# COMPUTER NETWORKS

*SAKSHAM KUMAR*

COMPUTER SCIENCE AND ENGINEERING
ID - 2022UCP1700
SECTION- A4

# ASSIGNMENT – 11

# Analyzing Packets:

## Browsing a website:

```
▾ Internet Protocol Version 4, Src: 172.18.12.13, Dst: 34.107.221.82
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 355
    Identification: 0x7a51 (31313)
  ▸ 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0x0767 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 172.18.12.13
    Destination Address: 34.107.221.82
```

## Sending an email:

```
▾ Internet Protocol Version 4, Src: mnit-HP-Elite-Tower-600-G9-Desktop-PC-11.local (172.18.12.13), Dst: prod.detectportal.prod.cloudops.mozgcp.net (34.107.221
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 353
    Identification: 0x1d4d (7501)
  ▸ 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0x646d [validation disabled]
    [Header checksum status: Unverified]
    Source Address: mnit-HP-Elite-Tower-600-G9-Desktop-PC-11.local (172.18.12.13)
    Destination Address: prod.detectportal.prod.cloudops.mozgcp.net (34.107.221.82)
```

## Streaming a video:

```
▾ Internet Protocol Version 4, Src: mnit-HP-Elite-Tower-600-G9-Desktop-PC.local (172.18.12.13), Dst: 117.236.66.236 (117.236.66.236)
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1385
    Identification: 0x0000 (0)
  ▸ 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: UDP (17)
    Header Checksum: 0xc48c [validation disabled]
    [Header checksum status: Unverified]
    Source Address: mnit-HP-Elite-Tower-600-G9-Desktop-PC.local (172.18.12.13)
    Destination Address: 117.236.66.236 (117.236.66.236)
▸ User Datagram Protocol, Src Port: 35294, Dst Port: 443
▸ Data (1357 bytes)
```

## Downloading a file:

```
▾ Internet Protocol Version 4, Src: mnit-HP-Elite-Tower-600-G9-Desktop-PC.local (172.18.12.13), Dst: prod.detectportal.prod.cloudops.mozgcp.net (34.107.221.82
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 52
    Identification: 0x8d79 (36217)
  ▸ 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0xf56d [validation disabled]
    [Header checksum status: Unverified]
    Source Address: mnit-HP-Elite-Tower-600-G9-Desktop-PC.local (172.18.12.13)
    Destination Address: prod.detectportal.prod.cloudops.mozgcp.net (34.107.221.82)
```

## TCP:

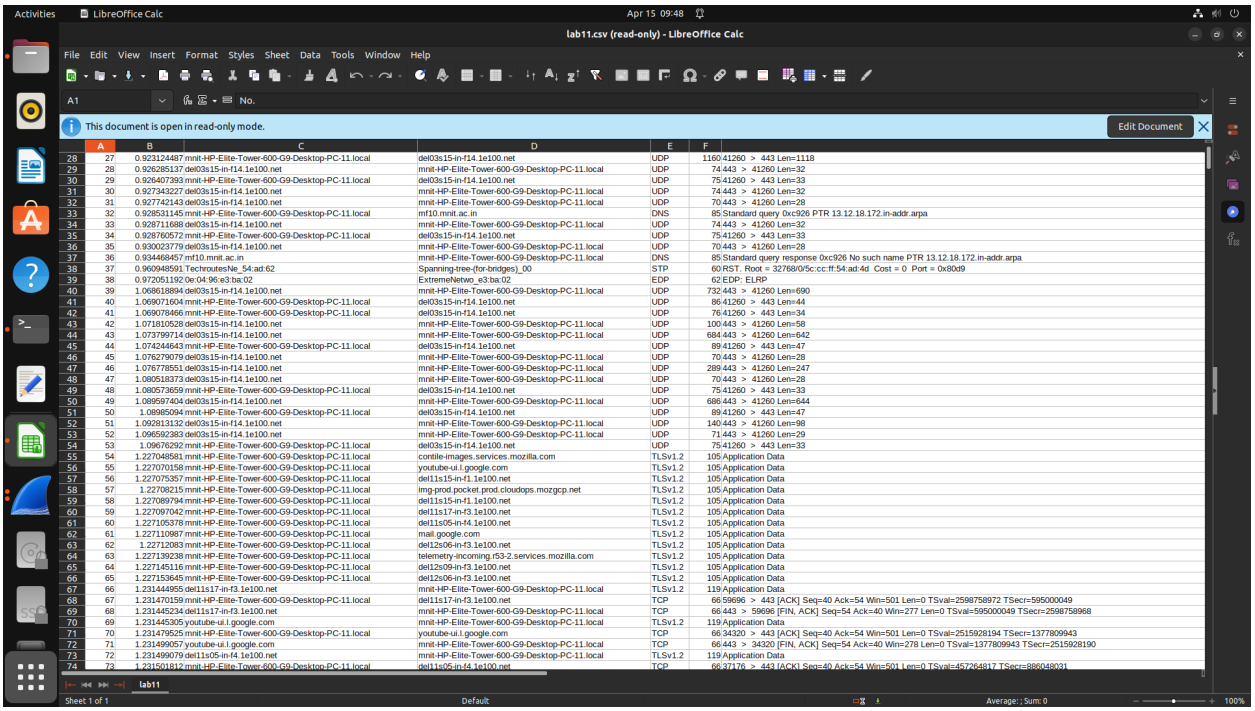
```
Internet Protocol Version 4, Src: mnit-HP-Elite-Tower-600-G9-Desktop-PC.local (172.18.12.13), Dst: prod.detectportal.prod.cloudops.mozgcp.net (34.107.221.82)
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 52
    Identification: 0x8d79 (36217)
  ▸ 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0xf56d [validation disabled]
    [Header checksum status: Unverified]
    Source Address: mnit-HP-Elite-Tower-600-G9-Desktop-PC-11.local (172.18.12.13)
    Destination Address: prod.detectportal.prod.cloudops.mozgcp.net (34.107.221.82)
▸ Transmission Control Protocol, Src Port: 51194, Dst Port: 80, Seq: 305, Ack: 217, Len: 0
```

## ICMP:

```
Internet Protocol Version 6, Src: mnit-HP-Elite-Tower-600-G9-Desktop-PC.local (fe80::2fb0:de7a:3f2a:605d), Dst: ff02::16 (ff02::16)
    0110 .... = Version: 6
  ▸ .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... 0000 0000 0000 0000 0000 = Flow Label: 0x00000
    Payload Length: 56
    Next Header: IPv6 Hop-by-Hop Option (0)
    Hop Limit: 1
    Source Address: mnit-HP-Elite-Tower-600-G9-Desktop-PC.local (fe80::2fb0:de7a:3f2a:605d)
    Destination Address: ff02::16 (ff02::16)
  ▸ IPv6 Hop-by-Hop Option
▸ Internet Control Message Protocol v6
```

# Exporting Results:

## CSV File:



## Q1)

When a packet is created, it contains the destination IP address, indicating where it needs to be sent. Routers along the path use this information to forward the packet towards its destination.

Routers use the destination IP address to make routing decisions. Each router maintains a routing table that contains information about how to reach different networks or hosts. When a router receives a packet, it looks at the destination IP address and consults its routing table to determine the next hop towards the destination.

1. **Source IP Address**: This address identifies the sender of the packet. When a device sends a packet, it includes its own IP address as the source. Routers along the path use this address to know where the packet originated. The source IP address helps routers determine how to send response packets back to the sender.
2. **Destination IP Address**: This address identifies the intended recipient of the packet. Routers use the destination IP address to make forwarding decisions. Each router in the path examines the destination IP address and consults its routing table to determine the next hop (next router) to which it should send the packet. This process continues until the packet reaches its final destination.

## Q2)

The TTL field is primarily used to prevent packets from circulating endlessly in a network. Each time a router forwards a packet, it decrements the TTL value by at least one. If the TTL field reaches zero before the packet reaches its destination, the packet is discarded, and an ICMP (Internet Control Message Protocol) error message, specifically a "Time Exceeded" message, may be sent back to the source.

1. **Significance of TTL**:
   a. **Preventing Infinite Loops**: TTL prevents packets from circulating endlessly in a network. Each router that forwards a packet decrements the TTL value by at least one. If the TTL reaches zero before reaching the destination, the packet is discarded, preventing infinite loops and ensuring that packets do not congest the network indefinitely.
   a. **Packet Aging**: TTL also serves as a mechanism for packet aging. Since TTL is decremented at each hop, packets with low TTL values are considered older and are less likely to be delivered successfully. This helps prevent outdated or stale packets from reaching their destinations.

## Q3)

IPv4:

1) The header length is variable, typically ranging from 20 to 60 bytes.
2) Uses 32-bit (4-byte) addresses, resulting in approximately 4.3 billion unique addresses.
3) Contains fields such as Version, Header Length, Type of Service (TOS), Total Length, Identification, Flags, Fragment Offset, Time to Live (TTL), Protocol, Header Checksum, Source Address, and Destination Address.

IPv6:

1) The header length is fixed at 40 bytes.
2) Uses 128-bit (16-byte) addresses, resulting in an enormously larger address space, capable of accommodating approximately 340 undecillion unique addresses.
3) Contains fields such as Version, Traffic Class, Flow Label, Payload Length, Next Header, Hop Limit, Source Address, and Destination Address.

# THE END