【高等電腦網路】

作業別 ： 【HW1】

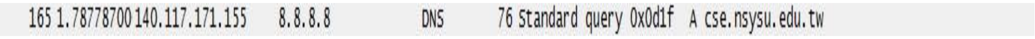
學號、姓名 ：M043040026 蒲宏易

作業內容 ：

Part1 Web Browsing (DNS, TCP) :

1. Find the first DNS request packet sent by the client.(Request for cse.nsysu.edu.tw) You can find a record like below on Wireshark. And you can answer the question.

(query picture) :



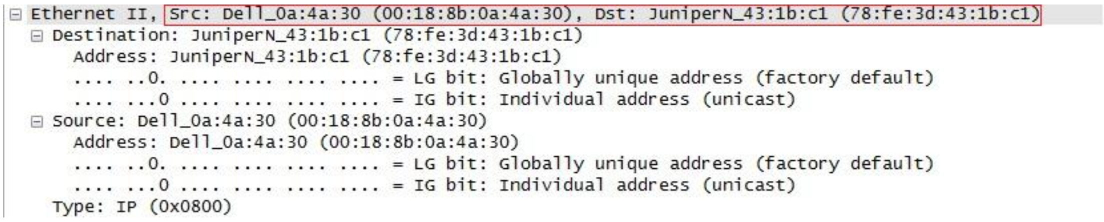
```
165 1.78778700 140.117.171.155   8.8.8.8        DNS    76 Standard query 0x0d1f  A cse.nsysu.edu.tw
```

- (1) Examine the Ethernet

a. What is the Ethernet address of the source and destination?

A : Source : Dell_0a:4a:30(00:18:8b:0a:4a:30)

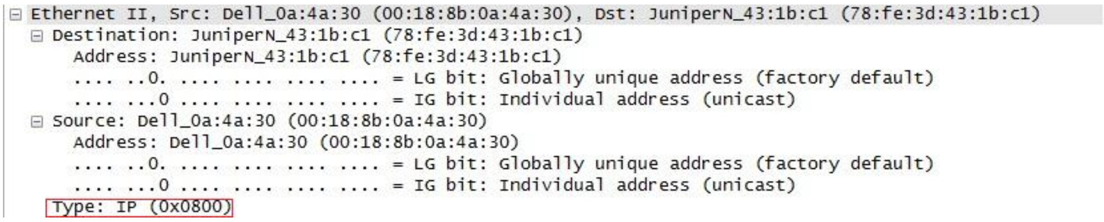
Destination : JuniperN_43:1b:c1 (78:fe:3d:43:1b:c1)



```
⊟ Ethernet II, Src: Dell_0a:4a:30 (00:18:8b:0a:4a:30), Dst: JuniperN_43:1b:c1 (78:fe:3d:43:1b:c1)
  ⊟ Destination: JuniperN_43:1b:c1 (78:fe:3d:43:1b:c1)
      Address: JuniperN_43:1b:c1 (78:fe:3d:43:1b:c1)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ⊟ Source: Dell_0a:4a:30 (00:18:8b:0a:4a:30)
      Address: Dell_0a:4a:30 (00:18:8b:0a:4a:30)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IP (0x0800)
```

b. what is the content of the type field in the Ethernet frame?

A : IP (0x0800)

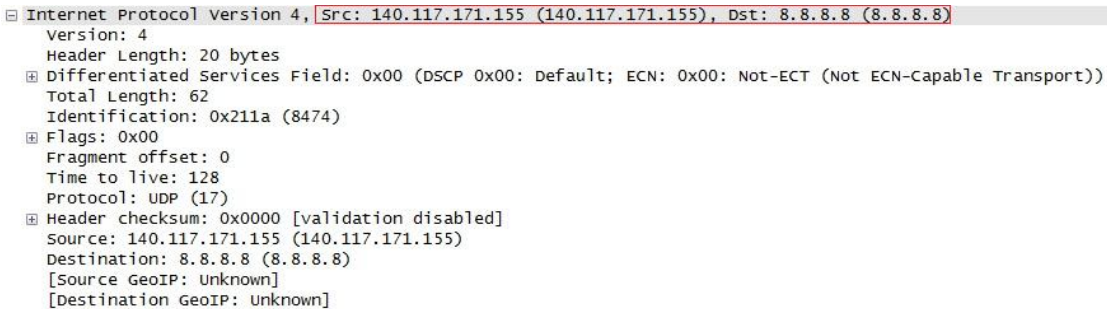


```
⊟ Ethernet II, Src: Dell_0a:4a:30 (00:18:8b:0a:4a:30), Dst: JuniperN_43:1b:c1 (78:fe:3d:43:1b:c1)
  ⊟ Destination: JuniperN_43:1b:c1 (78:fe:3d:43:1b:c1)
      Address: JuniperN_43:1b:c1 (78:fe:3d:43:1b:c1)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ⊟ Source: Dell_0a:4a:30 (00:18:8b:0a:4a:30)
      Address: Dell_0a:4a:30 (00:18:8b:0a:4a:30)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IP (0x0800)
```

- (2) Examine the Internet Protocol

a. What is the IP address of the source and destination?

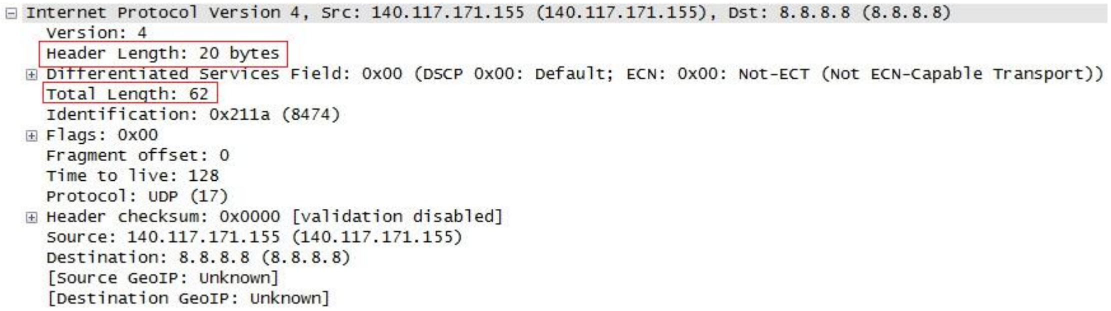
A : Source : 140.117.171.155 , Destination : 8.8.8.8



```
⊟ Internet Protocol Version 4, Src: 140.117.171.155 (140.117.171.155), Dst: 8.8.8.8 (8.8.8.8)
    Version: 4
    Header Length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 62
    Identification: 0x211a (8474)
  ⊞ Flags: 0x00
    Fragment offset: 0
    Time to live: 128
    Protocol: UDP (17)
  ⊞ Header checksum: 0x0000 [validation disabled]
    Source: 140.117.171.155 (140.117.171.155)
    Destination: 8.8.8.8 (8.8.8.8)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
```

b. What is the header length? What is the total packet length?

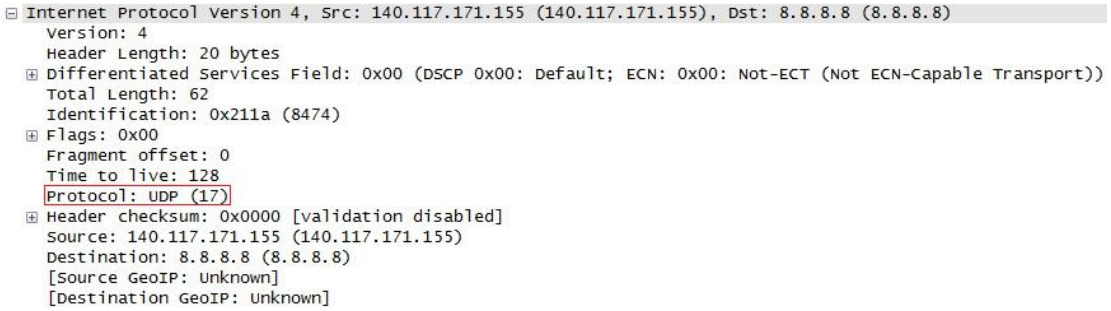
A : header length : 20 bytes , total packet length : 62 bytes



```
⊟ Internet Protocol Version 4, Src: 140.117.171.155 (140.117.171.155), Dst: 8.8.8.8 (8.8.8.8)
    Version: 4
    Header Length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 62
    Identification: 0x211a (8474)
  ⊞ Flags: 0x00
    Fragment offset: 0
    Time to live: 128
    Protocol: UDP (17)
  ⊞ Header checksum: 0x0000 [validation disabled]
    Source: 140.117.171.155 (140.117.171.155)
    Destination: 8.8.8.8 (8.8.8.8)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
```

c. Identify the protocol type field. What is the number and type of the protocol in the payload?

A : UDP (17)

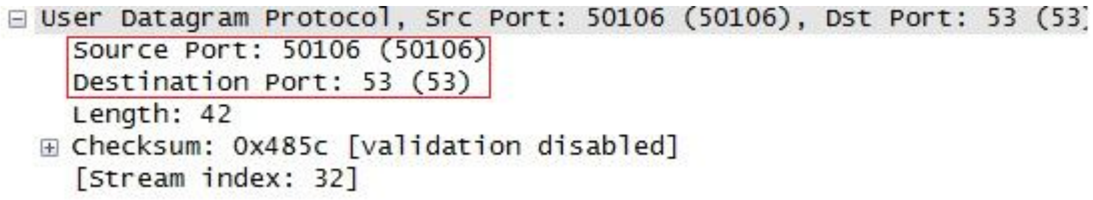


```
⊟ Internet Protocol Version 4, Src: 140.117.171.155 (140.117.171.155), Dst: 8.8.8.8 (8.8.8.8)
    Version: 4
    Header Length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 62
    Identification: 0x211a (8474)
  ⊞ Flags: 0x00
    Fragment offset: 0
    Time to live: 128
    Protocol: UDP (17)
  ⊞ Header checksum: 0x0000 [validation disabled]
    Source: 140.117.171.155 (140.117.171.155)
    Destination: 8.8.8.8 (8.8.8.8)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
```

- (3) Examine the User Datagram Protocol

a. Identify the client ephemeral port number and the server well-known port number .

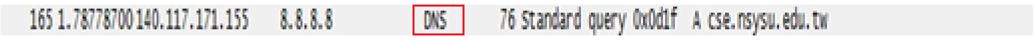
A : client port : 50106 , server port : 53



```
⊟ User Datagram Protocol, Src Port: 50106 (50106), Dst Port: 53 (53)
    Source Port: 50106 (50106)
    Destination Port: 53 (53)
    Length: 42
  ⊞ Checksum: 0x485c [validation disabled]
    [Stream index: 32]
```

b. What type of application layer protocol is in the payload?

A : DNS , DNS use Port 53 on UDP protocol.

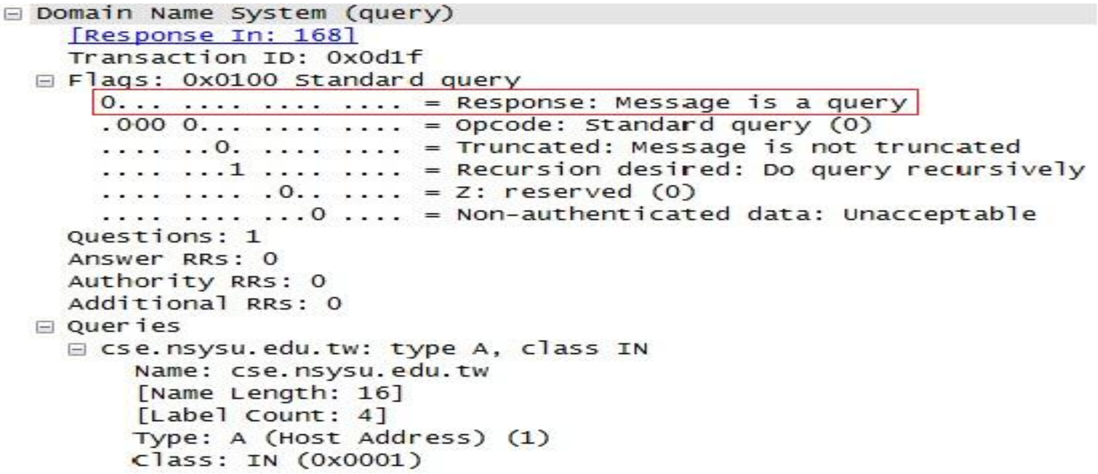


```
165 1.78778700 140.117.171.155   8.8.8.8   DNS   76 Standard query 0x0d1f  A cse.nsysu.edu.tw
```

- (4) Examine the Domain Name System (query)

a. What field indicates whether the message is a query or a response?

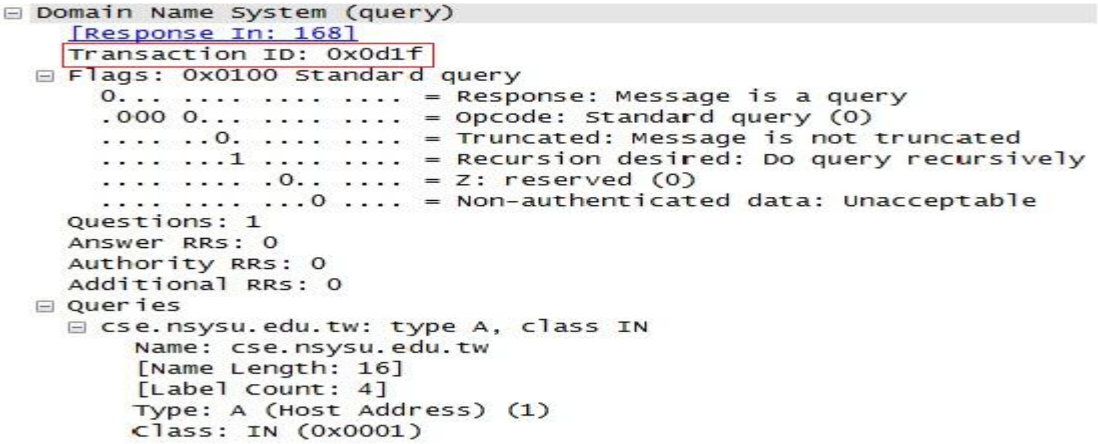
A : Flags highest bit , 0 = query



```
⊟ Domain Name System (query)
    [Response In: 168]
    Transaction ID: 0x0d1f
  ⊟ Flags: 0x0100 Standard query
      0... .... .... .... = Response: Message is a query
      .000 0... .... .... = Opcode: Standard query (0)
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... .0.. .... = Z: reserved (0)
      .... .... ...0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ⊟ Queries
    ⊟ cse.nsysu.edu.tw: type A, class IN
        Name: cse.nsysu.edu.tw
        [Name Length: 16]
        [Label Count: 4]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
```

b. What is the query transaction ID?

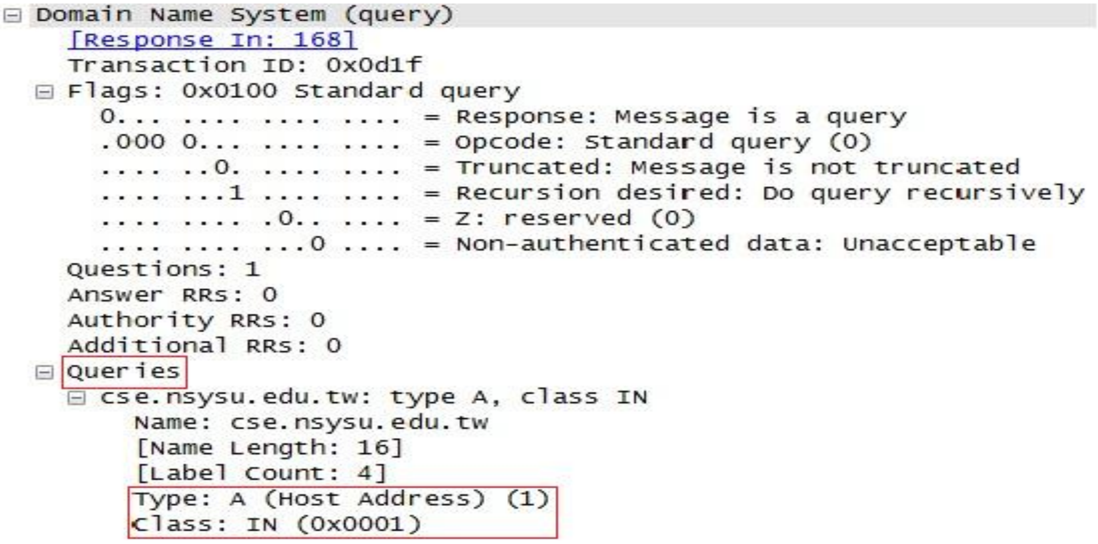
A : 0x0d1f



```
⊟ Domain Name System (query)
    [Response In: 168]
    Transaction ID: 0x0d1f
  ⊟ Flags: 0x0100 Standard query
      0... .... .... .... = Response: Message is a query
      .000 0... .... .... = Opcode: Standard query (0)
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... .0.. .... = Z: reserved (0)
      .... .... ...0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ⊟ Queries
    ⊟ cse.nsysu.edu.tw: type A, class IN
        Name: cse.nsysu.edu.tw
        [Name Length: 16]
        [Label Count: 4]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
```

c. Identify the fields that carry the type and class of the query.

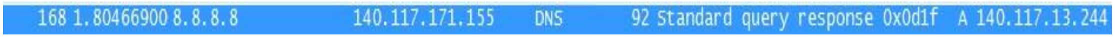
A : In the Queries , Type : A   Class : In



```
⊟ Domain Name System (query)
    [Response In: 168]
    Transaction ID: 0x0d1f
  ⊟ Flags: 0x0100 Standard query
      0... .... .... .... = Response: Message is a query
      .000 0... .... .... = Opcode: Standard query (0)
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... .0.. .... = Z: reserved (0)
      .... .... ...0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ⊟ Queries
    ⊟ cse.nsysu.edu.tw: type A, class IN
        Name: cse.nsysu.edu.tw
        [Name Length: 16]
        [Label Count: 4]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
```

2. Find the DNS response packet which is response to the DNS request packet from the above question. You can find a record like below on Wireshark. And you can answer the question.

(response picture):



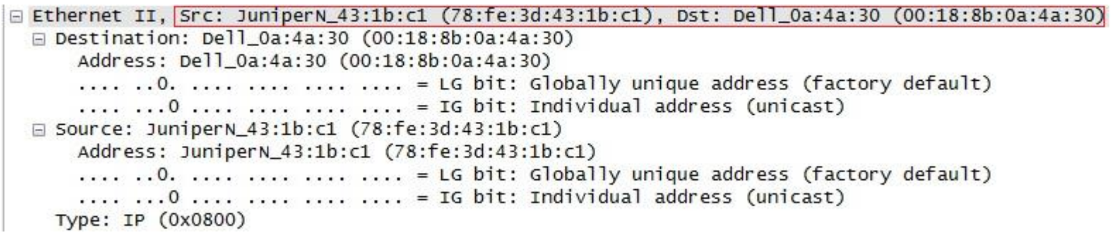
```
168 1.80466900 8.8.8.8          140.117.171.155     DNS       92 Standard query response 0x0d1f  A 140.117.13.244
```

- (1) Examine the Ethernet.

a. What is the Ethernet address of the source and destination?

A : Source : JuniperN_43:1b:c1 (78:fe:3d:43:1b:c1)

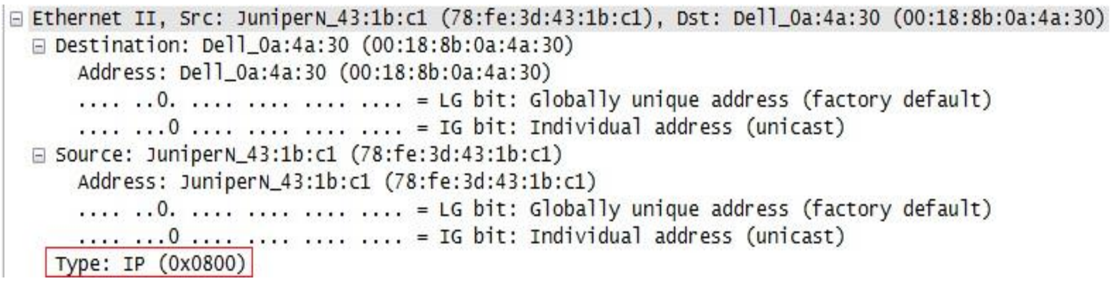
Destination : Dell_0a:4a:30(00:18:8b:0a:4a:30)



```
⊟ Ethernet II, Src: JuniperN_43:1b:c1 (78:fe:3d:43:1b:c1), Dst: Dell_0a:4a:30 (00:18:8b:0a:4a:30)
  ⊟ Destination: Dell_0a:4a:30 (00:18:8b:0a:4a:30)
      Address: Dell_0a:4a:30 (00:18:8b:0a:4a:30)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ⊟ Source: JuniperN_43:1b:c1 (78:fe:3d:43:1b:c1)
      Address: JuniperN_43:1b:c1 (78:fe:3d:43:1b:c1)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IP (0x0800)
```

b. What is the content of the type field in the Ethernet frame?

A : IP (0x0800)

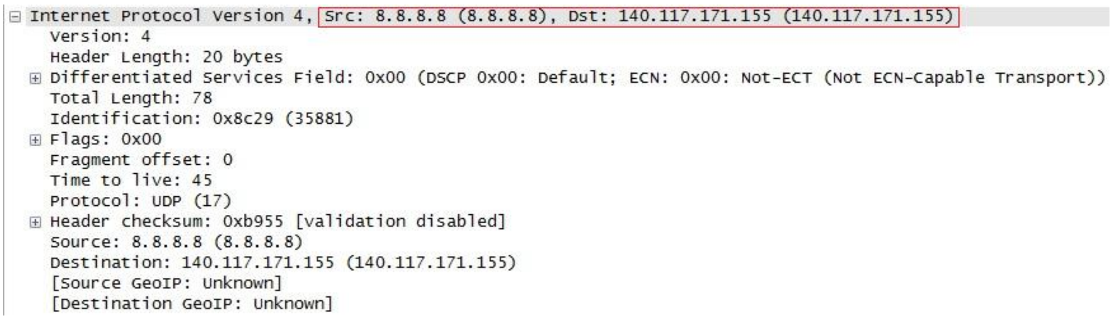


```
⊟ Ethernet II, Src: JuniperN_43:1b:c1 (78:fe:3d:43:1b:c1), Dst: Dell_0a:4a:30 (00:18:8b:0a:4a:30)
  ⊟ Destination: Dell_0a:4a:30 (00:18:8b:0a:4a:30)
      Address: Dell_0a:4a:30 (00:18:8b:0a:4a:30)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ⊟ Source: JuniperN_43:1b:c1 (78:fe:3d:43:1b:c1)
      Address: JuniperN_43:1b:c1 (78:fe:3d:43:1b:c1)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IP (0x0800)
```

- (2) Examine the Internet Protocol & Domain Name System (response)

a. What is the IP address of the source and destination?

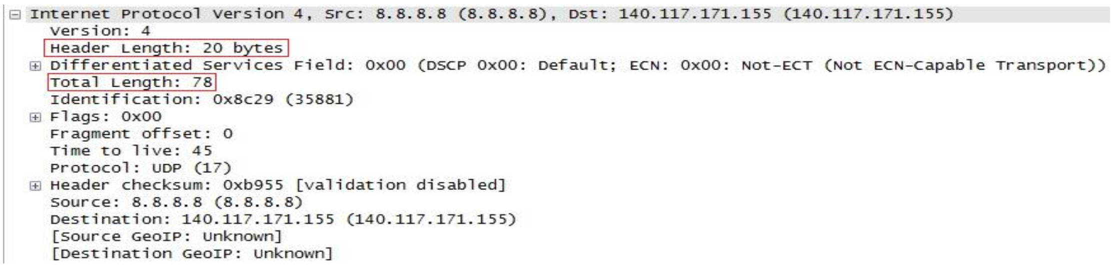
A : Source : 8.8.8.8 , Destination : 140.117.171.155



```
⊟ Internet Protocol Version 4, Src: 8.8.8.8 (8.8.8.8), Dst: 140.117.171.155 (140.117.171.155)
    Version: 4
    Header Length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 78
    Identification: 0x8c29 (35881)
  ⊞ Flags: 0x00
    Fragment offset: 0
    Time to live: 45
    Protocol: UDP (17)
  ⊞ Header checksum: 0xb955 [validation disabled]
    Source: 8.8.8.8 (8.8.8.8)
    Destination: 140.117.171.155 (140.117.171.155)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
```

b. What is the header length? What is the total packet length? Is it longer than the query?

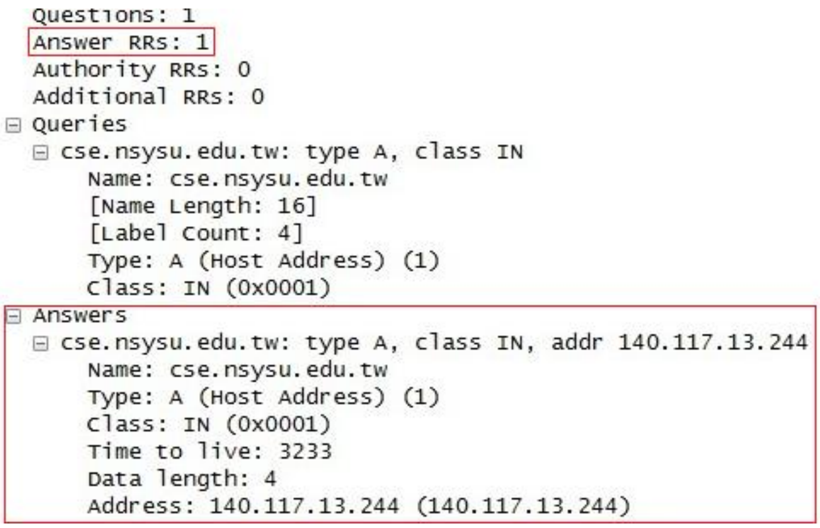
A : header length : 20 bytes , packet length : 78 bytes (longer than query's 68 bytes)



```
⊟ Internet Protocol Version 4, Src: 8.8.8.8 (8.8.8.8), Dst: 140.117.171.155 (140.117.171.155)
    Version: 4
    Header Length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 78
    Identification: 0x8c29 (35881)
  ⊞ Flags: 0x00
    Fragment offset: 0
    Time to live: 45
    Protocol: UDP (17)
  ⊞ Header checksum: 0xb955 [validation disabled]
    Source: 8.8.8.8 (8.8.8.8)
    Destination: 140.117.171.155 (140.117.171.155)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
```

c. How many answers are provided in the response message? Compare the answers and their time-to-live values.

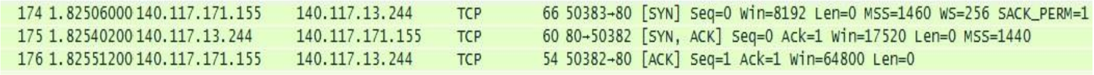
A : only 1 answer. Time-to-live is 3600.



```
  Questions: 1
  Answer RRs: 1
  Authority RRs: 0
  Additional RRs: 0
⊟ Queries
  ⊟ cse.nsysu.edu.tw: type A, class IN
      Name: cse.nsysu.edu.tw
      [Name Length: 16]
      [Label Count: 4]
      Type: A (Host Address) (1)
      Class: IN (0x0001)
⊟ Answers
  ⊟ cse.nsysu.edu.tw: type A, class IN, addr 140.117.13.244
      Name: cse.nsysu.edu.tw
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 3233
      Data length: 4
      Address: 140.117.13.244 (140.117.13.244)
```

3. Find the first TCP packet sent by client. (The destination IP address is response from above question.) You can find three record like below on Wireshark. It's TCP three-way handshake.

(Three-way handshake picture) :

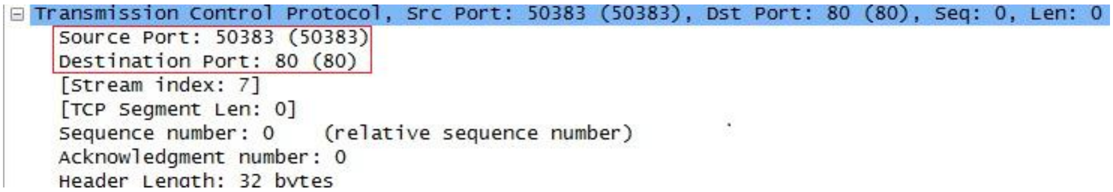


```
174 1.82506000 140.117.171.155   140.117.13.244    TCP    66 50383→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
175 1.82540200 140.117.13.244    140.117.171.155   TCP    60 80→50382 [SYN, ACK] Seq=0 Ack=1 Win=17520 Len=0 MSS=1440
176 1.82551200 140.117.171.155   140.117.13.244    TCP    54 50382→80 [ACK] Seq=1 Ack=1 Win=64800 Len=0
```

- (1) Examine the Transmission Control Protocol.

a. What are the ephemeral port number used by the client and the well-known port number used by the server?

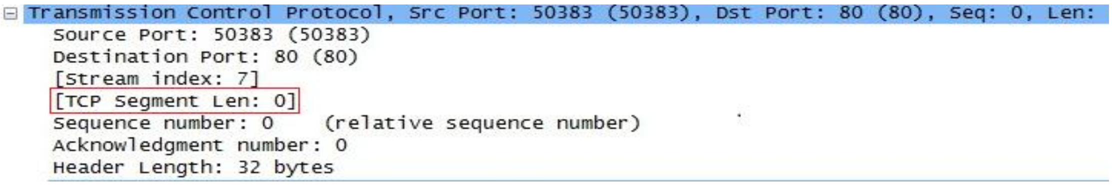
A : client port : 50383 , server port : 80



```
⊟ Transmission Control Protocol, Src Port: 50383 (50383), Dst Port: 80 (80), Seq: 0, Len: 0
    Source Port: 50383 (50383)
    Destination Port: 80 (80)
    [Stream index: 7]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    Acknowledgment number: 0
    Header Length: 32 bytes
```

b. What is the length of the TCP segment?

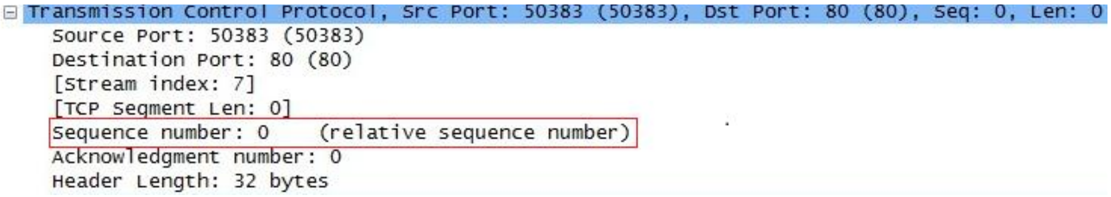
A : 0



```
⊟ Transmission Control Protocol, Src Port: 50383 (50383), Dst Port: 80 (80), Seq: 0, Len:
    Source Port: 50383 (50383)
    Destination Port: 80 (80)
    [Stream index: 7]
    [TCP Segment Len: 0]
    Sequence number: 0     (relative sequence number)
    Acknowledgment number: 0
    Header Length: 32 bytes
```

c. What is the initial sequence number for the segments from the client to the server?

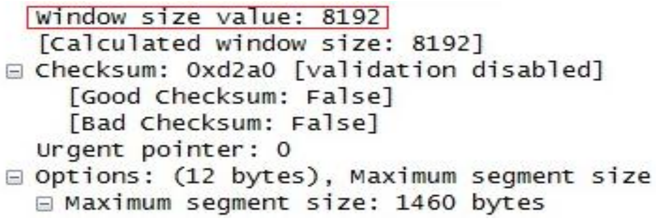
A : 0



```
⊟ Transmission Control Protocol, Src Port: 50383 (50383), Dst Port: 80 (80), Seq: 0, Len: 0
    Source Port: 50383 (50383)
    Destination Port: 80 (80)
    [Stream index: 7]
    [TCP Segment Len: 0]
    Sequence number: 0     (relative sequence number)
    Acknowledgment number: 0
    Header Length: 32 bytes
```

d. What is the initial window size?

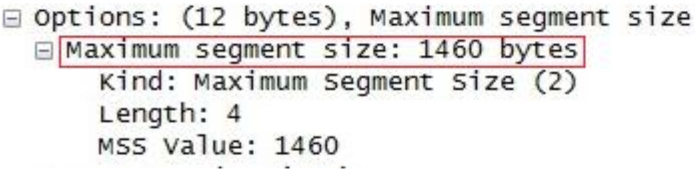
A : 8192



```
  Window size value: 8192
  [Calculated window size: 8192]
⊟ Checksum: 0xd2a0 [validation disabled]
    [Good Checksum: False]
    [Bad Checksum: False]
  Urgent pointer: 0
⊟ Options: (12 bytes), Maximum segment size
  ⊟ Maximum segment size: 1460 bytes
```

e. What is the maximum segment size?

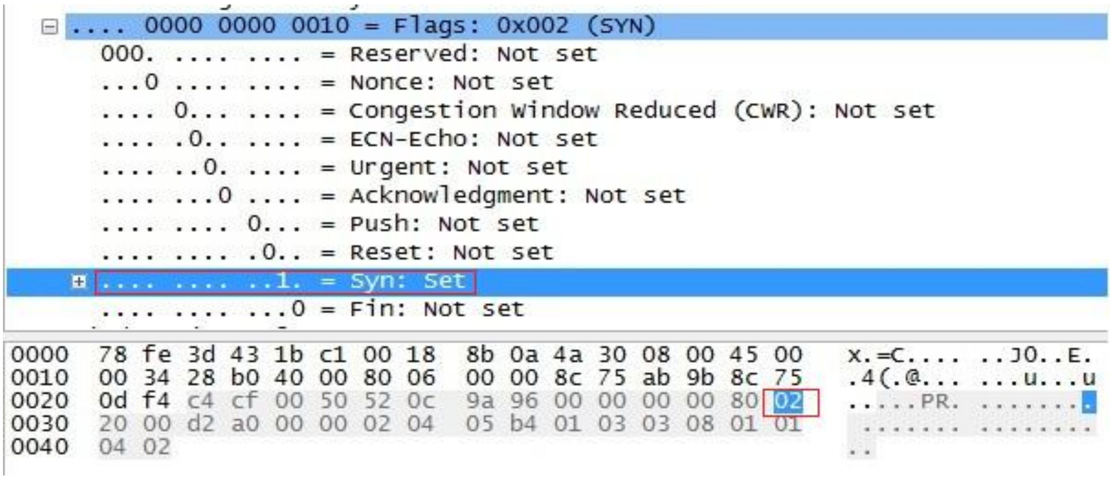
A : 1460 bytes



```
⊟ Options: (12 bytes), Maximum segment size
  ⊟ Maximum segment size: 1460 bytes
      Kind: Maximum Segment Size (2)
      Length: 4
      MSS Value: 1460
```

f. Find the hex character that contains the SYN flag bit

A :



```
  ⊟ .... 0000 0000 0010 = Flags: 0x002 (SYN)
       000. .... .... = Reserved: Not set
       ...0 .... .... = Nonce: Not set
       .... 0... .... = Congestion Window Reduced (CWR): Not set
       .... .0.. .... = ECN-Echo: Not set
       .... ..0. .... = Urgent: Not set
       .... ...0 .... = Acknowledgment: Not set
       .... .... 0... = Push: Not set
       .... .... .0.. = Reset: Not set
     ⊞ .... .... ..1. = Syn: Set
       .... .... ...0 = Fin: Not set

0000  78 fe 3d 43 1b c1 00 18  8b 0a 4a 30 08 00 45 00   x.=C.... ..J0..E.
0010  00 34 28 b0 40 00 80 06  00 00 8c 75 ab 9b 8c 75   .4(.@... ...u...u
0020  0d f4 c4 cf 00 50 52 0c  9a 96 00 00 00 00 80 02   .....PR. ........
0030  20 00 d2 a0 00 00 02 04  05 b4 01 03 03 08 01 01    ....... ........
0040  04 02                                              ..
```

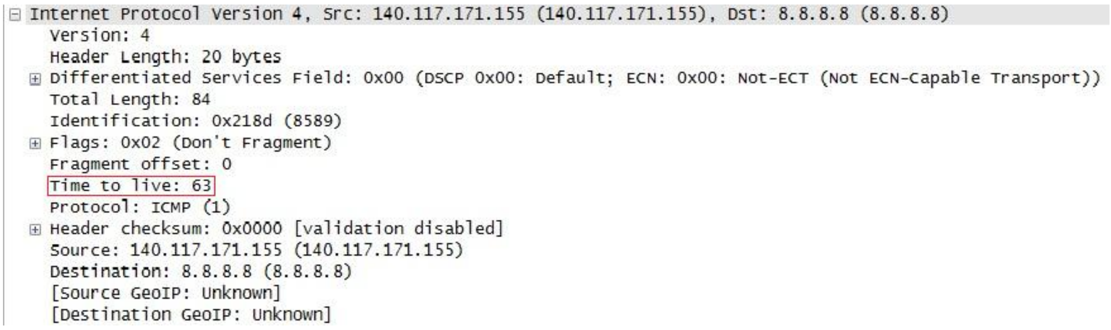
Part 2 Probing the Internet (ICMP, PING, Traceroute)

1. Ping Captured.

- (1) Find the first ICMP Echo Request packet.

a. First, examine the Internet Protocol. What is the Time-to-Live?

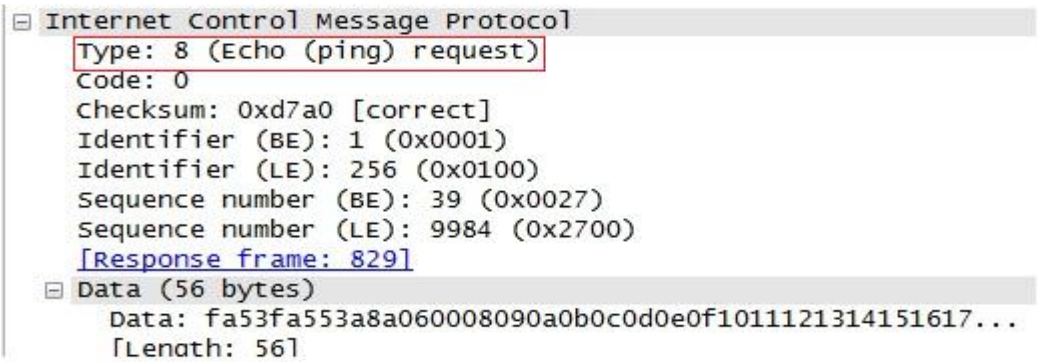
A : 63



```
⊟ Internet Protocol Version 4, Src: 140.117.171.155 (140.117.171.155), Dst: 8.8.8.8 (8.8.8.8)
    Version: 4
    Header Length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 84
    Identification: 0x218d (8589)
  ⊞ Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 63
    Protocol: ICMP (1)
  ⊞ Header checksum: 0x0000 [validation disabled]
    Source: 140.117.171.155 (140.117.171.155)
    Destination: 8.8.8.8 (8.8.8.8)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
```

b. Next examine the Internet Control Message Protocol. What is the ICMP message type?

A : Type : 8(Echo (ping) request)

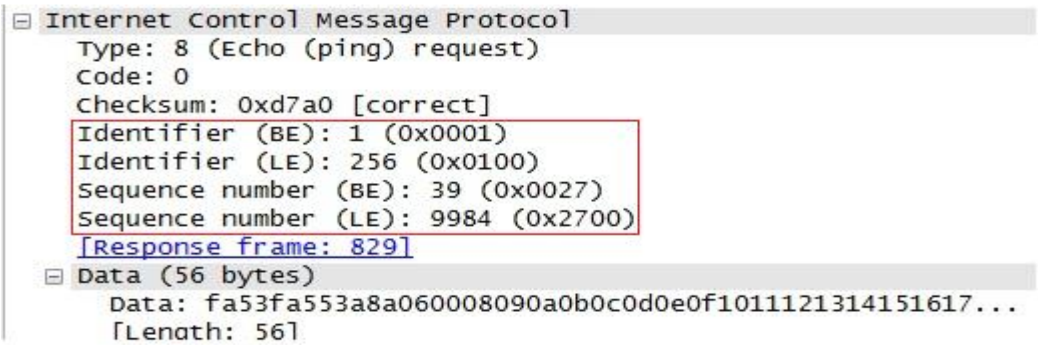


```
⊟ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xd7a0 [correct]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 39 (0x0027)
    Sequence number (LE): 9984 (0x2700)
    [Response frame: 829]
  ⊟ Data (56 bytes)
      Data: fa53fa553a8a060008090a0b0c0d0e0f1011121314151617...
      [Length: 56]
```

c. What is the message identifier and sequence number?

A : Identifier (BE) : 1 , Identifier (LE) : 256

Sequence (BE) : 39 , Sequence (LE) : 9984

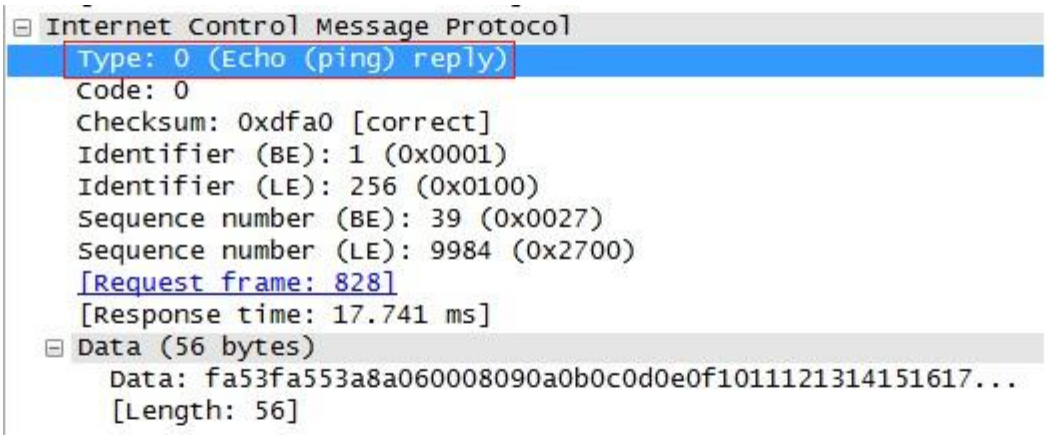


```
⊟ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xd7a0 [correct]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 39 (0x0027)
    Sequence number (LE): 9984 (0x2700)
    [Response frame: 829]
  ⊟ Data (56 bytes)
      Data: fa53fa553a8a060008090a0b0c0d0e0f1011121314151617...
      [Length: 56]
```

- (2) Find the first ICMP Echo Reply packet.

a. Now examine the Internet Control Message Protocol. What is the ICMP message type?

A : Type : 0 (Echo (ping) reply)



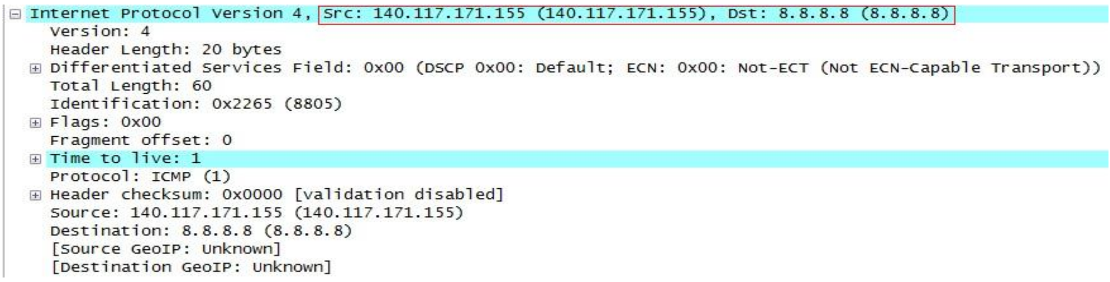
```
⊟ Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0xdfa0 [correct]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 39 (0x0027)
    Sequence number (LE): 9984 (0x2700)
    [Request frame: 828]
    [Response time: 17.741 ms]
  ⊟ Data (56 bytes)
      Data: fa53fa553a8a060008090a0b0c0d0e0f1011121314151617...
      [Length: 56]
```

2. Traceroute Captured.

- (1) Find the first ICMP Echo Request packet.

a. Examine the Internet Protocol. What are the source and destination addresses?

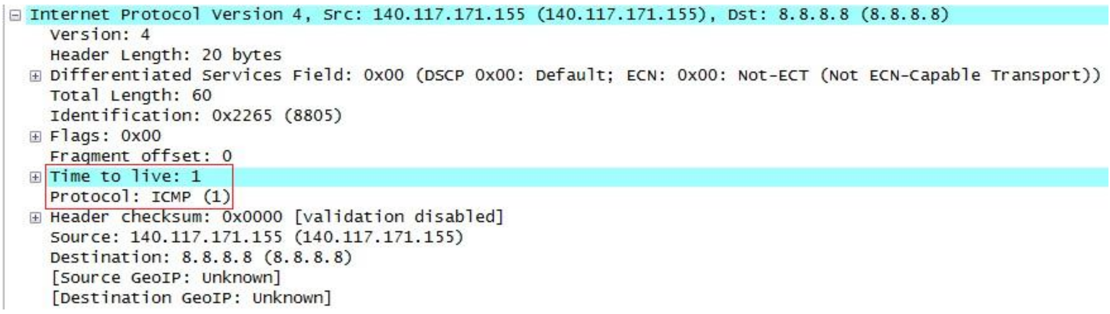
A : Source : 140.117.171.155 , Destination : 8.8.8.8



```
⊟ Internet Protocol Version 4, Src: 140.117.171.155 (140.117.171.155), Dst: 8.8.8.8 (8.8.8.8)
    Version: 4
    Header Length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 60
    Identification: 0x2265 (8805)
  ⊞ Flags: 0x00
    Fragment offset: 0
  ⊞ Time to live: 1
    Protocol: ICMP (1)
  ⊞ Header checksum: 0x0000 [validation disabled]
    Source: 140.117.171.155 (140.117.171.155)
    Destination: 8.8.8.8 (8.8.8.8)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
```

b. What are the protocol type and the Time-to-Live in the IP packet?

A : Protocol type : ICMP , Time to live : 1



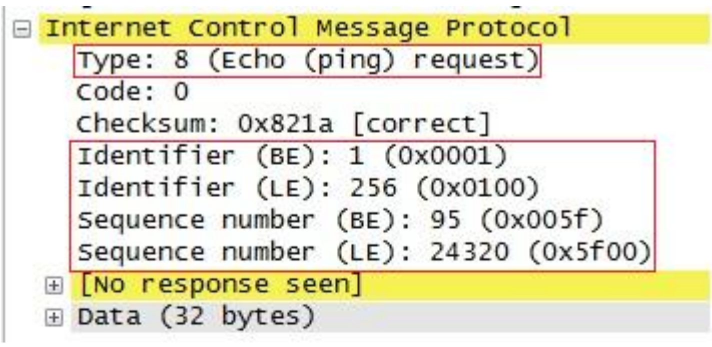
```
⊟ Internet Protocol Version 4, Src: 140.117.171.155 (140.117.171.155), Dst: 8.8.8.8 (8.8.8.8)
    Version: 4
    Header Length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 60
    Identification: 0x2265 (8805)
  ⊞ Flags: 0x00
    Fragment offset: 0
  ⊞ Time to live: 1
    Protocol: ICMP (1)
  ⊞ Header checksum: 0x0000 [validation disabled]
    Source: 140.117.171.155 (140.117.171.155)
    Destination: 8.8.8.8 (8.8.8.8)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
```

c. Next, examine the Internet Control Message Protocol. What is the ICMP message type? What are the message identifier and sequence number?

A : ICMP message type : 8 (Echo (ping) request)

Identifier (BE) : 1 , Identifier (LE) : 256

Sequence (BE) : 95 , Sequence (LE) : 24320

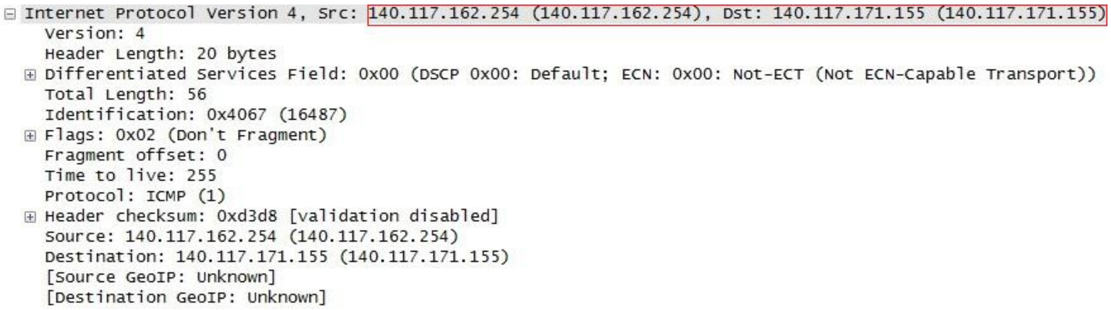


```
⊟ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x821a [correct]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 95 (0x005f)
    Sequence number (LE): 24320 (0x5f00)
  ⊞ [No response seen]
  ⊞ Data (32 bytes)
```

- (2) Find an ICMP Time-to-live exceeded packet.

a. Examine the Internet Protocol. What are the source and destination addresses?

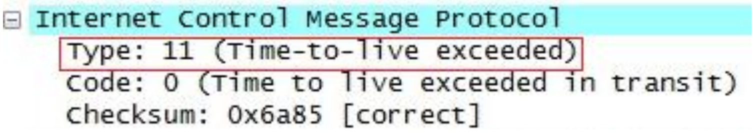
A : Source : 140.117.162.254 , Destination : 140.117.171.151



```
⊟ Internet Protocol Version 4, Src: 140.117.162.254 (140.117.162.254), Dst: 140.117.171.155 (140.117.171.155)
    Version: 4
    Header Length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 56
    Identification: 0x4067 (16487)
  ⊞ Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 255
    Protocol: ICMP (1)
  ⊞ Header checksum: 0xd3d8 [validation disabled]
    Source: 140.117.162.254 (140.117.162.254)
    Destination: 140.117.171.155 (140.117.171.155)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
```

b. Next, examine the Internet Control Message Protocol. What is the ICMP message type?

A : Type : 11 (Time-to-live exceeded)

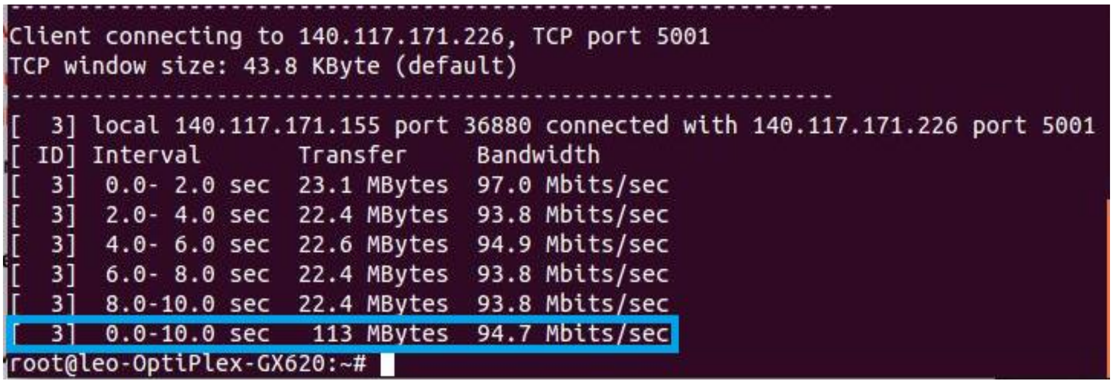


```
⊟ Internet Control Message Protocol
    Type: 11 (Time-to-live exceeded)
    Code: 0 (Time to live exceeded in transit)
    Checksum: 0x6a85 [correct]
```

Part 3 Measuring Network Bandwidth

1. **Measure the bandwidth for Transmission Control Protocol**

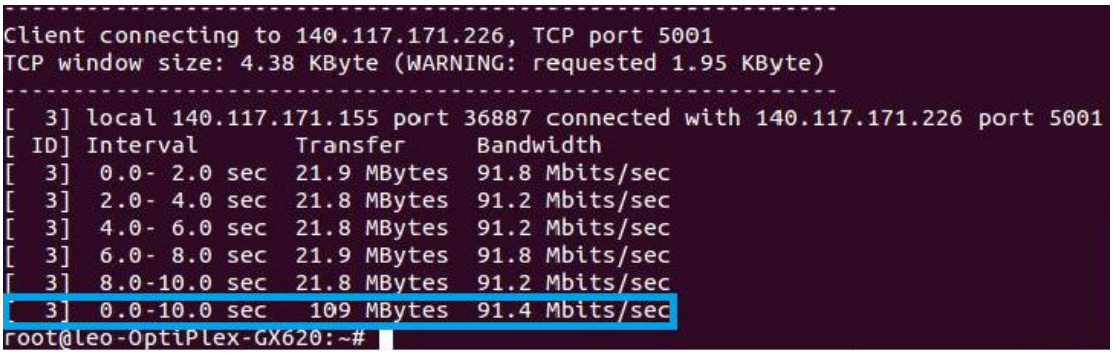
   A : average bandwidth : 94.7Mbit/sec



```
------------------------------------------------------------
Client connecting to 140.117.171.226, TCP port 5001
TCP window size: 43.8 KByte (default)
------------------------------------------------------------
[  3] local 140.117.171.155 port 36880 connected with 140.117.171.226 port 5001
[ ID] Interval       Transfer     Bandwidth
[  3]  0.0- 2.0 sec  23.1 MBytes  97.0 Mbits/sec
[  3]  2.0- 4.0 sec  22.4 MBytes  93.8 Mbits/sec
[  3]  4.0- 6.0 sec  22.6 MBytes  94.9 Mbits/sec
[  3]  6.0- 8.0 sec  22.4 MBytes  93.8 Mbits/sec
[  3]  8.0-10.0 sec  22.4 MBytes  93.8 Mbits/sec
[  3]  0.0-10.0 sec   113 MBytes  94.7 Mbits/sec
root@leo-OptiPlex-GX620:~#
```

2. **Adjust the window size for Transmission Control Protocol. See what's different.**

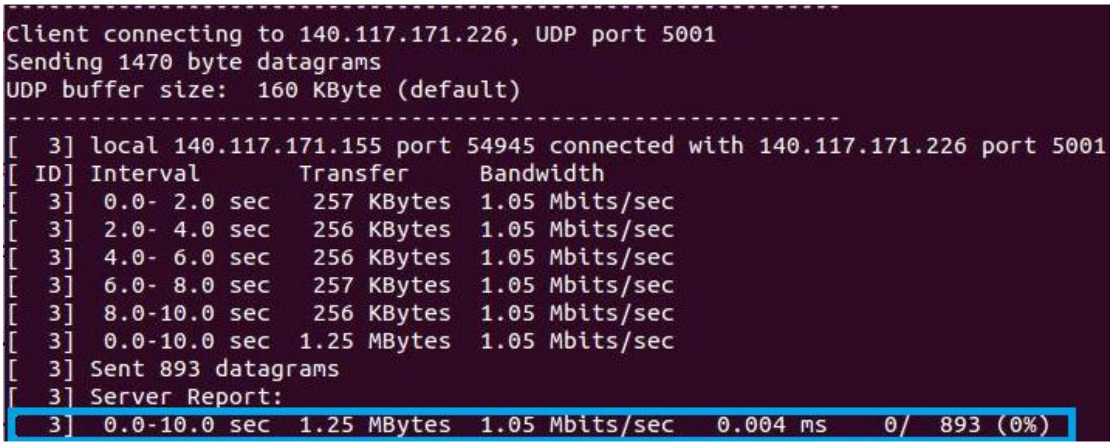
A : When window size is reduced , the average bandwidth will also been reduced.



```
------------------------------------------------------------
Client connecting to 140.117.171.226, TCP port 5001
TCP window size: 4.38 KByte (WARNING: requested 1.95 KByte)
------------------------------------------------------------
[  3] local 140.117.171.155 port 36887 connected with 140.117.171.226 port 5001
[ ID] Interval       Transfer     Bandwidth
[  3]  0.0- 2.0 sec  21.9 MBytes  91.8 Mbits/sec
[  3]  2.0- 4.0 sec  21.8 MBytes  91.2 Mbits/sec
[  3]  4.0- 6.0 sec  21.8 MBytes  91.2 Mbits/sec
[  3]  6.0- 8.0 sec  21.9 MBytes  91.8 Mbits/sec
[  3]  8.0-10.0 sec  21.8 MBytes  91.2 Mbits/sec
[  3]  0.0-10.0 sec   109 MBytes  91.4 Mbits/sec
root@leo-OptiPlex-GX620:~#
```

3. **Measure the bandwidth for User Datagram Protocol**

A : average bandwidth : 1.05Mbits/sec

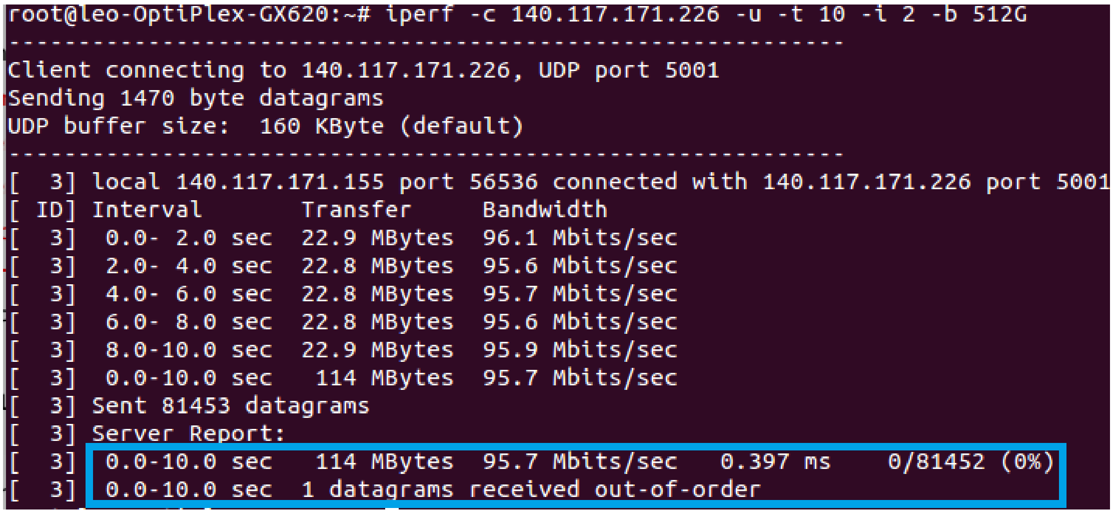


```
------------------------------------------------------------
Client connecting to 140.117.171.226, UDP port 5001
Sending 1470 byte datagrams
UDP buffer size:  160 KByte (default)
------------------------------------------------------------
[  3] local 140.117.171.155 port 54945 connected with 140.117.171.226 port 5001
[ ID] Interval       Transfer     Bandwidth
[  3]  0.0- 2.0 sec   257 KBytes  1.05 Mbits/sec
[  3]  2.0- 4.0 sec   256 KBytes  1.05 Mbits/sec
[  3]  4.0- 6.0 sec   256 KBytes  1.05 Mbits/sec
[  3]  6.0- 8.0 sec   257 KBytes  1.05 Mbits/sec
[  3]  8.0-10.0 sec   256 KBytes  1.05 Mbits/sec
[  3]  0.0-10.0 sec  1.25 MBytes  1.05 Mbits/sec
[  3] Sent 893 datagrams
[  3] Server Report:
[  3]  0.0-10.0 sec  1.25 MBytes  1.05 Mbits/sec   0.004 ms    0/  893 (0%)
```

4. **Adjust the bandwidth for User Datagram Protocol. Measure the package lost rate or any else happened.**

A : 1 data out-of-ordered / 81453 data ,

lost rate would be : 1 / 81453 * 100% = 0.00123%



```
root@leo-OptiPlex-GX620:~# iperf -c 140.117.171.226 -u -t 10 -i 2 -b 512G
------------------------------------------------------------
Client connecting to 140.117.171.226, UDP port 5001
Sending 1470 byte datagrams
UDP buffer size:  160 KByte (default)
------------------------------------------------------------
[  3] local 140.117.171.155 port 56536 connected with 140.117.171.226 port 5001
[ ID] Interval       Transfer     Bandwidth
[  3]  0.0- 2.0 sec  22.9 MBytes  96.1 Mbits/sec
[  3]  2.0- 4.0 sec  22.8 MBytes  95.6 Mbits/sec
[  3]  4.0- 6.0 sec  22.8 MBytes  95.7 Mbits/sec
[  3]  6.0- 8.0 sec  22.8 MBytes  95.6 Mbits/sec
[  3]  8.0-10.0 sec  22.9 MBytes  95.9 Mbits/sec
[  3]  0.0-10.0 sec   114 MBytes  95.7 Mbits/sec
[  3] Sent 81453 datagrams
[  3] Server Report:
[  3]  0.0-10.0 sec   114 MBytes  95.7 Mbits/sec   0.397 ms    0/81452 (0%)
[  3]  0.0-10.0 sec  1 datagrams received out-of-order
```