Gasser Ahmed
gasser18@vt.edu
ECE 5484, Project 4

Section 1 – Objectives:

Reinforce the understanding of the TCP/IP protocol suite by using Wireshark network protocol analyzer to examine details of TCP, UDP, and IP protocols from the TCP/IP protocol suite.

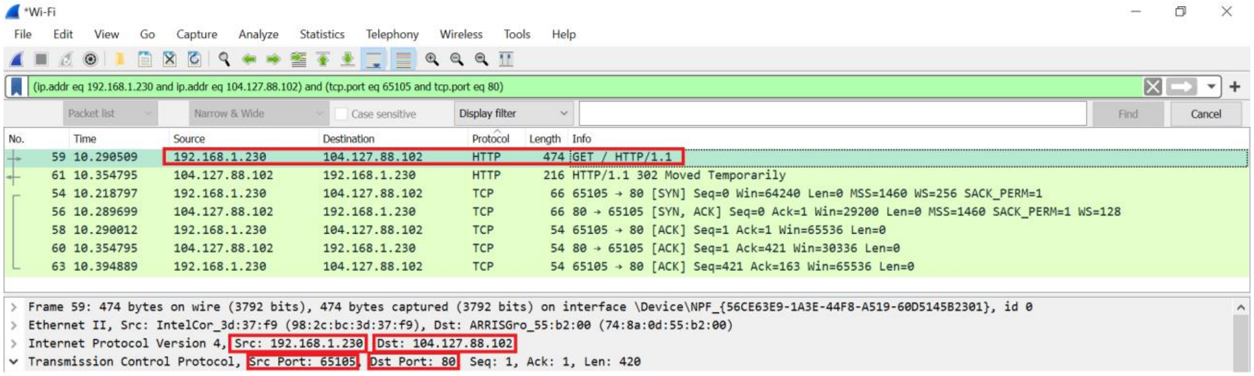
By following the steps below:

1. Capture and analyze TCP segments.
2. Capture and analyze UDP datagrams.
3. Capture and analyze IP datagrams.

Section 2 – Questions:

2.1. TCP:

1. What is the IP address of the client? 192.168.1.230
2. What is the port number used on the client for the TCP session with the server? 65105
3. What is the IP address of the server? 104.127.88.102
4. What is the port number used by the server for the TCP session with the client? 80

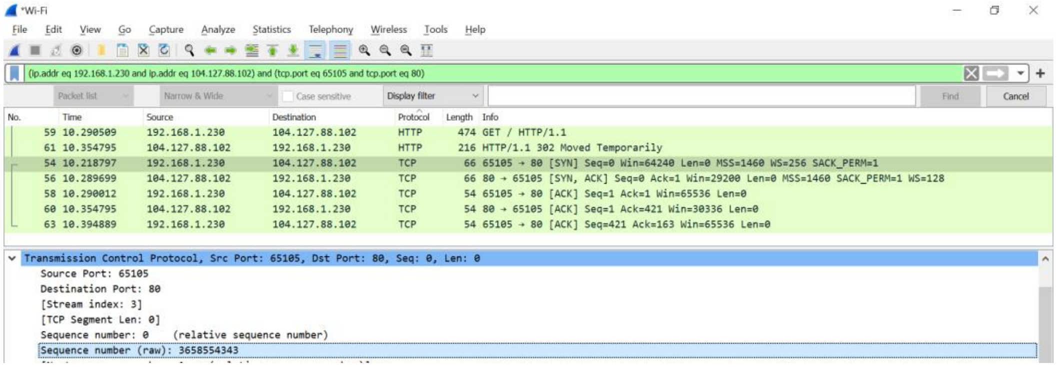


```
(ip.addr eq 192.168.1.230 and ip.addr eq 104.127.88.102) and (tcp.port eq 65105 and tcp.port eq 80)

No.   Time        Source           Destination      Protocol  Length  Info
  59  10.290509   192.168.1.230    104.127.88.102   HTTP        474   GET / HTTP/1.1
  61  10.354795   104.127.88.102   192.168.1.230    HTTP        216   HTTP/1.1 302 Moved Temporarily
  54  10.218797   192.168.1.230    104.127.88.102   TCP          66   65105 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  56  10.289699   104.127.88.102   192.168.1.230    TCP          66   80 → 65105 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
  58  10.290012   192.168.1.230    104.127.88.102   TCP          54   65105 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
  60  10.354795   104.127.88.102   192.168.1.230    TCP          54   80 → 65105 [ACK] Seq=1 Ack=421 Win=30336 Len=0
  63  10.394889   192.168.1.230    104.127.88.102   TCP          54   65105 → 80 [ACK] Seq=421 Ack=163 Win=65536 Len=0

> Frame 59: 474 bytes on wire (3792 bits), 474 bytes captured (3792 bits) on interface \Device\NPF_{56CE63E9-1A3E-44F8-A519-60D5145B2301}, id 0
> Ethernet II, Src: IntelCor_3d:37:f9 (98:2c:bc:3d:37:f9), Dst: ARRISGro_55:b2:00 (74:8a:0d:55:b2:00)
> Internet Protocol Version 4, Src: 192.168.1.230, Dst: 104.127.88.102
v Transmission Control Protocol, Src Port: 65105, Dst Port: 80, Seq: 1, Ack: 1, Len: 420
```

5. What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and the server?
   Absolute (raw) sequence number: 3658554343
   Relative sequence number: 0

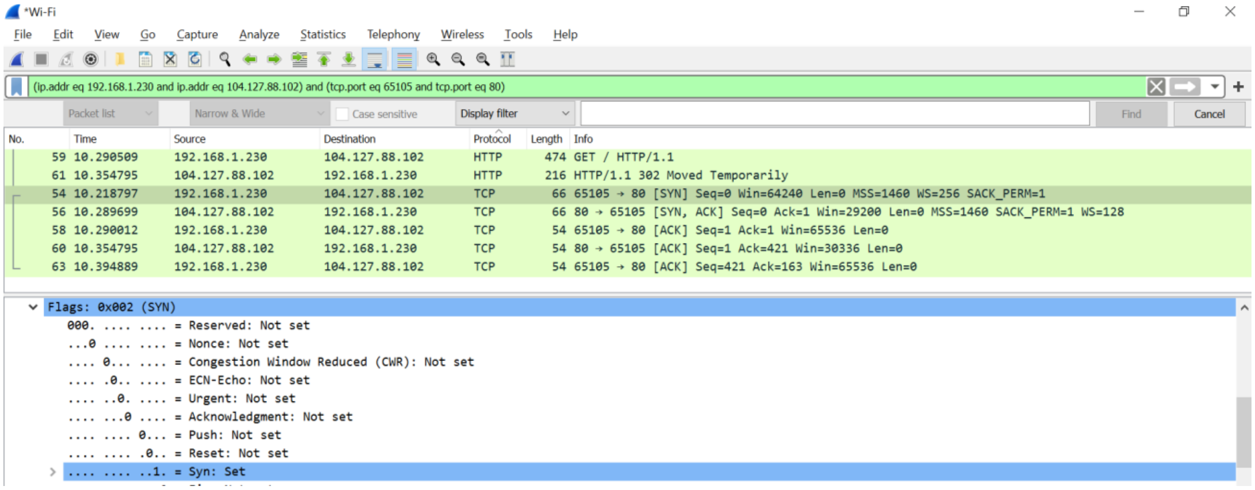


```
(ip.addr eq 192.168.1.230 and ip.addr eq 104.127.88.102) and (tcp.port eq 65105 and tcp.port eq 80)

No.   Time        Source           Destination      Protocol  Length  Info
  59  10.290509   192.168.1.230    104.127.88.102   HTTP        474   GET / HTTP/1.1
  61  10.354795   104.127.88.102   192.168.1.230    HTTP        216   HTTP/1.1 302 Moved Temporarily
  54  10.218797   192.168.1.230    104.127.88.102   TCP          66   65105 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  56  10.289699   104.127.88.102   192.168.1.230    TCP          66   80 → 65105 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
  58  10.290012   192.168.1.230    104.127.88.102   TCP          54   65105 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
  60  10.354795   104.127.88.102   192.168.1.230    TCP          54   80 → 65105 [ACK] Seq=1 Ack=421 Win=30336 Len=0
  63  10.394889   192.168.1.230    104.127.88.102   TCP          54   65105 → 80 [ACK] Seq=421 Ack=163 Win=65536 Len=0

v Transmission Control Protocol, Src Port: 65105, Dst Port: 80, Seq: 0, Len: 0
    Source Port: 65105
    Destination Port: 80
    [Stream index: 3]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    Sequence number (raw): 3658554343
```

6. What field and value in that field in the TCP segment identifies the segment as a SYN segment?
   Field: Syn (tcp.flags.syn) , value: Set (1) (under Flags)

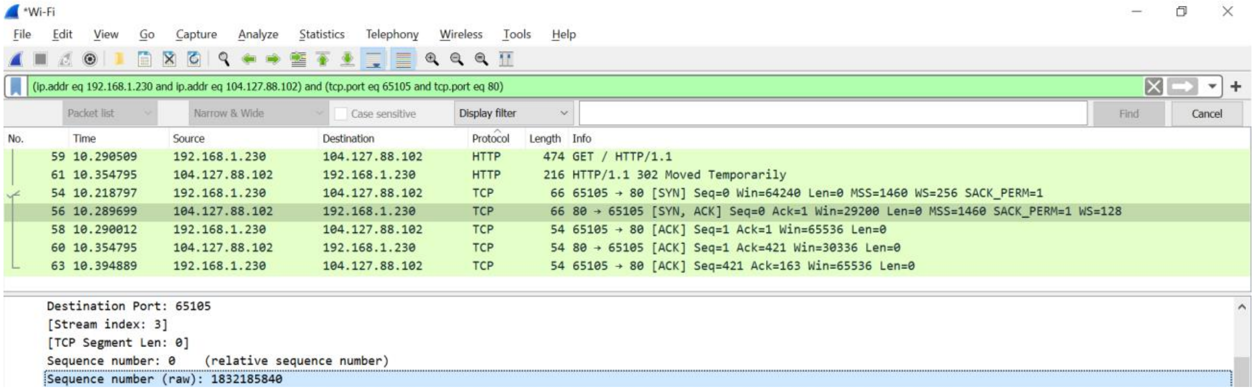


```
(ip.addr eq 192.168.1.230 and ip.addr eq 104.127.88.102) and (tcp.port eq 65105 and tcp.port eq 80)

No.  Time       Source          Destination     Protocol Length Info
  59 10.290509  192.168.1.230   104.127.88.102  HTTP     474 GET / HTTP/1.1
  61 10.354795  104.127.88.102  192.168.1.230   HTTP     216 HTTP/1.1 302 Moved Temporarily
  54 10.218797  192.168.1.230   104.127.88.102  TCP       66 65105 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  56 10.289699  104.127.88.102  192.168.1.230   TCP       66 80 → 65105 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
  58 10.290012  192.168.1.230   104.127.88.102  TCP       54 65105 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
  60 10.354795  104.127.88.102  192.168.1.230   TCP       54 80 → 65105 [ACK] Seq=1 Ack=421 Win=30336 Len=0
  63 10.394889  192.168.1.230   104.127.88.102  TCP       54 65105 → 80 [ACK] Seq=421 Ack=163 Win=65536 Len=0

Flags: 0x002 (SYN)
    000. .... .... = Reserved: Not set
    ...0 .... .... = Nonce: Not set
    .... 0... .... = Congestion Window Reduced (CWR): Not set
    .... .0.. .... = ECN-Echo: Not set
    .... ..0. .... = Urgent: Not set
    .... ...0 .... = Acknowledgment: Not set
    .... .... 0... = Push: Not set
    .... .... .0.. = Reset: Not set
    .... .... ..1. = Syn: Set
```

7. What is the sequence number of the SYN/ACK segment sent by the server to the client in reply to the SYN from the client?
   Absolute (raw) sequence number: 1832185840
   Relative sequence number: 0

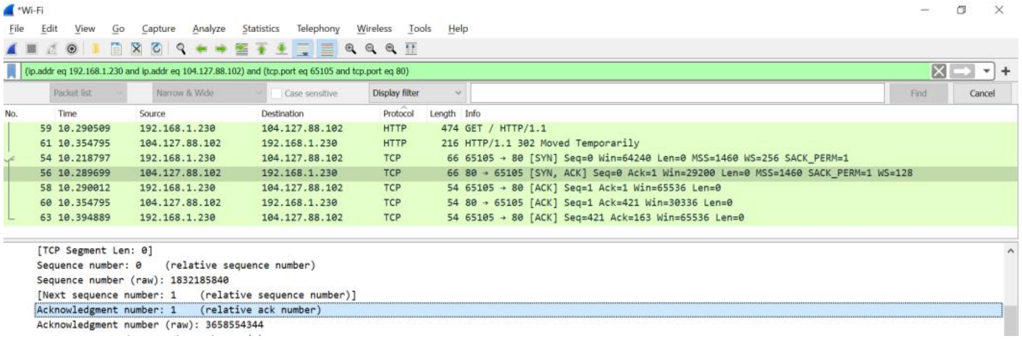


```
(ip.addr eq 192.168.1.230 and ip.addr eq 104.127.88.102) and (tcp.port eq 65105 and tcp.port eq 80)

No.  Time       Source          Destination     Protocol Length Info
  59 10.290509  192.168.1.230   104.127.88.102  HTTP     474 GET / HTTP/1.1
  61 10.354795  104.127.88.102  192.168.1.230   HTTP     216 HTTP/1.1 302 Moved Temporarily
  54 10.218797  192.168.1.230   104.127.88.102  TCP       66 65105 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  56 10.289699  104.127.88.102  192.168.1.230   TCP       66 80 → 65105 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
  58 10.290012  192.168.1.230   104.127.88.102  TCP       54 65105 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
  60 10.354795  104.127.88.102  192.168.1.230   TCP       54 80 → 65105 [ACK] Seq=1 Ack=421 Win=30336 Len=0
  63 10.394889  192.168.1.230   104.127.88.102  TCP       54 65105 → 80 [ACK] Seq=421 Ack=163 Win=65536 Len=0

Destination Port: 65105
[Stream index: 3]
[TCP Segment Len: 0]
Sequence number: 0    (relative sequence number)
Sequence number (raw): 1832185840
```

8. What is the value of the acknowledgement number in the SYN/ACK segment sent by the server to the client?
   Absolute (raw) ack number: 3658554344
   Relative ack number: 1



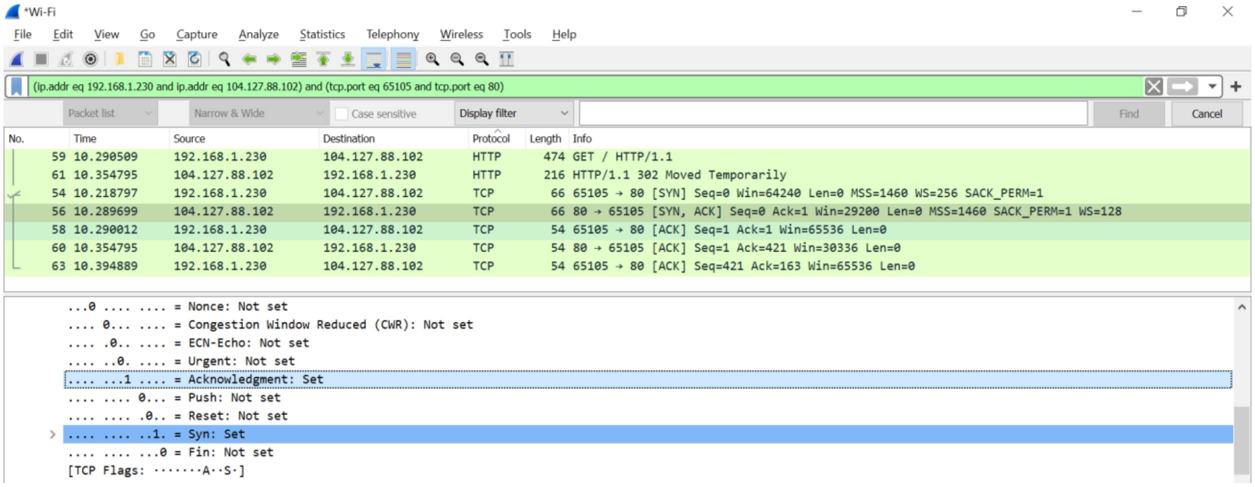
```
(ip.addr eq 192.168.1.230 and ip.addr eq 104.127.88.102) and (tcp.port eq 65105 and tcp.port eq 80)

No.  Time       Source          Destination     Protocol Length Info
  59 10.290509  192.168.1.230   104.127.88.102  HTTP     474 GET / HTTP/1.1
  61 10.354795  104.127.88.102  192.168.1.230   HTTP     216 HTTP/1.1 302 Moved Temporarily
  54 10.218797  192.168.1.230   104.127.88.102  TCP       66 65105 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  56 10.289699  104.127.88.102  192.168.1.230   TCP       66 80 → 65105 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
  58 10.290012  192.168.1.230   104.127.88.102  TCP       54 65105 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
  60 10.354795  104.127.88.102  192.168.1.230   TCP       54 80 → 65105 [ACK] Seq=1 Ack=421 Win=30336 Len=0
  63 10.394889  192.168.1.230   104.127.88.102  TCP       54 65105 → 80 [ACK] Seq=421 Ack=163 Win=65536 Len=0

[TCP Segment Len: 0]
Sequence number: 0    (relative sequence number)
Sequence number (raw): 1832185840
[Next sequence number: 1    (relative sequence number)]
Acknowledgment number: 1    (relative ack number)
Acknowledgment number (raw): 3658554344
```

9. What does this acknowledgment number indicate?
   The acknowledgement number is set to 1 to indicate the receipt of the client's SYN flag in packet #1. It also indicates that the sequence number of the next byte the receiver expects to receive is 1.

10. What field in the TCP segment and value in that field identifies the segment as a SYN/ACK segment?
    Under flags:
    Field: Acknowledgment (tcp.flags.ack), value: Set (1)
    Field: Syn (tcp.flags.syn) , value: Set (1)

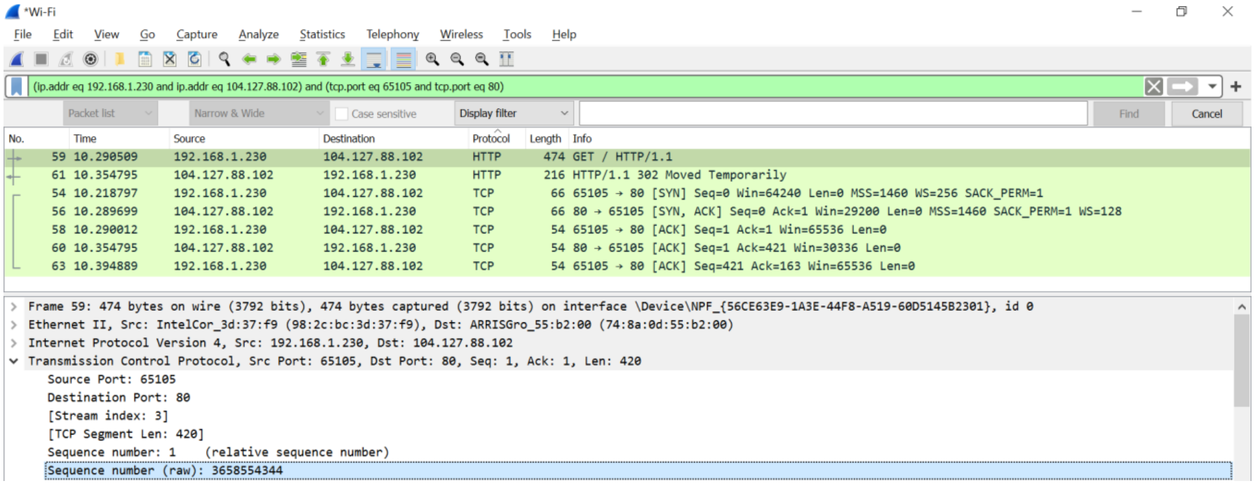

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Packet list
Narrow & Wide
Case sensitive
Display filter
Find
Cancel

(ip.addr eq 192.168.1.230 and ip.addr eq 104.127.88.102) and (tcp.port eq 65105 and tcp.port eq 80)

```
No.   Time        Source           Destination      Protocol  Length  Info
   59 10.290509   192.168.1.230    104.127.88.102   HTTP       474 GET / HTTP/1.1
   61 10.354795   104.127.88.102   192.168.1.230    HTTP       216 HTTP/1.1 302 Moved Temporarily
   54 10.218797   192.168.1.230    104.127.88.102   TCP         66 65105 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
   56 10.289699   104.127.88.102   192.168.1.230    TCP         66 80 → 65105 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
   58 10.290012   192.168.1.230    104.127.88.102   TCP         54 65105 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
   60 10.354795   104.127.88.102   192.168.1.230    TCP         54 80 → 65105 [ACK] Seq=1 Ack=421 Win=30336 Len=0
   63 10.394889   192.168.1.230    104.127.88.102   TCP         54 65105 → 80 [ACK] Seq=421 Ack=163 Win=65536 Len=0
```

```
...0 .... .... = Nonce: Not set
.... 0... .... = Congestion Window Reduced (CWR): Not set
.... .0.. .... = ECN-Echo: Not set
.... ..0. .... = Urgent: Not set
.... ...1 .... = Acknowledgment: Set
.... .... 0... = Push: Not set
.... .... .0.. = Reset: Not set
.... .... ..1. = Syn: Set
.... .... ...0 = Fin: Not set
[TCP Flags: ·······A··S·]
```

11. Locate the first GET message sent to the server. What is the sequence number of this message?
    Absolute (raw) sequence number: 3658554344
    Relative sequence number: 1

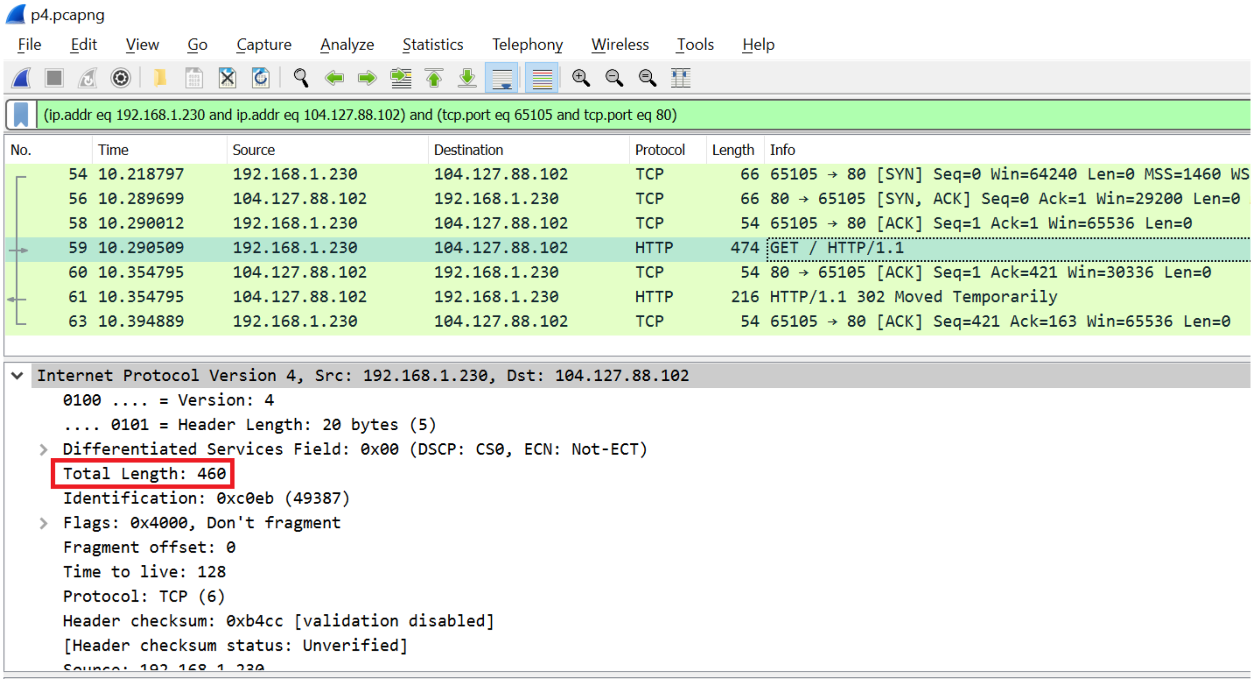

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Packet list
Narrow & Wide
Case sensitive
Display filter
Find
Cancel

(ip.addr eq 192.168.1.230 and ip.addr eq 104.127.88.102) and (tcp.port eq 65105 and tcp.port eq 80)

```
No.   Time        Source           Destination      Protocol  Length  Info
   59 10.290509   192.168.1.230    104.127.88.102   HTTP       474 GET / HTTP/1.1
   61 10.354795   104.127.88.102   192.168.1.230    HTTP       216 HTTP/1.1 302 Moved Temporarily
   54 10.218797   192.168.1.230    104.127.88.102   TCP         66 65105 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
   56 10.289699   104.127.88.102   192.168.1.230    TCP         66 80 → 65105 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
   58 10.290012   192.168.1.230    104.127.88.102   TCP         54 65105 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
   60 10.354795   104.127.88.102   192.168.1.230    TCP         54 80 → 65105 [ACK] Seq=1 Ack=421 Win=30336 Len=0
   63 10.394889   192.168.1.230    104.127.88.102   TCP         54 65105 → 80 [ACK] Seq=421 Ack=163 Win=65536 Len=0
```

```
> Frame 59: 474 bytes on wire (3792 bits), 474 bytes captured (3792 bits) on interface \Device\NPF_{56CE63E9-1A3E-44F8-A519-60D5145B2301}, id 0
> Ethernet II, Src: IntelCor_3d:37:f9 (98:2c:bc:3d:37:f9), Dst: ARRISGro_55:b2:00 (74:8a:0d:55:b2:00)
> Internet Protocol Version 4, Src: 192.168.1.230, Dst: 104.127.88.102
v Transmission Control Protocol, Src Port: 65105, Dst Port: 80, Seq: 1, Ack: 1, Len: 420
    Source Port: 65105
    Destination Port: 80
    [Stream index: 3]
    [TCP Segment Len: 420]
    Sequence number: 1    (relative sequence number)
    Sequence number (raw): 3658554344
```

12. What is the total length of the HTTP request containing the GET? 460 bytes

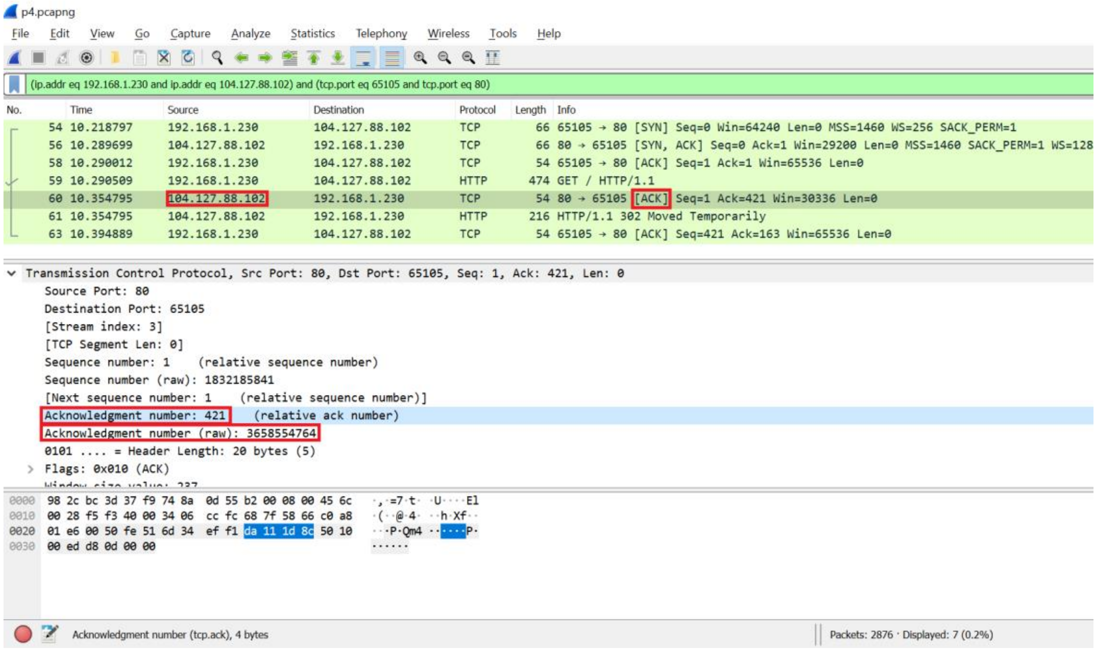


(ip.addr eq 192.168.1.230 and ip.addr eq 104.127.88.102) and (tcp.port eq 65105 and tcp.port eq 80)

```
No.     Time       Source          Destination     Protocol  Length Info
     54 10.218797  192.168.1.230   104.127.88.102  TCP          66 65105 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS
     56 10.289699  104.127.88.102  192.168.1.230   TCP          66 80 → 65105 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0
     58 10.290012  192.168.1.230   104.127.88.102  TCP          54 65105 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
     59 10.290509  192.168.1.230   104.127.88.102  HTTP        474 GET / HTTP/1.1
     60 10.354795  104.127.88.102  192.168.1.230   TCP          54 80 → 65105 [ACK] Seq=1 Ack=421 Win=30336 Len=0
     61 10.354795  104.127.88.102  192.168.1.230   HTTP        216 HTTP/1.1 302 Moved Temporarily
     63 10.394889  192.168.1.230   104.127.88.102  TCP          54 65105 → 80 [ACK] Seq=421 Ack=163 Win=65536 Len=0
```

```
v Internet Protocol Version 4, Src: 192.168.1.230, Dst: 104.127.88.102
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 460
    Identification: 0xc0eb (49387)
  > Flags: 0x4000, Don't fragment
    Fragment offset: 0
    Time to live: 128
    Protocol: TCP (6)
    Header checksum: 0xb4cc [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.230
```

13. Yes, the acknowledgment number agrees with what I would expect which is 421 (figure 13.a). Since the sequence number of the previous segment (figure 13.b) was 1 and its TCP segment length (TCP payload) was 420, so the acknowledgment number of the current segment should be 1 (previous seq #) + 420 (previous segment's TCP payload) = 421



```
(ip.addr eq 192.168.1.230 and ip.addr eq 104.127.88.102) and (tcp.port eq 65105 and tcp.port eq 80)
```

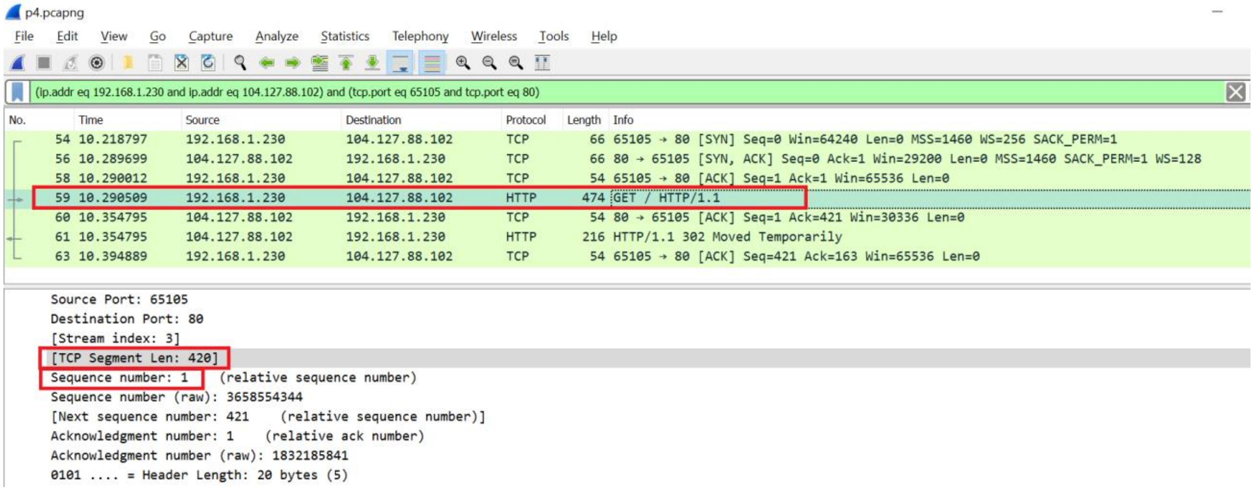
```
No.  Time        Source          Destination     Protocol  Length  Info
 54  10.218797   192.168.1.230   104.127.88.102  TCP           66  65105 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
 56  10.289699   104.127.88.102  192.168.1.230   TCP           66  80 → 65105 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
 58  10.290012   192.168.1.230   104.127.88.102  TCP           54  65105 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
 59  10.290509   192.168.1.230   104.127.88.102  HTTP         474  GET / HTTP/1.1
 60  10.354795   104.127.88.102  192.168.1.230   TCP           54  80 → 65105 [ACK] Seq=1 Ack=421 Win=30336 Len=0
 61  10.354795   104.127.88.102  192.168.1.230   HTTP         216  HTTP/1.1 302 Moved Temporarily
 63  10.394889   192.168.1.230   104.127.88.102  TCP           54  65105 → 80 [ACK] Seq=421 Ack=163 Win=65536 Len=0
```

```
v Transmission Control Protocol, Src Port: 80, Dst Port: 65105, Seq: 1, Ack: 421, Len: 0
    Source Port: 80
    Destination Port: 65105
    [Stream index: 3]
    [TCP Segment Len: 0]
    Sequence number: 1    (relative sequence number)
    Sequence number (raw): 1832185841
    [Next sequence number: 1    (relative sequence number)]
    Acknowledgment number: 421    (relative ack number)
    Acknowledgment number (raw): 3658554764
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x010 (ACK)
    Window size value: 237
```

```
0000  98 2c bc 3d 37 f9 74 8a  0d 55 b2 00 08 00 45 6c   ·,·=7·t· ·U····El
0010  00 28 f5 f3 40 00 34 06  cc fc 68 7f 58 66 c0 a8   ·(··@·4· ··h·Xf··
0020  01 e6 00 50 fe 51 6d 34  ef f1 da 11 1d 8c 50 10   ···P·Qm4 ······P·
0030  00 ed d8 0d 00 00                                  ······
```

Acknowledgment number (tcp.ack), 4 bytes   Packets: 2876 · Displayed: 7 (0.2%)

Figure 13.a



```
(ip.addr eq 192.168.1.230 and ip.addr eq 104.127.88.102) and (tcp.port eq 65105 and tcp.port eq 80)
```

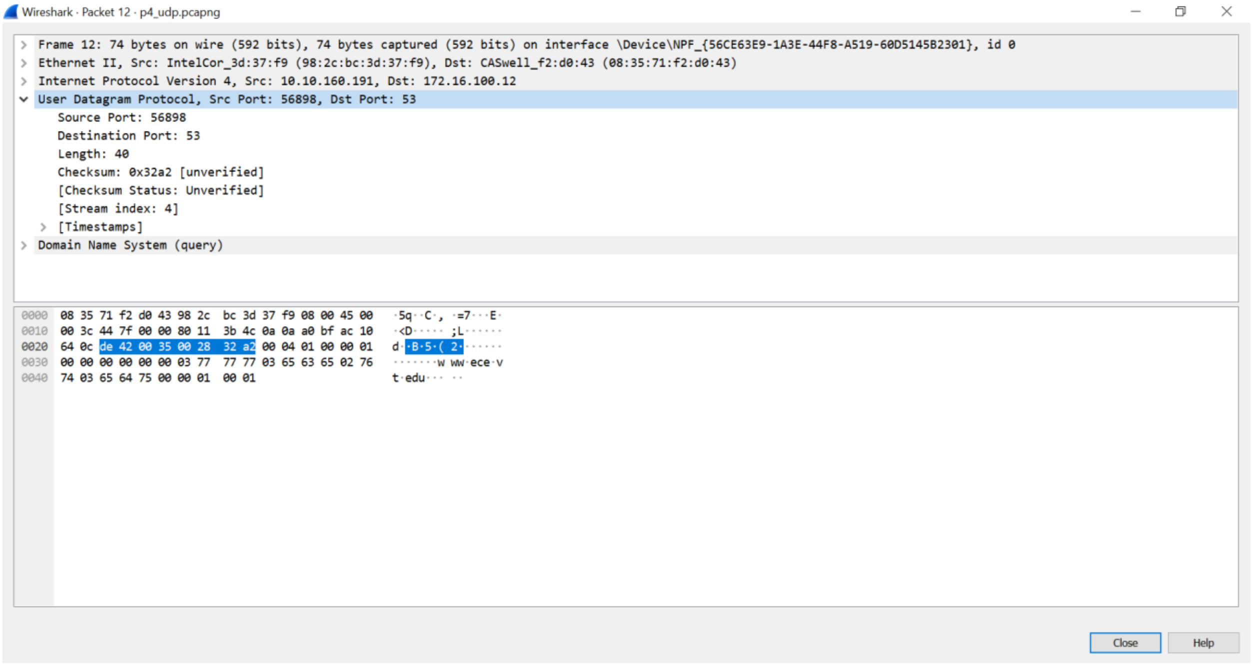
```
No.  Time        Source          Destination     Protocol  Length  Info
 54  10.218797   192.168.1.230   104.127.88.102  TCP           66  65105 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
 56  10.289699   104.127.88.102  192.168.1.230   TCP           66  80 → 65105 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
 58  10.290012   192.168.1.230   104.127.88.102  TCP           54  65105 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
 59  10.290509   192.168.1.230   104.127.88.102  HTTP         474  GET / HTTP/1.1
 60  10.354795   104.127.88.102  192.168.1.230   TCP           54  80 → 65105 [ACK] Seq=1 Ack=421 Win=30336 Len=0
 61  10.354795   104.127.88.102  192.168.1.230   HTTP         216  HTTP/1.1 302 Moved Temporarily
 63  10.394889   192.168.1.230   104.127.88.102  TCP           54  65105 → 80 [ACK] Seq=421 Ack=163 Win=65536 Len=0
```

```
    Source Port: 65105
    Destination Port: 80
    [Stream index: 3]
    [TCP Segment Len: 420]
    Sequence number: 1    (relative sequence number)
    Sequence number (raw): 3658554344
    [Next sequence number: 421    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    Acknowledgment number (raw): 1832185841
    0101 .... = Header Length: 20 bytes (5)
```

Figure 13.b

2.2. UDP:

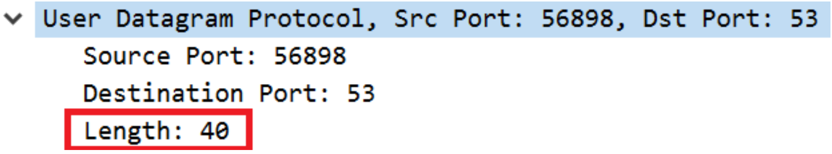
14. The UDP header has a fixed length of 8 bytes. Each of these 4 header fields is 2 bytes long.
    a. Source port, length: 2 bytes, value: 56898
    b. Destination port, length: 2 bytes, value: 53
    c. Length, length: 2 bytes, value: 40
    d. Checksum, length: 2 bytes, value: 0x000032a2



```
> Frame 12: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{56CE63E9-1A3E-44F8-A519-60D5145B2301}, id 0
> Ethernet II, Src: IntelCor_3d:37:f9 (98:2c:bc:3d:37:f9), Dst: CASwell_f2:d0:43 (08:35:71:f2:d0:43)
> Internet Protocol Version 4, Src: 10.10.160.191, Dst: 172.16.100.12
v User Datagram Protocol, Src Port: 56898, Dst Port: 53
     Source Port: 56898
     Destination Port: 53
     Length: 40
     Checksum: 0x32a2 [unverified]
     [Checksum Status: Unverified]
     [Stream index: 4]
   > [Timestamps]
> Domain Name System (query)

0000  08 35 71 f2 d0 43 98 2c  bc 3d 37 f9 08 00 45 00   ·5q··C·, ·=7···E·
0010  00 3c 44 7f 00 00 80 11  3b 4c 0a 0a a0 bf ac 10   ·<D····· ;L······
0020  64 0c de 42 00 35 00 28  32 a2 00 04 01 00 00 01   d··B·5·( 2·······
0030  00 00 00 00 00 00 03 77  77 77 03 65 63 65 02 76   ·······w ww·ece·v
0040  74 03 65 64 75 00 00 01  00 01                     t·edu··· ··
```

15. The length field specifies the number of bytes in the UDP segment (header plus data). An explicit length value is needed since the size of the data field may differ from one UDP segment to the next.

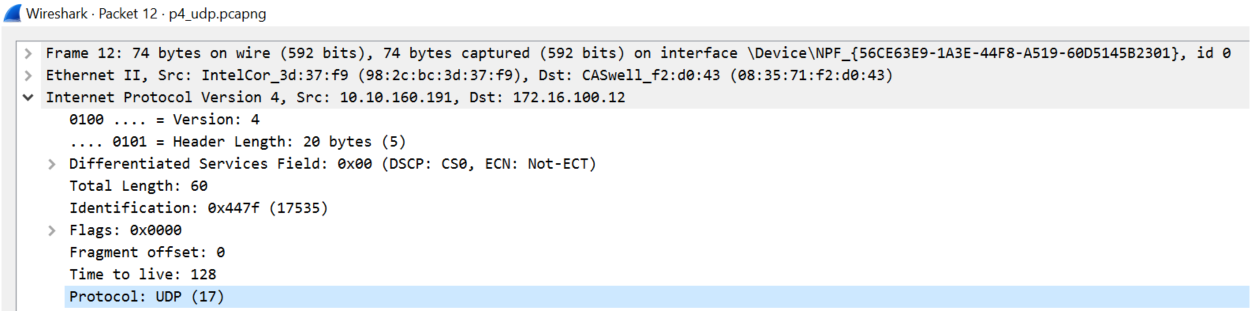


```
v User Datagram Protocol, Src Port: 56898, Dst Port: 53
     Source Port: 56898
     Destination Port: 53
     Length: 40
```

16. What is the maximum number of bytes that can be included in a UDP payload?
    The maximum number of bytes that can be included in a UDP payload is (2^16 – 1) bytes plus the header bytes. This gives 65535 bytes – 8 bytes = 65527 bytes.

17. What is the protocol number associated with UDP?

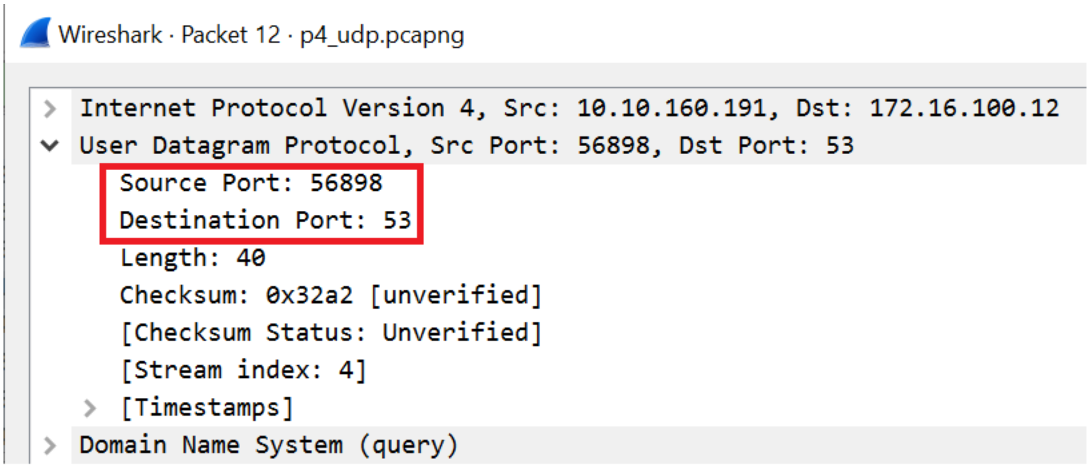
    17



Wireshark · Packet 12 · p4_udp.pcapng

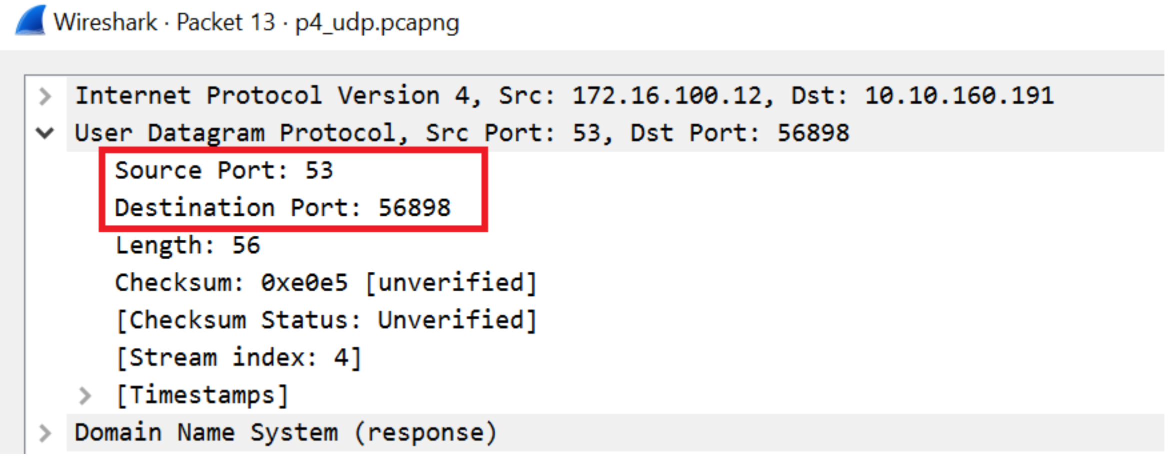
```
> Frame 12: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{56CE63E9-1A3E-44F8-A519-60D5145B2301}, id 0
> Ethernet II, Src: IntelCor_3d:37:f9 (98:2c:bc:3d:37:f9), Dst: CASwell_f2:d0:43 (08:35:71:f2:d0:43)
v Internet Protocol Version 4, Src: 10.10.160.191, Dst: 172.16.100.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0x447f (17535)
  > Flags: 0x0000
    Fragment offset: 0
    Time to live: 128
    Protocol: UDP (17)
```

18. The source port of the UDP packet sent by the host is the same as the destination port of the reply packet, and conversely the destination port of the UDP packet sent by the host is the same as the source port of the reply packet.



Wireshark · Packet 12 · p4_udp.pcapng

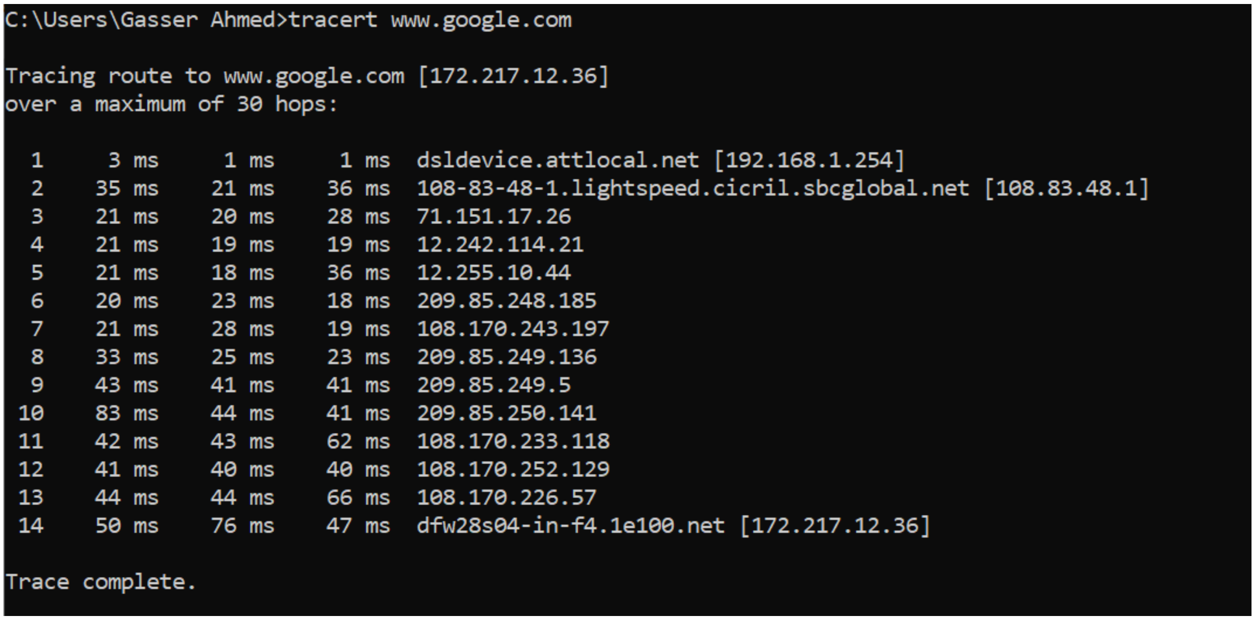
```
> Internet Protocol Version 4, Src: 10.10.160.191, Dst: 172.16.100.12
v User Datagram Protocol, Src Port: 56898, Dst Port: 53
    Source Port: 56898
    Destination Port: 53
    Length: 40
    Checksum: 0x32a2 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 4]
  > [Timestamps]
> Domain Name System (query)
```



Wireshark · Packet 13 · p4_udp.pcapng

```
> Internet Protocol Version 4, Src: 172.16.100.12, Dst: 10.10.160.191
v User Datagram Protocol, Src Port: 53, Dst Port: 56898
    Source Port: 53
    Destination Port: 56898
    Length: 56
    Checksum: 0xe0e5 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 4]
  > [Timestamps]
> Domain Name System (response)
```

2.3. IP:



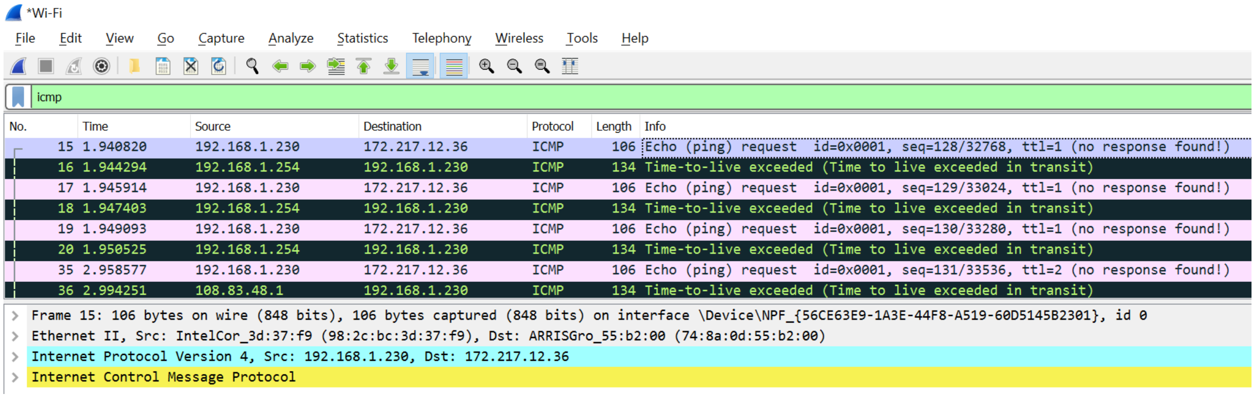
```
C:\Users\Gasser Ahmed>tracert www.google.com

Tracing route to www.google.com [172.217.12.36]
over a maximum of 30 hops:

  1     3 ms     1 ms     1 ms  dsldevice.attlocal.net [192.168.1.254]
  2    35 ms    21 ms    36 ms  108-83-48-1.lightspeed.cicril.sbcglobal.net [108.83.48.1]
  3    21 ms    20 ms    28 ms  71.151.17.26
  4    21 ms    19 ms    19 ms  12.242.114.21
  5    21 ms    18 ms    36 ms  12.255.10.44
  6    20 ms    23 ms    18 ms  209.85.248.185
  7    21 ms    28 ms    19 ms  108.170.243.197
  8    33 ms    25 ms    23 ms  209.85.249.136
  9    43 ms    41 ms    41 ms  209.85.249.5
 10    83 ms    44 ms    41 ms  209.85.250.141
 11    42 ms    43 ms    62 ms  108.170.233.118
 12    41 ms    40 ms    40 ms  108.170.252.129
 13    44 ms    44 ms    66 ms  108.170.226.57
 14    50 ms    76 ms    47 ms  dfw28s04-in-f4.1e100.net [172.217.12.36]

Trace complete.
```

19. The traceroute (tracert) operation used ICMP

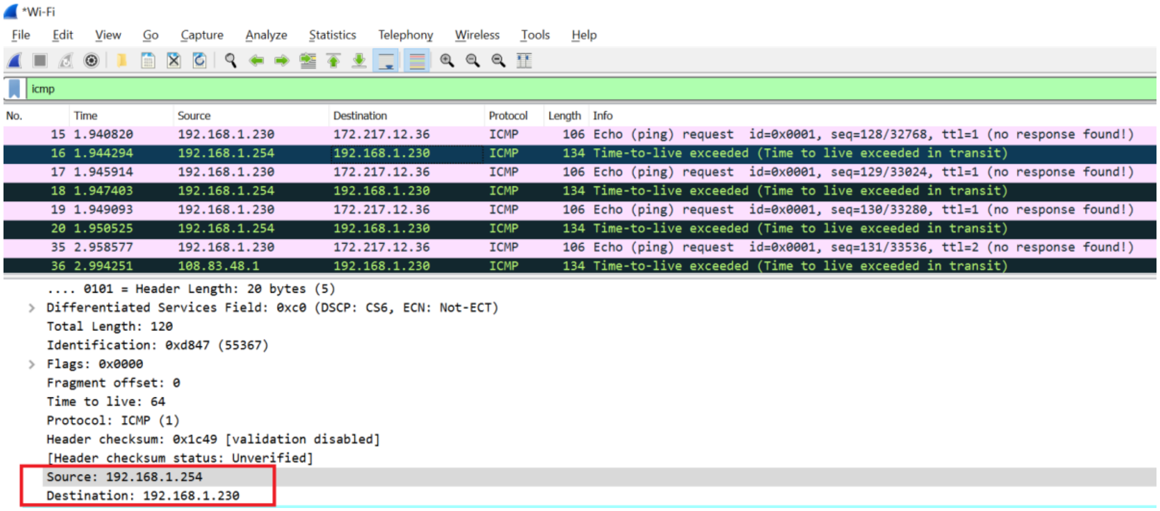


icmp

```
No.   Time       Source          Destination     Protocol  Length  Info
   15 1.940820   192.168.1.230   172.217.12.36   ICMP      106 Echo (ping) request  id=0x0001, seq=128/32768, ttl=1 (no response found!)
   16 1.944294   192.168.1.254   192.168.1.230   ICMP      134 Time-to-live exceeded (Time to live exceeded in transit)
   17 1.945914   192.168.1.230   172.217.12.36   ICMP      106 Echo (ping) request  id=0x0001, seq=129/33024, ttl=1 (no response found!)
   18 1.947403   192.168.1.254   192.168.1.230   ICMP      134 Time-to-live exceeded (Time to live exceeded in transit)
   19 1.949093   192.168.1.230   172.217.12.36   ICMP      106 Echo (ping) request  id=0x0001, seq=130/33280, ttl=1 (no response found!)
   20 1.950525   192.168.1.254   192.168.1.230   ICMP      134 Time-to-live exceeded (Time to live exceeded in transit)
   35 2.958577   192.168.1.230   172.217.12.36   ICMP      106 Echo (ping) request  id=0x0001, seq=131/33536, ttl=2 (no response found!)
   36 2.994251   108.83.48.1     192.168.1.230   ICMP      134 Time-to-live exceeded (Time to live exceeded in transit)

> Frame 15: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF_{56CE63E9-1A3E-44F8-A519-60D5145B2301}, id 0
> Ethernet II, Src: IntelCor_3d:37:f9 (98:2c:bc:3d:37:f9), Dst: ARRISGro_55:b2:00 (74:8a:0d:55:b2:00)
> Internet Protocol Version 4, Src: 192.168.1.230, Dst: 172.217.12.36
> Internet Control Message Protocol
```

20. 192.168.1.254

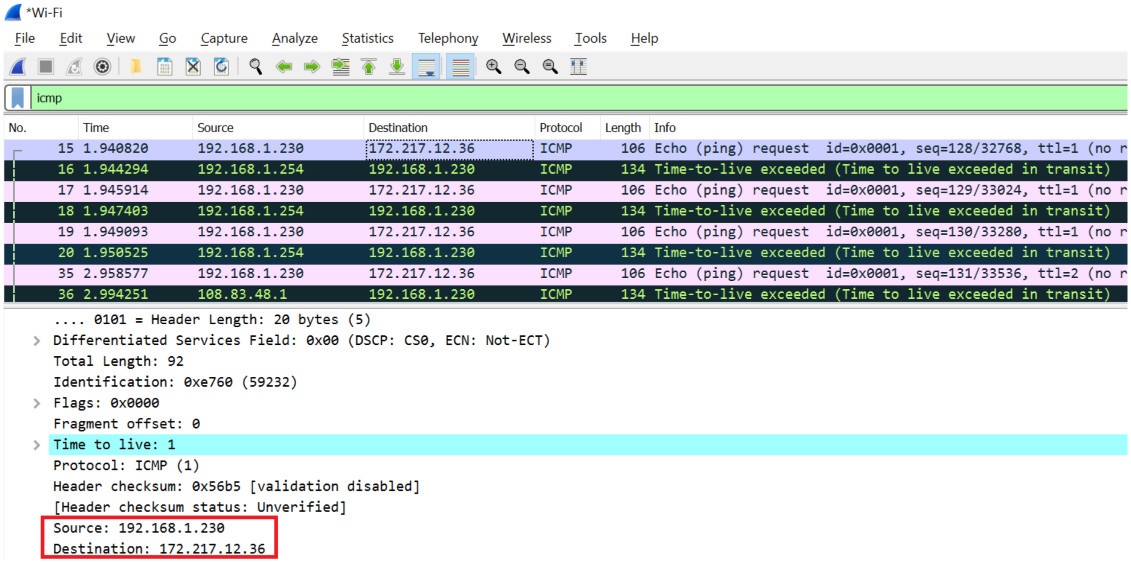


icmp

```
No.   Time       Source          Destination     Protocol  Length  Info
   15 1.940820   192.168.1.230   172.217.12.36   ICMP      106 Echo (ping) request  id=0x0001, seq=128/32768, ttl=1 (no response found!)
   16 1.944294   192.168.1.254   192.168.1.230   ICMP      134 Time-to-live exceeded (Time to live exceeded in transit)
   17 1.945914   192.168.1.230   172.217.12.36   ICMP      106 Echo (ping) request  id=0x0001, seq=129/33024, ttl=1 (no response found!)
   18 1.947403   192.168.1.254   192.168.1.230   ICMP      134 Time-to-live exceeded (Time to live exceeded in transit)
   19 1.949093   192.168.1.230   172.217.12.36   ICMP      106 Echo (ping) request  id=0x0001, seq=130/33280, ttl=1 (no response found!)
   20 1.950525   192.168.1.254   192.168.1.230   ICMP      134 Time-to-live exceeded (Time to live exceeded in transit)
   35 2.958577   192.168.1.230   172.217.12.36   ICMP      106 Echo (ping) request  id=0x0001, seq=131/33536, ttl=2 (no response found!)
   36 2.994251   108.83.48.1     192.168.1.230   ICMP      134 Time-to-live exceeded (Time to live exceeded in transit)

    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
    Total Length: 120
    Identification: 0xd847 (55367)
  > Flags: 0x0000
    Fragment offset: 0
    Time to live: 64
    Protocol: ICMP (1)
    Header checksum: 0x1c49 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.254
    Destination: 192.168.1.230
```

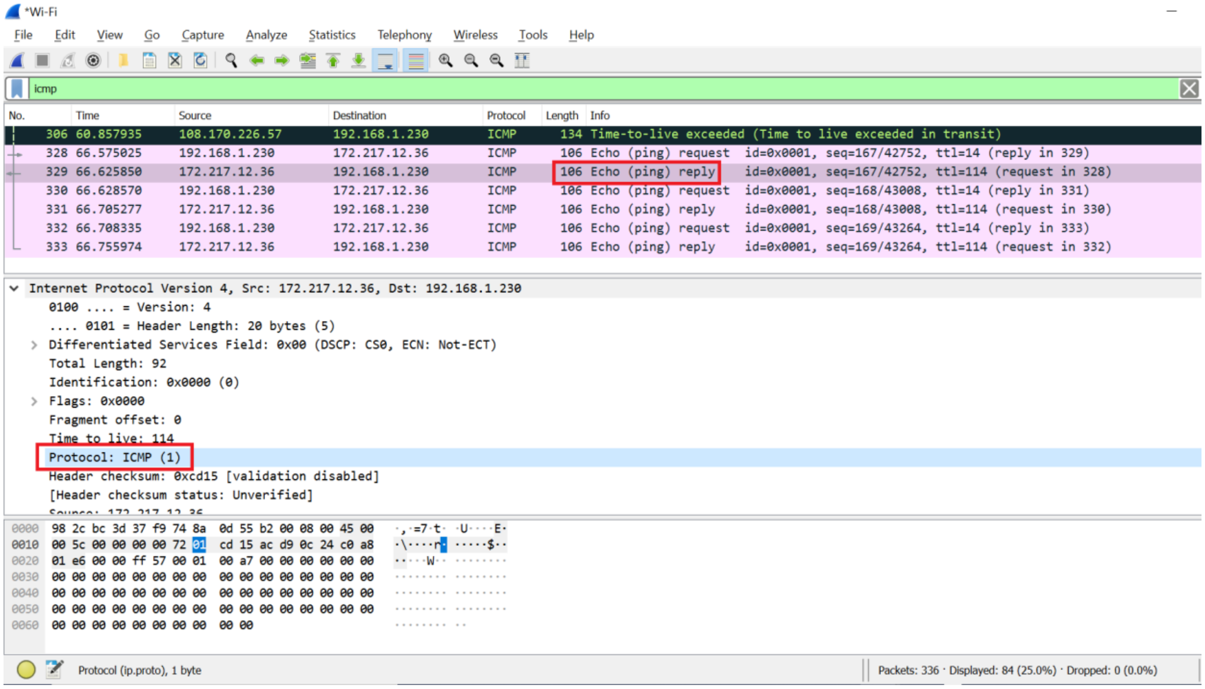
21. No



```
No.   Time       Source          Destination     Protocol Length Info
   15 1.940820   192.168.1.230   172.217.12.36   ICMP      106 Echo (ping) request  id=0x0001, seq=128/32768, ttl=1 (no r
   16 1.944294   192.168.1.254   192.168.1.230   ICMP      134 Time-to-live exceeded (Time to live exceeded in transit)
   17 1.945914   192.168.1.230   172.217.12.36   ICMP      106 Echo (ping) request  id=0x0001, seq=129/33024, ttl=1 (no r
   18 1.947403   192.168.1.254   192.168.1.230   ICMP      134 Time-to-live exceeded (Time to live exceeded in transit)
   19 1.949093   192.168.1.230   172.217.12.36   ICMP      106 Echo (ping) request  id=0x0001, seq=130/33280, ttl=1 (no r
   20 1.950525   192.168.1.254   192.168.1.230   ICMP      134 Time-to-live exceeded (Time to live exceeded in transit)
   35 2.958577   192.168.1.230   172.217.12.36   ICMP      106 Echo (ping) request  id=0x0001, seq=131/33536, ttl=2 (no r
   36 2.994251   108.83.48.1     192.168.1.230   ICMP      134 Time-to-live exceeded (Time to live exceeded in transit)
```

```
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 92
    Identification: 0xe760 (59232)
  > Flags: 0x0000
    Fragment offset: 0
  > Time to live: 1
    Protocol: ICMP (1)
    Header checksum: 0x56b5 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.230
    Destination: 172.217.12.36
```

22. ICMP (1)



```
No.   Time        Source           Destination     Protocol Length Info
  306 60.857935   108.170.226.57   192.168.1.230   ICMP      134 Time-to-live exceeded (Time to live exceeded in transit)
  328 66.575025   192.168.1.230    172.217.12.36   ICMP      106 Echo (ping) request  id=0x0001, seq=167/42752, ttl=14 (reply in 329)
  329 66.625850   172.217.12.36    192.168.1.230   ICMP      106 Echo (ping) reply    id=0x0001, seq=167/42752, ttl=114 (request in 328)
  330 66.628570   192.168.1.230    172.217.12.36   ICMP      106 Echo (ping) request  id=0x0001, seq=168/43008, ttl=14 (reply in 331)
  331 66.705277   172.217.12.36    192.168.1.230   ICMP      106 Echo (ping) reply    id=0x0001, seq=168/43008, ttl=114 (request in 330)
  332 66.708335   192.168.1.230    172.217.12.36   ICMP      106 Echo (ping) request  id=0x0001, seq=169/43264, ttl=14 (reply in 333)
  333 66.755974   172.217.12.36    192.168.1.230   ICMP      106 Echo (ping) reply    id=0x0001, seq=169/43264, ttl=114 (request in 332)
```

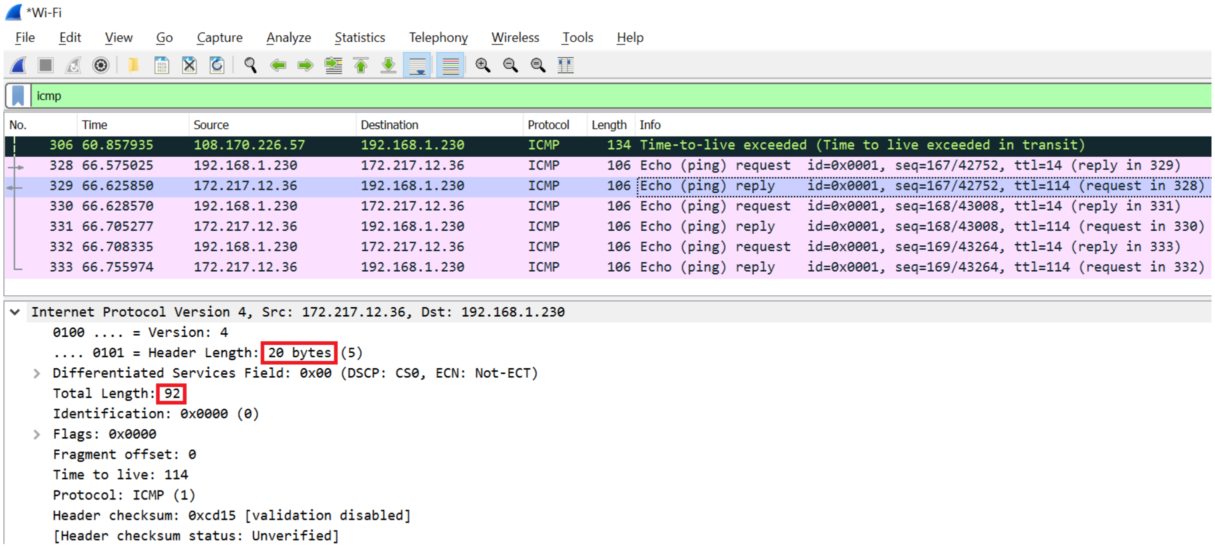
```
v Internet Protocol Version 4, Src: 172.217.12.36, Dst: 192.168.1.230
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 92
    Identification: 0x0000 (0)
  > Flags: 0x0000
    Fragment offset: 0
    Time to live: 114
    Protocol: ICMP (1)
    Header checksum: 0xcd15 [validation disabled]
    [Header checksum status: Unverified]
    Source: 172.217.12.36
```

```
0000  98 2c bc 3d 37 f9 74 8a  0d 55 b2 00 08 00 45 00   ·,·=7·t· ·U····E·
0010  00 5c 00 00 00 00 72 01  cd 15 ac d9 0c 24 c0 a8   ·\····r· ·····$··
0020  01 e6 00 00 ff 57 00 01  00 a7 00 00 00 00 00 00   ·····W·· ········
0030  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0060  00 00 00 00 00 00 00 00  00 00                     ········ ··
```

Protocol (ip.proto), 1 byte   Packets: 336 · Displayed: 84 (25.0%) · Dropped: 0 (0.0%)

23. The Protocol field in the IPv4 header contains a number indicating the type of data found in the payload portion of the datagram. It also provides a demultiplexing feature so that the IP protocol can be used to carry payloads of more than one protocol type.

24. 20 bytes



```
No.     Time          Source           Destination      Protocol  Length  Info
    306 60.857935     108.170.226.57   192.168.1.230    ICMP         134  Time-to-live exceeded (Time to live exceeded in transit)
    328 66.575025     192.168.1.230    172.217.12.36    ICMP         106  Echo (ping) request  id=0x0001, seq=167/42752, ttl=14 (reply in 329)
    329 66.625850     172.217.12.36    192.168.1.230    ICMP         106  Echo (ping) reply    id=0x0001, seq=167/42752, ttl=114 (request in 328)
    330 66.628570     192.168.1.230    172.217.12.36    ICMP         106  Echo (ping) request  id=0x0001, seq=168/43008, ttl=14 (reply in 331)
    331 66.705277     172.217.12.36    192.168.1.230    ICMP         106  Echo (ping) reply    id=0x0001, seq=168/43008, ttl=114 (request in 330)
    332 66.708335     192.168.1.230    172.217.12.36    ICMP         106  Echo (ping) request  id=0x0001, seq=169/43264, ttl=14 (reply in 333)
    333 66.755974     172.217.12.36    192.168.1.230    ICMP         106  Echo (ping) reply    id=0x0001, seq=169/43264, ttl=114 (request in 332)
```

```
Internet Protocol Version 4, Src: 172.217.12.36, Dst: 192.168.1.230
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 92
    Identification: 0x0000 (0)
  > Flags: 0x0000
    Fragment offset: 0
    Time to live: 114
    Protocol: ICMP (1)
    Header checksum: 0xcd15 [validation disabled]
    [Header checksum status: Unverified]
```

25. Number of bytes in the payload of the IP datagram = total length – header length

= 92 – 20 = 72 bytes

Section 3 – Conclusions:

After going through the TCP, UDP, and IP Capture and Analysis phases, I was able to become more familiar with Wireshark network analysis and have a better understanding how it works with different internet protocols. Also, using learning new commands like *nslookup* and *tracert* was very helpful in understanding those internet protocols. However, the nslookup part in the UDP section was a little tricky as it wasn't giving me any response until I used a different network i.e. WiFi then it started to give me the expected results.

In general, the project clarified how different protocols work and behave. Lastly, the approximate number of hours I devoted to the project was about 12-16 hours.
