Name of Student : Sunny Satish Halkatti		
Roll Number : 17		**LAB Assignment Number: 10**
Title of LAB Assignment: Program Analyze the network traffic and performance parameters of the network using Wireshark.		
DOP : 25-05-2023		**DOS :** 01-06-2023
CO Mapped : CO3	**PO Mapped:** PO1, PO3, PO4, PO5, PO7, PSO1	**Signature :**

Sunny S.H **DIVISION B** **ROLL NO 17**

NWL - Practical - 10

AIM: Program Analyze the network traffic and performance parameters of the network using Wireshark..

THEORY:

Wireshark:

Wireshark is a network or protocol analyser (also known as a network sniffer) available for free at the Wireshark website. It is used to analyze the structure of different network protocols and has the ability to demonstrate encapsulation. The analyser operates on Unix, Linux and Microsoft Windows operating systems, and employs the GTK+ widget toolkit and pcap for packet capturing. Wireshark and other terminal-based free software versions like Tshark are released under the GNU General Public License.

What Does Wireshark Mean?

- Wireshark is a free and open-source network protocol analyser that enables users to interactively browse the data traffic on a computer network. The development project was started under the name Ethereal, but was renamed Wireshark in 2006.
- Many networking developers from all around the world have contributed to this project with network analysis, troubleshooting, software development and communication protocols. Wireshark is used in many educational institutions and other industrial sectors.
- Wireshark shares many characteristics with tcpdump. The difference is that it supports a graphical user interface (GUI) and has information filtering features. In addition, Wireshark permits the user to see all the traffic being passed over the network.

Features of Wireshark include:

- Data is analyzed either from the wire over the network connection or from data files that have already captured data packets.
- Supports live data reading and analysis for a wide range of networks (including Ethernet, IEEE 802.11, point-to-point Protocol (PPP) and loopback).
- With the help of GUI or other versions, users can browse captured data networks.
- For programmatically editing and converting the captured files to the editcap application, users can use command line switches.
- Display filters are used to filter and organize the data display.
- New protocols can be scrutinized by creating plug-ins.
- Captured traffic can also trace Voice over Internet (VoIP) calls over the network.
- When using Linux, it is also possible to capture raw USB traffic.

What Does Network Traffic Mean?

- Network traffic refers to the amount of data moving across a network at a given point of time. Network data is mostly encapsulated in network packets, which provide the load in the network. Network traffic is the main component for network traffic measurement, network traffic control and simulation. The proper organization of network traffic helps in ensuring the quality of service in a given network. Network traffic is also known as data traffic.

Network Traffic:

Network traffic is the main component for bandwidth measurement and management. Moreover, various topologies of the network can only be implemented based on the amount of network traffic in the system.

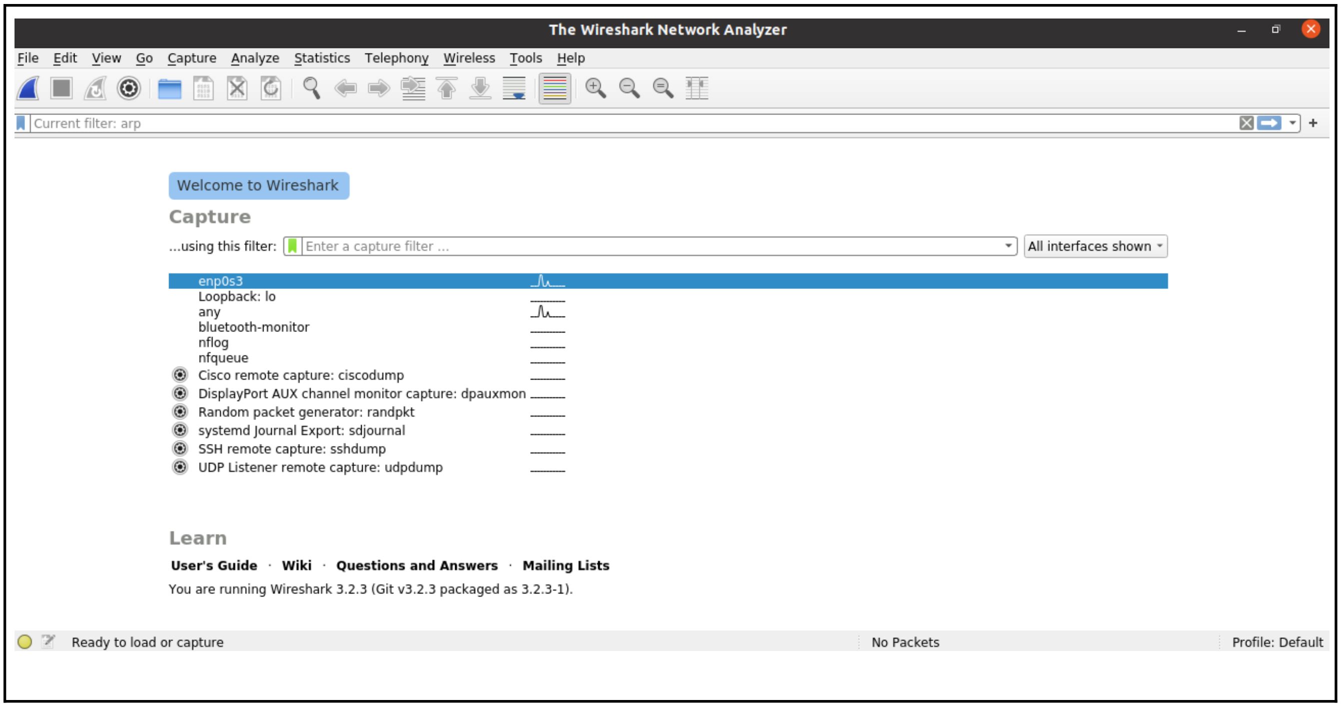
Network traffic can be broadly classified into the following categories:

- Busy/heavy traffic - High bandwidth is consumed in this traffic
- Non-real-time traffic - Consumption of bandwidth during working hours
- Interactive traffic - Is subject to competition for bandwidth and could result in poor response times if prioritization of applications and traffic is not set
- Latency-sensitive traffic - Is subject to competition for bandwidth andcould result in poor response times

Proper analysis of network traffic provides the organization with the following benefits:

- Identifying network bottlenecks - There could be users or applications that consume high amounts of bandwidth, thus constituting a major part of the network traffic. Different solutions can be implemented to tackle these.
- Network security - unusual amount of traffic in a network is a possible sign of an attack. Network traffic reports provide valuable insights into preventing such attacks.
- Network engineering - Knowing the usage levels of the network allows future requirements to be analysed.

Execution:



Current filter: arp

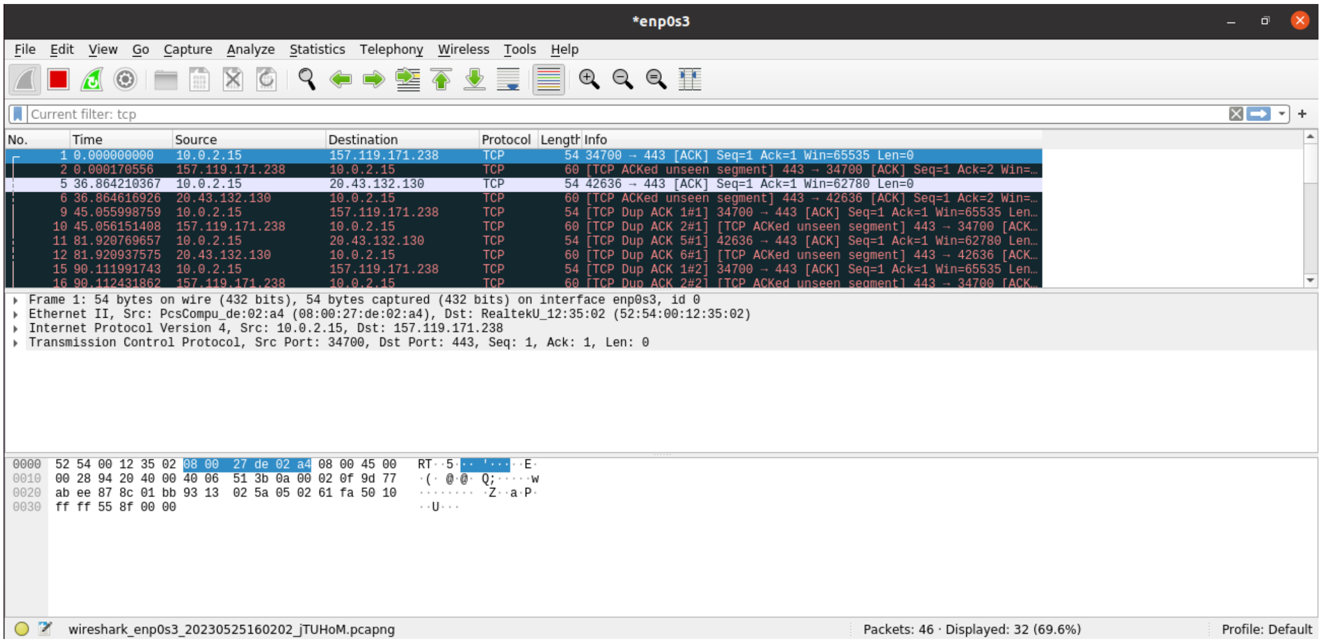
...using this filter: Enter a capture filter ... All interfaces shown

enp0s3
Loopback: lo
any
bluetooth-monitor
nflog
nfqueue
Cisco remote capture: ciscodump
DisplayPort AUX channel monitor capture: dpauxmon
Random packet generator: randpkt
systemd Journal Export: sdjournal
SSH remote capture: sshdump
UDP Listener remote capture: udpdump

You are running Wireshark 3.2.3 (Git v3.2.3 packaged as 3.2.3-1).

Ready to load or capture No Packets Profile: Default

Sunny S.H **DIVISION B** **ROLL NO 17**



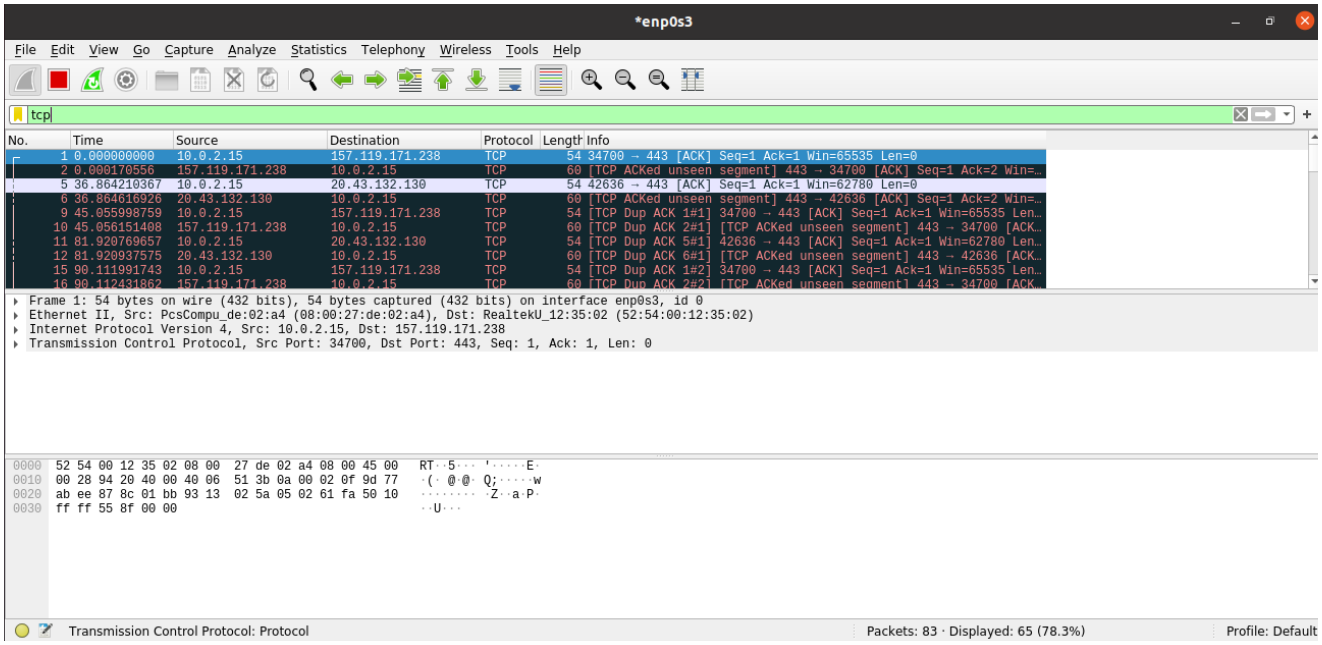
*enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Current filter: tcp

```
No.  Time            Source           Destination      Protocol Length Info
   1 0.000000000     10.0.2.15        157.119.171.238  TCP      54 34700 → 443 [ACK] Seq=1 Ack=1 Win=65535 Len=0
   2 0.000170556     157.119.171.238  10.0.2.15        TCP      60 [TCP ACKed unseen segment] 443 → 34700 [ACK] Seq=1 Ack=2 Win=…
   5 36.864210367    10.0.2.15        20.43.132.130    TCP      54 42636 → 443 [ACK] Seq=1 Ack=1 Win=62780 Len=0
   6 36.864616926    20.43.132.130    10.0.2.15        TCP      60 [TCP ACKed unseen segment] 443 → 42636 [ACK] Seq=1 Ack=2 Win=…
   9 45.055998759    10.0.2.15        157.119.171.238  TCP      54 [TCP Dup ACK 1#1] 34700 → 443 [ACK] Seq=1 Ack=1 Win=65535 Len…
  10 45.056151408    157.119.171.238  10.0.2.15        TCP      60 [TCP Dup ACK 2#1] [TCP ACKed unseen segment] 443 → 34700 [ACK…
  11 81.920769657    10.0.2.15        20.43.132.130    TCP      54 [TCP Dup ACK 5#1] 42636 → 443 [ACK] Seq=1 Ack=1 Win=62780 Len…
  12 81.920937575    20.43.132.130    10.0.2.15        TCP      60 [TCP Dup ACK 6#1] [TCP ACKed unseen segment] 443 → 42636 [ACK…
  15 90.111991743    10.0.2.15        157.119.171.238  TCP      54 [TCP Dup ACK 1#2] 34700 → 443 [ACK] Seq=1 Ack=1 Win=65535 Len…
  16 90.112431862    157.119.171.238  10.0.2.15        TCP      60 [TCP Dup ACK 2#2] [TCP ACKed unseen segment] 443 → 34700 [ACK…
```

```
Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface enp0s3, id 0
Ethernet II, Src: PcsCompu_de:02:a4 (08:00:27:de:02:a4), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 157.119.171.238
Transmission Control Protocol, Src Port: 34700, Dst Port: 443, Seq: 1, Ack: 1, Len: 0
```

```
0000  52 54 00 12 35 02 08 00  27 de 02 a4 08 00 45 00   RT··5··· '·····E·
0010  00 28 94 20 40 00 40 06  51 3b 0a 00 02 0f 9d 77   ·(· @·@· Q;·····w
0020  ab ee 87 8c 01 bb 93 13  02 5a 05 02 61 fa 50 10   ········ ·Z··a·P·
0030  ff ff 55 8f 00 00                                  ··U···
```

wireshark_enp0s3_20230525160202_jTUHoM.pcapng   Packets: 46 · Displayed: 32 (69.6%)   Profile: Default



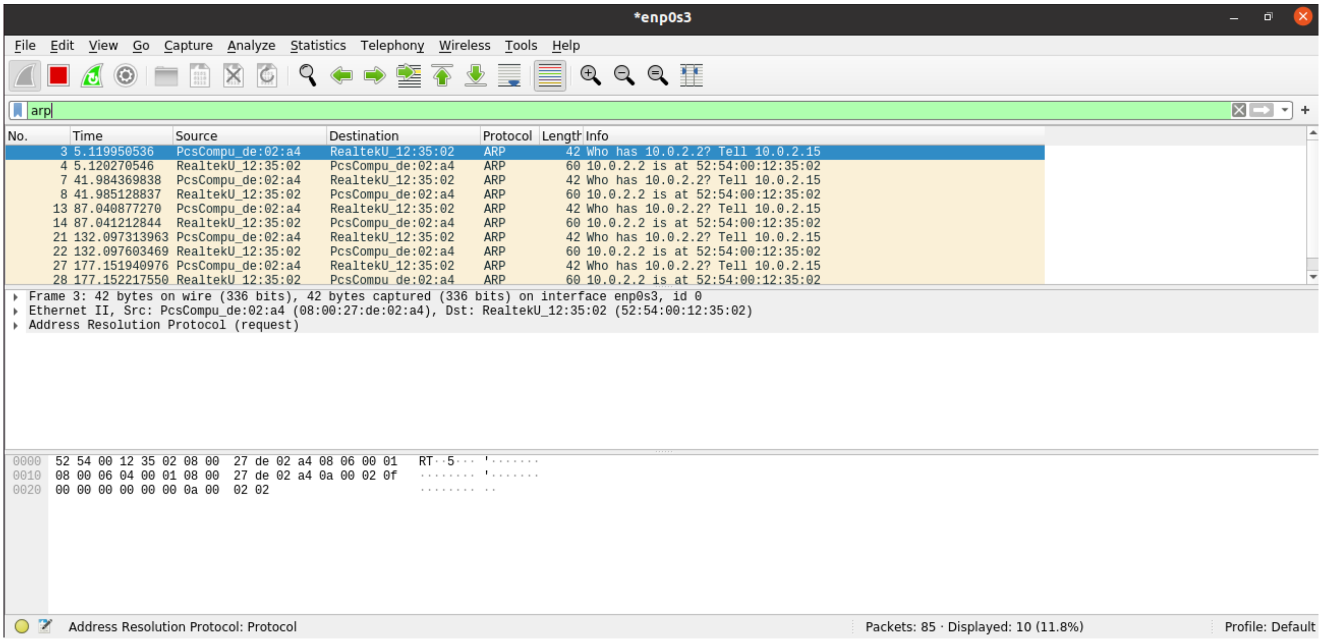
*enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp

```
No.  Time            Source           Destination      Protocol Length Info
   1 0.000000000     10.0.2.15        157.119.171.238  TCP      54 34700 → 443 [ACK] Seq=1 Ack=1 Win=65535 Len=0
   2 0.000170556     157.119.171.238  10.0.2.15        TCP      60 [TCP ACKed unseen segment] 443 → 34700 [ACK] Seq=1 Ack=2 Win=…
   5 36.864210367    10.0.2.15        20.43.132.130    TCP      54 42636 → 443 [ACK] Seq=1 Ack=1 Win=62780 Len=0
   6 36.864616926    20.43.132.130    10.0.2.15        TCP      60 [TCP ACKed unseen segment] 443 → 42636 [ACK] Seq=1 Ack=2 Win=…
   9 45.055998759    10.0.2.15        157.119.171.238  TCP      54 [TCP Dup ACK 1#1] 34700 → 443 [ACK] Seq=1 Ack=1 Win=65535 Len…
  10 45.056151408    157.119.171.238  10.0.2.15        TCP      60 [TCP Dup ACK 2#1] [TCP ACKed unseen segment] 443 → 34700 [ACK…
  11 81.920769657    10.0.2.15        20.43.132.130    TCP      54 [TCP Dup ACK 5#1] 42636 → 443 [ACK] Seq=1 Ack=1 Win=62780 Len…
  12 81.920937575    20.43.132.130    10.0.2.15        TCP      60 [TCP Dup ACK 6#1] [TCP ACKed unseen segment] 443 → 42636 [ACK…
  15 90.111991743    10.0.2.15        157.119.171.238  TCP      54 [TCP Dup ACK 1#2] 34700 → 443 [ACK] Seq=1 Ack=1 Win=65535 Len…
  16 90.112431862    157.119.171.238  10.0.2.15        TCP      60 [TCP Dup ACK 2#2] [TCP ACKed unseen segment] 443 → 34700 [ACK…
```

```
Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface enp0s3, id 0
Ethernet II, Src: PcsCompu_de:02:a4 (08:00:27:de:02:a4), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 157.119.171.238
Transmission Control Protocol, Src Port: 34700, Dst Port: 443, Seq: 1, Ack: 1, Len: 0
```

```
0000  52 54 00 12 35 02 08 00  27 de 02 a4 08 00 45 00   RT··5··· '·····E·
0010  00 28 94 20 40 00 40 06  51 3b 0a 00 02 0f 9d 77   ·(· @·@· Q;·····w
0020  ab ee 87 8c 01 bb 93 13  02 5a 05 02 61 fa 50 10   ········ ·Z··a·P·
0030  ff ff 55 8f 00 00                                  ··U···
```

Transmission Control Protocol: Protocol   Packets: 83 · Displayed: 65 (78.3%)   Profile: Default


*enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
arp

No.  Time          Source             Destination        Protocol Length Info
   3 5.119950536   PcsCompu_de:02:a4  RealtekU_12:35:02  ARP      42 Who has 10.0.2.2? Tell 10.0.2.15
   4 5.120270546   RealtekU_12:35:02  PcsCompu_de:02:a4  ARP      60 10.0.2.2 is at 52:54:00:12:35:02
   7 41.984369838  PcsCompu_de:02:a4  RealtekU_12:35:02  ARP      42 Who has 10.0.2.2? Tell 10.0.2.15
   8 41.985128837  RealtekU_12:35:02  PcsCompu_de:02:a4  ARP      60 10.0.2.2 is at 52:54:00:12:35:02
  13 87.040877270  PcsCompu_de:02:a4  RealtekU_12:35:02  ARP      42 Who has 10.0.2.2? Tell 10.0.2.15
  14 87.041212844  RealtekU_12:35:02  PcsCompu_de:02:a4  ARP      60 10.0.2.2 is at 52:54:00:12:35:02
  21 132.097313963 PcsCompu_de:02:a4  RealtekU_12:35:02  ARP      42 Who has 10.0.2.2? Tell 10.0.2.15
  22 132.097603469 RealtekU_12:35:02  PcsCompu_de:02:a4  ARP      60 10.0.2.2 is at 52:54:00:12:35:02
  27 177.151940976 PcsCompu_de:02:a4  RealtekU_12:35:02  ARP      42 Who has 10.0.2.2? Tell 10.0.2.15
  28 177.152217550 RealtekU_12:35:02  PcsCompu_de:02:a4  ARP      60 10.0.2.2 is at 52:54:00:12:35:02

▸ Frame 3: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface enp0s3, id 0
▸ Ethernet II, Src: PcsCompu_de:02:a4 (08:00:27:de:02:a4), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
▸ Address Resolution Protocol (request)

0000  52 54 00 12 35 02 08 00  27 de 02 a4 08 06 00 01   RT··5··· '·······
0010  08 00 06 04 00 01 08 00  27 de 02 a4 0a 00 02 0f   ········ '·······
0020  00 00 00 00 00 00 0a 00  02 02                     ········ ··

Address Resolution Protocol: Protocol          Packets: 85 · Displayed: 10 (11.8%)          Profile: Default
```

Conclusions:

We have successfully analyzed the network traffic and performance parameters of the network using Wireshark.