)** Check the Request URI in description on the packet



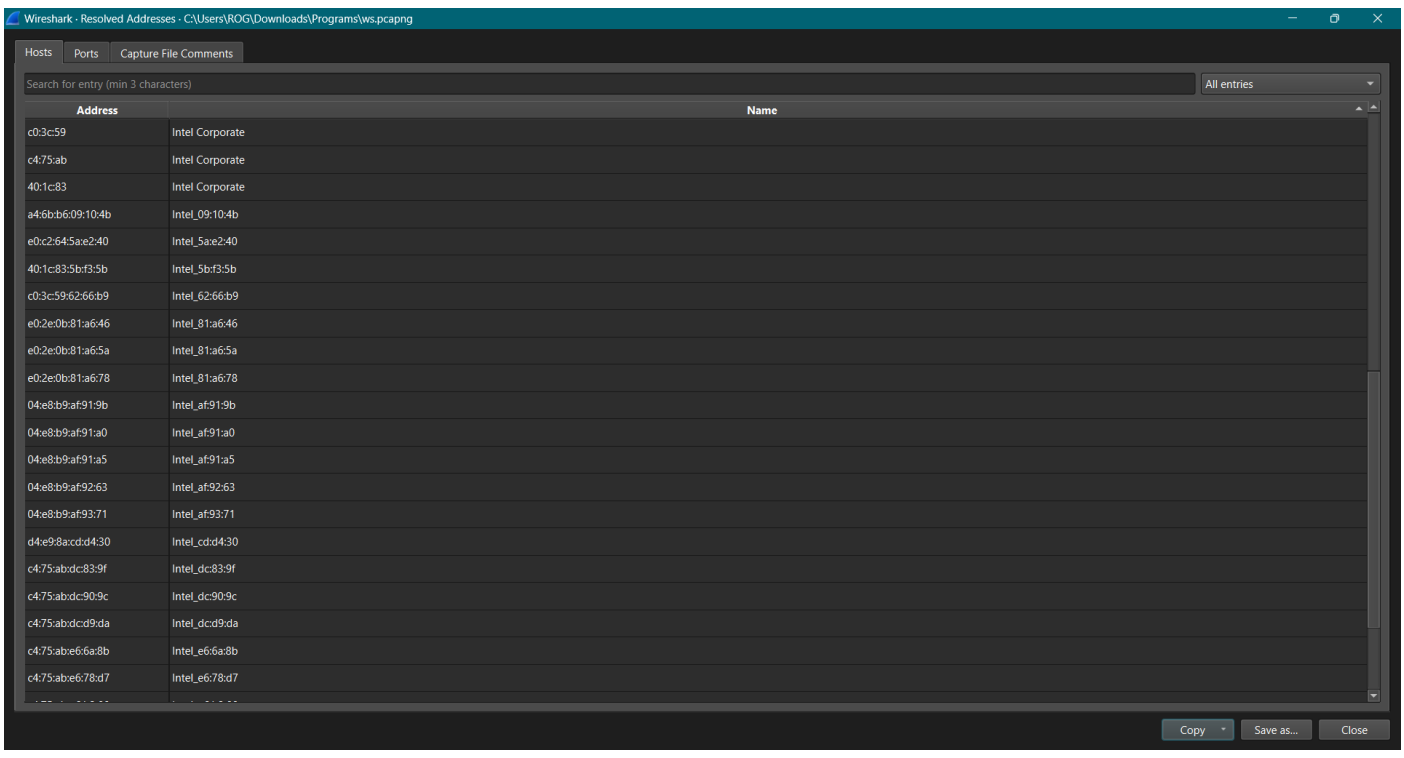
Task 3: DNS Analysis

- **DNS Query Logs**: Filter DNS traffic using dns.
  - Are there any **unusual domain names** being queried?
  - **Ans)** Yes, 1.0.0.127.IN-ADDR.ARPA
  - **Steps)**

    i) In filter bar, type “dns”
    ii) Then check for unusual domain names

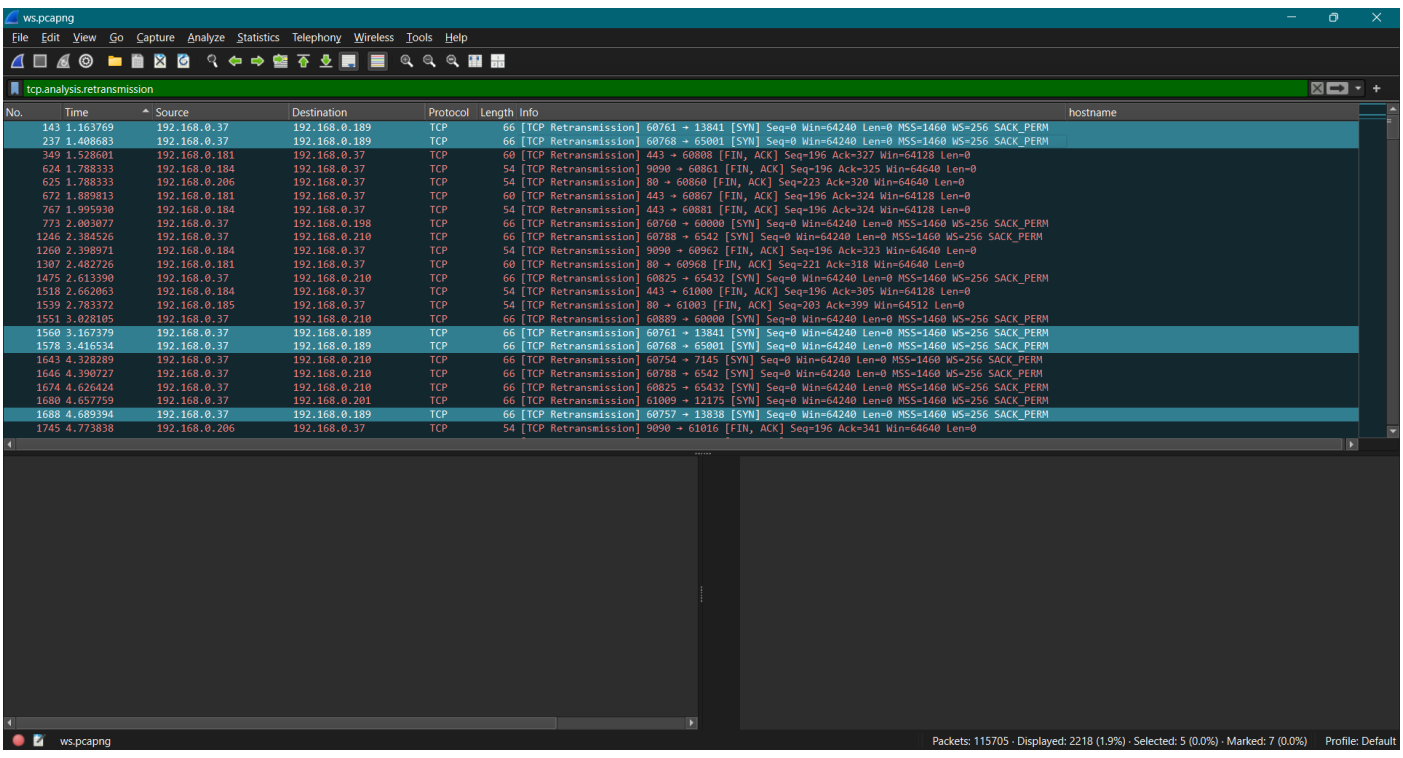


  - What are the **IP addresses** resolved from those queries?
  - **Ans)** Many IPs
  - **Steps)** Select packet then in the menu bar Statistics > Resolved IP

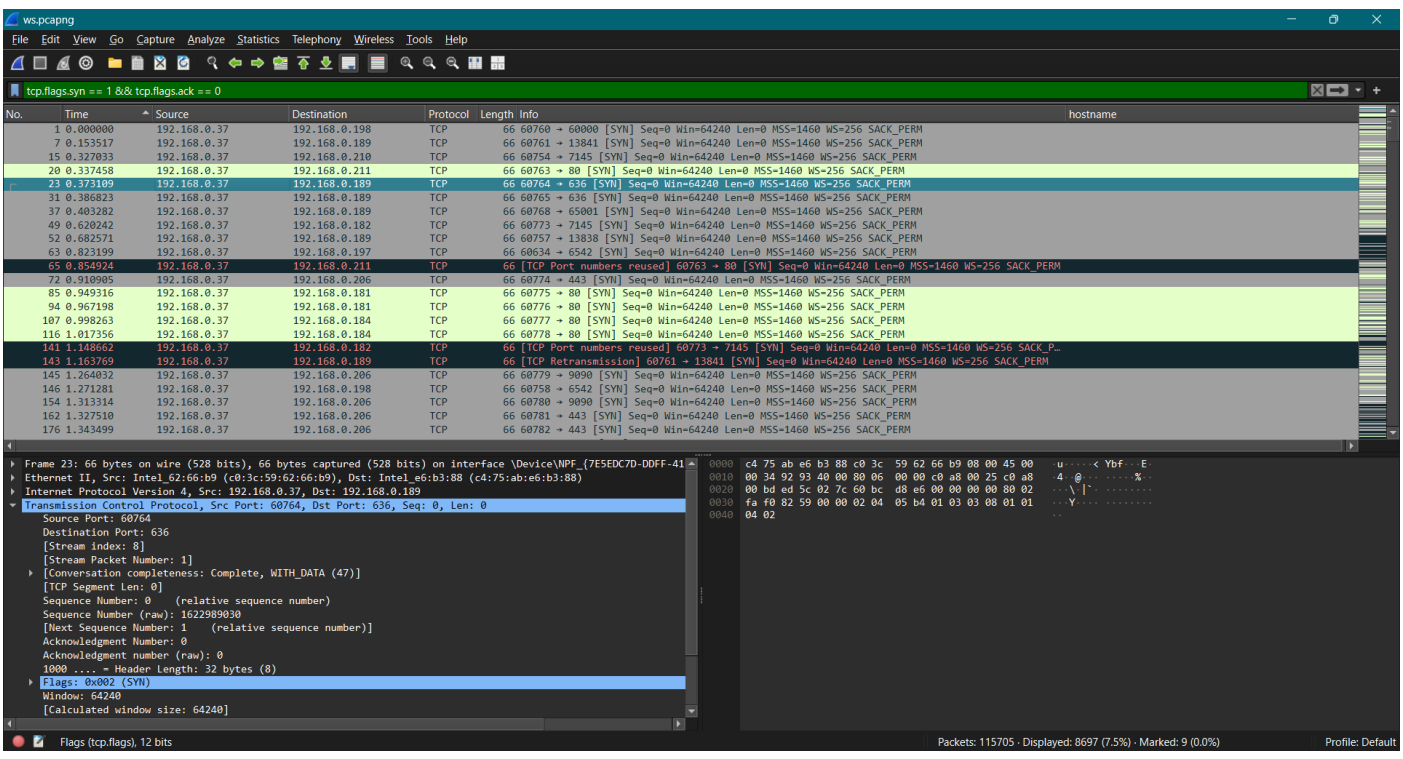


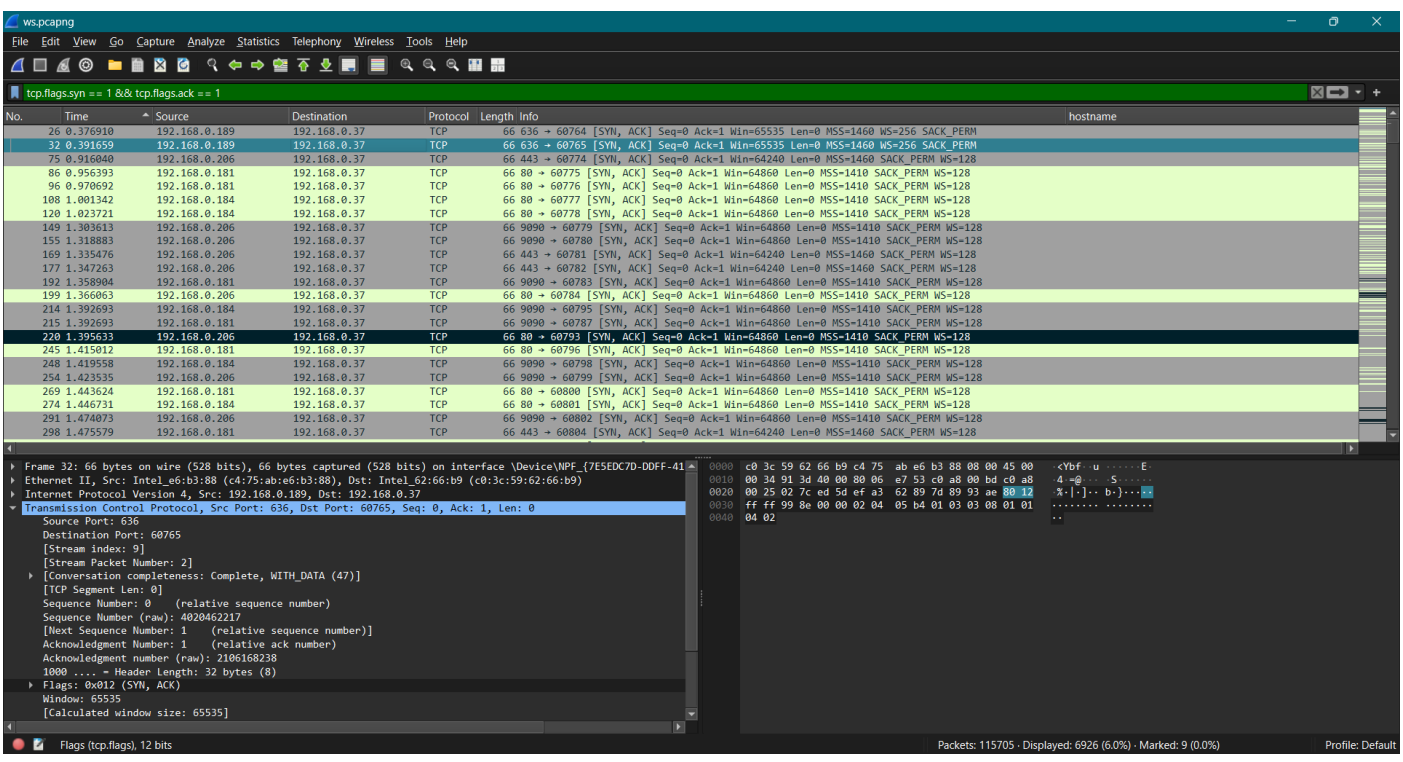
Task 4: Analyze Network Issues

- **Packet Loss and Latency**: Check for TCP retransmissions and high latency.
- Ans) filter by ”tcp.analysis.retransmission”

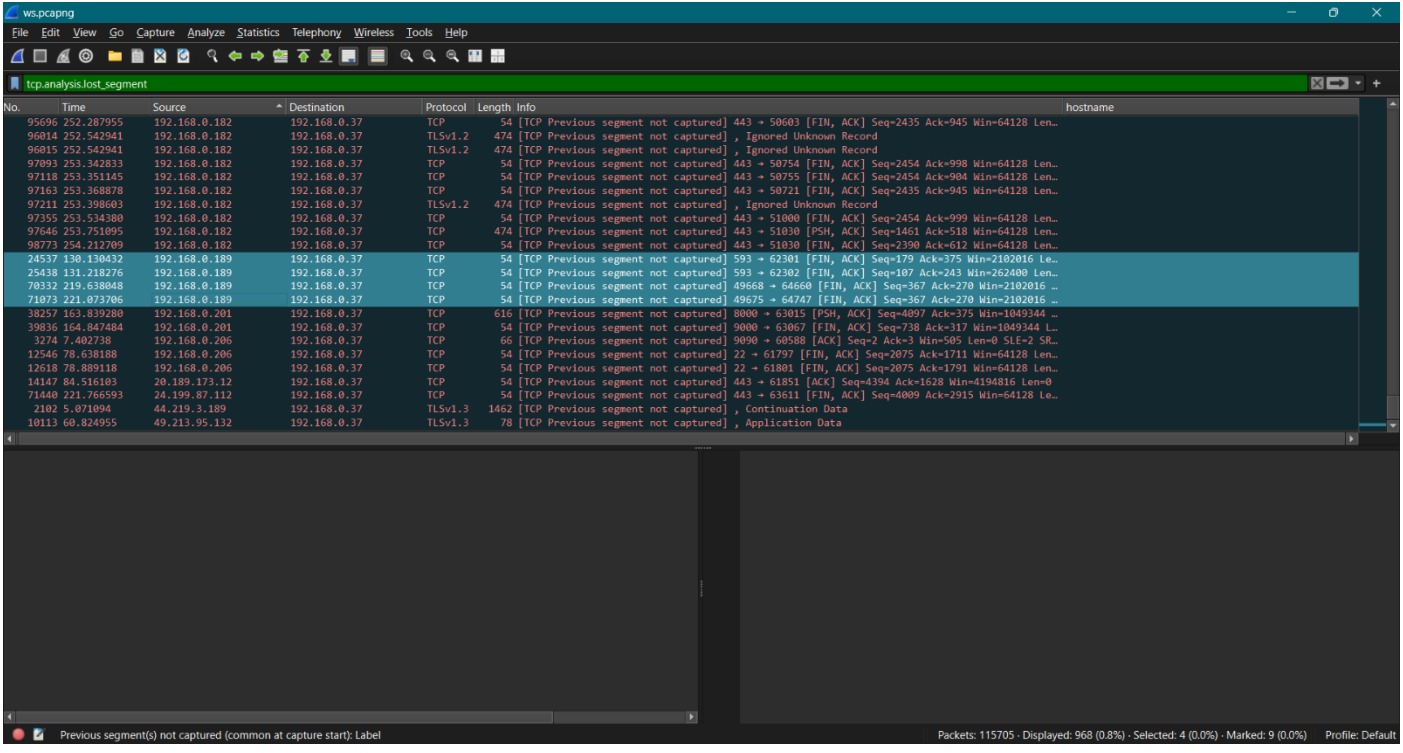


- **TCP Stream Inspection**: Choose one TCP stream with retransmissions and:
    - Examine the handshake (SYN, SYN-ACK, ACK).
    - **Ans) IP1:** 192.168.0.37, **IP2:** 192.168.0.189
    - **Steps)** Applied filters
        - i) tcp.flags.syn == 1 && tcp.flags.ack == 0
        - ii) tcp.flags.syn == 1 && tcp.flags.ack == 1
        - iii) tcp.flags.ack == 1 && tcp.flags.syn == 0



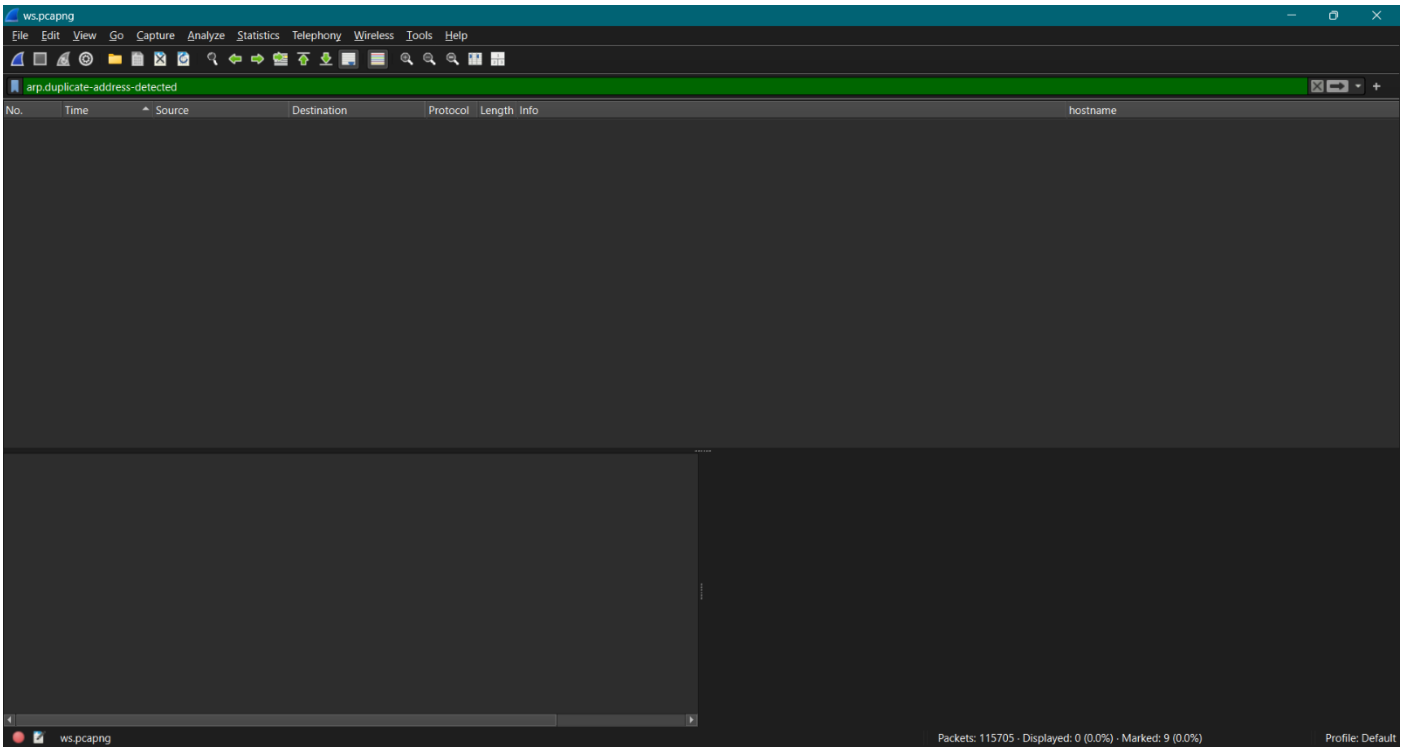


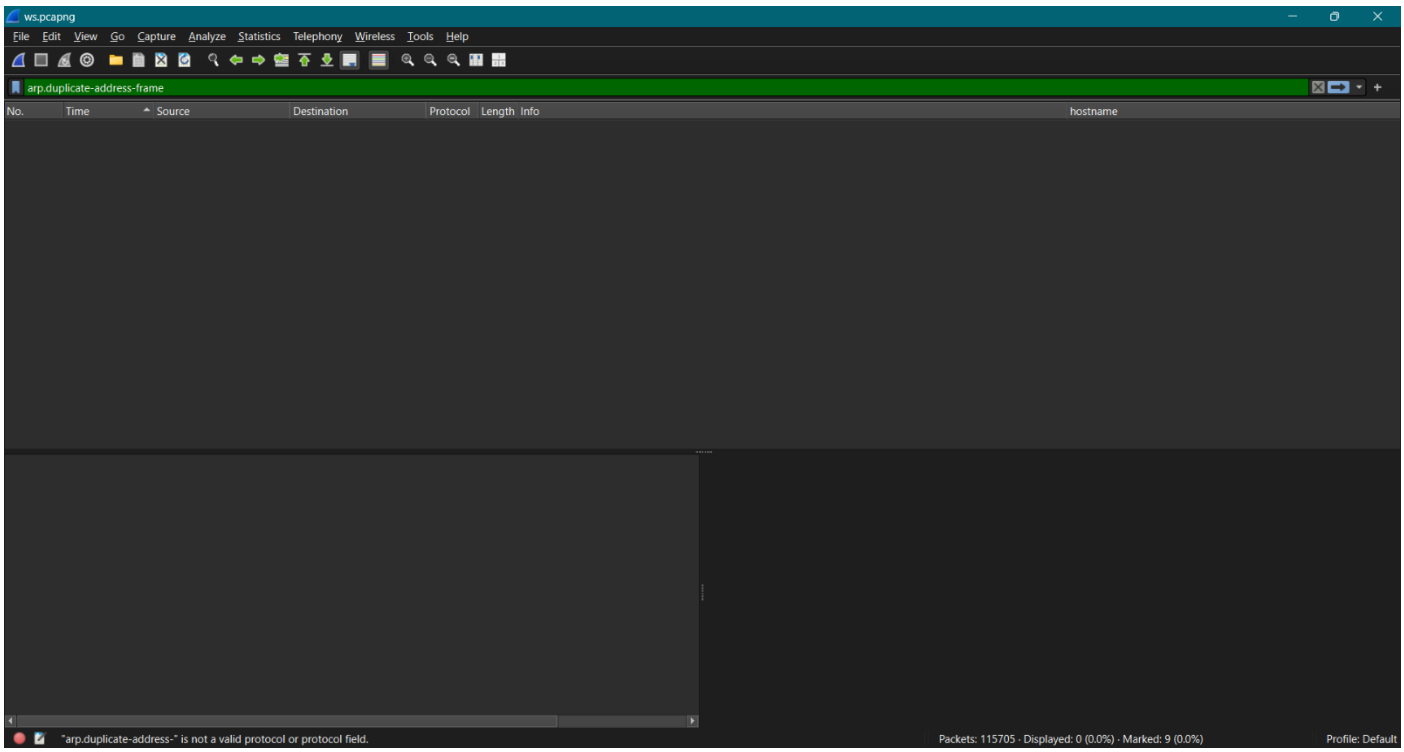
- Identify if there are delays or dropped packets.
- **Ans)** Some
- **Steps)** filter – **“**tcp.analysis.lost_segment”



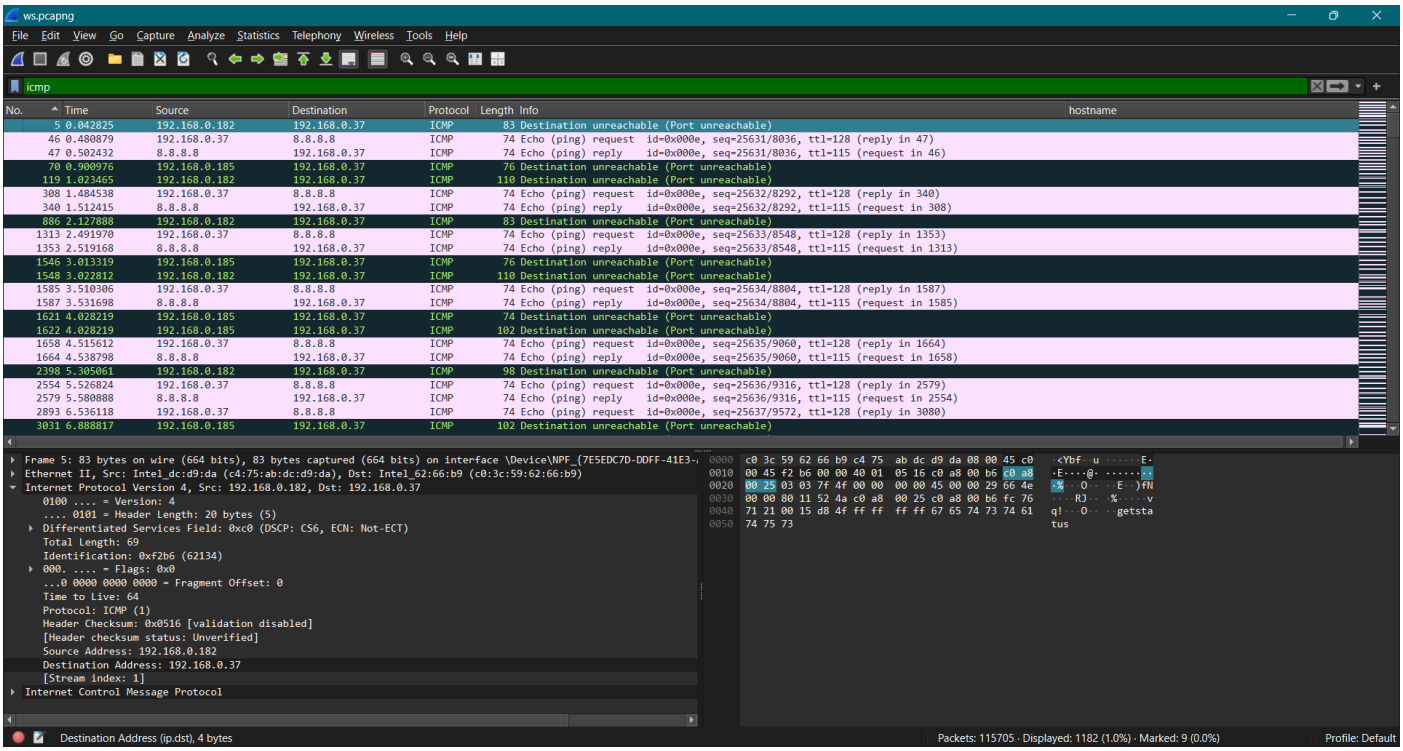
Task 5: Security Threat Detection

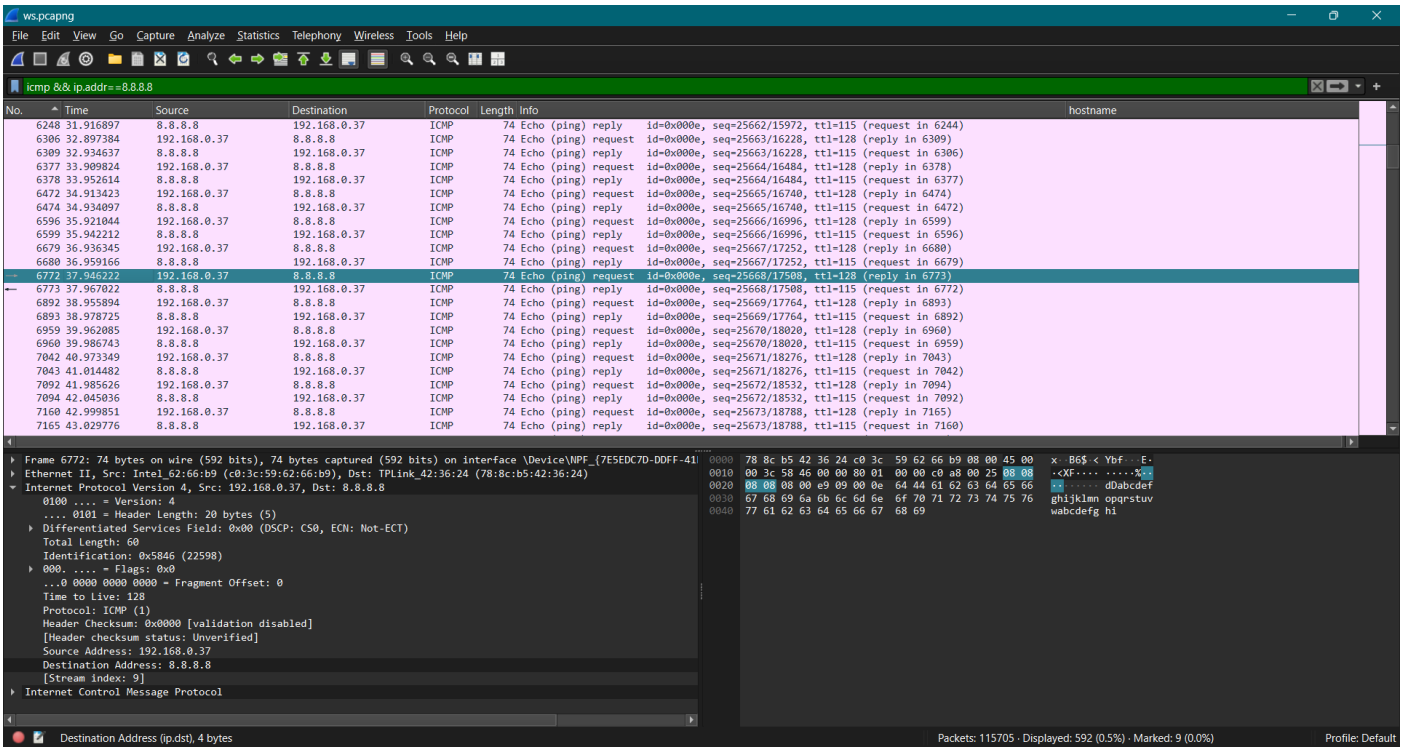
- **Identify ARP Spoofing**: Use arp filter to look for duplicate IPs in ARP replies.
- **Ans) No, duplicate**
- **Steps) Apply filters**
  i) arp.duplicate-address-detected
  ii) arp.duplicate-address-frame





- **Find Possible DoS Attack**: Use the filter icmp and inspect if a host is receiving a large number of ICMP requests in a short time (possible ping flood).
- **Ans)**
- **Steps) Apply filter**
  i) icmp
  ii) icmp && ip.addr==8.8.8.8





Step 3: Reporting and Conclusions

1. **Prepare a Report**:
   Write a short report with the following sections:
   - **Introduction**: Overview of your analysis.
   - **Key Findings**: Mention any suspicious behavior or network anomalies.
   - **Possible Causes/Explanations**: Explain the identified issues and what could cause them.
   - **Recommendations**: Provide suggestions to the network admin to mitigate these issues.

Network Traffic Analysis Report

Introduction

This report summarizes the findings from a comprehensive analysis of network traffic captured using Wireshark. The primary objective of this analysis was to identify potential security threats, network issues, and anomalies within the captured data. The analysis included examining HTTP communications, DNS queries, TCP handshakes, and ARP traffic, as well as assessing for signs of denial-of-service (DoS) attacks.

Key Findings

1. **Suspicious HTTP Requests**: Several HTTP GET requests were identified that targeted potentially malicious domains, including attempts to inject scripts into URLs, indicating a possible Cross-Site Scripting (XSS) vulnerability.
2. **DNS Anomalies**: Unusual domain names were queried, and multiple IP addresses were resolved for these domains, suggesting possible domain generation algorithms or malicious intent.
3. **TCP Retransmissions**: A significant number of TCP retransmissions were observed, indicating potential packet loss or network congestion.
4. **ARP Spoofing Indicators**: Duplicate IP addresses were detected in ARP replies, suggesting possible ARP spoofing attempts within the network.
5. **ICMP Flooding**: A high volume of ICMP Echo Requests directed at a single host was detected, indicative of a potential ping flood attack.

Possible Causes/Explanations

- **Malicious Activity**: The suspicious HTTP requests and DNS queries may indicate ongoing malicious activities such as phishing attempts or exploitation of web application vulnerabilities.
- **Network Congestion**: The observed TCP retransmissions could be attributed to network congestion or hardware issues affecting packet delivery.
- **ARP Spoofing**: The presence of duplicate IP addresses in ARP replies may suggest that an attacker is attempting to intercept traffic on the local network by impersonating legitimate devices.
- **DoS Attack**: The excessive ICMP requests could be part of a denial-of-service attack aimed at overwhelming the target host and disrupting its normal operations.

Recommendations

1. **Enhance Security Monitoring**: Implement continuous monitoring of HTTP and DNS traffic for suspicious patterns. Utilize intrusion detection systems (IDS) to alert on anomalies.
2. **Network Segmentation**: Consider segmenting the network to limit the impact of ARP spoofing and other attacks. Use VLANs to separate sensitive devices from general network traffic.
3. **Implement Rate Limiting**: Apply rate limiting on ICMP traffic to mitigate the risk of DoS attacks and prevent overwhelming critical services.
4. **Conduct Regular Security Audits**: Perform regular security audits and vulnerability assessments on web applications to identify and remediate potential vulnerabilities like XSS.
5. **Educate Users**: Provide training for users about the dangers of phishing and other social engineering attacks to reduce the likelihood of successful exploits.