VIT

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

LAB ASSESSMENT – 6

COMPUTER NETWORKS
SWE-2002

Vaidya urmila suman

21MIS1098

1) Develop a program that uses the Wireshark API to analyse network traffic and detect specific patterns or signatures, such as known malware traffic or suspicious network behaviour.

Problem Definition:

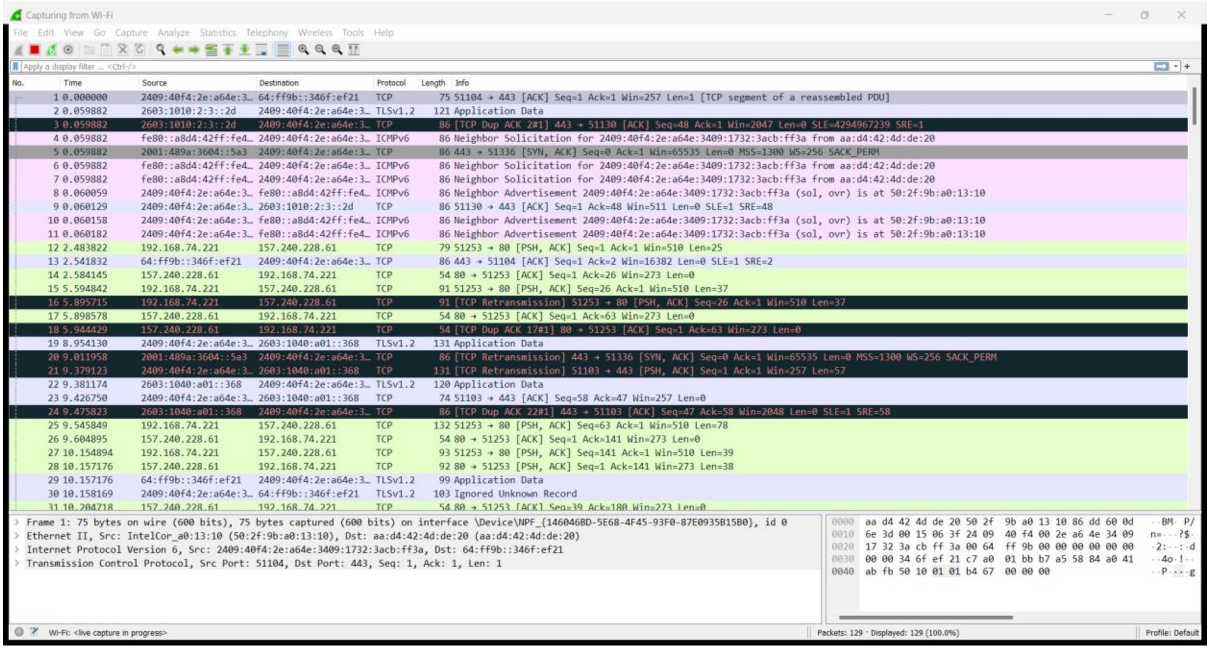
The problem is to develop a program that utilizes the Wireshark API to analyze network traffic and detect specific patterns or signatures, such as known malware traffic or suspicious network behaviour. The objective is to identify and flag packets that exhibit these patterns, allowing for proactive response and mitigation of potential security threats.

Method:

1. Capture Network Packets:

    - Use the Wireshark API to capture network packets from the desired network interface.

    - Set up filters to capture relevant traffic based on protocols, source/destination IP addresses, or ports of interest.


Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  Time       Source              Destination         Protocol Length Info
   1 0.000000   2409:40f4:2e:a64e:3… 64:ff9b::346f:ef21  TCP        75 51104 → 443 [ACK] Seq=1 Ack=1 Win=257 Len=1 [TCP segment of a reassembled PDU]
   2 0.059882   2603:1010:2:3::2d   2409:40f4:2e:a64e:3… TLSv1.2   121 Application Data
   3 0.059882   2603:1010:2:3::2d   2409:40f4:2e:a64e:3… TCP        86 [TCP Dup ACK 2#1] 443 → 51130 [ACK] Seq=48 Ack=1 Win=2047 Len=0 SLE=4294967239 SRE=1
   4 0.059882   fe80::a8d4:42ff:fe4… 2409:40f4:2e:a64e:3… ICMPv6    86 Neighbor Solicitation for 2409:40f4:2e:a64e:3409:1732:3acb:ff3a from aa:d4:42:4d:de:20
   5 0.059882   2001:489a:3604::5a3 2409:40f4:2e:a64e:3… TCP        86 443 → 51336 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1300 WS=256 SACK_PERM
   6 0.059882   fe80::a8d4:42ff:fe4… 2409:40f4:2e:a64e:3… ICMPv6    86 Neighbor Solicitation for 2409:40f4:2e:a64e:3409:1732:3acb:ff3a from aa:d4:42:4d:de:20
   7 0.059882   fe80::a8d4:42ff:fe4… 2409:40f4:2e:a64e:3… ICMPv6    86 Neighbor Solicitation for 2409:40f4:2e:a64e:3409:1732:3acb:ff3a from aa:d4:42:4d:de:20
   8 0.060059   2409:40f4:2e:a64e:3… fe80::a8d4:42ff:fe4… ICMPv6    86 Neighbor Advertisement 2409:40f4:2e:a64e:3409:1732:3acb:ff3a (sol, ovr) is at 50:2f:9b:a0:13:10
   9 0.060129   2409:40f4:2e:a64e:3… 2603:1010:2:3::2d   TCP        86 51130 → 443 [ACK] Seq=1 Ack=48 Win=511 Len=0 SLE=1 SRE=48
  10 0.060158   2409:40f4:2e:a64e:3… fe80::a8d4:42ff:fe4… ICMPv6    86 Neighbor Advertisement 2409:40f4:2e:a64e:3409:1732:3acb:ff3a (sol, ovr) is at 50:2f:9b:a0:13:10
  11 0.060182   2409:40f4:2e:a64e:3… fe80::a8d4:42ff:fe4… ICMPv6    86 Neighbor Advertisement 2409:40f4:2e:a64e:3409:1732:3acb:ff3a (sol, ovr) is at 50:2f:9b:a0:13:10
  12 2.483822   192.168.74.221      157.240.228.61      TCP        79 51253 → 80 [PSH, ACK] Seq=1 Ack=1 Win=510 Len=25
  13 2.541832   64:ff9b::346f:ef21  2409:40f4:2e:a64e:3… TCP        86 443 → 51104 [ACK] Seq=1 Ack=2 Win=16382 Len=0 SLE=1 SRE=2
  14 2.584145   157.240.228.61      192.168.74.221      TCP        54 80 → 51253 [ACK] Seq=1 Ack=26 Win=273 Len=0
  15 5.594842   192.168.74.221      157.240.228.61      TCP        91 51253 → 80 [PSH, ACK] Seq=26 Ack=1 Win=510 Len=37
  16 5.895715   192.168.74.221      157.240.228.61      TCP        91 [TCP Retransmission] 51253 → 80 [PSH, ACK] Seq=26 Ack=1 Win=510 Len=37
  17 5.898578   157.240.228.61      192.168.74.221      TCP        54 80 → 51253 [ACK] Seq=1 Ack=63 Win=273 Len=0
  18 5.944429   157.240.228.61      192.168.74.221      TCP        54 [TCP Dup ACK 17#1] 80 → 51253 [ACK] Seq=1 Ack=63 Win=273 Len=0
  19 8.954130   2409:40f4:2e:a64e:3… 2603:1040:a01::368  TLSv1.2   131 Application Data
  20 9.011958   2001:489a:3604::5a3 2409:40f4:2e:a64e:3… TCP        86 [TCP Retransmission] 443 → 51336 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1300 WS=256 SACK_PERM
  21 9.379123   2409:40f4:2e:a64e:3… 2603:1040:a01::368  TCP       131 [TCP Retransmission] 51103 → 443 [PSH, ACK] Seq=1 Ack=1 Win=257 Len=57
  22 9.381174   2603:1040:a01::368  2409:40f4:2e:a64e:3… TLSv1.2   120 Application Data
  23 9.426750   2409:40f4:2e:a64e:3… 2603:1040:a01::368  TCP        74 51103 → 443 [ACK] Seq=58 Ack=47 Win=257 Len=0
  24 9.475823   2603:1040:a01::368  2409:40f4:2e:a64e:3… TCP        86 [TCP Dup ACK 22#1] 443 → 51103 [ACK] Seq=47 Ack=58 Win=2048 Len=0 SLE=1 SRE=58
  25 9.545849   192.168.74.221      157.240.228.61      TCP       132 51253 → 80 [PSH, ACK] Seq=63 Ack=1 Win=510 Len=78
  26 9.604895   157.240.228.61      192.168.74.221      TCP        54 80 → 51253 [ACK] Seq=1 Ack=141 Win=273 Len=0
  27 10.154894  192.168.74.221      157.240.228.61      TCP        93 51253 → 80 [PSH, ACK] Seq=141 Ack=1 Win=510 Len=39
  28 10.157176  157.240.228.61      192.168.74.221      TCP        92 80 → 51253 [PSH, ACK] Seq=1 Ack=141 Win=273 Len=38
  29 10.157176  64:ff9b::346f:ef21  2409:40f4:2e:a64e:3… TLSv1.2    99 Application Data
  30 10.158169  2409:40f4:2e:a64e:3… 64:ff9b::346f:ef21  TLSv1.2   103 Ignored Unknown Record
  31 10.204718  157.240.228.61      192.168.74.221      TCP        54 80 → 51253 [ACK] Seq=39 Ack=180 Win=273 Len=0
```

```
> Frame 1: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface \Device\NPF_{146046BD-5E68-4F45-93F0-87E0935B15B0}, id 0
> Ethernet II, Src: IntelCor_a0:13:10 (50:2f:9b:a0:13:10), Dst: aa:d4:42:4d:de:20 (aa:d4:42:4d:de:20)
> Internet Protocol Version 6, Src: 2409:40f4:2e:a64e:3409:1732:3acb:ff3a, Dst: 64:ff9b::346f:ef21
> Transmission Control Protocol, Src Port: 51104, Dst Port: 443, Seq: 1, Ack: 1, Len: 1
```

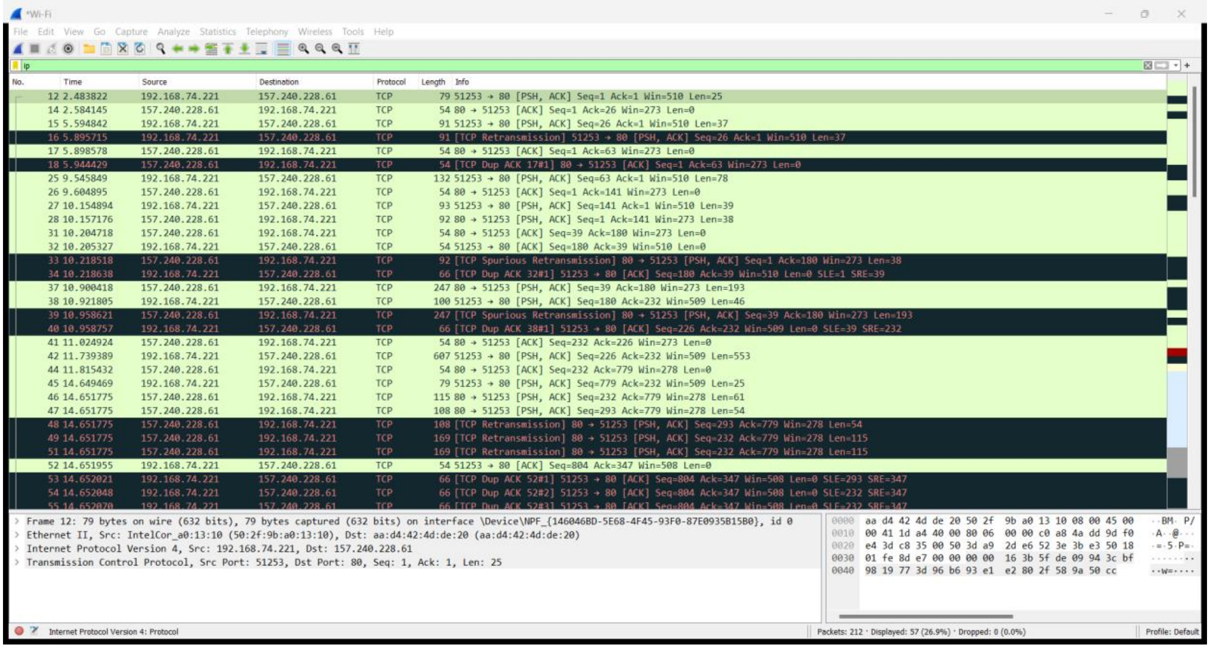
```
0000  aa d4 42 4d de 20 50 2f  9b a0 13 10 86 dd 60 0d   ··BM· P/
0010  6e 3d 00 15 06 3f 24 09  40 f4 00 2e a6 4e 34 09   n=···?$·
0020  17 32 3a cb ff 3a 00 64  ff 9b 00 00 00 00 00 00   ·2:··:·d
0030  00 00 34 6f ef 21 c7 a0  01 bb b7 a5 58 84 a0 41   ··4o·!··
0040  ab fb 50 10 01 01 b4 67  00 00 00                  ··P···g
```

```
Wi-Fi: <live capture in progress>    Packets: 129 · Displayed: 129 (100.0%)    Profile: Default
```

1. Identify Specific Patterns or Signatures:

    - Define the specific patterns or signatures you want to detect, such as known malware traffic or suspicious network behaviors.

    - This can include analyzing the content of packets, packet headers, or patterns associated with specific protocols.

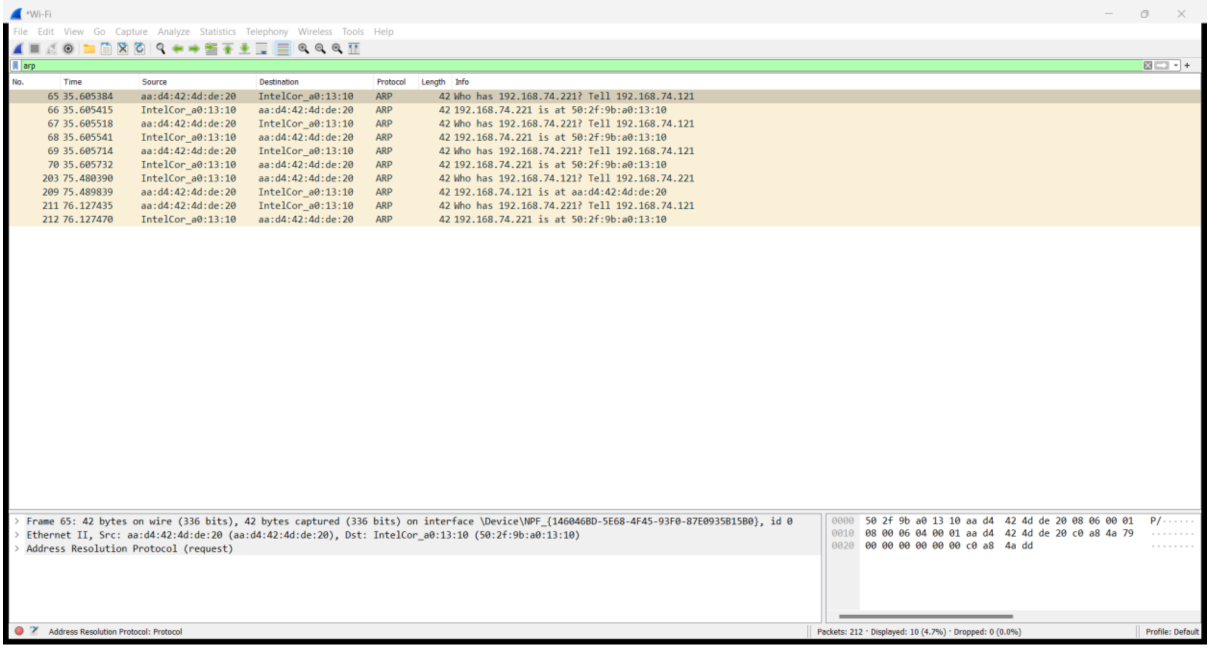

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip

```
No.   Time       Source          Destination     Protocol Length Info
   12 2.483822   192.168.74.221  157.240.228.61  TCP      79 51253 → 80 [PSH, ACK] Seq=1 Ack=1 Win=510 Len=25
   14 2.584145   157.240.228.61  192.168.74.221  TCP      54 80 → 51253 [ACK] Seq=1 Ack=26 Win=273 Len=0
   15 5.594842   192.168.74.221  157.240.228.61  TCP      91 51253 → 80 [PSH, ACK] Seq=26 Ack=1 Win=510 Len=37
   16 5.895715   192.168.74.221  157.240.228.61  TCP      91 [TCP Retransmission] 51253 → 80 [PSH, ACK] Seq=26 Ack=1 Win=510 Len=37
   17 5.898578   157.240.228.61  192.168.74.221  TCP      54 80 → 51253 [ACK] Seq=1 Ack=63 Win=273 Len=0
   18 5.944429   157.240.228.61  192.168.74.221  TCP      54 [TCP Dup ACK 17#1] 80 → 51253 [ACK] Seq=1 Ack=63 Win=273 Len=0
   25 9.545849   192.168.74.221  157.240.228.61  TCP     132 51253 → 80 [PSH, ACK] Seq=63 Ack=1 Win=510 Len=78
   26 9.604895   157.240.228.61  192.168.74.221  TCP      54 80 → 51253 [ACK] Seq=1 Ack=141 Win=273 Len=0
   27 10.154894  192.168.74.221  157.240.228.61  TCP      93 51253 → 80 [PSH, ACK] Seq=141 Ack=1 Win=510 Len=39
   28 10.157176  157.240.228.61  192.168.74.221  TCP      92 80 → 51253 [PSH, ACK] Seq=1 Ack=141 Win=273 Len=38
   31 10.204718  157.240.228.61  192.168.74.221  TCP      54 80 → 51253 [ACK] Seq=39 Ack=180 Win=273 Len=0
   32 10.205327  192.168.74.221  157.240.228.61  TCP      54 51253 → 80 [ACK] Seq=180 Ack=39 Win=510 Len=0
   33 10.218518  157.240.228.61  192.168.74.221  TCP      92 [TCP Spurious Retransmission] 80 → 51253 [PSH, ACK] Seq=1 Ack=180 Win=273 Len=38
   34 10.218638  192.168.74.221  157.240.228.61  TCP      66 [TCP Dup ACK 32#1] 51253 → 80 [ACK] Seq=180 Ack=39 Win=510 Len=0 SLE=1 SRE=39
   37 10.900418  157.240.228.61  192.168.74.221  TCP     247 80 → 51253 [PSH, ACK] Seq=39 Ack=180 Win=273 Len=193
   38 10.921805  192.168.74.221  157.240.228.61  TCP     100 51253 → 80 [PSH, ACK] Seq=180 Ack=232 Win=509 Len=46
   39 10.958621  157.240.228.61  192.168.74.221  TCP     247 [TCP Spurious Retransmission] 80 → 51253 [PSH, ACK] Seq=39 Ack=180 Win=273 Len=193
   40 10.958757  192.168.74.221  157.240.228.61  TCP      66 [TCP Dup ACK 38#1] 51253 → 80 [ACK] Seq=226 Ack=232 Win=509 Len=0 SLE=39 SRE=232
   41 11.024924  157.240.228.61  192.168.74.221  TCP      54 80 → 51253 [ACK] Seq=232 Ack=226 Win=273 Len=0
   42 11.739389  192.168.74.221  157.240.228.61  TCP     607 51253 → 80 [PSH, ACK] Seq=226 Ack=232 Win=509 Len=553
   44 11.815432  157.240.228.61  192.168.74.221  TCP      54 80 → 51253 [ACK] Seq=232 Ack=779 Win=278 Len=0
   45 14.649469  192.168.74.221  157.240.228.61  TCP      79 51253 → 80 [PSH, ACK] Seq=779 Ack=232 Win=509 Len=25
   46 14.651775  157.240.228.61  192.168.74.221  TCP     115 80 → 51253 [PSH, ACK] Seq=232 Ack=779 Win=278 Len=61
   47 14.651775  157.240.228.61  192.168.74.221  TCP     108 80 → 51253 [PSH, ACK] Seq=293 Ack=779 Win=278 Len=54
   48 14.651775  157.240.228.61  192.168.74.221  TCP     108 [TCP Retransmission] 80 → 51253 [PSH, ACK] Seq=293 Ack=779 Win=278 Len=54
   49 14.651775  157.240.228.61  192.168.74.221  TCP     169 [TCP Retransmission] 80 → 51253 [PSH, ACK] Seq=232 Ack=779 Win=278 Len=115
   51 14.651775  157.240.228.61  192.168.74.221  TCP     169 [TCP Retransmission] 80 → 51253 [PSH, ACK] Seq=232 Ack=779 Win=278 Len=115
   52 14.651955  192.168.74.221  157.240.228.61  TCP      54 51253 → 80 [ACK] Seq=804 Ack=347 Win=508 Len=0
   53 14.652021  192.168.74.221  157.240.228.61  TCP      66 [TCP Dup ACK 52#1] 51253 → 80 [ACK] Seq=804 Ack=347 Win=508 Len=0 SLE=293 SRE=347
   54 14.652048  192.168.74.221  157.240.228.61  TCP      66 [TCP Dup ACK 52#2] 51253 → 80 [ACK] Seq=804 Ack=347 Win=508 Len=0 SLE=232 SRE=347
   55 14.652070  192.168.74.221  157.240.228.61  TCP      66 [TCP Dup ACK 52#3] 51253 → 80 [ACK] Seq=804 Ack=347 Win=508 Len=0 SLE=232 SRE=347
```

```
> Frame 12: 79 bytes on wire (632 bits), 79 bytes captured (632 bits) on interface \Device\NPF_{146046BD-5E68-4F45-93F0-87E0935B15B0}, id 0
> Ethernet II, Src: IntelCor_a0:13:10 (50:2f:9b:a0:13:10), Dst: aa:d4:42:4d:de:20 (aa:d4:42:4d:de:20)
> Internet Protocol Version 4, Src: 192.168.74.221, Dst: 157.240.228.61
> Transmission Control Protocol, Src Port: 51253, Dst Port: 80, Seq: 1, Ack: 1, Len: 25
```

```
0000  aa d4 42 4d de 20 50 2f  9b a0 13 10 08 00 45 00   ··BM· P/
0010  00 41 1d a4 40 00 80 06  00 00 c0 a8 4a dd 9d f0   ·A··@···
0020  e4 3d c8 35 00 50 3d a9  2d e6 52 3e 3b e3 50 18   ·=·5·P=·
0030  01 fe 8d e7 00 00 00 00  16 3b 5f de 09 94 3c bf   ········
0040  98 19 77 3d 96 b6 93 e1  e2 80 2f 58 9a 50 cc      ··w=····
```

Internet Protocol Version 4: Protocol | Packets: 212 · Displayed: 57 (26.9%) · Dropped: 0 (0.0%) | Profile: Default


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
arp

```
No.   Time       Source             Destination        Protocol Length Info
   65 35.605384  aa:d4:42:4d:de:20  IntelCor_a0:13:10  ARP      42 Who has 192.168.74.221? Tell 192.168.74.121
   66 35.605415  IntelCor_a0:13:10  aa:d4:42:4d:de:20  ARP      42 192.168.74.221 is at 50:2f:9b:a0:13:10
   67 35.605518  aa:d4:42:4d:de:20  IntelCor_a0:13:10  ARP      42 Who has 192.168.74.221? Tell 192.168.74.121
   68 35.605541  IntelCor_a0:13:10  aa:d4:42:4d:de:20  ARP      42 192.168.74.221 is at 50:2f:9b:a0:13:10
   69 35.605714  aa:d4:42:4d:de:20  IntelCor_a0:13:10  ARP      42 Who has 192.168.74.221? Tell 192.168.74.121
   70 35.605732  IntelCor_a0:13:10  aa:d4:42:4d:de:20  ARP      42 192.168.74.221 is at 50:2f:9b:a0:13:10
  203 75.480390  IntelCor_a0:13:10  aa:d4:42:4d:de:20  ARP      42 Who has 192.168.74.121? Tell 192.168.74.221
  209 75.489839  aa:d4:42:4d:de:20  IntelCor_a0:13:10  ARP      42 192.168.74.121 is at aa:d4:42:4d:de:20
  211 76.127435  aa:d4:42:4d:de:20  IntelCor_a0:13:10  ARP      42 Who has 192.168.74.221? Tell 192.168.74.121
  212 76.127470  IntelCor_a0:13:10  aa:d4:42:4d:de:20  ARP      42 192.168.74.221 is at 50:2f:9b:a0:13:10
```

```
> Frame 65: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{146046BD-5E68-4F45-93F0-87E0935B15B0}, id 0
> Ethernet II, Src: aa:d4:42:4d:de:20 (aa:d4:42:4d:de:20), Dst: IntelCor_a0:13:10 (50:2f:9b:a0:13:10)
> Address Resolution Protocol (request)
```

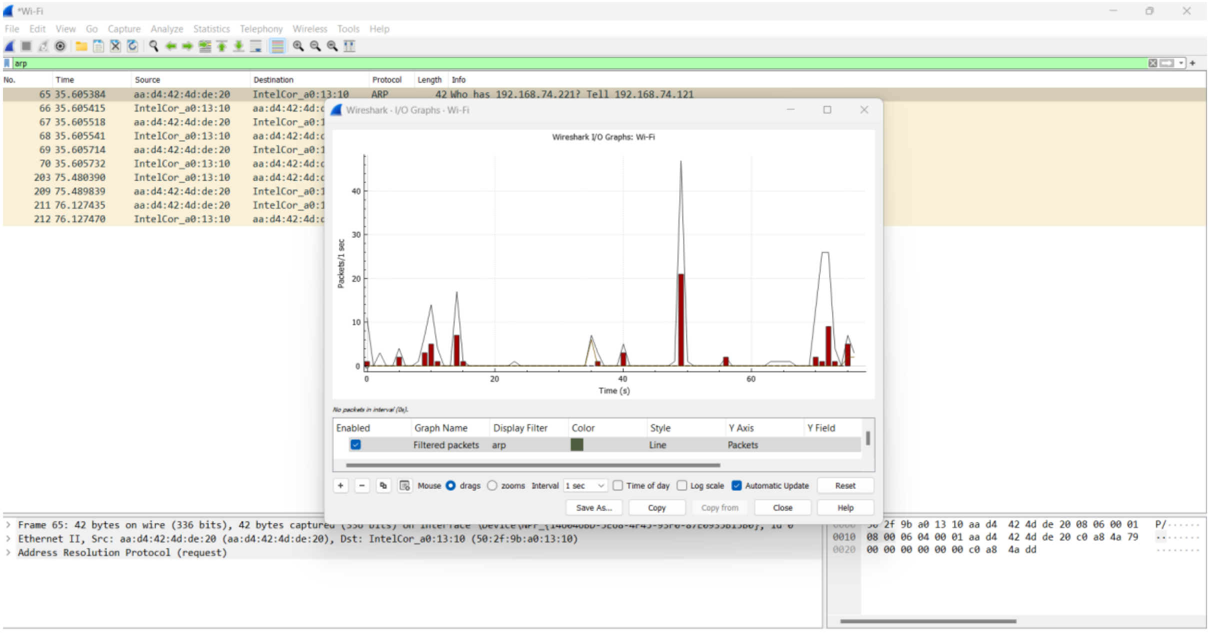
```
0000  50 2f 9b a0 13 10 aa d4  42 4d de 20 08 06 00 01   P/······
0010  08 00 06 04 00 01 aa d4  42 4d de 20 c0 a8 4a 79   ········
0020  00 00 00 00 00 00 c0 a8  4a dd                     ········
```

Address Resolution Protocol: Protocol | Packets: 212 · Displayed: 10 (4.7%) · Dropped: 0 (0.0%) | Profile: Default

2. Statistical Analysis for Anomaly Detection:

   - Utilize statistical analysis techniques to identify anomalies in the captured network traffic.

- Calculate statistical metrics like mean, standard deviation, or entropy for relevant attributes of the packets.
- Compare these metrics against established thresholds or baselines to flag packets that deviate significantly.


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireshark · I/O Graphs · Wi-Fi
Wireshark I/O Graphs: Wi-Fi
Packets/1 sec
0
10
20
30
40
Time (s)
0
20
40
60
Mouse
drags
zooms
Interval
Reset
Save As...
Copy
Copy from
Close
Help

arp

```
No.   Time       Source              Destination         Protocol Length Info
   65 35.605384  aa:d4:42:4d:de:20   IntelCor_a0:13:10   ARP          42 Who has 192.168.74.221? Tell 192.168.74.121
   66 35.605415  IntelCor_a0:13:10   aa:d4:42:4d:c
   67 35.605518  aa:d4:42:4d:de:20   IntelCor_a0:1
   68 35.605541  IntelCor_a0:13:10   aa:d4:42:4d:c
   69 35.605714  aa:d4:42:4d:de:20   IntelCor_a0:1
   70 35.605732  IntelCor_a0:13:10   aa:d4:42:4d:c
  203 75.480390  IntelCor_a0:13:10   aa:d4:42:4d:c
  209 75.489839  aa:d4:42:4d:de:20   IntelCor_a0:1
  211 76.127435  aa:d4:42:4d:de:20   IntelCor_a0:1
  212 76.127470  IntelCor_a0:13:10   aa:d4:42:4d:c
```

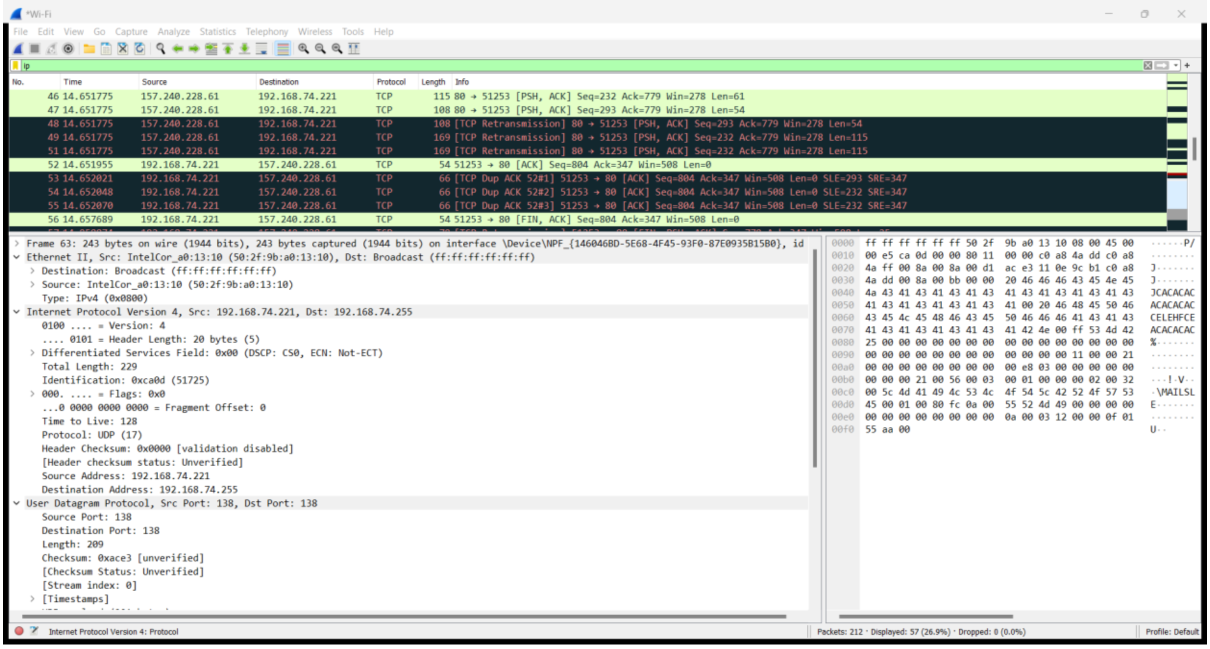
No packets in interval (0s).

Enabled	Graph Name	Display Filter	Color	Style	Y Axis	Y Field
☑	Filtered packets	arp	🟩	Line	Packets	

+ − ● drags ○ zooms Interval 1 sec □ Time of day □ Log scale ☑ Automatic Update

```
> Frame 65: 42 bytes on wire (336 bits), 42 bytes captured
> Ethernet II, Src: aa:d4:42:4d:de:20 (aa:d4:42:4d:de:20), Dst: IntelCor_a0:13:10 (50:2f:9b:a0:13:10)
> Address Resolution Protocol (request)
```

```
     2f 9b a0 13 10 aa d4  42 4d de 20 08 06 00 01   P/······
0010 08 00 06 04 00 01 aa d4  42 4d de 20 c0 a8 4a 79   ········
0020 00 00 00 00 00 00 c0 a8  4a dd                     ········
```


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip

```
No.   Time       Source          Destination     Protocol Length Info
   46 14.651775  157.240.228.61  192.168.74.221  TCP      115 80 → 51253 [PSH, ACK] Seq=232 Ack=779 Win=278 Len=61
   47 14.651775  157.240.228.61  192.168.74.221  TCP      108 80 → 51253 [PSH, ACK] Seq=293 Ack=779 Win=278 Len=54
   48 14.651775  157.240.228.61  192.168.74.221  TCP      108 [TCP Retransmission] 80 → 51253 [PSH, ACK] Seq=293 Ack=779 Win=278 Len=54
   49 14.651775  157.240.228.61  192.168.74.221  TCP      169 [TCP Retransmission] 80 → 51253 [PSH, ACK] Seq=232 Ack=779 Win=278 Len=115
   51 14.651775  157.240.228.61  192.168.74.221  TCP      169 [TCP Retransmission] 80 → 51253 [PSH, ACK] Seq=232 Ack=779 Win=278 Len=115
   52 14.651955  192.168.74.221  157.240.228.61  TCP       54 51253 → 80 [ACK] Seq=804 Ack=347 Win=508 Len=0
   53 14.652021  192.168.74.221  157.240.228.61  TCP       66 [TCP Dup ACK 52#1] 51253 → 80 [ACK] Seq=804 Ack=347 Win=508 Len=0 SLE=293 SRE=347
   54 14.652048  192.168.74.221  157.240.228.61  TCP       66 [TCP Dup ACK 52#2] 51253 → 80 [ACK] Seq=804 Ack=347 Win=508 Len=0 SLE=232 SRE=347
   55 14.652070  192.168.74.221  157.240.228.61  TCP       66 [TCP Dup ACK 52#3] 51253 → 80 [ACK] Seq=804 Ack=347 Win=508 Len=0 SLE=232 SRE=347
   56 14.657689  192.168.74.221  157.240.228.61  TCP       54 51253 → 80 [FIN, ACK] Seq=804 Ack=347 Win=508 Len=0
```

```
> Frame 63: 243 bytes on wire (1944 bits), 243 bytes captured (1944 bits) on interface \Device\NPF_{146046BD-5E68-4F45-93F0-87E0935B15B0}, id
v Ethernet II, Src: IntelCor_a0:13:10 (50:2f:9b:a0:13:10), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  > Source: IntelCor_a0:13:10 (50:2f:9b:a0:13:10)
    Type: IPv4 (0x0800)
v Internet Protocol Version 4, Src: 192.168.74.221, Dst: 192.168.74.255
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 229
    Identification: 0xca0d (51725)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.74.221
    Destination Address: 192.168.74.255
v User Datagram Protocol, Src Port: 138, Dst Port: 138
    Source Port: 138
    Destination Port: 138
    Length: 209
    Checksum: 0xace3 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
  > [Timestamps]
```

```
0000 ff ff ff ff ff ff 50 2f  9b a0 13 10 08 00 45 00   ······P/
0010 00 e5 ca 0d 00 00 80 11  00 00 c0 a8 4a dd c0 a8   ········
0020 4a ff 00 8a 00 8a 00 d1  ac e3 11 0e 9c b1 c0 a8   J·······
0030 4a dd 00 8a 00 bb 00 00  20 46 46 46 43 45 4e 45   J·······
0040 4a 43 41 43 41 43 41 43  41 43 41 43 41 43 41 43   JCACACAC
0050 41 43 41 43 41 43 41 43  41 00 20 46 48 45 50 46   ACACACAC
0060 43 45 4c 45 48 46 43 45  50 46 46 46 41 43 41 43   CELEHFCE
0070 41 43 41 43 41 43 41 43  41 42 4e 00 ff 53 4d 42   ACACACAC
0080 25 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   %·······
0090 00 00 00 00 00 00 00 00  00 00 00 00 11 00 00 21   ········
00a0 00 00 00 00 00 00 00 00  00 e8 03 00 00 00 00 00   ········
00b0 00 00 00 21 00 56 00 03  00 01 00 00 00 02 00 32   ···!·V··
00c0 00 5c 4d 41 49 4c 53 4c  4f 54 5c 42 52 4f 57 53   ·\MAILSL
00d0 45 00 01 00 80 fc 0a 00  55 52 4d 49 00 00 00 00   E·······
00e0 00 00 00 00 00 00 00 00  0a 00 03 12 00 00 0f 01   ········
00f0 55 aa 00                                           U··
```

Internet Protocol Version 4: Protocol

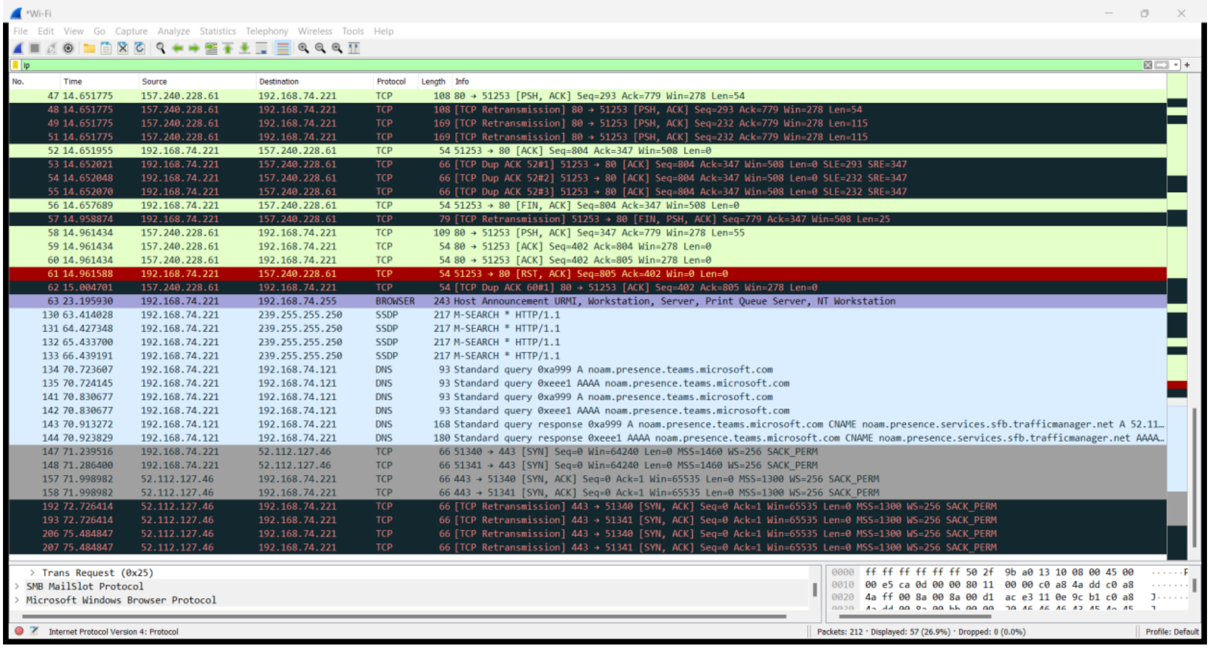
Packets: 212 · Displayed: 57 (26.9%) · Dropped: 0 (0.0%)

Profile: Default

3. Packet Coloring:

    - Implement packet coloring based on specific criteria to visually highlight packets of interest.

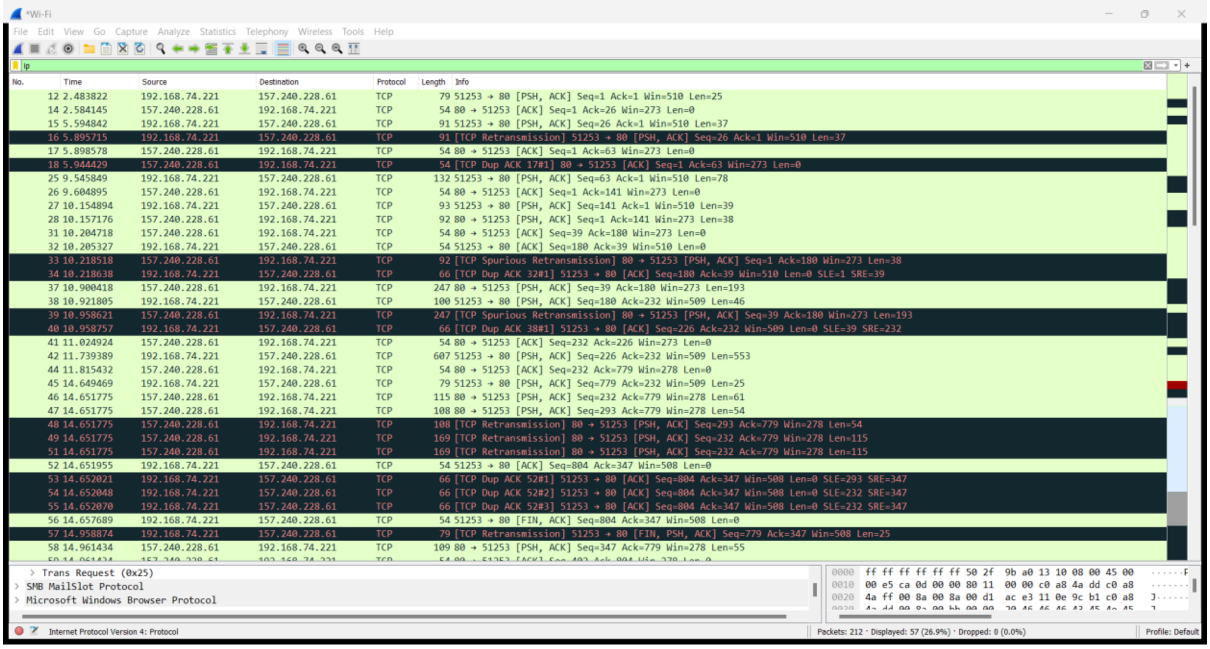
- Apply colors to packets that match specific patterns, signatures, or exhibit suspicious behavior.
- Packet coloring can help in quickly identifying and focusing on relevant packets during analysis.



*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip

```
No.   Time       Source          Destination     Protocol Length Info
   47 14.651775  157.240.228.61  192.168.74.221  TCP      108 80 → 51253 [PSH, ACK] Seq=293 Ack=779 Win=278 Len=54
   48 14.651775  157.240.228.61  192.168.74.221  TCP      108 [TCP Retransmission] 80 → 51253 [PSH, ACK] Seq=293 Ack=779 Win=278 Len=54
   49 14.651775  157.240.228.61  192.168.74.221  TCP      169 [TCP Retransmission] 80 → 51253 [PSH, ACK] Seq=232 Ack=779 Win=278 Len=115
   51 14.651775  157.240.228.61  192.168.74.221  TCP      169 [TCP Retransmission] 80 → 51253 [PSH, ACK] Seq=232 Ack=779 Win=278 Len=115
   52 14.651955  192.168.74.221  157.240.228.61  TCP       54 51253 → 80 [ACK] Seq=804 Ack=347 Win=508 Len=0
   53 14.652021  192.168.74.221  157.240.228.61  TCP       66 [TCP Dup ACK 52#1] 51253 → 80 [ACK] Seq=804 Ack=347 Win=508 Len=0 SLE=293 SRE=347
   54 14.652048  192.168.74.221  157.240.228.61  TCP       66 [TCP Dup ACK 52#2] 51253 → 80 [ACK] Seq=804 Ack=347 Win=508 Len=0 SLE=232 SRE=347
   55 14.652070  192.168.74.221  157.240.228.61  TCP       66 [TCP Dup ACK 52#3] 51253 → 80 [ACK] Seq=804 Ack=347 Win=508 Len=0 SLE=232 SRE=347
   56 14.657689  192.168.74.221  157.240.228.61  TCP       54 51253 → 80 [FIN, ACK] Seq=804 Ack=347 Win=508 Len=0
   57 14.958874  192.168.74.221  157.240.228.61  TCP       79 [TCP Retransmission] 51253 → 80 [FIN, PSH, ACK] Seq=779 Ack=347 Win=508 Len=25
   58 14.961434  157.240.228.61  192.168.74.221  TCP      109 80 → 51253 [PSH, ACK] Seq=347 Ack=779 Win=278 Len=55
   59 14.961434  157.240.228.61  192.168.74.221  TCP       54 80 → 51253 [ACK] Seq=402 Ack=804 Win=278 Len=0
   60 14.961434  157.240.228.61  192.168.74.221  TCP       54 80 → 51253 [ACK] Seq=402 Ack=805 Win=278 Len=0
   61 14.961588  192.168.74.221  157.240.228.61  TCP       54 51253 → 80 [RST, ACK] Seq=805 Ack=402 Win=0 Len=0
   62 15.004701  157.240.228.61  192.168.74.221  TCP       54 [TCP Dup ACK 60#1] 80 → 51253 [ACK] Seq=402 Ack=805 Win=278 Len=0
   63 23.195930  192.168.74.221  192.168.74.255  BROWSER  243 Host Announcement URMI, Workstation, Server, Print Queue Server, NT Workstation
  130 63.414028  192.168.74.221  239.255.255.250 SSDP     217 M-SEARCH * HTTP/1.1
  131 64.427348  192.168.74.221  239.255.255.250 SSDP     217 M-SEARCH * HTTP/1.1
  132 65.433700  192.168.74.221  239.255.255.250 SSDP     217 M-SEARCH * HTTP/1.1
  133 66.439191  192.168.74.221  239.255.255.250 SSDP     217 M-SEARCH * HTTP/1.1
  134 70.723607  192.168.74.221  192.168.74.121  DNS       93 Standard query 0xa999 A noam.presence.teams.microsoft.com
  135 70.724145  192.168.74.221  192.168.74.121  DNS       93 Standard query 0xeee1 AAAA noam.presence.teams.microsoft.com
  141 70.830677  192.168.74.221  192.168.74.121  DNS       93 Standard query 0xa999 A noam.presence.teams.microsoft.com
  142 70.830677  192.168.74.221  192.168.74.121  DNS       93 Standard query 0xeee1 AAAA noam.presence.teams.microsoft.com
  143 70.913272  192.168.74.121  192.168.74.221  DNS      168 Standard query response 0xa999 A noam.presence.teams.microsoft.com CNAME noam.presence.services.sfb.trafficmanager.net A 52.11…
  144 70.923829  192.168.74.121  192.168.74.221  DNS      180 Standard query response 0xeee1 AAAA noam.presence.teams.microsoft.com CNAME noam.presence.services.sfb.trafficmanager.net AAAA…
  147 71.239516  192.168.74.221  52.112.127.46   TCP       66 51340 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
  148 71.286400  192.168.74.221  52.112.127.46   TCP       66 51341 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
  157 71.998982  52.112.127.46   192.168.74.221  TCP       66 443 → 51340 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1300 WS=256 SACK_PERM
  158 71.998982  52.112.127.46   192.168.74.221  TCP       66 443 → 51341 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1300 WS=256 SACK_PERM
  192 72.726414  52.112.127.46   192.168.74.221  TCP       66 [TCP Retransmission] 443 → 51340 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1300 WS=256 SACK_PERM
  193 72.726414  52.112.127.46   192.168.74.221  TCP       66 [TCP Retransmission] 443 → 51341 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1300 WS=256 SACK_PERM
  206 75.484847  52.112.127.46   192.168.74.221  TCP       66 [TCP Retransmission] 443 → 51340 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1300 WS=256 SACK_PERM
  207 75.484847  52.112.127.46   192.168.74.221  TCP       66 [TCP Retransmission] 443 → 51341 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1300 WS=256 SACK_PERM
```

```
    > Trans Request (0x25)
  > SMB MailSlot Protocol
  > Microsoft Windows Browser Protocol

0000  ff ff ff ff ff ff 50 2f  9b a0 13 10 08 00 45 00   ······P
0010  00 e5 ca 0d 00 00 80 11  00 00 c0 a8 4a dd c0 a8   ········
0020  4a ff 00 8a 00 8a 00 d1  ac e3 11 0e 9c b1 c0 a8   J·······

Internet Protocol Version 4: Protocol     Packets: 212 · Displayed: 57 (26.9%) · Dropped: 0 (0.0%)     Profile: Default
```



*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip

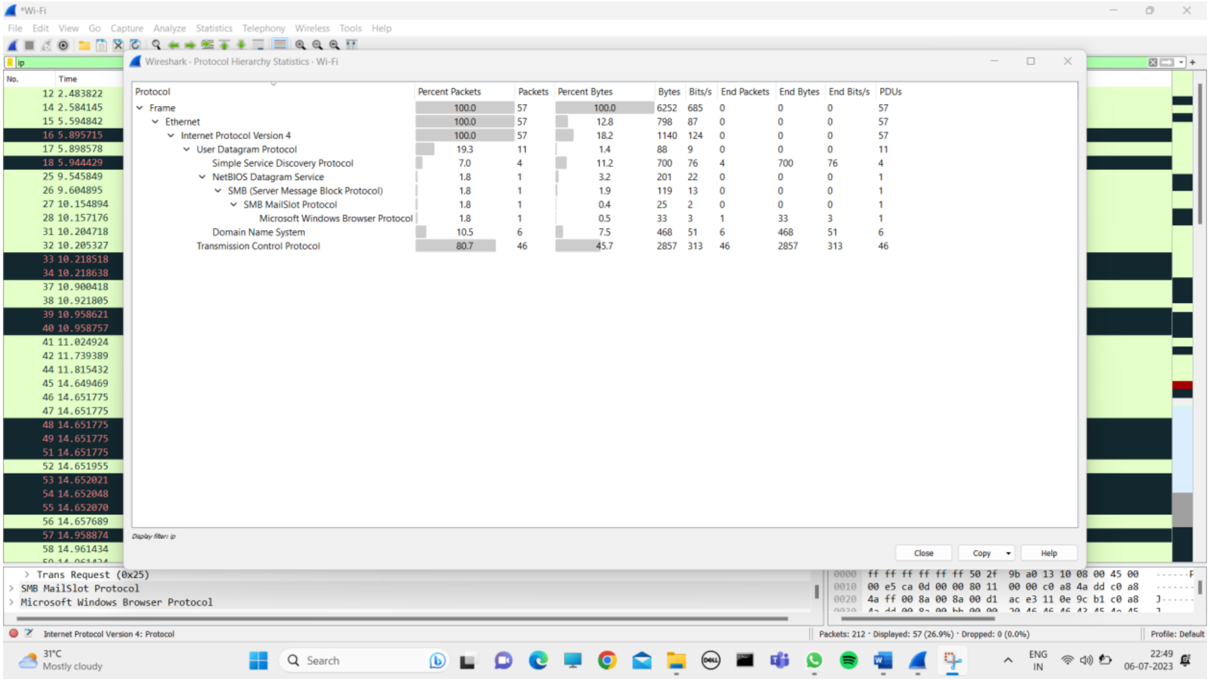
```
No.   Time       Source          Destination     Protocol Length Info
   12 2.483822   192.168.74.221  157.240.228.61  TCP       79 51253 → 80 [PSH, ACK] Seq=1 Ack=1 Win=510 Len=25
   14 2.584145   157.240.228.61  192.168.74.221  TCP       54 80 → 51253 [ACK] Seq=1 Ack=26 Win=273 Len=0
   15 5.594842   192.168.74.221  157.240.228.61  TCP       91 51253 → 80 [PSH, ACK] Seq=26 Ack=1 Win=510 Len=37
   16 5.895715   192.168.74.221  157.240.228.61  TCP       91 [TCP Retransmission] 51253 → 80 [PSH, ACK] Seq=26 Ack=1 Win=510 Len=37
   17 5.898578   157.240.228.61  192.168.74.221  TCP       54 80 → 51253 [ACK] Seq=1 Ack=63 Win=273 Len=0
   18 5.944429   157.240.228.61  192.168.74.221  TCP       54 [TCP Dup ACK 17#1] 80 → 51253 [ACK] Seq=1 Ack=63 Win=273 Len=0
   25 9.545849   192.168.74.221  157.240.228.61  TCP      132 51253 → 80 [PSH, ACK] Seq=63 Ack=1 Win=510 Len=78
   26 9.604895   157.240.228.61  192.168.74.221  TCP       54 80 → 51253 [ACK] Seq=1 Ack=141 Win=273 Len=0
   27 10.154894  192.168.74.221  157.240.228.61  TCP       93 51253 → 80 [PSH, ACK] Seq=141 Ack=1 Win=510 Len=39
   28 10.157176  157.240.228.61  192.168.74.221  TCP       92 80 → 51253 [PSH, ACK] Seq=1 Ack=141 Win=273 Len=38
   31 10.204718  157.240.228.61  192.168.74.221  TCP       54 80 → 51253 [ACK] Seq=39 Ack=180 Win=273 Len=0
   32 10.205327  192.168.74.221  157.240.228.61  TCP       54 51253 → 80 [ACK] Seq=180 Ack=39 Win=510 Len=0
   33 10.218518  157.240.228.61  192.168.74.221  TCP       92 [TCP Spurious Retransmission] 80 → 51253 [PSH, ACK] Seq=1 Ack=180 Win=273 Len=38
   34 10.218638  192.168.74.221  157.240.228.61  TCP       66 [TCP Dup ACK 32#1] 51253 → 80 [ACK] Seq=180 Ack=39 Win=510 Len=0 SLE=1 SRE=39
   37 10.900418  157.240.228.61  192.168.74.221  TCP      247 80 → 51253 [PSH, ACK] Seq=39 Ack=180 Win=273 Len=193
   38 10.921805  192.168.74.221  157.240.228.61  TCP      100 51253 → 80 [PSH, ACK] Seq=180 Ack=232 Win=509 Len=46
   39 10.958621  157.240.228.61  192.168.74.221  TCP      247 [TCP Spurious Retransmission] 80 → 51253 [PSH, ACK] Seq=39 Ack=180 Win=273 Len=193
   40 10.958757  192.168.74.221  157.240.228.61  TCP       66 [TCP Dup ACK 38#1] 51253 → 80 [ACK] Seq=226 Ack=232 Win=509 Len=0 SLE=39 SRE=232
   41 11.024924  157.240.228.61  192.168.74.221  TCP       54 80 → 51253 [ACK] Seq=232 Ack=226 Win=273 Len=0
   42 11.739389  192.168.74.221  157.240.228.61  TCP      607 51253 → 80 [PSH, ACK] Seq=226 Ack=232 Win=509 Len=553
   44 11.815432  157.240.228.61  192.168.74.221  TCP       54 80 → 51253 [ACK] Seq=232 Ack=779 Win=278 Len=0
   45 14.649469  192.168.74.221  157.240.228.61  TCP       79 51253 → 80 [PSH, ACK] Seq=779 Ack=232 Win=509 Len=25
   46 14.651775  157.240.228.61  192.168.74.221  TCP      115 80 → 51253 [PSH, ACK] Seq=232 Ack=779 Win=278 Len=61
   47 14.651775  157.240.228.61  192.168.74.221  TCP      108 80 → 51253 [PSH, ACK] Seq=293 Ack=779 Win=278 Len=54
   48 14.651775  157.240.228.61  192.168.74.221  TCP      108 [TCP Retransmission] 80 → 51253 [PSH, ACK] Seq=293 Ack=779 Win=278 Len=54
   49 14.651775  157.240.228.61  192.168.74.221  TCP      169 [TCP Retransmission] 80 → 51253 [PSH, ACK] Seq=232 Ack=779 Win=278 Len=115
   51 14.651775  157.240.228.61  192.168.74.221  TCP      169 [TCP Retransmission] 80 → 51253 [PSH, ACK] Seq=232 Ack=779 Win=278 Len=115
   52 14.651955  192.168.74.221  157.240.228.61  TCP       54 51253 → 80 [ACK] Seq=804 Ack=347 Win=508 Len=0
   53 14.652021  192.168.74.221  157.240.228.61  TCP       66 [TCP Dup ACK 52#1] 51253 → 80 [ACK] Seq=804 Ack=347 Win=508 Len=0 SLE=293 SRE=347
   54 14.652048  192.168.74.221  157.240.228.61  TCP       66 [TCP Dup ACK 52#2] 51253 → 80 [ACK] Seq=804 Ack=347 Win=508 Len=0 SLE=232 SRE=347
   55 14.652070  192.168.74.221  157.240.228.61  TCP       66 [TCP Dup ACK 52#3] 51253 → 80 [ACK] Seq=804 Ack=347 Win=508 Len=0 SLE=232 SRE=347
   56 14.657689  192.168.74.221  157.240.228.61  TCP       54 51253 → 80 [FIN, ACK] Seq=804 Ack=347 Win=508 Len=0
   57 14.958874  192.168.74.221  157.240.228.61  TCP       79 [TCP Retransmission] 51253 → 80 [FIN, PSH, ACK] Seq=779 Ack=347 Win=508 Len=25
   58 14.961434  157.240.228.61  192.168.74.221  TCP      109 80 → 51253 [PSH, ACK] Seq=347 Ack=779 Win=278 Len=55
```

```
    > Trans Request (0x25)
  > SMB MailSlot Protocol
  > Microsoft Windows Browser Protocol

0000  ff ff ff ff ff ff 50 2f  9b a0 13 10 08 00 45 00   ······P
0010  00 e5 ca 0d 00 00 80 11  00 00 c0 a8 4a dd c0 a8   ········
0020  4a ff 00 8a 00 8a 00 d1  ac e3 11 0e 9c b1 c0 a8   J·······

Internet Protocol Version 4: Protocol     Packets: 212 · Displayed: 57 (26.9%) · Dropped: 0 (0.0%)     Profile: Default
```

4. Protocol Hierarchy Analysis:

    - Use the "Protocol Hierarchy" feature of Wireshark's statistics to analyze the distribution of protocols in the captured packets.

- Look for abnormal or unexpected protocol usage, such as the presence of suspicious or uncommon protocols.
- Flag packets associated with protocols that indicate potential security risks.



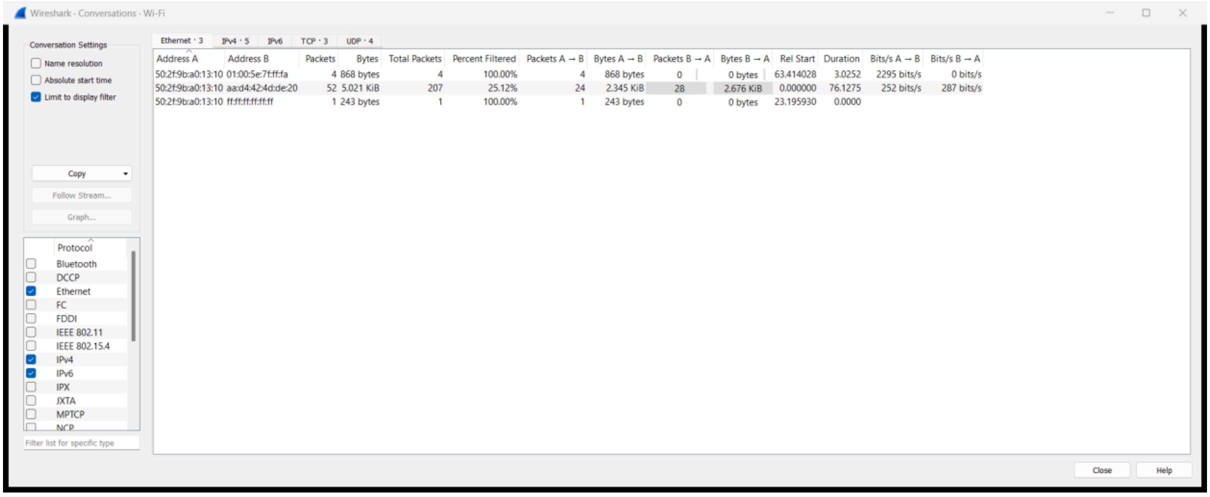
Wireshark · Protocol Hierarchy Statistics · Wi-Fi

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDUs
Frame	100.0	57	100.0	6252	685	0	0	0	57
Ethernet	100.0	57	12.8	798	87	0	0	0	57
Internet Protocol Version 4	100.0	57	18.2	1140	124	0	0	0	57
User Datagram Protocol	19.3	11	1.4	88	9	0	0	0	11
Simple Service Discovery Protocol	7.0	4	11.2	700	76	4	700	76	4
NetBIOS Datagram Service	1.8	1	3.2	201	22	0	0	0	1
SMB (Server Message Block Protocol)	1.8	1	1.9	119	13	0	0	0	1
SMB MailSlot Protocol	1.8	1	0.4	25	2	0	0	0	1
Microsoft Windows Browser Protocol	1.8	1	0.5	33	3	1	33	3	1
Domain Name System	10.5	6	7.5	468	51	6	468	51	6
Transmission Control Protocol	80.7	46	45.7	2857	313	46	2857	313	46

Display filter: ip

Packets: 212 · Displayed: 57 (26.9%) · Dropped: 0 (0.0%)

5. Conversation Tracking:
   - Utilize the "Conversation Tracking" feature to analyze the traffic between network endpoints.
   - Identify conversations that exhibit unusual patterns, such as excessive communication with suspicious hosts or unusual port combinations.
   - Flag packets involved in suspicious conversations for further analysis.



Wireshark · Conversations · Wi-Fi

Conversation Settings

☐ Name resolution
☐ Absolute start time
☑ Limit to display filter

Ethernet · 3 | IPv4 · 5 | IPv6 | TCP · 3 | UDP · 4

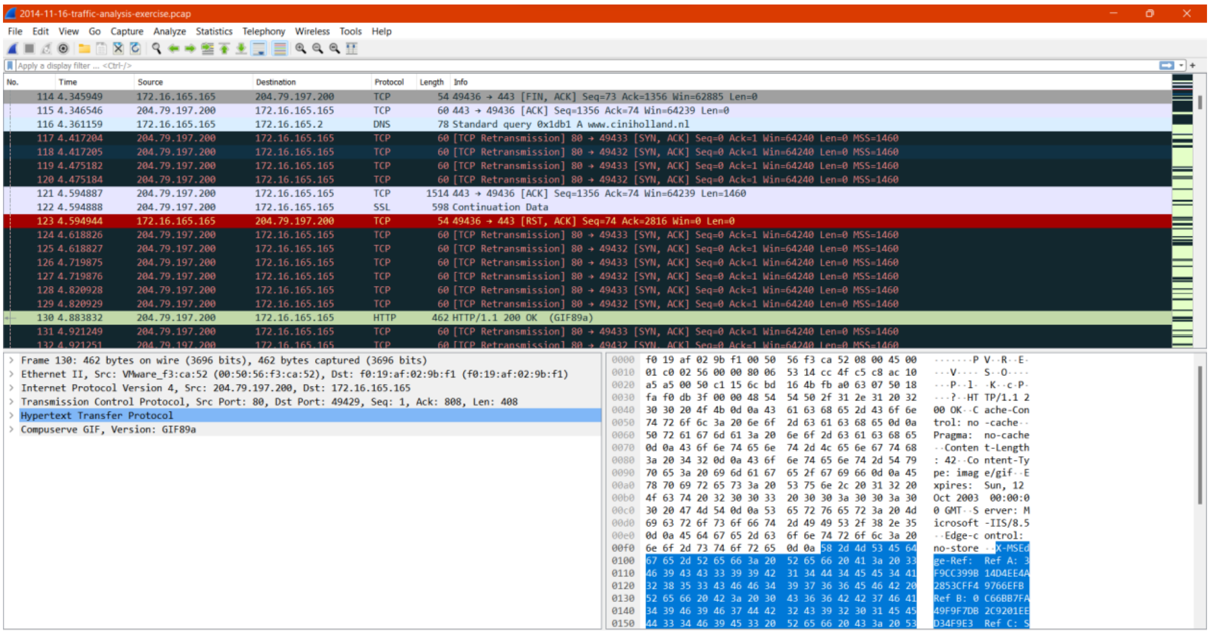
Address A	Address B	Packets	Bytes	Total Packets	Percent Filtered	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
50:2f:9b:a0:13:10	01:00:5e:7f:ff:fa	4	868 bytes	4	100.00%	4	868 bytes	0	0 bytes	63.414028	3.0252	2295 bits/s	0 bits/s
50:2f:9b:a0:13:10	aa:d4:42:4d:de:20	52	5.021 KiB	207	25.12%	24	2.345 KiB	28	2.676 KiB	0.000000	76.1275	252 bits/s	287 bits/s
50:2f:9b:a0:13:10	ff:ff:ff:ff:ff:ff	1	243 bytes	1	100.00%	1	243 bytes	0	0 bytes	23.195930	0.0000		

Protocol

☐ Bluetooth
☐ DCCP
☑ Ethernet
☐ FC
☐ FDDI
☐ IEEE 802.11
☐ IEEE 802.15.4
☑ IPv4
☑ IPv6
☐ IPX
☐ JXTA
☐ MPTCP
☐ NCP

2)) Create a script that leverages the Wireshark API to extract HTTP requests and responses from a pcap file and save them to separate files for further analysis.

Step-1: open the Wireshark and Check on the Http PNG protocol then go to file and click the Export objects then click HTTP .Check the PNG file click on the file and save it.


2014-11-16-traffic-analysis-exercise.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  Time      Source          Destination     Protocol Length Info
 114 4.345949  172.16.165.165  204.79.197.200  TCP        54 49436 → 443 [FIN, ACK] Seq=73 Ack=1356 Win=62885 Len=0
 115 4.346546  204.79.197.200  172.16.165.165  TCP        60 443 → 49436 [ACK] Seq=1356 Ack=74 Win=64239 Len=0
 116 4.361159  172.16.165.165  172.16.165.2    DNS        78 Standard query 0x1db1 A www.ciniholland.nl
 117 4.417204  204.79.197.200  172.16.165.165  TCP        60 [TCP Retransmission] 80 → 49433 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
 118 4.417205  204.79.197.200  172.16.165.165  TCP        60 [TCP Retransmission] 80 → 49432 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
 119 4.475182  204.79.197.200  172.16.165.165  TCP        60 [TCP Retransmission] 80 → 49433 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
 120 4.475184  204.79.197.200  172.16.165.165  TCP        60 [TCP Retransmission] 80 → 49432 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
 121 4.594887  204.79.197.200  172.16.165.165  TCP      1514 443 → 49436 [ACK] Seq=1356 Ack=74 Win=64239 Len=1460
 122 4.594888  204.79.197.200  172.16.165.165  SSL       598 Continuation Data
 123 4.594944  172.16.165.165  204.79.197.200  TCP        54 49436 → 443 [RST, ACK] Seq=74 Ack=2816 Win=0 Len=0
 124 4.618826  204.79.197.200  172.16.165.165  TCP        60 [TCP Retransmission] 80 → 49433 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
 125 4.618827  204.79.197.200  172.16.165.165  TCP        60 [TCP Retransmission] 80 → 49432 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
 126 4.719875  204.79.197.200  172.16.165.165  TCP        60 [TCP Retransmission] 80 → 49433 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
 127 4.719876  204.79.197.200  172.16.165.165  TCP        60 [TCP Retransmission] 80 → 49432 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
 128 4.820928  204.79.197.200  172.16.165.165  TCP        60 [TCP Retransmission] 80 → 49433 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
 129 4.820929  204.79.197.200  172.16.165.165  TCP        60 [TCP Retransmission] 80 → 49432 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
 130 4.883832  204.79.197.200  172.16.165.165  HTTP      462 HTTP/1.1 200 OK  (GIF89a)
 131 4.921249  204.79.197.200  172.16.165.165  TCP        60 [TCP Retransmission] 80 → 49433 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
 132 4.921251  204.79.197.200  172.16.165.165  TCP        60 [TCP Retransmission] 80 → 49432 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
```

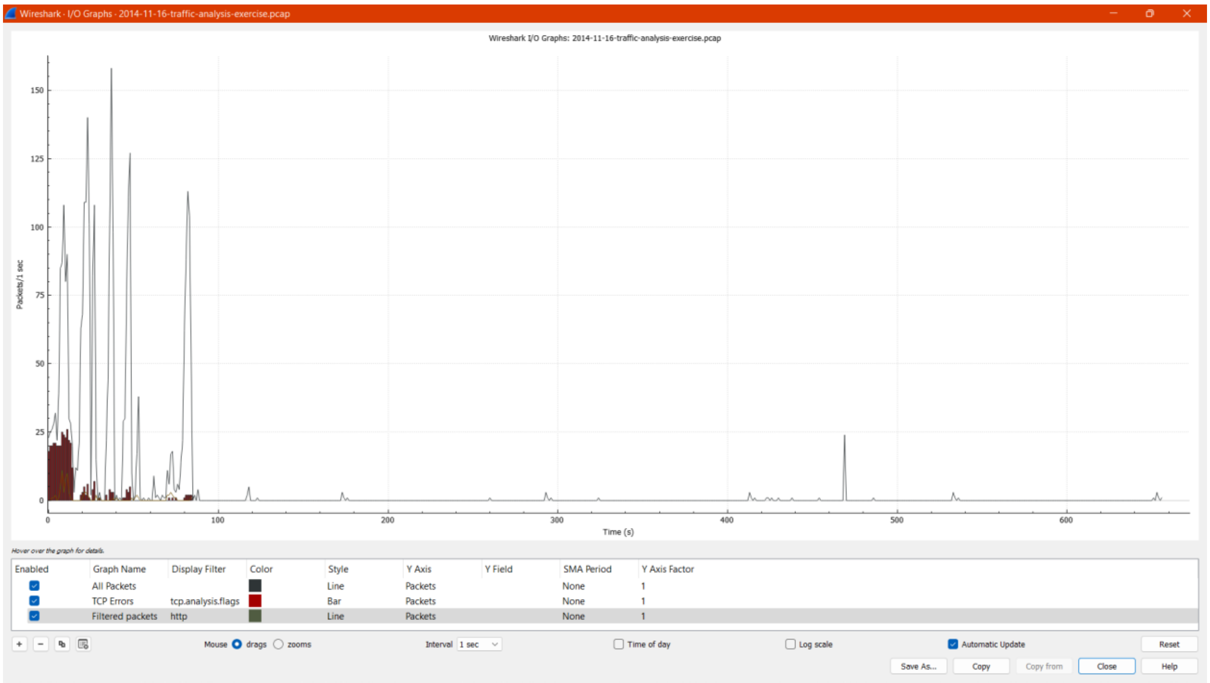
```
> Frame 130: 462 bytes on wire (3696 bits), 462 bytes captured (3696 bits)
> Ethernet II, Src: VMware_f3:ca:52 (00:50:56:f3:ca:52), Dst: f0:19:af:02:9b:f1 (f0:19:af:02:9b:f1)
> Internet Protocol Version 4, Src: 204.79.197.200, Dst: 172.16.165.165
> Transmission Control Protocol, Src Port: 80, Dst Port: 49429, Seq: 1, Ack: 808, Len: 408
> Hypertext Transfer Protocol
> Compuserve GIF, Version: GIF89a
```

```
0000  f0 19 af 02 9b f1 00 50  56 f3 ca 52 08 00 45 00   ·······P V··R··E·
0010  01 c0 02 56 00 00 80 06  53 14 cc 4f c5 c8 ac 10   ···V···· S··O····
0020  a5 a5 00 50 c1 15 6c bd  16 4b fb a0 63 07 50 18   ···P··l· ·K··c·P·
0030  fa f0 db 3f 00 00 48 54  54 50 2f 31 2e 31 20 32   ···?··HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 43  61 63 68 65 2d 43 6f 6e   00 OK··C ache-Con
0050  74 72 6f 6c 3a 20 6e 6f  2d 63 61 63 68 65 0d 0a   trol: no -cache··
0060  50 72 61 67 6d 61 3a 20  6e 6f 2d 63 61 63 68 65   Pragma:  no-cache
0070  0d 0a 43 6f 6e 74 65 6e  74 2d 4c 65 6e 67 74 68   ··Conten t-Length
0080  3a 20 34 32 0d 0a 43 6f  6e 74 65 6e 74 2d 54 79   : 42··Co ntent-Ty
0090  70 65 3a 20 69 6d 61 67  65 2f 67 69 66 0d 0a 45   pe: imag e/gif··E
00a0  78 70 69 72 65 73 3a 20  53 75 6e 2c 20 31 32 20   xpires:  Sun, 12
00b0  4f 63 74 20 32 30 30 33  20 30 30 3a 30 30 3a 30   Oct 2003  00:00:0
00c0  30 20 47 4d 54 0d 0a 53  65 72 76 65 72 3a 20 4d   0 GMT··S erver: M
00d0  69 63 72 6f 73 6f 66 74  2d 49 49 53 2f 38 2e 35   icrosoft -IIS/8.5
00e0  0d 0a 45 64 67 65 2d 63  6f 6e 74 72 6f 6c 3a 20   ··Edge-c ontrol:
00f0  6e 6f 2d 73 74 6f 72 65  0d 0a 58 2d 4d 53 45 64   no-store ··X-MSEd
0100  67 65 2d 52 65 66 3a 20  52 65 66 20 41 3a 20 33   ge-Ref:  Ref A: 3
0110  46 39 43 43 33 39 39 42  31 34 44 34 45 45 34 41   F9CC399B 14D4EE4A
0120  32 38 35 33 43 46 46 34  39 37 36 36 45 46 42 20   2853CFF4 9766EFB
0130  52 65 66 20 42 3a 20 30  43 36 36 42 42 37 46 41   Ref B: 0 C66BB7FA
0140  34 39 46 39 46 37 44 42  32 43 39 32 30 31 45 45   49F9F7DB 2C9201EE
0150  44 33 34 46 39 45 33 20  52 65 66 20 43 3a 20 53   D34F9E3  Ref C: S
```

PNG FILE

3)Implement a program that reads a pcap file using the Wireshark API and visualizes the network traffic data using graphs or charts, such as a histogram of packet sizes or a timeline of packet arrival times.

Step-1: Click on the Statistics then go to the I/O Graphs or Flow Graphs.

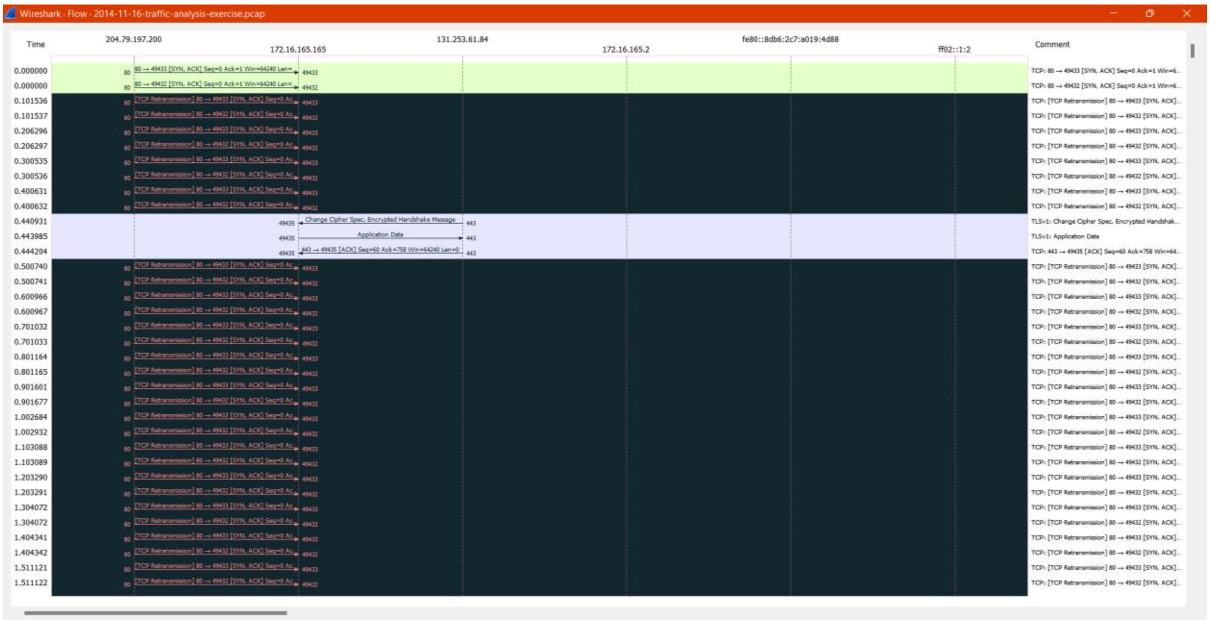

Wireshark · I/O Graphs · 2014-11-16-traffic-analysis-exercise.pcap
Wireshark I/O Graphs: 2014-11-16-traffic-analysis-exercise.pcap
Packets/1 sec
150
125
100
75
50
25
0
0
100
200
300
400
500
600
Time (s)
Hover over the graph for details.

Enabled	Graph Name	Display Filter	Color	Style	Y Axis	Y Field	SMA Period	Y Axis Factor
☑	All Packets		■	Line	Packets		None	1
☑	TCP Errors	tcp.analysis.flags	🟥	Bar	Packets		None	1
☑	Filtered packets	http	■	Line	Packets		None	1

Mouse ● drags ○ zooms   Interval 1 sec   □ Time of day   □ Log scale   ☑ Automatic Update

+
−
Reset
Save As...
Copy
Copy from
Close
Help

I/O GRAPH



```
Time      Comment
0.000000  TCP: 80 → 49433 [SYN, ACK] Seq=0 Ack=1 Win=6...
0.000000  TCP: 80 → 49432 [SYN, ACK] Seq=0 Ack=1 Win=6...
0.101536  TCP: [TCP Retransmission] 80 → 49433 [SYN, ACK]...
0.101537  TCP: [TCP Retransmission] 80 → 49432 [SYN, ACK]...
0.206296  TCP: [TCP Retransmission] 80 → 49433 [SYN, ACK]...
0.206297  TCP: [TCP Retransmission] 80 → 49432 [SYN, ACK]...
0.300535  TCP: [TCP Retransmission] 80 → 49433 [SYN, ACK]...
0.300536  TCP: [TCP Retransmission] 80 → 49432 [SYN, ACK]...
0.400631  TCP: [TCP Retransmission] 80 → 49433 [SYN, ACK]...
0.400632  TCP: [TCP Retransmission] 80 → 49432 [SYN, ACK]...
0.440931  TLSv1: Change Cipher Spec, Encrypted Handshak...
0.443985  TLSv1: Application Data
0.444204  TCP: 443 → 49435 [ACK] Seq=60 Ack=758 Win=64...
0.500740  TCP: [TCP Retransmission] 80 → 49433 [SYN, ACK]...
0.500741  TCP: [TCP Retransmission] 80 → 49432 [SYN, ACK]...
0.600966  TCP: [TCP Retransmission] 80 → 49433 [SYN, ACK]...
0.600967  TCP: [TCP Retransmission] 80 → 49432 [SYN, ACK]...
0.701032  TCP: [TCP Retransmission] 80 → 49433 [SYN, ACK]...
0.701033  TCP: [TCP Retransmission] 80 → 49432 [SYN, ACK]...
0.801164  TCP: [TCP Retransmission] 80 → 49433 [SYN, ACK]...
0.801165  TCP: [TCP Retransmission] 80 → 49432 [SYN, ACK]...
0.901601  TCP: [TCP Retransmission] 80 → 49433 [SYN, ACK]...
0.901677  TCP: [TCP Retransmission] 80 → 49432 [SYN, ACK]...
1.002684  TCP: [TCP Retransmission] 80 → 49433 [SYN, ACK]...
1.002932  TCP: [TCP Retransmission] 80 → 49432 [SYN, ACK]...
1.103088  TCP: [TCP Retransmission] 80 → 49433 [SYN, ACK]...
1.103089  TCP: [TCP Retransmission] 80 → 49432 [SYN, ACK]...
1.203290  TCP: [TCP Retransmission] 80 → 49433 [SYN, ACK]...
1.203291  TCP: [TCP Retransmission] 80 → 49432 [SYN, ACK]...
1.304072  TCP: [TCP Retransmission] 80 → 49433 [SYN, ACK]...
1.304072  TCP: [TCP Retransmission] 80 → 49432 [SYN, ACK]...
1.404341  TCP: [TCP Retransmission] 80 → 49433 [SYN, ACK]...
1.404342  TCP: [TCP Retransmission] 80 → 49432 [SYN, ACK]...
1.511121  TCP: [TCP Retransmission] 80 → 49433 [SYN, ACK]...
1.511122  TCP: [TCP Retransmission] 80 → 49432 [SYN, ACK]...
```

FLOW GRAPH