

## 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.

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

[illegible]

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter... <Ctrl-F>

No.	Time	Source	Destination	Protocol	Length	Info
27	0.35298868	34.36.137.203	10.0.2.15	TCP	60	443 → 59702 [ACK] Seq=3737 Ack=1062 Win=65535 Len=0
30	0.57284249	34.36.137.203	10.0.2.15	TCP	60	443 → 59702 [ACK] Seq=3914 Ack=1101 Win=65535 Len=0
36	0.706013569	10.0.2.15	34.36.137.203	TCP	54	59712 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=695414377 TSecr=0 WS=128
41	0.741432856	34.36.137.203	10.0.2.15	TCP	60	443 → 59712 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
42	0.741404500	10.0.2.15	34.36.137.203	TCP	54	59712 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
44	0.745382163	34.36.137.203	10.0.2.15	TCP	60	443 → 59712 [ACK] Seq=1 Ack=688 Win=65535 Len=0
49	0.815705624	10.0.2.15	34.36.137.203	TCP	54	59712 → 443 [ACK] Seq=668 Ack=2921 Win=65535 Len=0
51	0.816172451	10.0.2.15	34.36.137.203	TCP	54	59712 → 443 [ACK] Seq=668 Ack=4508 Win=65535 Len=0
60	0.995064257	10.0.2.15	142.251.43.131	TCP	74	48862 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=505712922 TSecr=0 WS=128
61	1.008570782	10.0.2.15	142.251.43.131	TCP	74	48872 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=585712936 TSecr=0 WS=128
62	1.049182349	142.251.43.131	10.0.2.15	TCP	60	80 → 48862 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
63	1.049233760	10.0.2.15	142.251.43.131	TCP	54	48862 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
65	1.050583409	142.251.43.131	10.0.2.15	TCP	60	80 → 48862 [ACK] Seq=1 Ack=435 Win=65535 Len=0
68	1.107170754	142.251.43.131	10.0.2.15	TCP	60	80 → 48872 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
69	1.107255951	10.0.2.15	142.251.43.131	TCP	54	48872 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
73	1.156290925	142.251.43.131	10.0.2.15	TCP	60	80 → 48872 [ACK] Seq=1 Ack=435 Win=65535 Len=0
75	1.162504989	10.0.2.15	142.251.43.131	TCP	54	48862 → 80 [ACK] Seq=435 Ack=1104 Win=64240 Len=0
80	1.227173788	10.0.2.15	142.251.43.131	TCP	54	48872 → 80 [ACK] Seq=435 Ack=1104 Win=64240 Len=0
81	1.230416356	10.0.2.15	34.160.144.191	TCP	74	57192 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=662473310 TSecr=0 WS=128
82	1.275685733	34.160.144.191	10.0.2.15	TCP	60	443 → 57192 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
83	1.275839261	10.0.2.15	34.160.144.191	TCP	54	57192 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0

\* Frame 146: 111 bytes on wire (888 bits), 111 bytes captured (888 bytes) on interface eth0, id 0 (0.0.0.0) → 0.0.0.0 (0.0.0.0)

\* 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)

\* Internet Protocol Version 4, Src: 192.168.0.1, Dst: 10.0.2.15

\* User Datagram Protocol, Src Port: 53, Dst Port: 47883

\* Domain Name System (response)

0010 00 01 00 27 95 bd 54 52 54 00 12 35 02 08 00 45 00 ... TRT 5 E

0020 02 0f 00 35 ba bb 00 4f 01 ad 8a c0 a8 00 01 0a 00 ... a J @

0030 00 01 00 00 00 13 63 6f 7a 65 06 74 2d 73 ... 5 M q

0040 69 67 6e 61 74 75 67 65 2d 32 03 63 6e 07 6d ... content:

0050 6f 7a 09 01 61 63 6e 75 7a 00 00 01 08 01 c0 ... ignature 2 cdm m

0060 0c 00 01 00 01 00 00 00 5a 00 04 22 08 38 b1 ... ozilla.net

## UDP Protocol :

Wireshark capture of UDP traffic on interface eth0. The packet list shows multiple UDP packets from 10.0.2.15 to 142.251.223.14. The packet details pane shows the structure of a UDP packet, including the UDP header and the application data payload.

No.	Time	Source	Destination	Protocol	Length	Info
98	0.542373855	142.250.205.10	10.0.2.15	TLSv1.3	884	Server Hello, Change Cipher Spec, Application Data, Application Data, Application Data
97	0.521685533	10.0.2.15	142.251.223.14	UDP	73	48584 → 443 Len=31
96	0.521072895	142.251.223.14	10.0.2.15	UDP	85	443 → 48584 Len=43
95	0.507572627	10.0.2.15	142.251.223.14	UDP	80	48584 → 443 Len=38
94	0.505357903	142.251.223.14	10.0.2.15	UDP	69	443 → 48584 Len=27
93	0.505357833	142.251.223.14	10.0.2.15	UDP	428	443 → 48584 Len=386
92	0.505357763	142.251.223.14	10.0.2.15	UDP	1399	443 → 48584 Len=1357
91	0.505357692	142.251.223.14	10.0.2.15	UDP	1399	443 → 48584 Len=1357
90	0.505357612	142.251.223.14	10.0.2.15	UDP	1399	443 → 48584 Len=1357
89	0.505357542	142.251.223.14	10.0.2.15	UDP	1399	443 → 48584 Len=1357
88	0.505357121	142.251.223.14	10.0.2.15	UDP	1394	443 → 48584 Len=1352
87	0.502691503	10.0.2.15	142.251.223.14	UDP	79	48584 → 443 Len=37
86	0.501805539	142.251.223.14	10.0.2.15	UDP	69	443 → 48584 Len=27
85	0.501805469	142.251.223.14	10.0.2.15	UDP	252	443 → 48584 Len=210
84	0.501805389	142.251.223.14	10.0.2.15	UDP	1399	443 → 48584 Len=1357
83	0.501805319	142.251.223.14	10.0.2.15	UDP	1399	443 → 48584 Len=1357
82	0.501805249	142.251.223.14	10.0.2.15	UDP	1399	443 → 48584 Len=1357
81	0.501805178	142.251.223.14	10.0.2.15	UDP	1399	443 → 48584 Len=1357
80	0.501804748	142.251.223.14	10.0.2.15	UDP	1394	443 → 48584 Len=1352
79	0.492141485	10.0.2.15	142.251.220.98	QUIC	334	Protected Payload (KP0), DCID=e0183093efa582b1
78	0.491520878	142.251.223.14	10.0.2.15	UDP	71	443 → 48584 Len=29

Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0, id 0  
Ethernet II, Src: PCSyswrmec\_95:bd:54 (52:54:00:12:35:02), Dst: PCSyswrmec\_95:bd:54 (08:00:27:95:bd:54)  
Internet Protocol Version 4, Src: 142.251.220.98, Dst: 10.0.2.15  
Transmission Control Protocol, Src Port: 443, Dst Port: 48780, Seq: 0, Ack: 1, Len: 0

## HTTP Protocol :

Wireshark capture of HTTP traffic on interface eth0. The packet list shows multiple HTTP requests and responses. The packet details pane shows the structure of an HTTP request, including the request line, headers, and the body.

No.	Time	Source	Destination	Protocol	Length	Info
150	1.698180825	10.0.2.15	34.107.221.82	HTTP	364	GET /success.txt?ipw4 HTTP/1.1
151	1.742067778	34.107.221.82	10.0.2.15	HTTP	270	HTTP/1.1 200 OK (text/plain)
352	4.732317110	10.0.2.15	34.107.221.82	HTTP	364	GET /success.txt?ipw4 HTTP/1.1
356	4.766534958	34.107.221.82	10.0.2.15	HTTP	270	HTTP/1.1 200 OK (text/plain)
64	1.050022223	10.0.2.15	142.251.43.131	OCSP	488	Request
72	1.155150890	10.0.2.15	142.251.43.131	OCSP	488	Request
74	1.162463240	142.251.43.131	10.0.2.15	OCSP	1157	Response
79	1.227138786	142.251.43.131	10.0.2.15	OCSP	1157	Response
216	3.036713911	10.0.2.15	142.251.43.131	OCSP	482	Request
222	3.108389590	142.251.43.131	10.0.2.15	OCSP	966	Response

Frame 150: 364 bytes on wire (2912 bits), 364 bytes captured (2912 bits) on interface eth0, id 0  
Ethernet II, Src: PCSyswrmec\_95:bd:54 (08:00:27:95:bd:54), Dst: 52:54:00:12:35:02 (52:54:00:12:35:02)  
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 34.107.221.82  
Transmission Control Protocol, Src Port: 35942, Dst Port: 80, Seq: 1, Ack: 1, Len: 310  
Hypertext Transfer Protocol

## Analysis of Captured data in the packets :

```
Wireshark - Follow TCP Stream (tcp.stream eq 21) - Task-5.pcapng

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/webp,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_3GME988535=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: 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: 109
  Identification: 0x14a0 (5280)
  ► 0000 .... = 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: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 2
  Authority RRs: 0
  Additional RRs: 0
```

```

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  ... ..TRT ...5...E

```