LAB 05 WIRESHARK2

Name	Tran Dang Khoa
Email address	Khoab2014926@student.ctu.edu.vn
Class	MO2
Browser	Safari, Chrome, IE, Firefox

Design Wireshark analyzing **scenario under Windows**

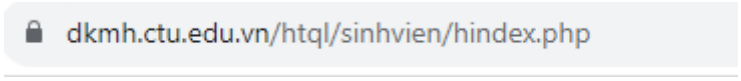
	scanner	target
OS	Windows Ubuntu	Windows, Linux
IP address	Test - bed host IP	Localhost CTU IP CICT IP Neighboring PC IP VM IP(Ubuntu, Centos)
scanning program	Wireshark	
scanning types	filter HTTP	

HTTP executing scenario

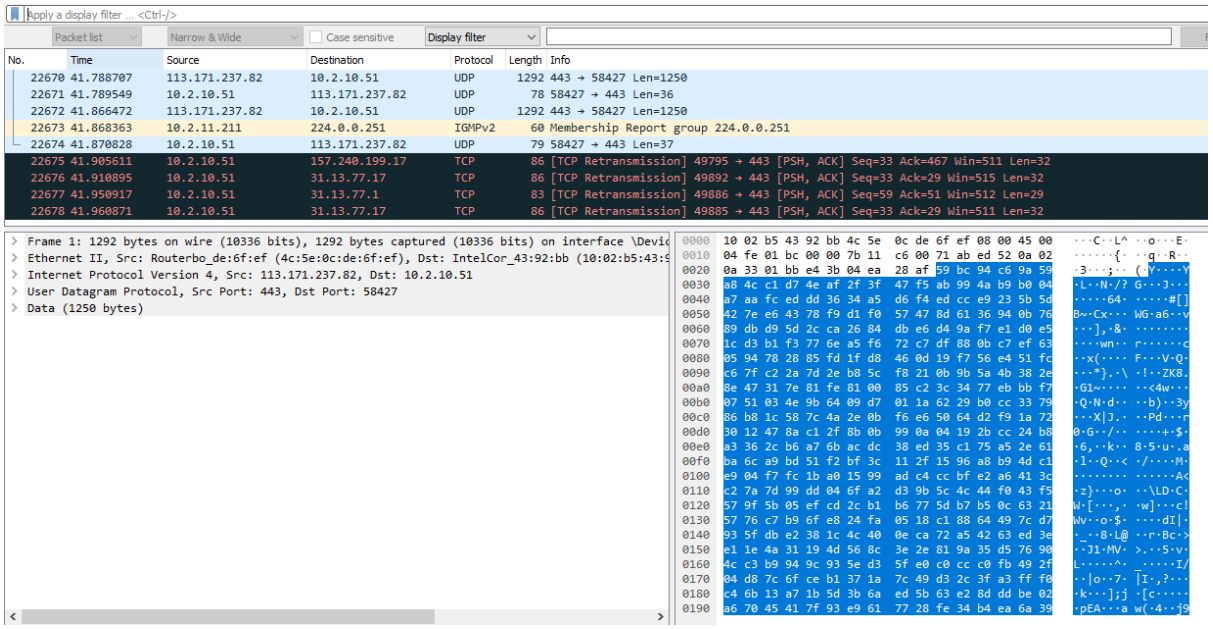
1 (browser) Visit one website

2 (website) Log in to home page

3 (browser) find input string on URL box



4 (wireshark) choose one packet

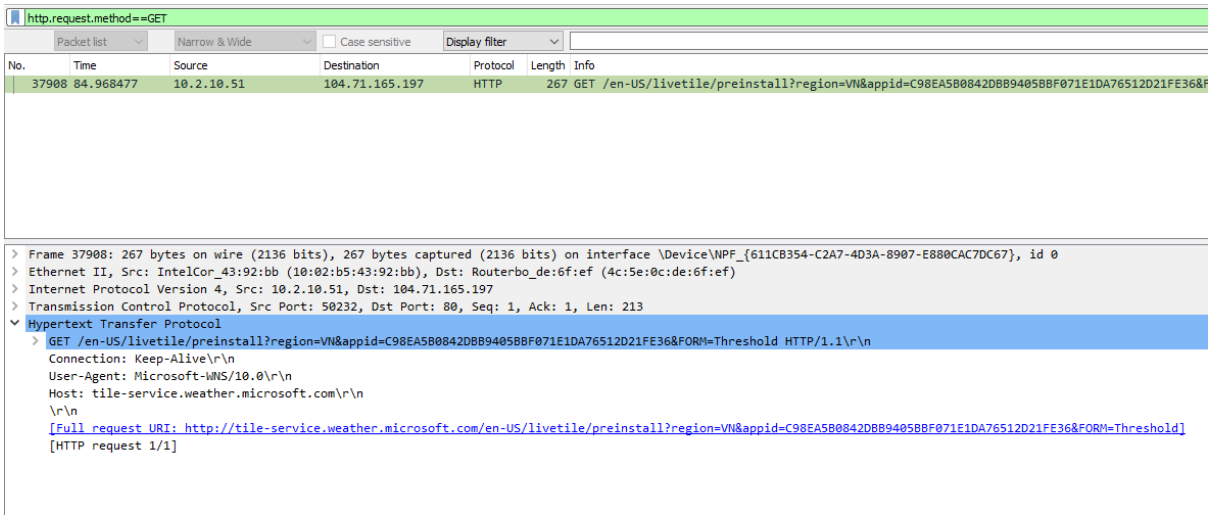



```
Frame 1: 1292 bytes on wire (10336 bits), 1292 bytes captured (10336 bits) on interface \Devic
    Section number: 1
  > Interface id: 0 (\Device\NPF_{611CB354-C2A7-4D3A-8907-E880CAC7DC67})
    Encapsulation type: Ethernet (1)
    Arrival Time: Sep 12, 2023 20:38:21.816549000 SE Asia Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1694525901.816549000 seconds
    [Time delta from previous captured frame: 0.000000000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.000000000 seconds]
    Frame Number: 1
    Frame Length: 1292 bytes (10336 bits)
    Capture Length: 1292 bytes (10336 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:udp:data]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
```

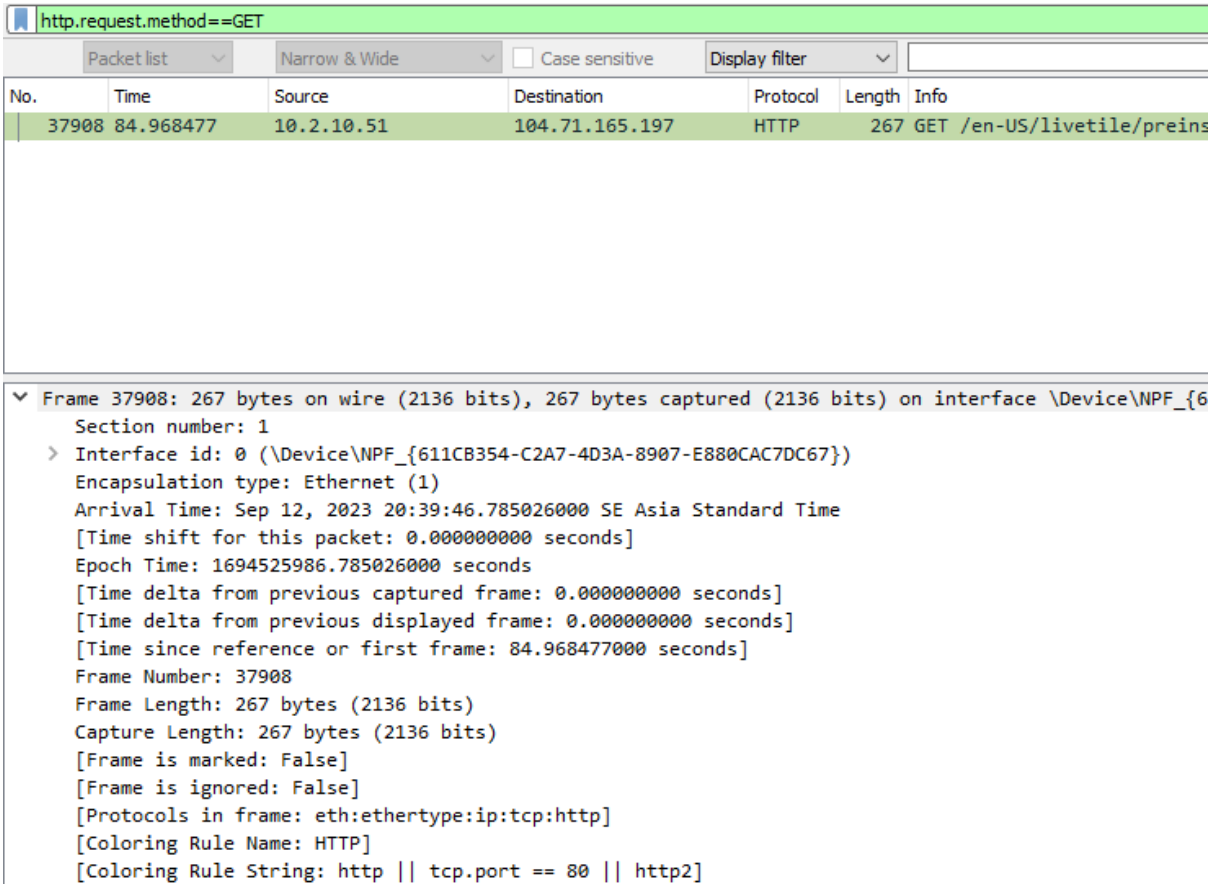
```
Internet Protocol Version 4, Src: 113.171.237.82, Dst: 10.2.10.51
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1278
    Identification: 0x01bc (444)
  v 000. .... = Flags: 0x0
      0... .... = 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: 123
    Protocol: UDP (17)
    Header Checksum: 0xc600 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 113.171.237.82
    Destination Address: 10.2.10.51
> User Datagram Protocol, Src Port: 443, Dst Port: 58427
```

```
User Datagram Protocol, Src Port: 443, Dst Port: 58427
    Source Port: 443
    Destination Port: 58427
    Length: 1258
    Checksum: 0x28af [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
  > [Timestamps]
    UDP payload (1250 bytes)
v Data (1250 bytes)
    Data: 59bc94c69a59a84cc1d74eaf2f3f47f5ab994ab9b004a7aafceddd3634a5d6f4edcce923…
    [Length: 1250]
```

5 (wireshark) filter : get method

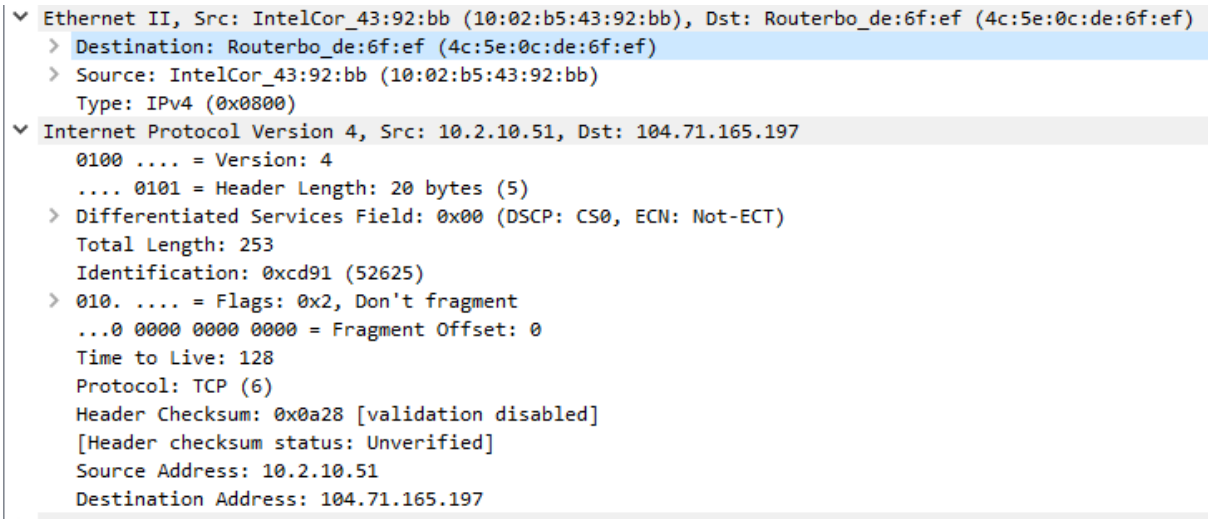


6 (wireshark) analyze get method in detail



I choose frame 37908. There are 267 bytes on wire and being captured.

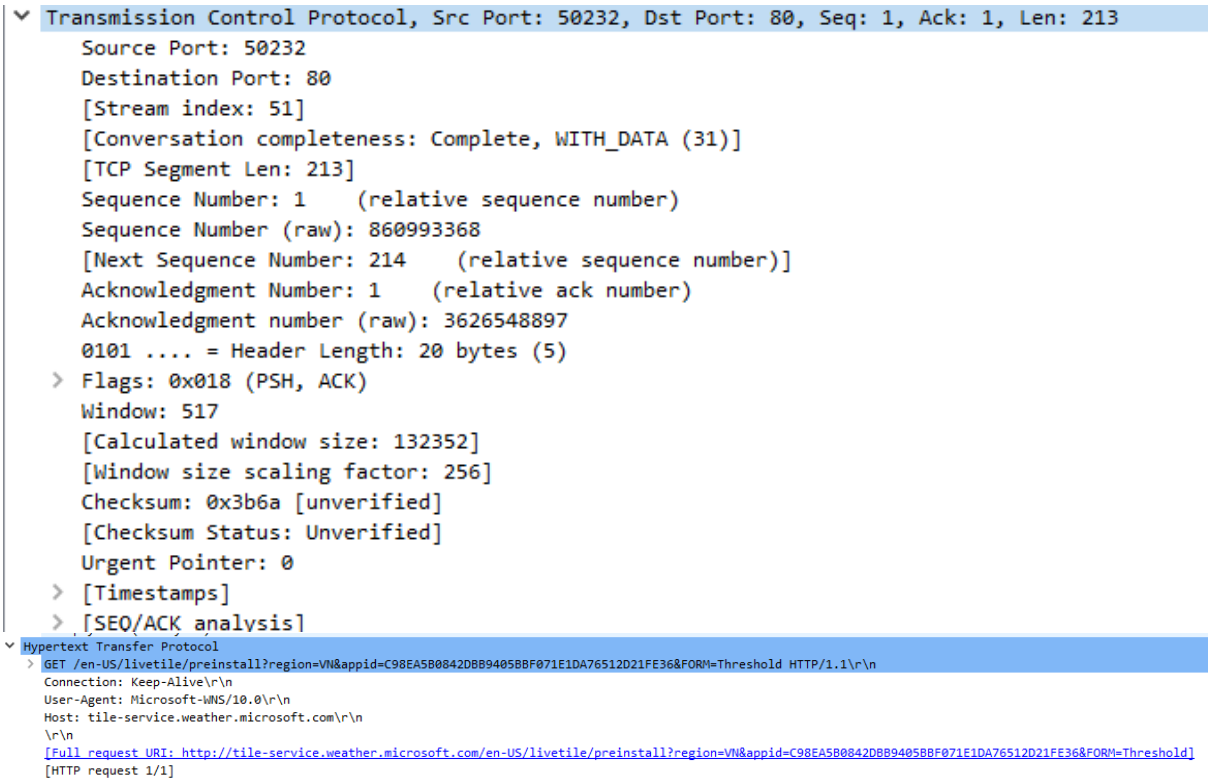
- The interface id is 0 (\Device\NPF_{611CB354-C2A7-4D3A-8907-E880CAC7DC67})
- Epouch time: 1694525986.785026000 second
- Frame number is 37908
- Frame Length: 267 bytes (2136 bits)



Ethernet II, Src: IntelCor_43:92:bb (10:02:b5:43:92:bb), Dst: Routerbo_de:6f:ef (4c:5e:0c:de:6f:ef)
Destination: Routerbo_de:6f:ef (4c:5e:0c:de:6f:ef)
Source: InterCol_43:92:bb (10:02:b5:43:92:bb)

Type: Ipv4 (0x0800)

- Internet Protocol Version 4
- Source address: 10.2.10.51
- Destination address: 104:71:165:197
- Total Length: 253
- Identification: 0xcd91 (52625)
- Time to Live: 128
- Protocol: TCP (6)
- Header Checksum: 0x0a28 [validation disabled]
- Header checksum status: Unverified

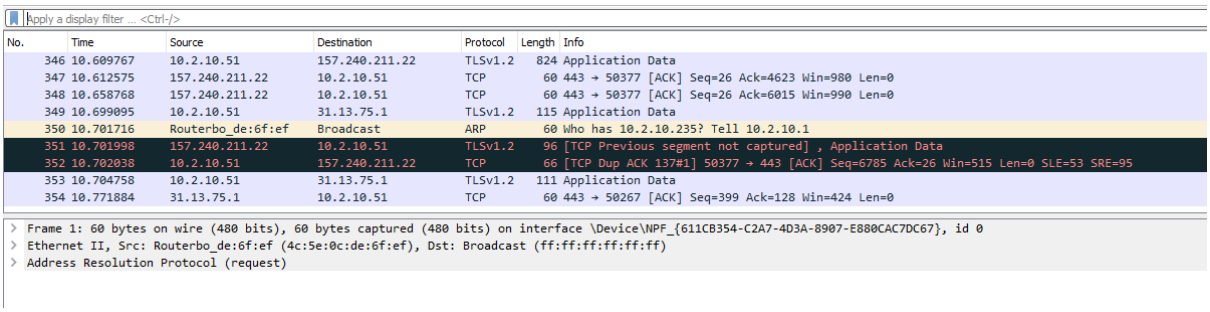


Transmission Control Protocol, Src Port: 50232, Dst Port: 80, Seq: 1, Ack: 1: Len: 123

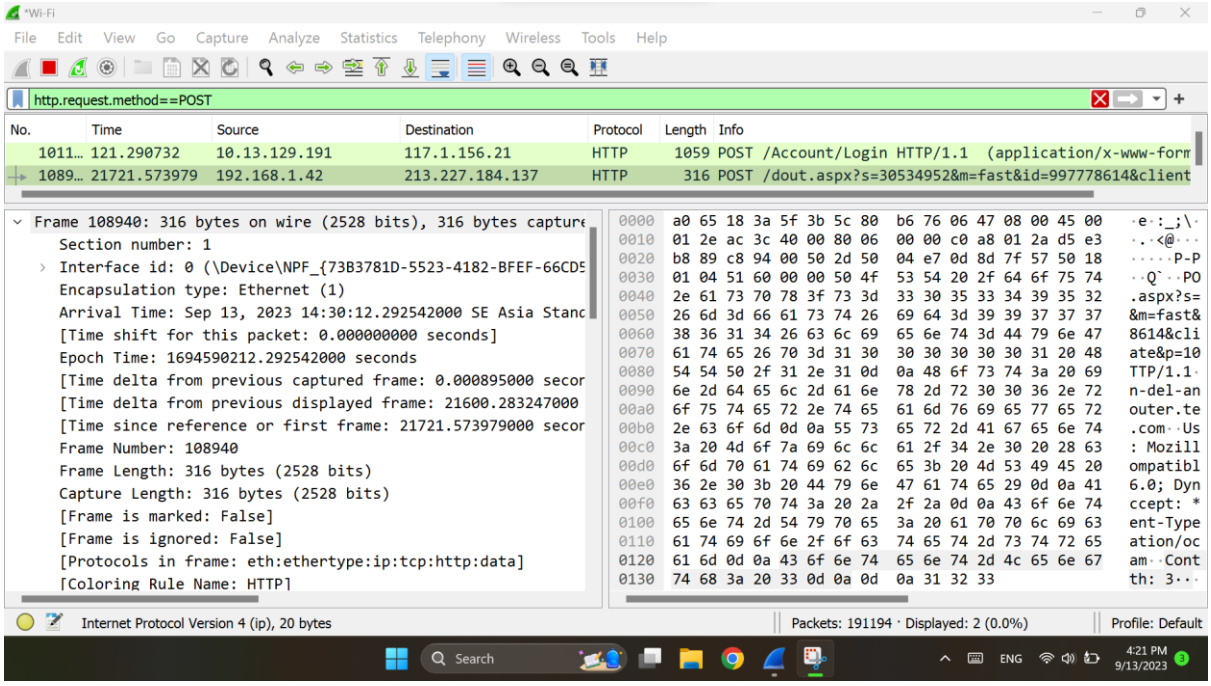
Flags: 0x018 (PSH, ACK)

The HTTP field shows the host and ‘full request URI)

7 (wireshark) choose one packet



8 (wireshark) filter : post method

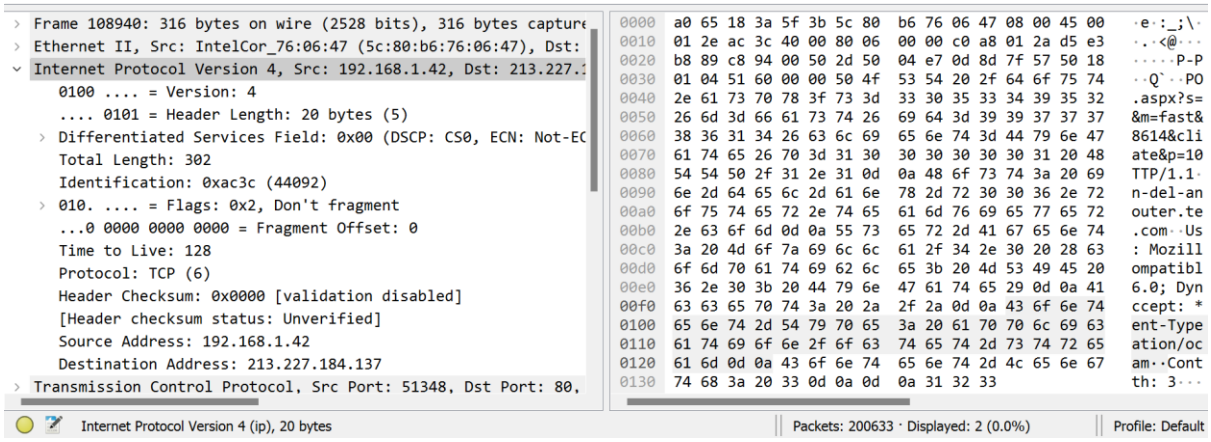


9 (wireshark) analyze post method in detail

```
> Frame 108940: 316 bytes on wire (2528 bits), 316 bytes capture
v Ethernet II, Src: IntelCor_76:06:47 (5c:80:b6:76:06:47), Dst:
  v Destination: VnptTech_3a:5f:3b (a0:65:18:3a:5f:3b)
      Address: VnptTech_3a:5f:3b (a0:65:18:3a:5f:3b)
      .... ..0. .... .... .... .... = LG bit: Globally unique
      .... ...0 .... .... .... .... = IG bit: Individual addre
  v Source: IntelCor_76:06:47 (5c:80:b6:76:06:47)
      Address: IntelCor_76:06:47 (5c:80:b6:76:06:47)
      .... ..0. .... .... .... .... = LG bit: Globally unique
      .... ...0 .... .... .... .... = IG bit: Individual addre
    Type: IPv4 (0x0800)
```

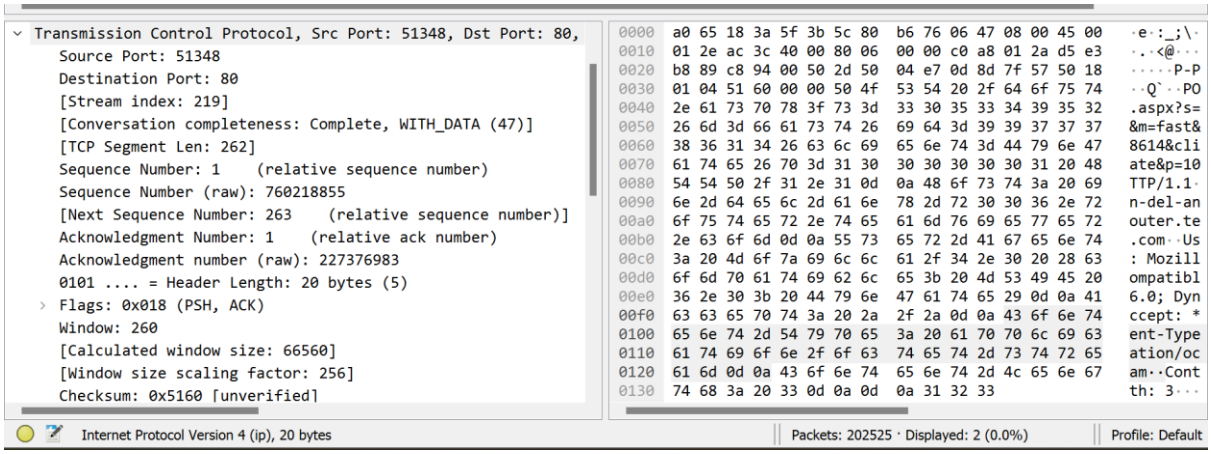
I chose frame 108940: 316 bytes on wire (2528 bits), 316 bytes capture

- Interface id: 0 (\Device\NPF_{738371D-5523-4182-BFEF-77CD5)
- Epoch Time: 1694590212.292542000 seconds
- Frame Number: 108940
- Frame Length: 316 bytes (2528 bits)



Internet Protocol Version 4, Src: 192.168.1.42, Dst: 213.227.2

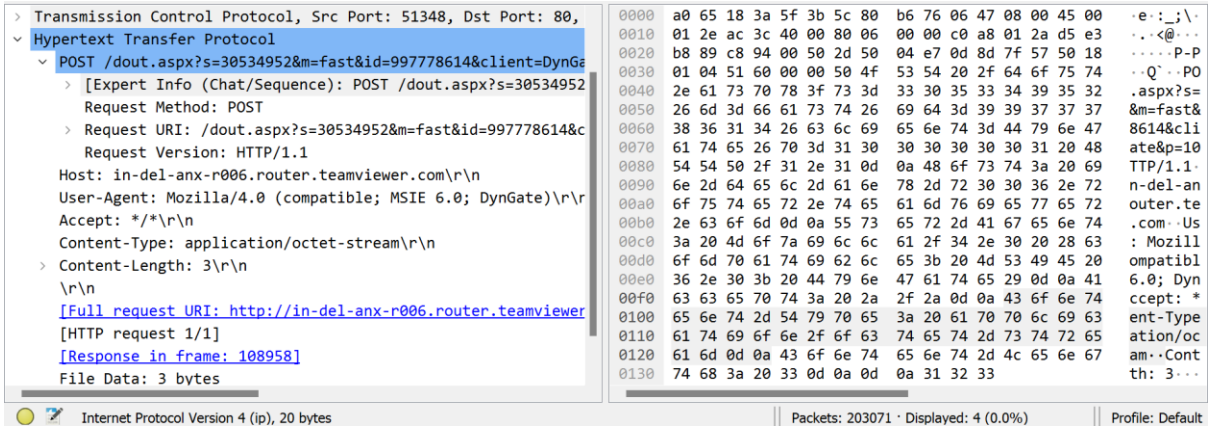
- Total Length: 302
- Time to Live: 128
- Protocol: TCP (6)
- Header Checksum: 0x000 [validation disabled]
- [Header checksum status: Unverified]
- Source Address: 192.168.1.42



Transmission Control Protocol, Src Port: 51348, Dst Port: 80

- Source Port: 51348
- Distination Port: 80
- [Stream index: 219]
- [TCP Segment Len: 262]
- Sequence Number: 1 (relative sequence number)
- Sequence Number (raw): 760218855
- [Next Sequence Number: 273 (relative sequence number)
- Acknowlegment Number: 1 (relative ack number)

- Flags: 0x018 (PSH, ACK)



The HTTP field shows some information about POST method like User-Agent, Enconding, Postman-Token, Connectopn. More information full request URI, HTTP request 1/1.