

# CSE421 Lab 2

## Tahsin Ashrafee Susmit

### ID:20301088

```
Command Prompt
Microsoft Windows [Version 10.0.22621.3007]
(c) Microsoft Corporation. All rights reserved.

C:\Users\tahsi>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

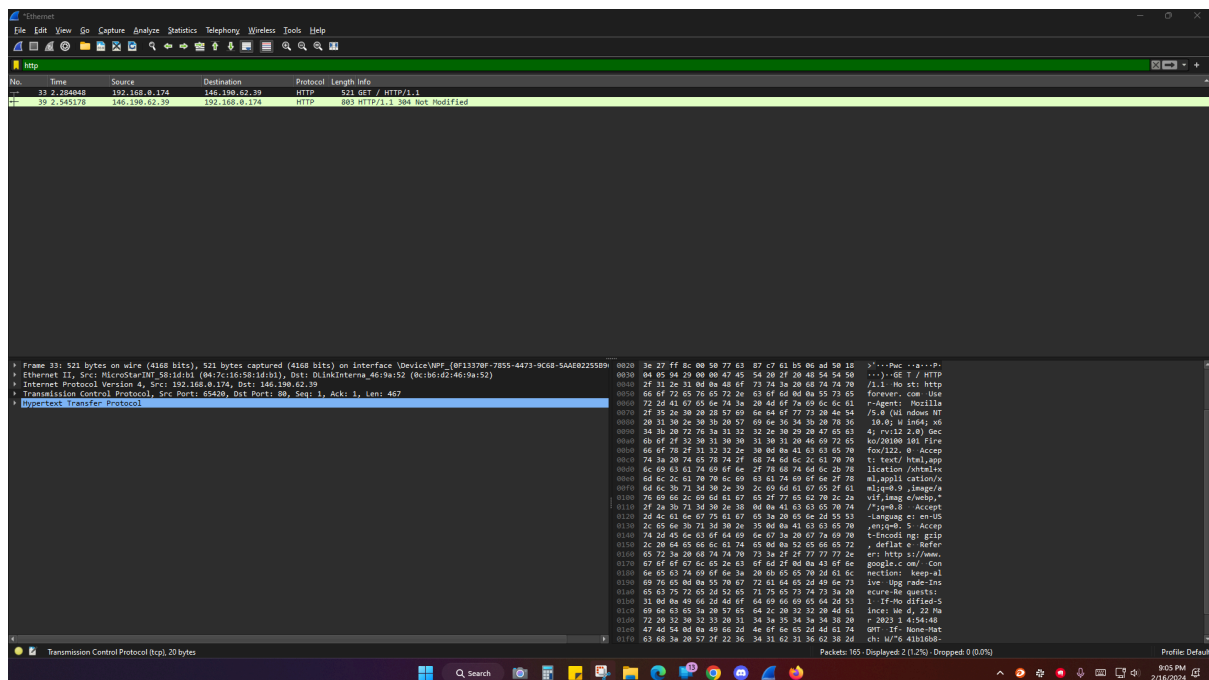
    Connection-specific DNS Suffix  . : 
    IPv6 Address. . . . . : 2401:f40:1323:39:abd6:2349:c9d8:d1be
    Temporary IPv6 Address. . . . . : 2401:f40:1323:39:4924:e05f:2b0f:f6d9
    Temporary IPv6 Address. . . . . : 2401:f40:1323:39:d876:9429:9884:6b63
    Temporary IPv6 Address. . . . . : 2401:f40:1323:39:f85b:857b:17f:134a
    Link-local IPv6 Address . . . . . : fe80::f9f3:b45a:5ef3:f8fd%3
    IPv4 Address. . . . . : 192.168.0.174
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::eb6:d2ff:fe46:9a52%3
                              192.168.0.1

Ethernet adapter Ethernet 3:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::57a1:6a4c:40e7:fb87%9
    IPv4 Address. . . . . : 192.168.56.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :

Wireless LAN adapter Wi-Fi:
```

## Wireshark



The IP address of my device is 192.168.0.174, and the IP address of HTTP Forever Website is 146.190.62.39

## Request Packet

### Frame:

```
▼ Frame 33: 521 bytes on wire (4168 bits), 521 bytes captured (4168 bits) on interface \Device\NPF_{0F13370F-7855-4473-9C68-5AAE02255B96}, id 0
  Section number: 1
  ▼ Interface id: 0 (\Device\NPF_{0F13370F-7855-4473-9C68-5AAE02255B96})
    Interface name: \Device\NPF_{0F13370F-7855-4473-9C68-5AAE02255B96}
    Interface description: Ethernet
    Encapsulation type: Ethernet (1)
    Arrival Time: Feb 16, 2024 20:58:38.597947000 Bangladesh Standard Time
    UTC Arrival Time: Feb 16, 2024 14:58:38.597947000 UTC
    Epoch Arrival Time: 1708095518.597947000
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.037821000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 2.284048000 seconds]
    Frame Number: 33
    Frame Length: 521 bytes (4168 bits)
    Capture Length: 521 bytes (4168 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
  ▶ Ethernet II, Src: MicroStarINT_58:1d:b1 (04:7c:16:58:1d:b1), Dst: DLinkInterna_46:9a:52 (0c:b6:d2:46:9a:52)
  ▶ Internet Protocol Version 4, Src: 192.168.0.174, Dst: 146.190.62.39
  ▶ Transmission Control Protocol, Src Port: 65420, Dst Port: 80, Seq: 1, Ack: 1, Len: 467
  ▶ Hypertext Transfer Protocol
```

Frames reside at the Data Link Layer.

### Ethernet II:

```
▼ Frame 33: 521 bytes on wire (4168 bits), 521 bytes captured (4168 bits) on interface \Device\NPF_{0F13370F-7855-4473-9C68-5AAE02255B96}, id 0
▼ Ethernet II, Src: MicroStarINT_58:1d:b1 (04:7c:16:58:1d:b1), Dst: DLinkInterna_46:9a:52 (0c:b6:d2:46:9a:52)
  Destination: DLinkInterna_46:9a:52 (0c:b6:d2:46:9a:52)
    Address: DLinkInterna_46:9a:52 (0c:b6:d2:46:9a:52)
    ....0. .... = LG bit: Globally unique address (factory default)
    ....0. .... = IG bit: Individual address (unicast)
  Source: MicroStarINT_58:1d:b1 (04:7c:16:58:1d:b1)
    Address: MicroStarINT_58:1d:b1 (04:7c:16:58:1d:b1)
    ....0. .... = LG bit: Globally unique address (factory default)
    ....0. .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
  ▶ Internet Protocol Version 4, Src: 192.168.0.174, Dst: 146.190.62.39
  ▶ Transmission Control Protocol, Src Port: 65420, Dst Port: 80, Seq: 1, Ack: 1, Len: 467
  ▶ Hypertext Transfer Protocol
```

The Ethernet II also falls on the Data Link Layer. We can see the Destination Mac Address at first then the source Mac Address is evident. Also, it shows that data transfer is done via the IPv4 protocol.

## IPV4:

```
Frame 33: 521 bytes on wire (4168 bits), 521 bytes captured (4168 bits) on interface \Device\NPF_{0F13370F-7855-4473-9C68-5AAE02255B96}, id 0
Ethernet II, Src: MicroStarINT_58:1d:b1 (04:7c:16:58:1d:b1), Dst: DLinkInterna_46:9a:52 (0c:b6:d2:46:9a:52)
Internet Protocol Version 4, Src: 192.168.0.174, Dst: 146.190.62.39
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    0000 00.. = Differentiated Services Codepoint: Default (0)
    .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 507
  Identification: 0xf221 (61985)
  010. .... = Flags: 0x2, Don't fragment
    0... .... = Reserved bit: Not set
    .1.. .... = Don't fragment: Set
    ..0. .... = More fragments: Not set
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 128
  Protocol: TCP (6)
  Header Checksum: 0x0000 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.168.0.174
  Destination Address: 146.190.62.39
Transmission Control Protocol, Src Port: 65420, Dst Port: 80, Seq: 1, Ack: 1, Len: 467
Hypertext Transfer Protocol
```

The IPV4 falls under Network Layer. The source is 192.168.0.174 meaning my PC, and the destination 146.190.62.39 meaning the website I searched for. The packet contains a header of 20 bytes, utilising TCP for data transmission. Its overall size is 507 bytes and includes a Time-to-Live (TTL) value 128.

## TCP:

```
Frame 33: 521 bytes on wire (4168 bits), 521 bytes captured (4168 bits) on interface \Device\NPF_{0F13370F-7855-4473-9C68-5AAE02255B96}, id 0
Ethernet II, Src: MicroStarINT_58:1d:b1 (04:7c:16:58:1d:b1), Dst: DLinkInterna_46:9a:52 (0c:b6:d2:46:9a:52)
Internet Protocol Version 4, Src: 192.168.0.174, Dst: 146.190.62.39
Transmission Control Protocol, Src Port: 65420, Dst Port: 80, Seq: 1, Ack: 1, Len: 467
  Source Port: 65420
  Destination Port: 80
  [Stream index: 8]
  [Conversation completeness: Incomplete (12)]
  [TCP Segment Len: 467]
  Sequence Number: 1 (relative sequence number)
  Sequence Number (raw): 2003011527
  [Next Sequence Number: 468 (relative sequence number)]
  Acknowledgment Number: 1 (relative ack number)
  Acknowledgment number (raw): 1639253677
  0101 .... = Header Length: 20 bytes (5)
  Flags: 0x018 (PSH, ACK)
  Window: 1029
  [Calculated window size: 1029]
  [Window size scaling factor: -1 (unknown)]
  Checksum: 0x9429 [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
  [Timestamps]
    [Time since first frame in this TCP stream: 0.000000000 seconds]
    [Time since previous frame in this TCP stream: 0.000000000 seconds]
  [SEQ/ACK analysis]
    [Bytes in flight: 467]
    [Bytes sent since last PSH flag: 467]
  TCP payload (467 bytes)
Hypertext Transfer Protocol
```

TCP operates within the transport layer. The destination port for the HTTP Forever website is 80, while the source port, originating from my PC, is designated as 65420. Both the sequence number and acknowledgment number are identified as 1. This signifies the successful initiation of the TCP communication session, where the sender has sent the initial segment of data with sequence number 1, and the receiver has acknowledged its receipt by confirming the sequence number as 1.

## HTTP:

```
▶ Frame 33: 521 bytes on wire (4168 bits), 521 bytes captured (4168 bits) on interface \Device\NPF_{0F13370F-7855-4473-9C68-5AAE02255896}, id 0
▶ Ethernet II, Src: MicroStarINT 58:1d:b1 (04:7c:16:58:1d:b1), Dst: DLinkInterna_46:9a:52 (0c:b6:d2:46:9a:52)
▶ Internet Protocol Version 4, Src: 192.168.0.174, Dst: 146.190.62.39
▶ Transmission Control Protocol, Src Port: 65420, Dst Port: 80, Seq: 1, Ack: 1, Len: 467
▼ Hypertext Transfer Protocol
  ▶ GET / HTTP/1.1\r\n
    Host: httpforever.com\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:122.0) Gecko/20100101 Firefox/122.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Referer: https://www.google.com/\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    If-Modified-Since: Wed, 22 Mar 2023 14:54:48 GMT\r\n
    If-None-Match: W/"641b16b8-1404"\r\n
    \r\n
    [Full request URI: http://httpforever.com/]
    [HTTP request 1/1]
    [Response in frame: 39]
```

HTTP falls under the Application Layer. Using the Get Method the client (My PC) is requesting data from the website HTTPforever.com. HTTP/1.1: is the version of the HTTP protocol being used. “\r\n” means 'Carriage Return' to the print head back to the start of line. Host: httpforever.com: specifies the host to which the request is being sent. It informs the server of the domain it should process the request for. Then the browser along with its version is specified. After that the acceptance of media type, language and encoding is declared. Then the Connection: keep-alive indicates the fact of Persistent Transmission. After that for the cache and proxy servers, the conditional get, IF-Modified-Since indicates when it was last updated and if required to be updated or not. Lastly, the server's response to that request is likely to contain 39 frames of data.

# Response Packet

## Frame:

```
▼ Frame 39: 803 bytes on wire (6424 bits), 803 bytes captured (6424 bits) on interface \Device\NPF_{0F13370F-7855-4473-9C68-5AAE02255B96}, id 0
  Section number: 1
  ▼ Interface id: 0 (\Device\NPF_{0F13370F-7855-4473-9C68-5AAE02255B96})
    Interface name: \Device\NPF_{0F13370F-7855-4473-9C68-5AAE02255B96}
    Interface description: Ethernet
    Encapsulation type: Ethernet (1)
    Arrival Time: Feb 16, 2024 20:58:38.859077000 Bangladesh Standard Time
    UTC Arrival Time: Feb 16, 2024 14:58:38.859077000 UTC
    Epoch Arrival Time: 1708095518.859077000
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.082427000 seconds]
    [Time delta from previous displayed frame: 0.261130000 seconds]
    [Time since reference or first frame: 2.545178000 seconds]
    Frame Number: 39
    Frame Length: 803 bytes (6424 bits)
    Capture Length: 803 bytes (6424 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
  ▶ Ethernet II, Src: DLinkInterna_46:9a:52 (0c:b6:d2:46:9a:52), Dst: MicroStarINT_58:1d:b1 (04:7c:16:58:1d:b1)
  ▶ Internet Protocol Version 4, Src: 146.190.62.39, Dst: 192.168.0.174
  ▶ Transmission Control Protocol, Src Port: 80, Dst Port: 65420, Seq: 1, Ack: 468, Len: 749
  ▶ Hypertext Transfer Protocol
```

Frames reside at the Data Link Layer.

## Ethernet II:

```
▼ Frame 39: 803 bytes on wire (6424 bits), 803 bytes captured (6424 bits) on interface \Device\NPF_{0F13370F-7855-4473-9C68-5AAE02255B96}, id 0
  ▼ Ethernet II, Src: DLinkInterna_46:9a:52 (0c:b6:d2:46:9a:52), Dst: MicroStarINT_58:1d:b1 (04:7c:16:58:1d:b1)
    Destination: MicroStarINT_58:1d:b1 (04:7c:16:58:1d:b1)
      Address: MicroStarINT_58:1d:b1 (04:7c:16:58:1d:b1)
      ....0. .... = LG bit: Globally unique address (factory default)
      ....0. .... = IG bit: Individual address (unicast)
    Source: DLinkInterna_46:9a:52 (0c:b6:d2:46:9a:52)
      Address: DLinkInterna_46:9a:52 (0c:b6:d2:46:9a:52)
      ....0. .... = LG bit: Globally unique address (factory default)
      ....0. .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
  ▶ Internet Protocol Version 4, Src: 146.190.62.39, Dst: 192.168.0.174
  ▶ Transmission Control Protocol, Src Port: 80, Dst Port: 65420, Seq: 1, Ack: 468, Len: 749
  ▶ Hypertext Transfer Protocol
```

The Ethernet II also falls on the Data Link Layer. We can see the Destination Mac Address at first then the source Mac Address is evident. Also, it shows that data transfer is done via the IPv4 protocol.

## IPV4:

```
Frame 39: 803 bytes on wire (6424 bits), 803 bytes captured (6424 bits) on interface \Device\NPF_{0F13370F-7855-4473-9C68-5AAE02255896}, id 0
Ethernet II, Src: DLinkInterna 46:9a:52 (0c:b6:d2:46:9a:52), Dst: MicroStarINT_58:1d:b1 (04:7c:16:58:1d:b1)
Internet Protocol Version 4, Src: 146.190.62.39, Dst: 192.168.0.174
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    0000 00.. = Differentiated Services Codepoint: Default (0)
    .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 789
  Identification: 0xcaf7 (51959)
  000. .... = Flags: 0x0
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
    ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 46
  Protocol: TCP (6)
  Header Checksum: 0x2cb0 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 146.190.62.39
  Destination Address: 192.168.0.174
Transmission Control Protocol, Src Port: 80, Dst Port: 65420, Seq: 1, Ack: 468, Len: 749
Hypertext Transfer Protocol
```

The IPV4 falls under the Network Layer. The source is 146.190.62.39 meaning the website HTTPforever.com, and the destination 192.168.0.174 meaning my PC. The packet contains a header of 20 bytes, utilising TCP for data transmission. Its overall size is 789 bytes and includes a Time-to-Live (TTL) value set at 46.

## TCP:

```
Frame 39: 803 bytes on wire (6424 bits), 803 bytes captured (6424 bits) on interface \Device\NPF_{0F13370F-7855-4473-9C68-5AAE02255896}, id 0
Ethernet II, Src: DLinkInterna 46:9a:52 (0c:b6:d2:46:9a:52), Dst: MicroStarINT_58:1d:b1 (04:7c:16:58:1d:b1)
Internet Protocol Version 4, Src: 146.190.62.39, Dst: 192.168.0.174
Transmission Control Protocol, Src Port: 80, Dst Port: 65420, Seq: 1, Ack: 468, Len: 749
  Source Port: 80
  Destination Port: 65420
  [Stream index: 8]
  [Conversation completeness: Incomplete (12)]
  [TCP Segment Len: 749]
  Sequence Number: 1 (relative sequence number)
  Sequence Number (raw): 1639253677
  [Next Sequence Number: 750 (relative sequence number)]
  Acknowledgment Number: 468 (relative ack number)
  Acknowledgment number (raw): 2003011994
  0101 .... = Header Length: 20 bytes (5)
  Flags: 0x018 (PSH, ACK)
  Window: 768
  [Calculated window size: 768]
  [Window size scaling factor: -1 (unknown)]
  Checksum: 0x56ae [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
  [Timestamps]
    [Time since first frame in this TCP stream: 0.261130000 seconds]
    [Time since previous frame in this TCP stream: 0.151119000 seconds]
  [SEQ/ACK analysis]
    [Bytes in flight: 749]
    [Bytes sent since last PSH flag: 749]
  TCP payload (749 bytes)
Hypertext Transfer Protocol
```

TCP operates within the transport layer. The source port for the HTTP Forever website is 80, while the destination port, originating from my PC, is designated as 65420. The sequence number 1 represents the sequence number of the first byte of data in this TCP segment and acknowledgment number 468 acknowledges receipt of data up to sequence number 468. It's a relative acknowledgment number. TCP Segment Len: 749 indicates the data payload carried within this TCP segment, which is 749 bytes in size.

## HTTP:

```

> Frame 39: 803 bytes on wire (6424 bits), 803 bytes captured (6424 bits) on interface \Device\NPF_{0F13370F-7855-4473-9C68-5AAE02255896}, id 0
> Ethernet II, Src: DLinkInterna 46:9a:52 (0c:b6:d2:46:9a:52), Dst: MicroStarINT_58:1d:b1 (04:7c:16:58:1d:b1)
> Internet Protocol Version 4, Src: 146.190.62.39, Dst: 192.168.0.174
> Transmission Control Protocol, Src Port: 80, Dst Port: 65420, Seq: 1, Ack: 468, Len: 749
▼ Hypertext Transfer Protocol
  > HTTP/1.1 304 Not Modified\r\n
    Server: nginx/1.18.0 (Ubuntu)\r\n
    Date: Fri, 16 Feb 2024 14:58:36 GMT\r\n
    Last-Modified: Wed, 22 Mar 2023 14:54:48 GMT\r\n
    Connection: keep-alive\r\n
    ETag: "641b16b8-1404"\r\n
    Referrer-Policy: strict-origin-when-cross-origin\r\n
    X-Content-Type-Options: nosniff\r\n
    Feature-Policy: accelerometer 'none'; camera 'none'; geolocation 'none'; gyroscope 'none'; magnetometer 'none'; microphone 'none'; payment
    [truncated]Content-Security-Policy: default-src 'self'; script-src cdnjs.cloudflare.com 'self'; style-src cdnjs.cloudflare.com 'self' font
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.261130000 seconds]
    [Request in frame: 33]
    [Request URI: http://httpforever.com/]

```

HTTP falls under the Application Layer. HTTP/1.1: Indicates the version of the HTTP protocol used. Then 304 Not Modified means that the requested resource has not been modified since the last requested time, and therefore, there is no need to resend the resource. Next the server lies on ubuntu. After that it is evident that the response was generated on 16th February 2024 with exact time and also when the requested resources were last modified, that is on 22 March 2023. Then the Connection: keep-alive indicates the fact of Persistent Transmission. Lastly, the server's response contains 33 frames of data.