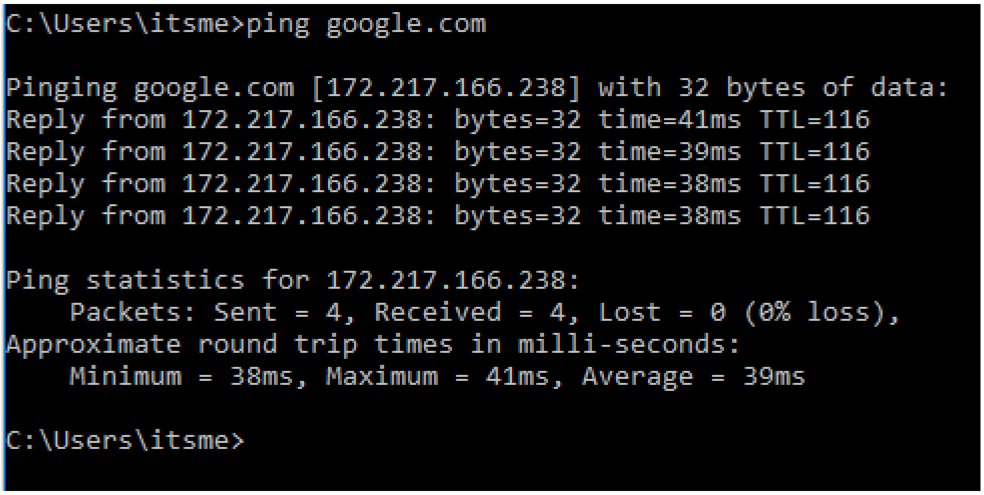
WireShark

A. ICMP

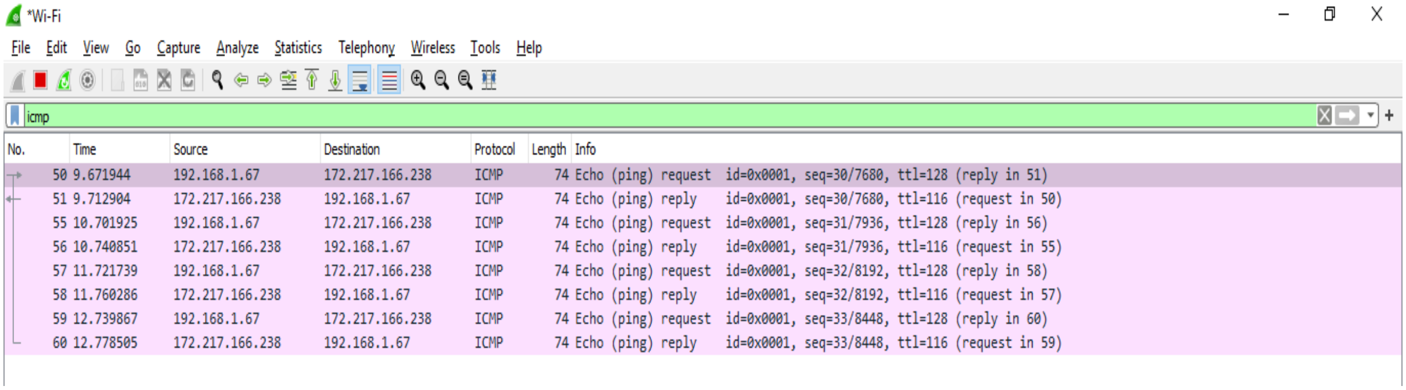
Command: ping



```
C:\Users\itsme>ping google.com

Pinging google.com [172.217.166.238] with 32 bytes of data:
Reply from 172.217.166.238: bytes=32 time=41ms TTL=116
Reply from 172.217.166.238: bytes=32 time=39ms TTL=116
Reply from 172.217.166.238: bytes=32 time=38ms TTL=116
Reply from 172.217.166.238: bytes=32 time=38ms TTL=116

Ping statistics for 172.217.166.238:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 38ms, Maximum = 41ms, Average = 39ms

C:\Users\itsme>
```

Packet Sniffed by Wireshark:

As the result of ping command, 4 packets were sent and all 4 were received. Same is captured by Wireshark as below.

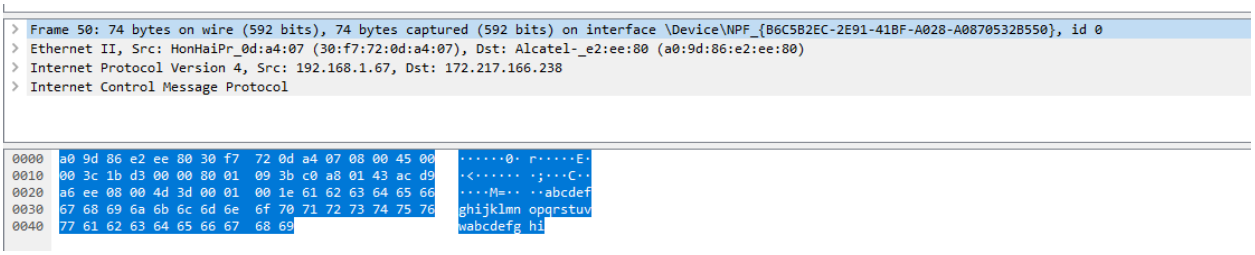

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

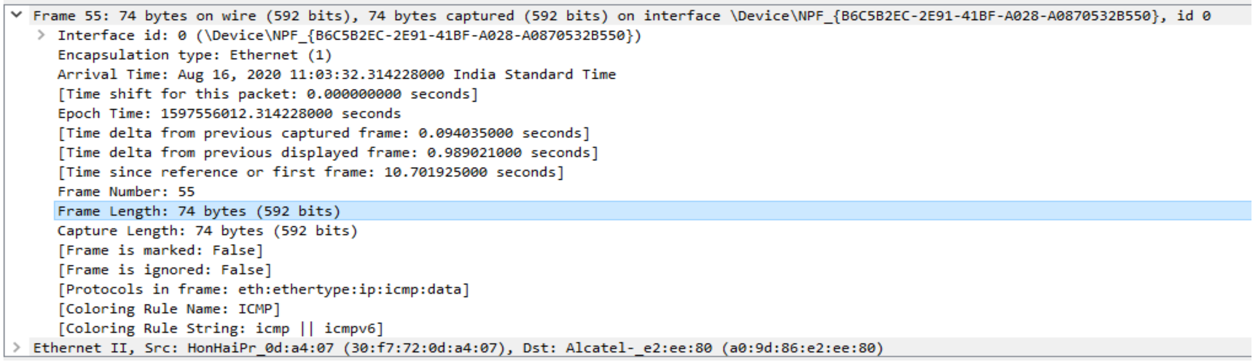
No.	Time	Source	Destination	Protocol	Length	Info
50	9.671944	192.168.1.67	172.217.166.238	ICMP	74	Echo (ping) request id=0x0001, seq=30/7680, ttl=128 (reply in 51)
51	9.712904	172.217.166.238	192.168.1.67	ICMP	74	Echo (ping) reply id=0x0001, seq=30/7680, ttl=116 (request in 50)
55	10.701925	192.168.1.67	172.217.166.238	ICMP	74	Echo (ping) request id=0x0001, seq=31/7936, ttl=128 (reply in 56)
56	10.740851	172.217.166.238	192.168.1.67	ICMP	74	Echo (ping) reply id=0x0001, seq=31/7936, ttl=116 (request in 55)
57	11.721739	192.168.1.67	172.217.166.238	ICMP	74	Echo (ping) request id=0x0001, seq=32/8192, ttl=128 (reply in 58)
58	11.760286	172.217.166.238	192.168.1.67	ICMP	74	Echo (ping) reply id=0x0001, seq=32/8192, ttl=116 (request in 57)
59	12.739867	192.168.1.67	172.217.166.238	ICMP	74	Echo (ping) request id=0x0001, seq=33/8448, ttl=128 (reply in 60)
60	12.778505	172.217.166.238	192.168.1.67	ICMP	74	Echo (ping) reply id=0x0001, seq=33/8448, ttl=116 (request in 59)

Explanation

- The Packet is of 74 bytes (592 bits) with all the details shown below.



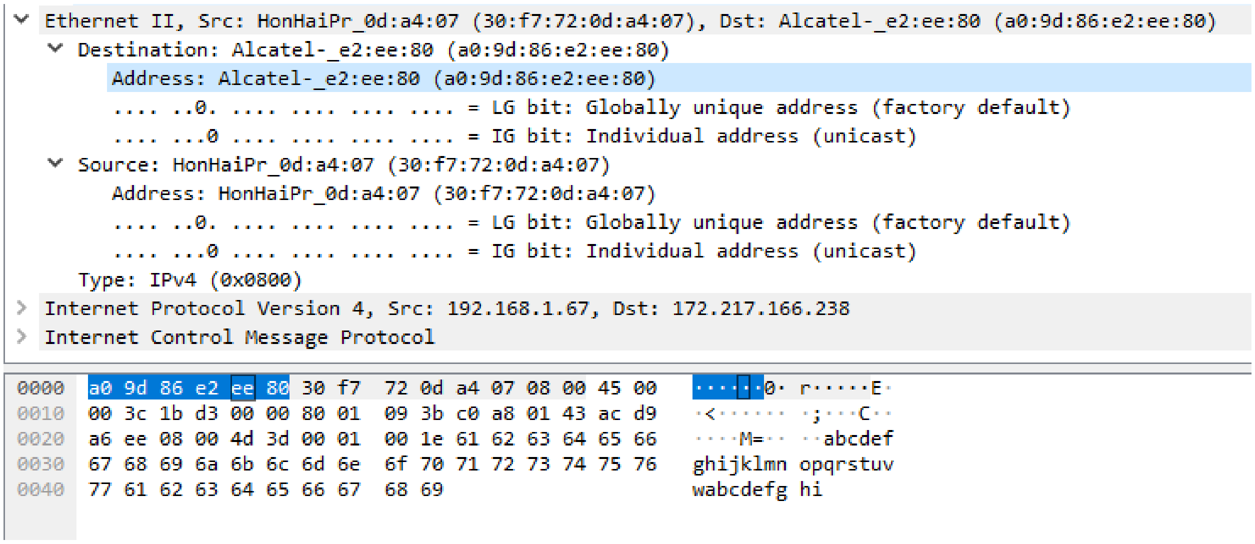
```
> Frame 50: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{B6C5B2EC-2E91-41BF-A028-A0870532B550}, id 0
> Ethernet II, Src: HonHaiPr_0d:a4:07 (30:f7:72:0d:a4:07), Dst: Alcatel-_e2:ee:80 (a0:9d:86:e2:ee:80)
> Internet Protocol Version 4, Src: 192.168.1.67, Dst: 172.217.166.238
> Internet Control Message Protocol

0000  a0 9d 86 e2 ee 80 30 f7  72 0d a4 07 08 00 45 00   ······0· r·····E·
0010  00 3c 1b d3 00 00 80 01  09 3b c0 a8 01 43 ac d9   ·<······ ·;···C··
0020  a6 ee 08 00 4d 3d 00 01  00 1e 61 62 63 64 65 66   ····M=·· ··abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```



```
v Frame 55: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{B6C5B2EC-2E91-41BF-A028-A0870532B550}, id 0
  > Interface id: 0 (\Device\NPF_{B6C5B2EC-2E91-41BF-A028-A0870532B550})
    Encapsulation type: Ethernet (1)
    Arrival Time: Aug 16, 2020 11:03:32.314228000 India Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1597556012.314228000 seconds
    [Time delta from previous captured frame: 0.094035000 seconds]
    [Time delta from previous displayed frame: 0.989021000 seconds]
    [Time since reference or first frame: 10.701925000 seconds]
    Frame Number: 55
    Frame Length: 74 bytes (592 bits)
    Capture Length: 74 bytes (592 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:icmp:data]
    [Coloring Rule Name: ICMP]
    [Coloring Rule String: icmp || icmpv6]
> Ethernet II, Src: HonHaiPr_0d:a4:07 (30:f7:72:0d:a4:07), Dst: Alcatel-_e2:ee:80 (a0:9d:86:e2:ee:80)
```

This all information includes Interface id, interface type, Arrival time, frame number, flame length, captured frame length, protocol that frame is being running on and a bunch of other details.

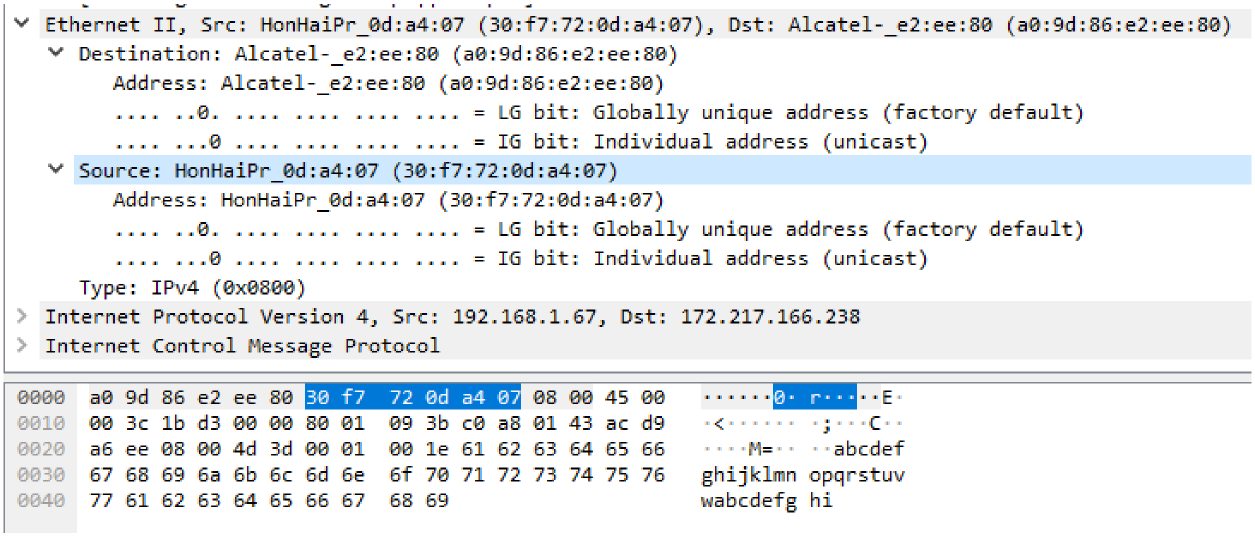
- It shows the physical addresses associated with the frame.



```
v Ethernet II, Src: HonHaiPr_0d:a4:07 (30:f7:72:0d:a4:07), Dst: Alcatel-_e2:ee:80 (a0:9d:86:e2:ee:80)
  v Destination: Alcatel-_e2:ee:80 (a0:9d:86:e2:ee:80)
      Address: Alcatel-_e2:ee:80 (a0:9d:86:e2:ee:80)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  v Source: HonHaiPr_0d:a4:07 (30:f7:72:0d:a4:07)
      Address: HonHaiPr_0d:a4:07 (30:f7:72:0d:a4:07)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 192.168.1.67, Dst: 172.217.166.238
> Internet Control Message Protocol

0000  a0 9d 86 e2 ee 80 30 f7  72 0d a4 07 08 00 45 00   ······0· r·····E·
0010  00 3c 1b d3 00 00 80 01  09 3b c0 a8 01 43 ac d9   ·<······ ·;···C··
0020  a6 ee 08 00 4d 3d 00 01  00 1e 61 62 63 64 65 66   ····M=·· ··abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```

The highlighted part shows the destination MAC address/Physical address, which is, a0:9d:86:e2:ee:80

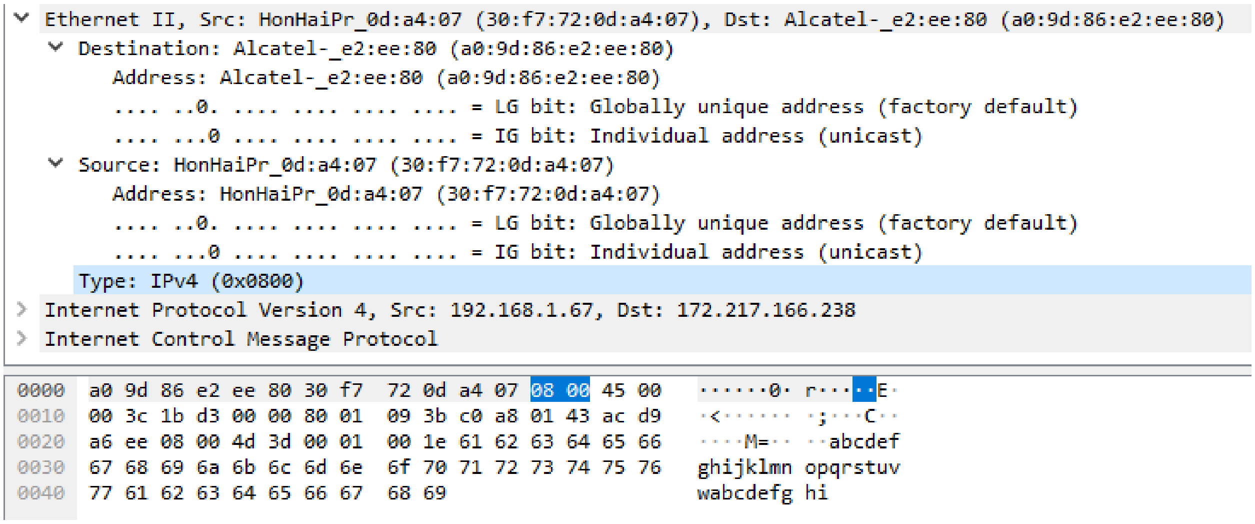
MAC address, as shown, is of 48 bits in hexadecimal format. First 24 bits describes the OEM (Original Equipment Manufacturer) and the rest of the bits describes unique ID, which is different for each machine, as it shows the individuals NIC (Network Interface Card). As I pinged google.com, it looks like the destination MAC address should be of the google.com host, but that’s not the case, it’s the MAC address of the router, the end point of my network. No-one can get the MAC address of any device connected outside the personal network.



```
v Ethernet II, Src: HonHaiPr_0d:a4:07 (30:f7:72:0d:a4:07), Dst: Alcatel-_e2:ee:80 (a0:9d:86:e2:ee:80)
   v Destination: Alcatel-_e2:ee:80 (a0:9d:86:e2:ee:80)
        Address: Alcatel-_e2:ee:80 (a0:9d:86:e2:ee:80)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
   v Source: HonHaiPr_0d:a4:07 (30:f7:72:0d:a4:07)
        Address: HonHaiPr_0d:a4:07 (30:f7:72:0d:a4:07)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
     Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 192.168.1.67, Dst: 172.217.166.238
> Internet Control Message Protocol

0000  a0 9d 86 e2 ee 80 30 f7  72 0d a4 07 08 00 45 00   ······0· r·····E·
0010  00 3c 1b d3 00 00 80 01  09 3b c0 a8 01 43 ac d9   ·<······ ·;···C··
0020  a6 ee 08 00 4d 3d 00 01  00 1e 61 62 63 64 65 66   ····M=·· ··abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```

The highlighted part shows the destination MAC address/Physical address, which is, 30:f7:72:0d:a4:07

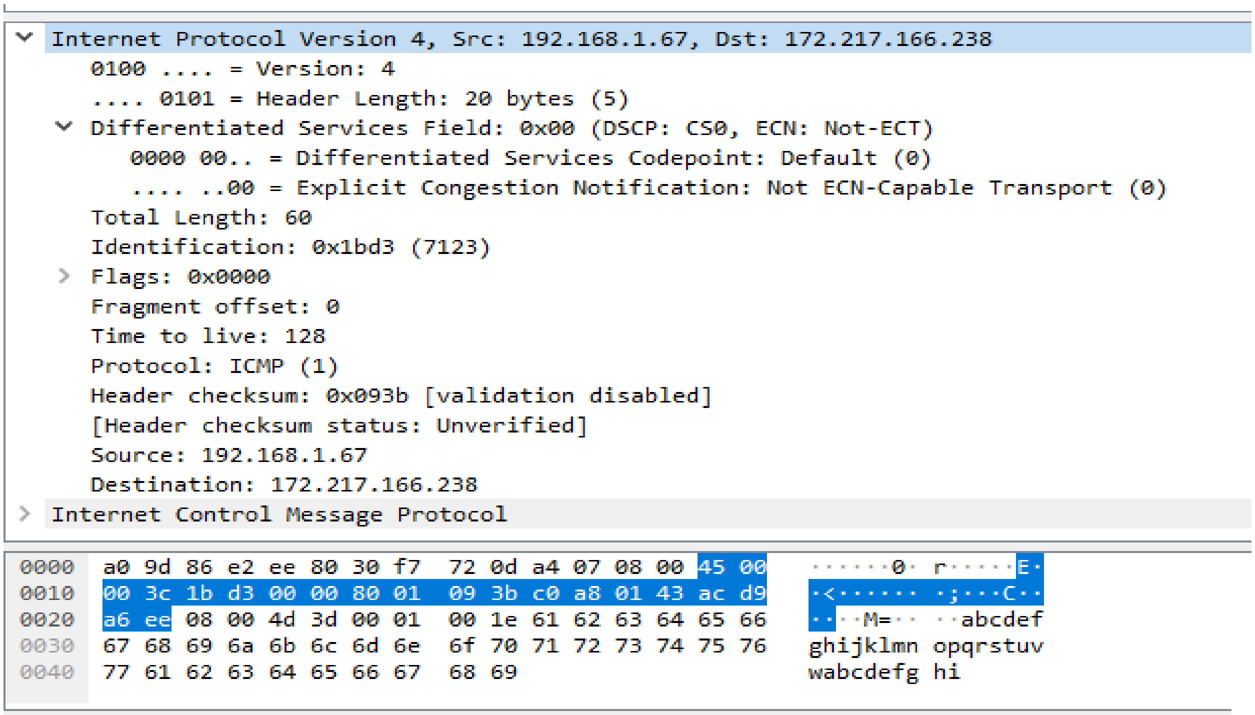
It’s the MAC address of my device on which I pinged google.com.



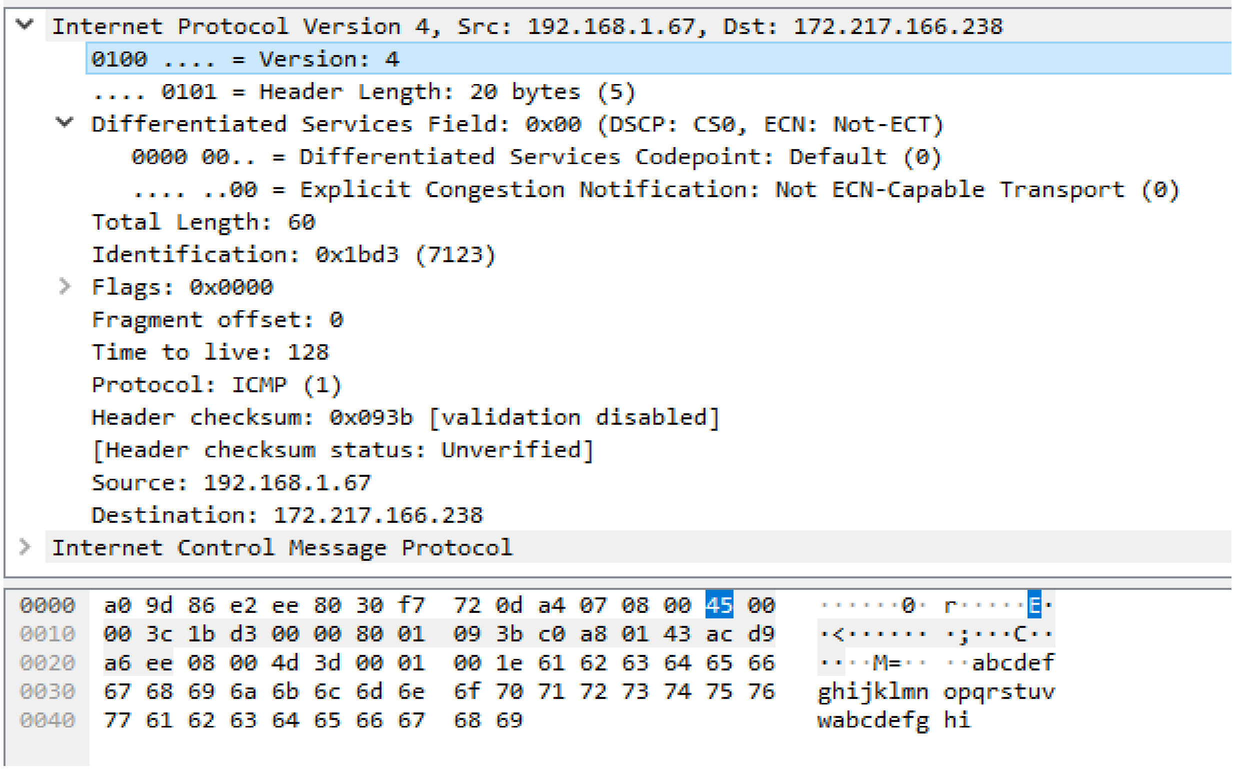
```
v Ethernet II, Src: HonHaiPr_0d:a4:07 (30:f7:72:0d:a4:07), Dst: Alcatel-_e2:ee:80 (a0:9d:86:e2:ee:80)
   v Destination: Alcatel-_e2:ee:80 (a0:9d:86:e2:ee:80)
        Address: Alcatel-_e2:ee:80 (a0:9d:86:e2:ee:80)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
   v Source: HonHaiPr_0d:a4:07 (30:f7:72:0d:a4:07)
        Address: HonHaiPr_0d:a4:07 (30:f7:72:0d:a4:07)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
     Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 192.168.1.67, Dst: 172.217.166.238
> Internet Control Message Protocol

0000  a0 9d 86 e2 ee 80 30 f7  72 0d a4 07 08 00 45 00   ······0· r·····E·
0010  00 3c 1b d3 00 00 80 01  09 3b c0 a8 01 43 ac d9   ·<······ ·;···C··
0020  a6 ee 08 00 4d 3d 00 01  00 1e 61 62 63 64 65 66   ····M=·· ··abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```

These 4 bits (0800) in hexadecimal format (0x0800) which tells the destination device that the IP format of the packet that is being transferred from physical layer to network layer is of Version 4 (IPv4).

- Now the Packet is in Network Layer. This shows first destination IP address and then Source IP address.



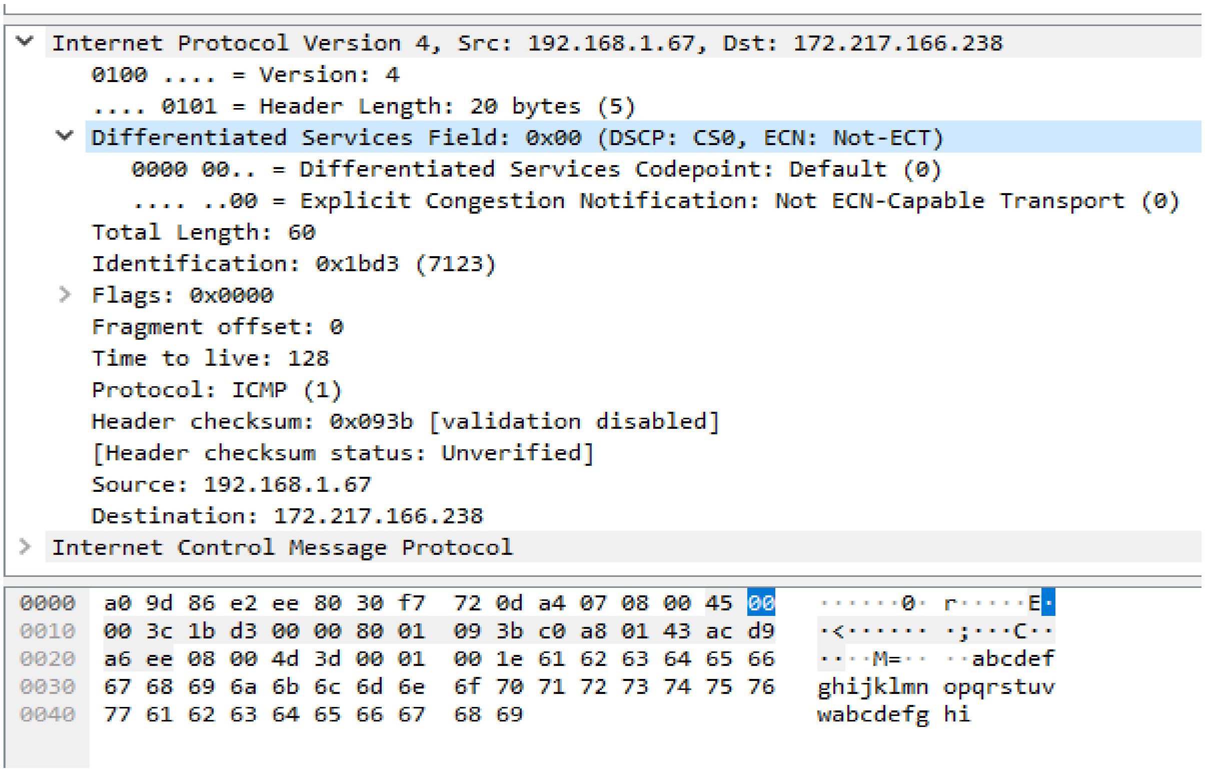
```
∨ Internet Protocol Version 4, Src: 192.168.1.67, Dst: 172.217.166.238
     0100 .... = Version: 4
     .... 0101 = Header Length: 20 bytes (5)
  ∨ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        0000 00.. = Differentiated Services Codepoint: Default (0)
        .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
     Total Length: 60
     Identification: 0x1bd3 (7123)
  > Flags: 0x0000
     Fragment offset: 0
     Time to live: 128
     Protocol: ICMP (1)
     Header checksum: 0x093b [validation disabled]
     [Header checksum status: Unverified]
     Source: 192.168.1.67
     Destination: 172.217.166.238
> Internet Control Message Protocol

0000  a0 9d 86 e2 ee 80 30 f7  72 0d a4 07 08 00 45 00   ······0· r·····E·
0010  00 3c 1b d3 00 00 80 01  09 3b c0 a8 01 43 ac d9   ·<······ ·;···C··
0020  a6 ee 08 00 4d 3d 00 01  00 1e 61 62 63 64 65 66   ····M=·· ··abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```



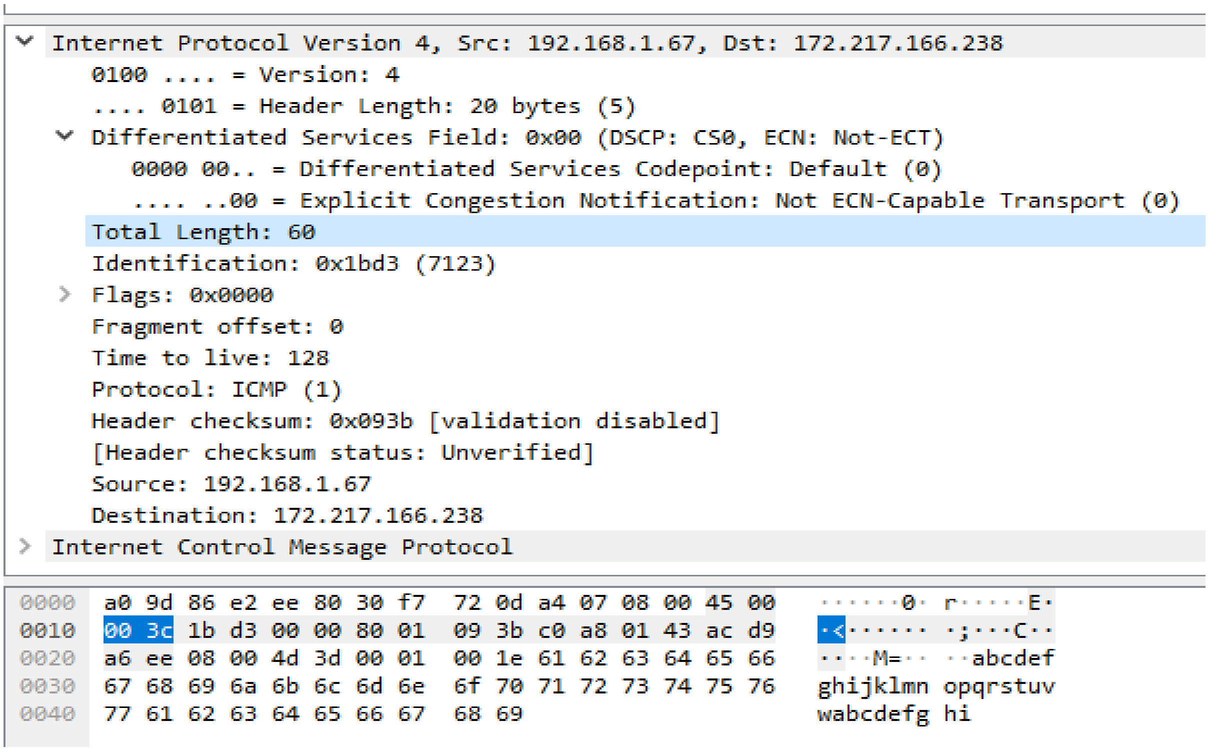
```
∨ Internet Protocol Version 4, Src: 192.168.1.67, Dst: 172.217.166.238
     0100 .... = Version: 4
     .... 0101 = Header Length: 20 bytes (5)
  ∨ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        0000 00.. = Differentiated Services Codepoint: Default (0)
        .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
     Total Length: 60
     Identification: 0x1bd3 (7123)
  > Flags: 0x0000
     Fragment offset: 0
     Time to live: 128
     Protocol: ICMP (1)
     Header checksum: 0x093b [validation disabled]
     [Header checksum status: Unverified]
     Source: 192.168.1.67
     Destination: 172.217.166.238
> Internet Control Message Protocol

0000  a0 9d 86 e2 ee 80 30 f7  72 0d a4 07 08 00 45 00   ······0· r·····E·
0010  00 3c 1b d3 00 00 80 01  09 3b c0 a8 01 43 ac d9   ·<······ ·;···C··
0020  a6 ee 08 00 4d 3d 00 01  00 1e 61 62 63 64 65 66   ····M=·· ··abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```

Out of First 8 bits, first four describes IP version, last four describes header length.

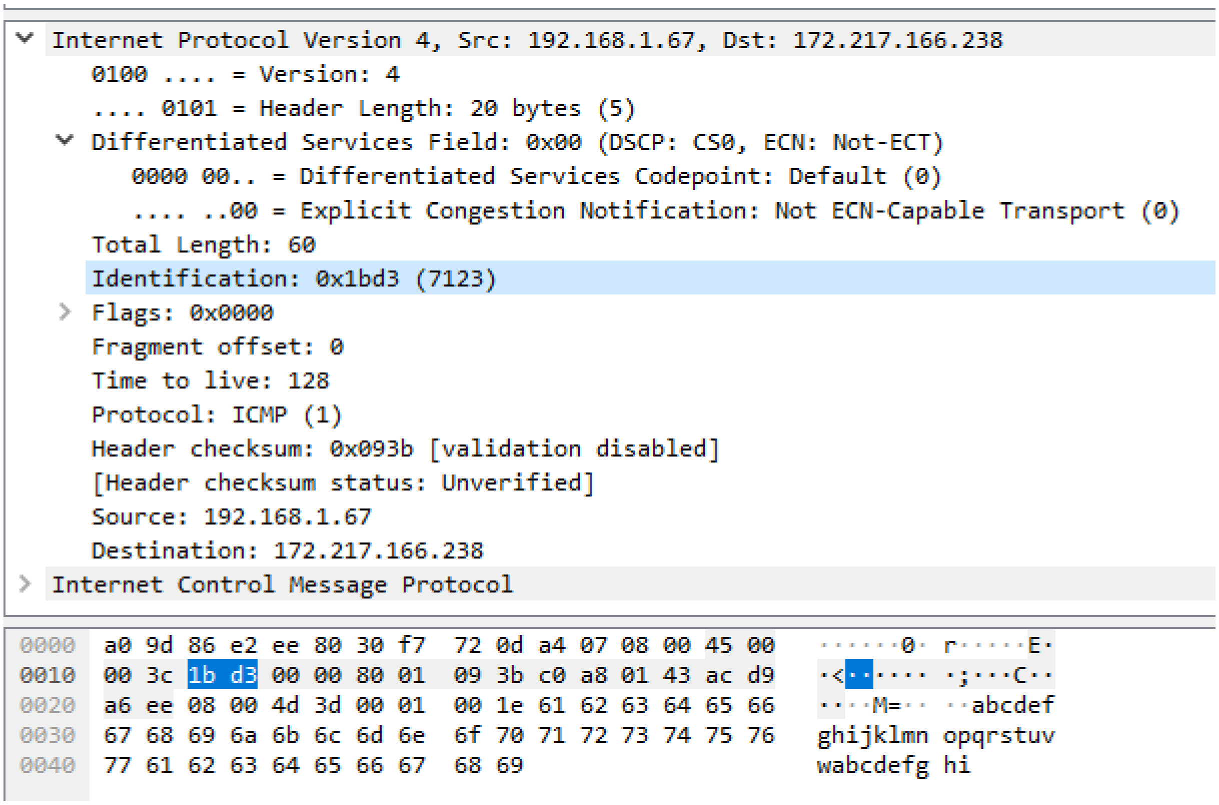
These are some other information regarding the packet.



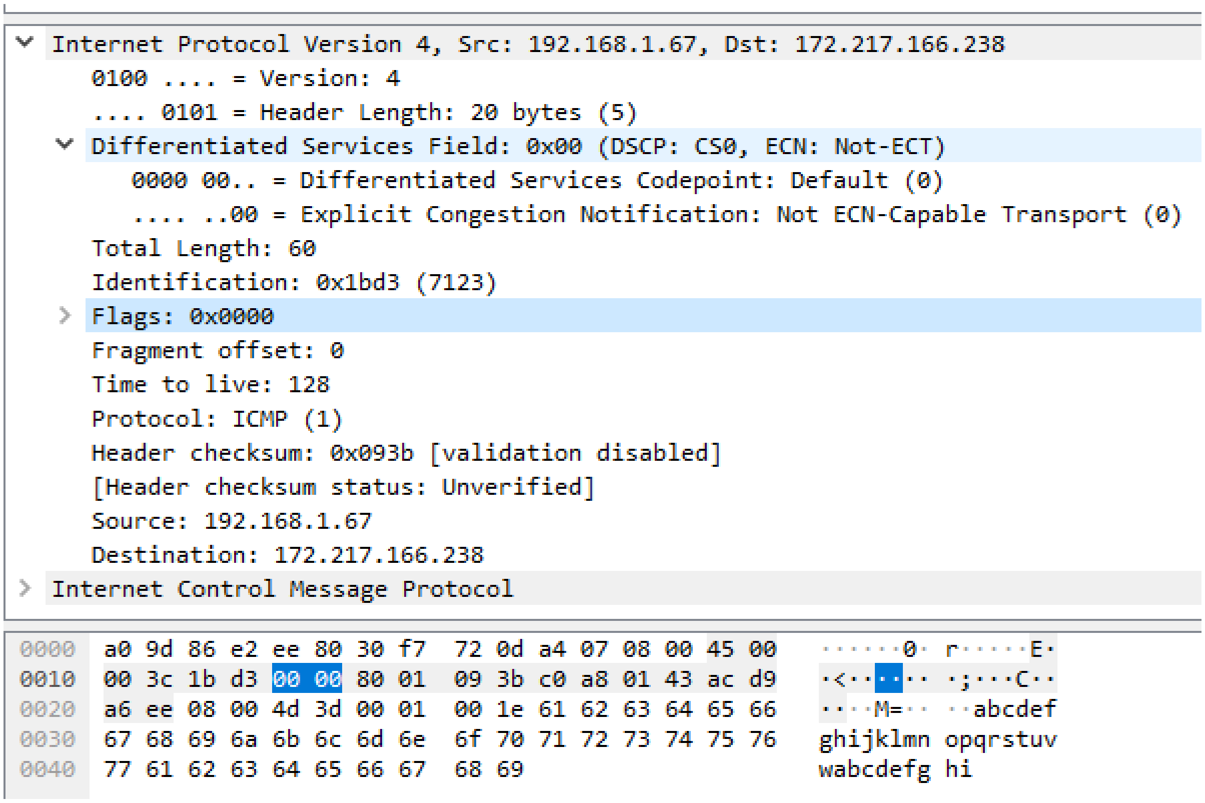
```
v Internet Protocol Version 4, Src: 192.168.1.67, Dst: 172.217.166.238
     0100 .... = Version: 4
     .... 0101 = Header Length: 20 bytes (5)
  v  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        0000 00.. = Differentiated Services Codepoint: Default (0)
        .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
     Total Length: 60
     Identification: 0x1bd3 (7123)
  >  Flags: 0x0000
     Fragment offset: 0
     Time to live: 128
     Protocol: ICMP (1)
     Header checksum: 0x093b [validation disabled]
     [Header checksum status: Unverified]
     Source: 192.168.1.67
     Destination: 172.217.166.238
> Internet Control Message Protocol

0000  a0 9d 86 e2 ee 80 30 f7  72 0d a4 07 08 00 45 00   ······0· r·····E·
0010  00 3c 1b d3 00 00 80 01  09 3b c0 a8 01 43 ac d9   ·<······ ·;···C··
0020  a6 ee 08 00 4d 3d 00 01  00 1e 61 62 63 64 65 66   ····M=·· ··abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```



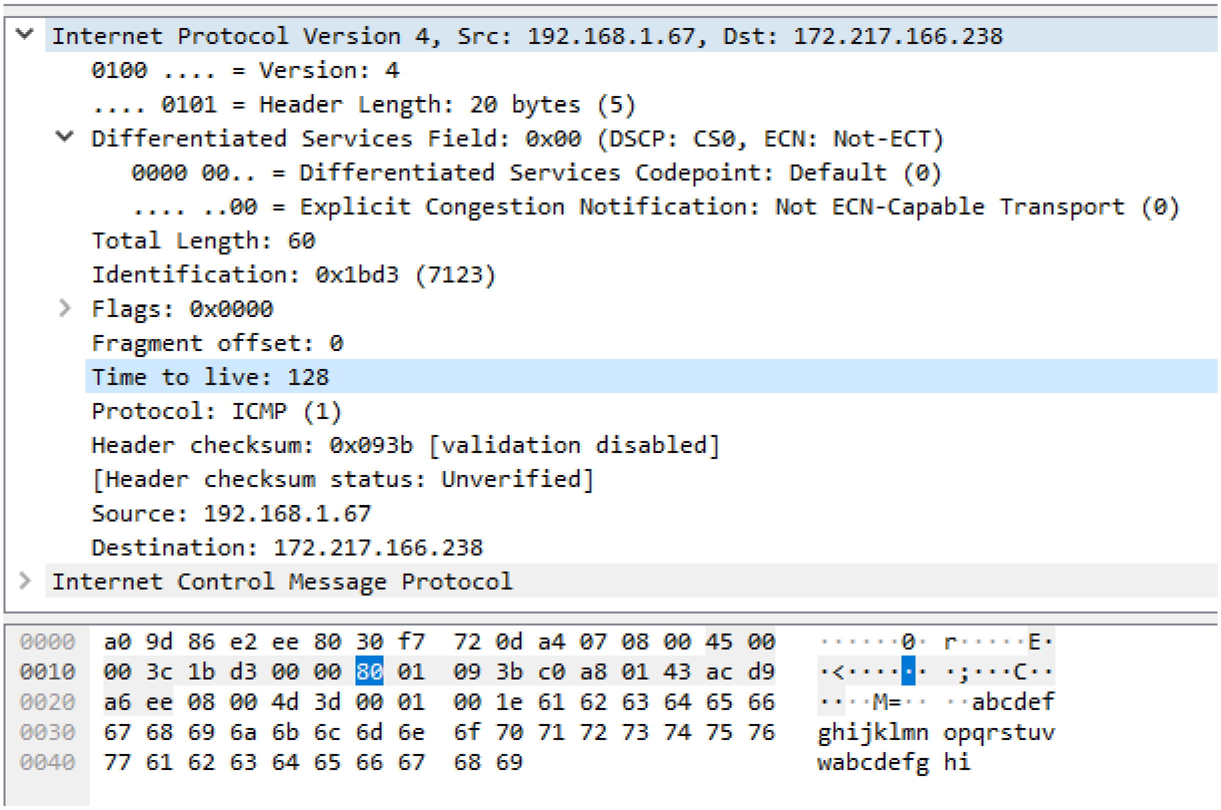
```
v Internet Protocol Version 4, Src: 192.168.1.67, Dst: 172.217.166.238
     0100 .... = Version: 4
     .... 0101 = Header Length: 20 bytes (5)
  v  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        0000 00.. = Differentiated Services Codepoint: Default (0)
        .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
     Total Length: 60
     Identification: 0x1bd3 (7123)
  >  Flags: 0x0000
     Fragment offset: 0
     Time to live: 128
     Protocol: ICMP (1)
     Header checksum: 0x093b [validation disabled]
     [Header checksum status: Unverified]
     Source: 192.168.1.67
     Destination: 172.217.166.238
> Internet Control Message Protocol

0000  a0 9d 86 e2 ee 80 30 f7  72 0d a4 07 08 00 45 00   ······0· r·····E·
0010  00 3c 1b d3 00 00 80 01  09 3b c0 a8 01 43 ac d9   ·<······ ·;···C··
0020  a6 ee 08 00 4d 3d 00 01  00 1e 61 62 63 64 65 66   ····M=·· ··abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```



```
v Internet Protocol Version 4, Src: 192.168.1.67, Dst: 172.217.166.238
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  v 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: 60
    Identification: 0x1bd3 (7123)
  > Flags: 0x0000
    Fragment offset: 0
    Time to live: 128
    Protocol: ICMP (1)
    Header checksum: 0x093b [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.67
    Destination: 172.217.166.238
> Internet Control Message Protocol

0000  a0 9d 86 e2 ee 80 30 f7  72 0d a4 07 08 00 45 00   ······0· r·····E·
0010  00 3c 1b d3 00 00 80 01  09 3b c0 a8 01 43 ac d9   ·<······ ·;···C··
0020  a6 ee 08 00 4d 3d 00 01  00 1e 61 62 63 64 65 66   ····M=·· ··abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```

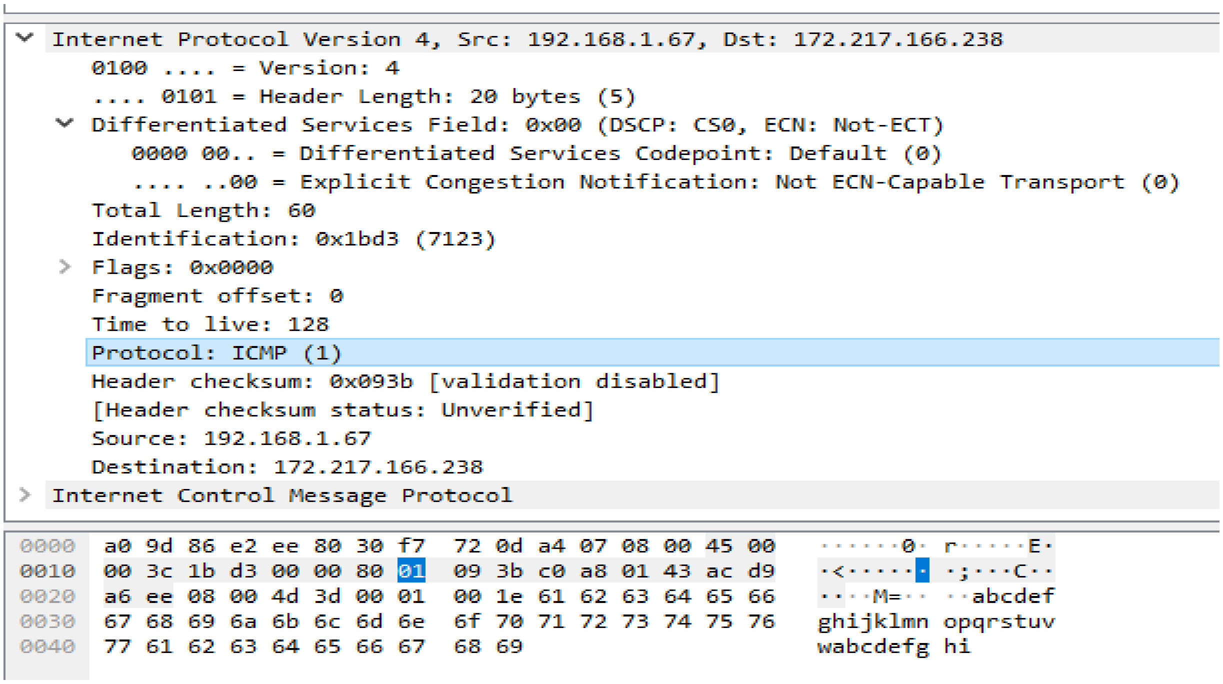


```
v Internet Protocol Version 4, Src: 192.168.1.67, Dst: 172.217.166.238
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  v Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 60
    Identification: 0x1bd3 (7123)
  > Flags: 0x0000
    Fragment offset: 0
    Time to live: 128
    Protocol: ICMP (1)
    Header checksum: 0x093b [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.67
    Destination: 172.217.166.238
> Internet Control Message Protocol

0000  a0 9d 86 e2 ee 80 30 f7  72 0d a4 07 08 00 45 00   ······0· r·····E·
0010  00 3c 1b d3 00 00 80 01  09 3b c0 a8 01 43 ac d9   ·<······ ·;···C··
0020  a6 ee 08 00 4d 3d 00 01  00 1e 61 62 63 64 65 66   ····M=·· ··abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```



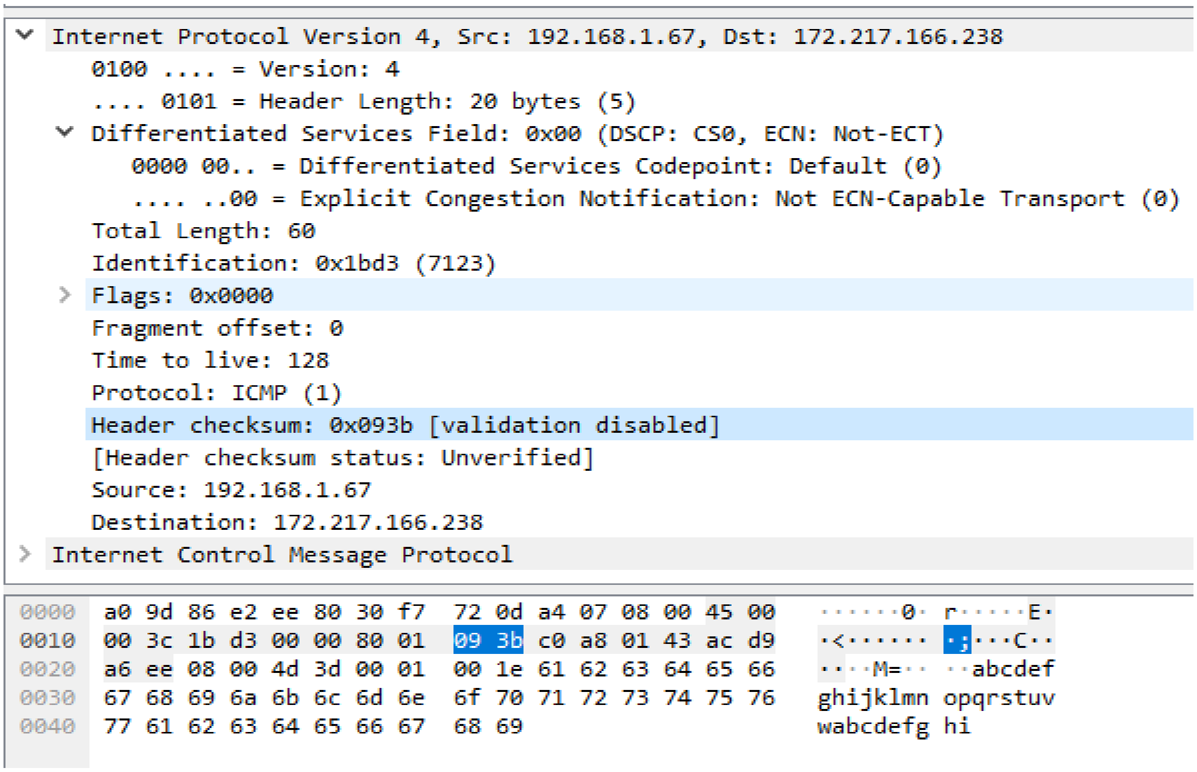
```
v Internet Protocol Version 4, Src: 192.168.1.67, Dst: 172.217.166.238
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  v Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 60
    Identification: 0x1bd3 (7123)
  > Flags: 0x0000
    Fragment offset: 0
    Time to live: 128
    Protocol: ICMP (1)
    Header checksum: 0x093b [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.67
    Destination: 172.217.166.238
> Internet Control Message Protocol

0000  a0 9d 86 e2 ee 80 30 f7  72 0d a4 07 08 00 45 00   ······0· r·····E·
0010  00 3c 1b d3 00 00 80 01  09 3b c0 a8 01 43 ac d9   ·<······ ·;···C··
0020  a6 ee 08 00 4d 3d 00 01  00 1e 61 62 63 64 65 66   ····M=·· ··abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```

Time to live is not actually time upto expiry, it’s the number of hops frame/packet covers to reach destination.



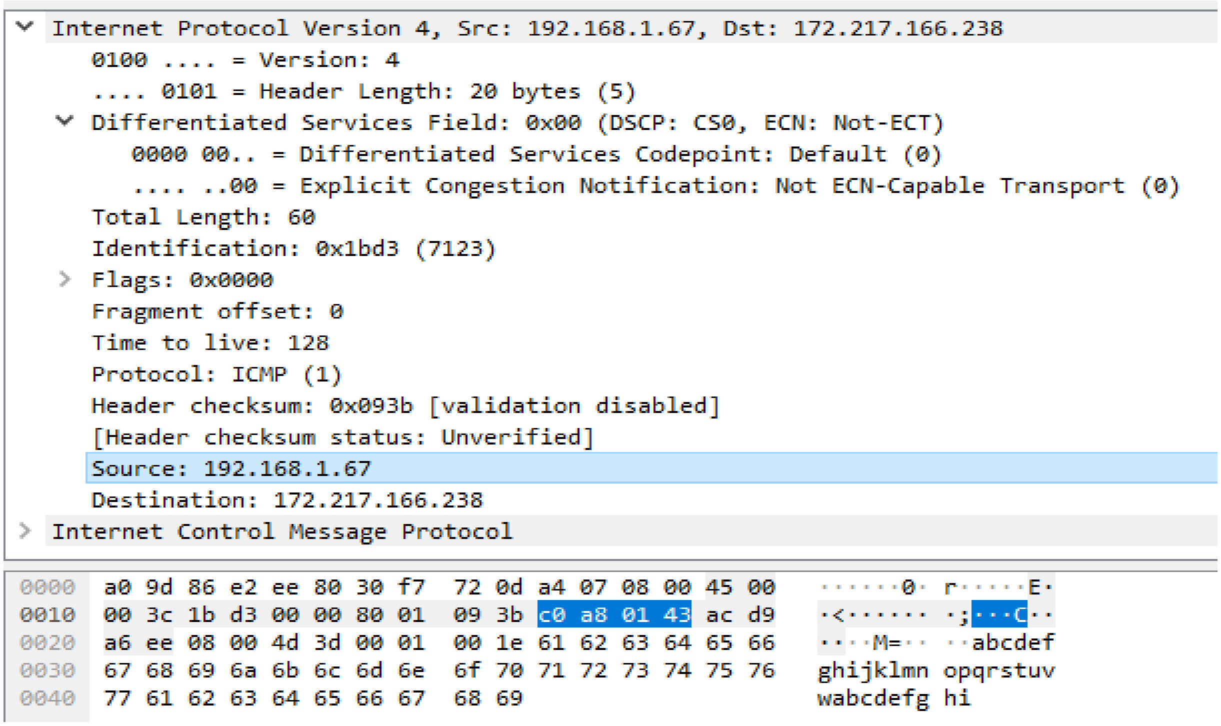
```
v Internet Protocol Version 4, Src: 192.168.1.67, Dst: 172.217.166.238
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  v Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 60
    Identification: 0x1bd3 (7123)
  > Flags: 0x0000
    Fragment offset: 0
    Time to live: 128
    Protocol: ICMP (1)
    Header checksum: 0x093b [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.67
    Destination: 172.217.166.238
> Internet Control Message Protocol

0000  a0 9d 86 e2 ee 80 30 f7  72 0d a4 07 08 00 45 00   ······0· r·····E·
0010  00 3c 1b d3 00 00 80 01  09 3b c0 a8 01 43 ac d9   ·<······ ·;···C··
0020  a6 ee 08 00 4d 3d 00 01  00 1e 61 62 63 64 65 66   ····M=·· ··abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```

The protocol regarding/ followed by frame, i.e, ICMP, here.



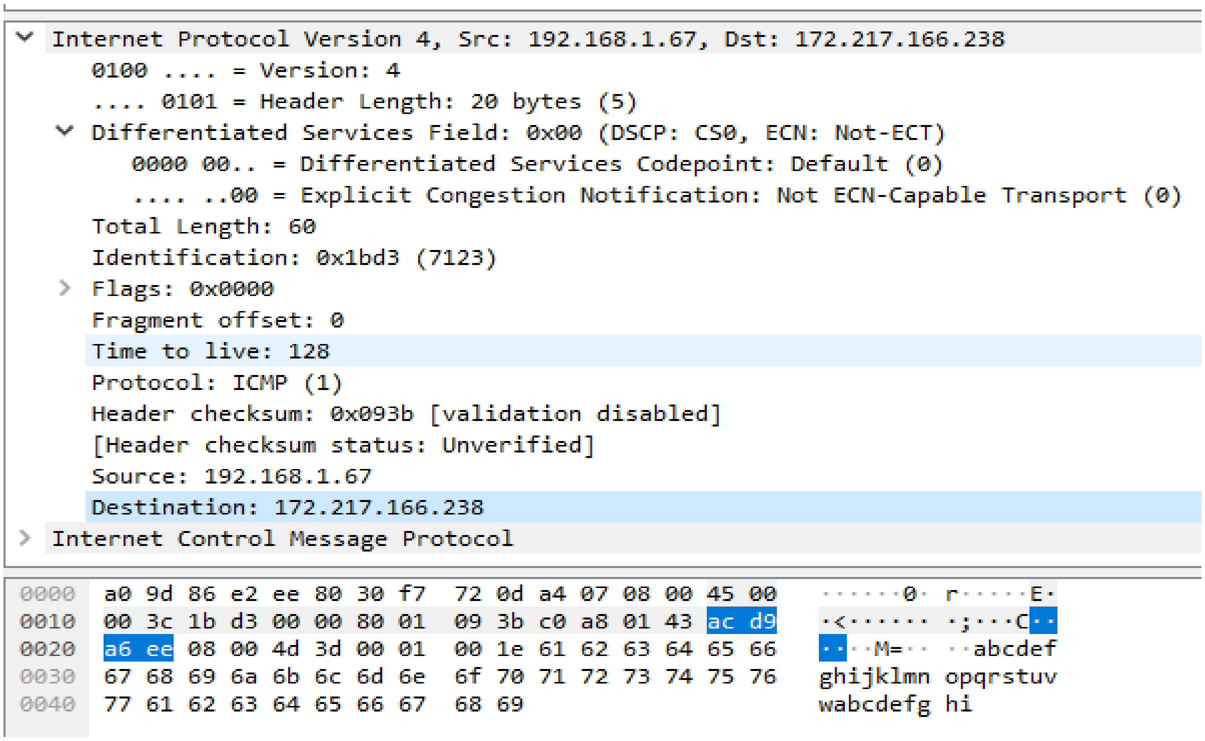
```
Internet Protocol Version 4, Src: 192.168.1.67, Dst: 172.217.166.238
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        0000 00.. = Differentiated Services Codepoint: Default (0)
        .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 60
    Identification: 0x1bd3 (7123)
  > Flags: 0x0000
    Fragment offset: 0
    Time to live: 128
    Protocol: ICMP (1)
    Header checksum: 0x093b [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.67
    Destination: 172.217.166.238
> Internet Control Message Protocol

0000  a0 9d 86 e2 ee 80 30 f7  72 0d a4 07 08 00 45 00   ······0· r·····E·
0010  00 3c 1b d3 00 00 80 01  09 3b c0 a8 01 43 ac d9   ·<······ ·;···C··
0020  a6 ee 08 00 4d 3d 00 01  00 1e 61 62 63 64 65 66   ····M=·· ··abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```

Header Checksum is a method to determine the frame is not corrupted or damaged.



```
Internet Protocol Version 4, Src: 192.168.1.67, Dst: 172.217.166.238
    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: 60
    Identification: 0x1bd3 (7123)
  > Flags: 0x0000
    Fragment offset: 0
    Time to live: 128
    Protocol: ICMP (1)
    Header checksum: 0x093b [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.67
    Destination: 172.217.166.238
> Internet Control Message Protocol

0000  a0 9d 86 e2 ee 80 30 f7  72 0d a4 07 08 00 45 00   ······0· r·····E·
0010  00 3c 1b d3 00 00 80 01  09 3b c0 a8 01 43 ac d9   ·<······ ·;···C··
0020  a6 ee 08 00 4d 3d 00 01  00 1e 61 62 63 64 65 66   ····M=·· ··abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```

Source: Source IP address, from whick the request was sent.

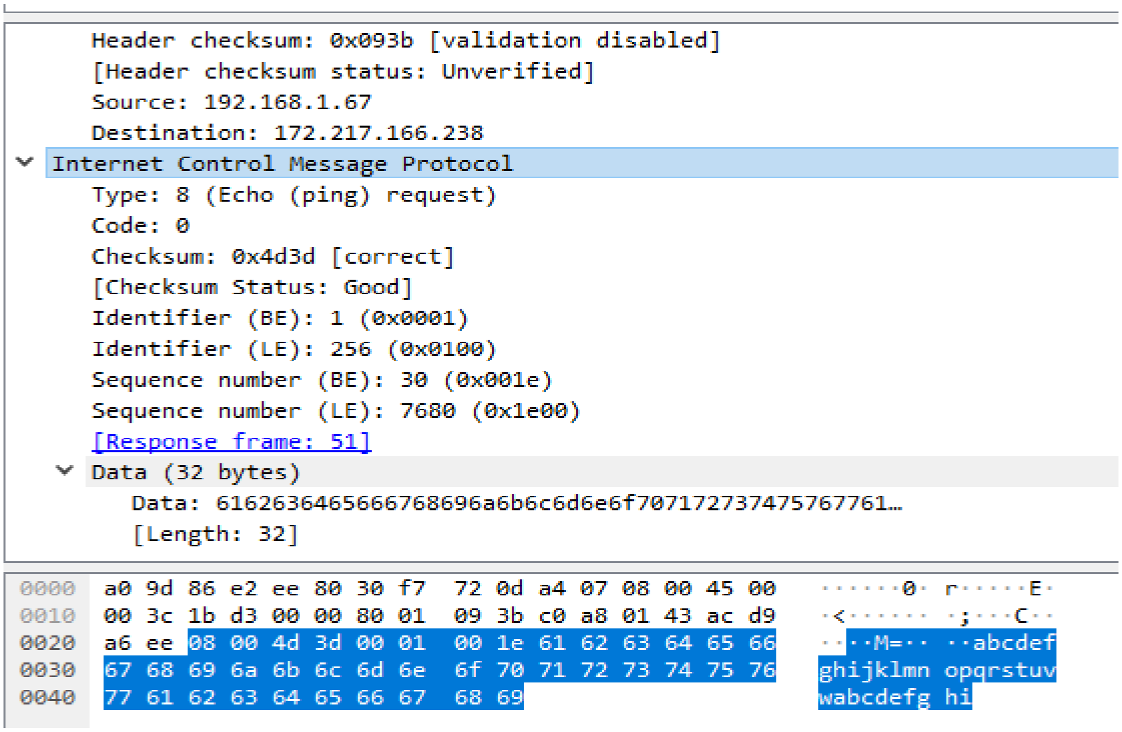


```
˅ Internet Protocol Version 4, Src: 192.168.1.67, Dst: 172.217.166.238
     0100 .... = Version: 4
     .... 0101 = Header Length: 20 bytes (5)
  ˅ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        0000 00.. = Differentiated Services Codepoint: Default (0)
        .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
     Total Length: 60
     Identification: 0x1bd3 (7123)
  > Flags: 0x0000
     Fragment offset: 0
     Time to live: 128
     Protocol: ICMP (1)
     Header checksum: 0x093b [validation disabled]
     [Header checksum status: Unverified]
     Source: 192.168.1.67
     Destination: 172.217.166.238
> Internet Control Message Protocol
```

```
0000  a0 9d 86 e2 ee 80 30 f7  72 0d a4 07 08 00 45 00   ······0· r·····E·
0010  00 3c 1b d3 00 00 80 01  09 3b c0 a8 01 43 ac d9   ·<······ ·;···C··
0020  a6 ee 08 00 4d 3d 00 01  00 1e 61 62 63 64 65 66   ····M=·· ··abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```

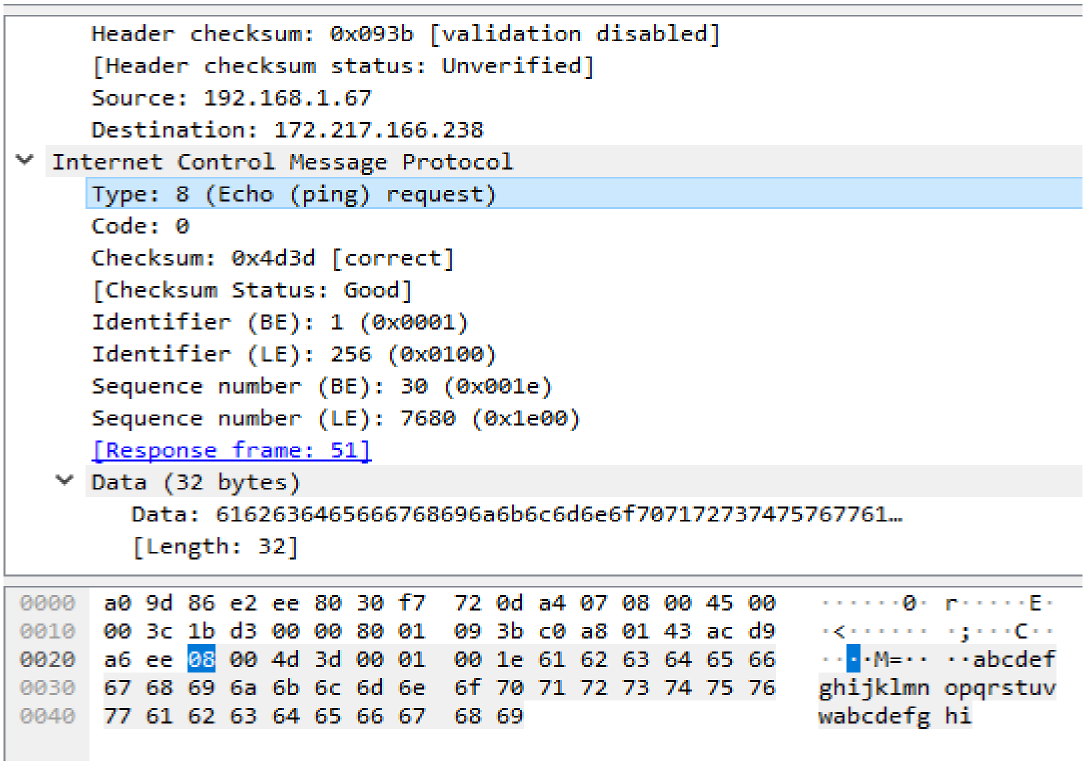
Destination: Destination IP address, Ip address of the host device where google.com is being hosted.

- It contains all the information regarding the protocol on which frame is being travelled.

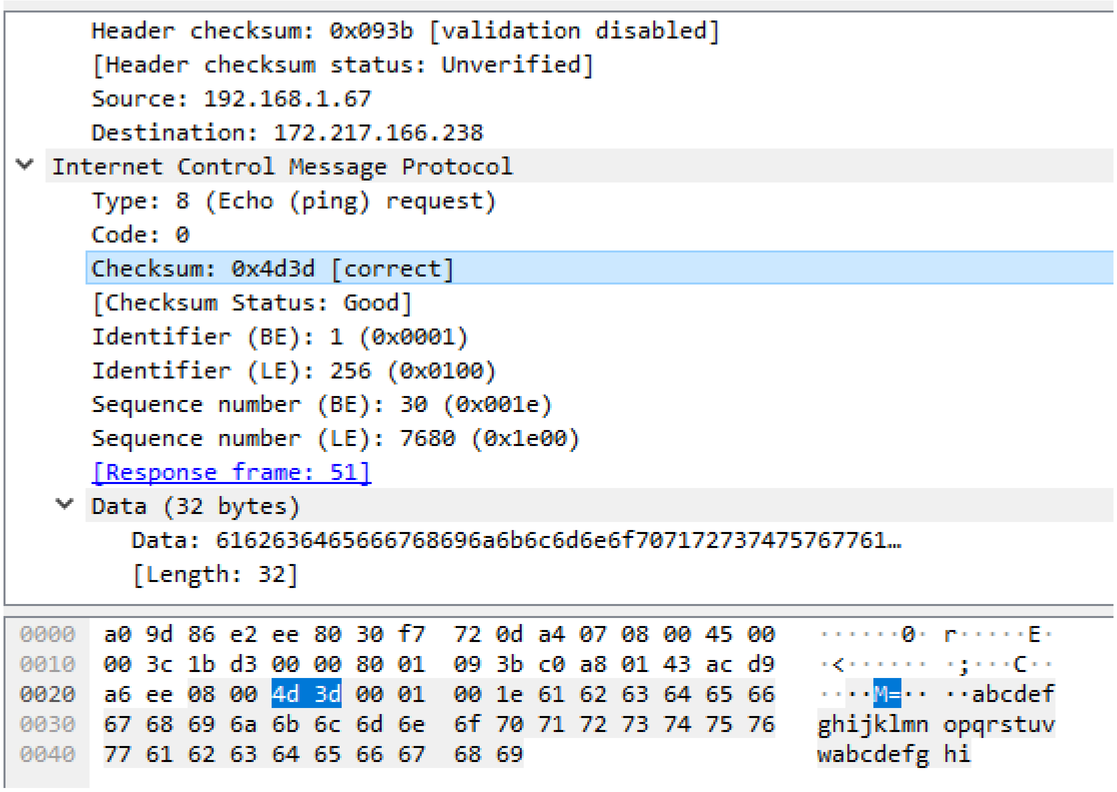


```
     Header checksum: 0x093b [validation disabled]
     [Header checksum status: Unverified]
     Source: 192.168.1.67
     Destination: 172.217.166.238
˅ Internet Control Message Protocol
     Type: 8 (Echo (ping) request)
     Code: 0
     Checksum: 0x4d3d [correct]
     [Checksum Status: Good]
     Identifier (BE): 1 (0x0001)
     Identifier (LE): 256 (0x0100)
     Sequence number (BE): 30 (0x001e)
     Sequence number (LE): 7680 (0x1e00)
     [Response frame: 51]
  ˅ Data (32 bytes)
        Data: 6162636465666768696a6b6c6d6e6f707172737475767761…
        [Length: 32]
```

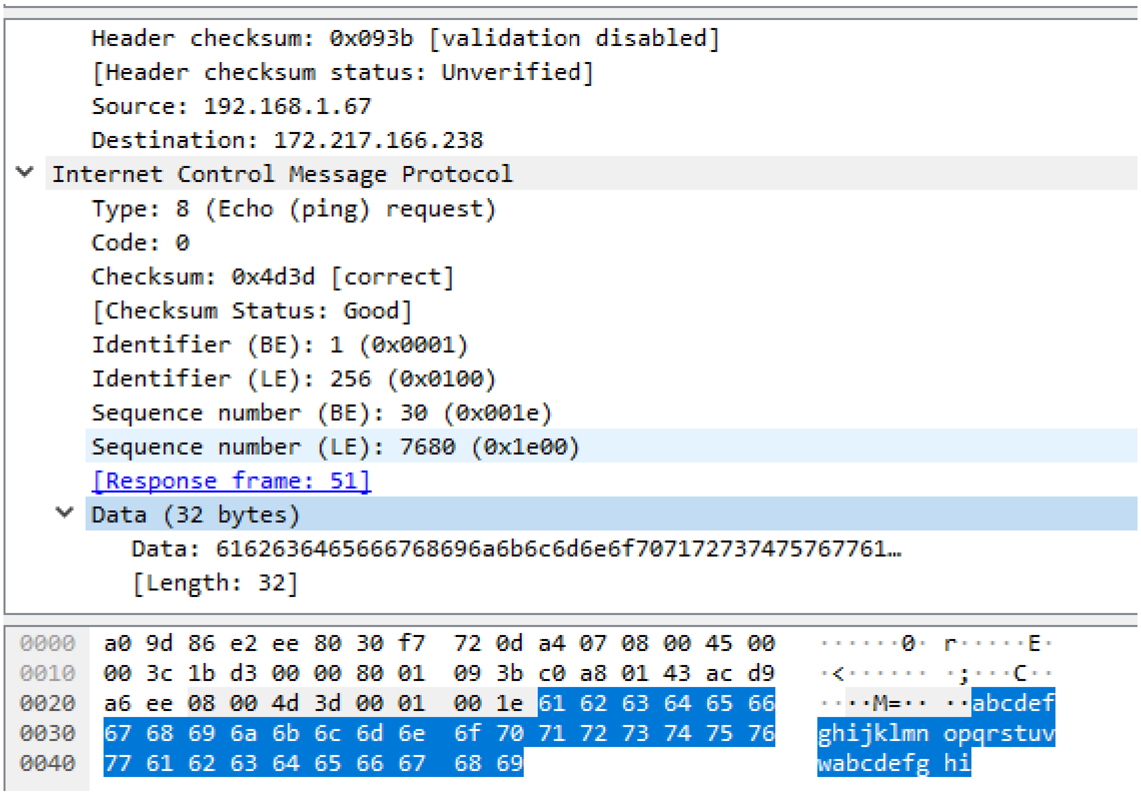
```
0000  a0 9d 86 e2 ee 80 30 f7  72 0d a4 07 08 00 45 00   ······0· r·····E·
0010  00 3c 1b d3 00 00 80 01  09 3b c0 a8 01 43 ac d9   ·<······ ·;···C··
0020  a6 ee 08 00 4d 3d 00 01  00 1e 61 62 63 64 65 66   ····M=·· ··abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```



```
    Header checksum: 0x093b [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.67
    Destination: 172.217.166.238
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4d3d [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 30 (0x001e)
    Sequence number (LE): 7680 (0x1e00)
    [Response frame: 51]
  v Data (32 bytes)
      Data: 6162636465666768696a6b6c6d6e6f7071727374757677761…
      [Length: 32]

0000  a0 9d 86 e2 ee 80 30 f7  72 0d a4 07 08 00 45 00   ······0· r·····E·
0010  00 3c 1b d3 00 00 80 01  09 3b c0 a8 01 43 ac d9   ·<······ ·;···C··
0020  a6 ee 08 00 4d 3d 00 01  00 1e 61 62 63 64 65 66   ····M=·· ··abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```



```
    Header checksum: 0x093b [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.67
    Destination: 172.217.166.238
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4d3d [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 30 (0x001e)
    Sequence number (LE): 7680 (0x1e00)
    [Response frame: 51]
  v Data (32 bytes)
      Data: 6162636465666768696a6b6c6d6e6f7071727374757677761…
      [Length: 32]

0000  a0 9d 86 e2 ee 80 30 f7  72 0d a4 07 08 00 45 00   ······0· r·····E·
0010  00 3c 1b d3 00 00 80 01  09 3b c0 a8 01 43 ac d9   ·<······ ·;···C··
0020  a6 ee 08 00 4d 3d 00 01  00 1e 61 62 63 64 65 66   ····M=·· ··abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```



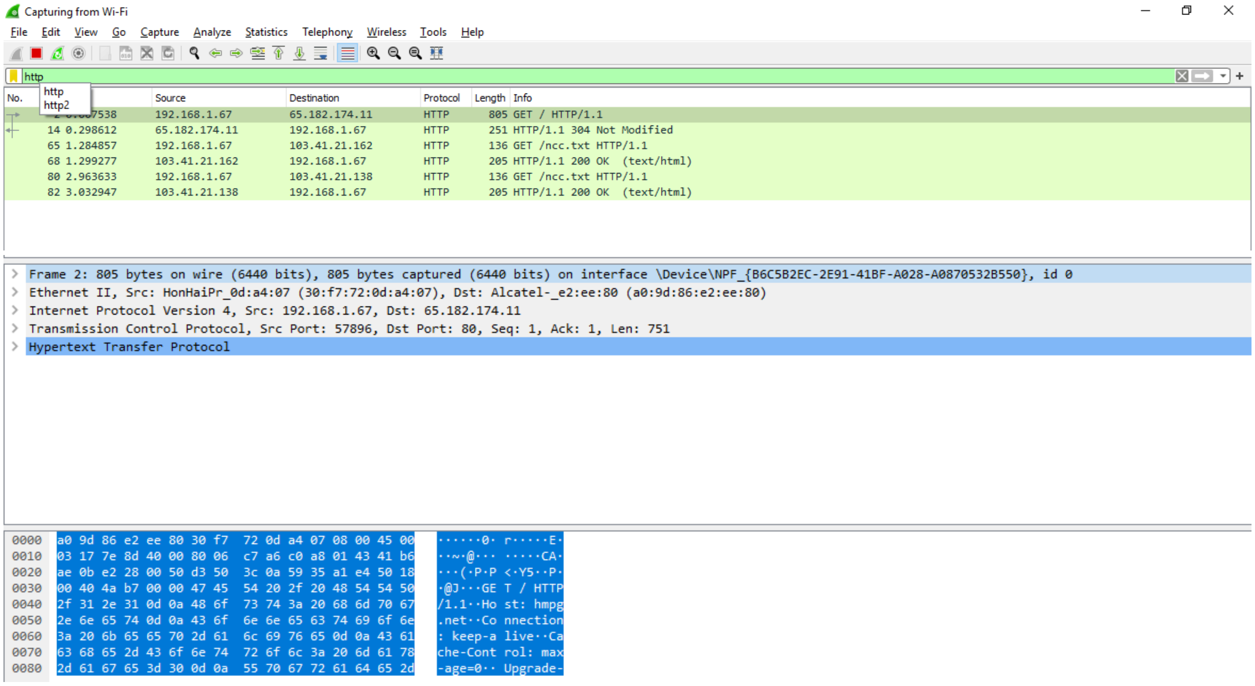
```
    Header checksum: 0x093b [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.67
    Destination: 172.217.166.238
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4d3d [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 30 (0x001e)
    Sequence number (LE): 7680 (0x1e00)
    [Response frame: 51]
  v Data (32 bytes)
      Data: 6162636465666768696a6b6c6d6e6f7071727374757677761…
      [Length: 32]
```

```
0000  a0 9d 86 e2 ee 80 30 f7  72 0d a4 07 08 00 45 00   ······0· r·····E·
0010  00 3c 1b d3 00 00 80 01  09 3b c0 a8 01 43 ac d9   ·<······ ·;···C··
0020  a6 ee 08 00 4d 3d 00 01  00 1e 61 62 63 64 65 66   ····M=·· ··abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```

Last 32 bytes describes the data being transferred in frame, in this case.

B. HTTP

On a web search of a website (http://hmpg.net/), I was able to sniff the HTTP frame in Wireshark.

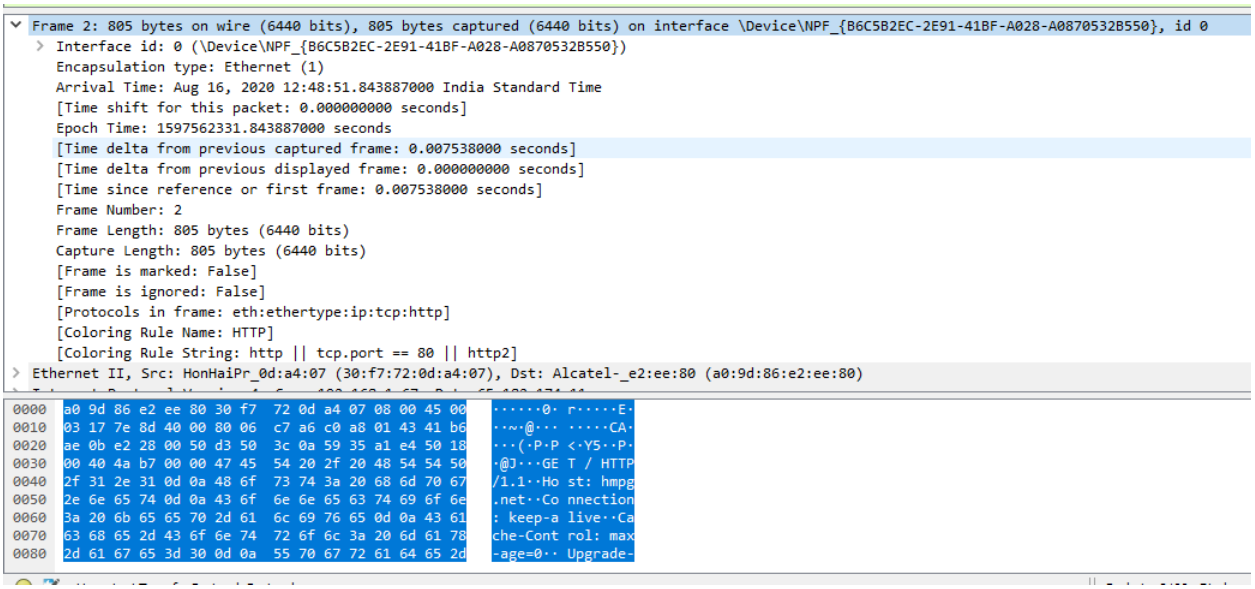

Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
http
http2

```
No.   Time        Source          Destination     Protocol Length Info
   2 0.007538    192.168.1.67    65.182.174.11   HTTP      805 GET / HTTP/1.1
  14 0.298612    65.182.174.11   192.168.1.67    HTTP      251 HTTP/1.1 304 Not Modified
  65 1.284857    192.168.1.67    103.41.21.162   HTTP      136 GET /ncc.txt HTTP/1.1
  68 1.299277    103.41.21.162   192.168.1.67    HTTP      205 HTTP/1.1 200 OK  (text/html)
  80 2.963633    192.168.1.67    103.41.21.138   HTTP      136 GET /ncc.txt HTTP/1.1
  82 3.032947    103.41.21.138   192.168.1.67    HTTP      205 HTTP/1.1 200 OK  (text/html)
```

```
> Frame 2: 805 bytes on wire (6440 bits), 805 bytes captured (6440 bits) on interface \Device\NPF_{B6C5B2EC-2E91-41BF-A028-A0870532B550}, id 0
> Ethernet II, Src: HonHaiPr_0d:a4:07 (30:f7:72:0d:a4:07), Dst: Alcatel-_e2:ee:80 (a0:9d:86:e2:ee:80)
> Internet Protocol Version 4, Src: 192.168.1.67, Dst: 65.182.174.11
> Transmission Control Protocol, Src Port: 57896, Dst Port: 80, Seq: 1, Ack: 1, Len: 751
> Hypertext Transfer Protocol
```

```
0000  a0 9d 86 e2 ee 80 30 f7  72 0d a4 07 08 00 45 00   ······0· r·····E·
0010  03 17 7e 8d 40 00 80 06  c7 a6 c0 a8 01 43 41 b6   ··~·@··· ·····CA·
0020  ae 0b e2 28 00 50 d3 50  3c 0a 59 35 a1 e4 50 18   ···(·P·P <·Y5··P·
0030  00 40 4a b7 00 00 47 45  54 20 2f 20 48 54 54 50   ·@J···GE T / HTTP
0040  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 68 6d 70 67   /1.1··Ho st: hmpg
0050  2e 6e 65 74 0d 0a 43 6f  6e 6e 65 63 74 69 6f 6e   .net··Co nnection
0060  3a 20 6b 65 65 70 2d 61  6c 69 76 65 0d 0a 43 61   : keep-a live··Ca
0070  63 68 65 2d 43 6f 6e 74  72 6f 6c 3a 20 6d 61 78   che-Cont rol: max
0080  2d 61 67 65 3d 30 0d 0a  55 70 67 72 61 64 65 2d   -age=0·· Upgrade-
```

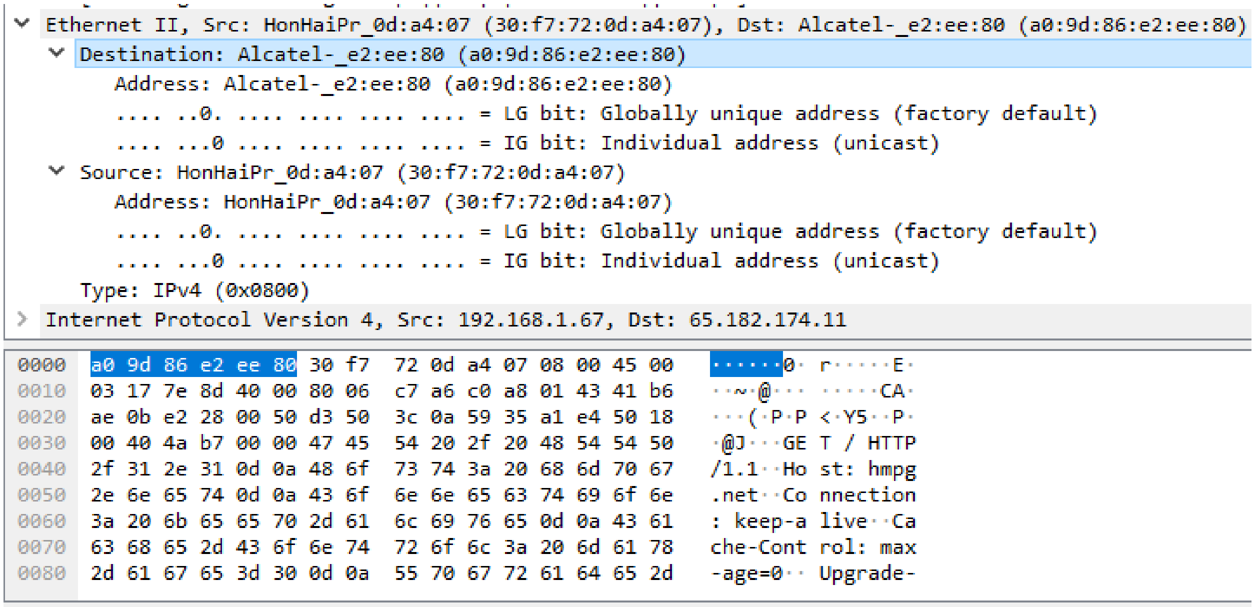
- Information regarding the frame (self explanatory).



```
v Frame 2: 805 bytes on wire (6440 bits), 805 bytes captured (6440 bits) on interface \Device\NPF_{B6C5B2EC-2E91-41BF-A028-A0870532B550}, id 0
  > Interface id: 0 (\Device\NPF_{B6C5B2EC-2E91-41BF-A028-A0870532B550})
    Encapsulation type: Ethernet (1)
    Arrival Time: Aug 16, 2020 12:48:51.843887000 India Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1597562331.843887000 seconds
    [Time delta from previous captured frame: 0.007538000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.007538000 seconds]
    Frame Number: 2
    Frame Length: 805 bytes (6440 bits)
    Capture Length: 805 bytes (6440 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: HonHaiPr_0d:a4:07 (30:f7:72:0d:a4:07), Dst: Alcatel-_e2:ee:80 (a0:9d:86:e2:ee:80)
```

```
0000  a0 9d 86 e2 ee 80 30 f7  72 0d a4 07 08 00 45 00   ······0· r·····E·
0010  03 17 7e 8d 40 00 80 06  c7 a6 c0 a8 01 43 41 b6   ··~·@··· ·····CA·
0020  ae 0b e2 28 00 50 d3 50  3c 0a 59 35 a1 e4 50 18   ···(·P·P <·Y5··P·
0030  00 40 4a b7 00 00 47 45  54 20 2f 20 48 54 54 50   ·@J···GE T / HTTP
0040  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 68 6d 70 67   /1.1··Ho st: hmpg
0050  2e 6e 65 74 0d 0a 43 6f  6e 6e 65 63 74 69 6f 6e   .net··Co nnection
0060  3a 20 6b 65 65 70 2d 61  6c 69 76 65 0d 0a 43 61   : keep-a live··Ca
0070  63 68 65 2d 43 6f 6e 74  72 6f 6c 3a 20 6d 61 78   che-Cont rol: max
0080  2d 61 67 65 3d 30 0d 0a  55 70 67 72 61 64 65 2d   -age=0·· Upgrade-
```

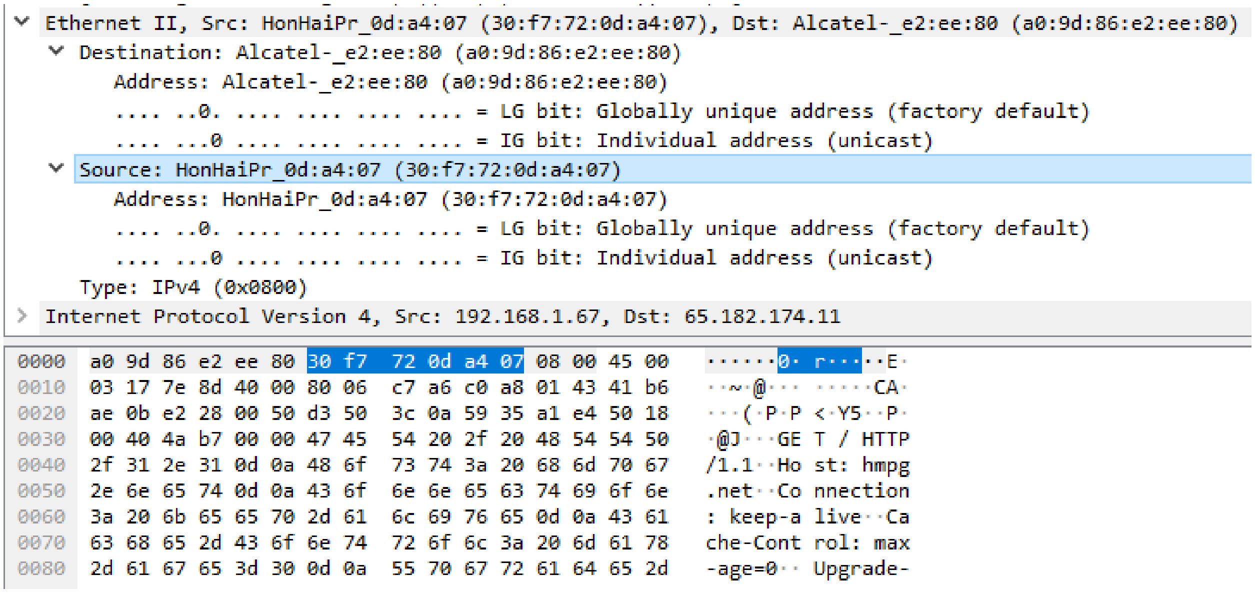
- Information regarding destination MAC address and source MAC address.



```
⌄ Ethernet II, Src: HonHaiPr_0d:a4:07 (30:f7:72:0d:a4:07), Dst: Alcatel-_e2:ee:80 (a0:9d:86:e2:ee:80)
  ⌄ Destination: Alcatel-_e2:ee:80 (a0:9d:86:e2:ee:80)
      Address: Alcatel-_e2:ee:80 (a0:9d:86:e2:ee:80)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ⌄ Source: HonHaiPr_0d:a4:07 (30:f7:72:0d:a4:07)
      Address: HonHaiPr_0d:a4:07 (30:f7:72:0d:a4:07)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 192.168.1.67, Dst: 65.182.174.11
```

```
0000  a0 9d 86 e2 ee 80 30 f7  72 0d a4 07 08 00 45 00   ······0· r·····E·
0010  03 17 7e 8d 40 00 80 06  c7 a6 c0 a8 01 43 41 b6   ··~·@··· ·····CA·
0020  ae 0b e2 28 00 50 d3 50  3c 0a 59 35 a1 e4 50 18   ···(·P·P <·Y5··P·
0030  00 40 4a b7 00 00 47 45  54 20 2f 20 48 54 54 50   ·@J···GE T / HTTP
0040  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 68 6d 70 67   /1.1··Ho st: hmpg
0050  2e 6e 65 74 0d 0a 43 6f  6e 6e 65 63 74 69 6f 6e   .net··Co nnection
0060  3a 20 6b 65 65 70 2d 61  6c 69 76 65 0d 0a 43 61   : keep-a live··Ca
0070  63 68 65 2d 43 6f 6e 74  72 6f 6c 3a 20 6d 61 78   che-Cont rol: max
0080  2d 61 67 65 3d 30 0d 0a  55 70 67 72 61 64 65 2d   -age=0·· Upgrade-
```

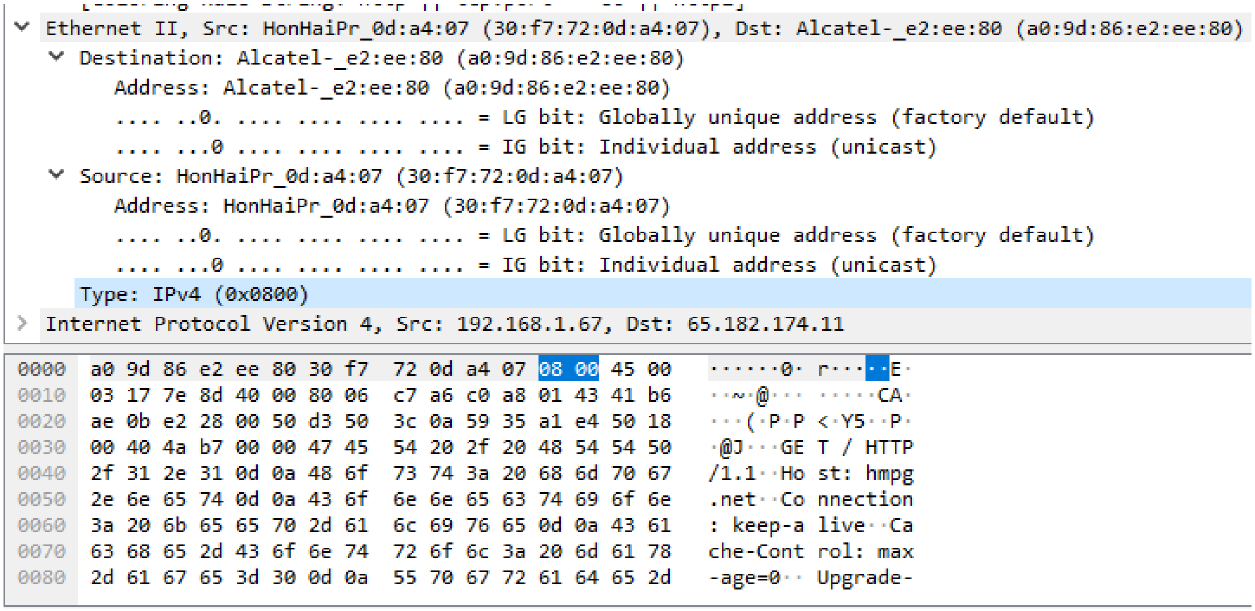
Destination MAC address is of my Router device as that’s the end point of MAC address range.



```
⌄ Ethernet II, Src: HonHaiPr_0d:a4:07 (30:f7:72:0d:a4:07), Dst: Alcatel-_e2:ee:80 (a0:9d:86:e2:ee:80)
  ⌄ Destination: Alcatel-_e2:ee:80 (a0:9d:86:e2:ee:80)
      Address: Alcatel-_e2:ee:80 (a0:9d:86:e2:ee:80)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ⌄ Source: HonHaiPr_0d:a4:07 (30:f7:72:0d:a4:07)
      Address: HonHaiPr_0d:a4:07 (30:f7:72:0d:a4:07)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 192.168.1.67, Dst: 65.182.174.11
```

```
0000  a0 9d 86 e2 ee 80 30 f7  72 0d a4 07 08 00 45 00   ······0· r·····E·
0010  03 17 7e 8d 40 00 80 06  c7 a6 c0 a8 01 43 41 b6   ··~·@··· ·····CA·
0020  ae 0b e2 28 00 50 d3 50  3c 0a 59 35 a1 e4 50 18   ···(·P·P <·Y5··P·
0030  00 40 4a b7 00 00 47 45  54 20 2f 20 48 54 54 50   ·@J···GE T / HTTP
0040  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 68 6d 70 67   /1.1··Ho st: hmpg
0050  2e 6e 65 74 0d 0a 43 6f  6e 6e 65 63 74 69 6f 6e   .net··Co nnection
0060  3a 20 6b 65 65 70 2d 61  6c 69 76 65 0d 0a 43 61   : keep-a live··Ca
0070  63 68 65 2d 43 6f 6e 74  72 6f 6c 3a 20 6d 61 78   che-Cont rol: max
0080  2d 61 67 65 3d 30 0d 0a  55 70 67 72 61 64 65 2d   -age=0·· Upgrade-
```

Source MAC address is of my device by which the request was made.

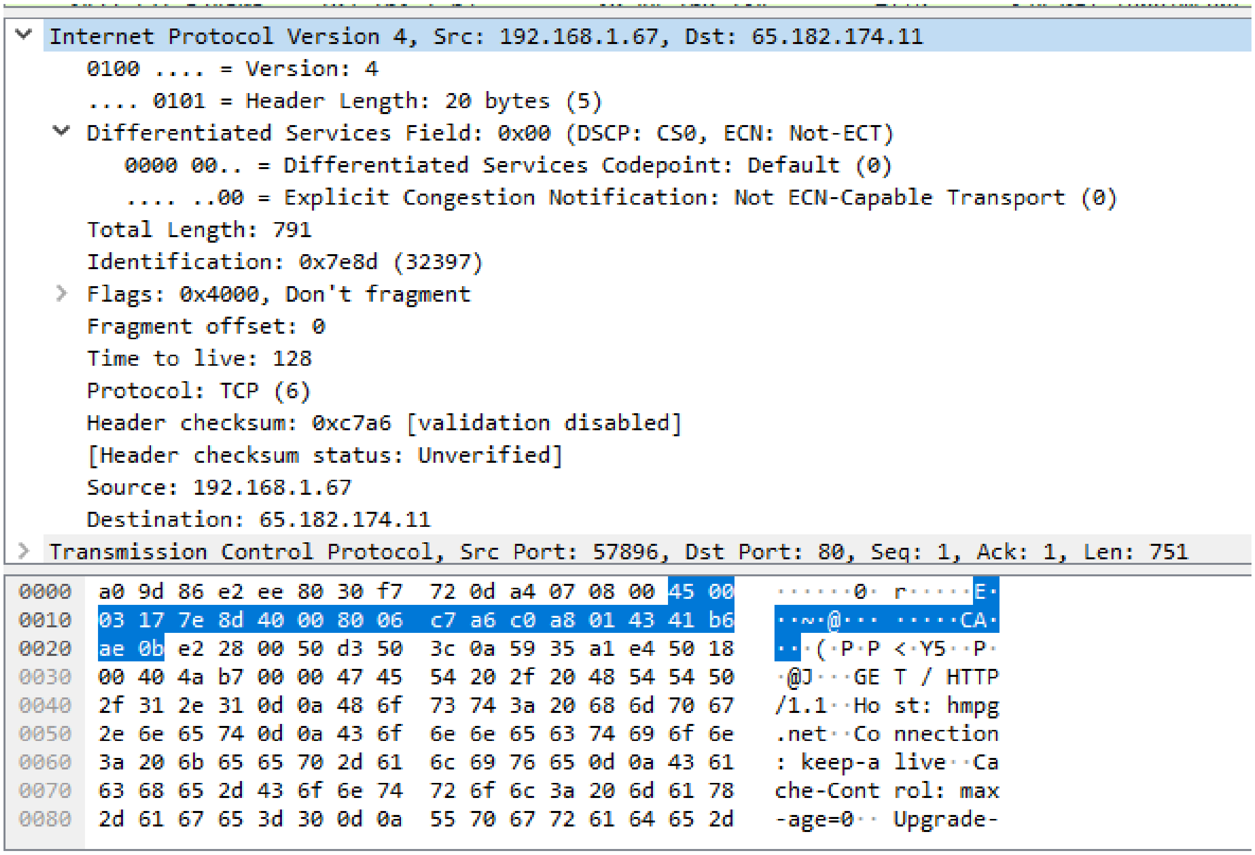


```
 Ethernet II, Src: HonHaiPr_0d:a4:07 (30:f7:72:0d:a4:07), Dst: Alcatel-_e2:ee:80 (a0:9d:86:e2:ee:80)
   Destination: Alcatel-_e2:ee:80 (a0:9d:86:e2:ee:80)
      Address: Alcatel-_e2:ee:80 (a0:9d:86:e2:ee:80)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
   Source: HonHaiPr_0d:a4:07 (30:f7:72:0d:a4:07)
      Address: HonHaiPr_0d:a4:07 (30:f7:72:0d:a4:07)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
   Type: IPv4 (0x0800)
 Internet Protocol Version 4, Src: 192.168.1.67, Dst: 65.182.174.11
```

```
0000  a0 9d 86 e2 ee 80 30 f7  72 0d a4 07 08 00 45 00   ······0· r·····E·
0010  03 17 7e 8d 40 00 80 06  c7 a6 c0 a8 01 43 41 b6   ··~·@··· ·····CA·
0020  ae 0b e2 28 00 50 d3 50  3c 0a 59 35 a1 e4 50 18   ···(·P·P <·Y5··P·
0030  00 40 4a b7 00 00 47 45  54 20 2f 20 48 54 54 50   ·@J···GE T / HTTP
0040  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 68 6d 70 67   /1.1··Ho st: hmpg
0050  2e 6e 65 74 0d 0a 43 6f  6e 6e 65 63 74 69 6f 6e   .net··Co nnection
0060  3a 20 6b 65 65 70 2d 61  6c 69 76 65 0d 0a 43 61   : keep-a live··Ca
0070  63 68 65 2d 43 6f 6e 74  72 6f 6c 3a 20 6d 61 78   che-Cont rol: max
0080  2d 61 67 65 3d 30 0d 0a  55 70 67 72 61 64 65 2d   -age=0·· Upgrade-
```

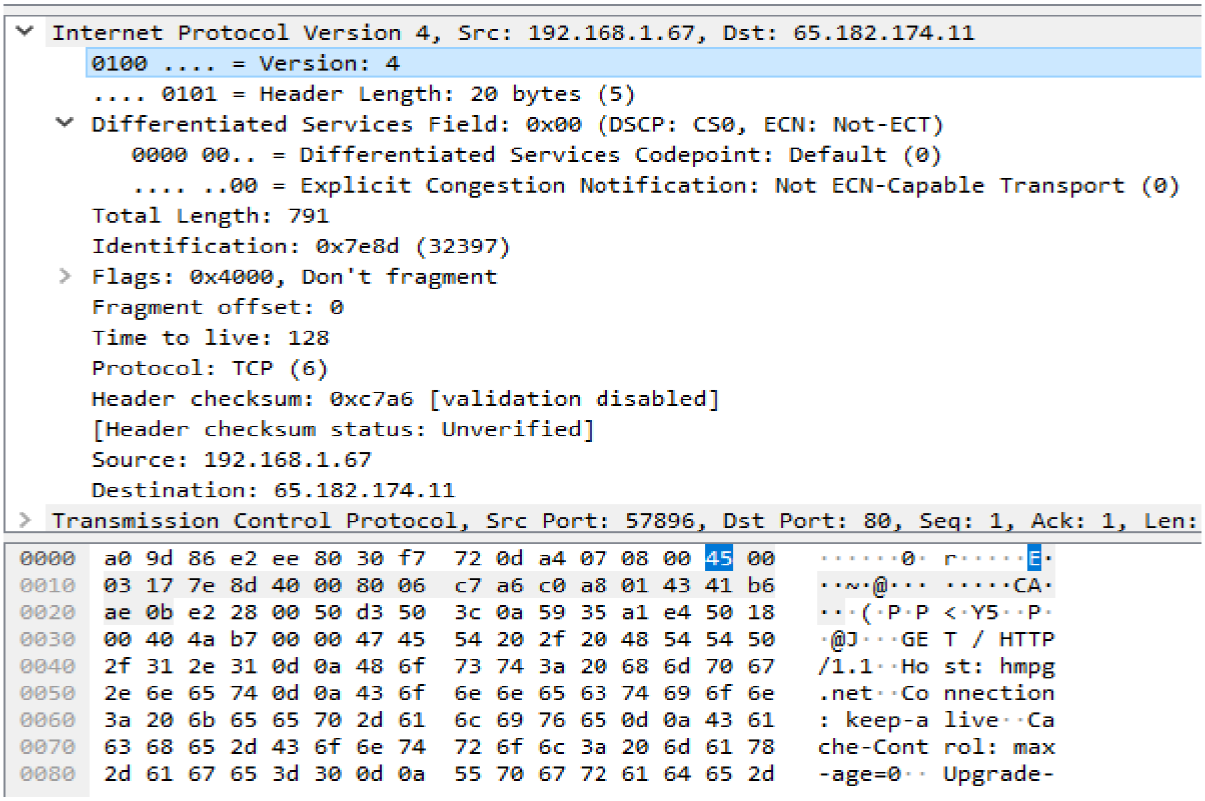
Tells the network layer next that the rest of from has version 4 of IP address.

- Here’s the information regarding IPs associated.



```
 Internet Protocol Version 4, Src: 192.168.1.67, Dst: 65.182.174.11
    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: 791
    Identification: 0x7e8d (32397)
    Flags: 0x4000, Don't fragment
    Fragment offset: 0
    Time to live: 128
    Protocol: TCP (6)
    Header checksum: 0xc7a6 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.67
    Destination: 65.182.174.11
 Transmission Control Protocol, Src Port: 57896, Dst Port: 80, Seq: 1, Ack: 1, Len: 751
```

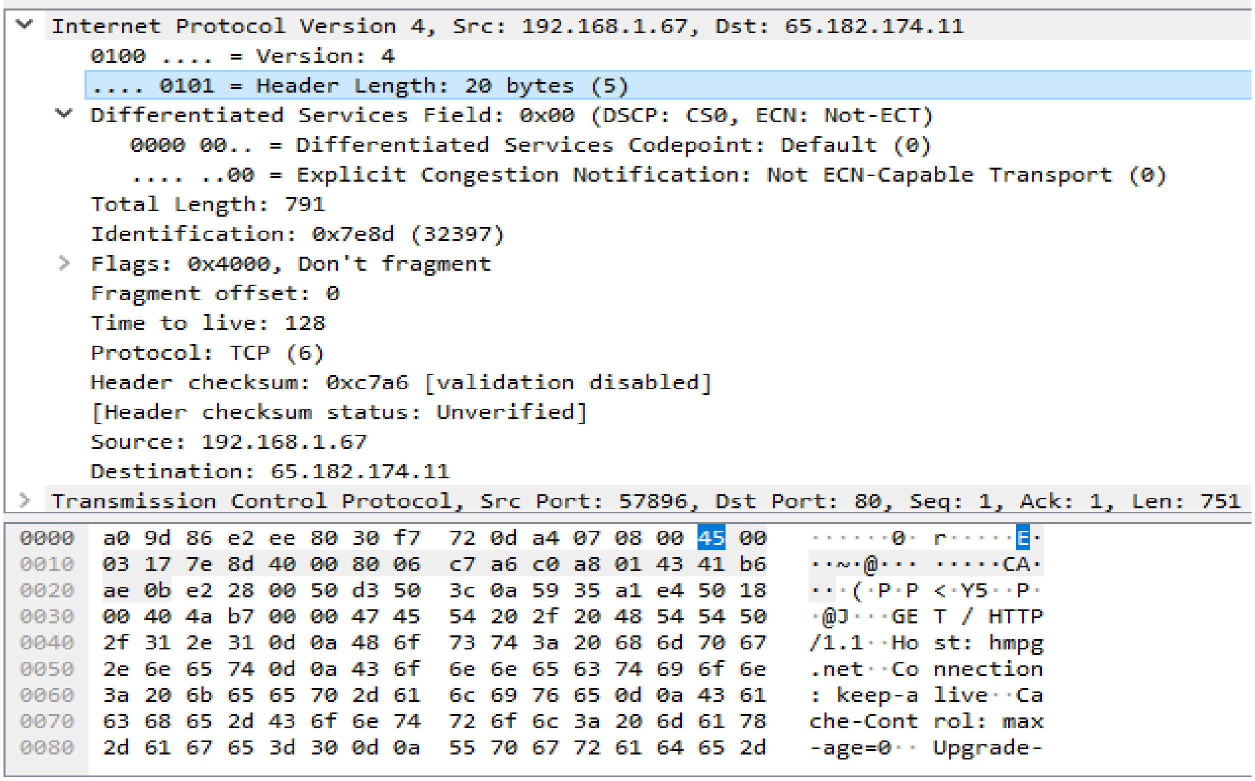
```
0000  a0 9d 86 e2 ee 80 30 f7  72 0d a4 07 08 00 45 00   ······0· r·····E·
0010  03 17 7e 8d 40 00 80 06  c7 a6 c0 a8 01 43 41 b6   ··~·@··· ·····CA·
0020  ae 0b e2 28 00 50 d3 50  3c 0a 59 35 a1 e4 50 18   ···(·P·P <·Y5··P·
0030  00 40 4a b7 00 00 47 45  54 20 2f 20 48 54 54 50   ·@J···GE T / HTTP
0040  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 68 6d 70 67   /1.1··Ho st: hmpg
0050  2e 6e 65 74 0d 0a 43 6f  6e 6e 65 63 74 69 6f 6e   .net··Co nnection
0060  3a 20 6b 65 65 70 2d 61  6c 69 76 65 0d 0a 43 61   : keep-a live··Ca
0070  63 68 65 2d 43 6f 6e 74  72 6f 6c 3a 20 6d 61 78   che-Cont rol: max
0080  2d 61 67 65 3d 30 0d 0a  55 70 67 72 61 64 65 2d   -age=0·· Upgrade-
```



```
Internet Protocol Version 4, Src: 192.168.1.67, Dst: 65.182.174.11
    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: 791
    Identification: 0x7e8d (32397)
  > Flags: 0x4000, Don't fragment
    Fragment offset: 0
    Time to live: 128
    Protocol: TCP (6)
    Header checksum: 0xc7a6 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.67
    Destination: 65.182.174.11
> Transmission Control Protocol, Src Port: 57896, Dst Port: 80, Seq: 1, Ack: 1, Len:
```

```
0000  a0 9d 86 e2 ee 80 30 f7  72 0d a4 07 08 00 45 00   ······0· r·····E·
0010  03 17 7e 8d 40 00 80 06  c7 a6 c0 a8 01 43 41 b6   ··~·@··· ·····CA·
0020  ae 0b e2 28 00 50 d3 50  3c 0a 59 35 a1 e4 50 18   ···(·P·P <·Y5··P·
0030  00 40 4a b7 00 00 47 45  54 20 2f 20 48 54 54 50   ·@J···GE T / HTTP
0040  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 68 6d 70 67   /1.1··Ho st: hmpg
0050  2e 6e 65 74 0d 0a 43 6f  6e 6e 65 63 74 69 6f 6e   .net··Co nnection
0060  3a 20 6b 65 65 70 2d 61  6c 69 76 65 0d 0a 43 61   : keep-a live··Ca
0070  63 68 65 2d 43 6f 6e 74  72 6f 6c 3a 20 6d 61 78   che-Cont rol: max
0080  2d 61 67 65 3d 30 0d 0a  55 70 67 72 61 64 65 2d   -age=0·· Upgrade-
```

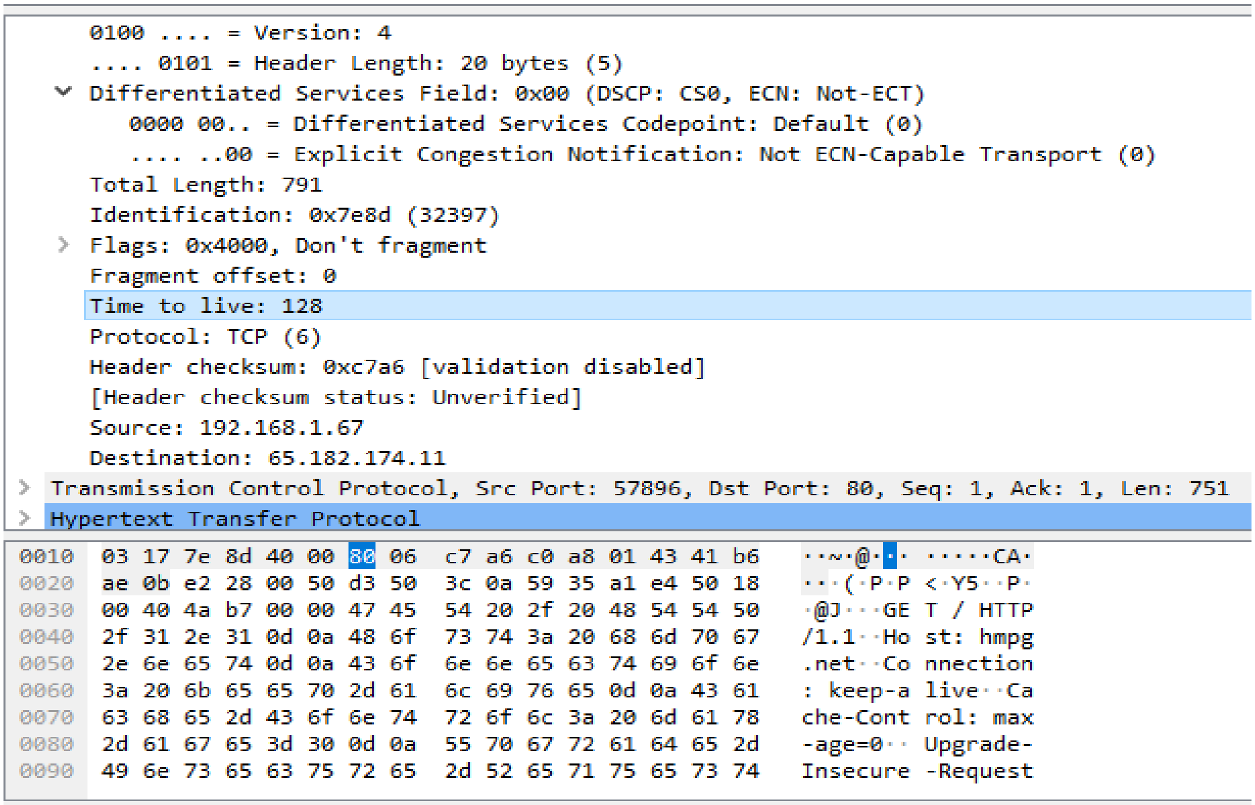
Shows the version of IP that is 4, IPv4.



```
Internet Protocol Version 4, Src: 192.168.1.67, Dst: 65.182.174.11
    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: 791
    Identification: 0x7e8d (32397)
  > Flags: 0x4000, Don't fragment
    Fragment offset: 0
    Time to live: 128
    Protocol: TCP (6)
    Header checksum: 0xc7a6 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.67
    Destination: 65.182.174.11
> Transmission Control Protocol, Src Port: 57896, Dst Port: 80, Seq: 1, Ack: 1, Len: 751
```

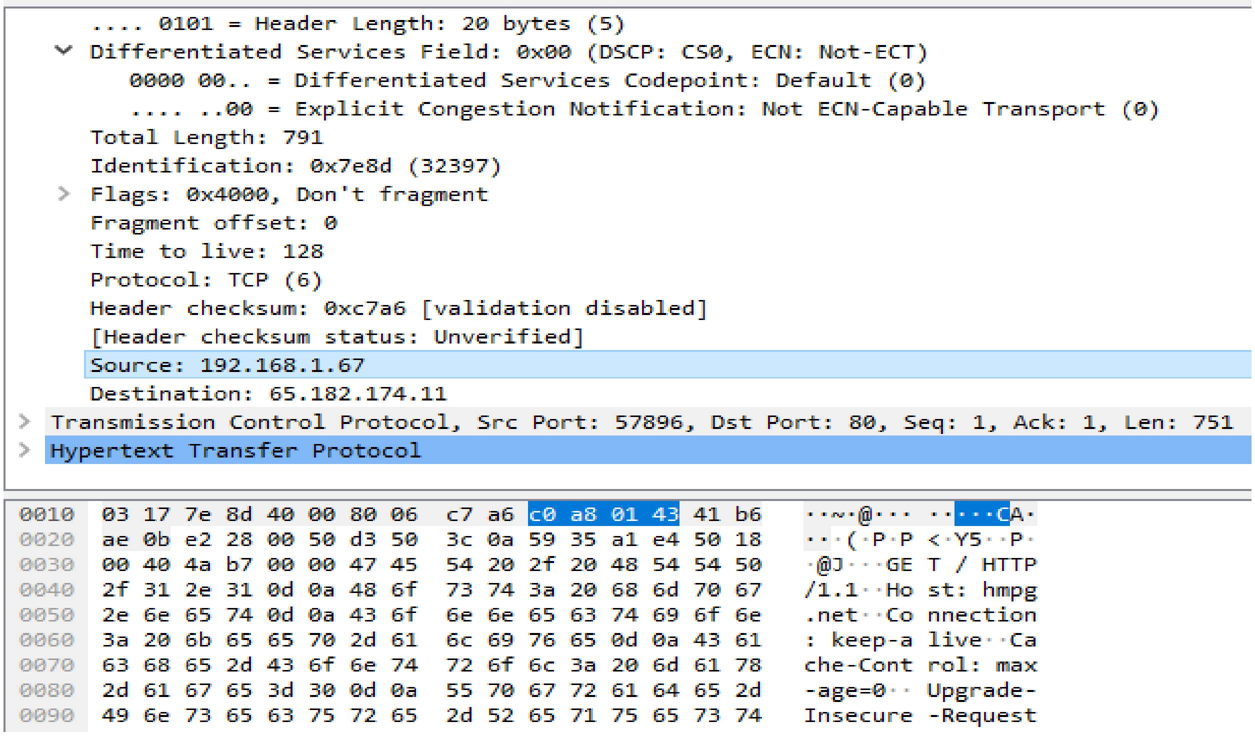
```
0000  a0 9d 86 e2 ee 80 30 f7  72 0d a4 07 08 00 45 00   ······0· r·····E·
0010  03 17 7e 8d 40 00 80 06  c7 a6 c0 a8 01 43 41 b6   ··~·@··· ·····CA·
0020  ae 0b e2 28 00 50 d3 50  3c 0a 59 35 a1 e4 50 18   ···(·P·P <·Y5··P·
0030  00 40 4a b7 00 00 47 45  54 20 2f 20 48 54 54 50   ·@J···GE T / HTTP
0040  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 68 6d 70 67   /1.1··Ho st: hmpg
0050  2e 6e 65 74 0d 0a 43 6f  6e 6e 65 63 74 69 6f 6e   .net··Co nnection
0060  3a 20 6b 65 65 70 2d 61  6c 69 76 65 0d 0a 43 61   : keep-a live··Ca
0070  63 68 65 2d 43 6f 6e 74  72 6f 6c 3a 20 6d 61 78   che-Cont rol: max
0080  2d 61 67 65 3d 30 0d 0a  55 70 67 72 61 64 65 2d   -age=0·· Upgrade-
```

Shows the Length of Header, i.e. 20 bytes.



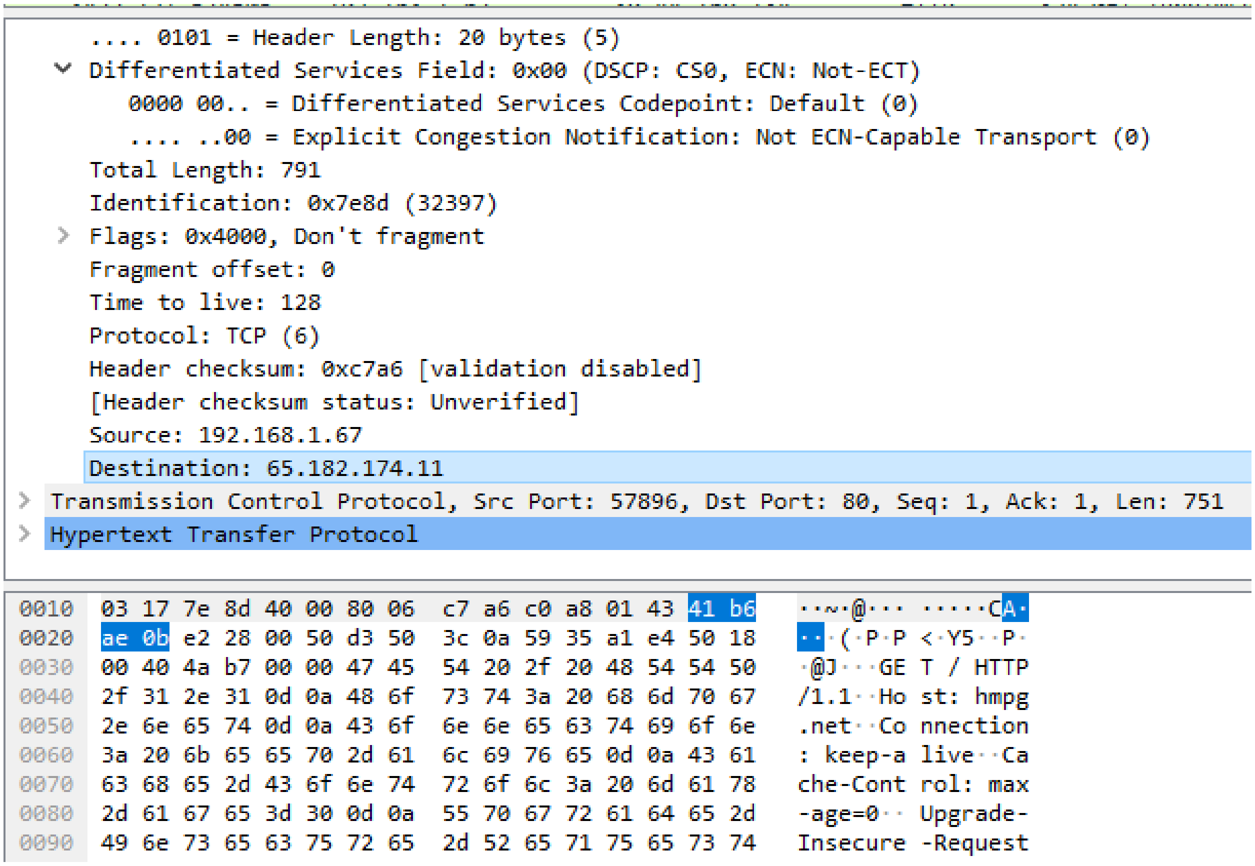
```
      0100 .... = Version: 4
      .... 0101 = Header Length: 20 bytes (5)
    ⌄ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
         0000 00.. = Differentiated Services Codepoint: Default (0)
         .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
      Total Length: 791
      Identification: 0x7e8d (32397)
    > Flags: 0x4000, Don't fragment
      Fragment offset: 0
      Time to live: 128
      Protocol: TCP (6)
      Header checksum: 0xc7a6 [validation disabled]
      [Header checksum status: Unverified]
      Source: 192.168.1.67
      Destination: 65.182.174.11
> Transmission Control Protocol, Src Port: 57896, Dst Port: 80, Seq: 1, Ack: 1, Len: 751
> Hypertext Transfer Protocol

0010  03 17 7e 8d 40 00 80 06  c7 a6 c0 a8 01 43 41 b6   ··~·@··· ·····CA·
0020  ae 0b e2 28 00 50 d3 50  3c 0a 59 35 a1 e4 50 18   ···(·P·P <·Y5··P·
0030  00 40 4a b7 00 00 47 45  54 20 2f 20 48 54 54 50   ·@J···GE T / HTTP
0040  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 68 6d 70 67   /1.1··Ho st: hmpg
0050  2e 6e 65 74 0d 0a 43 6f  6e 6e 65 63 74 69 6f 6e   .net··Co nnection
0060  3a 20 6b 65 65 70 2d 61  6c 69 76 65 0d 0a 43 61   : keep-a live··Ca
0070  63 68 65 2d 43 6f 6e 74  72 6f 6c 3a 20 6d 61 78   che-Cont rol: max
0080  2d 61 67 65 3d 30 0d 0a  55 70 67 72 61 64 65 2d   -age=0·· Upgrade-
0090  49 6e 73 65 63 75 72 65  2d 52 65 71 75 65 73 74   Insecure -Request
```

Time To Live (TTL) represents the number of hops the frame jumped from.



```
      .... 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: 791
      Identification: 0x7e8d (32397)
    > Flags: 0x4000, Don't fragment
      Fragment offset: 0
      Time to live: 128
      Protocol: TCP (6)
      Header checksum: 0xc7a6 [validation disabled]
      [Header checksum status: Unverified]
      Source: 192.168.1.67
      Destination: 65.182.174.11
> Transmission Control Protocol, Src Port: 57896, Dst Port: 80, Seq: 1, Ack: 1, Len: 751
> Hypertext Transfer Protocol

0010  03 17 7e 8d 40 00 80 06  c7 a6 c0 a8 01 43 41 b6   ··~·@··· ·····CA·
0020  ae 0b e2 28 00 50 d3 50  3c 0a 59 35 a1 e4 50 18   ···(·P·P <·Y5··P·
0030  00 40 4a b7 00 00 47 45  54 20 2f 20 48 54 54 50   ·@J···GE T / HTTP
0040  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 68 6d 70 67   /1.1··Ho st: hmpg
0050  2e 6e 65 74 0d 0a 43 6f  6e 6e 65 63 74 69 6f 6e   .net··Co nnection
0060  3a 20 6b 65 65 70 2d 61  6c 69 76 65 0d 0a 43 61   : keep-a live··Ca
0070  63 68 65 2d 43 6f 6e 74  72 6f 6c 3a 20 6d 61 78   che-Cont rol: max
0080  2d 61 67 65 3d 30 0d 0a  55 70 67 72 61 64 65 2d   -age=0·· Upgrade-
0090  49 6e 73 65 63 75 72 65  2d 52 65 71 75 65 73 74   Insecure -Request
```

Source: Source IP address, that's the device's IP address from which the HTTP request was made (192.168.1.67), Private IP address.

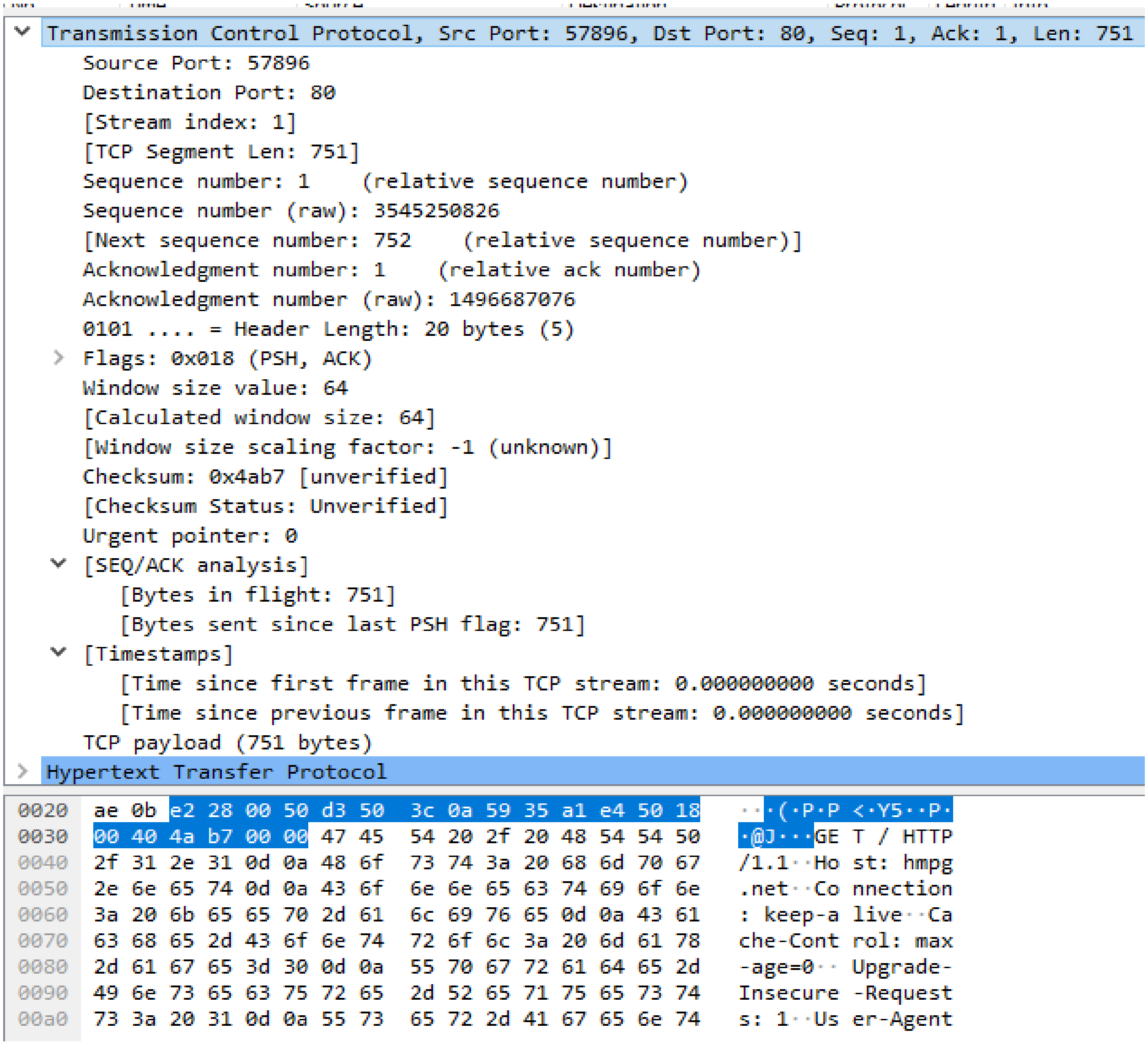


```
    .... 0101 = Header Length: 20 bytes (5)
  ˅ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 791
    Identification: 0x7e8d (32397)
  > Flags: 0x4000, Don't fragment
    Fragment offset: 0
    Time to live: 128
    Protocol: TCP (6)
    Header checksum: 0xc7a6 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.67
    Destination: 65.182.174.11
> Transmission Control Protocol, Src Port: 57896, Dst Port: 80, Seq: 1, Ack: 1, Len: 751
> Hypertext Transfer Protocol
```

```
0010  03 17 7e 8d 40 00 80 06  c7 a6 c0 a8 01 43 41 b6   ··~·@··· ·····CA·
0020  ae 0b e2 28 00 50 d3 50  3c 0a 59 35 a1 e4 50 18   ···(·P·P <·Y5··P·
0030  00 40 4a b7 00 00 47 45  54 20 2f 20 48 54 54 50   ·@J···GE T / HTTP
0040  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 68 6d 70 67   /1.1··Ho st: hmpg
0050  2e 6e 65 74 0d 0a 43 6f  6e 6e 65 63 74 69 6f 6e   .net··Co nnection
0060  3a 20 6b 65 65 70 2d 61  6c 69 76 65 0d 0a 43 61   : keep-a live··Ca
0070  63 68 65 2d 43 6f 6e 74  72 6f 6c 3a 20 6d 61 78   che-Cont rol: max
0080  2d 61 67 65 3d 30 0d 0a  55 70 67 72 61 64 65 2d   -age=0·· Upgrade-
0090  49 6e 73 65 63 75 72 65  2d 52 65 71 75 65 73 74   Insecure -Request
```

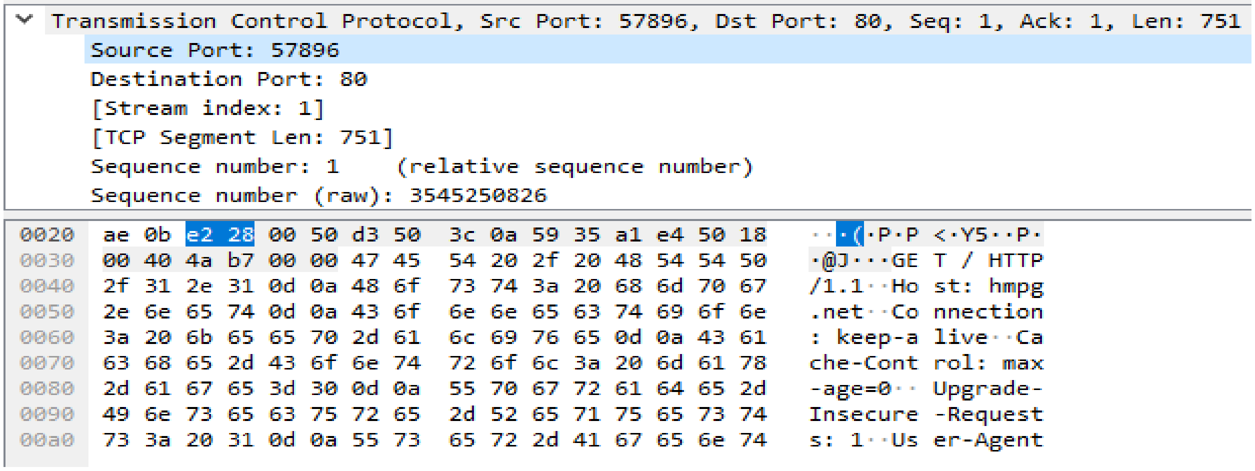
Destination: it's the IP address of destination or the host where the website searched in browser was hosted.

- Information about TCP (Transmission Control Protocol)



```
v Transmission Control Protocol, Src Port: 57896, Dst Port: 80, Seq: 1, Ack: 1, Len: 751
     Source Port: 57896
     Destination Port: 80
     [Stream index: 1]
     [TCP Segment Len: 751]
     Sequence number: 1    (relative sequence number)
     Sequence number (raw): 3545250826
     [Next sequence number: 752    (relative sequence number)]
     Acknowledgment number: 1    (relative ack number)
     Acknowledgment number (raw): 1496687076
     0101 .... = Header Length: 20 bytes (5)
   > Flags: 0x018 (PSH, ACK)
     Window size value: 64
     [Calculated window size: 64]
     [Window size scaling factor: -1 (unknown)]
     Checksum: 0x4ab7 [unverified]
     [Checksum Status: Unverified]
     Urgent pointer: 0
   v [SEQ/ACK analysis]
        [Bytes in flight: 751]
        [Bytes sent since last PSH flag: 751]
   v [Timestamps]
        [Time since first frame in this TCP stream: 0.000000000 seconds]
        [Time since previous frame in this TCP stream: 0.000000000 seconds]
     TCP payload (751 bytes)
> Hypertext Transfer Protocol
```

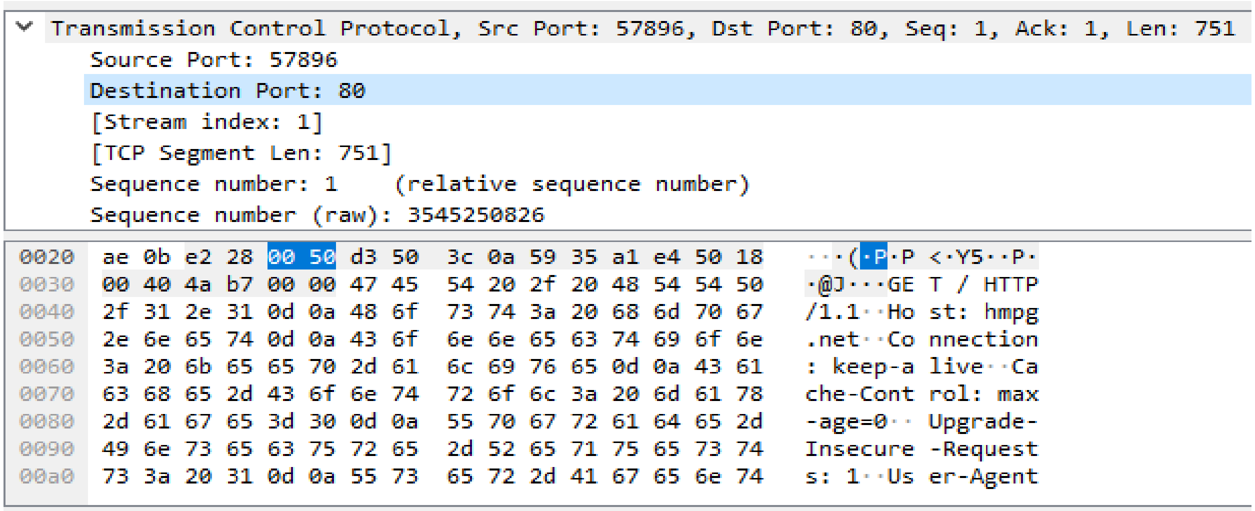
```
0020  ae 0b e2 28 00 50 d3 50  3c 0a 59 35 a1 e4 50 18   ···(·P·P <·Y5··P·
0030  00 40 4a b7 00 00 47 45  54 20 2f 20 48 54 54 50   ·@J···GE T / HTTP
0040  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 68 6d 70 67   /1.1··Ho st: hmpg
0050  2e 6e 65 74 0d 0a 43 6f  6e 6e 65 63 74 69 6f 6e   .net··Co nnection
0060  3a 20 6b 65 65 70 2d 61  6c 69 76 65 0d 0a 43 61   : keep-a live··Ca
0070  63 68 65 2d 43 6f 6e 74  72 6f 6c 3a 20 6d 61 78   che-Cont rol: max
0080  2d 61 67 65 3d 30 0d 0a  55 70 67 72 61 64 65 2d   -age=0·· Upgrade-
0090  49 6e 73 65 63 75 72 65  2d 52 65 71 75 65 73 74   Insecure -Request
00a0  73 3a 20 31 0d 0a 55 73  65 72 2d 41 67 65 6e 74   s: 1··Us er-Agent
```



```
v Transmission Control Protocol, Src Port: 57896, Dst Port: 80, Seq: 1, Ack: 1, Len: 751
     Source Port: 57896
     Destination Port: 80
     [Stream index: 1]
     [TCP Segment Len: 751]
     Sequence number: 1    (relative sequence number)
     Sequence number (raw): 3545250826
```

```
0020  ae 0b e2 28 00 50 d3 50  3c 0a 59 35 a1 e4 50 18   ···(·P·P <·Y5··P·
0030  00 40 4a b7 00 00 47 45  54 20 2f 20 48 54 54 50   ·@J···GE T / HTTP
0040  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 68 6d 70 67   /1.1··Ho st: hmpg
0050  2e 6e 65 74 0d 0a 43 6f  6e 6e 65 63 74 69 6f 6e   .net··Co nnection
0060  3a 20 6b 65 65 70 2d 61  6c 69 76 65 0d 0a 43 61   : keep-a live··Ca
0070  63 68 65 2d 43 6f 6e 74  72 6f 6c 3a 20 6d 61 78   che-Cont rol: max
0080  2d 61 67 65 3d 30 0d 0a  55 70 67 72 61 64 65 2d   -age=0·· Upgrade-
0090  49 6e 73 65 63 75 72 65  2d 52 65 71 75 65 73 74   Insecure -Request
00a0  73 3a 20 31 0d 0a 55 73  65 72 2d 41 67 65 6e 74   s: 1··Us er-Agent
```

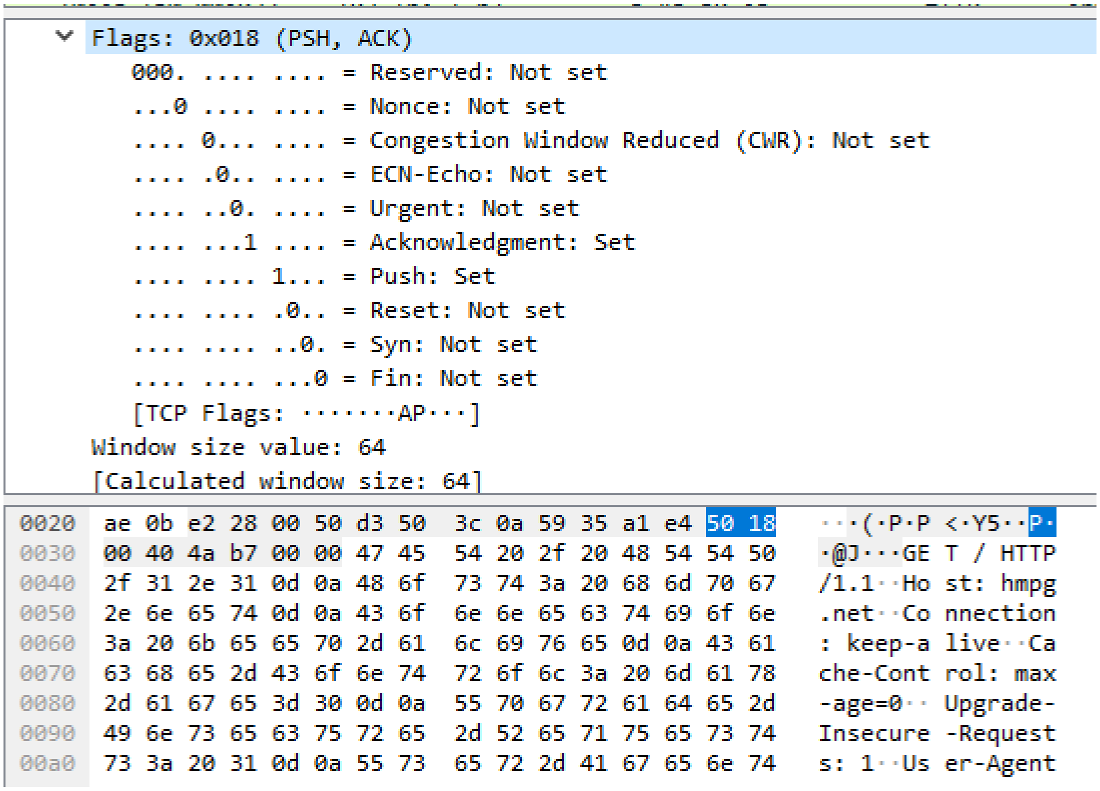
Source Port: 57896 (one of the temporary ports on the source device used for making requests for webpages)



```
∨ Transmission Control Protocol, Src Port: 57896, Dst Port: 80, Seq: 1, Ack: 1, Len: 751
    Source Port: 57896
    Destination Port: 80
    [Stream index: 1]
    [TCP Segment Len: 751]
    Sequence number: 1    (relative sequence number)
    Sequence number (raw): 3545250826
```

```
0020  ae 0b e2 28 00 50 d3 50  3c 0a 59 35 a1 e4 50 18   ···(·P·P <·Y5··P·
0030  00 40 4a b7 00 00 47 45  54 20 2f 20 48 54 54 50   ·@J···GE T / HTTP
0040  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 68 6d 70 67   /1.1··Ho st: hmpg
0050  2e 6e 65 74 0d 0a 43 6f  6e 6e 65 63 74 69 6f 6e   .net··Co nnection
0060  3a 20 6b 65 65 70 2d 61  6c 69 76 65 0d 0a 43 61   : keep-a live··Ca
0070  63 68 65 2d 43 6f 6e 74  72 6f 6c 3a 20 6d 61 78   che-Cont rol: max
0080  2d 61 67 65 3d 30 0d 0a  55 70 67 72 61 64 65 2d   -age=0·· Upgrade-
0090  49 6e 73 65 63 75 72 65  2d 52 65 71 75 65 73 74   Insecure -Request
00a0  73 3a 20 31 0d 0a 55 73  65 72 2d 41 67 65 6e 74   s: 1··Us er-Agent
```

Destination Port: 80 (Reserved port number for HTTP requests)

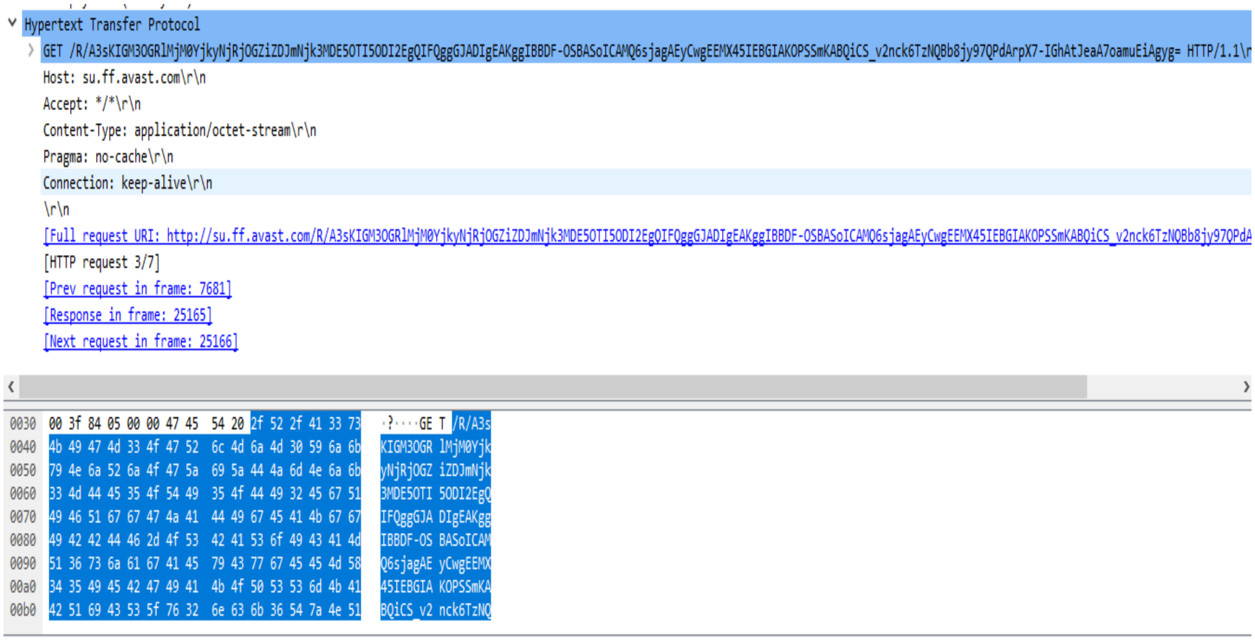


```
  ∨ Flags: 0x018 (PSH, ACK)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Nonce: Not set
      .... 0... .... = Congestion Window Reduced (CWR): Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...1 .... = Acknowledgment: Set
      .... .... 1... = Push: Set
      .... .... .0.. = Reset: Not set
      .... .... ..0. = Syn: Not set
      .... .... ...0 = Fin: Not set
      [TCP Flags: ·······AP···]
    Window size value: 64
    [Calculated window size: 64]
```

```
0020  ae 0b e2 28 00 50 d3 50  3c 0a 59 35 a1 e4 50 18   ···(·P·P <·Y5··P·
0030  00 40 4a b7 00 00 47 45  54 20 2f 20 48 54 54 50   ·@J···GE T / HTTP
0040  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 68 6d 70 67   /1.1··Ho st: hmpg
0050  2e 6e 65 74 0d 0a 43 6f  6e 6e 65 63 74 69 6f 6e   .net··Co nnection
0060  3a 20 6b 65 65 70 2d 61  6c 69 76 65 0d 0a 43 61   : keep-a live··Ca
0070  63 68 65 2d 43 6f 6e 74  72 6f 6c 3a 20 6d 61 78   che-Cont rol: max
0080  2d 61 67 65 3d 30 0d 0a  55 70 67 72 61 64 65 2d   -age=0·· Upgrade-
0090  49 6e 73 65 63 75 72 65  2d 52 65 71 75 65 73 74   Insecure -Request
00a0  73 3a 20 31 0d 0a 55 73  65 72 2d 41 67 65 6e 74   s: 1··Us er-Agent
```

This represents a number of flag bits for more information regarding the frame.

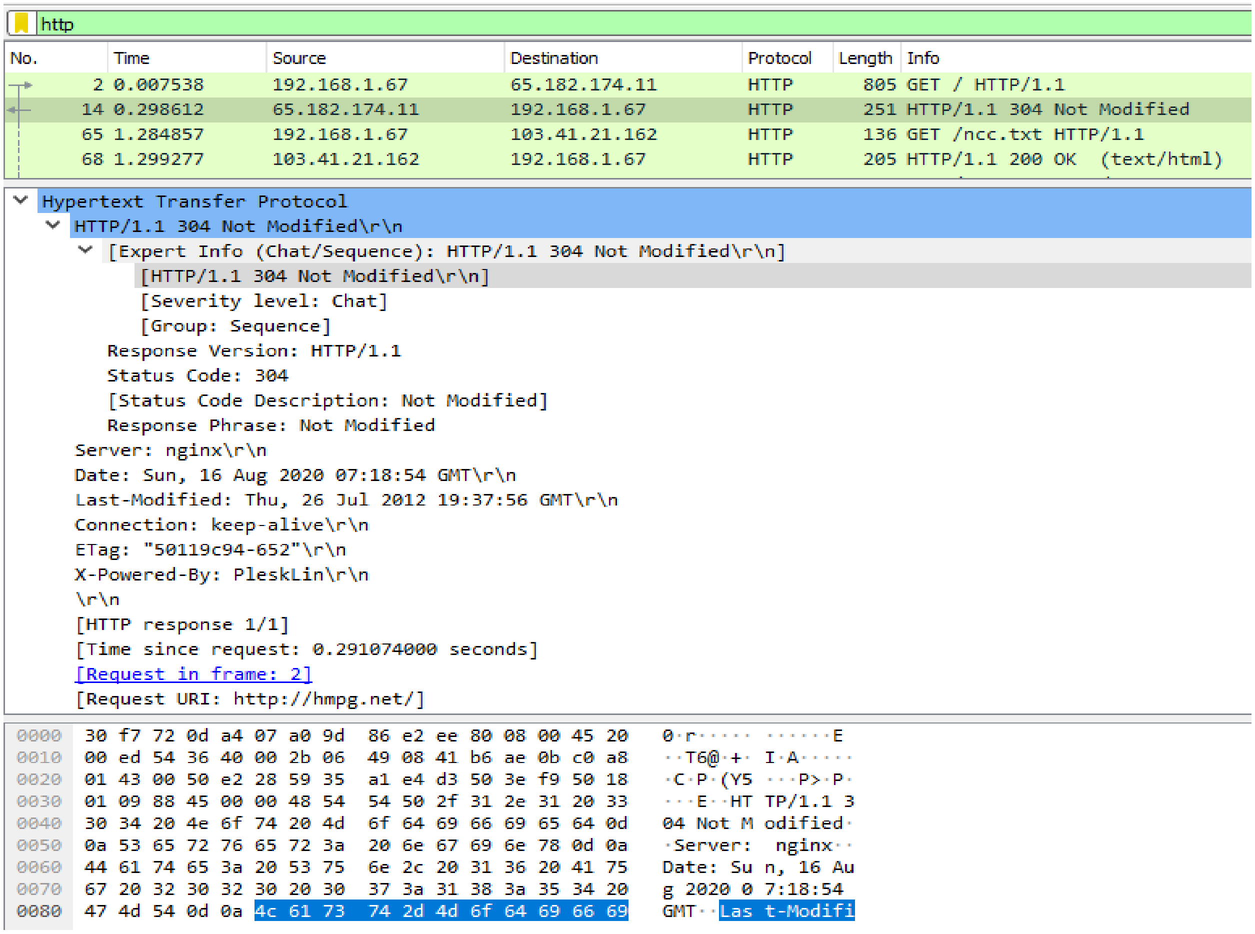
- HTTP



```
v Hypertext Transfer Protocol
  > GET /R/A3sKIGM3OGRlMjM0YjkyNjRjOGZiZDJmNjk3MDE5OTI5ODI2EgQIFQggGJADIgEAKggIBBDF-OSBASoICAMQ6sjagAEyCwgEEMX45IEBGIAKOPSSmKABQiCS_v2nck6TzNQBb8jy97QPdArpX7-IGhAtJeaA7oamuEiAgyg= HTTP/1.1\r
    Host: su.ff.avast.com\r\n
    Accept: */*\r\n
    Content-Type: application/octet-stream\r\n
    Pragma: no-cache\r\n
    Connection: keep-alive\r\n
    \r\n
    [Full request URI: http://su.ff.avast.com/R/A3sKIGM3OGRlMjM0YjkyNjRjOGZiZDJmNjk3MDE5OTI5ODI2EgQIFQggGJADIgEAKggIBBDF-OSBASoICAMQ6sjagAEyCwgEEMX45IEBGIAKOPSSmKABQiCS_v2nck6TzNQBb8jy97QPdA
    [HTTP request 3/7]
    [Prev request in frame: 7681]
    [Response in frame: 25165]
    [Next request in frame: 25166]
```

```
0030  00 3f 84 05 00 00 47 45  54 20 2f 52 2f 41 33 73   ·?····GE T /R/A3s
0040  4b 49 47 4d 33 4f 47 52  6c 4d 6a 4d 30 59 6a 6b   KIGM3OGR lMjM0Yjk
0050  79 4e 6a 52 6a 4f 47 5a  69 5a 44 4a 6d 4e 6a 6b   yNjRjOGZ iZDJmNjk
0060  33 4d 44 45 35 4f 54 49  35 4f 44 49 32 45 67 51   3MDE5OTI 5ODI2EgQ
0070  49 46 51 67 67 47 4a 41  44 49 67 45 41 4b 67 67   IFQggGJA DIgEAKgg
0080  49 42 42 44 46 2d 4f 53  42 41 53 6f 49 43 41 4d   IBBDF-OS BASoICAM
0090  51 36 73 6a 61 67 41 45  79 43 77 67 45 45 4d 58   Q6sjagAE yCwgEEMX
00a0  34 35 49 45 42 47 49 41  4b 4f 50 53 53 6d 4b 41   45IEBGIA KOPSSmKA
00b0  42 51 69 43 53 5f 76 32  6e 63 6b 36 54 7a 4e 51   BQiCS_v2 nck6TzNQ
```

- Response HTTP



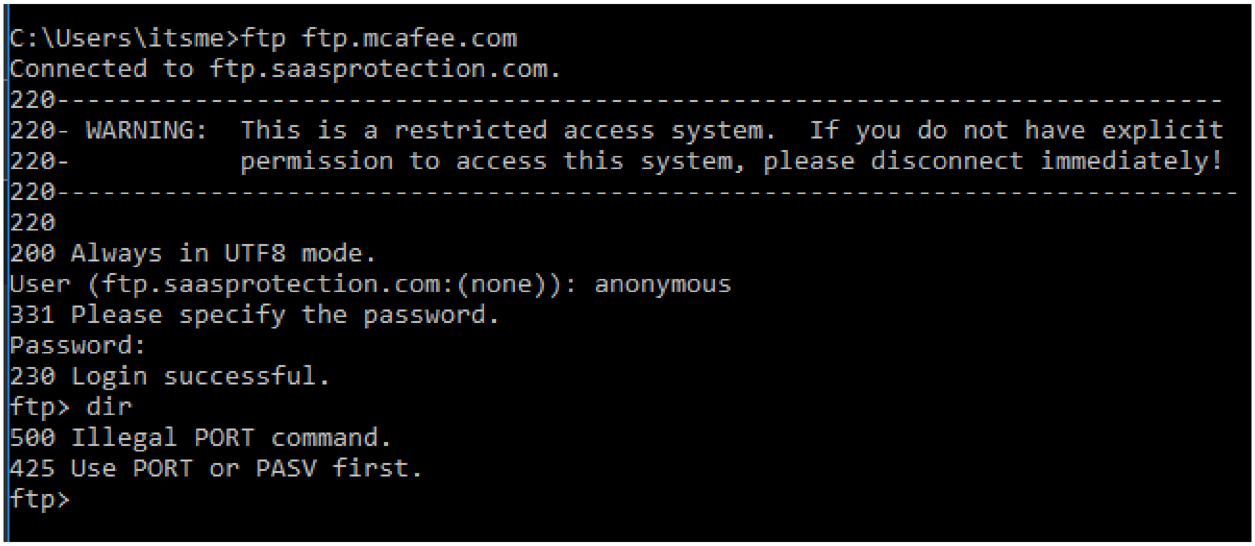
http

```
No.     Time        Source           Destination      Protocol  Length  Info
     2  0.007538    192.168.1.67     65.182.174.11    HTTP         805  GET / HTTP/1.1
    14  0.298612    65.182.174.11    192.168.1.67     HTTP         251  HTTP/1.1 304 Not Modified
    65  1.284857    192.168.1.67     103.41.21.162    HTTP         136  GET /ncc.txt HTTP/1.1
    68  1.299277    103.41.21.162    192.168.1.67     HTTP         205  HTTP/1.1 200 OK  (text/html)
```

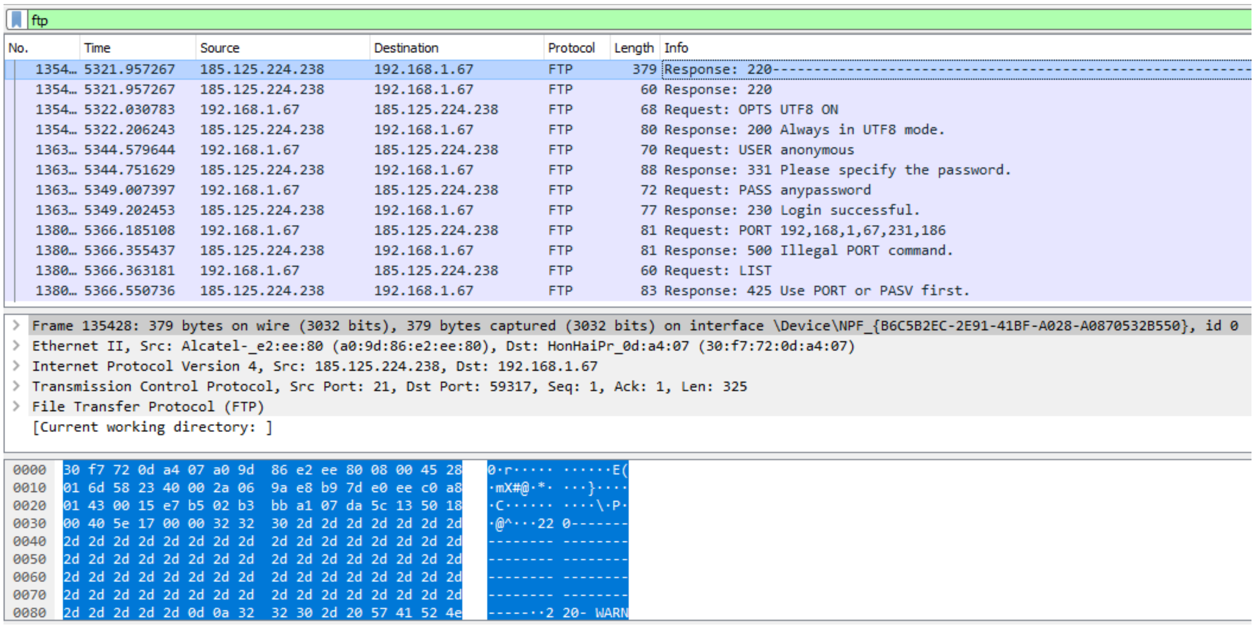
```
v Hypertext Transfer Protocol
  v HTTP/1.1 304 Not Modified\r\n
    v [Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]
        [HTTP/1.1 304 Not Modified\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Response Version: HTTP/1.1
      Status Code: 304
      [Status Code Description: Not Modified]
      Response Phrase: Not Modified
    Server: nginx\r\n
    Date: Sun, 16 Aug 2020 07:18:54 GMT\r\n
    Last-Modified: Thu, 26 Jul 2012 19:37:56 GMT\r\n
    Connection: keep-alive\r\n
    ETag: "50119c94-652"\r\n
    X-Powered-By: PleskLin\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.291074000 seconds]
    [Request in frame: 2]
    [Request URI: http://hmpg.net/]
```

```
0000  30 f7 72 0d a4 07 a0 9d  86 e2 ee 80 08 00 45 20   0·r····· ······E
0010  00 ed 54 36 40 00 2b 06  49 08 41 b6 ae 0b c0 a8   ··T6@·+· I·A·····
0020  01 43 00 50 e2 28 59 35  a1 e4 d3 50 3e f9 50 18   ·C·P·(Y5 ···P>·P·
0030  01 09 88 45 00 00 48 54  54 50 2f 31 2e 31 20 33   ···E··HT TP/1.1 3
0040  30 34 20 4e 6f 74 20 4d  6f 64 69 66 69 65 64 0d   04 Not M odified·
0050  0a 53 65 72 76 65 72 3a  20 6e 67 69 6e 78 0d 0a   ·Server:  nginx··
0060  44 61 74 65 3a 20 53 75  6e 2c 20 31 36 20 41 75   Date: Su n, 16 Au
0070  67 20 32 30 32 30 20 30  37 3a 31 38 3a 35 34 20   g 2020 0 7:18:54 
0080  47 4d 54 0d 0a 4c 61 73  74 2d 4d 6f 64 69 66 69   GMT··Las t-Modifi
```

C. FTP



```
C:\Users\itsme>ftp ftp.mcafee.com
Connected to ftp.saasprotection.com.
220----------------------------------------------------------------------------
220- WARNING:  This is a restricted access system.  If you do not have explicit
220-           permission to access this system, please disconnect immediately!
220-----------------------------------------------------------------------------
220
200 Always in UTF8 mode.
User (ftp.saasprotection.com:(none)): anonymous
331 Please specify the password.
Password:
230 Login successful.
ftp> dir
500 Illegal PORT command.
425 Use PORT or PASV first.
ftp>
```

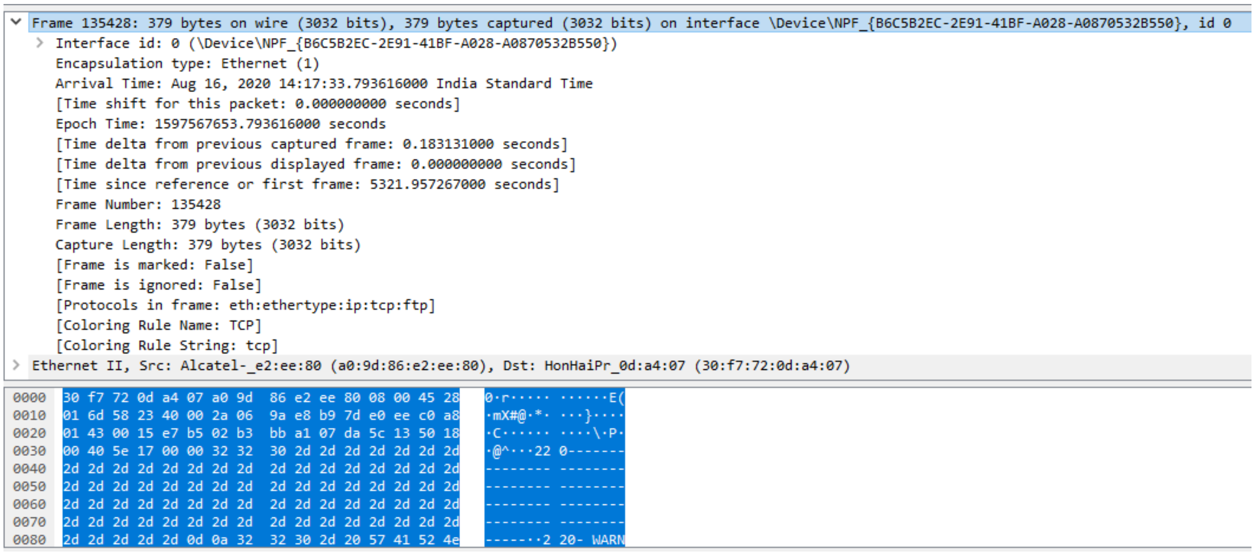


No.	Time	Source	Destination	Protocol	Length	Info
1354…	5321.957267	185.125.224.238	192.168.1.67	FTP	379	Response: 220--
1354…	5321.957267	185.125.224.238	192.168.1.67	FTP	60	Response: 220
1354…	5322.030783	192.168.1.67	185.125.224.238	FTP	68	Request: OPTS UTF8 ON
1354…	5322.206243	185.125.224.238	192.168.1.67	FTP	80	Response: 200 Always in UTF8 mode.
1363…	5344.579644	192.168.1.67	185.125.224.238	FTP	70	Request: USER anonymous
1363…	5344.751629	185.125.224.238	192.168.1.67	FTP	88	Response: 331 Please specify the password.
1363…	5349.007397	192.168.1.67	185.125.224.238	FTP	72	Request: PASS anypassword
1363…	5349.202453	185.125.224.238	192.168.1.67	FTP	77	Response: 230 Login successful.
1380…	5366.185108	192.168.1.67	185.125.224.238	FTP	81	Request: PORT 192,168,1,67,231,186
1380…	5366.355437	185.125.224.238	192.168.1.67	FTP	81	Response: 500 Illegal PORT command.
1380…	5366.363181	192.168.1.67	185.125.224.238	FTP	60	Request: LIST
1380…	5366.550736	185.125.224.238	192.168.1.67	FTP	83	Response: 425 Use PORT or PASV first.

```
> Frame 135428: 379 bytes on wire (3032 bits), 379 bytes captured (3032 bits) on interface \Device\NPF_{B6C5B2EC-2E91-41BF-A028-A0870532B550}, id 0
> Ethernet II, Src: Alcatel-_e2:ee:80 (a0:9d:86:e2:ee:80), Dst: HonHaiPr_0d:a4:07 (30:f7:72:0d:a4:07)
> Internet Protocol Version 4, Src: 185.125.224.238, Dst: 192.168.1.67
> Transmission Control Protocol, Src Port: 21, Dst Port: 59317, Seq: 1, Ack: 1, Len: 325
> File Transfer Protocol (FTP)
  [Current working directory: ]
```

```
0000  30 f7 72 0d a4 07 a0 9d  86 e2 ee 80 08 00 45 28   0·r····· ······E(
0010  01 6d 58 23 40 00 2a 06  9a e8 b9 7d e0 ee c0 a8   ·mX#@·*· ···}····
0020  01 43 00 15 e7 b5 02 b3  bb a1 07 da 5c 13 50 18   ·C······ ····\·P·
0030  00 40 5e 17 00 00 32 32  30 2d 2d 2d 2d 2d 2d 2d   ·@^···22 0-------
0040  2d 2d 2d 2d 2d 2d 2d 2d  2d 2d 2d 2d 2d 2d 2d 2d   -------- --------
0050  2d 2d 2d 2d 2d 2d 2d 2d  2d 2d 2d 2d 2d 2d 2d 2d   -------- --------
0060  2d 2d 2d 2d 2d 2d 2d 2d  2d 2d 2d 2d 2d 2d 2d 2d   -------- --------
0070  2d 2d 2d 2d 2d 2d 2d 2d  2d 2d 2d 2d 2d 2d 2d 2d   -------- --------
0080  2d 2d 2d 2d 2d 0d 0a 32  32 30 2d 20 57 41 52 4e   -----··2 20- WARN
```

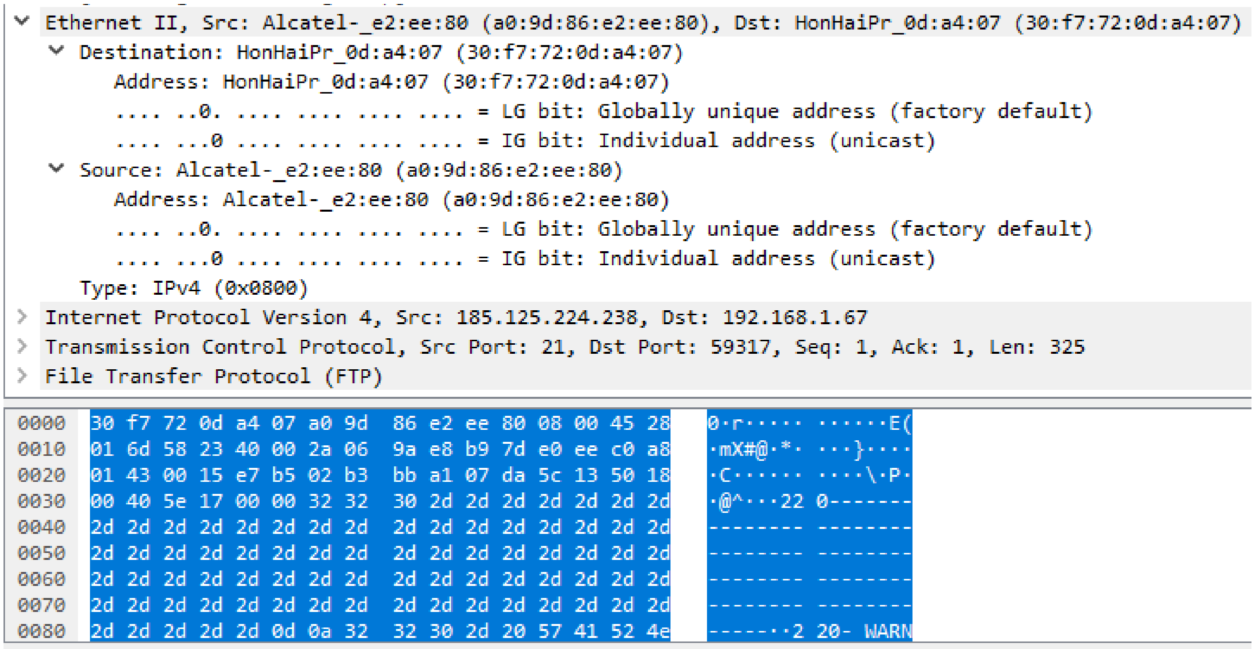
- Describes some basic information about frame.



```
∨ Frame 135428: 379 bytes on wire (3032 bits), 379 bytes captured (3032 bits) on interface \Device\NPF_{B6C5B2EC-2E91-41BF-A028-A0870532B550}, id 0
  > Interface id: 0 (\Device\NPF_{B6C5B2EC-2E91-41BF-A028-A0870532B550})
    Encapsulation type: Ethernet (1)
    Arrival Time: Aug 16, 2020 14:17:33.793616000 India Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1597567653.793616000 seconds
    [Time delta from previous captured frame: 0.183131000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 5321.957267000 seconds]
    Frame Number: 135428
    Frame Length: 379 bytes (3032 bits)
    Capture Length: 379 bytes (3032 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:ftp]
    [Coloring Rule Name: TCP]
    [Coloring Rule String: tcp]
> Ethernet II, Src: Alcatel-_e2:ee:80 (a0:9d:86:e2:ee:80), Dst: HonHaiPr_0d:a4:07 (30:f7:72:0d:a4:07)
```

```
0000  30 f7 72 0d a4 07 a0 9d  86 e2 ee 80 08 00 45 28   0·r····· ······E(
0010  01 6d 58 23 40 00 2a 06  9a e8 b9 7d e0 ee c0 a8   ·mX#@·*· ···}····
0020  01 43 00 15 e7 b5 02 b3  bb a1 07 da 5c 13 50 18   ·C······ ····\·P·
0030  00 40 5e 17 00 00 32 32  30 2d 2d 2d 2d 2d 2d 2d   ·@^···22 0-------
0040  2d 2d 2d 2d 2d 2d 2d 2d  2d 2d 2d 2d 2d 2d 2d 2d   -------- --------
0050  2d 2d 2d 2d 2d 2d 2d 2d  2d 2d 2d 2d 2d 2d 2d 2d   -------- --------
0060  2d 2d 2d 2d 2d 2d 2d 2d  2d 2d 2d 2d 2d 2d 2d 2d   -------- --------
0070  2d 2d 2d 2d 2d 2d 2d 2d  2d 2d 2d 2d 2d 2d 2d 2d   -------- --------
0080  2d 2d 2d 2d 2d 0d 0a 32  32 30 2d 20 57 41 52 4e   ------·2 20- WARN
```

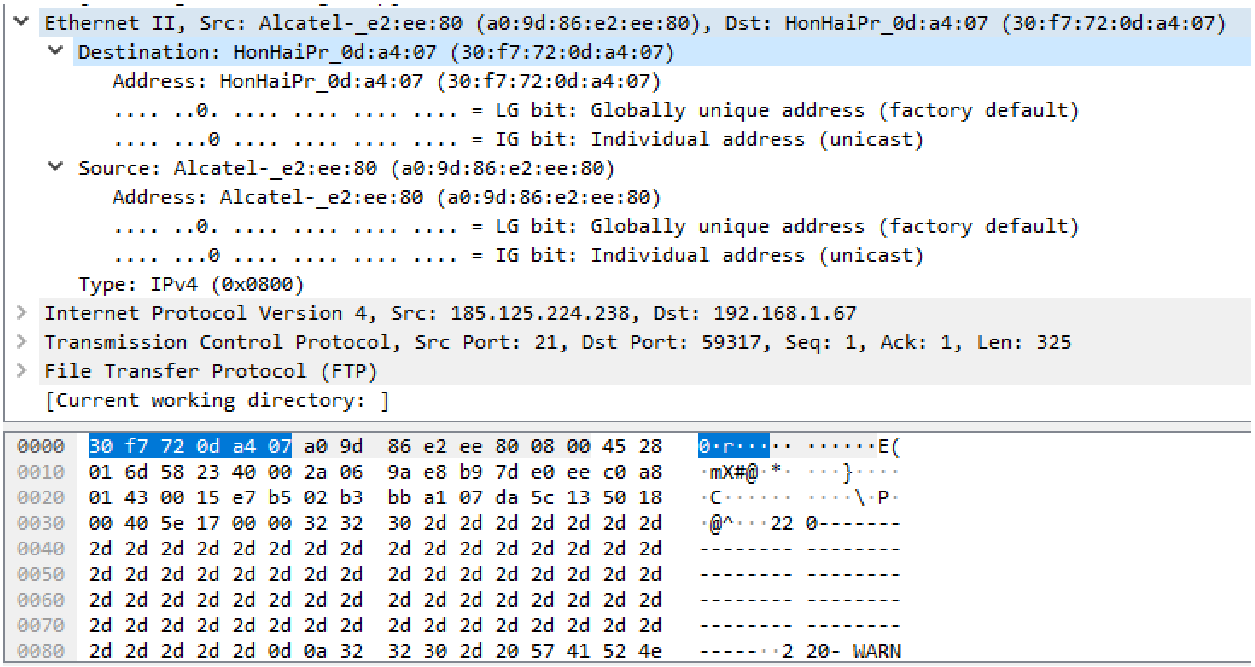
- Describes the MAC information associated with the frame.



```
∨ Ethernet II, Src: Alcatel-_e2:ee:80 (a0:9d:86:e2:ee:80), Dst: HonHaiPr_0d:a4:07 (30:f7:72:0d:a4:07)
  ∨ Destination: HonHaiPr_0d:a4:07 (30:f7:72:0d:a4:07)
      Address: HonHaiPr_0d:a4:07 (30:f7:72:0d:a4:07)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ∨ Source: Alcatel-_e2:ee:80 (a0:9d:86:e2:ee:80)
      Address: Alcatel-_e2:ee:80 (a0:9d:86:e2:ee:80)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 185.125.224.238, Dst: 192.168.1.67
> Transmission Control Protocol, Src Port: 21, Dst Port: 59317, Seq: 1, Ack: 1, Len: 325
> File Transfer Protocol (FTP)
```

```
0000  30 f7 72 0d a4 07 a0 9d  86 e2 ee 80 08 00 45 28   0·r····· ······E(
0010  01 6d 58 23 40 00 2a 06  9a e8 b9 7d e0 ee c0 a8   ·mX#@·*· ···}····
0020  01 43 00 15 e7 b5 02 b3  bb a1 07 da 5c 13 50 18   ·C······ ····\·P·
0030  00 40 5e 17 00 00 32 32  30 2d 2d 2d 2d 2d 2d 2d   ·@^···22 0-------
0040  2d 2d 2d 2d 2d 2d 2d 2d  2d 2d 2d 2d 2d 2d 2d 2d   -------- --------
0050  2d 2d 2d 2d 2d 2d 2d 2d  2d 2d 2d 2d 2d 2d 2d 2d   -------- --------
0060  2d 2d 2d 2d 2d 2d 2d 2d  2d 2d 2d 2d 2d 2d 2d 2d   -------- --------
0070  2d 2d 2d 2d 2d 2d 2d 2d  2d 2d 2d 2d 2d 2d 2d 2d   -------- --------
0080  2d 2d 2d 2d 2d 0d 0a 32  32 30 2d 20 57 41 52 4e   ------·2 20- WARN
```

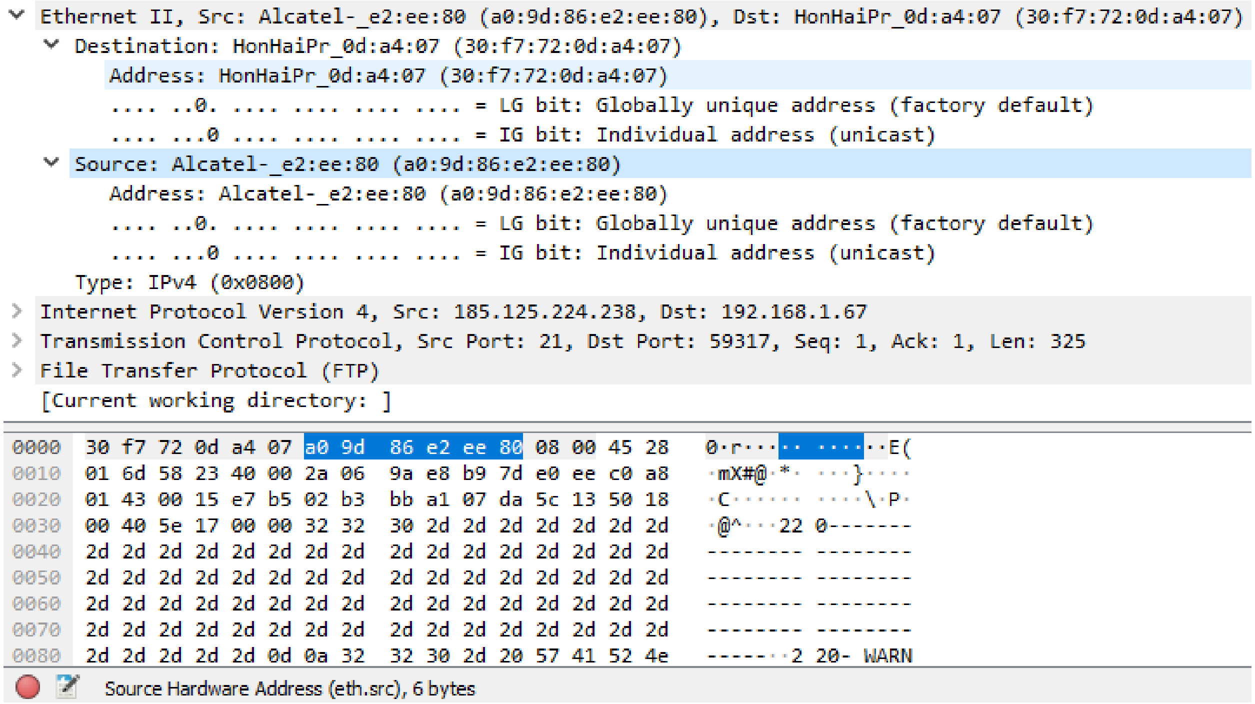
- Destination MAC address information (30:f7:72:0d:a4:07). It's the MAC address of Device this response is going to.



```
v Ethernet II, Src: Alcatel-_e2:ee:80 (a0:9d:86:e2:ee:80), Dst: HonHaiPr_0d:a4:07 (30:f7:72:0d:a4:07)
  v Destination: HonHaiPr_0d:a4:07 (30:f7:72:0d:a4:07)
      Address: HonHaiPr_0d:a4:07 (30:f7:72:0d:a4:07)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  v Source: Alcatel-_e2:ee:80 (a0:9d:86:e2:ee:80)
      Address: Alcatel-_e2:ee:80 (a0:9d:86:e2:ee:80)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 185.125.224.238, Dst: 192.168.1.67
> Transmission Control Protocol, Src Port: 21, Dst Port: 59317, Seq: 1, Ack: 1, Len: 325
> File Transfer Protocol (FTP)
  [Current working directory: ]
```

```
0000  30 f7 72 0d a4 07 a0 9d  86 e2 ee 80 08 00 45 28   0·r····· ······E(
0010  01 6d 58 23 40 00 2a 06  9a e8 b9 7d e0 ee c0 a8   ·mX#@·*· ···}····
0020  01 43 00 15 e7 b5 02 b3  bb a1 07 da 5c 13 50 18   ·C······ ····\·P·
0030  00 40 5e 17 00 00 32 32  30 2d 2d 2d 2d 2d 2d 2d   ·@^···22 0-------
0040  2d 2d 2d 2d 2d 2d 2d 2d  2d 2d 2d 2d 2d 2d 2d 2d   -------- --------
0050  2d 2d 2d 2d 2d 2d 2d 2d  2d 2d 2d 2d 2d 2d 2d 2d   -------- --------
0060  2d 2d 2d 2d 2d 2d 2d 2d  2d 2d 2d 2d 2d 2d 2d 2d   -------- --------
0070  2d 2d 2d 2d 2d 2d 2d 2d  2d 2d 2d 2d 2d 2d 2d 2d   -------- --------
0080  2d 2d 2d 2d 2d 0d 0a 32  32 30 2d 20 57 41 52 4e   -----··2 20- WARN
```

- Source MAC address information (a0:9d:86:e2:ee:80). It's the MAC address of the Router or Gateway as no one is allowed to go beyond the Gateway for MAC address.

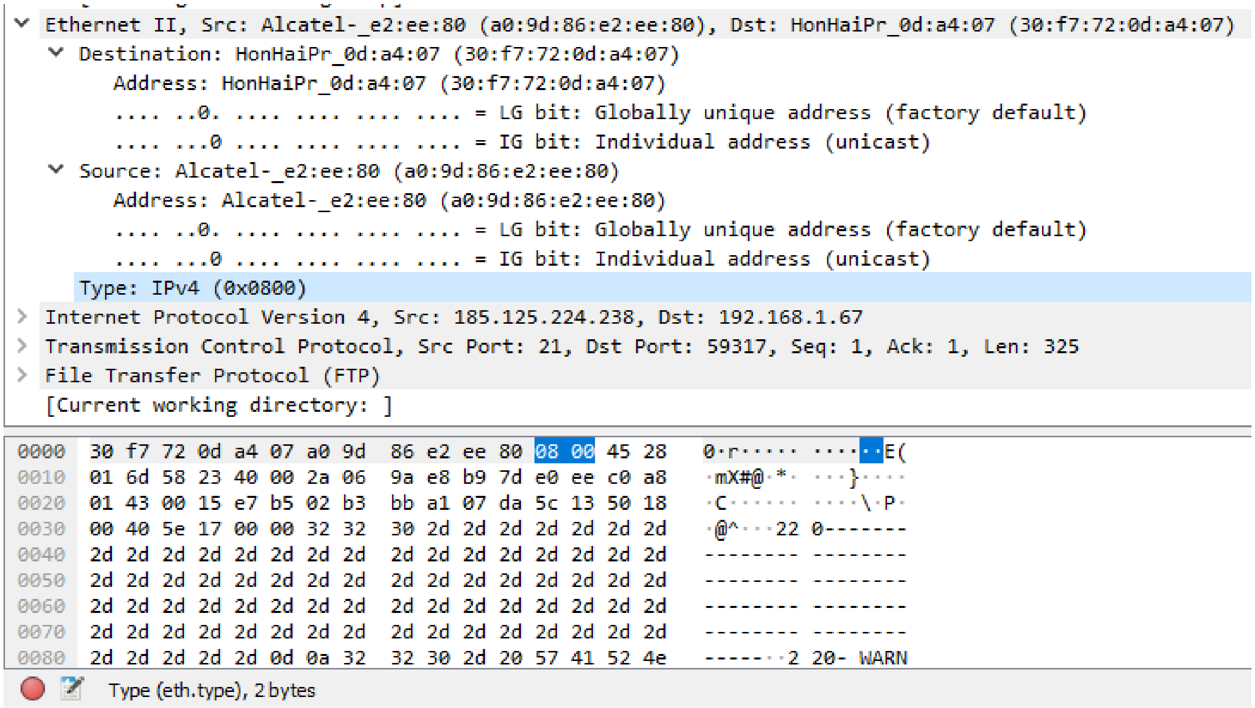


```
v Ethernet II, Src: Alcatel-_e2:ee:80 (a0:9d:86:e2:ee:80), Dst: HonHaiPr_0d:a4:07 (30:f7:72:0d:a4:07)
  v Destination: HonHaiPr_0d:a4:07 (30:f7:72:0d:a4:07)
      Address: HonHaiPr_0d:a4:07 (30:f7:72:0d:a4:07)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  v Source: Alcatel-_e2:ee:80 (a0:9d:86:e2:ee:80)
      Address: Alcatel-_e2:ee:80 (a0:9d:86:e2:ee:80)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 185.125.224.238, Dst: 192.168.1.67
> Transmission Control Protocol, Src Port: 21, Dst Port: 59317, Seq: 1, Ack: 1, Len: 325
> File Transfer Protocol (FTP)
  [Current working directory: ]
```

```
0000  30 f7 72 0d a4 07 a0 9d  86 e2 ee 80 08 00 45 28   0·r····· ······E(
0010  01 6d 58 23 40 00 2a 06  9a e8 b9 7d e0 ee c0 a8   ·mX#@·*· ···}····
0020  01 43 00 15 e7 b5 02 b3  bb a1 07 da 5c 13 50 18   ·C······ ····\·P·
0030  00 40 5e 17 00 00 32 32  30 2d 2d 2d 2d 2d 2d 2d   ·@^···22 0-------
0040  2d 2d 2d 2d 2d 2d 2d 2d  2d 2d 2d 2d 2d 2d 2d 2d   -------- --------
0050  2d 2d 2d 2d 2d 2d 2d 2d  2d 2d 2d 2d 2d 2d 2d 2d   -------- --------
0060  2d 2d 2d 2d 2d 2d 2d 2d  2d 2d 2d 2d 2d 2d 2d 2d   -------- --------
0070  2d 2d 2d 2d 2d 2d 2d 2d  2d 2d 2d 2d 2d 2d 2d 2d   -------- --------
0080  2d 2d 2d 2d 2d 0d 0a 32  32 30 2d 20 57 41 52 4e   -----··2 20- WARN
```

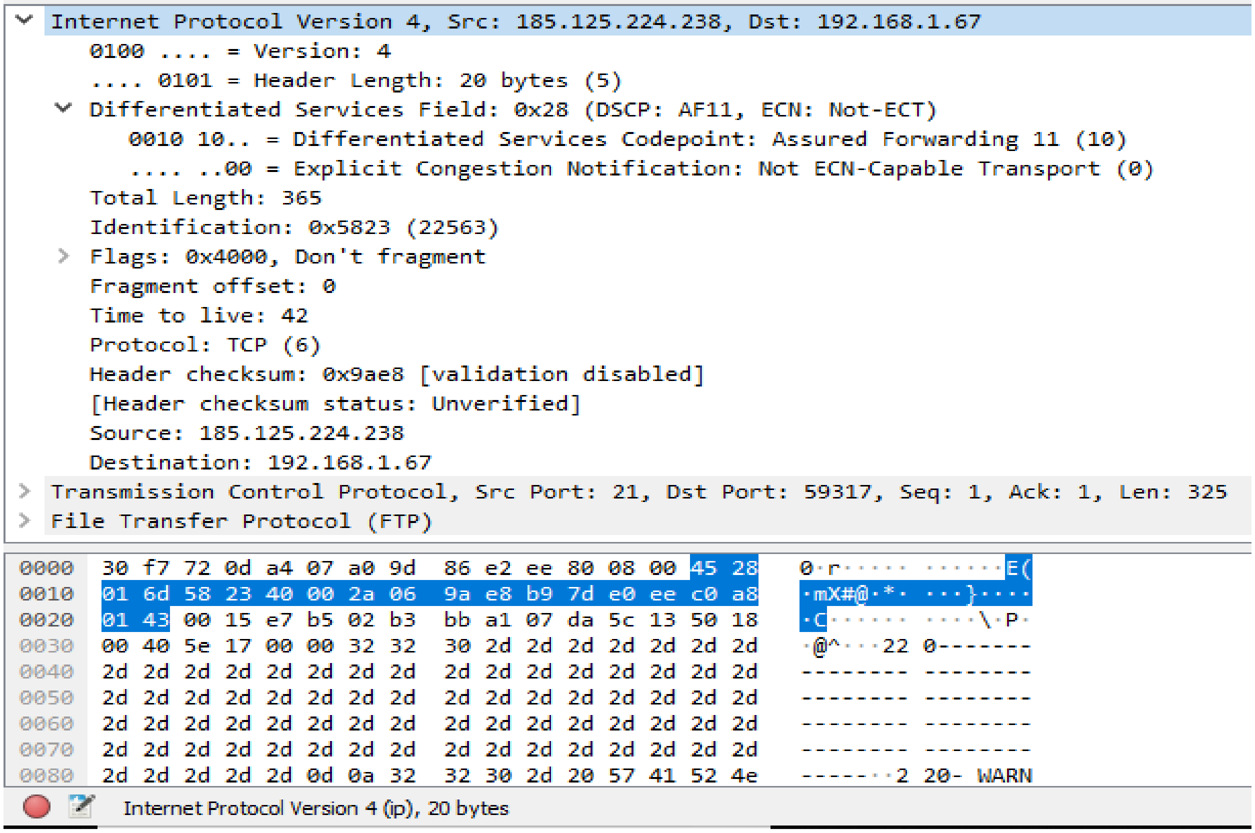
Source Hardware Address (eth.src), 6 bytes

- Ethernet type



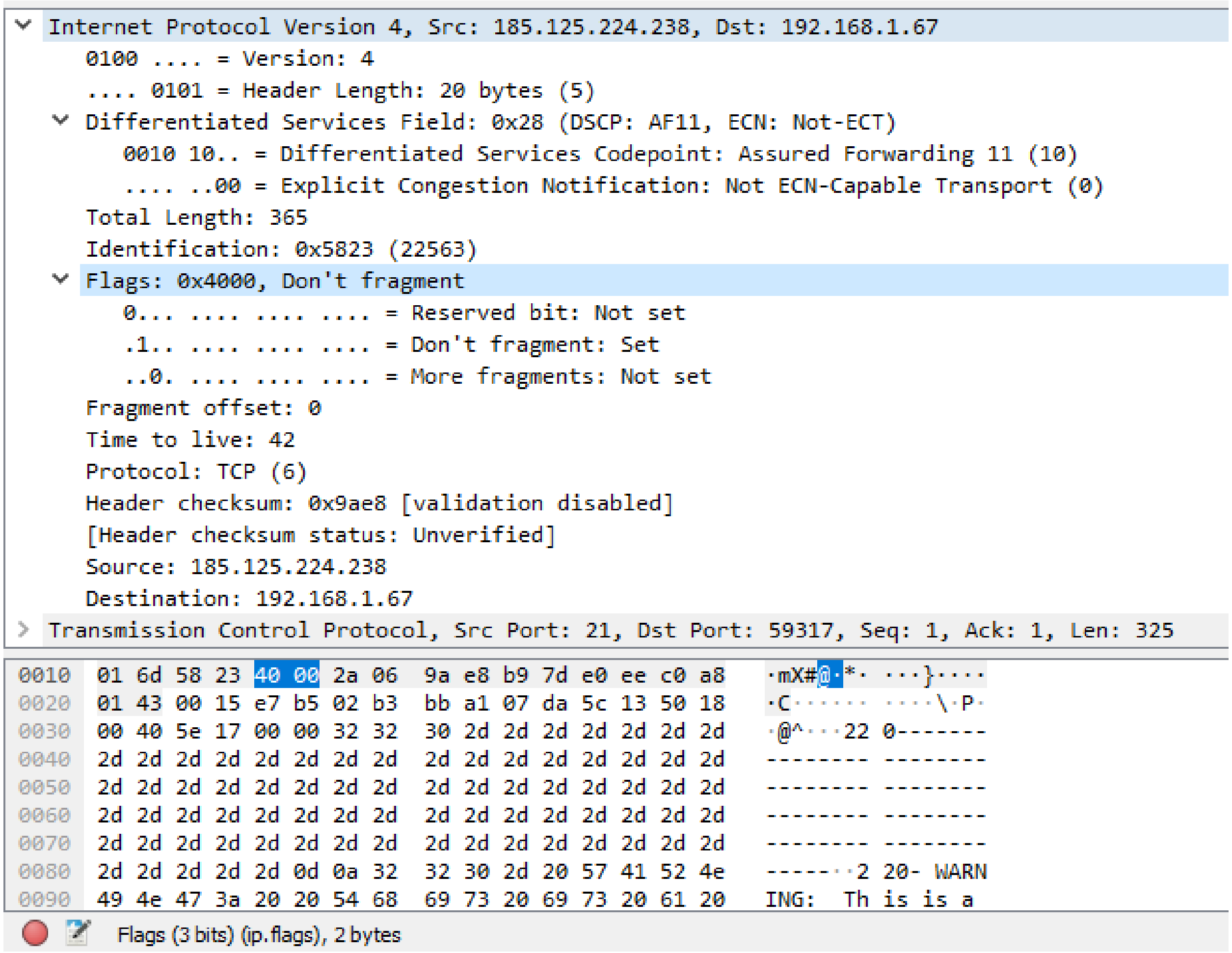
```
v Ethernet II, Src: Alcatel-_e2:ee:80 (a0:9d:86:e2:ee:80), Dst: HonHaiPr_0d:a4:07 (30:f7:72:0d:a4:07)
  v Destination: HonHaiPr_0d:a4:07 (30:f7:72:0d:a4:07)
      Address: HonHaiPr_0d:a4:07 (30:f7:72:0d:a4:07)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  v Source: Alcatel-_e2:ee:80 (a0:9d:86:e2:ee:80)
      Address: Alcatel-_e2:ee:80 (a0:9d:86:e2:ee:80)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 185.125.224.238, Dst: 192.168.1.67
> Transmission Control Protocol, Src Port: 21, Dst Port: 59317, Seq: 1, Ack: 1, Len: 325
> File Transfer Protocol (FTP)
  [Current working directory: ]

0000  30 f7 72 0d a4 07 a0 9d  86 e2 ee 80 08 00 45 28   0·r·····  ······E(
0010  01 6d 58 23 40 00 2a 06  9a e8 b9 7d e0 ee c0 a8   ·mX#@·*·  ···}····
0020  01 43 00 15 e7 b5 02 b3  bb a1 07 da 5c 13 50 18   ·C······  ····\·P·
0030  00 40 5e 17 00 00 32 32  30 2d 2d 2d 2d 2d 2d 2d   ·@^···22  0-------
0040  2d 2d 2d 2d 2d 2d 2d 2d  2d 2d 2d 2d 2d 2d 2d 2d   --------  --------
0050  2d 2d 2d 2d 2d 2d 2d 2d  2d 2d 2d 2d 2d 2d 2d 2d   --------  --------
0060  2d 2d 2d 2d 2d 2d 2d 2d  2d 2d 2d 2d 2d 2d 2d 2d   --------  --------
0070  2d 2d 2d 2d 2d 2d 2d 2d  2d 2d 2d 2d 2d 2d 2d 2d   --------  --------
0080  2d 2d 2d 2d 2d 0d 0a 32  32 30 2d 20 57 41 52 4e   -----··2  20- WARN

Type (eth.type), 2 bytes
```

- IPv4 information



```
v Internet Protocol Version 4, Src: 185.125.224.238, Dst: 192.168.1.67
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  v Differentiated Services Field: 0x28 (DSCP: AF11, ECN: Not-ECT)
      0010 10.. = Differentiated Services Codepoint: Assured Forwarding 11 (10)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 365
    Identification: 0x5823 (22563)
  > Flags: 0x4000, Don't fragment
    Fragment offset: 0
    Time to live: 42
    Protocol: TCP (6)
    Header checksum: 0x9ae8 [validation disabled]
    [Header checksum status: Unverified]
    Source: 185.125.224.238
    Destination: 192.168.1.67
> Transmission Control Protocol, Src Port: 21, Dst Port: 59317, Seq: 1, Ack: 1, Len: 325
> File Transfer Protocol (FTP)

0000  30 f7 72 0d a4 07 a0 9d  86 e2 ee 80 08 00 45 28   0·r·····  ······E(
0010  01 6d 58 23 40 00 2a 06  9a e8 b9 7d e0 ee c0 a8   ·mX#@·*·  ···}····
0020  01 43 00 15 e7 b5 02 b3  bb a1 07 da 5c 13 50 18   ·C······  ····\·P·
0030  00 40 5e 17 00 00 32 32  30 2d 2d 2d 2d 2d 2d 2d   ·@^···22  0-------
0040  2d 2d 2d 2d 2d 2d 2d 2d  2d 2d 2d 2d 2d 2d 2d 2d   --------  --------
0050  2d 2d 2d 2d 2d 2d 2d 2d  2d 2d 2d 2d 2d 2d 2d 2d   --------  --------
0060  2d 2d 2d 2d 2d 2d 2d 2d  2d 2d 2d 2d 2d 2d 2d 2d   --------  --------
0070  2d 2d 2d 2d 2d 2d 2d 2d  2d 2d 2d 2d 2d 2d 2d 2d   --------  --------
0080  2d 2d 2d 2d 2d 0d 0a 32  32 30 2d 20 57 41 52 4e   -----··2  20- WARN

Internet Protocol Version 4 (ip), 20 bytes
```

- This section describes the information, first the IP version, then the header length, then some other helpful information with IP flags, TTL (Number of hops jumped by frame), Protocol an transport layer (TCP), Header checksum (to check if the frame is not damaged or distorted).

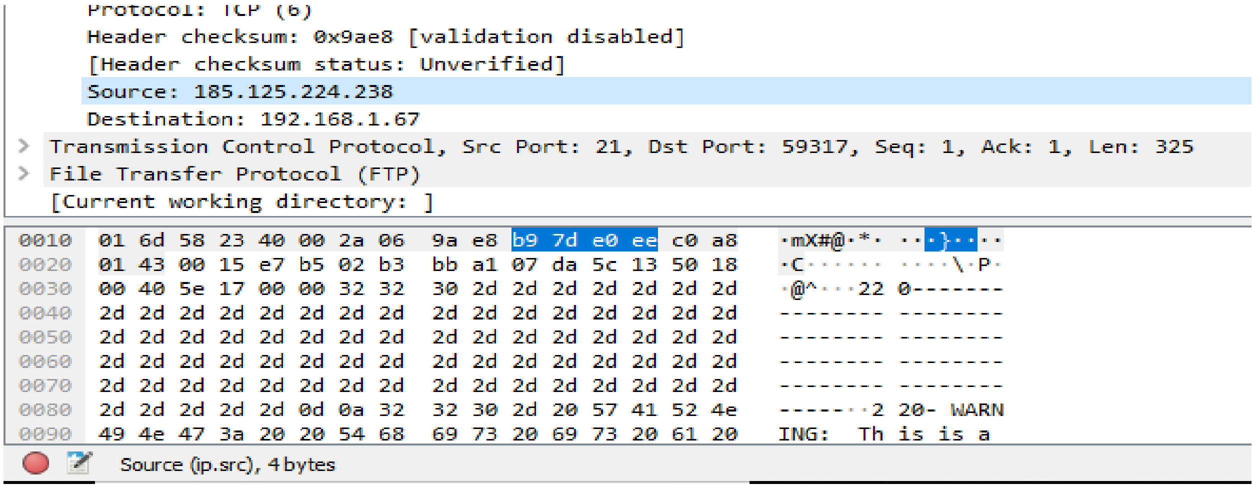


```
v Internet Protocol Version 4, Src: 185.125.224.238, Dst: 192.168.1.67
     0100 .... = Version: 4
     .... 0101 = Header Length: 20 bytes (5)
  v  Differentiated Services Field: 0x28 (DSCP: AF11, ECN: Not-ECT)
        0010 10.. = Differentiated Services Codepoint: Assured Forwarding 11 (10)
        .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
     Total Length: 365
     Identification: 0x5823 (22563)
  v  Flags: 0x4000, Don't fragment
        0... .... .... .... = Reserved bit: Not set
        .1.. .... .... .... = Don't fragment: Set
        ..0. .... .... .... = More fragments: Not set
     Fragment offset: 0
     Time to live: 42
     Protocol: TCP (6)
     Header checksum: 0x9ae8 [validation disabled]
     [Header checksum status: Unverified]
     Source: 185.125.224.238
     Destination: 192.168.1.67
> Transmission Control Protocol, Src Port: 21, Dst Port: 59317, Seq: 1, Ack: 1, Len: 325
```

```
0010  01 6d 58 23 40 00 2a 06  9a e8 b9 7d e0 ee c0 a8   ·mX#@·*·  ···}····
0020  01 43 00 15 e7 b5 02 b3  bb a1 07 da 5c 13 50 18   ·C······  ····\·P·
0030  00 40 5e 17 00 00 32 32  30 2d 2d 2d 2d 2d 2d 2d   ·@^···22  0-------
0040  2d 2d 2d 2d 2d 2d 2d 2d  2d 2d 2d 2d 2d 2d 2d 2d   --------  --------
0050  2d 2d 2d 2d 2d 2d 2d 2d  2d 2d 2d 2d 2d 2d 2d 2d   --------  --------
0060  2d 2d 2d 2d 2d 2d 2d 2d  2d 2d 2d 2d 2d 2d 2d 2d   --------  --------
0070  2d 2d 2d 2d 2d 2d 2d 2d  2d 2d 2d 2d 2d 2d 2d 2d   --------  --------
0080  2d 2d 2d 2d 2d 0d 0a 32  32 30 2d 20 57 41 52 4e   -----··2  20- WARN
0090  49 4e 47 3a 20 20 54 68  69 73 20 69 73 20 61 20   ING:  Th  is is a
```

Flags (3 bits) (ip.flags), 2 bytes

- Source IP address (185:125:224:238). This is the IP of ftp.mcafee.com → sender

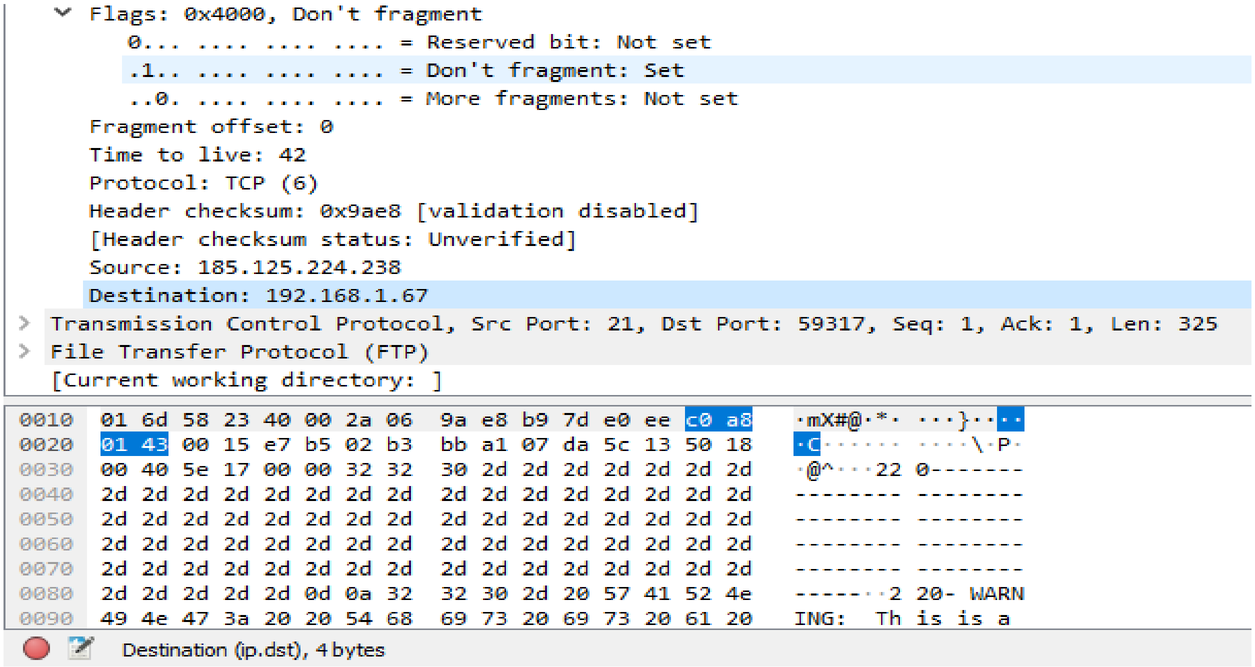


```
     Protocol: TCP (6)
     Header checksum: 0x9ae8 [validation disabled]
     [Header checksum status: Unverified]
     Source: 185.125.224.238
     Destination: 192.168.1.67
> Transmission Control Protocol, Src Port: 21, Dst Port: 59317, Seq: 1, Ack: 1, Len: 325
> File Transfer Protocol (FTP)
  [Current working directory: ]
```

```
0010  01 6d 58 23 40 00 2a 06  9a e8 b9 7d e0 ee c0 a8   ·mX#@·*·  ···}····
0020  01 43 00 15 e7 b5 02 b3  bb a1 07 da 5c 13 50 18   ·C······  ····\·P·
0030  00 40 5e 17 00 00 32 32  30 2d 2d 2d 2d 2d 2d 2d   ·@^···22  0-------
0040  2d 2d 2d 2d 2d 2d 2d 2d  2d 2d 2d 2d 2d 2d 2d 2d   --------  --------
0050  2d 2d 2d 2d 2d 2d 2d 2d  2d 2d 2d 2d 2d 2d 2d 2d   --------  --------
0060  2d 2d 2d 2d 2d 2d 2d 2d  2d 2d 2d 2d 2d 2d 2d 2d   --------  --------
0070  2d 2d 2d 2d 2d 2d 2d 2d  2d 2d 2d 2d 2d 2d 2d 2d   --------  --------
0080  2d 2d 2d 2d 2d 0d 0a 32  32 30 2d 20 57 41 52 4e   -----··2  20- WARN
0090  49 4e 47 3a 20 20 54 68  69 73 20 69 73 20 61 20   ING:  Th  is is a
```

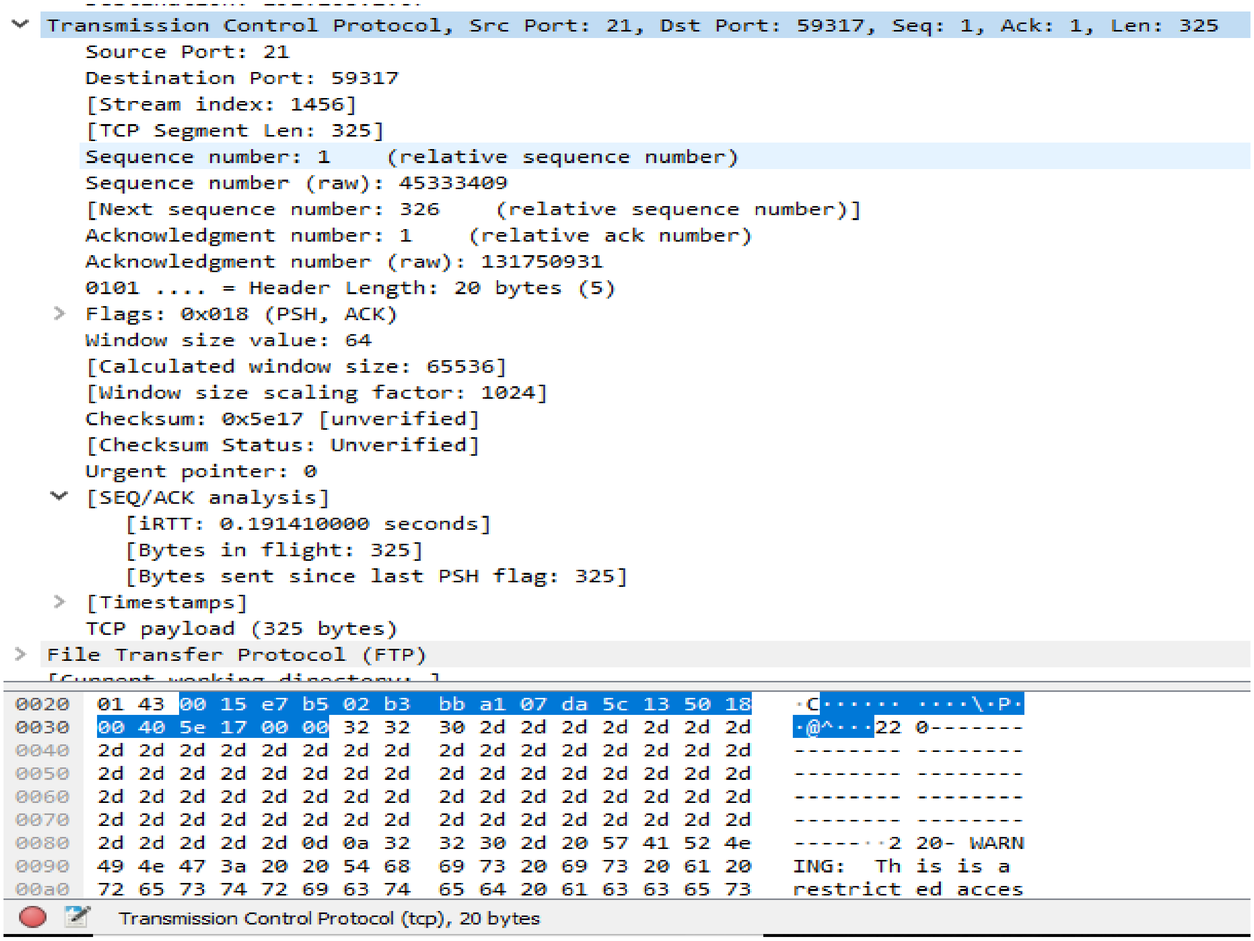
Source (ip.src), 4 bytes

- Destination IP address (192.168.1.67). this is the IP address of device getting the response.



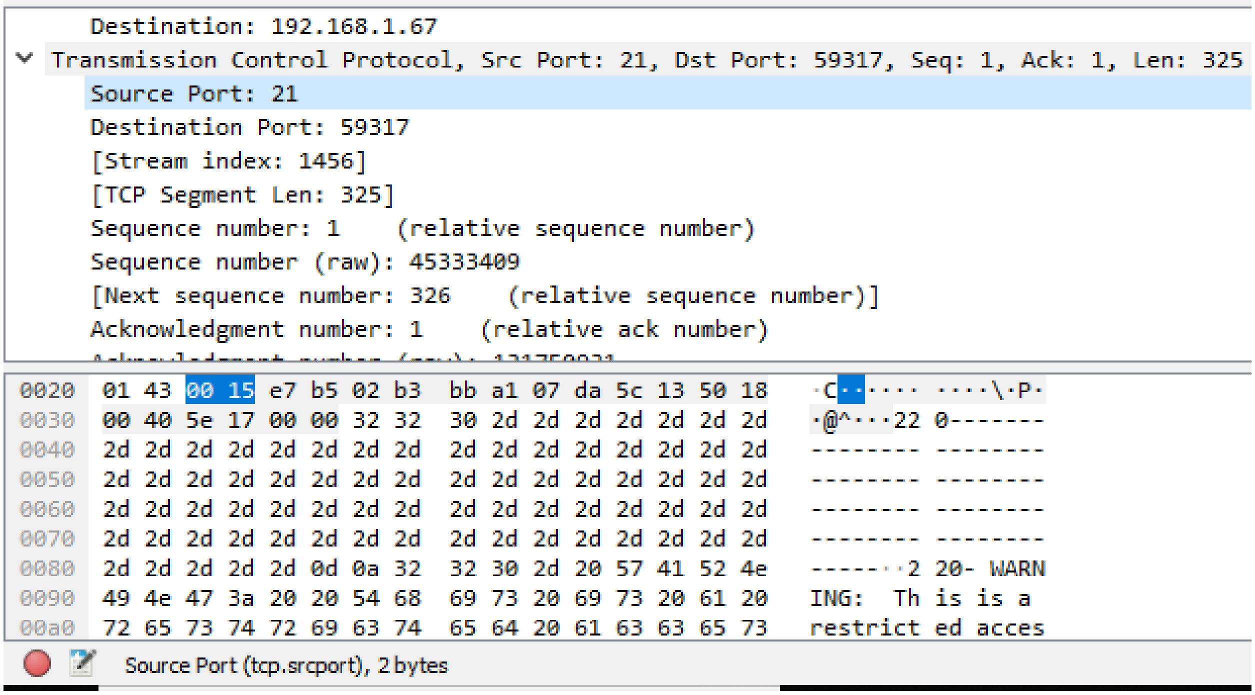
```
    Flags: 0x4000, Don't fragment
        0... .... .... .... = Reserved bit: Not set
        .1.. .... .... .... = Don't fragment: Set
        ..0. .... .... .... = More fragments: Not set
    Fragment offset: 0
    Time to live: 42
    Protocol: TCP (6)
    Header checksum: 0x9ae8 [validation disabled]
    [Header checksum status: Unverified]
    Source: 185.125.224.238
    Destination: 192.168.1.67
> Transmission Control Protocol, Src Port: 21, Dst Port: 59317, Seq: 1, Ack: 1, Len: 325
> File Transfer Protocol (FTP)
  [Current working directory: ]

0010  01 6d 58 23 40 00 2a 06  9a e8 b9 7d e0 ee c0 a8   ·mX#@·*·  ···}····
0020  01 43 00 15 e7 b5 02 b3  bb a1 07 da 5c 13 50 18   ·C······ ····\·P·
0030  00 40 5e 17 00 00 32 32  30 2d 2d 2d 2d 2d 2d 2d   ·@^···22 0-------
0040  2d 2d 2d 2d 2d 2d 2d 2d  2d 2d 2d 2d 2d 2d 2d 2d   -------- --------
0050  2d 2d 2d 2d 2d 2d 2d 2d  2d 2d 2d 2d 2d 2d 2d 2d   -------- --------
0060  2d 2d 2d 2d 2d 2d 2d 2d  2d 2d 2d 2d 2d 2d 2d 2d   -------- --------
0070  2d 2d 2d 2d 2d 2d 2d 2d  2d 2d 2d 2d 2d 2d 2d 2d   -------- --------
0080  2d 2d 2d 2d 2d 0d 0a 32  32 30 2d 20 57 41 52 4e   -----··2 20- WARN
0090  49 4e 47 3a 20 20 54 68  69 73 20 69 73 20 61 20   ING:  Th is is a

Destination (ip.dst), 4 bytes
```

- Transmission Control Protocol



```
v Transmission Control Protocol, Src Port: 21, Dst Port: 59317, Seq: 1, Ack: 1, Len: 325
    Source Port: 21
    Destination Port: 59317
    [Stream index: 1456]
    [TCP Segment Len: 325]
    Sequence number: 1    (relative sequence number)
    Sequence number (raw): 45333409
    [Next sequence number: 326    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    Acknowledgment number (raw): 131750931
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window size value: 64
    [Calculated window size: 65536]
    [Window size scaling factor: 1024]
    Checksum: 0x5e17 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  v [SEQ/ACK analysis]
        [iRTT: 0.191410000 seconds]
        [Bytes in flight: 325]
        [Bytes sent since last PSH flag: 325]
  > [Timestamps]
    TCP payload (325 bytes)
> File Transfer Protocol (FTP)
  [Current working directory: ]

0020  01 43 00 15 e7 b5 02 b3  bb a1 07 da 5c 13 50 18   ·C······ ····\·P·
0030  00 40 5e 17 00 00 32 32  30 2d 2d 2d 2d 2d 2d 2d   ·@^···22 0-------
0040  2d 2d 2d 2d 2d 2d 2d 2d  2d 2d 2d 2d 2d 2d 2d 2d   -------- --------
0050  2d 2d 2d 2d 2d 2d 2d 2d  2d 2d 2d 2d 2d 2d 2d 2d   -------- --------
0060  2d 2d 2d 2d 2d 2d 2d 2d  2d 2d 2d 2d 2d 2d 2d 2d   -------- --------
0070  2d 2d 2d 2d 2d 2d 2d 2d  2d 2d 2d 2d 2d 2d 2d 2d   -------- --------
0080  2d 2d 2d 2d 2d 0d 0a 32  32 30 2d 20 57 41 52 4e   -----··2 20- WARN
0090  49 4e 47 3a 20 20 54 68  69 73 20 69 73 20 61 20   ING:  Th is is a
00a0  72 65 73 74 72 69 63 74  65 64 20 61 63 63 65 73   restrict ed acces

Transmission Control Protocol (tcp), 20 bytes
```

- Source port → 21, reserved for ftp

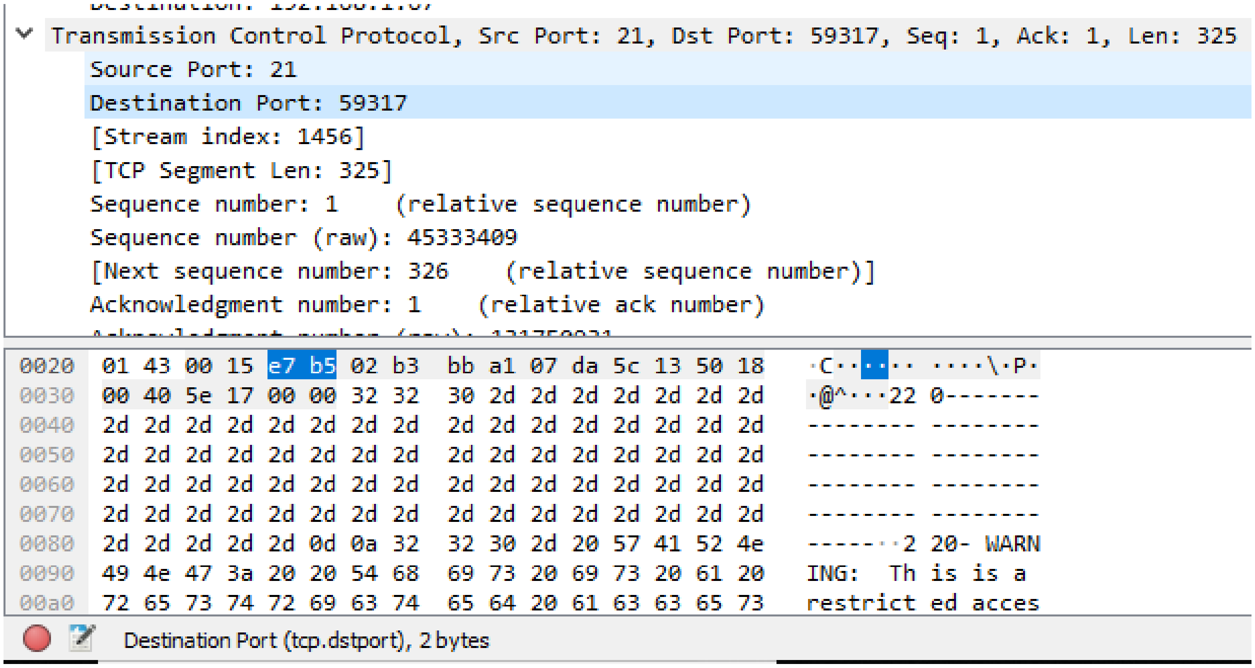


```
    Destination: 192.168.1.67
v Transmission Control Protocol, Src Port: 21, Dst Port: 59317, Seq: 1, Ack: 1, Len: 325
    Source Port: 21
    Destination Port: 59317
    [Stream index: 1456]
    [TCP Segment Len: 325]
    Sequence number: 1    (relative sequence number)
    Sequence number (raw): 45333409
    [Next sequence number: 326    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    Acknowledgment number (raw): 121750021
```

```
0020  01 43 00 15 e7 b5 02 b3  bb a1 07 da 5c 13 50 18   ·C······ ····\·P·
0030  00 40 5e 17 00 00 32 32  30 2d 2d 2d 2d 2d 2d 2d   ·@^···22 0-------
0040  2d 2d 2d 2d 2d 2d 2d 2d  2d 2d 2d 2d 2d 2d 2d 2d   -------- --------
0050  2d 2d 2d 2d 2d 2d 2d 2d  2d 2d 2d 2d 2d 2d 2d 2d   -------- --------
0060  2d 2d 2d 2d 2d 2d 2d 2d  2d 2d 2d 2d 2d 2d 2d 2d   -------- --------
0070  2d 2d 2d 2d 2d 2d 2d 2d  2d 2d 2d 2d 2d 2d 2d 2d   -------- --------
0080  2d 2d 2d 2d 2d 0d 0a 32  32 30 2d 20 57 41 52 4e   -----··2 20- WARN
0090  49 4e 47 3a 20 20 54 68  69 73 20 69 73 20 61 20   ING:  Th is is a
00a0  72 65 73 74 72 69 63 74  65 64 20 61 63 63 65 73   restrict ed acces
```

Source Port (tcp.srcport), 2 bytes

- Destination port, temporary, for my device.

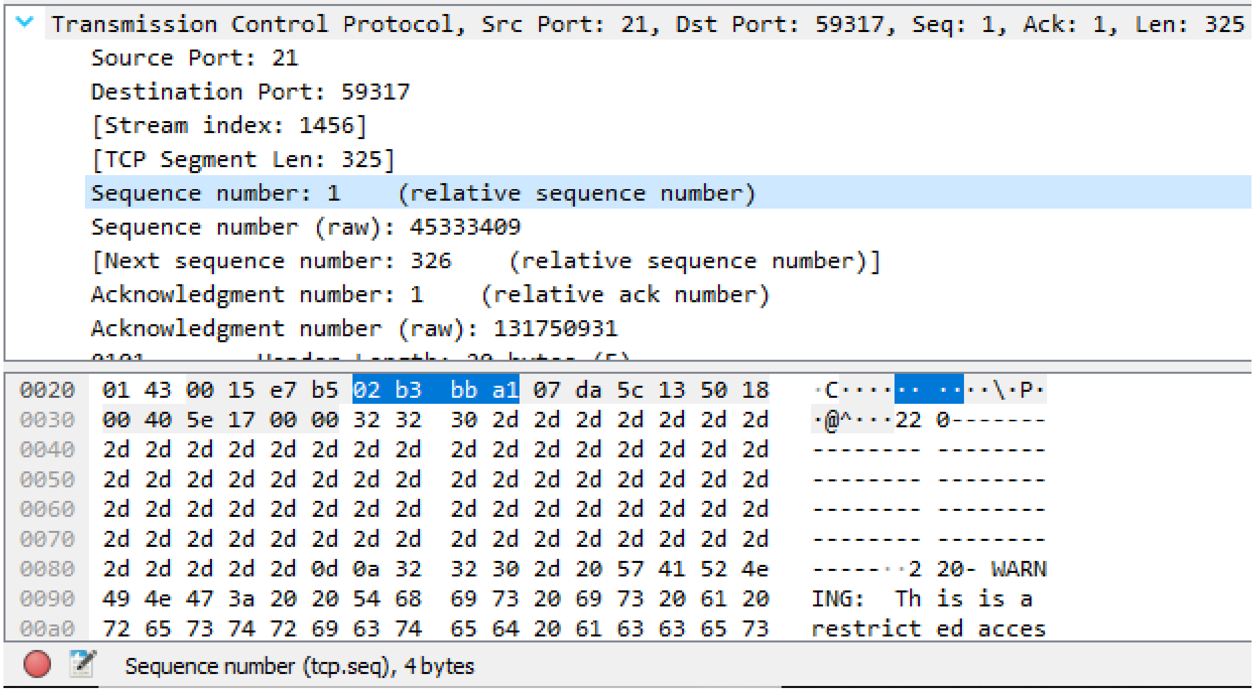


```
    Destination: 192.168.1.67
v Transmission Control Protocol, Src Port: 21, Dst Port: 59317, Seq: 1, Ack: 1, Len: 325
    Source Port: 21
    Destination Port: 59317
    [Stream index: 1456]
    [TCP Segment Len: 325]
    Sequence number: 1    (relative sequence number)
    Sequence number (raw): 45333409
    [Next sequence number: 326    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    Acknowledgment number (raw): 121750021
```

```
0020  01 43 00 15 e7 b5 02 b3  bb a1 07 da 5c 13 50 18   ·C······ ····\·P·
0030  00 40 5e 17 00 00 32 32  30 2d 2d 2d 2d 2d 2d 2d   ·@^···22 0-------
0040  2d 2d 2d 2d 2d 2d 2d 2d  2d 2d 2d 2d 2d 2d 2d 2d   -------- --------
0050  2d 2d 2d 2d 2d 2d 2d 2d  2d 2d 2d 2d 2d 2d 2d 2d   -------- --------
0060  2d 2d 2d 2d 2d 2d 2d 2d  2d 2d 2d 2d 2d 2d 2d 2d   -------- --------
0070  2d 2d 2d 2d 2d 2d 2d 2d  2d 2d 2d 2d 2d 2d 2d 2d   -------- --------
0080  2d 2d 2d 2d 2d 0d 0a 32  32 30 2d 20 57 41 52 4e   -----··2 20- WARN
0090  49 4e 47 3a 20 20 54 68  69 73 20 69 73 20 61 20   ING:  Th is is a
00a0  72 65 73 74 72 69 63 74  65 64 20 61 63 63 65 73   restrict ed acces
```

Destination Port (tcp.dstport), 2 bytes

- Sequence number

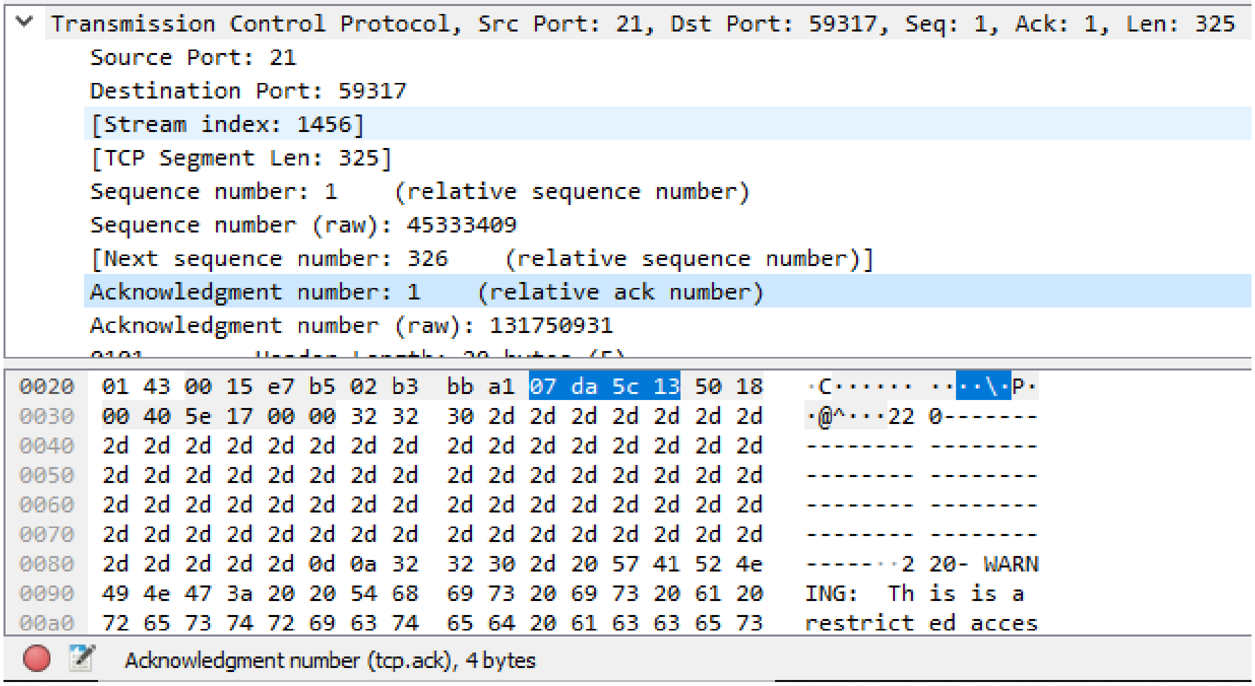


```
⌄ Transmission Control Protocol, Src Port: 21, Dst Port: 59317, Seq: 1, Ack: 1, Len: 325
      Source Port: 21
      Destination Port: 59317
      [Stream index: 1456]
      [TCP Segment Len: 325]
      Sequence number: 1    (relative sequence number)
      Sequence number (raw): 45333409
      [Next sequence number: 326    (relative sequence number)]
      Acknowledgment number: 1    (relative ack number)
      Acknowledgment number (raw): 131750931
      0101 .... = Header Length: 20 bytes (5)
```

```
0020  01 43 00 15 e7 b5 02 b3  bb a1 07 da 5c 13 50 18   ·C······ ··\·P·
0030  00 40 5e 17 00 00 32 32  30 2d 2d 2d 2d 2d 2d 2d   ·@^···22 0-------
0040  2d 2d 2d 2d 2d 2d 2d 2d  2d 2d 2d 2d 2d 2d 2d 2d   -------- --------
0050  2d 2d 2d 2d 2d 2d 2d 2d  2d 2d 2d 2d 2d 2d 2d 2d   -------- --------
0060  2d 2d 2d 2d 2d 2d 2d 2d  2d 2d 2d 2d 2d 2d 2d 2d   -------- --------
0070  2d 2d 2d 2d 2d 2d 2d 2d  2d 2d 2d 2d 2d 2d 2d 2d   -------- --------
0080  2d 2d 2d 2d 2d 0d 0a 32  32 30 2d 20 57 41 52 4e   -----··2 20- WARN
0090  49 4e 47 3a 20 20 54 68  69 73 20 69 73 20 61 20   ING:  Th is is a 
00a0  72 65 73 74 72 69 63 74  65 64 20 61 63 63 65 73   restrict ed acces
```

Sequence number (tcp.seq), 4 bytes

- Acknowledgment number

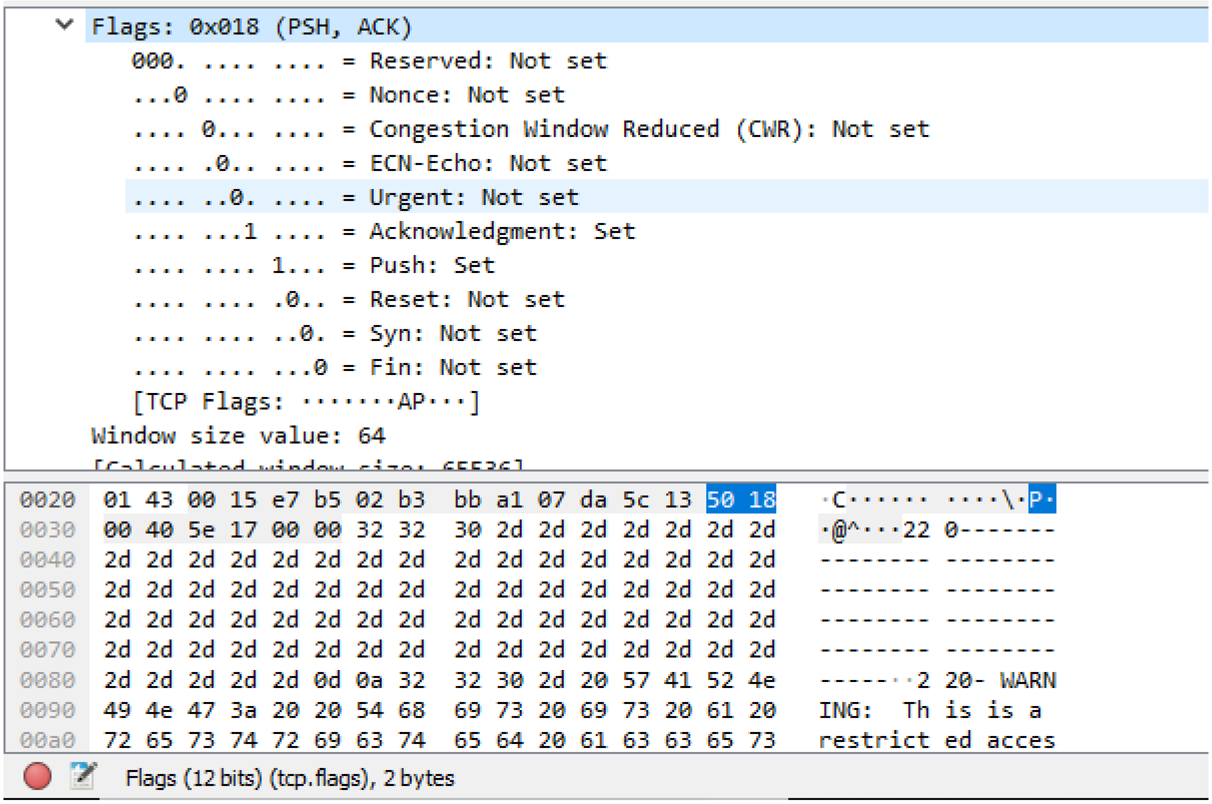


```
⌄ Transmission Control Protocol, Src Port: 21, Dst Port: 59317, Seq: 1, Ack: 1, Len: 325
      Source Port: 21
      Destination Port: 59317
      [Stream index: 1456]
      [TCP Segment Len: 325]
      Sequence number: 1    (relative sequence number)
      Sequence number (raw): 45333409
      [Next sequence number: 326    (relative sequence number)]
      Acknowledgment number: 1    (relative ack number)
      Acknowledgment number (raw): 131750931
      0101 .... = Header Length: 20 bytes (5)
```

```
0020  01 43 00 15 e7 b5 02 b3  bb a1 07 da 5c 13 50 18   ·C······ ··\·P·
0030  00 40 5e 17 00 00 32 32  30 2d 2d 2d 2d 2d 2d 2d   ·@^···22 0-------
0040  2d 2d 2d 2d 2d 2d 2d 2d  2d 2d 2d 2d 2d 2d 2d 2d   -------- --------
0050  2d 2d 2d 2d 2d 2d 2d 2d  2d 2d 2d 2d 2d 2d 2d 2d   -------- --------
0060  2d 2d 2d 2d 2d 2d 2d 2d  2d 2d 2d 2d 2d 2d 2d 2d   -------- --------
0070  2d 2d 2d 2d 2d 2d 2d 2d  2d 2d 2d 2d 2d 2d 2d 2d   -------- --------
0080  2d 2d 2d 2d 2d 0d 0a 32  32 30 2d 20 57 41 52 4e   -----··2 20- WARN
0090  49 4e 47 3a 20 20 54 68  69 73 20 69 73 20 61 20   ING:  Th is is a 
00a0  72 65 73 74 72 69 63 74  65 64 20 61 63 63 65 73   restrict ed acces
```

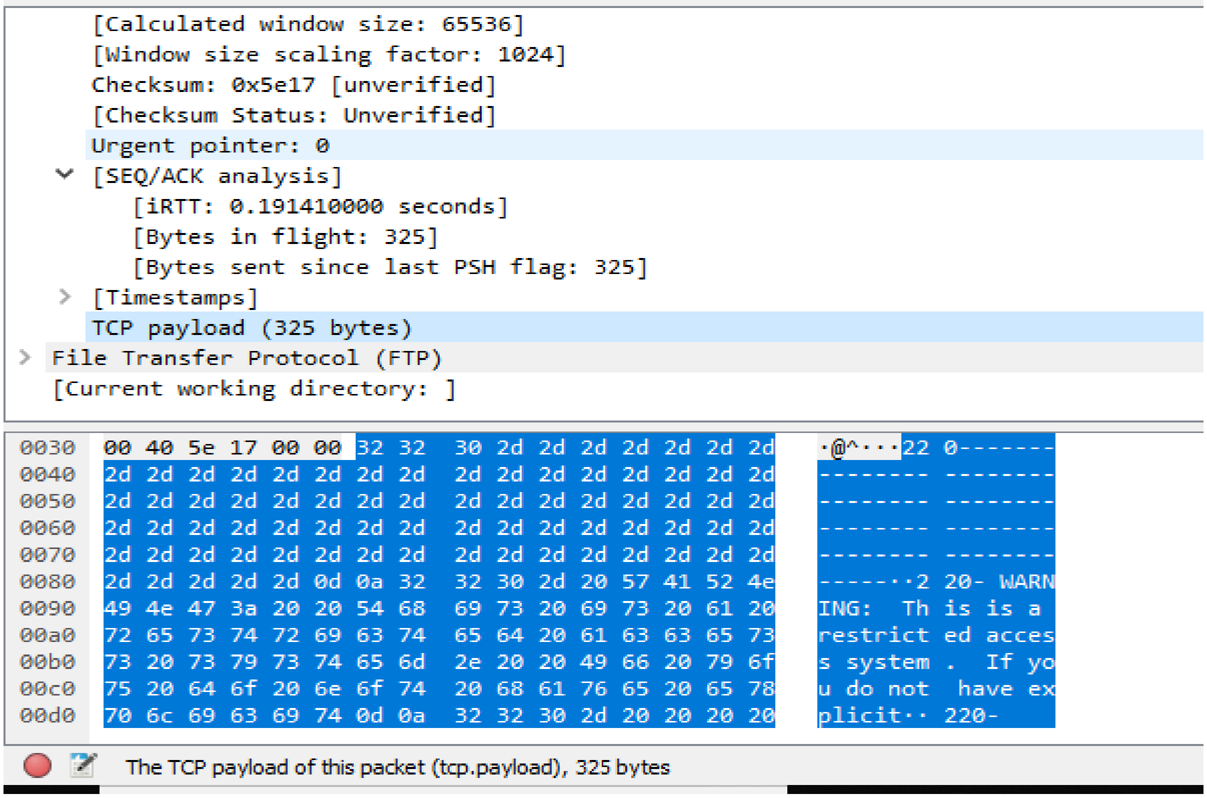
Acknowledgment number (tcp.ack), 4 bytes

- TCP Flags information



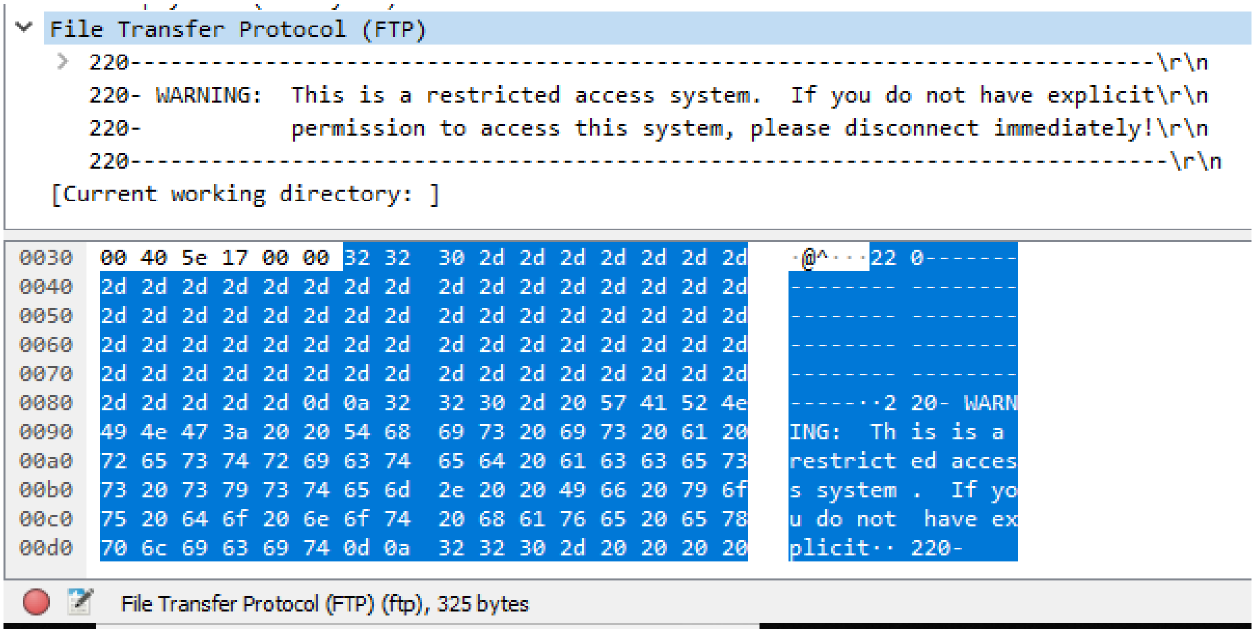
```
  Flags: 0x018 (PSH, ACK)
     000. .... .... = Reserved: Not set
     ...0 .... .... = Nonce: Not set
     .... 0... .... = Congestion Window Reduced (CWR): Not set
     .... .0.. .... = ECN-Echo: Not set
     .... ..0. .... = Urgent: Not set
     .... ...1 .... = Acknowledgment: Set
     .... .... 1... = Push: Set
     .... .... .0.. = Reset: Not set
     .... .... ..0. = Syn: Not set
     .... .... ...0 = Fin: Not set
     [TCP Flags: ·······AP···]
  Window size value: 64
  [Calculated window size: 65536]

0020  01 43 00 15 e7 b5 02 b3  bb a1 07 da 5c 13 50 18   ·C······ ····\·P·
0030  00 40 5e 17 00 00 32 32  30 2d 2d 2d 2d 2d 2d 2d   ·@^···22 0-------
0040  2d 2d 2d 2d 2d 2d 2d 2d  2d 2d 2d 2d 2d 2d 2d 2d   -------- --------
0050  2d 2d 2d 2d 2d 2d 2d 2d  2d 2d 2d 2d 2d 2d 2d 2d   -------- --------
0060  2d 2d 2d 2d 2d 2d 2d 2d  2d 2d 2d 2d 2d 2d 2d 2d   -------- --------
0070  2d 2d 2d 2d 2d 2d 2d 2d  2d 2d 2d 2d 2d 2d 2d 2d   -------- --------
0080  2d 2d 2d 2d 2d 0d 0a 32  32 30 2d 20 57 41 52 4e   -----··2 20- WARN
0090  49 4e 47 3a 20 20 54 68  69 73 20 69 73 20 61 20   ING:  Th is is a 
00a0  72 65 73 74 72 69 63 74  65 64 20 61 63 63 65 73   restrict ed acces

Flags (12 bits) (tcp.flags), 2 bytes
```

- TCP payload → FTP based data left as trailer



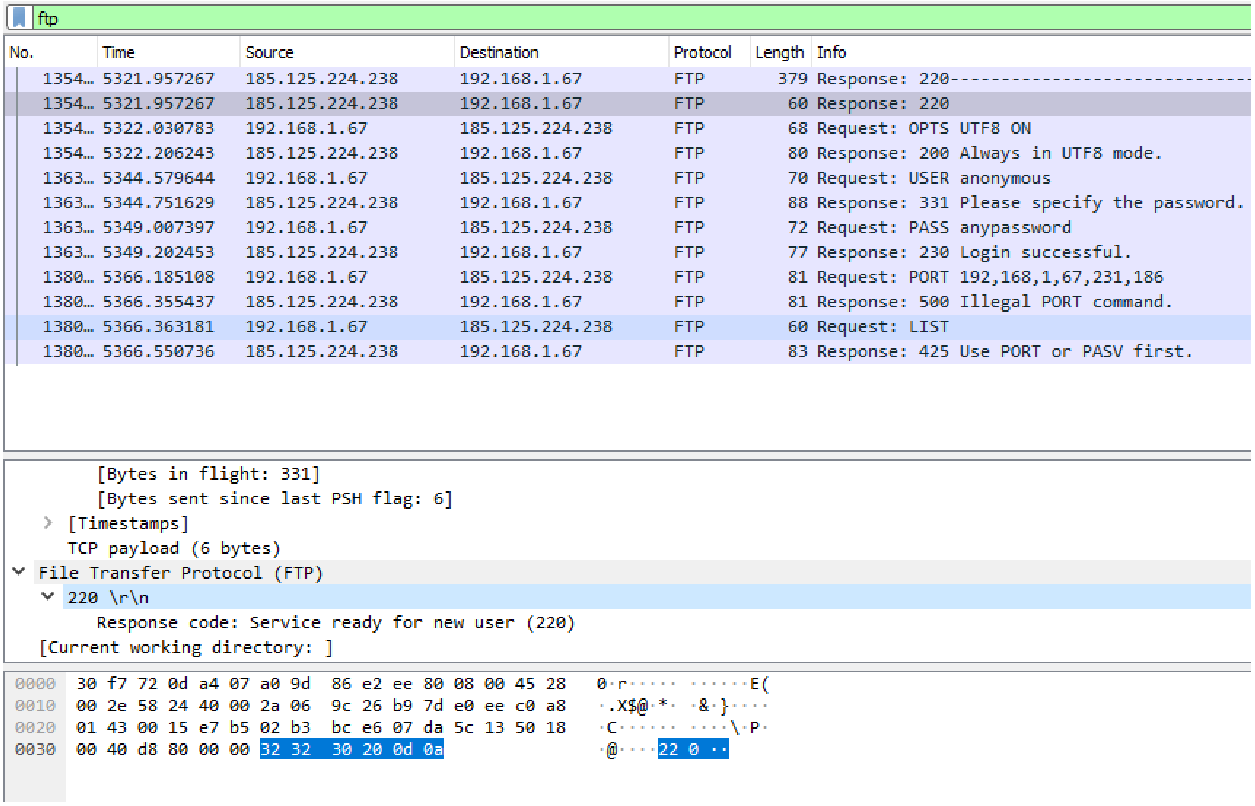
```
  [Calculated window size: 65536]
  [Window size scaling factor: 1024]
  Checksum: 0x5e17 [unverified]
  [Checksum Status: Unverified]
  Urgent pointer: 0
  [SEQ/ACK analysis]
     [iRTT: 0.191410000 seconds]
     [Bytes in flight: 325]
     [Bytes sent since last PSH flag: 325]
  [Timestamps]
  TCP payload (325 bytes)
File Transfer Protocol (FTP)
[Current working directory: ]

0030  00 40 5e 17 00 00 32 32  30 2d 2d 2d 2d 2d 2d 2d   ·@^···22 0-------
0040  2d 2d 2d 2d 2d 2d 2d 2d  2d 2d 2d 2d 2d 2d 2d 2d   -------- --------
0050  2d 2d 2d 2d 2d 2d 2d 2d  2d 2d 2d 2d 2d 2d 2d 2d   -------- --------
0060  2d 2d 2d 2d 2d 2d 2d 2d  2d 2d 2d 2d 2d 2d 2d 2d   -------- --------
0070  2d 2d 2d 2d 2d 2d 2d 2d  2d 2d 2d 2d 2d 2d 2d 2d   -------- --------
0080  2d 2d 2d 2d 2d 0d 0a 32  32 30 2d 20 57 41 52 4e   -----··2 20- WARN
0090  49 4e 47 3a 20 20 54 68  69 73 20 69 73 20 61 20   ING:  Th is is a 
00a0  72 65 73 74 72 69 63 74  65 64 20 61 63 63 65 73   restrict ed acces
00b0  73 20 73 79 73 74 65 6d  2e 20 20 49 66 20 79 6f   s system .  If yo
00c0  75 20 64 6f 20 6e 6f 74  20 68 61 76 65 20 65 78   u do not  have ex
00d0  70 6c 69 63 69 74 0d 0a  32 32 30 2d 20 20 20 20   plicit·· 220-    

The TCP payload of this packet (tcp.payload), 325 bytes
```

- FTP



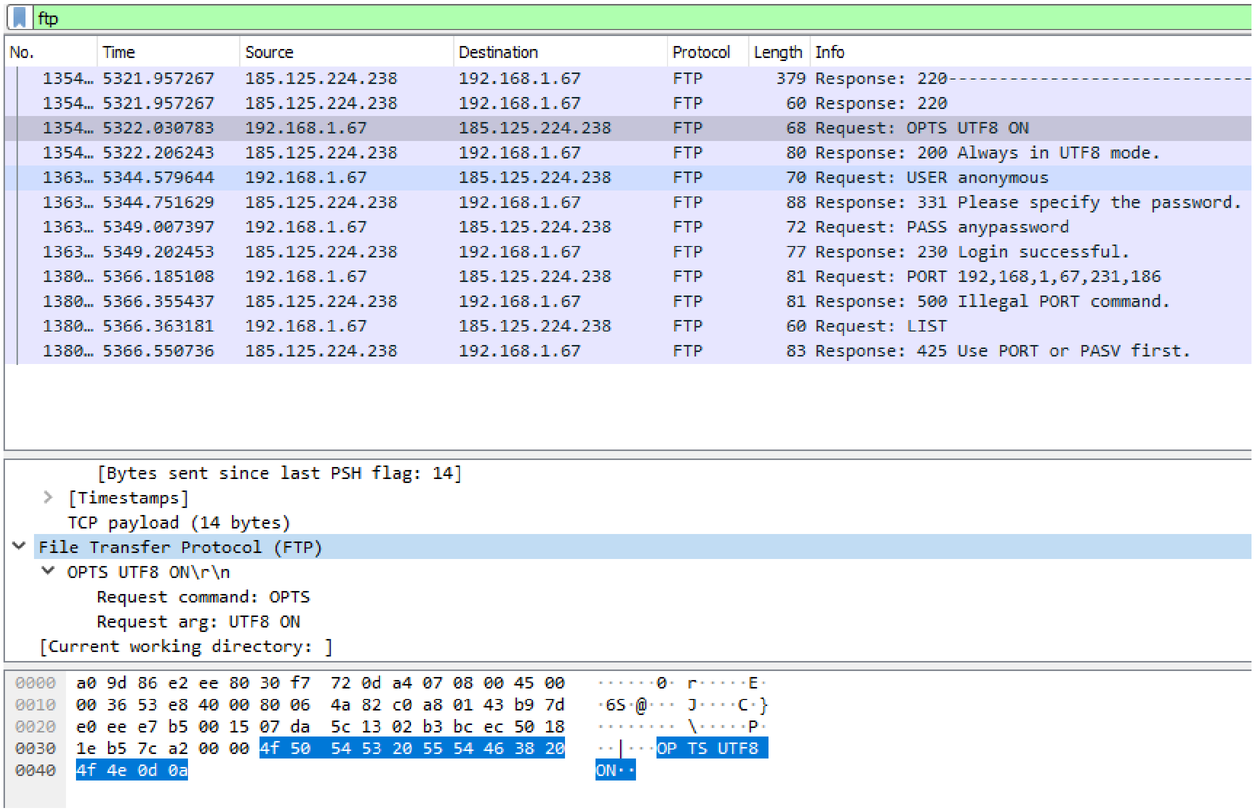
```
v File Transfer Protocol (FTP)
  > 220-----------------------------------------------------------------------\r\n
    220- WARNING:  This is a restricted access system.  If you do not have explicit\r\n
    220-           permission to access this system, please disconnect immediately!\r\n
    220------------------------------------------------------------------------\r\n
  [Current working directory: ]

0030  00 40 5e 17 00 00 32 32  30 2d 2d 2d 2d 2d 2d 2d   ·@^···22 0-------
0040  2d 2d 2d 2d 2d 2d 2d 2d  2d 2d 2d 2d 2d 2d 2d 2d   -------- --------
0050  2d 2d 2d 2d 2d 2d 2d 2d  2d 2d 2d 2d 2d 2d 2d 2d   -------- --------
0060  2d 2d 2d 2d 2d 2d 2d 2d  2d 2d 2d 2d 2d 2d 2d 2d   -------- --------
0070  2d 2d 2d 2d 2d 2d 2d 2d  2d 2d 2d 2d 2d 2d 2d 2d   -------- --------
0080  2d 2d 2d 2d 2d 0d 0a 32  32 30 2d 20 57 41 52 4e   -----··2 20- WARN
0090  49 4e 47 3a 20 20 54 68  69 73 20 69 73 20 61 20   ING:  Th is is a 
00a0  72 65 73 74 72 69 63 74  65 64 20 61 63 63 65 73   restrict ed acces
00b0  73 20 73 79 73 74 65 6d  2e 20 20 49 66 20 79 6f   s system .  If yo
00c0  75 20 64 6f 20 6e 6f 74  20 68 61 76 65 20 65 78   u do not  have ex
00d0  70 6c 69 63 69 74 0d 0a  32 32 30 2d 20 20 20 20   plicit·· 220-    

File Transfer Protocol (FTP) (ftp), 325 bytes
```

- FTP response



```
ftp

No.    Time         Source           Destination      Protocol Length Info
1354…  5321.957267  185.125.224.238  192.168.1.67     FTP         379 Response: 220-----------------------------
1354…  5321.957267  185.125.224.238  192.168.1.67     FTP          60 Response: 220
1354…  5322.030783  192.168.1.67     185.125.224.238  FTP          68 Request: OPTS UTF8 ON
1354…  5322.206243  185.125.224.238  192.168.1.67     FTP          80 Response: 200 Always in UTF8 mode.
1363…  5344.579644  192.168.1.67     185.125.224.238  FTP          70 Request: USER anonymous
1363…  5344.751629  185.125.224.238  192.168.1.67     FTP          88 Response: 331 Please specify the password.
1363…  5349.007397  192.168.1.67     185.125.224.238  FTP          72 Request: PASS anypassword
1363…  5349.202453  185.125.224.238  192.168.1.67     FTP          77 Response: 230 Login successful.
1380…  5366.185108  192.168.1.67     185.125.224.238  FTP          81 Request: PORT 192,168,1,67,231,186
1380…  5366.355437  185.125.224.238  192.168.1.67     FTP          81 Response: 500 Illegal PORT command.
1380…  5366.363181  192.168.1.67     185.125.224.238  FTP          60 Request: LIST
1380…  5366.550736  185.125.224.238  192.168.1.67     FTP          83 Response: 425 Use PORT or PASV first.

        [Bytes in flight: 331]
        [Bytes sent since last PSH flag: 6]
    > [Timestamps]
      TCP payload (6 bytes)
v File Transfer Protocol (FTP)
  v 220 \r\n
        Response code: Service ready for new user (220)
    [Current working directory: ]

0000  30 f7 72 0d a4 07 a0 9d  86 e2 ee 80 08 00 45 28   0·r····· ······E(
0010  00 2e 58 24 40 00 2a 06  9c 26 b9 7d e0 ee c0 a8   ·.X$@·*· ·&·}····
0020  01 43 00 15 e7 b5 02 b3  bc e6 07 da 5c 13 50 18   ·C······ ····\·P·
0030  00 40 d8 80 00 00 32 32  30 20 0d 0a               ·@····22 0 ··
```

- ftp request

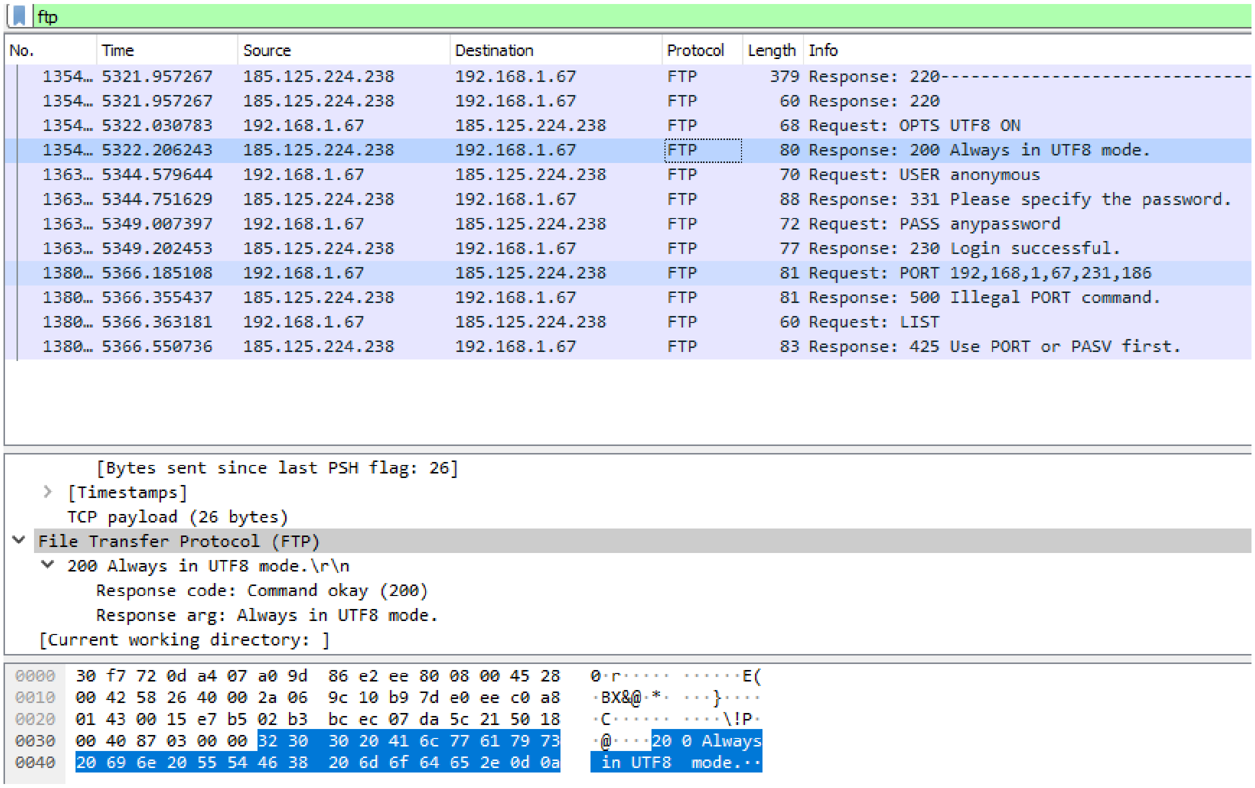


```
ftp

No.      Time          Source            Destination       Protocol  Length  Info
 1354…  5321.957267   185.125.224.238   192.168.1.67      FTP         379  Response: 220-----------------------------
 1354…  5321.957267   185.125.224.238   192.168.1.67      FTP          60  Response: 220
 1354…  5322.030783   192.168.1.67      185.125.224.238   FTP          68  Request: OPTS UTF8 ON
 1354…  5322.206243   185.125.224.238   192.168.1.67      FTP          80  Response: 200 Always in UTF8 mode.
 1363…  5344.579644   192.168.1.67      185.125.224.238   FTP          70  Request: USER anonymous
 1363…  5344.751629   185.125.224.238   192.168.1.67      FTP          88  Response: 331 Please specify the password.
 1363…  5349.007397   192.168.1.67      185.125.224.238   FTP          72  Request: PASS anypassword
 1363…  5349.202453   185.125.224.238   192.168.1.67      FTP          77  Response: 230 Login successful.
 1380…  5366.185108   192.168.1.67      185.125.224.238   FTP          81  Request: PORT 192,168,1,67,231,186
 1380…  5366.355437   185.125.224.238   192.168.1.67      FTP          81  Response: 500 Illegal PORT command.
 1380…  5366.363181   192.168.1.67      185.125.224.238   FTP          60  Request: LIST
 1380…  5366.550736   185.125.224.238   192.168.1.67      FTP          83  Response: 425 Use PORT or PASV first.
```

```
        [Bytes sent since last PSH flag: 14]
    > [Timestamps]
      TCP payload (14 bytes)
  v File Transfer Protocol (FTP)
    v OPTS UTF8 ON\r\n
          Request command: OPTS
          Request arg: UTF8 ON
    [Current working directory: ]
```

```
0000  a0 9d 86 e2 ee 80 30 f7  72 0d a4 07 08 00 45 00   ······0· r·····E·
0010  00 36 53 e8 40 00 80 06  4a 82 c0 a8 01 43 b9 7d   ·6S·@··· J····C·}
0020  e0 ee e7 b5 00 15 07 da  5c 13 02 b3 bc ec 50 18   ········ \·····P·
0030  1e b5 7c a2 00 00 4f 50  54 53 20 55 54 46 38 20   ··|···OP TS UTF8 
0040  4f 4e 0d 0a                                        ON··
```

- ftp response

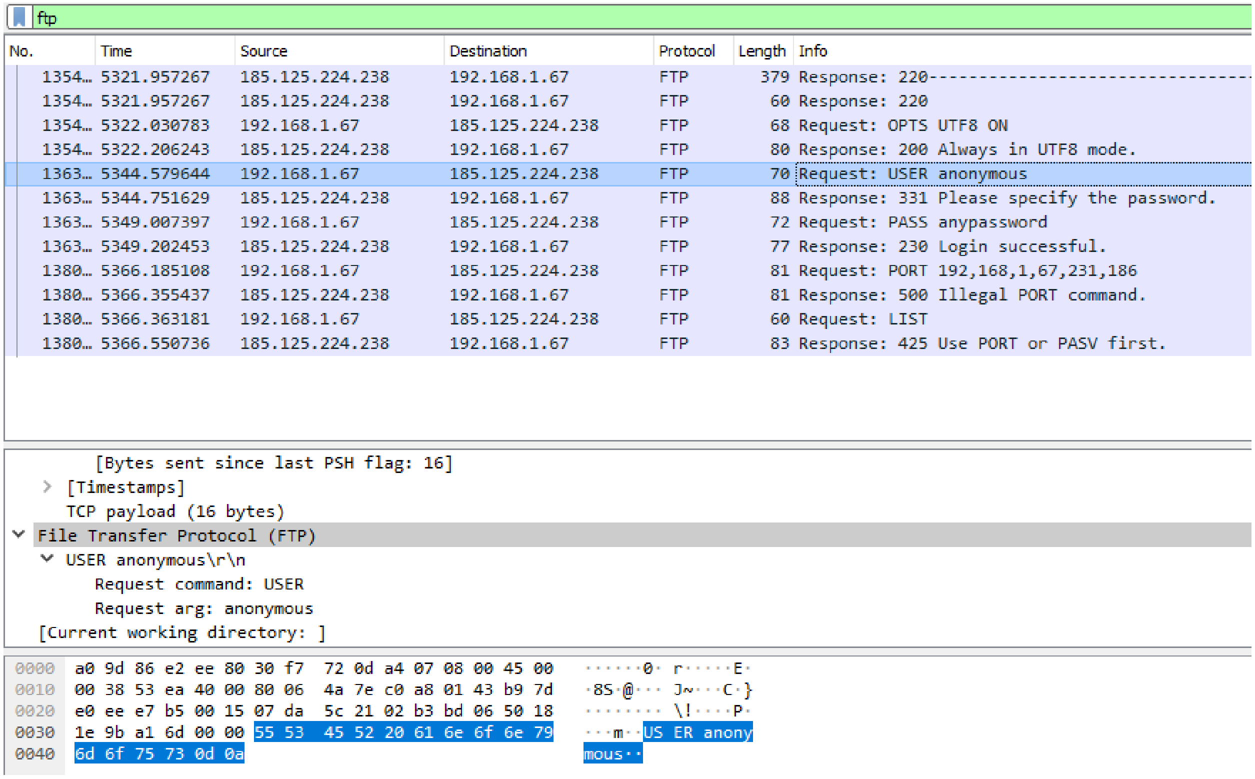


```
ftp

No.      Time          Source            Destination       Protocol  Length  Info
 1354…  5321.957267   185.125.224.238   192.168.1.67      FTP         379  Response: 220----------------------------
 1354…  5321.957267   185.125.224.238   192.168.1.67      FTP          60  Response: 220
 1354…  5322.030783   192.168.1.67      185.125.224.238   FTP          68  Request: OPTS UTF8 ON
 1354…  5322.206243   185.125.224.238   192.168.1.67      FTP          80  Response: 200 Always in UTF8 mode.
 1363…  5344.579644   192.168.1.67      185.125.224.238   FTP          70  Request: USER anonymous
 1363…  5344.751629   185.125.224.238   192.168.1.67      FTP          88  Response: 331 Please specify the password.
 1363…  5349.007397   192.168.1.67      185.125.224.238   FTP          72  Request: PASS anypassword
 1363…  5349.202453   185.125.224.238   192.168.1.67      FTP          77  Response: 230 Login successful.
 1380…  5366.185108   192.168.1.67      185.125.224.238   FTP          81  Request: PORT 192,168,1,67,231,186
 1380…  5366.355437   185.125.224.238   192.168.1.67      FTP          81  Response: 500 Illegal PORT command.
 1380…  5366.363181   192.168.1.67      185.125.224.238   FTP          60  Request: LIST
 1380…  5366.550736   185.125.224.238   192.168.1.67      FTP          83  Response: 425 Use PORT or PASV first.
```

```
        [Bytes sent since last PSH flag: 26]
    > [Timestamps]
      TCP payload (26 bytes)
  v File Transfer Protocol (FTP)
    v 200 Always in UTF8 mode.\r\n
          Response code: Command okay (200)
          Response arg: Always in UTF8 mode.
    [Current working directory: ]
```

```
0000  30 f7 72 0d a4 07 a0 9d  86 e2 ee 80 08 00 45 28   0·r····· ······E(
0010  00 42 58 26 40 00 2a 06  9c 10 b9 7d e0 ee c0 a8   ·BX&@·*· ···}····
0020  01 43 00 15 e7 b5 02 b3  bc ec 07 da 5c 21 50 18   ·C······ ····\!P·
0030  00 40 87 03 00 00 32 30  30 20 41 6c 77 61 79 73   ·@····20 0 Always
0040  20 69 6e 20 55 54 46 38  20 6d 6f 64 65 2e 0d 0a    in UTF8  mode.··
```

- ftp login with username → request to login

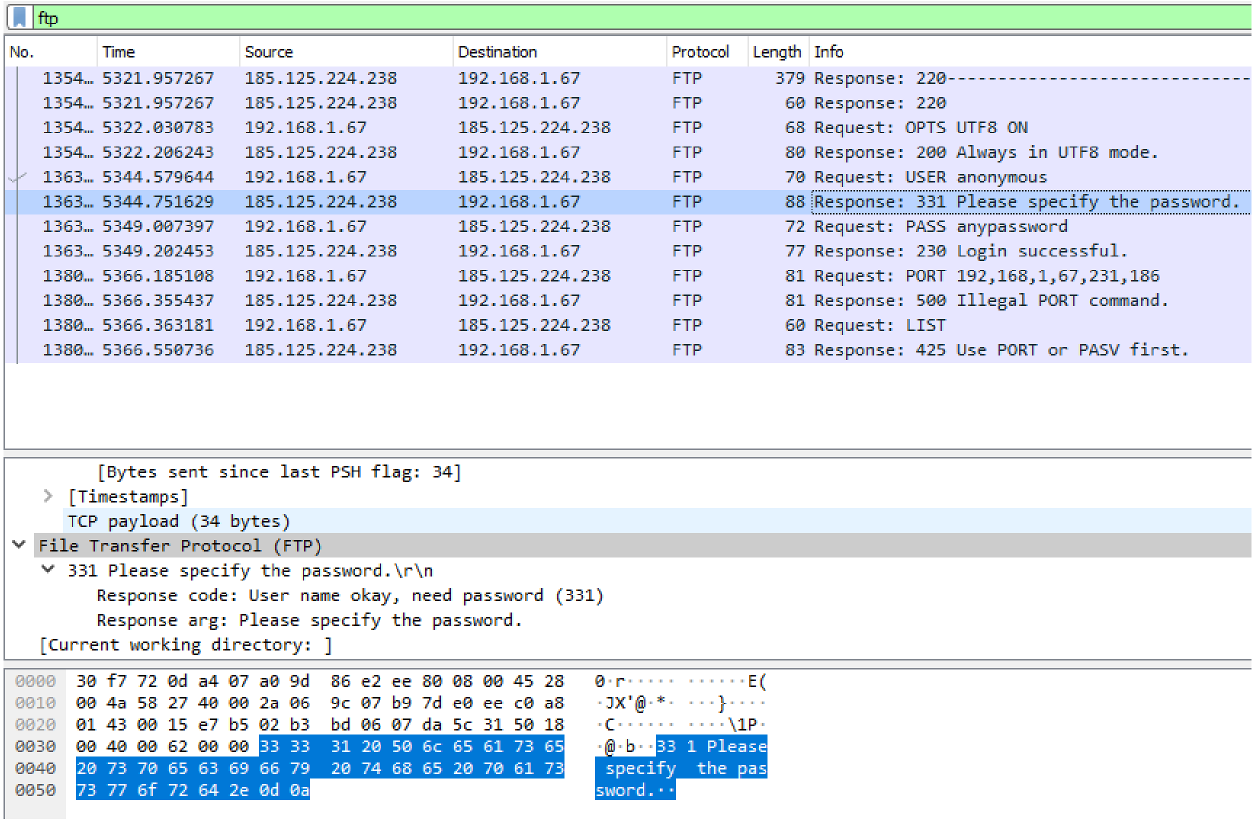


```
No.      Time         Source           Destination      Protocol  Length  Info
  1354…  5321.957267  185.125.224.238  192.168.1.67     FTP          379  Response: 220--------------------------------
  1354…  5321.957267  185.125.224.238  192.168.1.67     FTP           60  Response: 220
  1354…  5322.030783  192.168.1.67     185.125.224.238  FTP           68  Request: OPTS UTF8 ON
  1354…  5322.206243  185.125.224.238  192.168.1.67     FTP           80  Response: 200 Always in UTF8 mode.
  1363…  5344.579644  192.168.1.67     185.125.224.238  FTP           70  Request: USER anonymous
  1363…  5344.751629  185.125.224.238  192.168.1.67     FTP           88  Response: 331 Please specify the password.
  1363…  5349.007397  192.168.1.67     185.125.224.238  FTP           72  Request: PASS anypassword
  1363…  5349.202453  185.125.224.238  192.168.1.67     FTP           77  Response: 230 Login successful.
  1380…  5366.185108  192.168.1.67     185.125.224.238  FTP           81  Request: PORT 192,168,1,67,231,186
  1380…  5366.355437  185.125.224.238  192.168.1.67     FTP           81  Response: 500 Illegal PORT command.
  1380…  5366.363181  192.168.1.67     185.125.224.238  FTP           60  Request: LIST
  1380…  5366.550736  185.125.224.238  192.168.1.67     FTP           83  Response: 425 Use PORT or PASV first.
```

```
      [Bytes sent since last PSH flag: 16]
    > [Timestamps]
    TCP payload (16 bytes)
v File Transfer Protocol (FTP)
  v USER anonymous\r\n
      Request command: USER
      Request arg: anonymous
  [Current working directory: ]
```

```
0000  a0 9d 86 e2 ee 80 30 f7  72 0d a4 07 08 00 45 00   ······0· r·····E·
0010  00 38 53 ea 40 00 80 06  4a 7e c0 a8 01 43 b9 7d   ·8S·@··· J~···C·}
0020  e0 ee e7 b5 00 15 07 da  5c 21 02 b3 bd 06 50 18   ········ \!····P·
0030  1e 9b a1 6d 00 00 55 53  45 52 20 61 6e 6f 6e 79   ···m··US ER anony
0040  6d 6f 75 73 0d 0a                                 mous··
```

- ftp response asking for password

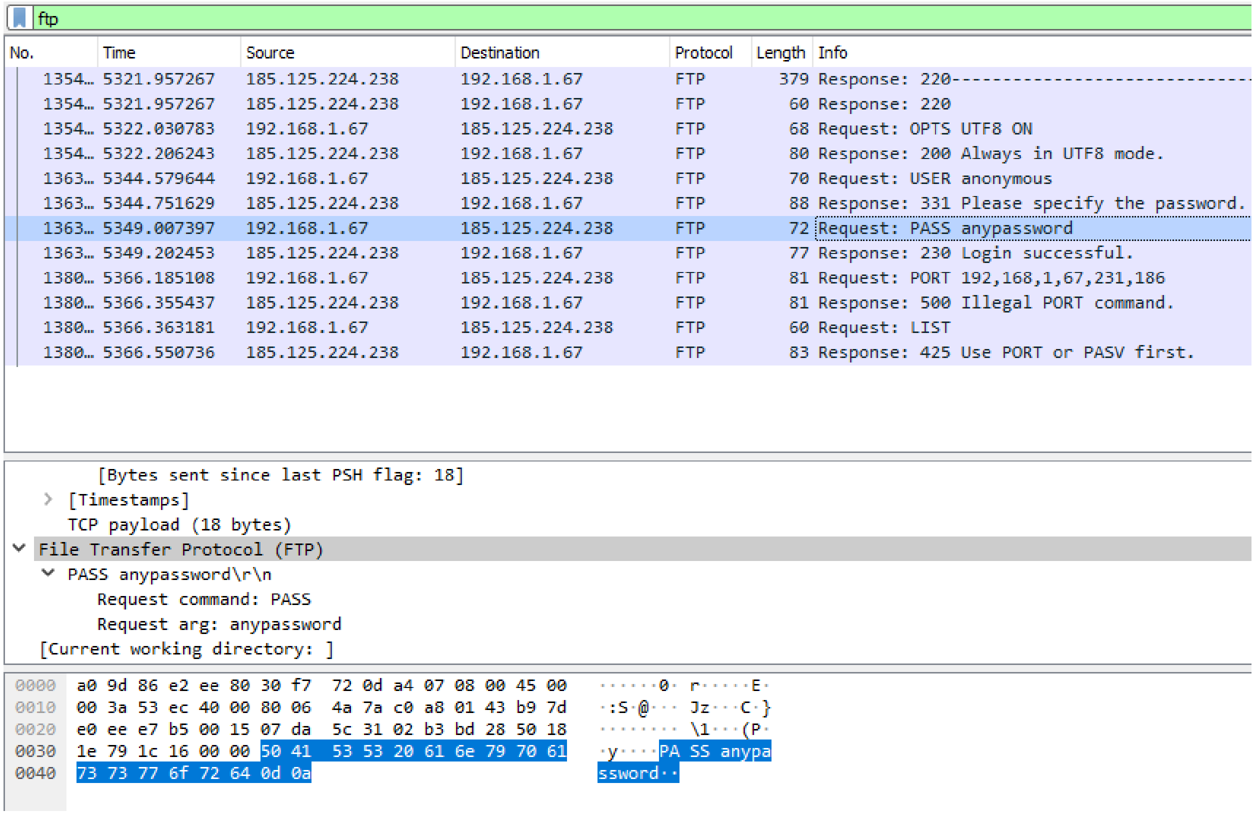


```
No.      Time         Source           Destination      Protocol  Length  Info
  1354…  5321.957267  185.125.224.238  192.168.1.67     FTP          379  Response: 220-----------------------------
  1354…  5321.957267  185.125.224.238  192.168.1.67     FTP           60  Response: 220
  1354…  5322.030783  192.168.1.67     185.125.224.238  FTP           68  Request: OPTS UTF8 ON
  1354…  5322.206243  185.125.224.238  192.168.1.67     FTP           80  Response: 200 Always in UTF8 mode.
  1363…  5344.579644  192.168.1.67     185.125.224.238  FTP           70  Request: USER anonymous
  1363…  5344.751629  185.125.224.238  192.168.1.67     FTP           88  Response: 331 Please specify the password.
  1363…  5349.007397  192.168.1.67     185.125.224.238  FTP           72  Request: PASS anypassword
  1363…  5349.202453  185.125.224.238  192.168.1.67     FTP           77  Response: 230 Login successful.
  1380…  5366.185108  192.168.1.67     185.125.224.238  FTP           81  Request: PORT 192,168,1,67,231,186
  1380…  5366.355437  185.125.224.238  192.168.1.67     FTP           81  Response: 500 Illegal PORT command.
  1380…  5366.363181  192.168.1.67     185.125.224.238  FTP           60  Request: LIST
  1380…  5366.550736  185.125.224.238  192.168.1.67     FTP           83  Response: 425 Use PORT or PASV first.
```

```
      [Bytes sent since last PSH flag: 34]
    > [Timestamps]
    TCP payload (34 bytes)
v File Transfer Protocol (FTP)
  v 331 Please specify the password.\r\n
      Response code: User name okay, need password (331)
      Response arg: Please specify the password.
  [Current working directory: ]
```

```
0000  30 f7 72 0d a4 07 a0 9d  86 e2 ee 80 08 00 45 28   0·r····· ······E(
0010  00 4a 58 27 40 00 2a 06  9c 07 b9 7d e0 ee c0 a8   ·JX'@·*· ···}····
0020  01 43 00 15 e7 b5 02 b3  bd 06 07 da 5c 31 50 18   ·C······ ····\1P·
0030  00 40 00 62 00 00 33 33  31 20 50 6c 65 61 73 65   ·@·b··33 1 Please
0040  20 73 70 65 63 69 66 79  20 74 68 65 20 70 61 73    specify  the pas
0050  73 77 6f 72 64 2e 0d 0a                           sword.··
```

- ftp request to access after entering the password



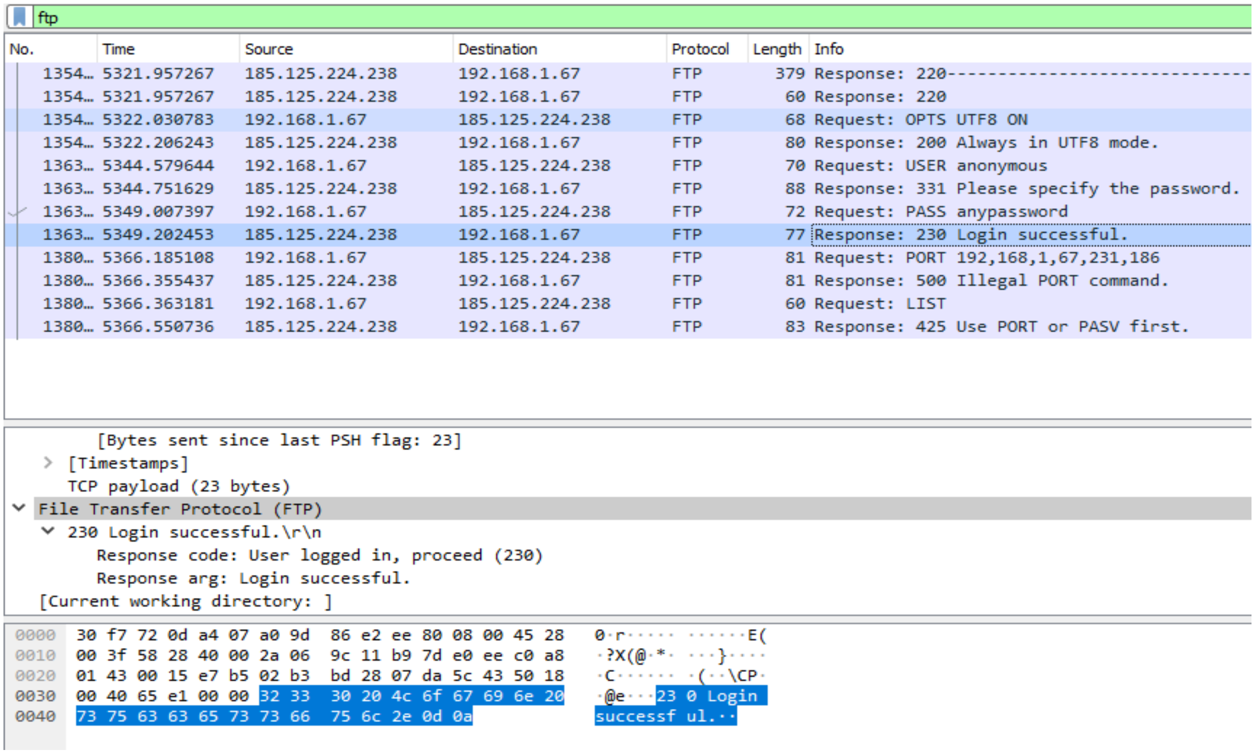
ftp

No.	Time	Source	Destination	Protocol	Length	Info
1354…	5321.957267	185.125.224.238	192.168.1.67	FTP	379	Response: 220-----------------------------
1354…	5321.957267	185.125.224.238	192.168.1.67	FTP	60	Response: 220
1354…	5322.030783	192.168.1.67	185.125.224.238	FTP	68	Request: OPTS UTF8 ON
1354…	5322.206243	185.125.224.238	192.168.1.67	FTP	80	Response: 200 Always in UTF8 mode.
1363…	5344.579644	192.168.1.67	185.125.224.238	FTP	70	Request: USER anonymous
1363…	5344.751629	185.125.224.238	192.168.1.67	FTP	88	Response: 331 Please specify the password.
1363…	5349.007397	192.168.1.67	185.125.224.238	FTP	72	Request: PASS anypassword
1363…	5349.202453	185.125.224.238	192.168.1.67	FTP	77	Response: 230 Login successful.
1380…	5366.185108	192.168.1.67	185.125.224.238	FTP	81	Request: PORT 192,168,1,67,231,186
1380…	5366.355437	185.125.224.238	192.168.1.67	FTP	81	Response: 500 Illegal PORT command.
1380…	5366.363181	192.168.1.67	185.125.224.238	FTP	60	Request: LIST
1380…	5366.550736	185.125.224.238	192.168.1.67	FTP	83	Response: 425 Use PORT or PASV first.

```
      [Bytes sent since last PSH flag: 18]
  > [Timestamps]
    TCP payload (18 bytes)
v File Transfer Protocol (FTP)
  v PASS anypassword\r\n
      Request command: PASS
      Request arg: anypassword
  [Current working directory: ]
```

```
0000  a0 9d 86 e2 ee 80 30 f7  72 0d a4 07 08 00 45 00   ······0· r·····E·
0010  00 3a 53 ec 40 00 80 06  4a 7a c0 a8 01 43 b9 7d   ·:S·@··· Jz···C·}
0020  e0 ee e7 b5 00 15 07 da  5c 31 02 b3 bd 28 50 18   ········ \1···(P·
0030  1e 79 1c 16 00 00 50 41  53 53 20 61 6e 79 70 61   ·y····PA SS anypa
0040  73 73 77 6f 72 64 0d 0a                            ssword··
```

- ftp response with message about login validation



ftp

No.	Time	Source	Destination	Protocol	Length	Info
1354…	5321.957267	185.125.224.238	192.168.1.67	FTP	379	Response: 220-----------------------------
1354…	5321.957267	185.125.224.238	192.168.1.67	FTP	60	Response: 220
1354…	5322.030783	192.168.1.67	185.125.224.238	FTP	68	Request: OPTS UTF8 ON
1354…	5322.206243	185.125.224.238	192.168.1.67	FTP	80	Response: 200 Always in UTF8 mode.
1363…	5344.579644	192.168.1.67	185.125.224.238	FTP	70	Request: USER anonymous
1363…	5344.751629	185.125.224.238	192.168.1.67	FTP	88	Response: 331 Please specify the password.
1363…	5349.007397	192.168.1.67	185.125.224.238	FTP	72	Request: PASS anypassword
1363…	5349.202453	185.125.224.238	192.168.1.67	FTP	77	Response: 230 Login successful.
1380…	5366.185108	192.168.1.67	185.125.224.238	FTP	81	Request: PORT 192,168,1,67,231,186
1380…	5366.355437	185.125.224.238	192.168.1.67	FTP	81	Response: 500 Illegal PORT command.
1380…	5366.363181	192.168.1.67	185.125.224.238	FTP	60	Request: LIST
1380…	5366.550736	185.125.224.238	192.168.1.67	FTP	83	Response: 425 Use PORT or PASV first.

```
      [Bytes sent since last PSH flag: 23]
  > [Timestamps]
    TCP payload (23 bytes)
v File Transfer Protocol (FTP)
  v 230 Login successful.\r\n
      Response code: User logged in, proceed (230)
      Response arg: Login successful.
  [Current working directory: ]
```

```
0000  30 f7 72 0d a4 07 a0 9d  86 e2 ee 80 08 00 45 28   0·r····· ······E(
0010  00 3f 58 28 40 00 2a 06  9c 11 b9 7d e0 ee c0 a8   ·?X(@·*· ···}····
0020  01 43 00 15 e7 b5 02 b3  bd 28 07 da 5c 43 50 18   ·C······ ·(··\CP·
0030  00 40 65 e1 00 00 32 33  30 20 4c 6f 67 69 6e 20   ·@e···23 0 Login 
0040  73 75 63 63 65 73 73 66  75 6c 2e 0d 0a            successf ul.··
```