Experiment-7 **Date:08/09/2025**

ANALYSIS OF TRAFFIC PACKETS USING WIRESHARK

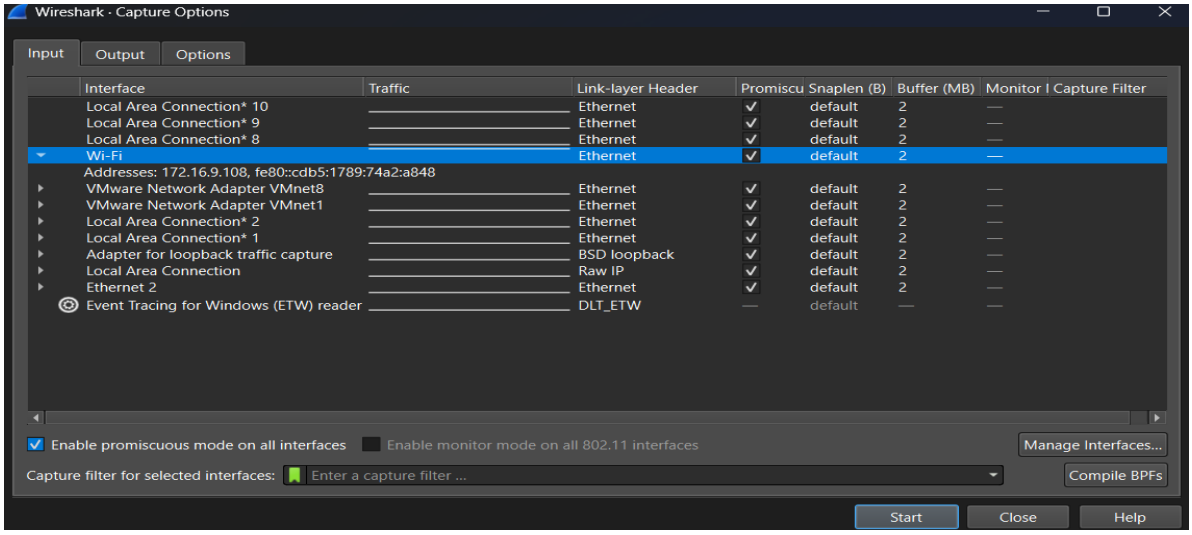
AIM: To capture and analyze network packets using Wireshark, understand the structure of Ethernet, IP, TCP, and HTTP messages, and apply filters for efficient traffic analysis.

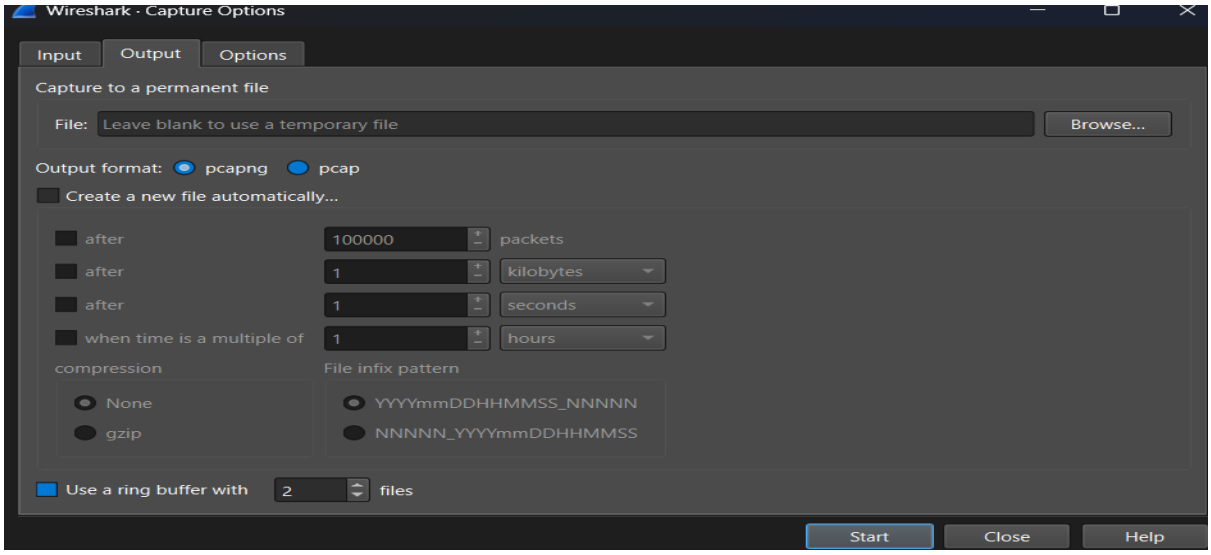
Step-1: Install Wireshark

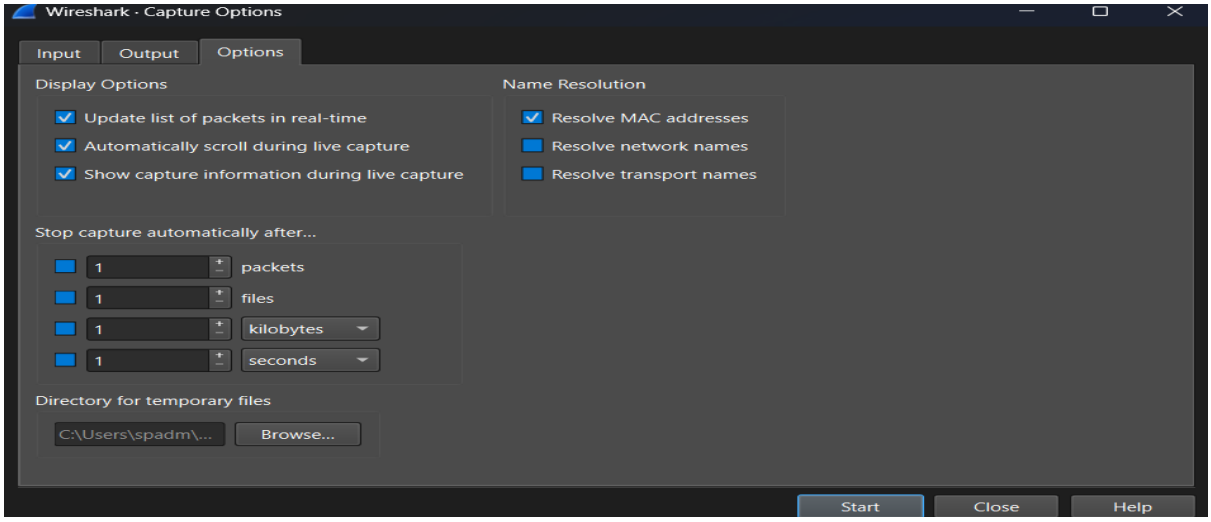
1. Download Wireshark from wireshark.org/download.html.
2. Install required capture library (libpcap/WinPcap).

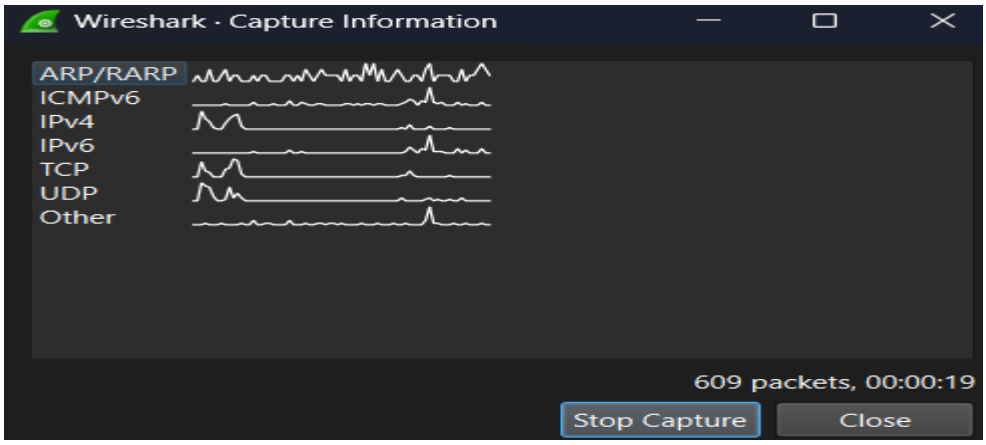
Step-2: Start Wireshark

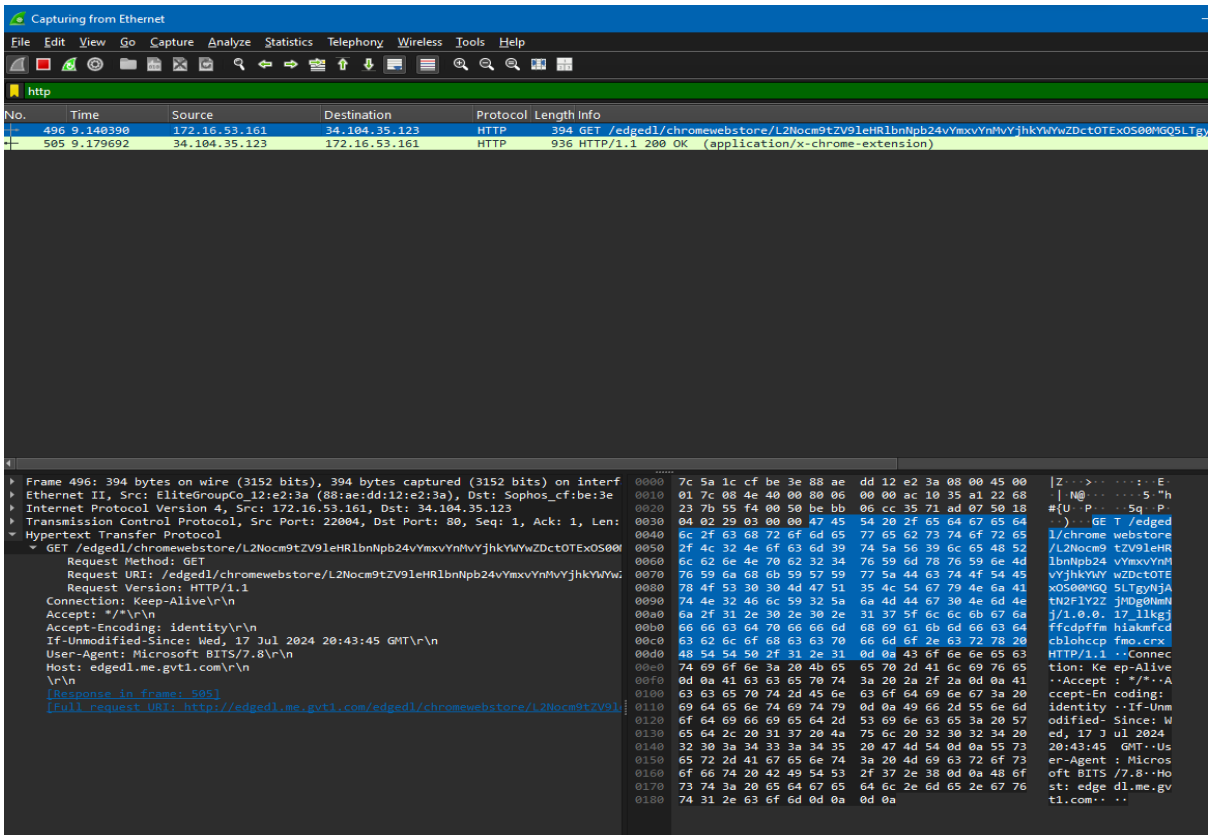
1. Open Wireshark GUI → Choose Capture Interface (Ethernet/Wi-Fi).
2. Start capturing packets





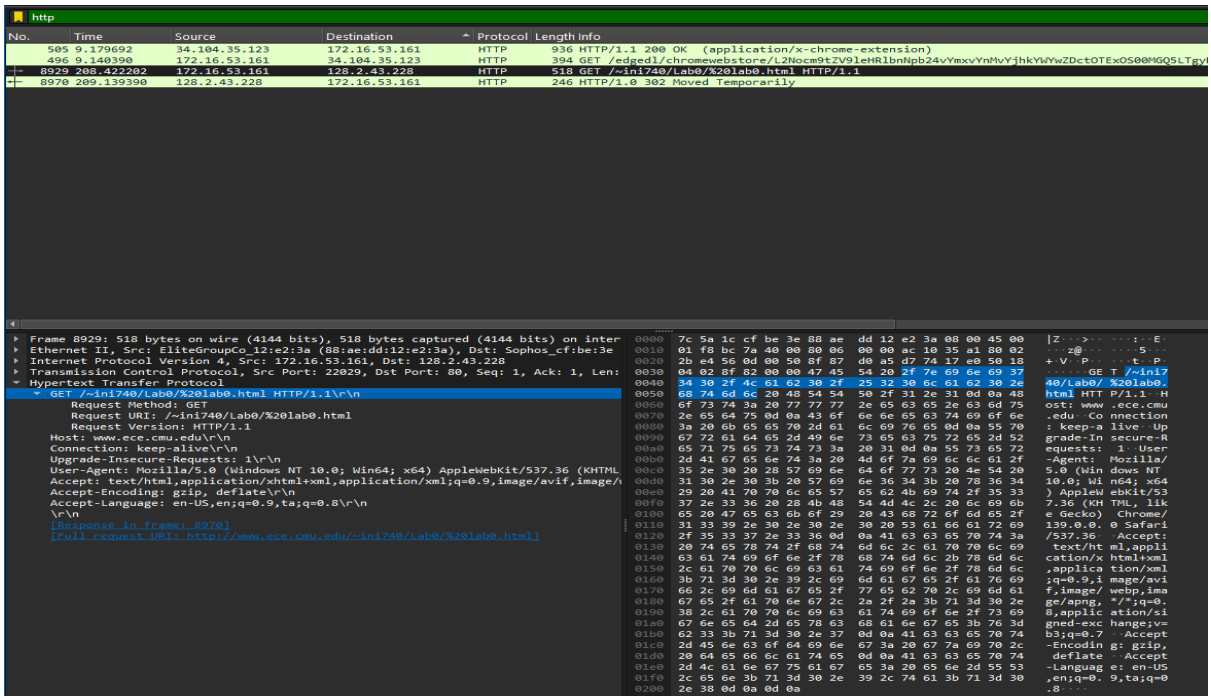

Wireshark · Capture Options
Input
Output
Options
Display Options
Update list of packets in real-time
Automatically scroll during live capture
Show capture information during live capture
Name Resolution
Resolve MAC addresses
Resolve network names
Resolve transport names
Stop capture automatically after...
1
packets
1
files
1
kilobytes
1
seconds
Directory for temporary files
C:\Users\spadm\...
Browse...
Start
Close
Help


Wireshark · Capture Information
ARP/RARP
ICMPv6
IPv4
IPv6
TCP
UDP
Other
609 packets, 00:00:19
Stop Capture
Close


Capturing from Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
496 9.140390 172.16.53.161 34.104.35.123 HTTP 394 GET /edgedl/chromewebstore/L2Nocm9tZV9leHRlbnNpb24vYmxvYnMvYjhkYWYwZDctOTExOS00MGQ5LTgy
505 9.179692 34.104.35.123 172.16.53.161 HTTP 936 HTTP/1.1 200 OK (application/x-chrome-extension)
Frame 496: 394 bytes on wire (3152 bits), 394 bytes captured (3152 bits) on interf
Ethernet II, Src: EliteGroupCo_12:e2:3a (88:ae:dd:12:e2:3a), Dst: Sophos_cf:be:3e
Internet Protocol Version 4, Src: 172.16.53.161, Dst: 34.104.35.123
Transmission Control Protocol, Src Port: 22004, Dst Port: 80, Seq: 1, Ack: 1, Len:
Hypertext Transfer Protocol
GET /edgedl/chromewebstore/L2Nocm9tZV9leHRlbnNpb24vYmxvYnMvYjhkYWYwZDctOTExOS00
Request Method: GET
Request URI: /edgedl/chromewebstore/L2Nocm9tZV9leHRlbnNpb24vYmxvYnMvYjhkYWYw
Request Version: HTTP/1.1
Connection: Keep-Alive\r\n
Accept: */*\r\n
Accept-Encoding: identity\r\n
If-Unmodified-Since: Wed, 17 Jul 2024 20:43:45 GMT\r\n
User-Agent: Microsoft BITS/7.8\r\n
Host: edgedl.me.gvt1.com\r\n
\r\n
[Response in frame: 505]
[Full request URI: http://edgedl.me.gvt1.com/edgedl/chromewebstore/L2Nocm9tZV9l
0000 7c 5a 1c cf be 3e 88 ae dd 12 e2 3a 08 00 45 00 |Z ···>·· ···:··E·
0010 01 7c 08 4e 40 00 80 06 00 00 ac 10 35 a1 22 68 ·|·N@··· ····5·"h
0020 23 7b 55 f4 00 50 be bb 06 cc 35 71 ad 07 50 18 #{U··P·· ··5q··P·
0030 04 02 29 03 00 00 47 45 54 20 2f 65 64 67 65 64 ··)···GE T /edged
0040 6c 2f 63 68 72 6f 6d 65 77 65 62 73 74 6f 72 65 l/chrome webstore
0050 2f 4c 32 4e 6f 63 6d 39 74 5a 56 39 6c 65 48 52 /L2Nocm9 tZV9leHR
0060 6c 62 6e 4e 70 62 32 34 76 59 6d 78 76 59 6e 4d lbnNpb24 vYmxvYnM
0070 76 59 6a 68 6b 59 57 59 77 5a 44 63 74 4f 54 45 vYjhkYWY wZDctOTE
0080 78 4f 53 30 30 4d 47 51 35 4c 54 67 79 4e 6a 41 xOS00MGQ 5LTgyNjA
0090 74 4e 32 46 6c 59 32 5a 6a 4d 44 67 30 4e 6d 4e tN2FlY2Z jMDg0NmN
00a0 6a 2f 31 2e 30 2e 30 2e 31 37 5f 6c 6c 6b 67 6a j/1.0.0. 17_llkgj
00b0 66 66 63 64 70 66 66 6d 68 69 61 6b 6d 66 63 64 ffcdpffm hiakmfcd
00c0 63 62 6c 6f 68 63 63 70 66 6d 6f 2e 63 72 78 20 cblohccp fmo.crx
00d0 48 54 54 50 2f 31 2e 31 0d 0a 43 6f 6e 6e 65 63 HTTP/1.1 ··Connec
00e0 74 69 6f 6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65 tion: Ke ep-Alive
00f0 0d 0a 41 63 63 65 70 74 3a 20 2a 2f 2a 0d 0a 41 ··Accept : */*··A
0100 63 63 65 70 74 2d 45 6e 63 6f 64 69 6e 67 3a 20 ccept-En coding:
0110 69 64 65 6e 74 69 74 79 0d 0a 49 66 2d 55 6e 6d identity ··If-Unm
0120 6f 64 69 66 69 65 64 2d 53 69 6e 63 65 3a 20 57 odified- Since: W
0130 65 64 2c 20 31 37 20 4a 75 6c 20 32 30 32 34 20 ed, 17 J ul 2024
0140 32 30 3a 34 33 3a 34 35 20 47 4d 54 0d 0a 55 73 20:43:45 GMT··Us
0150 65 72 2d 41 67 65 6e 74 3a 20 4d 69 63 72 6f 73 er-Agent : Micros
0160 6f 66 74 20 42 49 54 53 2f 37 2e 38 0d 0a 48 6f oft BITS /7.8··Ho
0170 73 74 3a 20 65 64 67 65 64 6c 2e 6d 65 2e 67 76 st: edge dl.me.gv
0180 74 31 2e 63 6f 6d 0d 0a 0d 0a t1.com·· ··

Step-3: Generate Network Traffic

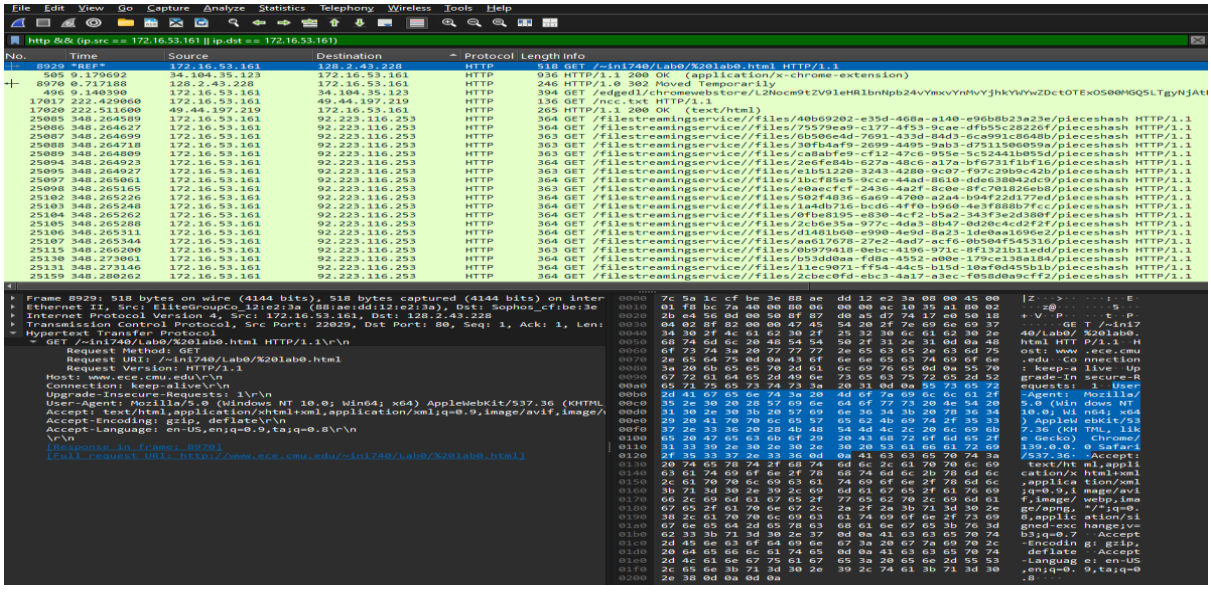
1. Open browser → Visit: http://www.ece.cmu.edu/~ini740/Lab0/lab0.html.
2. Packets exchanged with the HTTP server will be captured.



Step-4: Apply Filters

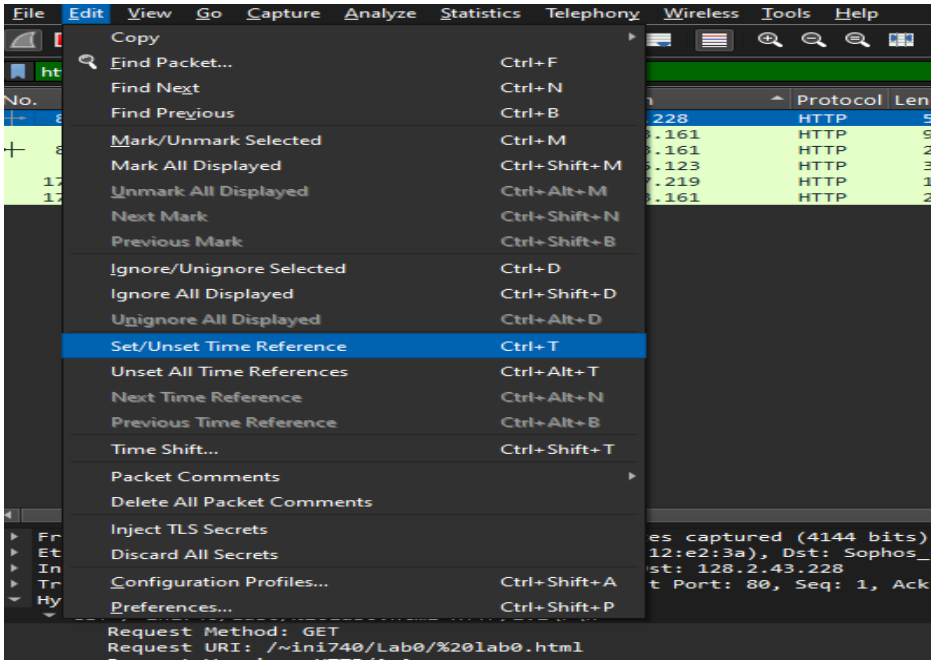
1. In filter bar:
   - http → Show only HTTP traffic.
   - http && (ip.src == YOUR_IP || ip.dst == YOUR_IP) → Show only your traffic.
2. Capture filters (before starting capture):

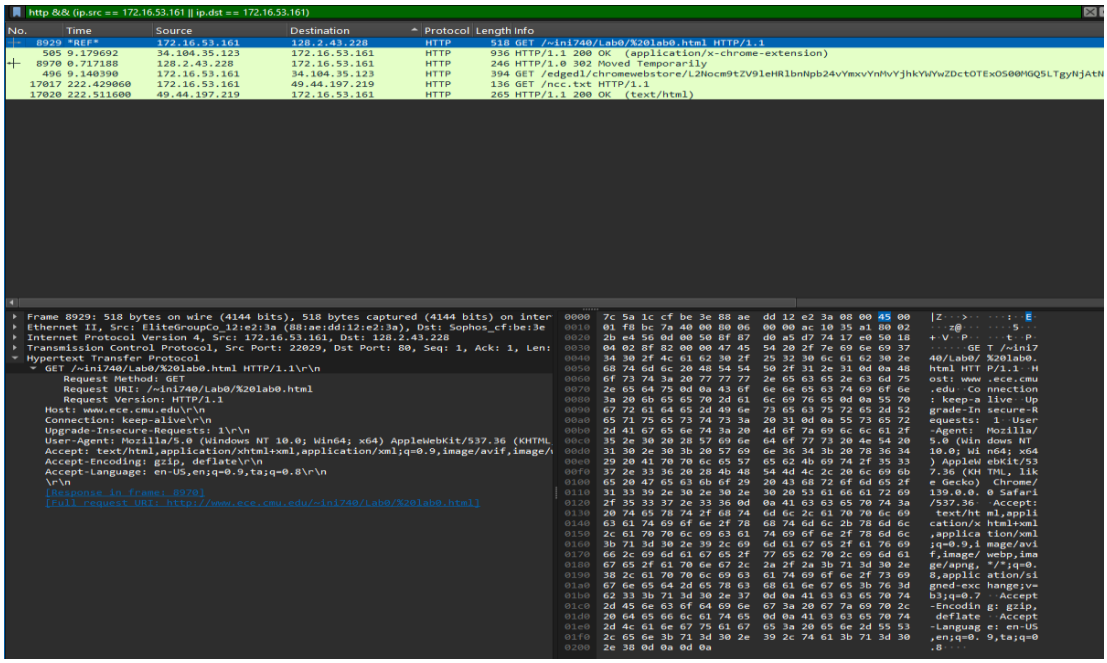
   Example: host 192.168.1.10 → Only capture traffic for a specific host



Step-5: Analyze Packets

1. Select an HTTP GET request.
2. Expand layers:
    - Ethernet Frame → MAC addresses.
    - IP Datagram → Source/Destination IP, TTL, Protocol.
    - TCP Segment → Port numbers, sequence/ack numbers.
    - HTTP Message → Request method (GET/POST), Host header, User-Agent, etc.
3. Note timestamps and calculate Round Trip Time (RTT) using Set Time Reference.





Step-6: Stop packet capture.

RESULT: The wireshark is installed and captured live network traffic and applied filters to isolate HTTP traffic.