WIRESHARK

Network Traffic Analysis with WireShark

Name-Sarada Sankar Nayak

University-Vellore Institute of Technology,Chennai

Description

Network traffic analysis is a crucial skill in cybersecurity. Wireshark is a popular network protocol analyzer used to capture and analyze network traffic.This project is a complete guide for installing ,capturing and analyzing network traffic using wireshark.

Procedure

Step-1)

Download Wireshark

Visit the wireshark download page at chrome and download the installer for your operating system.(I used kali Linux which has wireshark tool pre-installed in its OS.)

Step-2)

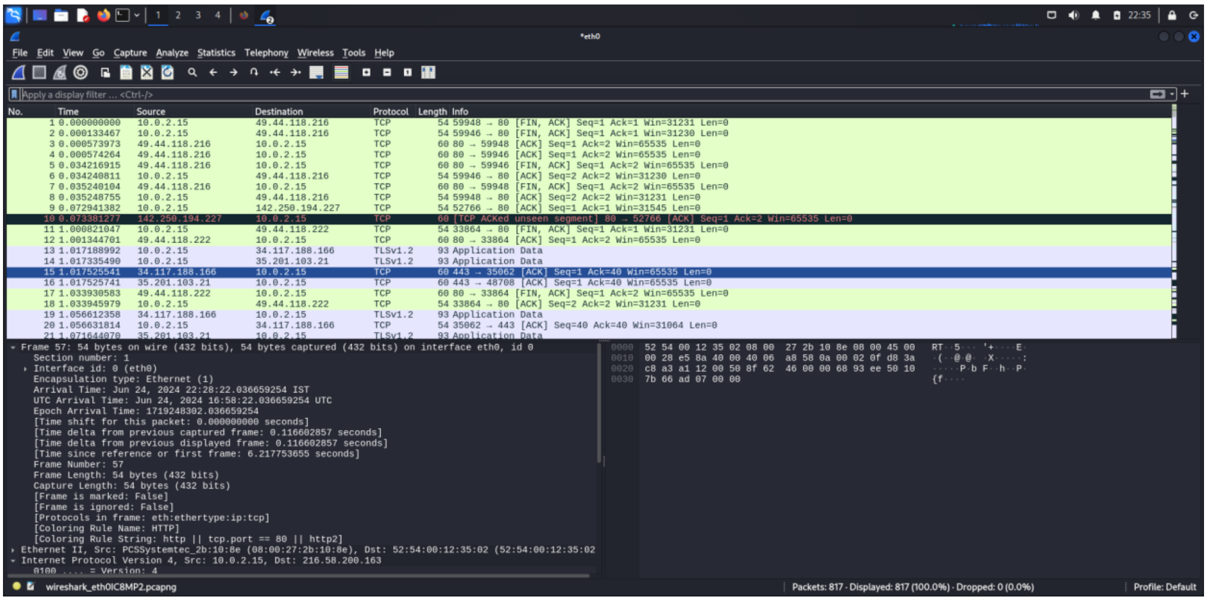
Capture Network Traffic

- Generate Traffic

To see some traffic ,open a web browser and visit a few web sites .This will generate http/https traffic that wireshark will capture .

- Start capturing :

Click on the network interface to start capturing traffic.


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
22:35

```
No.   Time         Source           Destination      Protocol Length Info
    1 0.000000000  10.0.2.15        49.44.118.216    TCP      54 59948 → 80 [FIN, ACK] Seq=1 Ack=1 Win=31231 Len=0
    2 0.000133467  10.0.2.15        49.44.118.216    TCP      54 59946 → 80 [FIN, ACK] Seq=1 Ack=1 Win=31230 Len=0
    3 0.000573973  49.44.118.216    10.0.2.15        TCP      60 80 → 59948 [ACK] Seq=1 Ack=2 Win=65535 Len=0
    4 0.000574264  49.44.118.216    10.0.2.15        TCP      60 80 → 59946 [ACK] Seq=1 Ack=2 Win=65535 Len=0
    5 0.034216915  49.44.118.216    10.0.2.15        TCP      60 80 → 59946 [FIN, ACK] Seq=1 Ack=2 Win=65535 Len=0
    6 0.034240811  10.0.2.15        49.44.118.216    TCP      54 59946 → 80 [ACK] Seq=2 Ack=2 Win=31230 Len=0
    7 0.035240104  49.44.118.216    10.0.2.15        TCP      60 80 → 59948 [FIN, ACK] Seq=1 Ack=2 Win=65535 Len=0
    8 0.035248755  10.0.2.15        49.44.118.216    TCP      54 59948 → 80 [ACK] Seq=2 Ack=2 Win=31231 Len=0
    9 0.072941382  10.0.2.15        142.250.194.227  TCP      54 52766 → 80 [ACK] Seq=1 Ack=1 Win=31545 Len=0
   10 0.073381277  142.250.194.227  10.0.2.15        TCP      60 [TCP ACKed unseen segment] 80 → 52766 [ACK] Seq=1 Ack=2 Win=65535 Len=0
   11 1.000821047  10.0.2.15        49.44.118.222    TCP      54 33864 → 80 [FIN, ACK] Seq=1 Ack=1 Win=31231 Len=0
   12 1.001344701  49.44.118.222    10.0.2.15        TCP      60 80 → 33864 [ACK] Seq=1 Ack=2 Win=65535 Len=0
   13 1.017188992  10.0.2.15        34.117.188.166   TLSv1.2  93 Application Data
   14 1.017335490  10.0.2.15        35.201.103.21    TLSv1.2  93 Application Data
   15 1.017525541  34.117.188.166   10.0.2.15        TCP      60 443 → 35062 [ACK] Seq=1 Ack=40 Win=65535 Len=0
   16 1.017525741  35.201.103.21    10.0.2.15        TCP      60 443 → 48708 [ACK] Seq=1 Ack=40 Win=65535 Len=0
   17 1.033930583  49.44.118.222    10.0.2.15        TCP      60 80 → 33864 [FIN, ACK] Seq=1 Ack=2 Win=65535 Len=0
   18 1.033945979  10.0.2.15        49.44.118.222    TCP      54 33864 → 80 [ACK] Seq=2 Ack=2 Win=31231 Len=0
   19 1.056612358  34.117.188.166   10.0.2.15        TLSv1.2  93 Application Data
   20 1.056631814  10.0.2.15        34.117.188.166   TCP      54 35062 → 443 [ACK] Seq=40 Ack=40 Win=31064 Len=0
   21 1.071644070  35.201.103.21    10.0.2.15        TLSv1.2  93 Application Data
```

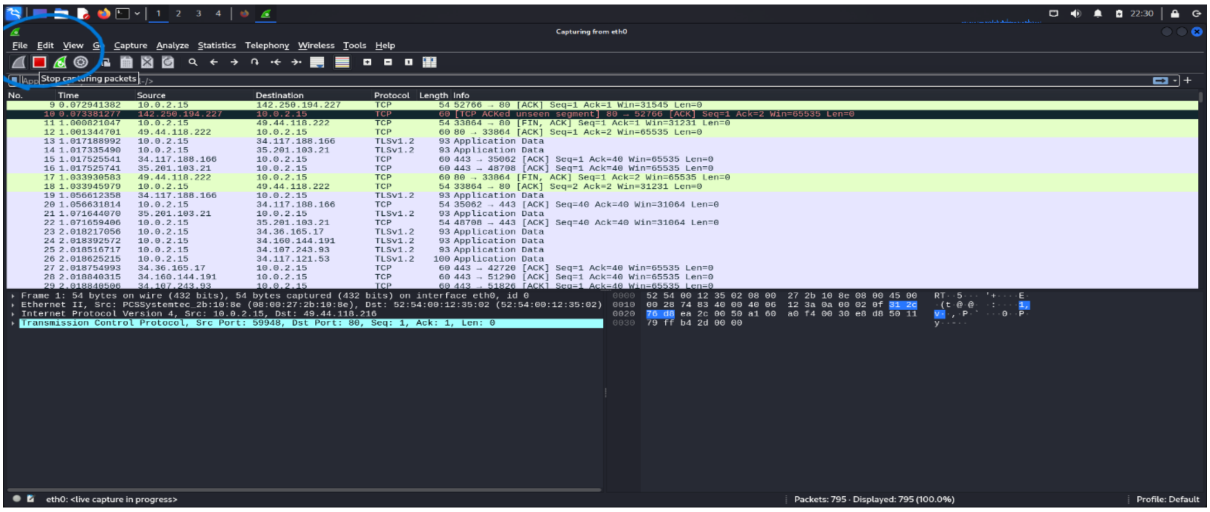
```
▾ Frame 57: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id 0
    Section number: 1
  ▸ Interface id: 0 (eth0)
    Encapsulation type: Ethernet (1)
    Arrival Time: Jun 24, 2024 22:28:22.036659254 IST
    UTC Arrival Time: Jun 24, 2024 16:58:22.036659254 UTC
    Epoch Arrival Time: 1719248302.036659254
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.116602857 seconds]
    [Time delta from previous displayed frame: 0.116602857 seconds]
    [Time since reference or first frame: 6.217753655 seconds]
    Frame Number: 57
    Frame Length: 54 bytes (432 bits)
    Capture Length: 54 bytes (432 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
▸ Ethernet II, Src: PCSSystemtec_2b:10:8e (08:00:27:2b:10:8e), Dst: 52:54:00:12:35:02 (52:54:00:12:35:02
▾ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 216.58.200.163
    0100 .... = Version: 4
```

```
0000  52 54 00 12 35 02 08 00  27 2b 10 8e 08 00 45 00   RT··5···'+····E·
0010  00 28 e5 8a 40 00 40 06  a8 58 0a 00 02 0f d8 3a   ·(··@·@··X·····:
0020  c8 a3 a1 12 00 50 8f 62  46 00 00 68 93 ee 50 10   ·····P·bF··h··P·
0030  7b 66 ad 07 00 00                                  {f····
```

wireshark_eth0IC8MP2.pcapng | Packets: 817 · Displayed: 817 (100.0%) · Dropped: 0 (0.0%) | Profile: Default

- Stop Capturing:

Click on the red square button to stop capturing packets


Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Stop capturing packets
22:30

```
No.   Time         Source           Destination      Protocol Length Info
    9 0.072941382  10.0.2.15        142.250.194.227  TCP      54 52766 → 80 [ACK] Seq=1 Ack=1 Win=31545 Len=0
   10 0.073381277  142.250.194.227  10.0.2.15        TCP      60 [TCP ACKed unseen segment] 80 → 52766 [ACK] Seq=1 Ack=2 Win=65535 Len=0
   11 1.000821047  10.0.2.15        49.44.118.222    TCP      54 33864 → 80 [FIN, ACK] Seq=1 Ack=1 Win=31231 Len=0
   12 1.001344701  49.44.118.222    10.0.2.15        TCP      60 80 → 33864 [ACK] Seq=1 Ack=2 Win=65535 Len=0
   13 1.017188992  10.0.2.15        34.117.188.166   TLSv1.2  93 Application Data
   14 1.017335490  10.0.2.15        35.201.103.21    TLSv1.2  93 Application Data
   15 1.017525541  34.117.188.166   10.0.2.15        TCP      60 443 → 35062 [ACK] Seq=1 Ack=40 Win=65535 Len=0
   16 1.017525741  35.201.103.21    10.0.2.15        TCP      60 443 → 48708 [ACK] Seq=1 Ack=40 Win=65535 Len=0
   17 1.033930583  49.44.118.222    10.0.2.15        TCP      60 80 → 33864 [FIN, ACK] Seq=1 Ack=2 Win=65535 Len=0
   18 1.033945979  10.0.2.15        49.44.118.222    TCP      54 33864 → 80 [ACK] Seq=2 Ack=2 Win=31231 Len=0
   19 1.056612358  34.117.188.166   10.0.2.15        TLSv1.2  93 Application Data
   20 1.056631814  10.0.2.15        34.117.188.166   TCP      54 35062 → 443 [ACK] Seq=40 Ack=40 Win=31064 Len=0
   21 1.071644070  35.201.103.21    10.0.2.15        TLSv1.2  93 Application Data
   22 1.071659406  10.0.2.15        35.201.103.21    TCP      54 48708 → 443 [ACK] Seq=40 Ack=40 Win=31064 Len=0
   23 2.018217056  10.0.2.15        34.36.165.17     TLSv1.2  93 Application Data
   24 2.018392572  10.0.2.15        34.160.144.191   TLSv1.2  93 Application Data
   25 2.018516717  10.0.2.15        34.107.243.93    TLSv1.2  93 Application Data
   26 2.018625215  10.0.2.15        34.117.121.53    TLSv1.2  100 Application Data
   27 2.018754993  34.36.165.17     10.0.2.15        TCP      60 443 → 42720 [ACK] Seq=1 Ack=40 Win=65535 Len=0
   28 2.018840315  34.160.144.191   10.0.2.15        TCP      60 443 → 51290 [ACK] Seq=1 Ack=40 Win=65535 Len=0
   29 2.018840506  34.107.243.93    10.0.2.15        TCP      60 443 → 51826 [ACK] Seq=1 Ack=40 Win=65535 Len=0
```

```
▸ Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id 0
▸ Ethernet II, Src: PCSSystemtec_2b:10:8e (08:00:27:2b:10:8e), Dst: 52:54:00:12:35:02 (52:54:00:12:35:02)
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 49.44.118.216
▸ Transmission Control Protocol, Src Port: 59948, Dst Port: 80, Seq: 1, Ack: 1, Len: 0
```

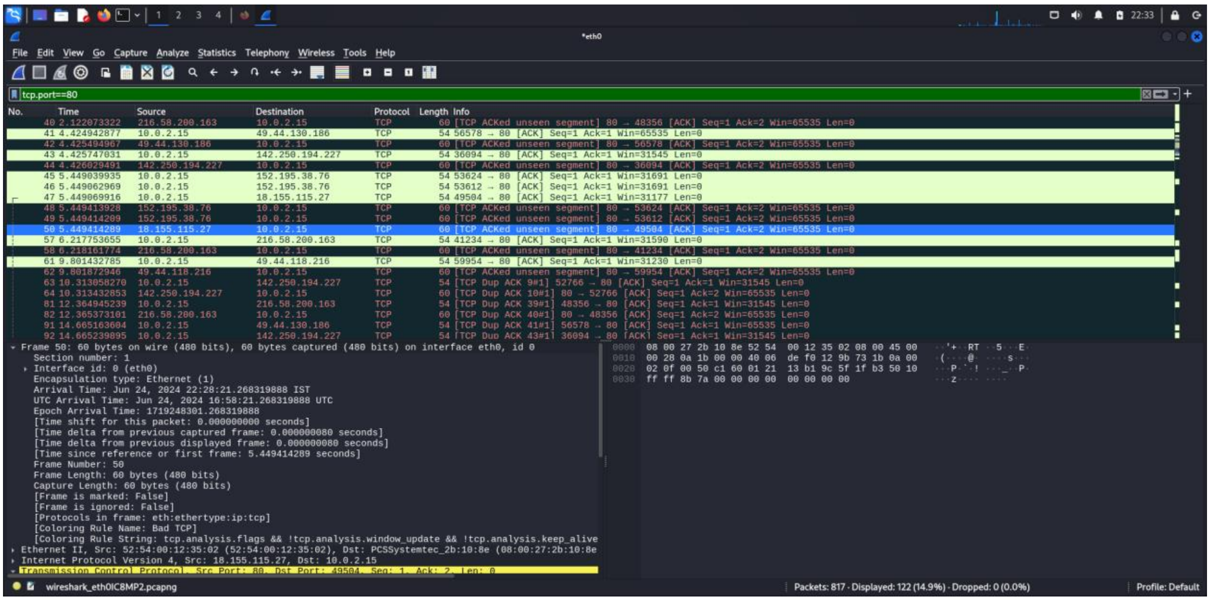
```
0000  52 54 00 12 35 02 08 00  27 2b 10 8e 08 00 45 00   RT··5···'+····E·
0010  00 28 74 83 40 00 40 06  12 3a 0a 00 02 0f 31 2c   ·(t·@·@··:····1,
0020  76 d8 ea 2c 00 50 a1 60  a0 f4 00 30 e8 d8 50 11   v··,·P·`···0··P·
0030  79 ff b4 2d 00 00                                  y··-··
```

eth0: <live capture in progress> | Packets: 795 · Displayed: 795 (100.0%) | Profile: Default

Step-3)

- Analyze Network Traffic

Click on a packet to view its details.



```
tcp.port==80
```

```
No.  Time           Source           Destination      Protocol  Length Info
  40 2.122073322    216.58.200.163   10.0.2.15        TCP       60 [TCP ACKed unseen segment] 80 → 48356 [ACK] Seq=1 Ack=2 Win=65535 Len=0
  41 4.424942877    10.0.2.15        49.44.130.186    TCP       54 56578 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0
  42 4.425494967    49.44.130.186    10.0.2.15        TCP       60 [TCP ACKed unseen segment] 80 → 56578 [ACK] Seq=1 Ack=2 Win=65535 Len=0
  43 4.425747031    10.0.2.15        142.250.194.227  TCP       54 36094 → 80 [ACK] Seq=1 Ack=1 Win=31545 Len=0
  44 4.426029491    142.250.194.227  10.0.2.15        TCP       60 [TCP ACKed unseen segment] 80 → 36094 [ACK] Seq=1 Ack=2 Win=65535 Len=0
  45 5.449039935    10.0.2.15        152.195.38.76    TCP       54 53624 → 80 [ACK] Seq=1 Ack=1 Win=31691 Len=0
  46 5.449062969    10.0.2.15        152.195.38.76    TCP       54 53612 → 80 [ACK] Seq=1 Ack=1 Win=31691 Len=0
  47 5.449069916    10.0.2.15        18.155.115.27    TCP       54 49504 → 80 [ACK] Seq=1 Ack=1 Win=31177 Len=0
  48 5.449413928    152.195.38.76    10.0.2.15        TCP       60 [TCP ACKed unseen segment] 80 → 53624 [ACK] Seq=1 Ack=2 Win=65535 Len=0
  49 5.449414209    152.195.38.76    10.0.2.15        TCP       60 [TCP ACKed unseen segment] 80 → 53612 [ACK] Seq=1 Ack=2 Win=65535 Len=0
  50 5.449414289    18.155.115.27    10.0.2.15        TCP       60 [TCP ACKed unseen segment] 80 → 49504 [ACK] Seq=1 Ack=2 Win=65535 Len=0
  57 6.217753655    10.0.2.15        216.58.200.163   TCP       54 41234 → 80 [ACK] Seq=1 Ack=1 Win=31590 Len=0
  58 6.218161774    216.58.200.163   10.0.2.15        TCP       60 [TCP ACKed unseen segment] 80 → 41234 [ACK] Seq=1 Ack=2 Win=65535 Len=0
  61 9.801432785    10.0.2.15        49.44.118.216    TCP       54 59954 → 80 [ACK] Seq=1 Ack=1 Win=31230 Len=0
  62 9.801872946    49.44.118.216    10.0.2.15        TCP       60 [TCP ACKed unseen segment] 80 → 59954 [ACK] Seq=1 Ack=2 Win=65535 Len=0
  63 10.313058270   10.0.2.15        142.250.194.227  TCP       54 [TCP Dup ACK 9#1] 52766 → 80 [ACK] Seq=1 Ack=1 Win=31545 Len=0
  64 10.313432853   142.250.194.227  10.0.2.15        TCP       60 [TCP Dup ACK 10#1] 80 → 52766 [ACK] Seq=1 Ack=2 Win=65535 Len=0
  81 12.364945239   10.0.2.15        216.58.200.163   TCP       54 [TCP Dup ACK 39#1] 48356 → 80 [ACK] Seq=1 Ack=1 Win=31545 Len=0
  82 12.365373101   216.58.200.163   10.0.2.15        TCP       60 [TCP Dup ACK 40#1] 80 → 48356 [ACK] Seq=1 Ack=2 Win=65535 Len=0
  91 14.665163604   10.0.2.15        49.44.130.186    TCP       54 [TCP Dup ACK 41#1] 56578 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0
  92 14.665239895   10.0.2.15        142.250.194.227  TCP       54 [TCP Dup ACK 43#1] 36094 → 80 [ACK] Seq=1 Ack=1 Win=31545 Len=0
```

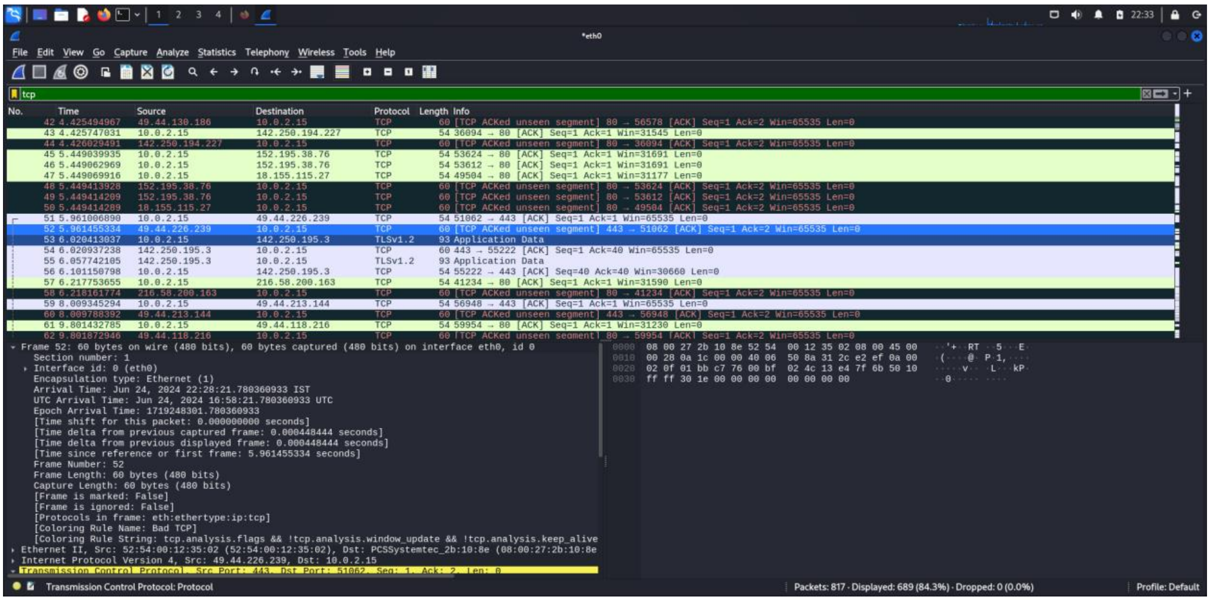
```
▾ Frame 50: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0, id 0
    Section number: 1
  ▸ Interface id: 0 (eth0)
    Encapsulation type: Ethernet (1)
    Arrival Time: Jun 24, 2024 22:28:21.268319888 IST
    UTC Arrival Time: Jun 24, 2024 16:58:21.268319888 UTC
    Epoch Arrival Time: 1719248301.268319888
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.000000080 seconds]
    [Time delta from previous displayed frame: 0.000000080 seconds]
    [Time since reference or first frame: 5.449414289 seconds]
    Frame Number: 50
    Frame Length: 60 bytes (480 bits)
    Capture Length: 60 bytes (480 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp]
    [Coloring Rule Name: Bad TCP]
    [Coloring Rule String: tcp.analysis.flags && !tcp.analysis.window_update && !tcp.analysis.keep_alive
▸ Ethernet II, Src: 52:54:00:12:35:02 (52:54:00:12:35:02), Dst: PCSSystemtec_2b:10:8e (08:00:27:2b:10:8e
▸ Internet Protocol Version 4, Src: 18.155.115.27, Dst: 10.0.2.15
▾ Transmission Control Protocol, Src Port: 80, Dst Port: 49504, Seq: 1, Ack: 2, Len: 0
```

```
0000  08 00 27 2b 10 8e 52 54  00 12 35 02 08 00 45 00   ··'+··RT ··5···E·
0010  00 28 0a 1b 00 00 40 06  de f0 12 9b 73 1b 0a 00   ·(····@· ····s···
0020  02 0f 00 50 c1 60 01 21  13 b1 9c 5f 1f b3 50 10   ···P·`·! ···_··P·
0030  ff ff 8b 7a 00 00 00 00  00 00 00 00               ···z···· ····
```

wireshark_eth0IC8MP2.pcapng   Packets: 817 · Displayed: 122 (14.9%) · Dropped: 0 (0.0%)   Profile: Default

- Filter Traffic

TCP traffic



```
tcp
```

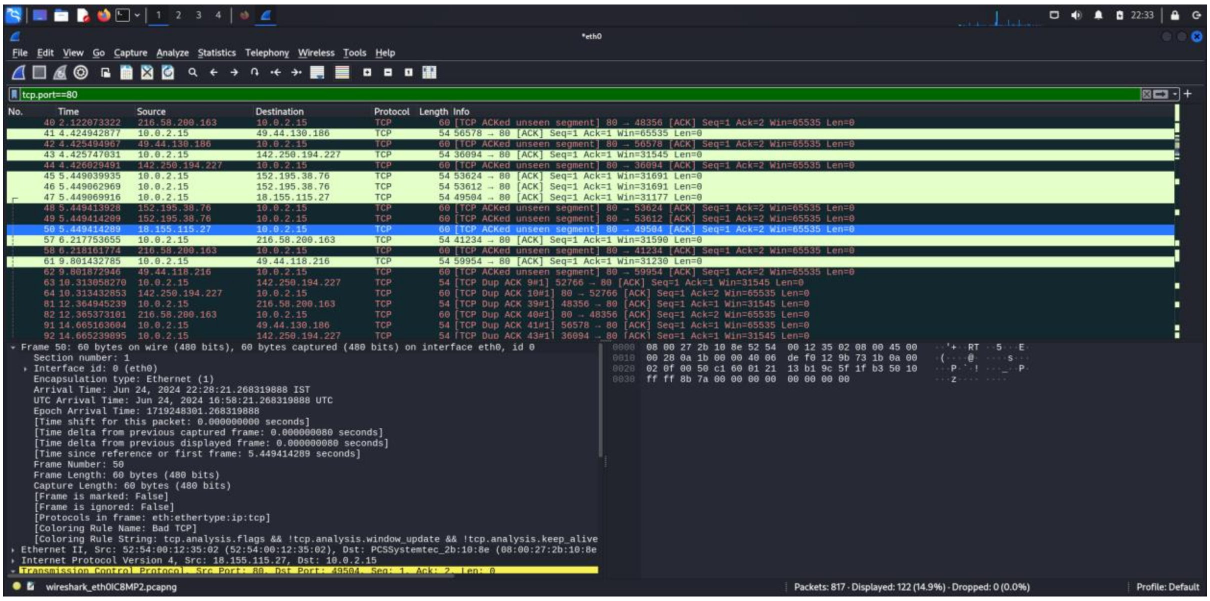
```
No.  Time           Source           Destination      Protocol  Length Info
  42 4.425494967    49.44.130.186    10.0.2.15        TCP       60 [TCP ACKed unseen segment] 80 → 56578 [ACK] Seq=1 Ack=2 Win=65535 Len=0
  43 4.425747031    10.0.2.15        142.250.194.227  TCP       54 36094 → 80 [ACK] Seq=1 Ack=1 Win=31545 Len=0
  44 4.426029491    142.250.194.227  10.0.2.15        TCP       60 [TCP ACKed unseen segment] 80 → 36094 [ACK] Seq=1 Ack=2 Win=65535 Len=0
  45 5.449039935    10.0.2.15        152.195.38.76    TCP       54 53624 → 80 [ACK] Seq=1 Ack=1 Win=31691 Len=0
  46 5.449062969    10.0.2.15        152.195.38.76    TCP       54 53612 → 80 [ACK] Seq=1 Ack=1 Win=31691 Len=0
  47 5.449069916    10.0.2.15        18.155.115.27    TCP       54 49504 → 80 [ACK] Seq=1 Ack=1 Win=31177 Len=0
  48 5.449413928    152.195.38.76    10.0.2.15        TCP       60 [TCP ACKed unseen segment] 80 → 53624 [ACK] Seq=1 Ack=2 Win=65535 Len=0
  49 5.449414209    152.195.38.76    10.0.2.15        TCP       60 [TCP ACKed unseen segment] 80 → 53612 [ACK] Seq=1 Ack=2 Win=65535 Len=0
  50 5.449414289    18.155.115.27    10.0.2.15        TCP       60 [TCP ACKed unseen segment] 80 → 49504 [ACK] Seq=1 Ack=2 Win=65535 Len=0
  51 5.961006890    10.0.2.15        49.44.226.239    TCP       54 51062 → 443 [ACK] Seq=1 Ack=1 Win=65535 Len=0
  52 5.961455334    49.44.226.239    10.0.2.15        TCP       60 [TCP ACKed unseen segment] 443 → 51062 [ACK] Seq=1 Ack=2 Win=65535 Len=0
  53 6.020413037    10.0.2.15        142.250.195.3    TLSv1.2   93 Application Data
  54 6.020937238    142.250.195.3    10.0.2.15        TCP       60 443 → 55222 [ACK] Seq=1 Ack=40 Win=65535 Len=0
  55 6.057742105    142.250.195.3    10.0.2.15        TLSv1.2   93 Application Data
  56 6.101150798    10.0.2.15        142.250.195.3    TCP       54 55222 → 443 [ACK] Seq=40 Ack=40 Win=30660 Len=0
  57 6.217753655    10.0.2.15        216.58.200.163   TCP       54 41234 → 80 [ACK] Seq=1 Ack=1 Win=31590 Len=0
  58 6.218161774    216.58.200.163   10.0.2.15        TCP       60 [TCP ACKed unseen segment] 80 → 41234 [ACK] Seq=1 Ack=2 Win=65535 Len=0
  59 8.009345294    10.0.2.15        49.44.213.144    TCP       54 56948 → 443 [ACK] Seq=1 Ack=1 Win=65535 Len=0
  60 8.009788392    49.44.213.144    10.0.2.15        TCP       60 [TCP ACKed unseen segment] 443 → 56948 [ACK] Seq=1 Ack=2 Win=65535 Len=0
  61 9.801432785    10.0.2.15        49.44.118.216    TCP       54 59954 → 80 [ACK] Seq=1 Ack=1 Win=31230 Len=0
  62 9.801872946    49.44.118.216    10.0.2.15        TCP       60 [TCP ACKed unseen segment] 80 → 59954 [ACK] Seq=1 Ack=2 Win=65535 Len=0
```

```
▾ Frame 52: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0, id 0
    Section number: 1
  ▸ Interface id: 0 (eth0)
    Encapsulation type: Ethernet (1)
    Arrival Time: Jun 24, 2024 22:28:21.780360933 IST
    UTC Arrival Time: Jun 24, 2024 16:58:21.780360933 UTC
    Epoch Arrival Time: 1719248301.780360933
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.000448444 seconds]
    [Time delta from previous displayed frame: 0.000448444 seconds]
    [Time since reference or first frame: 5.961455334 seconds]
    Frame Number: 52
    Frame Length: 60 bytes (480 bits)
    Capture Length: 60 bytes (480 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp]
    [Coloring Rule Name: Bad TCP]
    [Coloring Rule String: tcp.analysis.flags && !tcp.analysis.window_update && !tcp.analysis.keep_alive
▸ Ethernet II, Src: 52:54:00:12:35:02 (52:54:00:12:35:02), Dst: PCSSystemtec_2b:10:8e (08:00:27:2b:10:8e
▸ Internet Protocol Version 4, Src: 49.44.226.239, Dst: 10.0.2.15
▾ Transmission Control Protocol, Src Port: 443, Dst Port: 51062, Seq: 1, Ack: 2, Len: 0
```

```
0000  08 00 27 2b 10 8e 52 54  00 12 35 02 08 00 45 00   ··'+··RT ··5···E·
0010  00 28 0a 1c 00 00 40 06  50 8a 31 2c e2 ef 0a 00   ·(····@· P·1,····
0020  02 0f 01 bb c7 76 00 bf  02 4c 13 e4 7f 6b 50 10   ·····v·· ·L···kP·
0030  ff ff 30 1e 00 00 00 00  00 00 00 00               ··0····· ····
```

Transmission Control Protocol: Protocol   Packets: 817 · Displayed: 689 (84.3%) · Dropped: 0 (0.0%)   Profile: Default

Traffic at tcp.port==80


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.port==80

```
No.  Time           Source           Destination      Protocol Length Info
  40 2.122073322    216.58.200.163   10.0.2.15        TCP      60 [TCP ACKed unseen segment] 80 → 48356 [ACK] Seq=1 Ack=2 Win=65535 Len=0
  41 4.424942877    10.0.2.15        49.44.130.186    TCP      54 56578 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0
  42 4.425494967    49.44.130.186    10.0.2.15        TCP      60 [TCP ACKed unseen segment] 80 → 56578 [ACK] Seq=1 Ack=2 Win=65535 Len=0
  43 4.425747031    10.0.2.15        142.250.194.227  TCP      54 36094 → 80 [ACK] Seq=1 Ack=1 Win=31545 Len=0
  44 4.426029491    142.250.194.227  10.0.2.15        TCP      60 [TCP ACKed unseen segment] 80 → 36094 [ACK] Seq=1 Ack=2 Win=65535 Len=0
  45 5.449039935    10.0.2.15        152.195.38.76    TCP      54 53624 → 80 [ACK] Seq=1 Ack=1 Win=31691 Len=0
  46 5.449062969    10.0.2.15        152.195.38.76    TCP      54 53612 → 80 [ACK] Seq=1 Ack=1 Win=31691 Len=0
  47 5.449069916    10.0.2.15        18.155.115.27    TCP      54 49504 → 80 [ACK] Seq=1 Ack=1 Win=31177 Len=0
  48 5.449413928    152.195.38.76    10.0.2.15        TCP      60 [TCP ACKed unseen segment] 80 → 53624 [ACK] Seq=1 Ack=2 Win=65535 Len=0
  49 5.449414209    152.195.38.76    10.0.2.15        TCP      60 [TCP ACKed unseen segment] 80 → 53612 [ACK] Seq=1 Ack=2 Win=65535 Len=0
  50 5.449414289    18.155.115.27    10.0.2.15        TCP      60 [TCP ACKed unseen segment] 80 → 49504 [ACK] Seq=1 Ack=2 Win=65535 Len=0
  57 6.217753655    10.0.2.15        216.58.200.163   TCP      54 41234 → 80 [ACK] Seq=1 Ack=1 Win=31590 Len=0
  58 6.218161774    216.58.200.163   10.0.2.15        TCP      60 [TCP ACKed unseen segment] 80 → 41234 [ACK] Seq=1 Ack=2 Win=65535 Len=0
  61 9.801432785    10.0.2.15        49.44.118.216    TCP      54 59954 → 80 [ACK] Seq=1 Ack=1 Win=31230 Len=0
  62 9.801872946    49.44.118.216    10.0.2.15        TCP      60 [TCP ACKed unseen segment] 80 → 59954 [ACK] Seq=1 Ack=2 Win=65535 Len=0
  63 10.313058270   10.0.2.15        142.250.194.227  TCP      54 [TCP Dup ACK 9#1] 52766 → 80 [ACK] Seq=1 Ack=1 Win=31545 Len=0
  64 10.313432853   142.250.194.227  10.0.2.15        TCP      60 [TCP Dup ACK 10#1] 80 → 52766 [ACK] Seq=1 Ack=2 Win=65535 Len=0
  81 12.364945239   10.0.2.15        216.58.200.163   TCP      54 [TCP Dup ACK 39#1] 48356 → 80 [ACK] Seq=1 Ack=1 Win=31545 Len=0
  82 12.365373101   216.58.200.163   10.0.2.15        TCP      60 [TCP Dup ACK 40#1] 80 → 48356 [ACK] Seq=1 Ack=2 Win=65535 Len=0
  91 14.665163604   10.0.2.15        49.44.130.186    TCP      54 [TCP Dup ACK 41#1] 56578 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0
  92 14.665239895   10.0.2.15        142.250.194.227  TCP      54 [TCP Dup ACK 43#1] 36094 → 80 [ACK] Seq=1 Ack=1 Win=31545 Len=0
```

```
▾ Frame 50: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0, id 0
    Section number: 1
  ▸ Interface id: 0 (eth0)
    Encapsulation type: Ethernet (1)
    Arrival Time: Jun 24, 2024 22:28:21.268319888 IST
    UTC Arrival Time: Jun 24, 2024 16:58:21.268319888 UTC
    Epoch Arrival Time: 1719248301.268319888
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.000000080 seconds]
    [Time delta from previous displayed frame: 0.000000080 seconds]
    [Time since reference or first frame: 5.449414289 seconds]
    Frame Number: 50
    Frame Length: 60 bytes (480 bits)
    Capture Length: 60 bytes (480 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp]
    [Coloring Rule Name: Bad TCP]
    [Coloring Rule String: tcp.analysis.flags && !tcp.analysis.window_update && !tcp.analysis.keep_alive
▸ Ethernet II, Src: 52:54:00:12:35:02 (52:54:00:12:35:02), Dst: PCSSystemtec_2b:10:8e (08:00:27:2b:10:8e
▸ Internet Protocol Version 4, Src: 18.155.115.27, Dst: 10.0.2.15
▾ Transmission Control Protocol, Src Port: 80, Dst Port: 49504, Seq: 1, Ack: 2, Len: 0
```

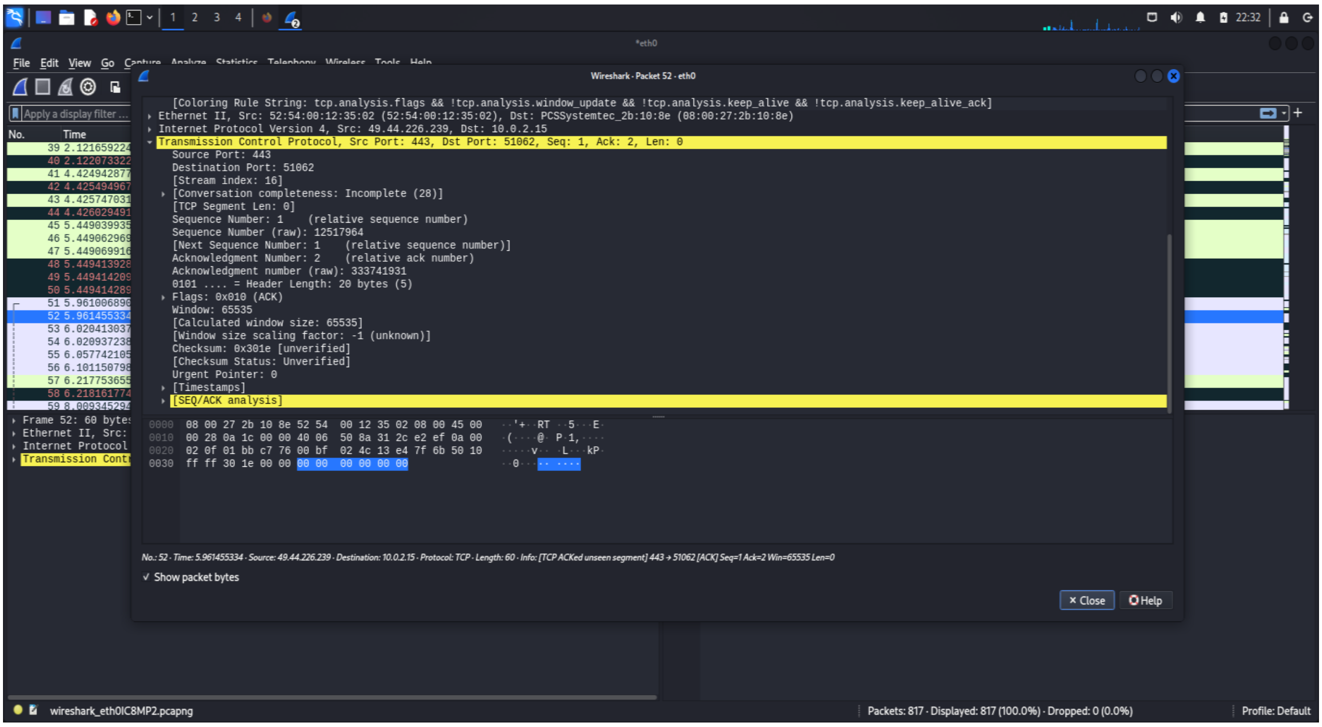
```
0000  08 00 27 2b 10 8e 52 54  00 12 35 02 08 00 45 00   ··'+··RT ··5···E·
0010  00 28 0a 1b 00 00 40 06  de f0 12 9b 73 1b 0a 00   ·(····@· ····s···
0020  02 0f 00 50 c1 60 01 21  13 b1 9c 5f 1f b3 50 10   ···P·`·! ···_··P·
0030  ff ff 8b 7a 00 00 00 00  00 00 00 00               ···z···· ····
```

wireshark_eth0IC8MP2.pcapng | Packets: 817 · Displayed: 122 (14.9%) · Dropped: 0 (0.0%) | Profile: Default

Step-4)

Inspect Packet Contents

Expand the packet details to inspect the header and payload of each layer.


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter …
Wireshark · Packet 52 · eth0
× Close
Help

```
No.  Time
  39 2.121659224
  40 2.122073322
  41 4.424942877
  42 4.425494967
  43 4.425747031
  44 4.426029491
  45 5.449039935
  46 5.449062969
  47 5.449069916
  48 5.449413928
  49 5.449414209
  50 5.449414289
  51 5.961006890
  52 5.961455334
  53 6.020413037
  54 6.020937238
  55 6.057742105
  56 6.101150798
  57 6.217753655
  58 6.218161774
  59 8.009345294
▸ Frame 52: 60 bytes
▸ Ethernet II, Src:
▸ Internet Protocol
▸ Transmission Cont
```

```
    [Coloring Rule String: tcp.analysis.flags && !tcp.analysis.window_update && !tcp.analysis.keep_alive && !tcp.analysis.keep_alive_ack]
▸ Ethernet II, Src: 52:54:00:12:35:02 (52:54:00:12:35:02), Dst: PCSSystemtec_2b:10:8e (08:00:27:2b:10:8e)
▸ Internet Protocol Version 4, Src: 49.44.226.239, Dst: 10.0.2.15
▾ Transmission Control Protocol, Src Port: 443, Dst Port: 51062, Seq: 1, Ack: 2, Len: 0
    Source Port: 443
    Destination Port: 51062
    [Stream index: 16]
  ▸ [Conversation completeness: Incomplete (28)]
    [TCP Segment Len: 0]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 12517964
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 2    (relative ack number)
    Acknowledgment number (raw): 333741931
    0101 .... = Header Length: 20 bytes (5)
  ▸ Flags: 0x010 (ACK)
    Window: 65535
    [Calculated window size: 65535]
    [Window size scaling factor: -1 (unknown)]
    Checksum: 0x301e [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  ▸ [Timestamps]
  ▸ [SEQ/ACK analysis]
```

```
0000  08 00 27 2b 10 8e 52 54  00 12 35 02 08 00 45 00   ··'+··RT ··5···E·
0010  00 28 0a 1c 00 00 40 06  50 8a 31 2c e2 ef 0a 00   ·(····@· P·1,····
0020  02 0f 01 bb c7 76 00 bf  02 4c 13 e4 7f 6b 50 10   ·····v·· ·L···kP·
0030  ff ff 30 1e 00 00 00 00  00 00 00 00               ··0···· ····
```

No.: 52 · Time: 5.961455334 · Source: 49.44.226.239 · Destination: 10.0.2.15 · Protocol: TCP · Length: 60 · Info: [TCP ACKed unseen segment] 443 → 51062 [ACK] Seq=1 Ack=2 Win=65535 Len=0

☑ Show packet bytes

wireshark_eth0IC8MP2.pcapng | Packets: 817 · Displayed: 817 (100.0%) · Dropped: 0 (0.0%) | Profile: Default

Step-5)

- Save and Export Captures
- Save capture file(which would be a pcap/pcapng file extension)
- Export specific packets

Conclusion

This Setup allows you to explore and understand network traffic.