TASK - 5

Objective: Capture live network packets and identify basic protocols and traffic types.
Tools: Wireshark (free).
Deliverables: A packet capture (.pcap) file and a short report of protocols identified.

~> Step 1: Install Wireshark

Windows:

Download from https://www.wireshark.org/download.html
Install with default settings (includes WinPcap/Npcap)

Kali Linux:

sudo apt update
sudo apt install wireshark

~> Step 2: Start Capturing Packets

Launch Wireshark (may require administrator privileges)

Select your active network interface (Common interfaces: Wi-Fi, Ethernet, Local Area Connection)

Click the blue shark fin icon or double-click the interface to start capture

~> Step 3: Browser different applications on browser

This will capture the data packets from your network to web application you visit.
(Example : visit https://www.google.com)

~> Step 4 : stop the capture (which is on the top left)

~> Step 5 : Use filters for to view and analyze specific protocols .
(example : dns , http , udp , tcp , telnet)

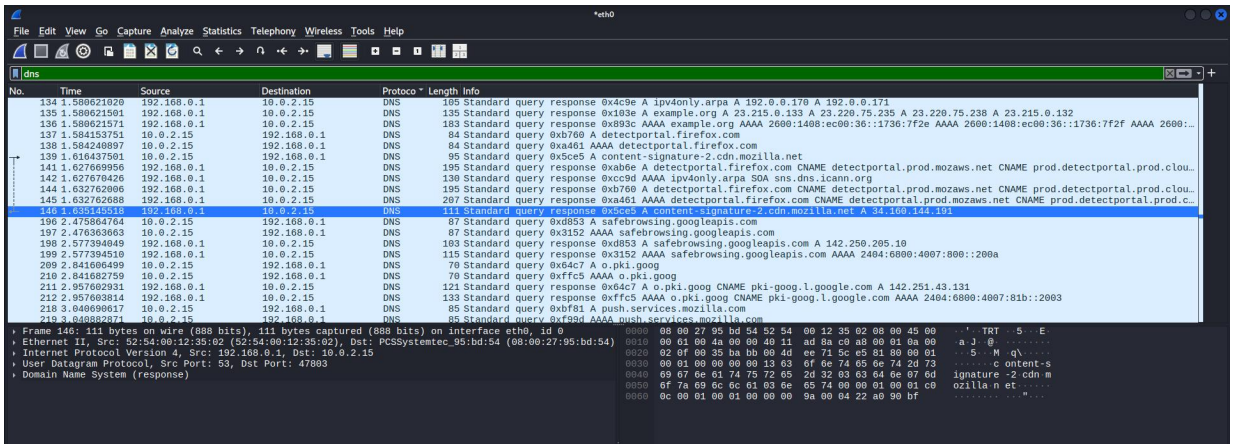
~> Step 6 : export as file (.pcap file)
Simply open the file tab and click on the save as this will download and create a pcap file of your captured data.

Summary :

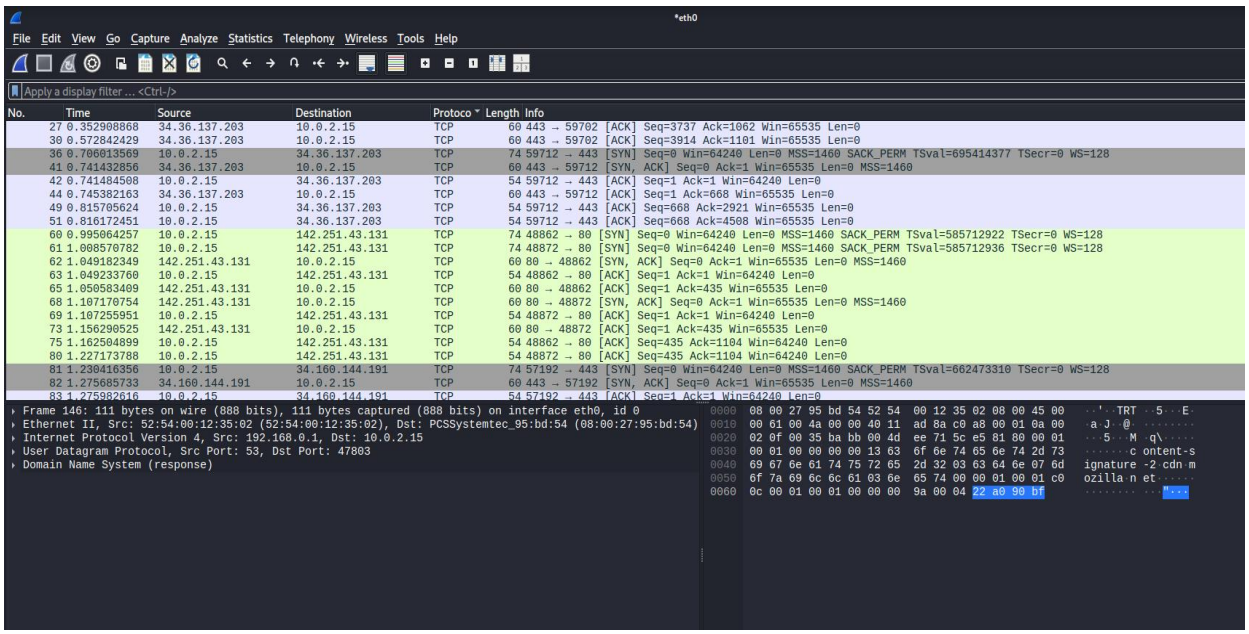
Screenshot of specific protocols analyzed using filters.

(Most common protocols : HTTP , DNS , TCP , UDP , ICMP)

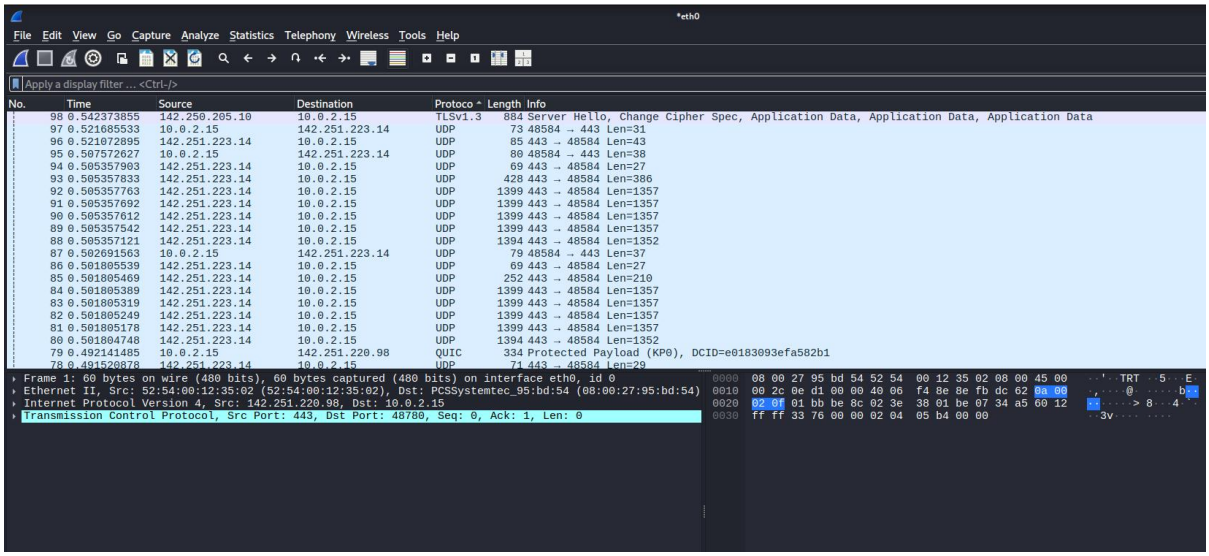
DNS protocol :



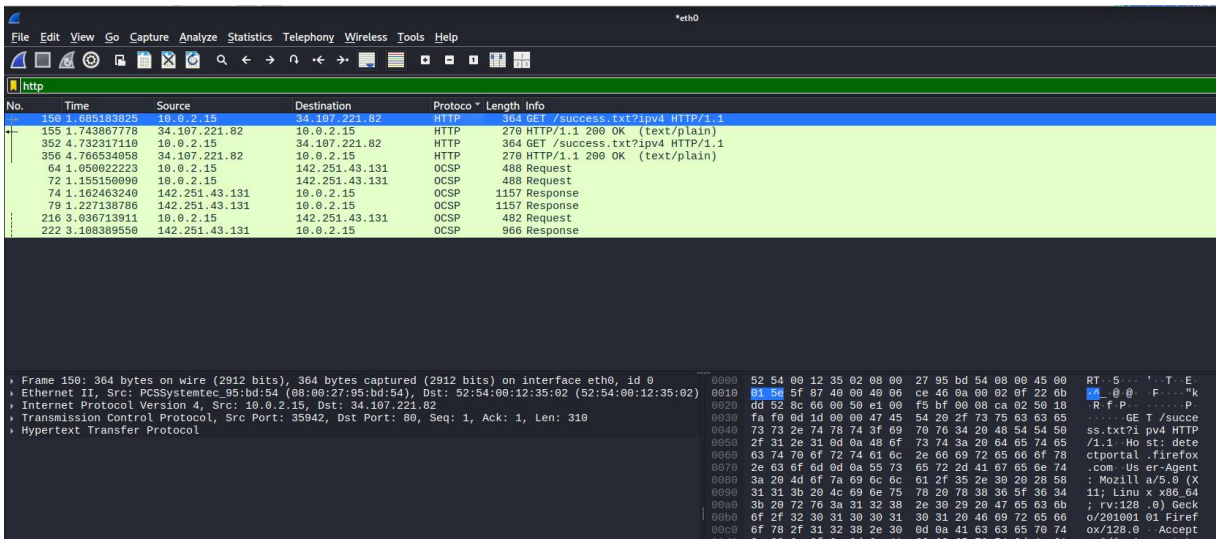
TCP Protocol :



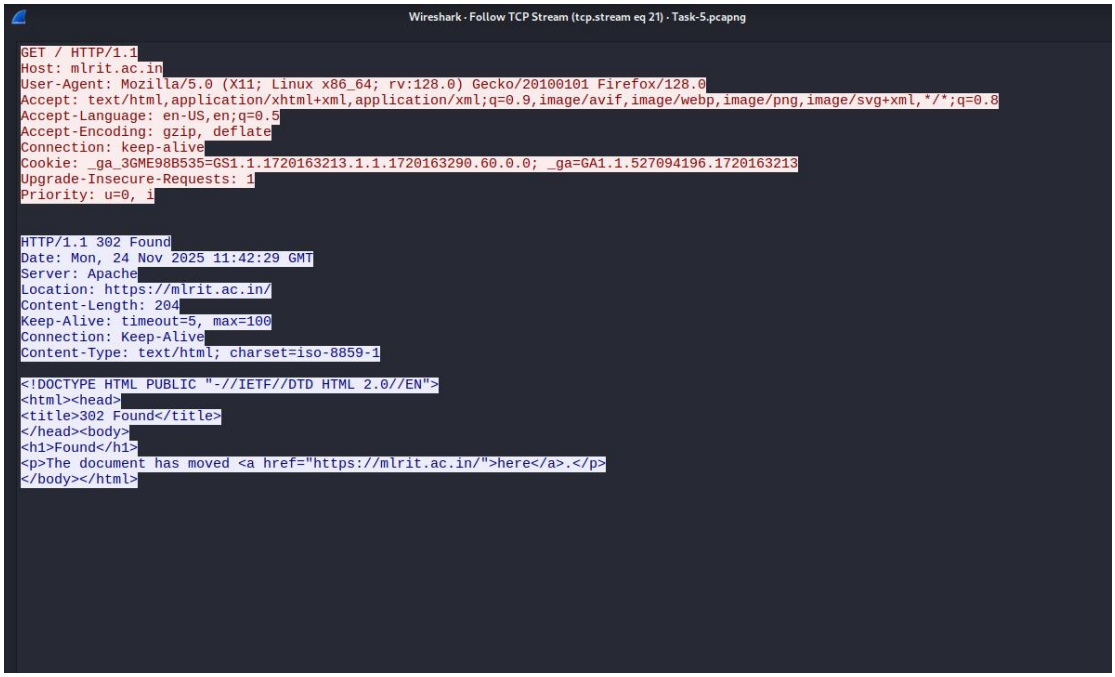
UDP Protocol :

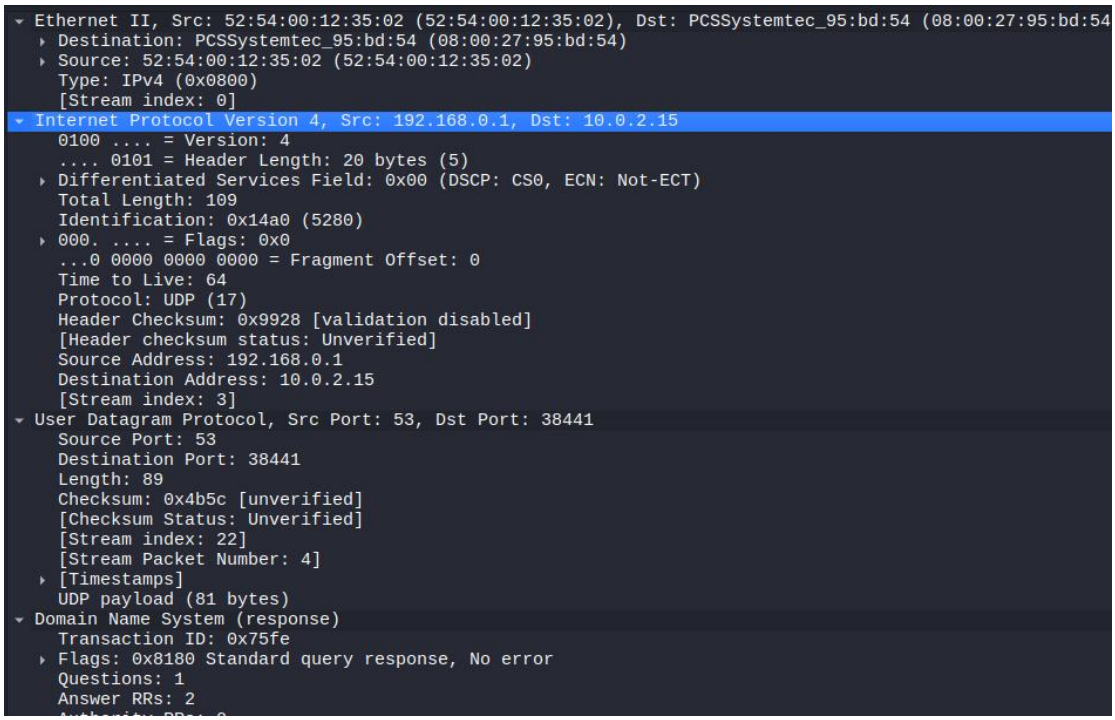


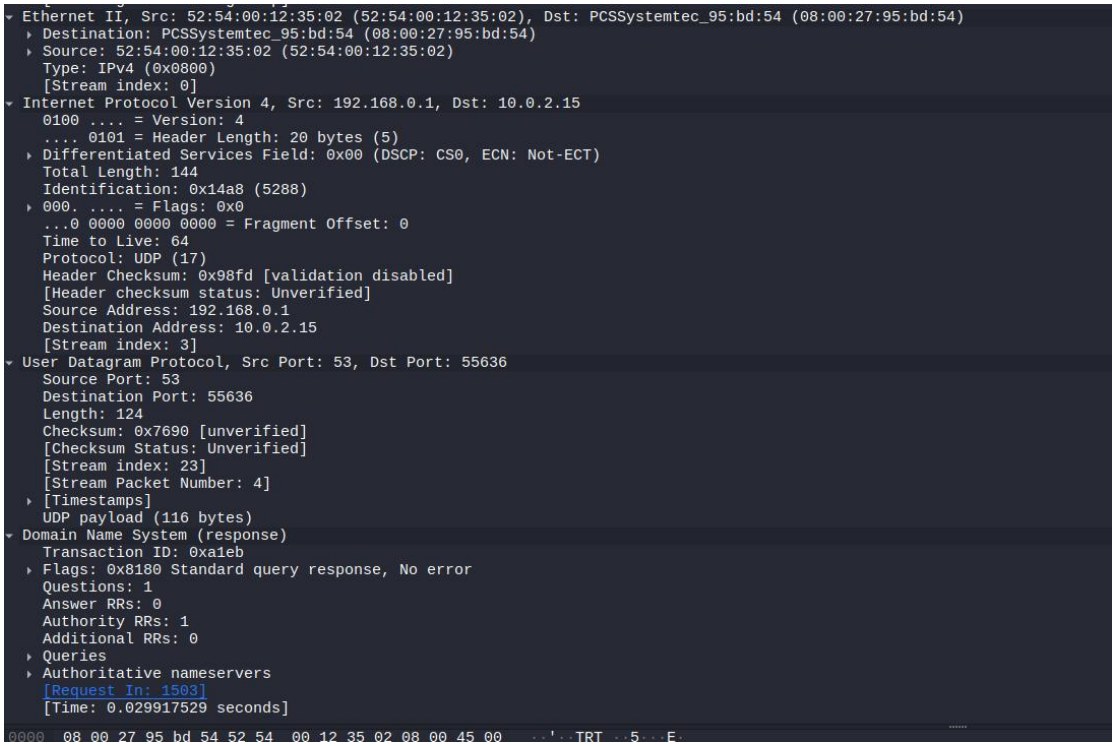
HTTP Protocol :



Analysis of Captured data in the packets :






Ethernet II, Src: 52:54:00:12:35:02 (52:54:00:12:35:02), Dst: PCSSystemtec_95:bd:54 (08:00:27:95:bd:54)
Destination: PCSSystemtec_95:bd:54 (08:00:27:95:bd:54)
Source: 52:54:00:12:35:02 (52:54:00:12:35:02)
Type: IPv4 (0x0800)
[Stream index: 0]
Internet Protocol Version 4, Src: 192.168.0.1, Dst: 10.0.2.15
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 144
Identification: 0x14a8 (5288)
000. .... = Flags: 0x0
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 64
Protocol: UDP (17)
Header Checksum: 0x98fd [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.0.1
Destination Address: 10.0.2.15
[Stream index: 3]
User Datagram Protocol, Src Port: 53, Dst Port: 55636
Source Port: 53
Destination Port: 55636
Length: 124
Checksum: 0x7690 [unverified]
[Checksum Status: Unverified]
[Stream index: 23]
[Stream Packet Number: 4]
[Timestamps]
UDP payload (116 bytes)
Domain Name System (response)
Transaction ID: 0xa1eb
Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 0
Authority RRs: 1
Additional RRs: 0
Queries
Authoritative nameservers
[Request In: 1503]
[Time: 0.029917529 seconds]
0000 08 00 27 95 bd 54 52 54 00 12 35 02 08 00 45 00