

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 :

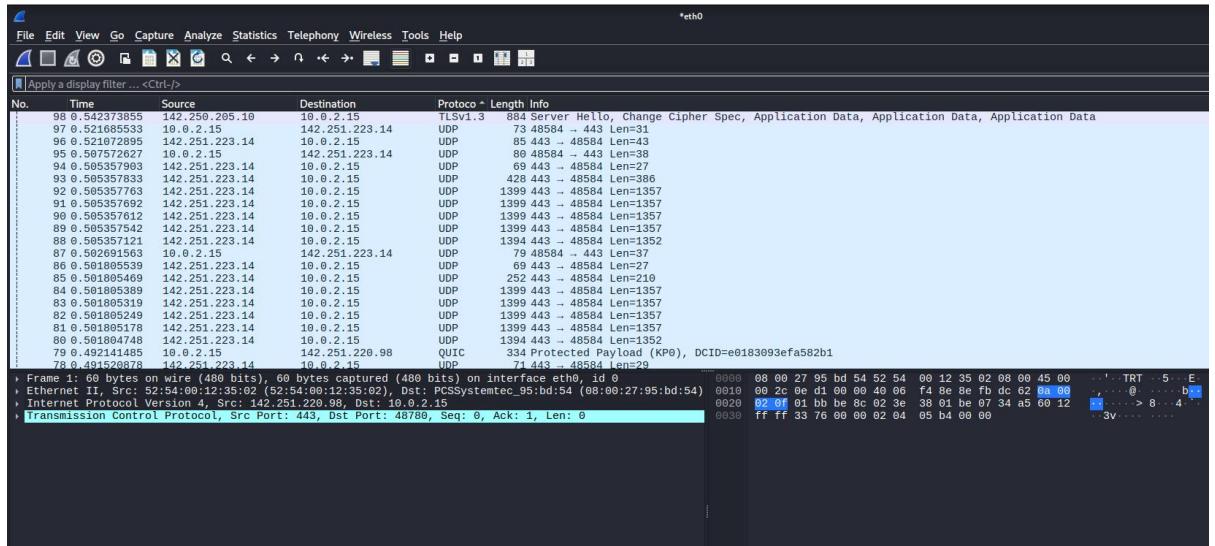
Screenshot of specific protocols analyzed using filters.

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

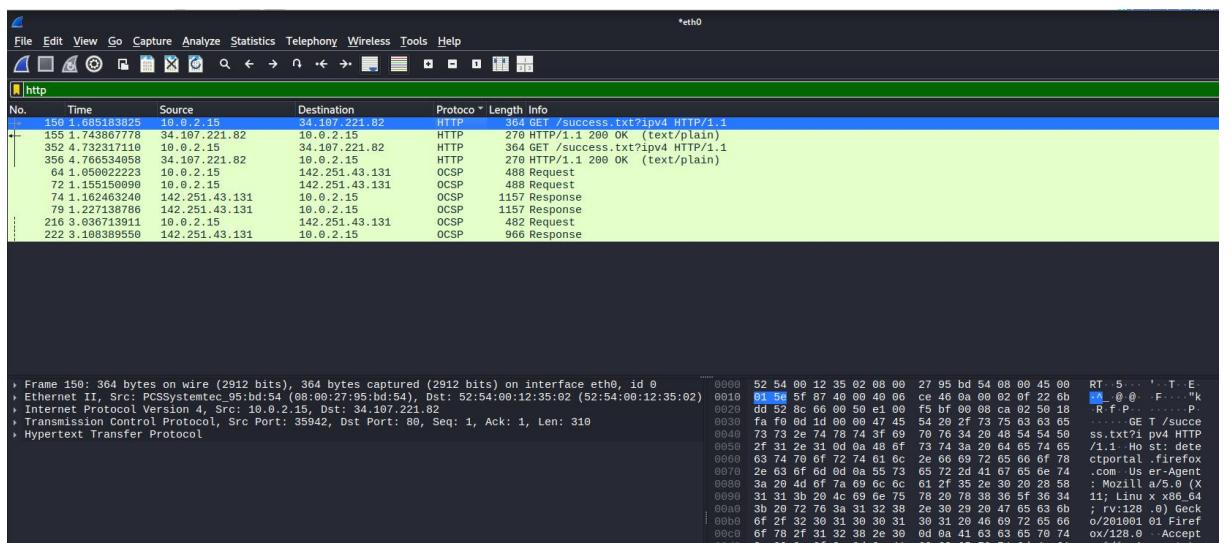
DNS protocol :

TCP Protocol :

UDP Protocol :



HTTP Protocol :



Analysis of Captured data in the packets :

```
GET / HTTP/1.1
Host: mlrit.ac.in
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Cookie: _ga_3GME98B535=GS1.1.1720163213.1.1.1720163290.60.0.0; _ga=GA1.1.527094196.1720163213
Upgrade-Insecure-Requests: 1
Priority: u=0, i

HTTP/1.1 302 Found
Date: Mon, 24 Nov 2025 11:42:29 GMT
Server: Apache
Location: https://mlrit.ac.in/
Content-Length: 204
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>302 Found</title>
</head><body>
<h1>Found</h1>
<p>The document has moved <a href="https://mlrit.ac.in/">here</a>.</p>
</body></html>
```

```
Ethernet II, Src: PCSSystemtec_95:bd:54 (08:00:27:95:bd:54), 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
  Version: 4
  Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 109
  Identification: 0x14a0 (5280)
  Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 64
  Protocol: UDP (17)
  Header Checksum: 0x9928 [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: 38441
  Source Port: 53
  Destination Port: 38441
  Length: 89
  Checksum: 0x4b5c [unverified]
    [Checksum Status: Unverified]
    [Stream index: 22]
    [Stream Packet Number: 4]
  [Timestamps]
  UDP payload (81 bytes)
Domain Name System (response)
  Transaction ID: 0x75fe
  Flags: 0x8100 Standard query response, No error
  Questions: 1
  Answer RRs: 2
    [Timestamps]
```

```
✗ 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: 0x8100 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  ...'...TRT ...5...E.
```