Computer Networks Lab (CS302)

Report Submission: CN Assignment Lab-5

Group Member Details:

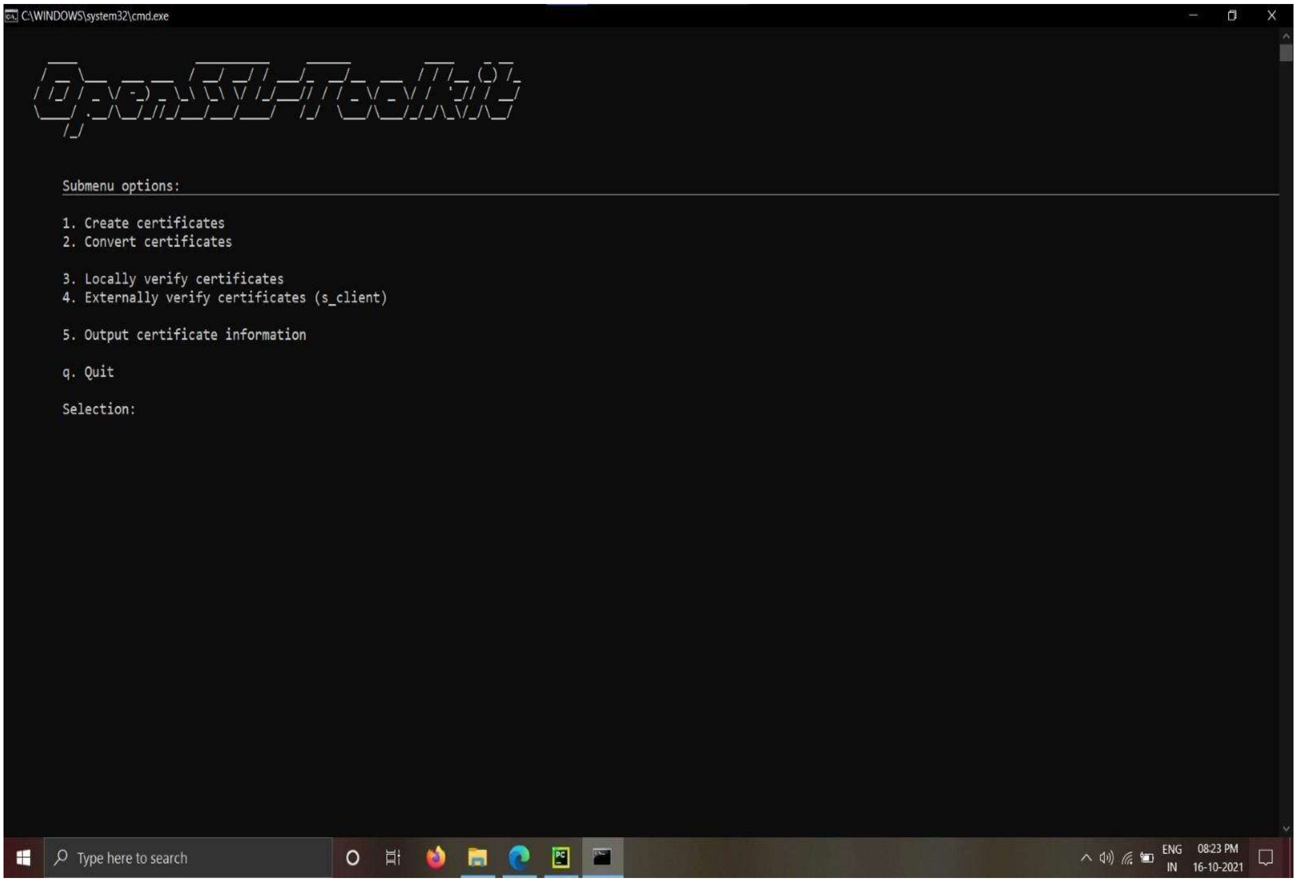
1.Mahadev M Hatti 191CS133

2.Darshan A V 191CS219

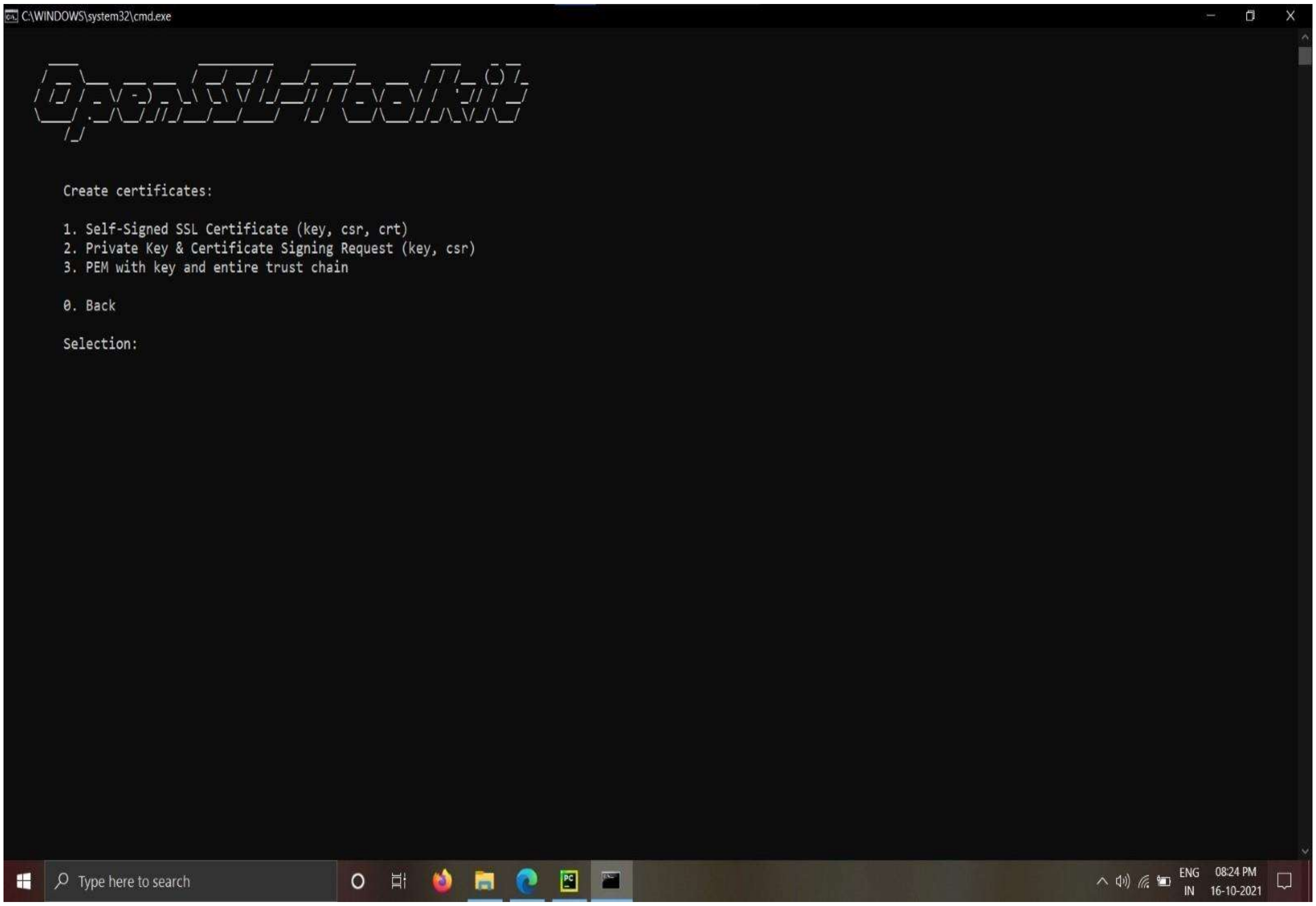
1. Develop a code to illustrate a secure socket connection between client and server.

- First, we need to generate SSL certificates:

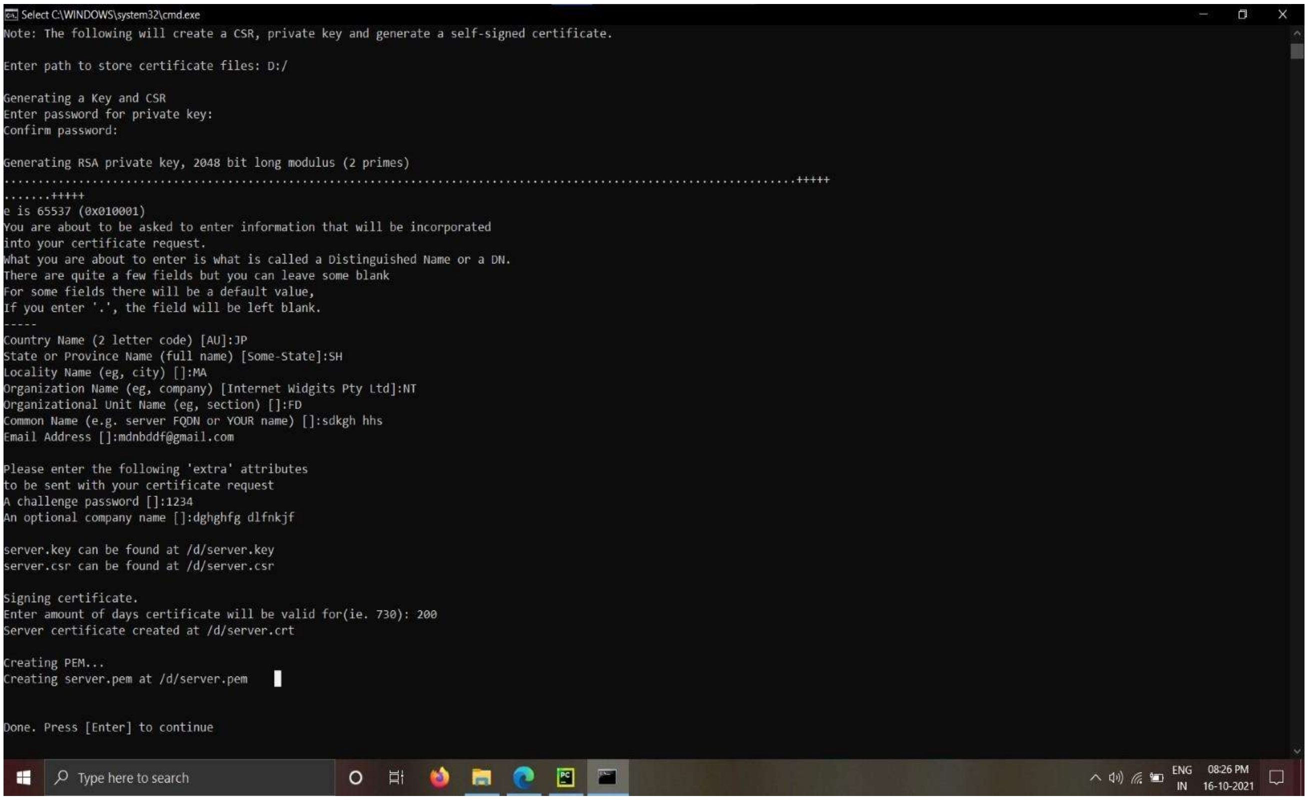
I used OPENSSL Toolkit to generate SSL certificate.



```
Submenu options:

1. Create certificates
2. Convert certificates

3. Locally verify certificates
4. Externally verify certificates (s_client)

5. Output certificate information

q. Quit

Selection:
```



```
Create certificates:

1. Self-Signed SSL Certificate (key, csr, crt)
2. Private Key & Certificate Signing Request (key, csr)
3. PEM with key and entire trust chain

0. Back

Selection:
```



```
Note: The following will create a CSR, private key and generate a self-signed certificate.

Enter path to store certificate files: D:/

Generating a Key and CSR
Enter password for private key:
Confirm password:

Generating RSA private key, 2048 bit long modulus (2 primes)
.......................................................................................................................+++++
.......+++++
e is 65537 (0x010001)
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:JP
State or Province Name (full name) [Some-State]:SH
Locality Name (eg, city) []:MA
Organization Name (eg, company) [Internet Widgits Pty Ltd]:NT
Organizational Unit Name (eg, section) []:FD
Common Name (e.g. server FQDN or YOUR name) []:sdkgh hhs
Email Address []:mdnbddf@gmail.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:1234
An optional company name []:dghghfg dlfnkjf

server.key can be found at /d/server.key
server.csr can be found at /d/server.csr

Signing certificate.
Enter amount of days certificate will be valid for(ie. 730): 200
Server certificate created at /d/server.crt

Creating PEM...
Creating server.pem at /d/server.pem


Done. Press [Enter] to continue
```

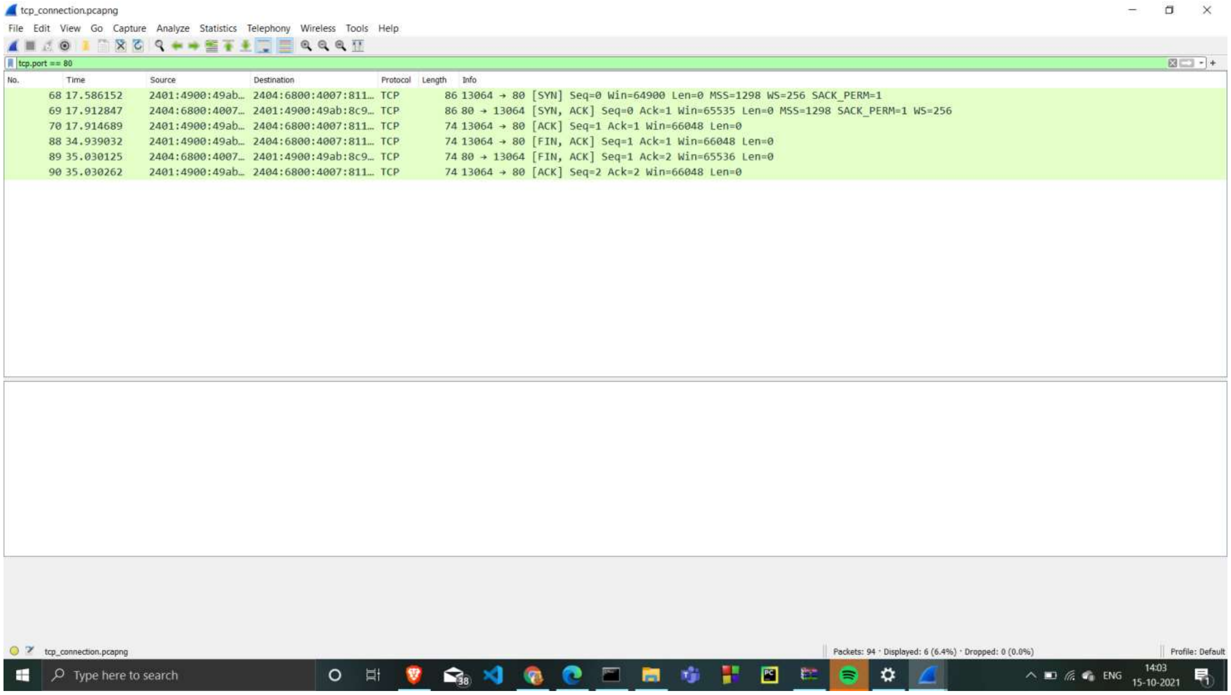
- Now lets write the actual code to implement a secure socket connection between client and server.
    - Client

```
import socket
import ssl

hostname = 'localhost'
context = ssl.SSLContext(ssl.PROTOCOL_TLS_CLIENT)
context.load_verify_locations('server.pem')

with socket.socket(socket.AF_INET, socket.SOCK_STREAM, 0)
as sock:
    with context.wrap_socket(sock,
server_hostname=hostname) as ssock:
        print(ssock.version())
```

- Server

```
import socket
import ssl

context = ssl.SSLContext(ssl.PROTOCOL_TLS_SERVER)
context.load_cert_chain('server.pem', 'server.key')

with socket.socket(socket.AF_INET, socket.SOCK_STREAM, 0) as sock:
    sock.bind(('127.0.0.1', 8443))
    sock.listen(5)
    with context.wrap_socket(sock, server_side=True) as ssock:
        conn, addr = ssock.accept()
```

2. Capture TCP Packets


tcp_connection.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Type here to search
ENG
14:03
15-10-2021

tcp.port == 80

```
No.     Time       Source            Destination          Protocol Length Info
     68 17.586152  2401:4900:49ab…   2404:6800:4007:811…  TCP          86 13064 → 80 [SYN] Seq=0 Win=64900 Len=0 MSS=1298 WS=256 SACK_PERM=1
     69 17.912847  2404:6800:4007…   2401:4900:49ab:8c9…  TCP          86 80 → 13064 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1298 SACK_PERM=1 WS=256
     70 17.914689  2401:4900:49ab…   2404:6800:4007:811…  TCP          74 13064 → 80 [ACK] Seq=1 Ack=1 Win=66048 Len=0
     88 34.939032  2401:4900:49ab…   2404:6800:4007:811…  TCP          74 13064 → 80 [FIN, ACK] Seq=1 Ack=1 Win=66048 Len=0
     89 35.030125  2404:6800:4007…   2401:4900:49ab:8c9…  TCP          74 80 → 13064 [FIN, ACK] Seq=1 Ack=2 Win=65536 Len=0
     90 35.030262  2401:4900:49ab…   2404:6800:4007:811…  TCP          74 13064 → 80 [ACK] Seq=2 Ack=2 Win=66048 Len=0
```

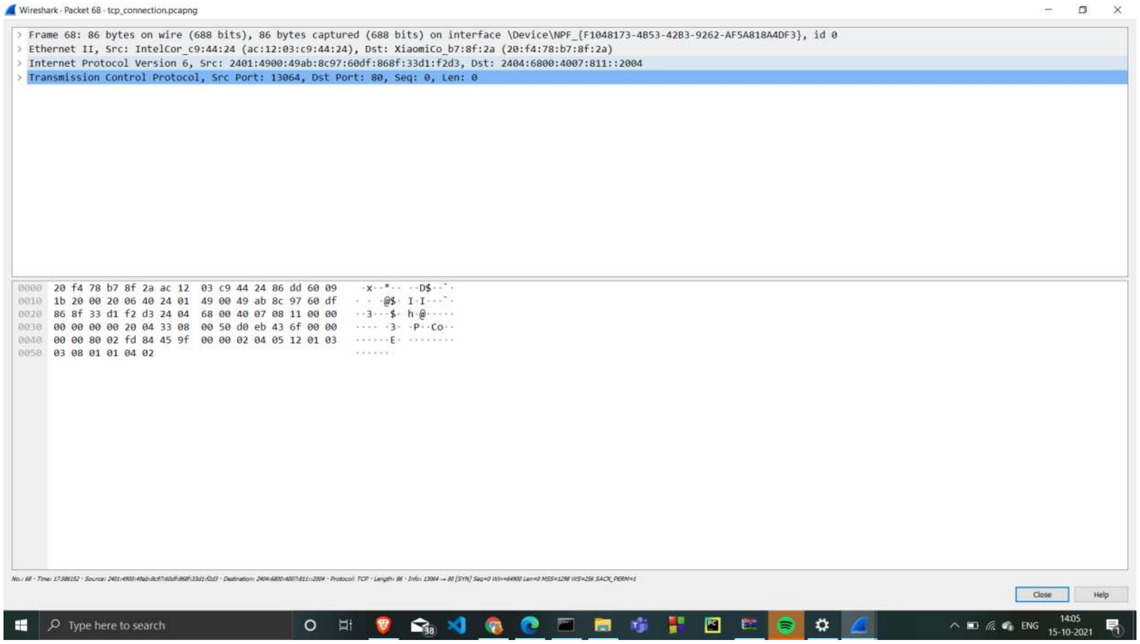
tcp_connection.pcapng | Packets: 94 · Displayed: 6 (6.4%) · Dropped: 0 (0.0%) | Profile: Default

1. Started the a Wireshark capture.
2. Open a command prompt.
3. Type **telnet www.google.com 80** and press **Enter**.

4. Close the command prompt to close the TCP connection.
5. [Stop the Wireshark capture](#).

a. Analyse the three-way handshake during the establishment of the communication

Selectect the first TCP packet, labelled **http [SYN]**



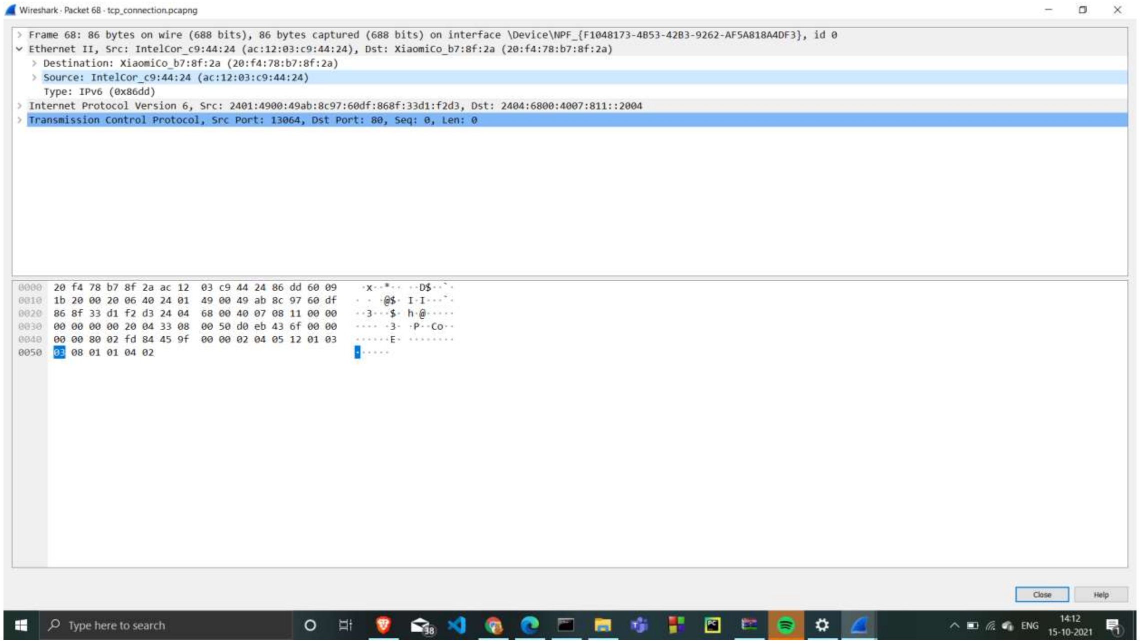
```
> Frame 68: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface \Device\NPF_{F1048173-4B53-42B3-9262-AF5A818A4DF3}, id 0
> Ethernet II, Src: IntelCor_c9:44:24 (ac:12:03:c9:44:24), Dst: XiaomiCo_b7:8f:2a (20:f4:78:b7:8f:2a)
> Internet Protocol Version 6, Src: 2401:4900:49ab:8c97:60df:868f:33d1:f2d3, Dst: 2404:6800:4007:811::2004
> Transmission Control Protocol, Src Port: 13064, Dst Port: 80, Seq: 0, Len: 0
```

```
0000  20 f4 78 b7 8f 2a ac 12  03 c9 44 24 86 dd 60 09    ·x··*··  ··D$··`·
0010  1b 20 00 20 06 40 24 01  49 00 49 ab 8c 97 60 df   · · ·@$·  I·I···`·
0020  86 8f 33 d1 f2 d3 24 04  68 00 40 07 08 11 00 00   ··3···$·  h·@·····
0030  00 00 00 00 20 04 33 08  00 50 d0 eb 43 6f 00 00   ···· ·3·  ·P··Co··
0040  00 00 80 02 fd 84 45 9f  00 00 02 04 05 12 01 03   ······E·  ········
0050  03 08 01 01 04 02                                  ······
```

No.: 68 · Time: 17.586152 · Source: 2401:4900:49ab:8c97:60df:868f:33d1:f2d3 · Destination: 2404:6800:4007:811::2004 · Protocol: TCP · Length: 86 · Info: 13064 → 80 [SYN] Seq=0 Win=64900 Len=0 MSS=1298 WS=256 SACK_PERM=1

it is an Ethernet II / Internet Protocol Version 4 / Transmission Control Protocol frame.

Expand Ethernet II

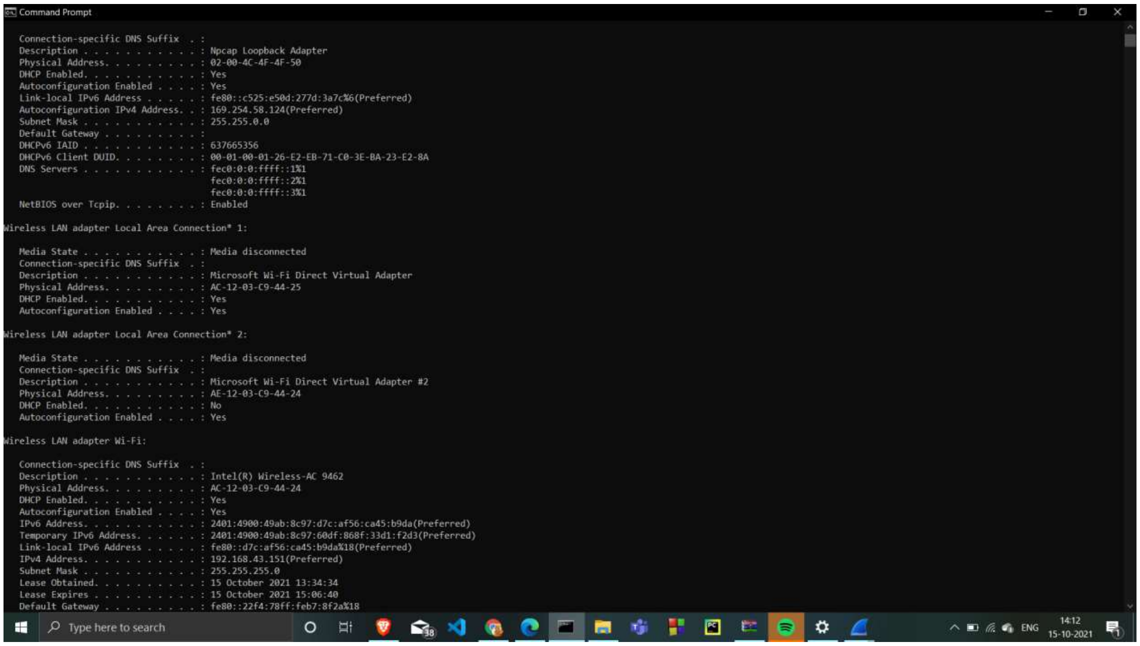


```
> Frame 68: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface \Device\NPF_{F1048173-4B53-42B3-9262-AF5A818A4DF3}, id 0
v Ethernet II, Src: IntelCor_c9:44:24 (ac:12:03:c9:44:24), Dst: XiaomiCo_b7:8f:2a (20:f4:78:b7:8f:2a)
  > Destination: XiaomiCo_b7:8f:2a (20:f4:78:b7:8f:2a)
  > Source: IntelCor_c9:44:24 (ac:12:03:c9:44:24)
    Type: IPv6 (0x86dd)
> Internet Protocol Version 6, Src: 2401:4900:49ab:8c97:60df:868f:33d1:f2d3, Dst: 2404:6800:4007:811::2004
> Transmission Control Protocol, Src Port: 13064, Dst Port: 80, Seq: 0, Len: 0
```

```
0000  20 f4 78 b7 8f 2a ac 12  03 c9 44 24 86 dd 60 09    ·x··*·· ··D$··`·
0010  1b 20 00 20 06 40 24 01  49 00 49 ab 8c 97 60 df   · · ·@$· I·I···`·
0020  86 8f 33 d1 f2 d3 24 04  68 00 40 07 08 11 00 00   ··3···$· h·@·····
0030  00 00 00 00 20 04 33 08  00 50 d0 eb 43 6f 00 00   ···· ·3· ·P··Co··
0040  00 00 80 02 fd 84 45 9f  00 00 02 04 05 12 01 03   ······E· ········
0050  03 08 01 01 04 02                                  ······
```

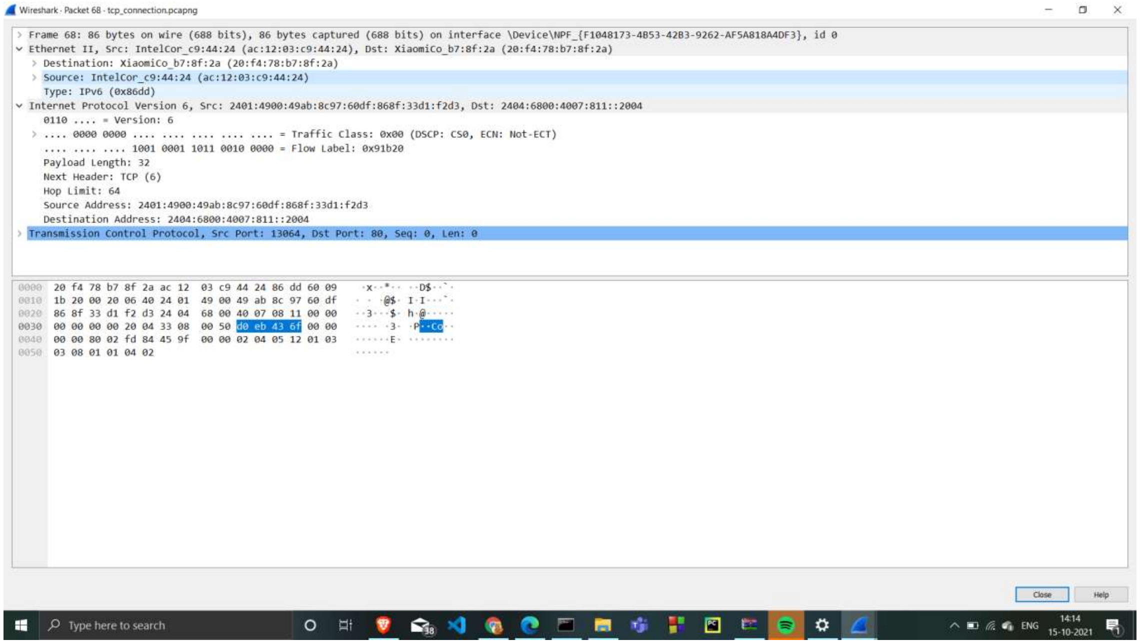
The destination is default gateway's MAC address

the source should be your MAC address



```
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Npcap Loopback Adapter
   Physical Address. . . . . . . . . : 02-00-4C-4F-4F-50
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::c525:e50d:277d:3a7c%6(Preferred)
   Autoconfiguration IPv4 Address. . : 169.254.58.124(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . :
   DHCPv6 IAID . . . . . . . . . . . : 637665356
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-26-E2-EB-71-C0-3E-BA-23-E2-8A
   DNS Servers . . . . . . . . . . . : fec0:0:0:ffff::1%1
                                       fec0:0:0:ffff::2%1
                                       fec0:0:0:ffff::3%1
   NetBIOS over Tcpip. . . . . . . . : Enabled

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
   Physical Address. . . . . . . . . : AC-12-03-C9-44-25
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
   Physical Address. . . . . . . . . : AE-12-03-C9-44-24
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Wireless-AC 9462
   Physical Address. . . . . . . . . : AC-12-03-C9-44-24
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : 2401:4900:49ab:8c97:d7c:af56:ca45:b9da(Preferred)
   Temporary IPv6 Address. . . . . . : 2401:4900:49ab:8c97:60df:868f:33d1:f2d3(Preferred)
   Link-local IPv6 Address . . . . . : fe80::d7c:af56:ca45:b9da%18(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.43.151(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : 15 October 2021 13:34:34
   Lease Expires . . . . . . . . . . : 15 October 2021 15:06:40
   Default Gateway . . . . . . . . . : fe80::22f4:78ff:feb7:8f2a%18
```

Expand Internet Protocol Version 4 to view IP details



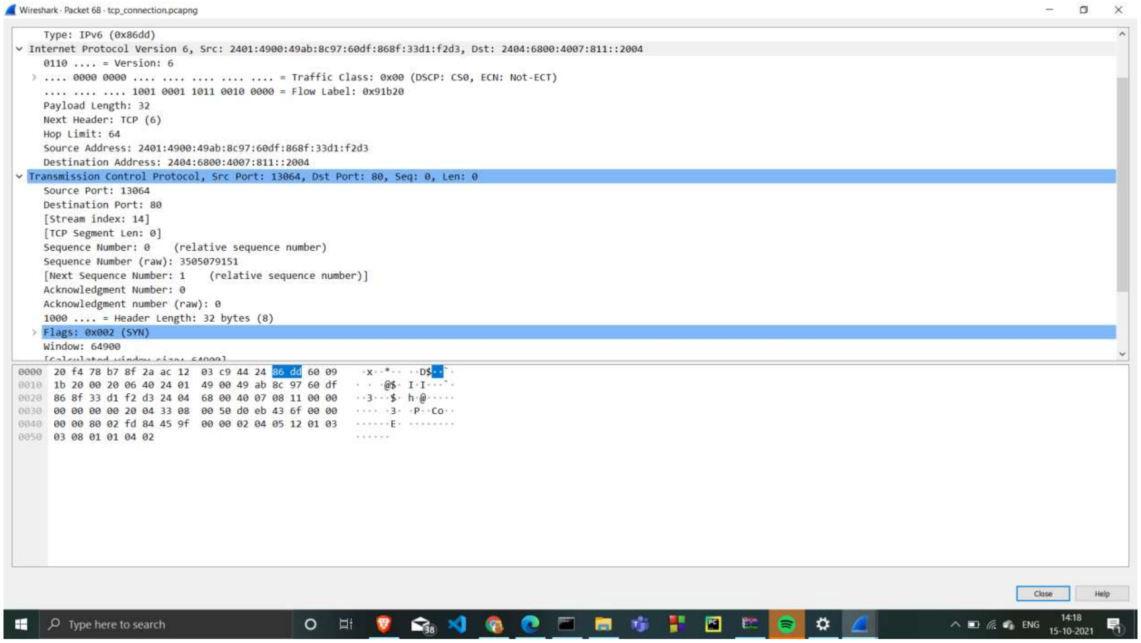
```
> Frame 68: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface \Device\NPF_{F1048173-4B53-42B3-9262-AF5A818A4DF3}, id 0
v Ethernet II, Src: IntelCor_c9:44:24 (ac:12:03:c9:44:24), Dst: XiaomiCo_b7:8f:2a (20:f4:78:b7:8f:2a)
  > Destination: XiaomiCo_b7:8f:2a (20:f4:78:b7:8f:2a)
  > Source: IntelCor_c9:44:24 (ac:12:03:c9:44:24)
    Type: IPv6 (0x86dd)
v Internet Protocol Version 6, Src: 2401:4900:49ab:8c97:60df:868f:33d1:f2d3, Dst: 2404:6800:4007:811::2004
    0110 .... = Version: 6
  > .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... .... .... 1001 0001 1011 0010 0000 = Flow Label: 0x91b20
    Payload Length: 32
    Next Header: TCP (6)
    Hop Limit: 64
    Source Address: 2401:4900:49ab:8c97:60df:868f:33d1:f2d3
    Destination Address: 2404:6800:4007:811::2004
> Transmission Control Protocol, Src Port: 13064, Dst Port: 80, Seq: 0, Len: 0

0000  20 f4 78 b7 8f 2a ac 12  03 c9 44 24 86 dd 60 09    ·x··*·· ··D$··`·
0010  1b 20 00 20 06 40 24 01  49 00 49 ab 8c 97 60 df    · · ·@$· I·I···`·
0020  86 8f 33 d1 f2 d3 24 04  68 00 40 07 08 11 00 00    ··3···$· h·@·····
0030  00 00 00 00 20 04 33 08  00 50 d0 eb 43 6f 00 00    ···· ·3· ·P··Co··
0040  00 00 80 02 fd 84 45 9f  00 00 02 04 05 12 01 03    ······E· ········
0050  03 08 01 01 04 02                                   ······
```

the source address is system IP address.

2401:4900:49ab:8c97:d7c:af56:ca45:b9da

destination address is the IP address of one of Google's web servers.

Expand Transmission Control Protoco



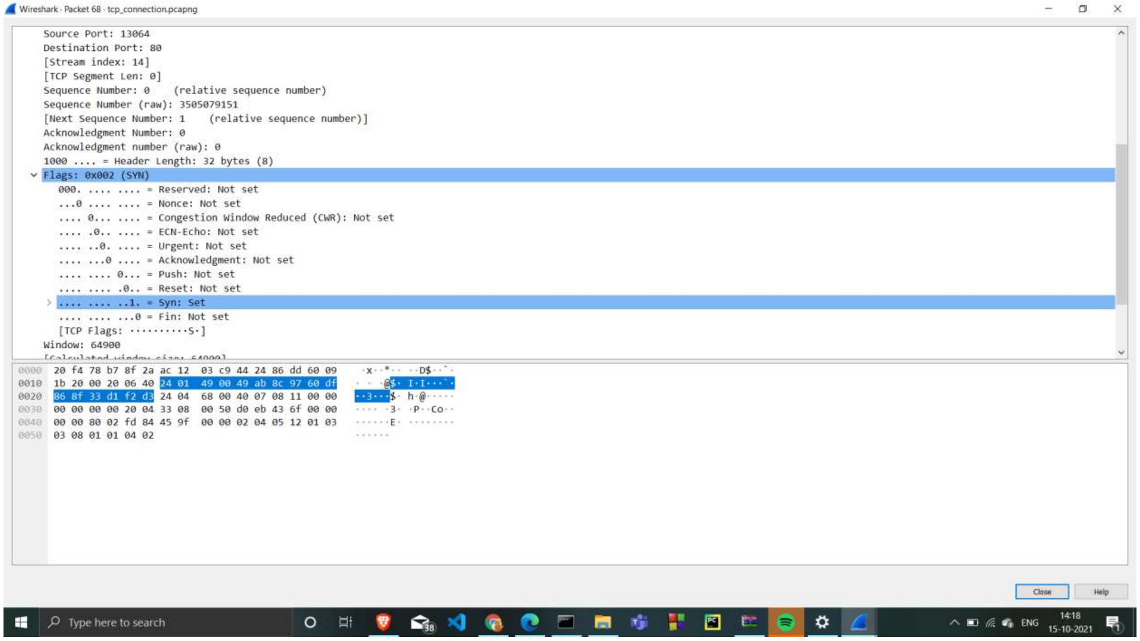
```
    Type: IPv6 (0x86dd)
v Internet Protocol Version 6, Src: 2401:4900:49ab:8c97:60df:868f:33d1:f2d3, Dst: 2404:6800:4007:811::2004
    0110 .... = Version: 6
  > .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... .... .... 1001 0001 1011 0010 0000 = Flow Label: 0x91b20
    Payload Length: 32
    Next Header: TCP (6)
    Hop Limit: 64
    Source Address: 2401:4900:49ab:8c97:60df:868f:33d1:f2d3
    Destination Address: 2404:6800:4007:811::2004
v Transmission Control Protocol, Src Port: 13064, Dst Port: 80, Seq: 0, Len: 0
    Source Port: 13064
    Destination Port: 80
    [Stream index: 14]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 3505079151
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 0
    Acknowledgment number (raw): 0
    1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x002 (SYN)
    Window: 64900
    [Calculated window size: 64900]

0000  20 f4 78 b7 8f 2a ac 12  03 c9 44 24 86 dd 60 09    ·x··*·· ··D$··`·
0010  1b 20 00 20 06 40 24 01  49 00 49 ab 8c 97 60 df    · · ·@$· I·I···`·
0020  86 8f 33 d1 f2 d3 24 04  68 00 40 07 08 11 00 00    ··3···$· h·@·····
0030  00 00 00 00 20 04 33 08  00 50 d0 eb 43 6f 00 00    ···· ·3· ·P··Co··
0040  00 00 80 02 fd 84 45 9f  00 00 02 04 05 12 01 03    ······E· ········
0050  03 08 01 01 04 02                                   ······
```

Source port is a dynamic port selected for this connection.

Destination port. Notice that it is http 80

Sequence number is 0

Expand Flags

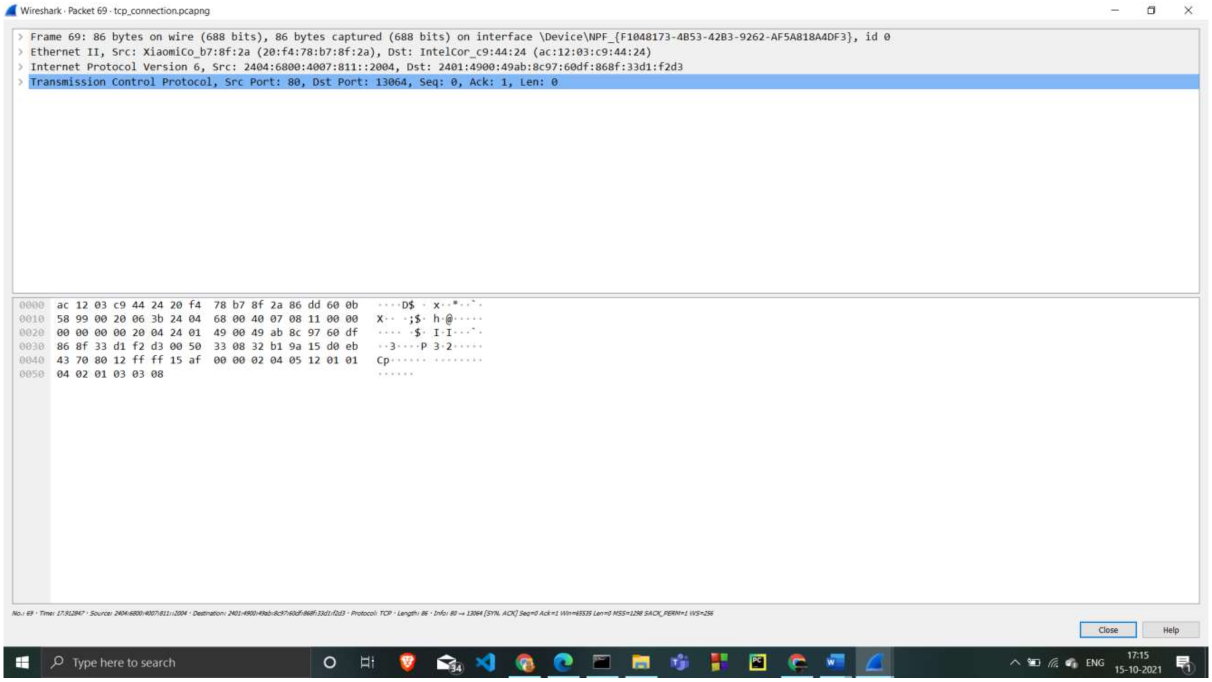


```
Source Port: 13064
Destination Port: 80
[Stream index: 14]
[TCP Segment Len: 0]
Sequence Number: 0    (relative sequence number)
Sequence Number (raw): 3505079151
[Next Sequence Number: 1    (relative sequence number)]
Acknowledgment Number: 0
Acknowledgment number (raw): 0
1000 .... = Header Length: 32 bytes (8)
Flags: 0x002 (SYN)
   000. .... .... = Reserved: Not set
   ...0 .... .... = Nonce: Not set
   .... 0... .... = Congestion Window Reduced (CWR): Not set
   .... .0.. .... = ECN-Echo: Not set
   .... ..0. .... = Urgent: Not set
   .... ...0 .... = Acknowledgment: Not set
   .... .... 0... = Push: Not set
   .... .... .0.. = Reset: Not set
   .... .... ..1. = Syn: Set
   .... .... ...0 = Fin: Not set
   [TCP Flags: ··········S·]
Window: 64900
```

```
0000  20 f4 78 b7 8f 2a ac 12  03 c9 44 24 86 dd 60 09    ·x··*·····D$··`·
0010  1b 20 00 20 06 40 24 01  49 00 49 ab 8c 97 60 df    ··· ·@$·I·I···`·
0020  86 8f 33 d1 f2 d3 24 04  68 00 40 07 08 11 00 00    ··3···$·h·@·····
0030  00 00 00 00 20 04 33 08  00 50 d0 eb 43 6f 00 00    ···· ·3··P··Co··
0040  00 00 80 02 fd 84 45 9f  00 00 02 04 05 12 01 03    ······E·········
0050  03 08 01 01 04 02                                    ······
```

SYN is set ,indicating first segment in the TCP three-way handshake.

Analyse TCP SYN, ACK Traffic



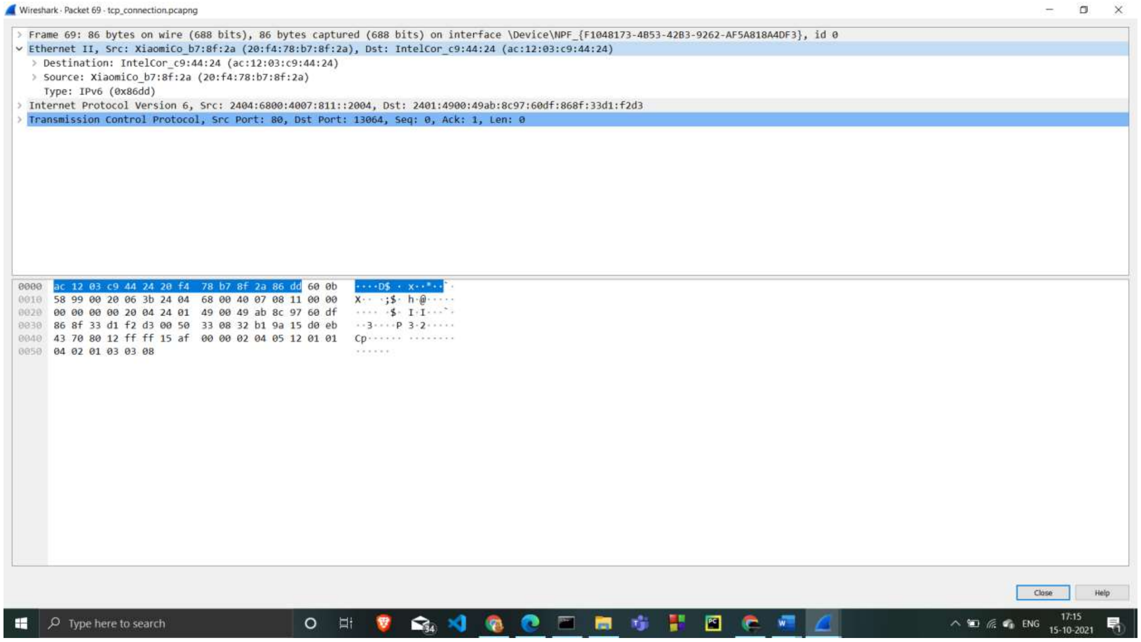
```
> Frame 69: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface \Device\NPF_{F1048173-4B53-42B3-9262-AF5A818A4DF3}, id 0
> Ethernet II, Src: XiaomiCo_b7:8f:2a (20:f4:78:b7:8f:2a), Dst: IntelCor_c9:44:24 (ac:12:03:c9:44:24)
> Internet Protocol Version 6, Src: 2404:6800:4007:811::2004, Dst: 2401:4900:49ab:8c97:60df:868f:33d1:f2d3
> Transmission Control Protocol, Src Port: 80, Dst Port: 13064, Seq: 0, Ack: 1, Len: 0
```

```
0000  ac 12 03 c9 44 24 20 f4  78 b7 8f 2a 86 dd 60 0b    ····D$ ·x··*··`·
0010  58 99 00 20 06 3b 24 04  68 00 40 07 08 11 00 00    X·· ·;$·h·@·····
0020  00 00 00 00 20 04 24 01  49 00 49 ab 8c 97 60 df    ···· ·$·I·I···`·
0030  86 8f 33 d1 f2 d3 00 50  33 08 32 b1 9a 15 d0 eb    ··3····P3·2·····
0040  43 70 80 12 ff ff 15 af  00 00 02 04 05 12 01 01    Cp··············
0050  04 02 01 03 03 08                                    ······
```

```
No.: 69 · Time: 17.912847 · Source: 2404:6800:4007:811::2004 · Destination: 2401:4900:49ab:8c97:60df:868f:33d1:f2d3 · Protocol: TCP · Length: 86 · Info: 80 → 13064 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1298 SACK_PERM=1 WS=256
```

it is an Ethernet II / Internet Protocol Version 4 / Transmission Control Protocol frame.

Expand Ethernet II



Wireshark · Packet 69 · tcp_connection.pcapng

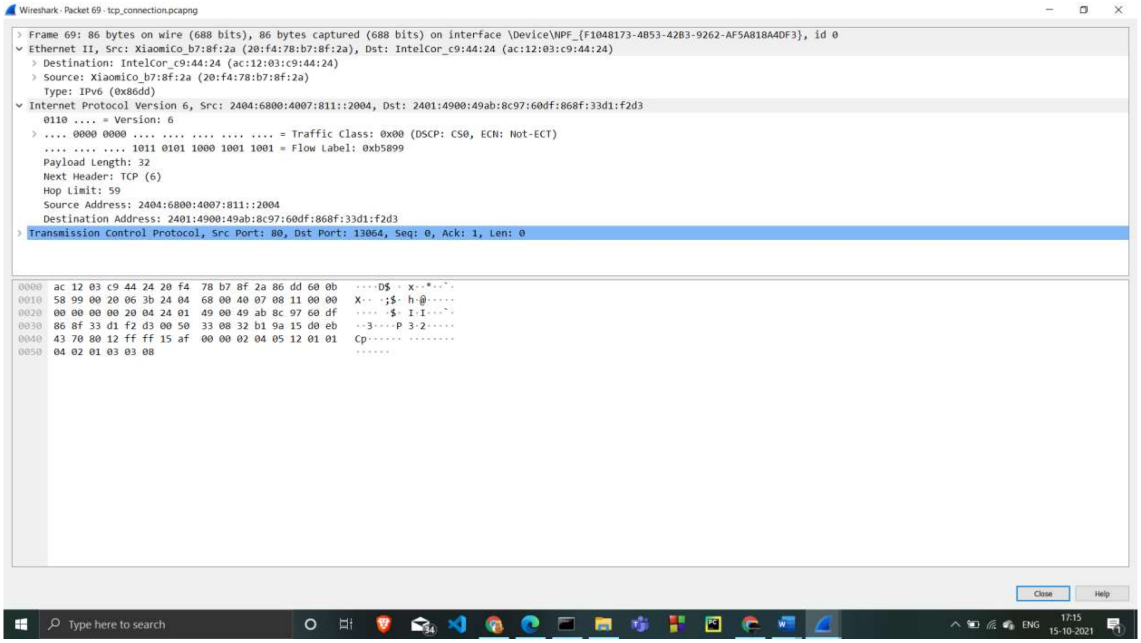
```
> Frame 69: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface \Device\NPF_{F1048173-4B53-42B3-9262-AF5A818A4DF3}, id 0
v Ethernet II, Src: XiaomiCo_b7:8f:2a (20:f4:78:b7:8f:2a), Dst: IntelCor_c9:44:24 (ac:12:03:c9:44:24)
  > Destination: IntelCor_c9:44:24 (ac:12:03:c9:44:24)
  > Source: XiaomiCo_b7:8f:2a (20:f4:78:b7:8f:2a)
    Type: IPv6 (0x86dd)
> Internet Protocol Version 6, Src: 2404:6800:4007:811::2004, Dst: 2401:4900:49ab:8c97:60df:868f:33d1:f2d3
> Transmission Control Protocol, Src Port: 80, Dst Port: 13064, Seq: 0, Ack: 1, Len: 0
```

```
0000  ac 12 03 c9 44 24 20 f4  78 b7 8f 2a 86 dd 60 0b   ····D$ · x··*··`·
0010  58 99 00 20 06 3b 24 04  68 00 40 07 08 11 00 00   X·· ·;$· h·@·····
0020  00 00 00 00 20 04 24 01  49 00 49 ab 8c 97 60 df   ···· ·$· I·I···`·
0030  86 8f 33 d1 f2 d3 00 50  33 08 32 b1 9a 15 d0 eb   ··3····P 3·2·····
0040  43 70 80 12 ff ff 15 af  00 00 02 04 05 12 01 01   Cp······ ········
0050  04 02 01 03 03 08                                  ······
```

The destination is MAC address

The source is default gateway MAC address

Expand Internet Protocol Version 4



Wireshark · Packet 69 · tcp_connection.pcapng

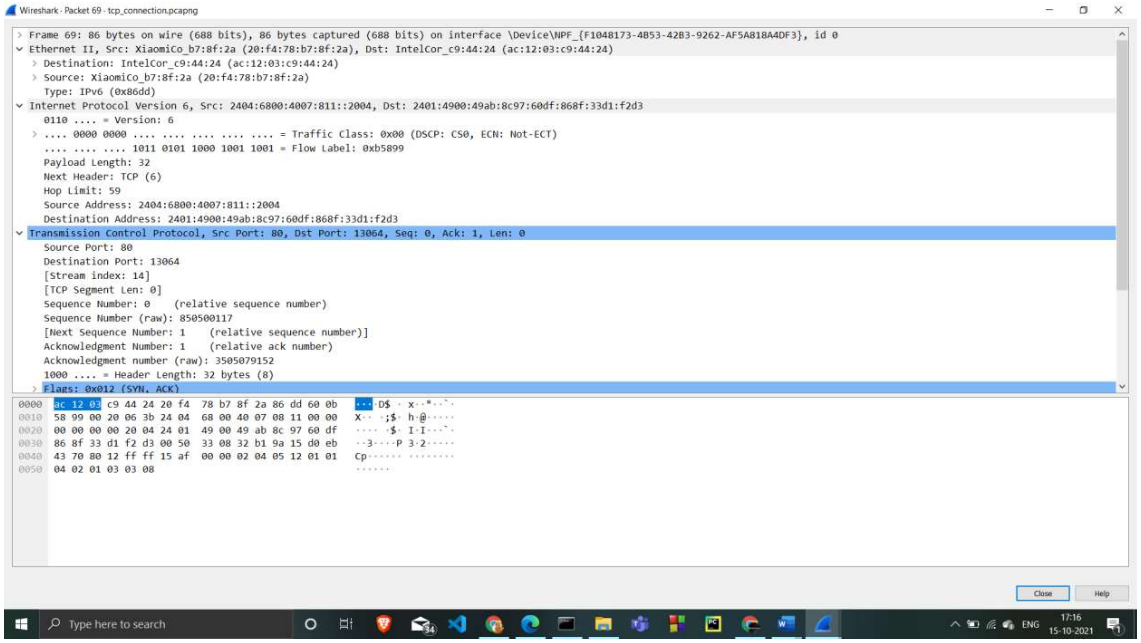
```
> Frame 69: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface \Device\NPF_{F1048173-4B53-42B3-9262-AF5A818A4DF3}, id 0
v Ethernet II, Src: XiaomiCo_b7:8f:2a (20:f4:78:b7:8f:2a), Dst: IntelCor_c9:44:24 (ac:12:03:c9:44:24)
  > Destination: IntelCor_c9:44:24 (ac:12:03:c9:44:24)
  > Source: XiaomiCo_b7:8f:2a (20:f4:78:b7:8f:2a)
    Type: IPv6 (0x86dd)
v Internet Protocol Version 6, Src: 2404:6800:4007:811::2004, Dst: 2401:4900:49ab:8c97:60df:868f:33d1:f2d3
    0110 .... = Version: 6
  > .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... .... .... 1011 0101 1000 1001 1001 = Flow Label: 0xb5899
    Payload Length: 32
    Next Header: TCP (6)
    Hop Limit: 59
    Source Address: 2404:6800:4007:811::2004
    Destination Address: 2401:4900:49ab:8c97:60df:868f:33d1:f2d3
> Transmission Control Protocol, Src Port: 80, Dst Port: 13064, Seq: 0, Ack: 1, Len: 0
```

```
0000  ac 12 03 c9 44 24 20 f4  78 b7 8f 2a 86 dd 60 0b   ····D$ · x··*··`·
0010  58 99 00 20 06 3b 24 04  68 00 40 07 08 11 00 00   X·· ·;$· h·@·····
0020  00 00 00 00 20 04 24 01  49 00 49 ab 8c 97 60 df   ···· ·$· I·I···`·
0030  86 8f 33 d1 f2 d3 00 50  33 08 32 b1 9a 15 d0 eb   ··3····P 3·2·····
0040  43 70 80 12 ff ff 15 af  00 00 02 04 05 12 01 01   Cp······ ········
0050  04 02 01 03 03 08                                  ······
```

the source address is the Google web server IP address

the destination address is system IP address.

Expand Transmission Control Protocol



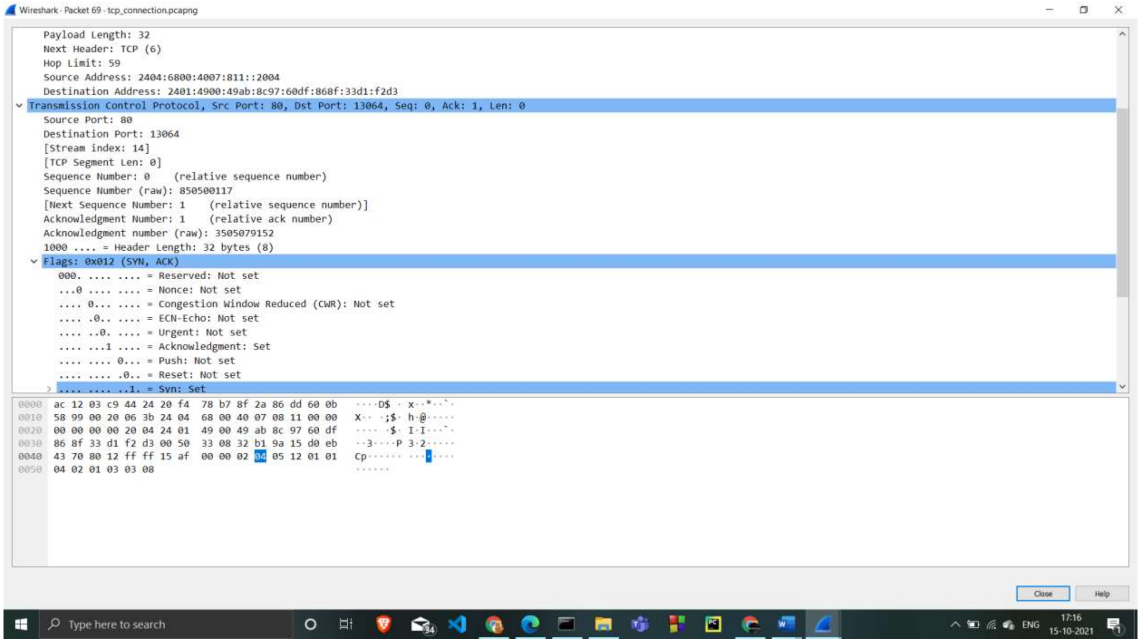
```
> Frame 69: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface \Device\NPF_{F1048173-4B53-42B3-9262-AF5A818A4DF3}, id 0
v Ethernet II, Src: XiaomiCo_b7:8f:2a (20:f4:78:b7:8f:2a), Dst: IntelCor_c9:44:24 (ac:12:03:c9:44:24)
  > Destination: IntelCor_c9:44:24 (ac:12:03:c9:44:24)
  > Source: XiaomiCo_b7:8f:2a (20:f4:78:b7:8f:2a)
    Type: IPv6 (0x86dd)
v Internet Protocol Version 6, Src: 2404:6800:4007:811::2004, Dst: 2401:4900:49ab:8c97:60df:868f:33d1:f2d3
    0110 .... = Version: 6
  > .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... .... .... 1011 0101 1000 1001 1001 = Flow Label: 0xb5899
    Payload Length: 32
    Next Header: TCP (6)
    Hop Limit: 59
    Source Address: 2404:6800:4007:811::2004
    Destination Address: 2401:4900:49ab:8c97:60df:868f:33d1:f2d3
v Transmission Control Protocol, Src Port: 80, Dst Port: 13064, Seq: 0, Ack: 1, Len: 0
    Source Port: 80
    Destination Port: 13064
    [Stream index: 14]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 850500117
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 3505079152
    1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x012 (SYN, ACK)

0000  ac 12 03 c9 44 24 20 f4  78 b7 8f 2a 86 dd 60 0b   ····D$ · x··*··`·
0010  58 99 00 20 06 3b 24 04  68 00 40 07 08 11 00 00   X·· ·;$· h·@·····
0020  00 00 00 00 20 04 24 01  49 00 49 ab 8c 97 60 df   ···· ·$· I·I···`·
0030  86 8f 33 d1 f2 d3 00 50  33 08 32 b1 9a 15 d0 eb   ··3····P 3·2·····
0040  43 70 80 12 ff ff 15 af  00 00 02 04 05 12 01 01   Cp······ ········
0050  04 02 01 03 03 08                                  ······
```

the Source port is http (80)

Destination port is the same dynamic port selected for this connection.

Sequence number is 0, Acknowledgement number is 1

Expand Flags

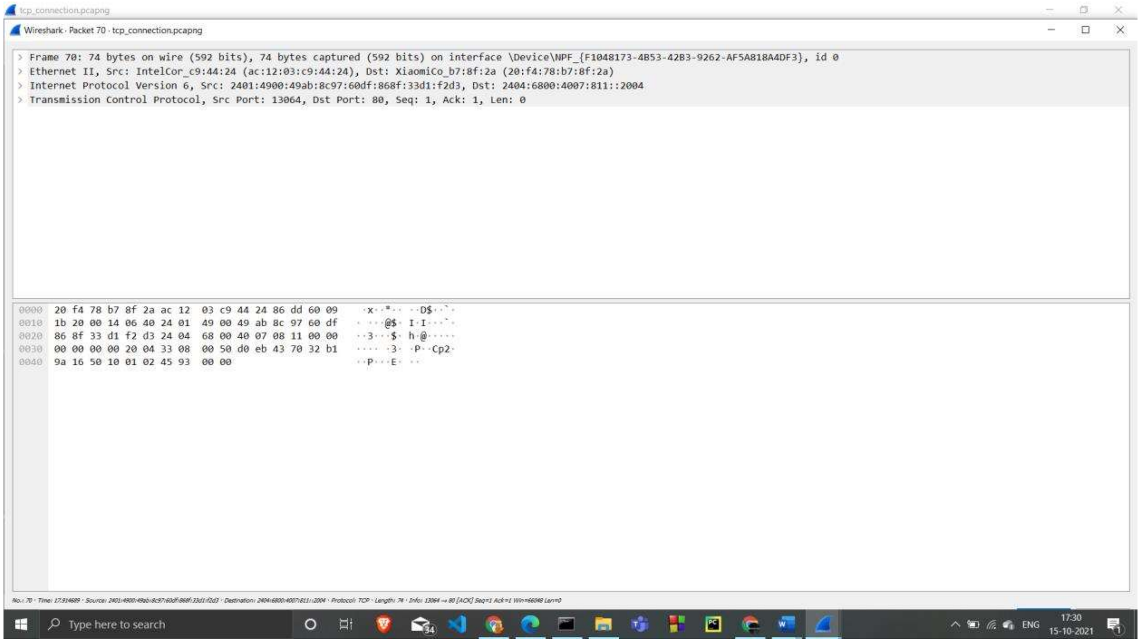


```
    Payload Length: 32
    Next Header: TCP (6)
    Hop Limit: 59
    Source Address: 2404:6800:4007:811::2004
    Destination Address: 2401:4900:49ab:8c97:60df:868f:33d1:f2d3
v Transmission Control Protocol, Src Port: 80, Dst Port: 13064, Seq: 0, Ack: 1, Len: 0
    Source Port: 80
    Destination Port: 13064
    [Stream index: 14]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 850500117
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 3505079152
    1000 .... = Header Length: 32 bytes (8)
  v Flags: 0x012 (SYN, ACK)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Nonce: Not set
      .... 0... .... = Congestion Window Reduced (CWR): Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...1 .... = Acknowledgment: Set
      .... .... 0... = Push: Not set
      .... .... .0.. = Reset: Not set
    > .... .... ..1. = Syn: Set

0000  ac 12 03 c9 44 24 20 f4  78 b7 8f 2a 86 dd 60 0b   ····D$ · x··*··`·
0010  58 99 00 20 06 3b 24 04  68 00 40 07 08 11 00 00   X·· ·;$· h·@·····
0020  00 00 00 00 20 04 24 01  49 00 49 ab 8c 97 60 df   ···· ·$· I·I···`·
0030  86 8f 33 d1 f2 d3 00 50  33 08 32 b1 9a 15 d0 eb   ··3····P 3·2·····
0040  43 70 80 12 ff ff 15 af  00 00 02 04 05 12 01 01   Cp······ ········
0050  04 02 01 03 03 08                                  ······
```

SYN and ACK are set

indicating the second segment in the TCP three-way handshake.

Analysing TCP ACK Traffic



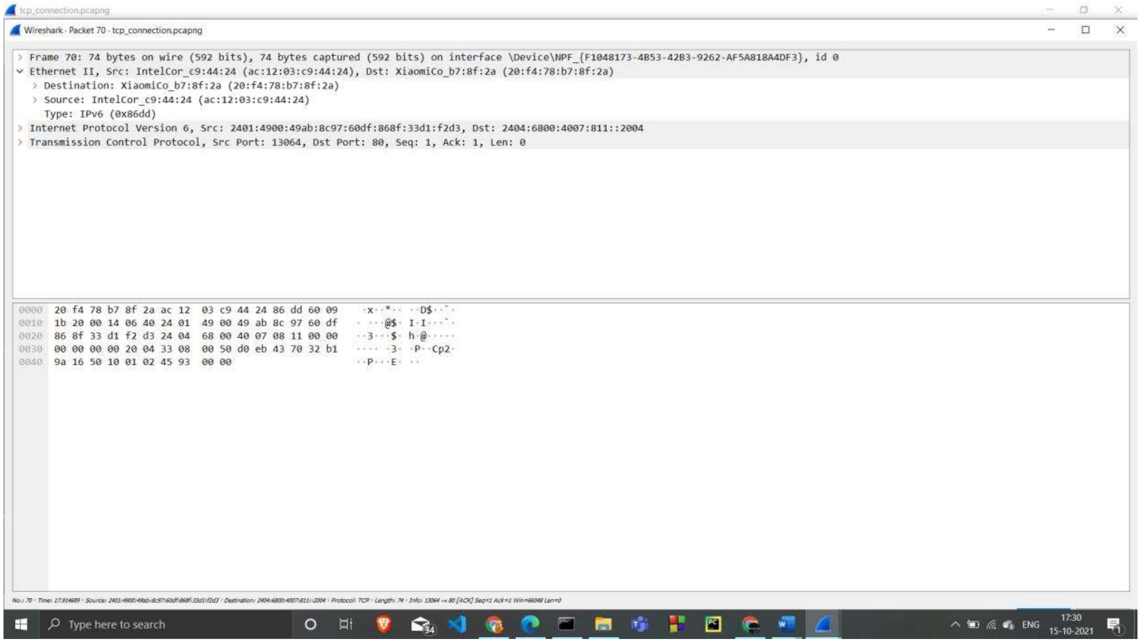
```
> Frame 70: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{F1048173-4B53-42B3-9262-AF5A818A4DF3}, id 0
> Ethernet II, Src: IntelCor_c9:44:24 (ac:12:03:c9:44:24), Dst: XiaomiCo_b7:8f:2a (20:f4:78:b7:8f:2a)
> Internet Protocol Version 6, Src: 2401:4900:49ab:8c97:60df:868f:33d1:f2d3, Dst: 2404:6800:4007:811::2004
> Transmission Control Protocol, Src Port: 13064, Dst Port: 80, Seq: 1, Ack: 1, Len: 0
```

```
0000  20 f4 78 b7 8f 2a ac 12  03 c9 44 24 86 dd 60 09    ·x··*··  ··D$··`·
0010  1b 20 00 14 06 40 24 01  49 00 49 ab 8c 97 60 df   · ···@$· I·I···`·
0020  86 8f 33 d1 f2 d3 24 04  68 00 40 07 08 11 00 00   ··3···$· h·@·····
0030  00 00 00 00 20 04 33 08  00 50 d0 eb 43 70 32 b1   ···· ·3· ·P··Cp2·
0040  9a 16 50 10 01 02 45 93  00 00                     ··P···E· ··
```

```
No.: 70 · Time: 17.914689 · Source: 2401:4900:49ab:8c97:60df:868f:33d1:f2d3 · Destination: 2404:6800:4007:811::2004 · Protocol: TCP · Length: 74 · Info: 13064 → 80 [ACK] Seq=1 Ack=1 Win=66048 Len=0
```

it is an Ethernet II / Internet Protocol Version 4 / Transmission Control Protocol frame.

Expand Ethernet II



```
> Frame 70: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{F1048173-4B53-42B3-9262-AF5A818A4DF3}, id 0
v Ethernet II, Src: IntelCor_c9:44:24 (ac:12:03:c9:44:24), Dst: XiaomiCo_b7:8f:2a (20:f4:78:b7:8f:2a)
  > Destination: XiaomiCo_b7:8f:2a (20:f4:78:b7:8f:2a)
  > Source: IntelCor_c9:44:24 (ac:12:03:c9:44:24)
    Type: IPv6 (0x86dd)
> Internet Protocol Version 6, Src: 2401:4900:49ab:8c97:60df:868f:33d1:f2d3, Dst: 2404:6800:4007:811::2004
> Transmission Control Protocol, Src Port: 13064, Dst Port: 80, Seq: 1, Ack: 1, Len: 0
```

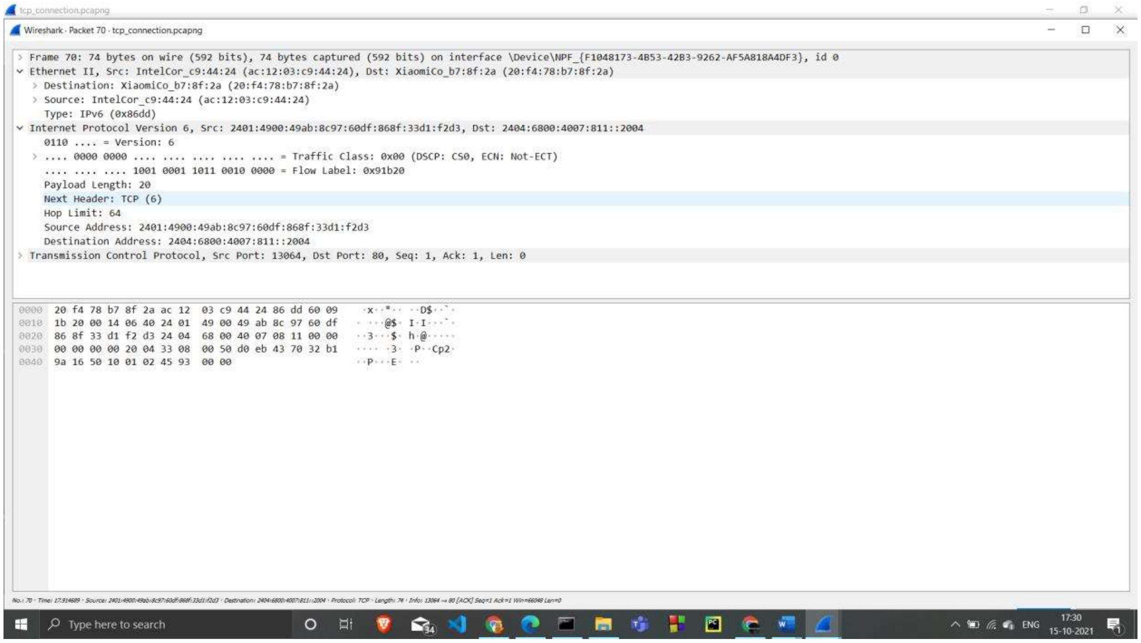
```
0000  20 f4 78 b7 8f 2a ac 12  03 c9 44 24 86 dd 60 09    ·x··*·· ··D$··`·
0010  1b 20 00 14 06 40 24 01  49 00 49 ab 8c 97 60 df   · ···@$· I·I···`·
0020  86 8f 33 d1 f2 d3 24 04  68 00 40 07 08 11 00 00   ··3···$· h·@·····
0030  00 00 00 00 20 04 33 08  00 50 d0 eb 43 70 32 b1   ···· ·3· ·P··Cp2·
0040  9a 16 50 10 01 02 45 93  00 00                     ··P···E· ··
```

```
No.: 70 · Time: 17.914689 · Source: 2401:4900:49ab:8c97:60df:868f:33d1:f2d3 · Destination: 2404:6800:4007:811::2004 · Protocol: TCP · Length: 74 · Info: 13064 → 80 [ACK] Seq=1 Ack=1 Win=66048 Len=0
```

the source address is systeam IP address.

the destination address is the Google web server IP address.

Expand Internet Protocol Version 6



```
> Frame 70: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{F1048173-4B53-42B3-9262-AF5A818A4DF3}, id 0
v Ethernet II, Src: IntelCor_c9:44:24 (ac:12:03:c9:44:24), Dst: XiaomiCo_b7:8f:2a (20:f4:78:b7:8f:2a)
  > Destination: XiaomiCo_b7:8f:2a (20:f4:78:b7:8f:2a)
  > Source: IntelCor_c9:44:24 (ac:12:03:c9:44:24)
    Type: IPv6 (0x86dd)
v Internet Protocol Version 6, Src: 2401:4900:49ab:8c97:60df:868f:33d1:f2d3, Dst: 2404:6800:4007:811::2004
    0110 .... = Version: 6
  > .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... .... .... 1001 0001 1011 0010 0000 = Flow Label: 0x91b20
    Payload Length: 20
    Next Header: TCP (6)
    Hop Limit: 64
    Source Address: 2401:4900:49ab:8c97:60df:868f:33d1:f2d3
    Destination Address: 2404:6800:4007:811::2004
> Transmission Control Protocol, Src Port: 13064, Dst Port: 80, Seq: 1, Ack: 1, Len: 0
```

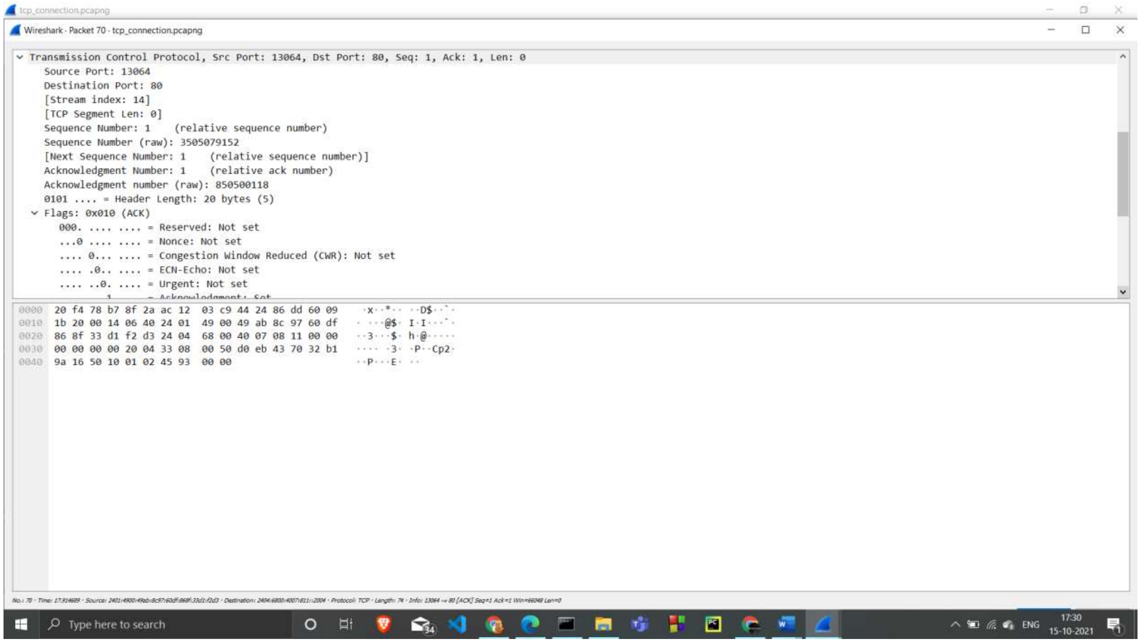
```
0000  20 f4 78 b7 8f 2a ac 12  03 c9 44 24 86 dd 60 09    ·x··*·· ··D$··`·
0010  1b 20 00 14 06 40 24 01  49 00 49 ab 8c 97 60 df   · ···@$· I·I···`·
0020  86 8f 33 d1 f2 d3 24 04  68 00 40 07 08 11 00 00   ··3···$· h·@·····
0030  00 00 00 00 20 04 33 08  00 50 d0 eb 43 70 32 b1   ···· ·3· ·P··Cp2·
0040  9a 16 50 10 01 02 45 93  00 00                     ··P···E· ··
```

```
No.: 70 · Time: 17.914689 · Source: 2401:4900:49ab:8c97:60df:868f:33d1:f2d3 · Destination: 2404:6800:4007:811::2004 · Protocol: TCP · Length: 74 · Info: 13064 → 80 [ACK] Seq=1 Ack=1 Win=66048 Len=0
```

the source address is IP address.

the destination address is the Google web server IP address.

Expand Transmission Control Protocol



```
v Transmission Control Protocol, Src Port: 13064, Dst Port: 80, Seq: 1, Ack: 1, Len: 0
    Source Port: 13064
    Destination Port: 80
    [Stream index: 14]
    [TCP Segment Len: 0]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 3505079152
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 850500118
    0101 .... = Header Length: 20 bytes (5)
  v Flags: 0x010 (ACK)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Nonce: Not set
      .... 0... .... = Congestion Window Reduced (CWR): Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
```

```
0000  20 f4 78 b7 8f 2a ac 12  03 c9 44 24 86 dd 60 09    ·x··*··  ··D$··`·
0010  1b 20 00 14 06 40 24 01  49 00 49 ab 8c 97 60 df    · ···@$·  I·I···`·
0020  86 8f 33 d1 f2 d3 24 04  68 00 40 07 08 11 00 00    ··3···$·  h·@·····
0030  00 00 00 00 20 04 33 08  00 50 d0 eb 43 70 32 b1    ····  ·3·  ·P··Cp2·
0040  9a 16 50 10 01 02 45 93  00 00                      ··P···E·  ··
```

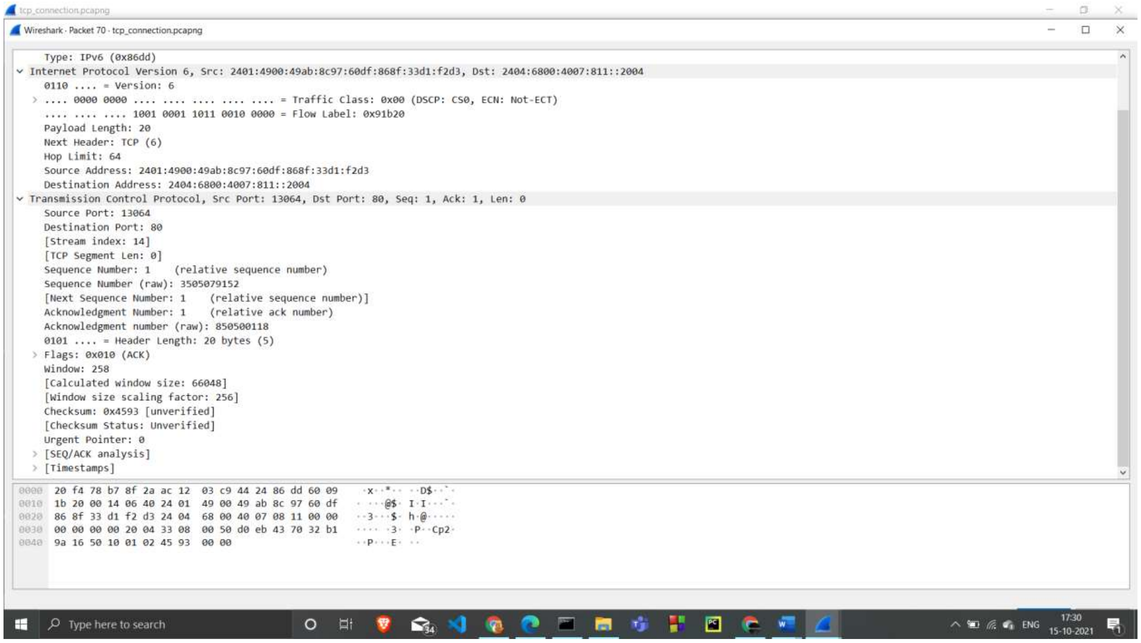
```
No.: 70 · Time: 17.914689 · Source: 2401:4900:49ab:8c97:60df:868f:33d1:f2d3 · Destination: 2404:6800:4007:811::2004 · Protocol: TCP · Length: 74 · Info: 13064 → 80 [ACK] Seq=1 Ack=1 Win=66048 Len=0
```

Source port is the same dynamic port selected for this connection

Destination port is http (80)

Sequence number is 1 , Acknowledgement number is 1

Expand Flags

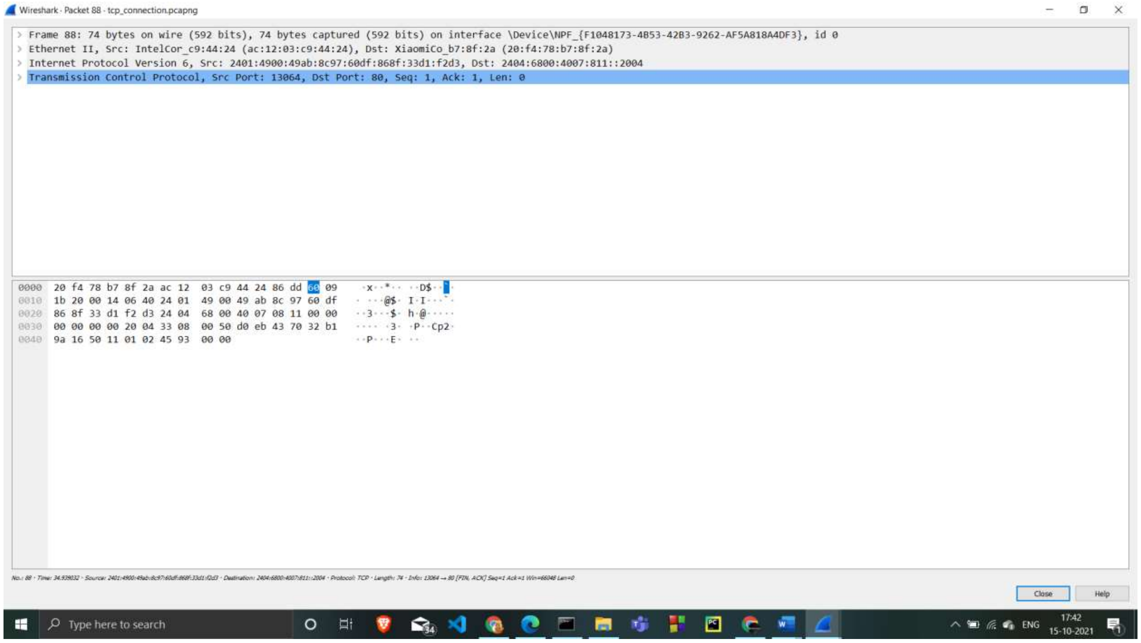


```
    Type: IPv6 (0x86dd)
v Internet Protocol Version 6, Src: 2401:4900:49ab:8c97:60df:868f:33d1:f2d3, Dst: 2404:6800:4007:811::2004
    0110 .... = Version: 6
  > .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... .... .... 1001 0001 1011 0010 0000 = Flow Label: 0x91b20
    Payload Length: 20
    Next Header: TCP (6)
    Hop Limit: 64
    Source Address: 2401:4900:49ab:8c97:60df:868f:33d1:f2d3
    Destination Address: 2404:6800:4007:811::2004
v Transmission Control Protocol, Src Port: 13064, Dst Port: 80, Seq: 1, Ack: 1, Len: 0
    Source Port: 13064
    Destination Port: 80
    [Stream index: 14]
    [TCP Segment Len: 0]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 3505079152
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 850500118
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x010 (ACK)
    Window: 258
    [Calculated window size: 66048]
    [Window size scaling factor: 256]
    Checksum: 0x4593 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > [SEQ/ACK analysis]
  > [Timestamps]
```

```
0000  20 f4 78 b7 8f 2a ac 12  03 c9 44 24 86 dd 60 09    ·x··*··  ··D$··`·
0010  1b 20 00 14 06 40 24 01  49 00 49 ab 8c 97 60 df    · ···@$·  I·I···`·
0020  86 8f 33 d1 f2 d3 24 04  68 00 40 07 08 11 00 00    ··3···$·  h·@·····
0030  00 00 00 00 20 04 33 08  00 50 d0 eb 43 70 32 b1    ····  ·3·  ·P··Cp2·
0040  9a 16 50 10 01 02 45 93  00 00                      ··P···E·  ··
```

ACK is set, indicating the third segment in the TCP three-way handshake. client has established a TCP connection with the server.

Analyse TCP FIN ACK Traffic

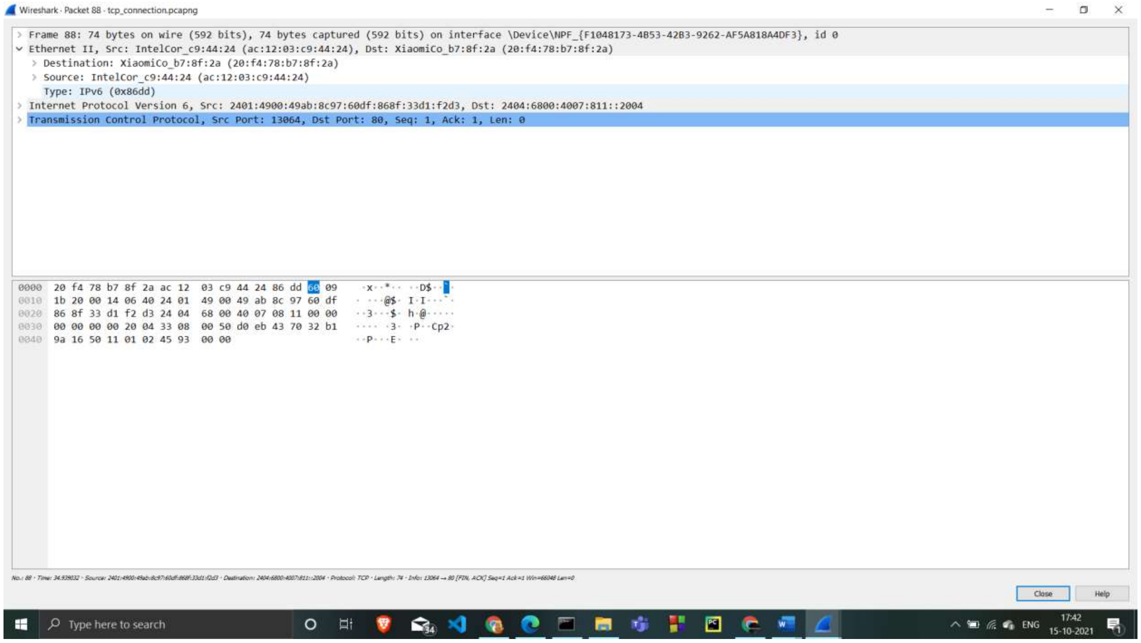


```
> Frame 88: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{F1048173-4B53-42B3-9262-AF5A818A4DF3}, id 0
> Ethernet II, Src: IntelCor_c9:44:24 (ac:12:03:c9:44:24), Dst: XiaomiCo_b7:8f:2a (20:f4:78:b7:8f:2a)
> Internet Protocol Version 6, Src: 2401:4900:49ab:8c97:60df:868f:33d1:f2d3, Dst: 2404:6800:4007:811::2004
> Transmission Control Protocol, Src Port: 13064, Dst Port: 80, Seq: 1, Ack: 1, Len: 0
```

```
0000  20 f4 78 b7 8f 2a ac 12  03 c9 44 24 86 dd 60 09    ·x··*·· ··D$··`·
0010  1b 20 00 14 06 40 24 01  49 00 49 ab 8c 97 60 df   · ···@$· I·I···`·
0020  86 8f 33 d1 f2 d3 24 04  68 00 40 07 08 11 00 00   ··3···$· h·@·····
0030  00 00 00 00 20 04 33 08  00 50 d0 eb 43 70 32 b1   ····· ·3· ·P··Cp2·
0040  9a 16 50 11 01 02 45 93  00 00                     ··P···E· ··
```

No.: 88 · Time: 34.939032 · Source: 2401:4900:49ab:8c97:60df:868f:33d1:f2d3 · Destination: 2404:6800:4007:811::2004 · Protocol: TCP · Length: 74 · Info: 13064 → 80 [FIN, ACK] Seq=1 Ack=1 Win=66048 Len=0 is an Ethernet II / Internet Protocol Version 4 / Transmission Control Protocol frame

Expand Ethernet II

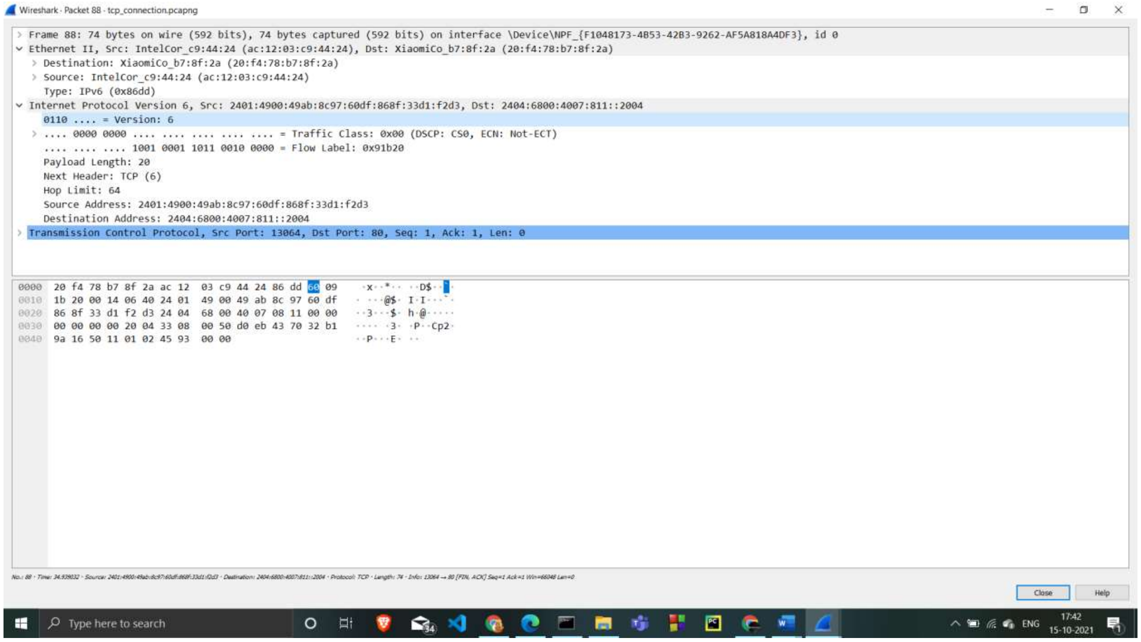


```
> Frame 88: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{F1048173-4B53-42B3-9262-AF5A818A4DF3}, id 0
v Ethernet II, Src: IntelCor_c9:44:24 (ac:12:03:c9:44:24), Dst: XiaomiCo_b7:8f:2a (20:f4:78:b7:8f:2a)
  > Destination: XiaomiCo_b7:8f:2a (20:f4:78:b7:8f:2a)
  > Source: IntelCor_c9:44:24 (ac:12:03:c9:44:24)
    Type: IPv6 (0x86dd)
> Internet Protocol Version 6, Src: 2401:4900:49ab:8c97:60df:868f:33d1:f2d3, Dst: 2404:6800:4007:811::2004
> Transmission Control Protocol, Src Port: 13064, Dst Port: 80, Seq: 1, Ack: 1, Len: 0

0000  20 f4 78 b7 8f 2a ac 12  03 c9 44 24 86 dd 60 09    ·x··*·· ··D$··`·
0010  1b 20 00 14 06 40 24 01  49 00 49 ab 8c 97 60 df    · ···@$· I·I···`·
0020  86 8f 33 d1 f2 d3 24 04  68 00 40 07 08 11 00 00    ··3···$· h·@·····
0030  00 00 00 00 20 04 33 08  00 50 d0 eb 43 70 32 b1    ···· ·3· ·P··Cp2·
0040  9a 16 50 11 01 02 45 93  00 00                      ··P···E· ··

No.: 88 · Time: 34.939032 · Source: 2401:4900:49ab:8c97:60df:868f:33d1:f2d3 · Destination: 2404:6800:4007:811::2004 · Protocol: TCP · Length: 74 · Info: 13064 → 80 [FIN, ACK] Seq=1 Ack=1 Win=66048 Len=0
```

The destination is default gateway MAC address

the source is MAC address

Expand Internet Protocol Version 4

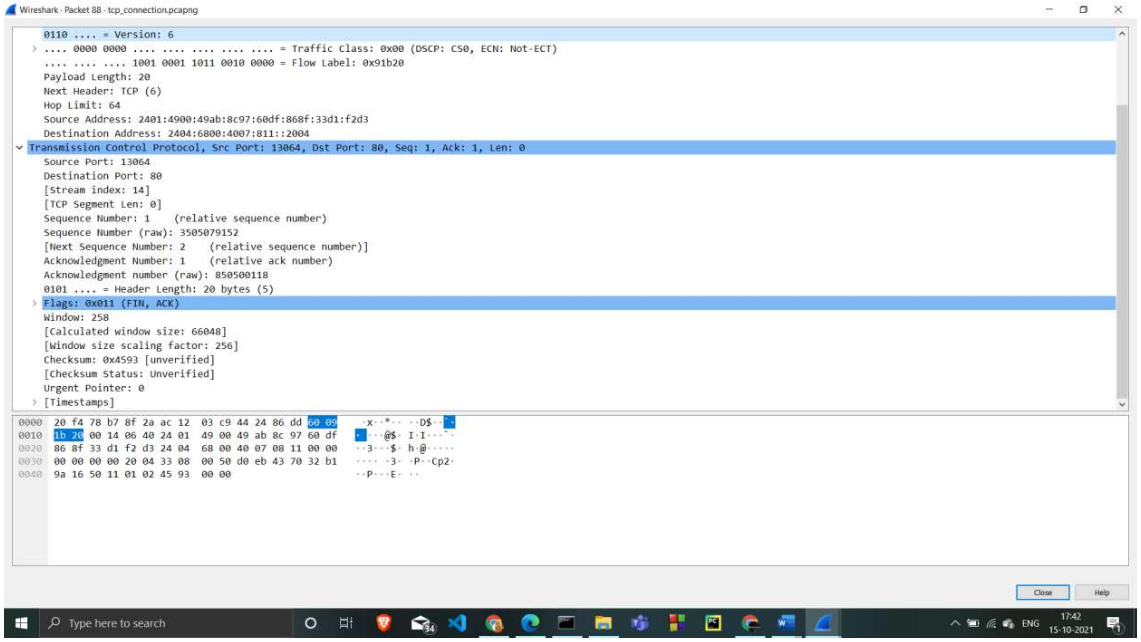


```
> Frame 88: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{F1048173-4B53-42B3-9262-AF5A818A4DF3}, id 0
v Ethernet II, Src: IntelCor_c9:44:24 (ac:12:03:c9:44:24), Dst: XiaomiCo_b7:8f:2a (20:f4:78:b7:8f:2a)
  > Destination: XiaomiCo_b7:8f:2a (20:f4:78:b7:8f:2a)
  > Source: IntelCor_c9:44:24 (ac:12:03:c9:44:24)
    Type: IPv6 (0x86dd)
v Internet Protocol Version 6, Src: 2401:4900:49ab:8c97:60df:868f:33d1:f2d3, Dst: 2404:6800:4007:811::2004
    0110 .... = Version: 6
  > .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... .... .... 1001 0001 1011 0010 0000 = Flow Label: 0x91b20
    Payload Length: 20
    Next Header: TCP (6)
    Hop Limit: 64
    Source Address: 2401:4900:49ab:8c97:60df:868f:33d1:f2d3
    Destination Address: 2404:6800:4007:811::2004
> Transmission Control Protocol, Src Port: 13064, Dst Port: 80, Seq: 1, Ack: 1, Len: 0

0000  20 f4 78 b7 8f 2a ac 12  03 c9 44 24 86 dd 60 09    ·x··*·· ··D$··`·
0010  1b 20 00 14 06 40 24 01  49 00 49 ab 8c 97 60 df    · ···@$· I·I···`·
0020  86 8f 33 d1 f2 d3 24 04  68 00 40 07 08 11 00 00    ··3···$· h·@·····
0030  00 00 00 00 20 04 33 08  00 50 d0 eb 43 70 32 b1    ···· ·3· ·P··Cp2·
0040  9a 16 50 11 01 02 45 93  00 00                      ··P···E· ··

No.: 88 · Time: 34.939032 · Source: 2401:4900:49ab:8c97:60df:868f:33d1:f2d3 · Destination: 2404:6800:4007:811::2004 · Protocol: TCP · Length: 74 · Info: 13064 → 80 [FIN, ACK] Seq=1 Ack=1 Win=66048 Len=0
```

The source address is systeam IP address.

the destination address is the Google web server IP address.

Expand Transmission Control Protocol



```
    0110 .... = Version: 6
  > .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... .... .... 1001 0001 1011 0010 0000 = Flow Label: 0x91b20
    Payload Length: 20
    Next Header: TCP (6)
    Hop Limit: 64
    Source Address: 2401:4900:49ab:8c97:60df:868f:33d1:f2d3
    Destination Address: 2404:6800:4007:811::2004
v Transmission Control Protocol, Src Port: 13064, Dst Port: 80, Seq: 1, Ack: 1, Len: 0
    Source Port: 13064
    Destination Port: 80
    [Stream index: 14]
    [TCP Segment Len: 0]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 3505079152
    [Next Sequence Number: 2    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 850500118
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x011 (FIN, ACK)
    Window: 258
    [Calculated window size: 66048]
    [Window size scaling factor: 256]
    Checksum: 0x4593 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > [Timestamps]
```

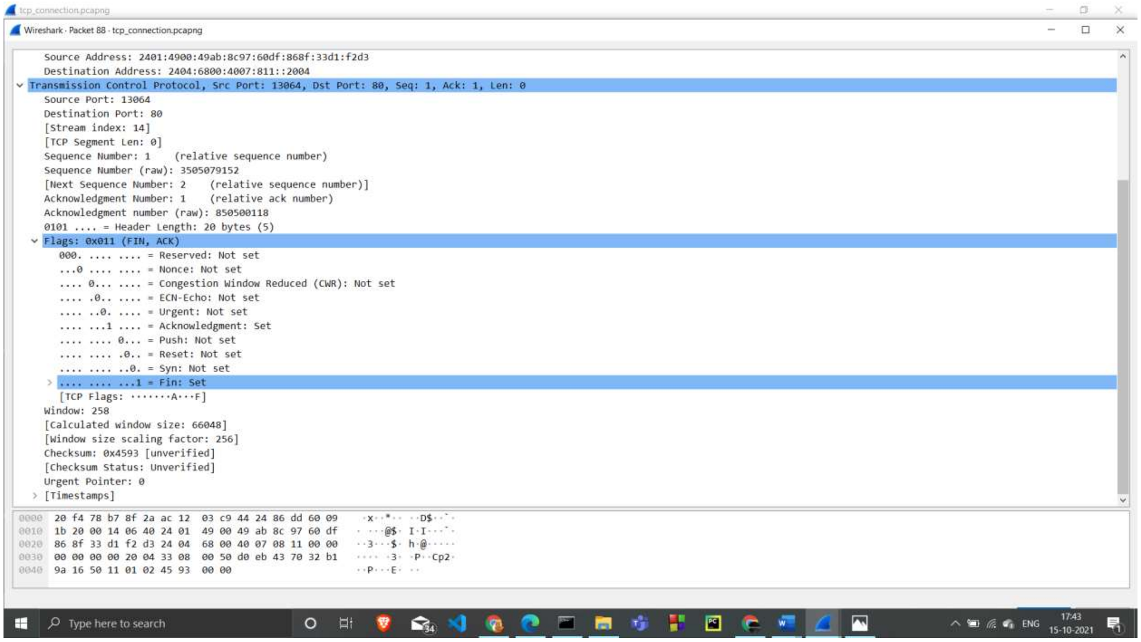
```
0000  20 f4 78 b7 8f 2a ac 12  03 c9 44 24 86 dd 60 09    ·x··*··· ··D$··`·
0010  1b 20 00 14 06 40 24 01  49 00 49 ab 8c 97 60 df   · ···@$· I·I···`·
0020  86 8f 33 d1 f2 d3 24 04  68 00 40 07 08 11 00 00   ··3···$· h·@·····
0030  00 00 00 00 20 04 33 08  00 50 d0 eb 43 70 32 b1   ···· ·3· ·P··Cp2·
0040  9a 16 50 11 01 02 45 93  00 00                     ··P···E· ··
```

Source port is dynamic port selected for this connection.

the Destination is http (80).

Sequence number is 1, Acknowledgement number is 1

Expand Flags



```
    Source Address: 2401:4900:49ab:8c97:60df:868f:33d1:f2d3
    Destination Address: 2404:6800:4007:811::2004
v Transmission Control Protocol, Src Port: 13064, Dst Port: 80, Seq: 1, Ack: 1, Len: 0
    Source Port: 13064
    Destination Port: 80
    [Stream index: 14]
    [TCP Segment Len: 0]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 3505079152
    [Next Sequence Number: 2    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 850500118
    0101 .... = Header Length: 20 bytes (5)
  v Flags: 0x011 (FIN, ACK)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Nonce: Not set
      .... 0... .... = Congestion Window Reduced (CWR): Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...1 .... = Acknowledgment: Set
      .... .... 0... = Push: Not set
      .... .... .0.. = Reset: Not set
      .... .... ..0. = Syn: Not set
    > .... .... ...1 = Fin: Set
      [TCP Flags: ·······A···F]
    Window: 258
    [Calculated window size: 66048]
    [Window size scaling factor: 256]
    Checksum: 0x4593 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > [Timestamps]
```

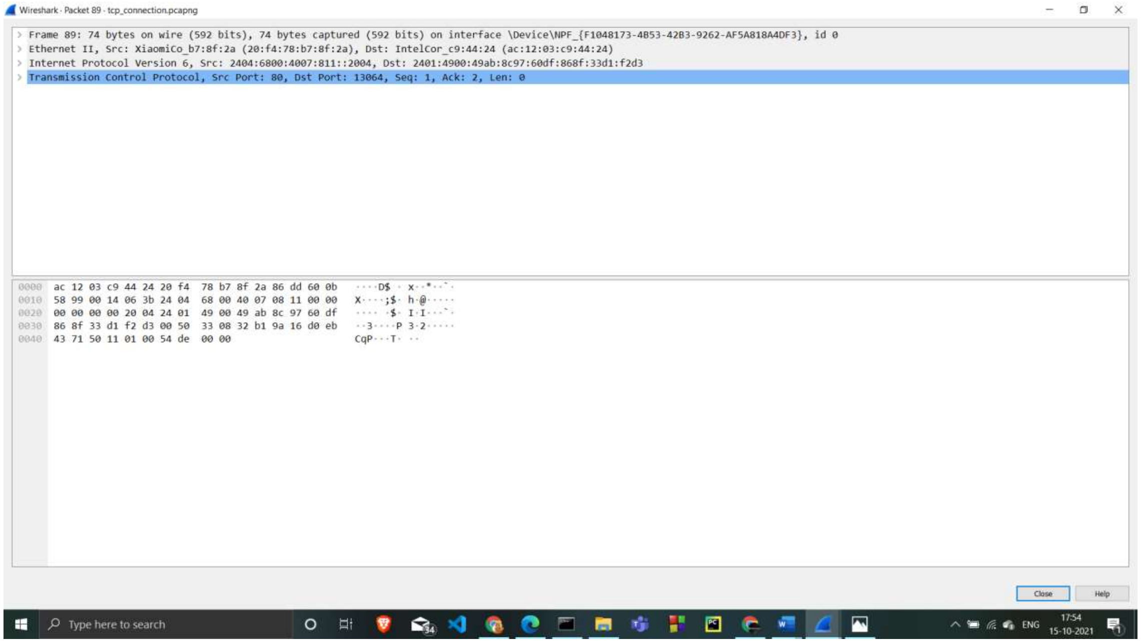
```
0000  20 f4 78 b7 8f 2a ac 12  03 c9 44 24 86 dd 60 09    ·x··*··· ··D$··`·
0010  1b 20 00 14 06 40 24 01  49 00 49 ab 8c 97 60 df   · ···@$· I·I···`·
0020  86 8f 33 d1 f2 d3 24 04  68 00 40 07 08 11 00 00   ··3···$· h·@·····
0030  00 00 00 00 20 04 33 08  00 50 d0 eb 43 70 32 b1   ···· ·3· ·P··Cp2·
0040  9a 16 50 11 01 02 45 93  00 00                     ··P···E· ··
```

FIN and ACK are set

indicating the first segment in the TCP teardown handshake .

The client has indicated it is closing the TCP connection with the

Analyse TCP FIN ACK Traffic

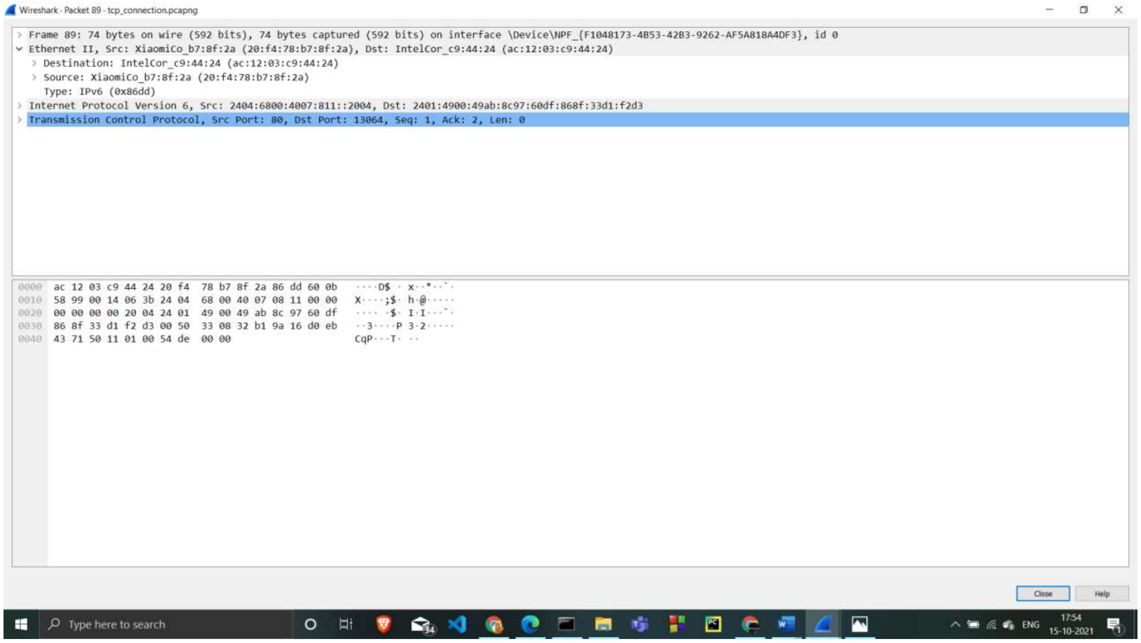


```
> Frame 89: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{F1048173-4B53-42B3-9262-AF5A818A4DF3}, id 0
> Ethernet II, Src: XiaomiCo_b7:8f:2a (20:f4:78:b7:8f:2a), Dst: IntelCor_c9:44:24 (ac:12:03:c9:44:24)
> Internet Protocol Version 6, Src: 2404:6800:4007:811::2004, Dst: 2401:4900:49ab:8c97:60df:868f:33d1:f2d3
> Transmission Control Protocol, Src Port: 80, Dst Port: 13064, Seq: 1, Ack: 2, Len: 0
```

```
0000  ac 12 03 c9 44 24 20 f4  78 b7 8f 2a 86 dd 60 0b   ····D$ · x··*··`·
0010  58 99 00 14 06 3b 24 04  68 00 40 07 08 11 00 00   X····;$· h·@·····
0020  00 00 00 00 20 04 24 01  49 00 49 ab 8c 97 60 df   ···· ·$· I·I···`·
0030  86 8f 33 d1 f2 d3 00 50  33 08 32 b1 9a 16 d0 eb   ··3····P 3·2·····
0040  43 71 50 11 01 00 54 de  00 00                     CqP···T· ··
```

is an Ethernet II / Internet Protocol Version 4 / Transmission Control Protocol frame.

Expand Ethernet II to view Ethernet details



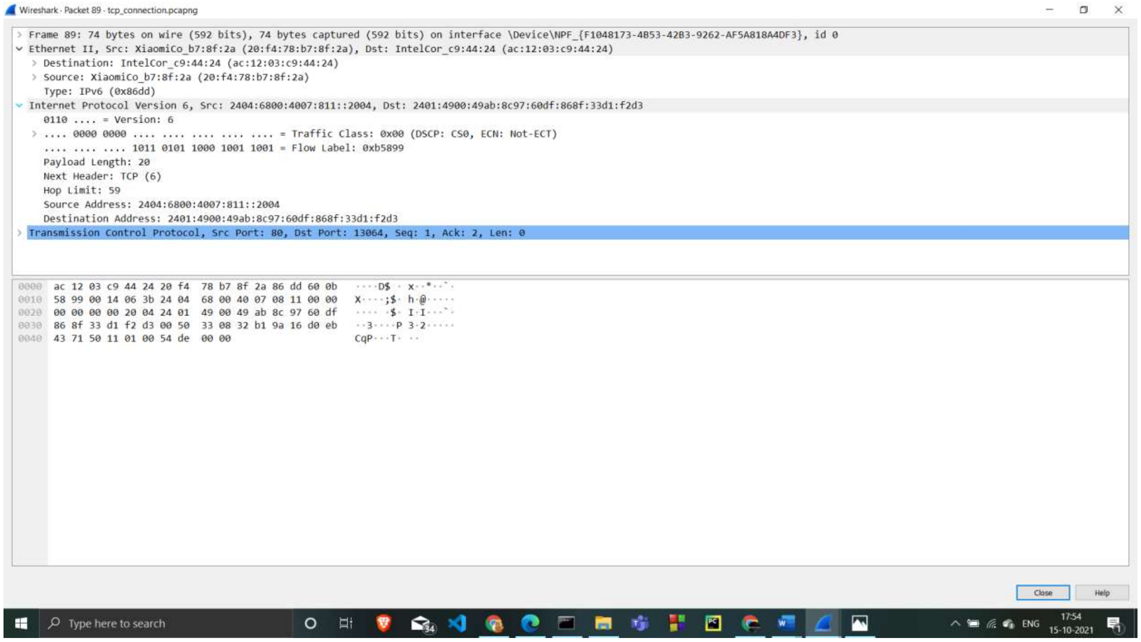
```
> Frame 89: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{F1048173-4B53-42B3-9262-AF5A818A4DF3}, id 0
v Ethernet II, Src: XiaomiCo_b7:8f:2a (20:f4:78:b7:8f:2a), Dst: IntelCor_c9:44:24 (ac:12:03:c9:44:24)
  > Destination: IntelCor_c9:44:24 (ac:12:03:c9:44:24)
  > Source: XiaomiCo_b7:8f:2a (20:f4:78:b7:8f:2a)
    Type: IPv6 (0x86dd)
> Internet Protocol Version 6, Src: 2404:6800:4007:811::2004, Dst: 2401:4900:49ab:8c97:60df:868f:33d1:f2d3
> Transmission Control Protocol, Src Port: 80, Dst Port: 13064, Seq: 1, Ack: 2, Len: 0
```

```
0000  ac 12 03 c9 44 24 20 f4  78 b7 8f 2a 86 dd 60 0b   ····D$ · x··*··`·
0010  58 99 00 14 06 3b 24 04  68 00 40 07 08 11 00 00   X····;$· h·@·····
0020  00 00 00 00 20 04 24 01  49 00 49 ab 8c 97 60 df   ···· ·$· I·I···`·
0030  86 8f 33 d1 f2 d3 00 50  33 08 32 b1 9a 16 d0 eb   ··3····P 3·2·····
0040  43 71 50 11 01 00 54 de  00 00                     CqP···T· ··
```

The destination system MAC address

the source should be system default gateway MAC address

Expand Internet Protocol Version 4



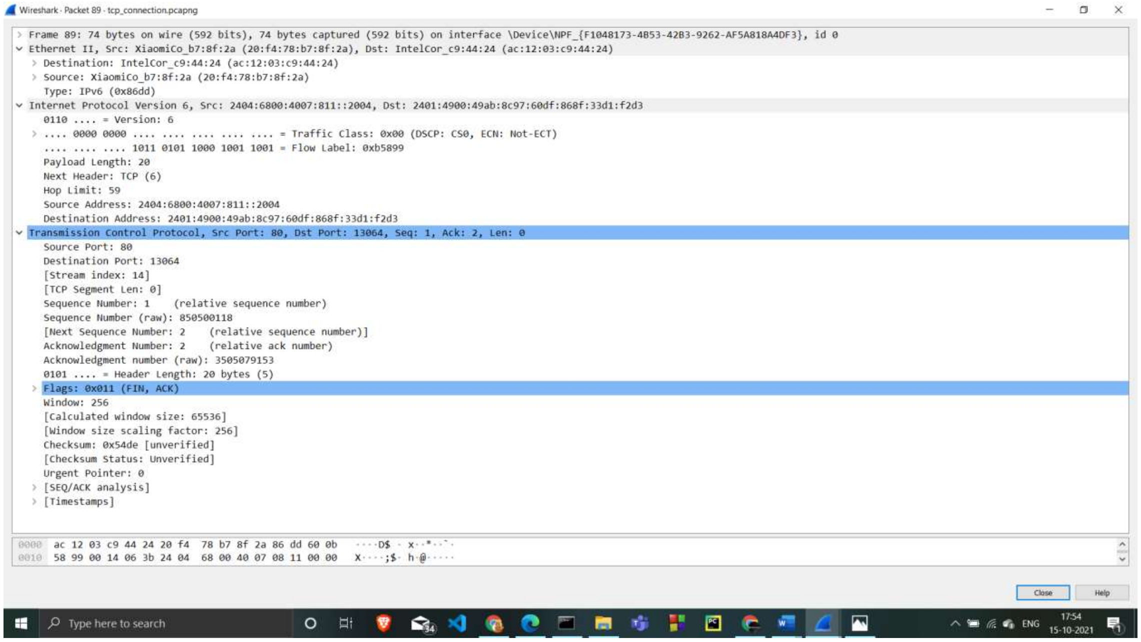
```
> Frame 89: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{F1048173-4B53-42B3-9262-AF5A818A4DF3}, id 0
v Ethernet II, Src: XiaomiCo_b7:8f:2a (20:f4:78:b7:8f:2a), Dst: IntelCor_c9:44:24 (ac:12:03:c9:44:24)
  > Destination: IntelCor_c9:44:24 (ac:12:03:c9:44:24)
  > Source: XiaomiCo_b7:8f:2a (20:f4:78:b7:8f:2a)
    Type: IPv6 (0x86dd)
v Internet Protocol Version 6, Src: 2404:6800:4007:811::2004, Dst: 2401:4900:49ab:8c97:60df:868f:33d1:f2d3
    0110 .... = Version: 6
  > .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... .... .... 1011 0101 1000 1001 1001 = Flow Label: 0xb5899
    Payload Length: 20
    Next Header: TCP (6)
    Hop Limit: 59
    Source Address: 2404:6800:4007:811::2004
    Destination Address: 2401:4900:49ab:8c97:60df:868f:33d1:f2d3
> Transmission Control Protocol, Src Port: 80, Dst Port: 13064, Seq: 1, Ack: 2, Len: 0
```

```
0000  ac 12 03 c9 44 24 20 f4  78 b7 8f 2a 86 dd 60 0b   ····D$ · x··*··`·
0010  58 99 00 14 06 3b 24 04  68 00 40 07 08 11 00 00   X····;$· h·@·····
0020  00 00 00 00 20 04 24 01  49 00 49 ab 8c 97 60 df   ···· ·$· I·I···`·
0030  86 8f 33 d1 f2 d3 00 50  33 08 32 b1 9a 16 d0 eb   ··3····P 3·2·····
0040  43 71 50 11 01 00 54 de  00 00                     CqP···T· ··
```

the source address is the Google web server IP address

the destination address is system IP address

Expand Transmission Control Protocol



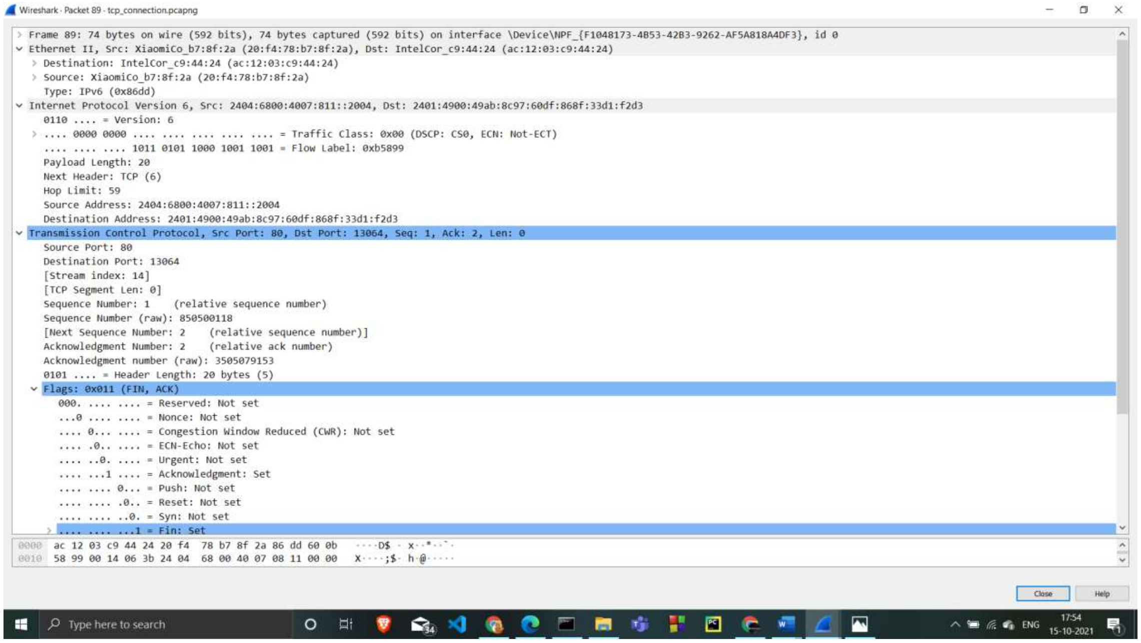
```
> Frame 89: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{F1048173-4B53-42B3-9262-AF5A818A4DF3}, id 0
v Ethernet II, Src: XiaomiCo_b7:8f:2a (20:f4:78:b7:8f:2a), Dst: IntelCor_c9:44:24 (ac:12:03:c9:44:24)
  > Destination: IntelCor_c9:44:24 (ac:12:03:c9:44:24)
  > Source: XiaomiCo_b7:8f:2a (20:f4:78:b7:8f:2a)
    Type: IPv6 (0x86dd)
v Internet Protocol Version 6, Src: 2404:6800:4007:811::2004, Dst: 2401:4900:49ab:8c97:60df:868f:33d1:f2d3
    0110 .... = Version: 6
  > .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... .... .... 1011 0101 1000 1001 1001 = Flow Label: 0xb5899
    Payload Length: 20
    Next Header: TCP (6)
    Hop Limit: 59
    Source Address: 2404:6800:4007:811::2004
    Destination Address: 2401:4900:49ab:8c97:60df:868f:33d1:f2d3
v Transmission Control Protocol, Src Port: 80, Dst Port: 13064, Seq: 1, Ack: 2, Len: 0
    Source Port: 80
    Destination Port: 13064
    [Stream index: 14]
    [TCP Segment Len: 0]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 850500118
    [Next Sequence Number: 2    (relative sequence number)]
    Acknowledgment Number: 2    (relative ack number)
    Acknowledgment number (raw): 3505079153
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x011 (FIN, ACK)
    Window: 256
    [Calculated window size: 65536]
    [Window size scaling factor: 256]
    Checksum: 0x54de [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > [SEQ/ACK analysis]
  > [Timestamps]

0000  ac 12 03 c9 44 24 20 f4  78 b7 8f 2a 86 dd 60 0b   ····D$ · x··*··`·
0010  58 99 00 14 06 3b 24 04  68 00 40 07 08 11 00 00   X····;$· h·@·····
```

the Source port is http (80).

he same dynamic port selected for this connection

Sequence number is 1, Acknowledgement number is 2

Expand Flags



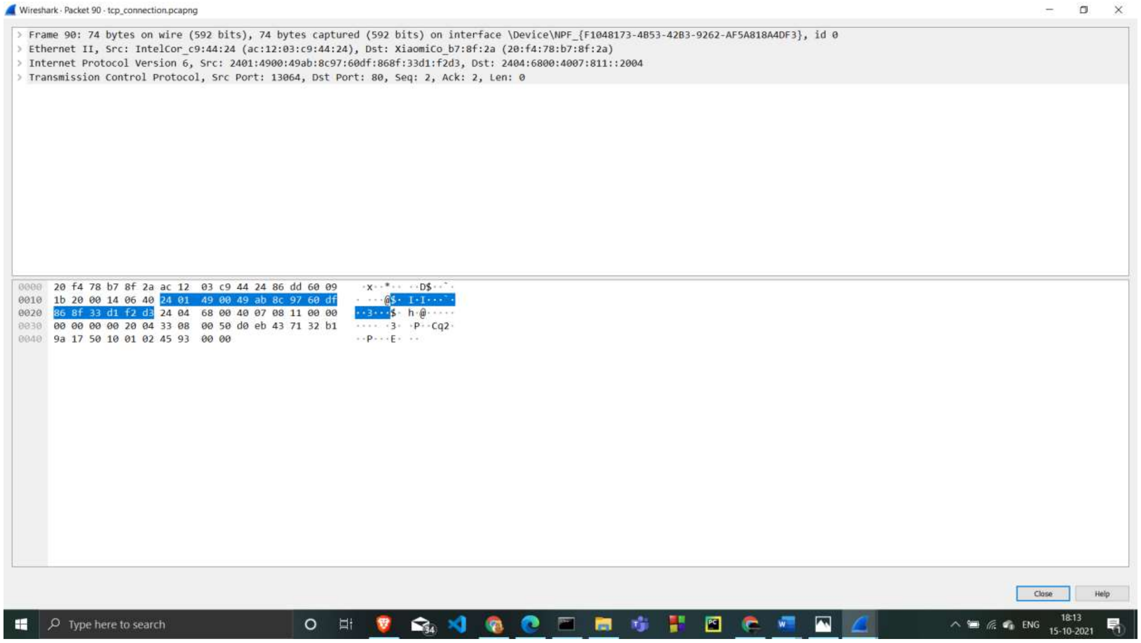
```
> Frame 89: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{F1048173-4B53-42B3-9262-AF5A818A4DF3}, id 0
v Ethernet II, Src: XiaomiCo_b7:8f:2a (20:f4:78:b7:8f:2a), Dst: IntelCor_c9:44:24 (ac:12:03:c9:44:24)
  > Destination: IntelCor_c9:44:24 (ac:12:03:c9:44:24)
  > Source: XiaomiCo_b7:8f:2a (20:f4:78:b7:8f:2a)
    Type: IPv6 (0x86dd)
v Internet Protocol Version 6, Src: 2404:6800:4007:811::2004, Dst: 2401:4900:49ab:8c97:60df:868f:33d1:f2d3
    0110 .... = Version: 6
  > .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... .... .... 1011 0101 1000 1001 1001 = Flow Label: 0xb5899
    Payload Length: 20
    Next Header: TCP (6)
    Hop Limit: 59
    Source Address: 2404:6800:4007:811::2004
    Destination Address: 2401:4900:49ab:8c97:60df:868f:33d1:f2d3
v Transmission Control Protocol, Src Port: 80, Dst Port: 13064, Seq: 1, Ack: 2, Len: 0
    Source Port: 80
    Destination Port: 13064
    [Stream index: 14]
    [TCP Segment Len: 0]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 850500118
    [Next Sequence Number: 2    (relative sequence number)]
    Acknowledgment Number: 2    (relative ack number)
    Acknowledgment number (raw): 3505079153
    0101 .... = Header Length: 20 bytes (5)
  v Flags: 0x011 (FIN, ACK)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Nonce: Not set
      .... 0... .... = Congestion Window Reduced (CWR): Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...1 .... = Acknowledgment: Set
      .... .... 0... = Push: Not set
      .... .... .0.. = Reset: Not set
      .... .... ..0. = Syn: Not set
    > .... .... ...1 = Fin: Set

0000  ac 12 03 c9 44 24 20 f4  78 b7 8f 2a 86 dd 60 0b   ····D$ · x··*··`·
0010  58 99 00 14 06 3b 24 04  68 00 40 07 08 11 00 00   X····;$· h·@·····
```

FIN and ACK are set

indicating the second segment in the TCP three-way handshake

The server has indicated it is closing the TCP connection with the client.

Analyse TCP ACK Traffic



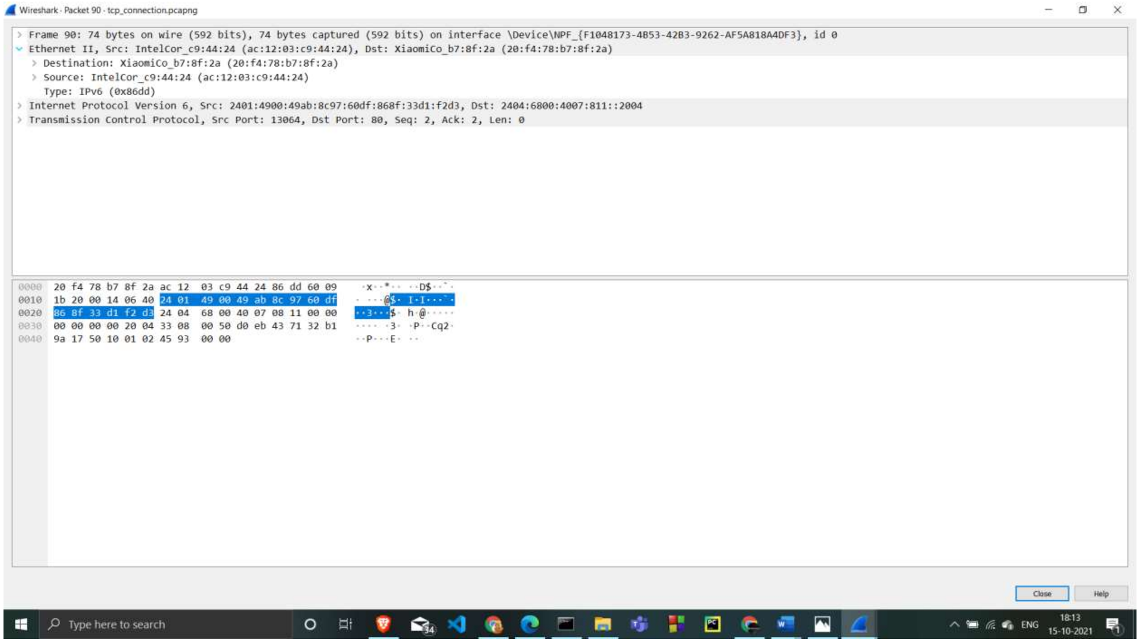
Wireshark · Packet 90 · tcp_connection.pcapng

```
> Frame 90: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{F1048173-4B53-42B3-9262-AF5A818A4DF3}, id 0
> Ethernet II, Src: IntelCor_c9:44:24 (ac:12:03:c9:44:24), Dst: XiaomiCo_b7:8f:2a (20:f4:78:b7:8f:2a)
> Internet Protocol Version 6, Src: 2401:4900:49ab:8c97:60df:868f:33d1:f2d3, Dst: 2404:6800:4007:811::2004
> Transmission Control Protocol, Src Port: 13064, Dst Port: 80, Seq: 2, Ack: 2, Len: 0
```

```
0000  20 f4 78 b7 8f 2a ac 12  03 c9 44 24 86 dd 60 09    ·x··*·· ··D$··`·
0010  1b 20 00 14 06 40 24 01  49 00 49 ab 8c 97 60 df    · ···@$· I·I···`·
0020  86 8f 33 d1 f2 d3 24 04  68 00 40 07 08 11 00 00    ··3···$· h·@·····
0030  00 00 00 00 20 04 33 08  00 50 d0 eb 43 71 32 b1    ···· ·3· ·P··Cq2·
0040  9a 17 50 10 01 02 45 93  00 00                      ··P···E· ··
```

it is an Ethernet II / Internet Protocol Version 4 / Transmission Control Protocol frame.

Expand Ethernet II to view Ethernet details.



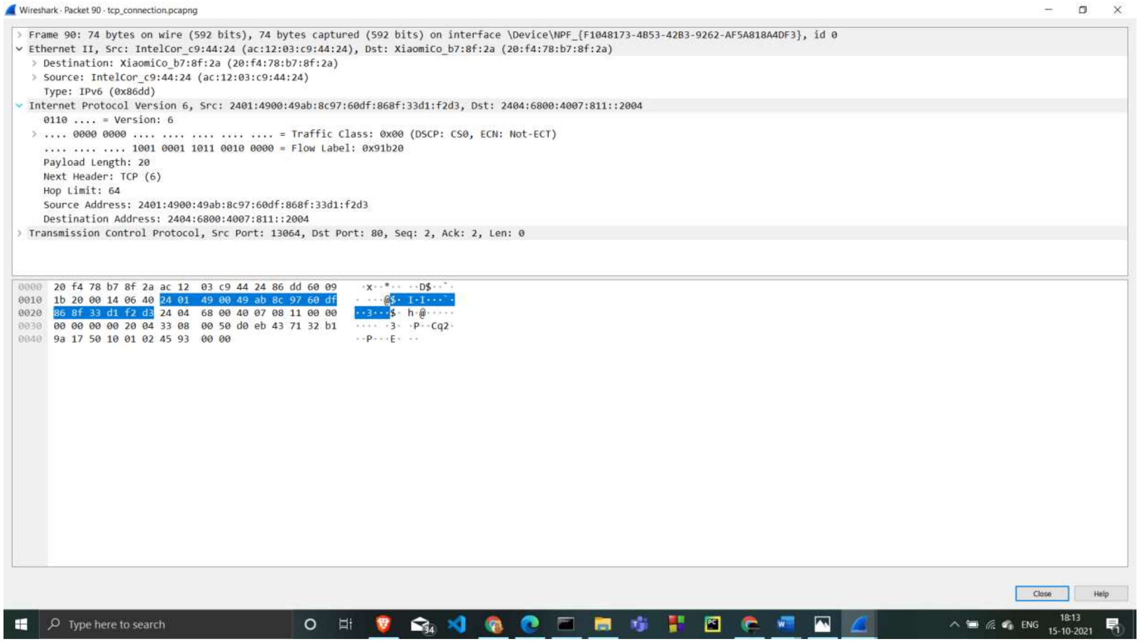
```
> Frame 90: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{F1048173-4B53-42B3-9262-AF5A818A4DF3}, id 0
v Ethernet II, Src: IntelCor_c9:44:24 (ac:12:03:c9:44:24), Dst: XiaomiCo_b7:8f:2a (20:f4:78:b7:8f:2a)
  > Destination: XiaomiCo_b7:8f:2a (20:f4:78:b7:8f:2a)
  > Source: IntelCor_c9:44:24 (ac:12:03:c9:44:24)
    Type: IPv6 (0x86dd)
> Internet Protocol Version 6, Src: 2401:4900:49ab:8c97:60df:868f:33d1:f2d3, Dst: 2404:6800:4007:811::2004
> Transmission Control Protocol, Src Port: 13064, Dst Port: 80, Seq: 2, Ack: 2, Len: 0
```

```
0000  20 f4 78 b7 8f 2a ac 12  03 c9 44 24 86 dd 60 09   ·x··*·····D$··`·
0010  1b 20 00 14 06 40 24 01  49 00 49 ab 8c 97 60 df   ·····@$·I·I···`·
0020  86 8f 33 d1 f2 d3 24 04  68 00 40 07 08 11 00 00   ··3···$·h·@·····
0030  00 00 00 00 20 04 33 08  00 50 d0 eb 43 71 32 b1   ······3··P··Cq2·
0040  9a 17 50 10 01 02 45 93  00 00                     ··P···E···
```

The destination system system default gateway MAC address

the source systeam MAC address.

Expand Internet Protocol Version 4 to view IP details



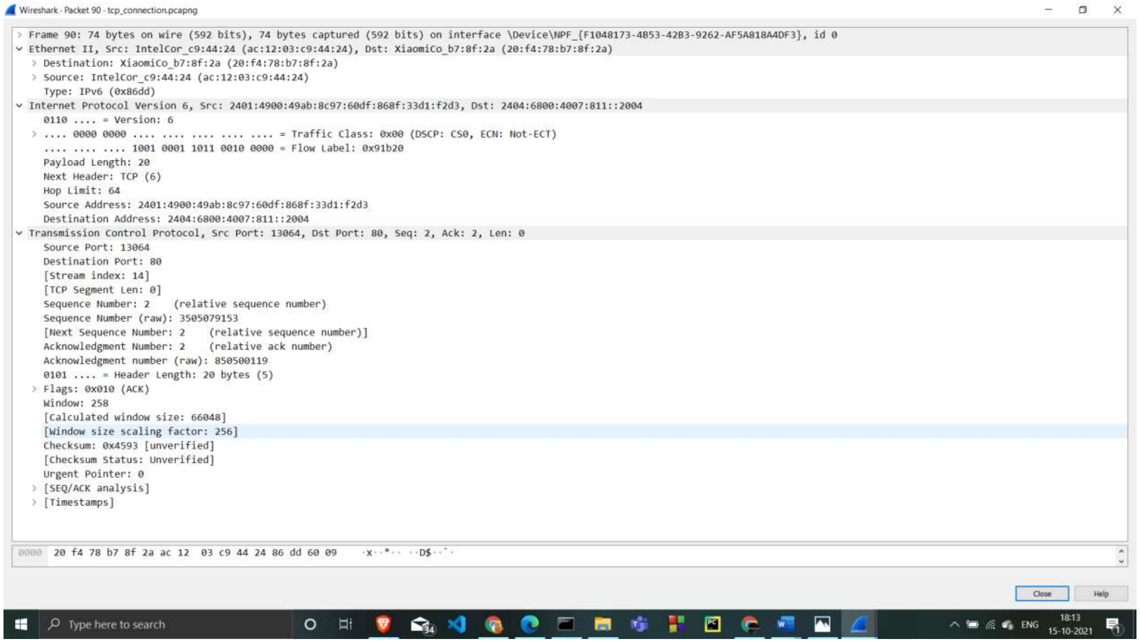
```
> Frame 90: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{F1048173-4B53-42B3-9262-AF5A818A4DF3}, id 0
v Ethernet II, Src: IntelCor_c9:44:24 (ac:12:03:c9:44:24), Dst: XiaomiCo_b7:8f:2a (20:f4:78:b7:8f:2a)
  > Destination: XiaomiCo_b7:8f:2a (20:f4:78:b7:8f:2a)
  > Source: IntelCor_c9:44:24 (ac:12:03:c9:44:24)
    Type: IPv6 (0x86dd)
v Internet Protocol Version 6, Src: 2401:4900:49ab:8c97:60df:868f:33d1:f2d3, Dst: 2404:6800:4007:811::2004
    0110 .... = Version: 6
  > .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... .... .... 1001 0001 1011 0010 0000 = Flow Label: 0x91b20
    Payload Length: 20
    Next Header: TCP (6)
    Hop Limit: 64
    Source Address: 2401:4900:49ab:8c97:60df:868f:33d1:f2d3
    Destination Address: 2404:6800:4007:811::2004
> Transmission Control Protocol, Src Port: 13064, Dst Port: 80, Seq: 2, Ack: 2, Len: 0
```

```
0000  20 f4 78 b7 8f 2a ac 12  03 c9 44 24 86 dd 60 09   ·x··*·····D$··`·
0010  1b 20 00 14 06 40 24 01  49 00 49 ab 8c 97 60 df   ·····@$·I·I···`·
0020  86 8f 33 d1 f2 d3 24 04  68 00 40 07 08 11 00 00   ··3···$·h·@·····
0030  00 00 00 00 20 04 33 08  00 50 d0 eb 43 71 32 b1   ······3··P··Cq2·
0040  9a 17 50 10 01 02 45 93  00 00                     ··P···E···
```

the source address is your IP address.

the destination address is the Google web server IP address

Expand Transmission Control Protocol to view TCP details.



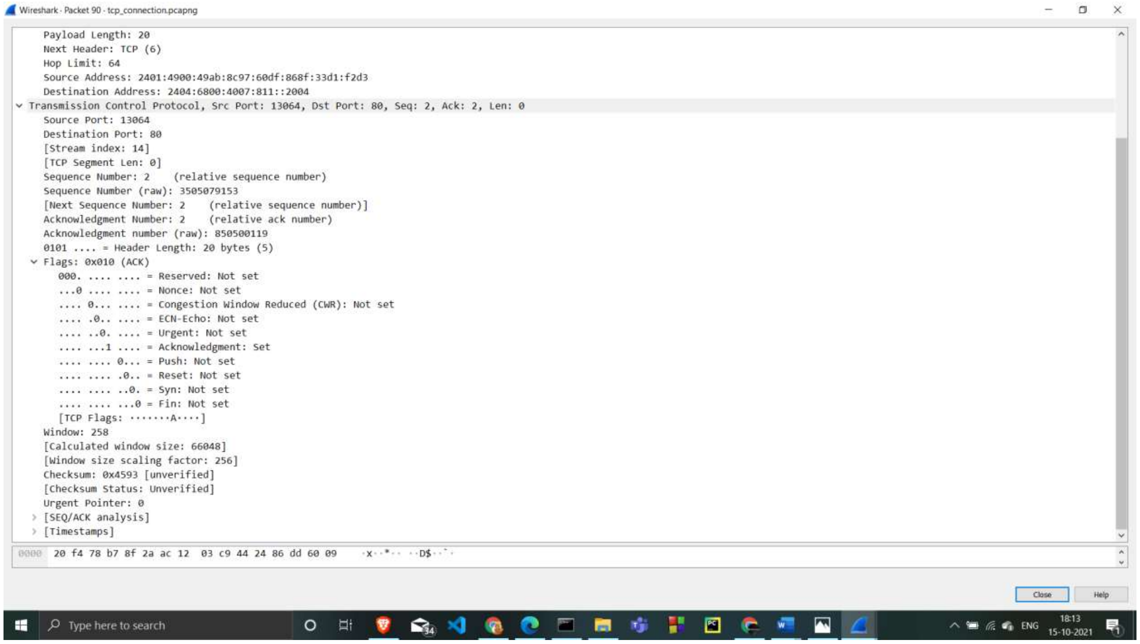
```
> Frame 90: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{F1048173-4B53-42B3-9262-AF5A818A4DF3}, id 0
v Ethernet II, Src: IntelCor_c9:44:24 (ac:12:03:c9:44:24), Dst: XiaomiCo_b7:8f:2a (20:f4:78:b7:8f:2a)
  > Destination: XiaomiCo_b7:8f:2a (20:f4:78:b7:8f:2a)
  > Source: IntelCor_c9:44:24 (ac:12:03:c9:44:24)
    Type: IPv6 (0x86dd)
v Internet Protocol Version 6, Src: 2401:4900:49ab:8c97:60df:868f:33d1:f2d3, Dst: 2404:6800:4007:811::2004
    0110 .... = Version: 6
  > .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... .... .... 1001 0001 1011 0010 0000 = Flow Label: 0x91b20
    Payload Length: 20
    Next Header: TCP (6)
    Hop Limit: 64
    Source Address: 2401:4900:49ab:8c97:60df:868f:33d1:f2d3
    Destination Address: 2404:6800:4007:811::2004
v Transmission Control Protocol, Src Port: 13064, Dst Port: 80, Seq: 2, Ack: 2, Len: 0
    Source Port: 13064
    Destination Port: 80
    [Stream index: 14]
    [TCP Segment Len: 0]
    Sequence Number: 2    (relative sequence number)
    Sequence Number (raw): 3505079153
    [Next Sequence Number: 2    (relative sequence number)]
    Acknowledgment Number: 2    (relative ack number)
    Acknowledgment number (raw): 850500119
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x010 (ACK)
    Window: 258
    [Calculated window size: 66048]
    [Window size scaling factor: 256]
    Checksum: 0x4593 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > [SEQ/ACK analysis]
  > [Timestamps]

0000  20 f4 78 b7 8f 2a ac 12  03 c9 44 24 86 dd 60 09    ·x··*·· ··D$··`·
```

the Source port is the same dynamic port selected for this connection.

Destination port is http (80).

Sequence number is 2, Acknowledgement number is 2

Expand Flags to view flag details.



```
    Payload Length: 20
    Next Header: TCP (6)
    Hop Limit: 64
    Source Address: 2401:4900:49ab:8c97:60df:868f:33d1:f2d3
    Destination Address: 2404:6800:4007:811::2004
v Transmission Control Protocol, Src Port: 13064, Dst Port: 80, Seq: 2, Ack: 2, Len: 0
    Source Port: 13064
    Destination Port: 80
    [Stream index: 14]
    [TCP Segment Len: 0]
    Sequence Number: 2    (relative sequence number)
    Sequence Number (raw): 3505079153
    [Next Sequence Number: 2    (relative sequence number)]
    Acknowledgment Number: 2    (relative ack number)
    Acknowledgment number (raw): 850500119
    0101 .... = Header Length: 20 bytes (5)
  v Flags: 0x010 (ACK)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Nonce: Not set
      .... 0... .... = Congestion Window Reduced (CWR): Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...1 .... = Acknowledgment: Set
      .... .... 0... = Push: Not set
      .... .... .0.. = Reset: Not set
      .... .... ..0. = Syn: Not set
      .... .... ...0 = Fin: Not set
      [TCP Flags: ·······A····]
    Window: 258
    [Calculated window size: 66048]
    [Window size scaling factor: 256]
    Checksum: 0x4593 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > [SEQ/ACK analysis]
  > [Timestamps]
0000  20 f4 78 b7 8f 2a ac 12  03 c9 44 24 86 dd 60 09    ·x··*··· ··D$··`·
```

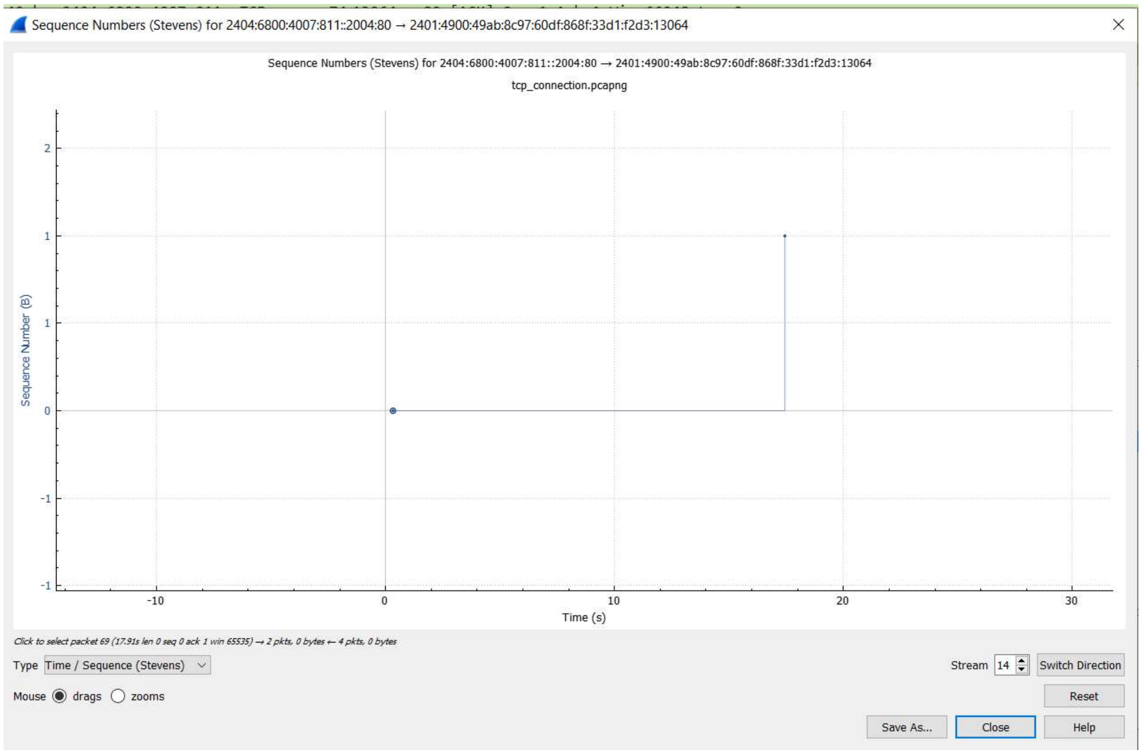
ACK is set

indicating the third segment in the TCP teardown handshake

The client has acknowledged the server closing the TCP connection

b. Identify if there are any retransmitted segments

There are no retransmitted segments . We can verify this by checking the sequence numbers of the TCP segments in the trace file. In the Time-Sequence-Graph (Stevens) of this trace, all sequence numbers from the source to the destination are increasing monotonically with respect to time. If there is a retransmitted segment, the sequence number of this retransmitted segment should be smaller than those of its neighbours segments



Sequence Numbers (Stevens) for 2404:6800:4007:811::2004:80 → 2401:4900:49ab:8c97:60df:868f:33d1:f2d3:13064

Sequence Numbers (Stevens) for 2404:6800:4007:811::2004:80 → 2401:4900:49ab:8c97:60df:868f:33d1:f2d3:13064

tcp_connection.pcapng

Click to select packet 69 (17.91s len 0 seq 0 ack 1 win 65535) → 2 pkts, 0 bytes ← 4 pkts, 0 bytes

Type: Time / Sequence (Stevens)

Mouse ● drags ○ zooms

Stream 14