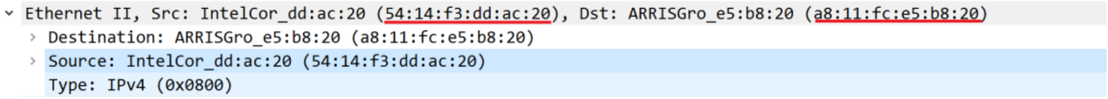
Protocol Analysis Questions

To answer the following questions, start Wireshark and open the packet capture file created above.

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.

(1) Examine the Ethernet

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

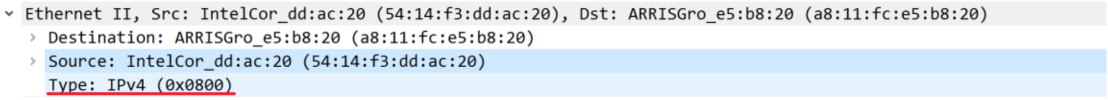


```
⌄ Ethernet II, Src: IntelCor_dd:ac:20 (54:14:f3:dd:ac:20), Dst: ARRISGro_e5:b8:20 (a8:11:fc:e5:b8:20)
  › Destination: ARRISGro_e5:b8:20 (a8:11:fc:e5:b8:20)
  › Source: IntelCor_dd:ac:20 (54:14:f3:dd:ac:20)
    Type: IPv4 (0x0800)
```

Source: 54:14:f3:dd:ac:20

Destination: a8:11:fc:e5:b8:20

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

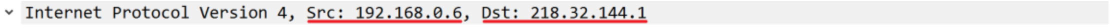


```
⌄ Ethernet II, Src: IntelCor_dd:ac:20 (54:14:f3:dd:ac:20), Dst: ARRISGro_e5:b8:20 (a8:11:fc:e5:b8:20)
  › Destination: ARRISGro_e5:b8:20 (a8:11:fc:e5:b8:20)
  › Source: IntelCor_dd:ac:20 (54:14:f3:dd:ac:20)
    Type: IPv4 (0x0800)
```

IPv4 (0x0800)

(2) Examine the Internet Protocol

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

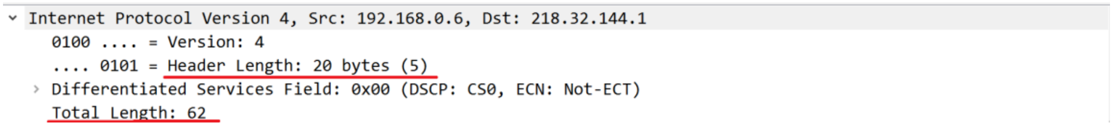


```
⌄ Internet Protocol Version 4, Src: 192.168.0.6, Dst: 218.32.144.1
```

Source: 192.168.0.6

Destination: 218.32.144.1

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

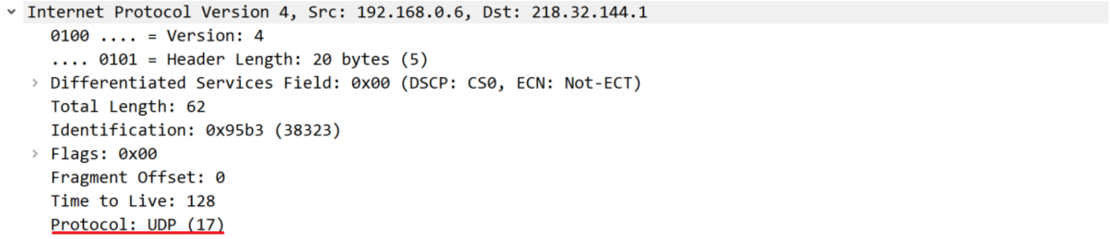


```
⌄ Internet Protocol Version 4, Src: 192.168.0.6, Dst: 218.32.144.1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  › Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 62
```

Header length: 20 bytes

Total packet length: 62 bytes

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

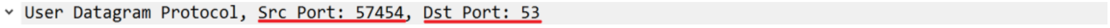


```
⌄ Internet Protocol Version 4, Src: 192.168.0.6, Dst: 218.32.144.1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  › Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 62
    Identification: 0x95b3 (38323)
  › Flags: 0x00
    Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
```

UDP (17)

(3) Examine the User Datagram Protocol

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



```
⌄ User Datagram Protocol, Src Port: 57454, Dst Port: 53
```

Client Port: 57454,

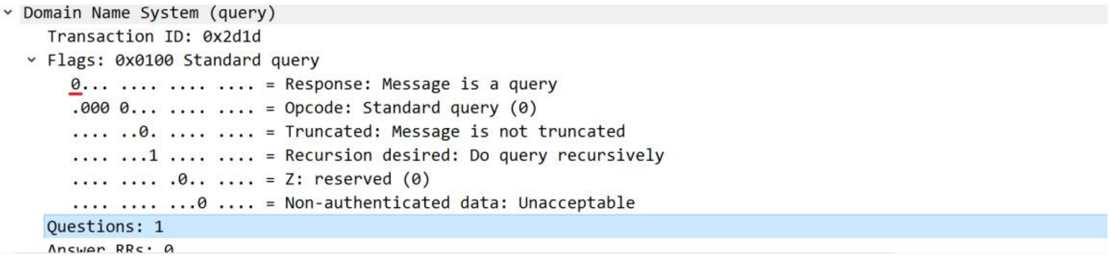
Server Port: 53

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

DNS

(4) Examine the Domain Name System (query)

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

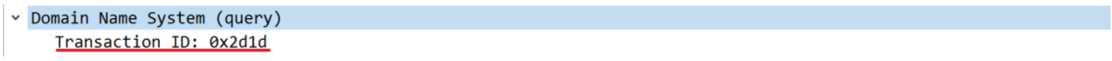


```
⌄ Domain Name System (query)
    Transaction ID: 0x2d1d
  ⌄ Flags: 0x0100 Standard query
      0... .... .... .... = Response: Message is a query
      .000 0... .... .... = Opcode: Standard query (0)
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... .0.. .... = Z: reserved (0)
      .... .... ...0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
```

第一個bit說明message是query或response，

0 為query，而 1 則是 response。

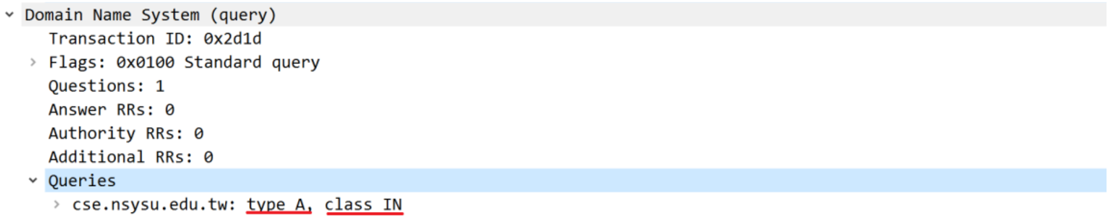
b. What is the query transaction ID?



```
⌄ Domain Name System (query)
    Transaction ID: 0x2d1d
```

Transaction ID: 0X2d1d

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



```
⌄ Domain Name System (query)
    Transaction ID: 0x2d1d
  › Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ⌄ Queries
    › cse.nsysu.edu.tw: type A, class IN
```

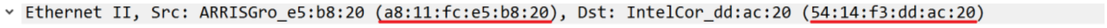
Type: A

Class: IN

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. (cse.nsysu.edu.tw == 140.117.13.244)

(1) Examine the Ethernet

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

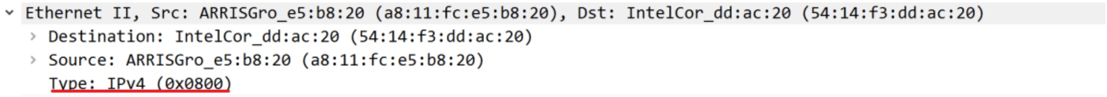


```
⌄ Ethernet II, Src: ARRISGro_e5:b8:20 (a8:11:fc:e5:b8:20), Dst: IntelCor_dd:ac:20 (54:14:f3:dd:ac:20)
```

Source: a8:11:fc:e5:b8:20

Destination: 54:14:f3:dd:ac:20

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

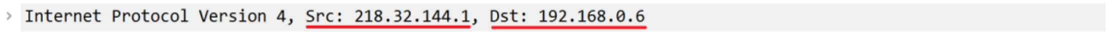


```
⌄ Ethernet II, Src: ARRISGro_e5:b8:20 (a8:11:fc:e5:b8:20), Dst: IntelCor_dd:ac:20 (54:14:f3:dd:ac:20)
  › Destination: IntelCor_dd:ac:20 (54:14:f3:dd:ac:20)
  › Source: ARRISGro_e5:b8:20 (a8:11:fc:e5:b8:20)
    Type: IPv4 (0x0800)
```

IPv4 (0x0800)

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

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

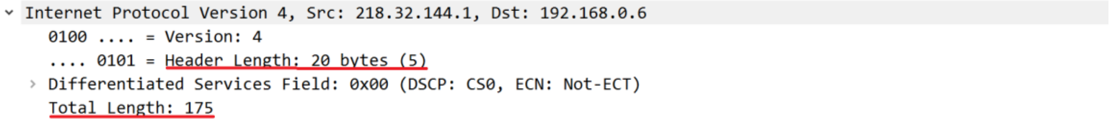


```
› Internet Protocol Version 4, Src: 218.32.144.1, Dst: 192.168.0.6
```

Source: 218.32.144.1

Destination: 192.168.0.6

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



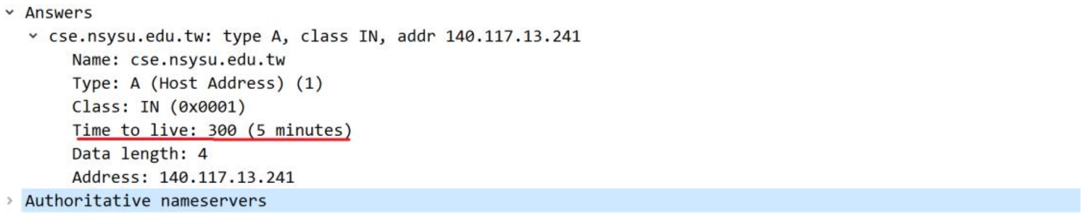
```
˅ Internet Protocol Version 4, Src: 218.32.144.1, Dst: 192.168.0.6
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  › Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 175
```

Header length: 20 bytes

Total packet length: 175 bytes

Yes, it is longer than query.

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



```
˅ Answers
  ˅ cse.nsysu.edu.tw: type A, class IN, addr 140.117.13.241
      Name: cse.nsysu.edu.tw
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 300 (5 minutes)
      Data length: 4
      Address: 140.117.13.241
› Authoritative nameservers
```

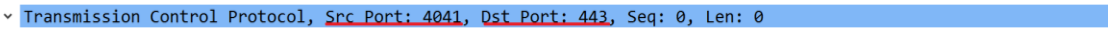
Only one answer.

Time-to-live: 5 minutes

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

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?

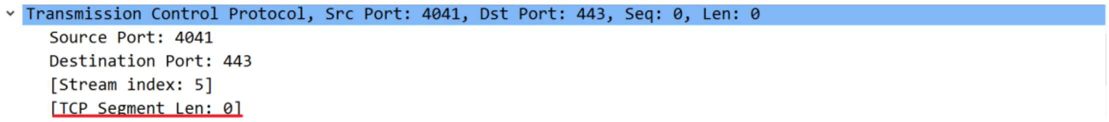


```
˅ Transmission Control Protocol, Src Port: 4041, Dst Port: 443, Seq: 0, Len: 0
```

Client port: 4041

Server port: 443

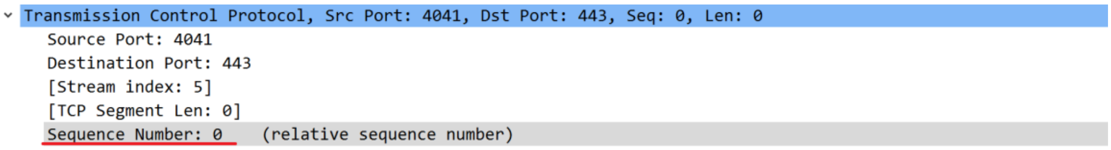
b. What is the length of the TCP segment?



```
⌄ Transmission Control Protocol, Src Port: 4041, Dst Port: 443, Seq: 0, Len: 0
    Source Port: 4041
    Destination Port: 443
    [Stream index: 5]
    [TCP Segment Len: 0]
```

Length: 0

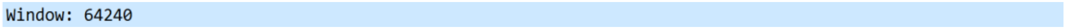
c. What is the initial sequence number for the segments from the client to the server?



```
⌄ Transmission Control Protocol, Src Port: 4041, Dst Port: 443, Seq: 0, Len: 0
    Source Port: 4041
    Destination Port: 443
    [Stream index: 5]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
```

Sequence number: 0

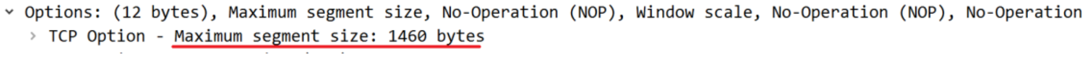
c. What is the initial window size?



```
Window: 64240
```

Window size: 64240 bytes

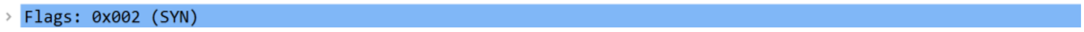
d. What is the maximum segment size?



```
⌄ Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation
  › TCP Option - Maximum segment size: 1460 bytes
```

Maximum segment size: 1460 bytes

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



```
› Flags: 0x002 (SYN)
```

Hex character: 0x002

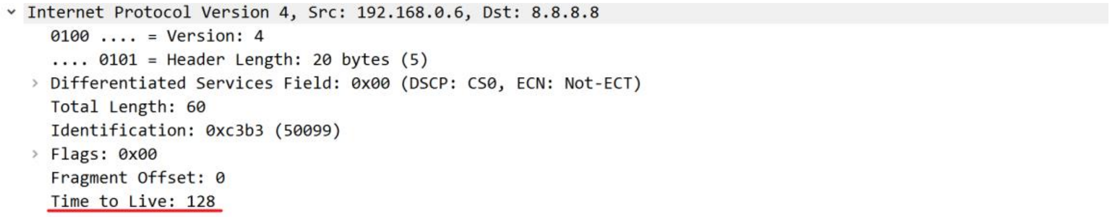
Part 2 Probing the Internet (ICMP, PING, Traceroute)

Objective

1. Ping Captured.

(1) Find the first ICMP Echo Request packet.

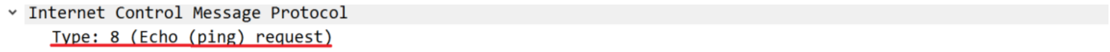
a. First, examine the Internet Protocol. What is the Time-to-Live?



```
⌄ Internet Protocol Version 4, Src: 192.168.0.6, Dst: 8.8.8.8
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  › Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0xc3b3 (50099)
  › Flags: 0x00
    Fragment Offset: 0
    Time to Live: 128
```

128 seconds

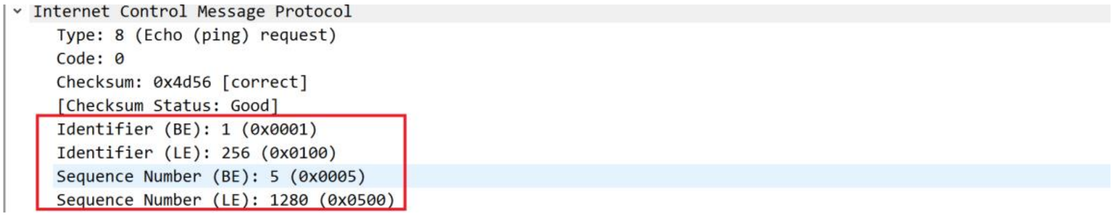
b. Next examine the Internet Control Message Protocol. What is the ICMP message type?



```
⌄ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
```

Type: 8 (Echo (ping) request)

d. What is the message identifier and sequence number?



```
⌄ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4d56 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 5 (0x0005)
    Sequence Number (LE): 1280 (0x0500)
```

Identifier (BE): 1 (0x0001)

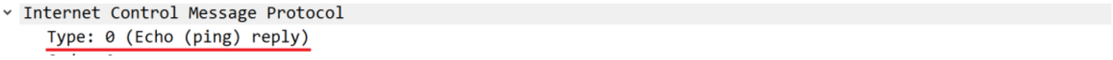
Identifier (LE): 256 (0x0100)

Sequence Number (BE): 5 (0x0005)

Sequence Number (LE): 1280 (0x0500)

(2) Find the first ICMP Echo Reply packet.

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



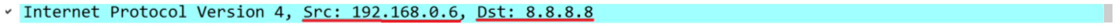
```
⌄ Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
```

Type: 0 (Echo (ping) reply)

2. Traceroute Captured.

(1) Find the first ICMP Echo Request packet.

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

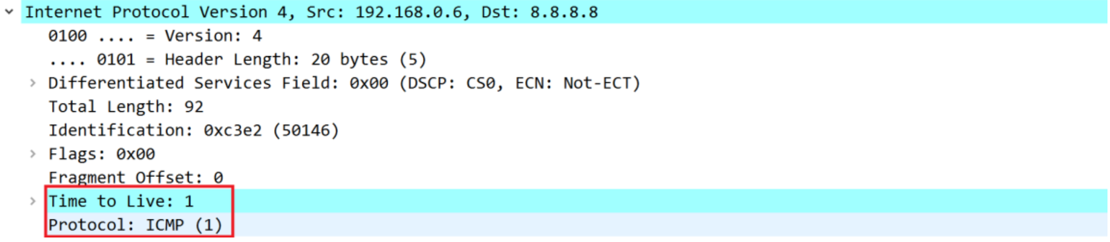


```
˅ Internet Protocol Version 4, Src: 192.168.0.6, Dst: 8.8.8.8
```

Source: 192.168.0.6

Destination: 8.8.8.8

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

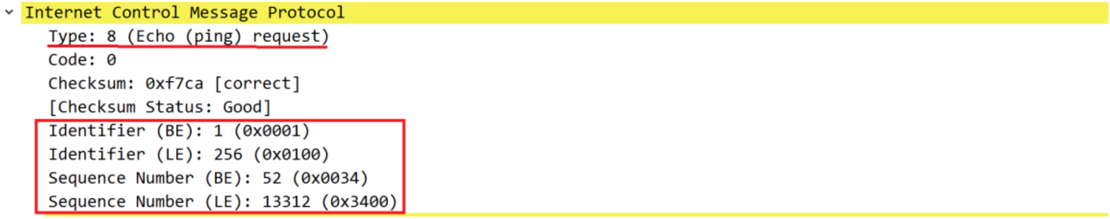


```
˅ Internet Protocol Version 4, Src: 192.168.0.6, Dst: 8.8.8.8
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  › Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 92
    Identification: 0xc3e2 (50146)
  › Flags: 0x00
    Fragment Offset: 0
  › Time to Live: 1
    Protocol: ICMP (1)
```

Protocol type: ICMP

Time-to-Live: 1 second

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



```
˅ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xf7ca [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 52 (0x0034)
    Sequence Number (LE): 13312 (0x3400)
```

Type: 8 (Echo (ping) request)

Identifier (BE): 1 (0x0001)

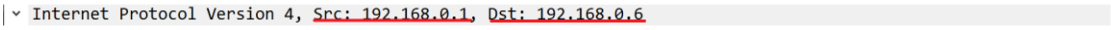
Identifier (LE): 256 (0x0100)

Sequence Number (BE): 52 (0x0034)

Sequence Number (LE): 13312 (0x3400)

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

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

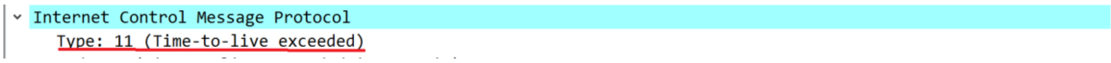


```
⌄ Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.6
```

Source: 192.168.0.1

Destination: 192.168.0.6

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



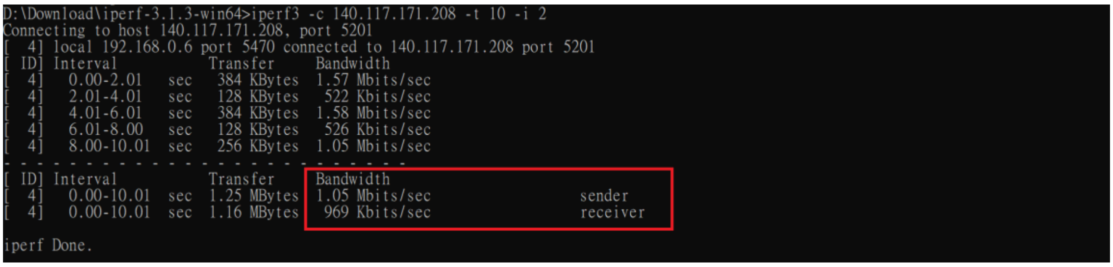
```
⌄ Internet Control Message Protocol
    Type: 11 (Time-to-live exceeded)
```

Type: 11 (Time-to-live exceeded)

Part 3 Measuring Network Bandwidth

Objective

1. Measure the bandwidth for Transmission Control Protocol Type "iperf3 -c 140.117.171.208 -t 10 -i 2"

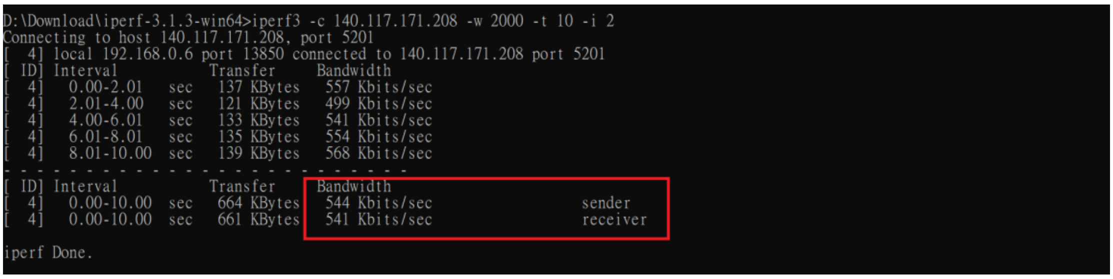


```
D:\Download\iperf-3.1.3-win64>iperf3 -c 140.117.171.208 -t 10 -i 2
Connecting to host 140.117.171.208, port 5201
[  4] local 192.168.0.6 port 5470 connected to 140.117.171.208 port 5201
[ ID] Interval           Transfer     Bandwidth
[  4]   0.00-2.01   sec   384 KBytes  1.57 Mbits/sec
[  4]   2.01-4.01   sec   128 KBytes   522 Kbits/sec
[  4]   4.01-6.01   sec   384 KBytes  1.58 Mbits/sec
[  4]   6.01-8.00   sec   128 KBytes   526 Kbits/sec
[  4]   8.00-10.01  sec   256 KBytes  1.05 Mbits/sec
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bandwidth
[  4]   0.00-10.01  sec  1.25 MBytes  1.05 Mbits/sec                  sender
[  4]   0.00-10.01  sec  1.16 MBytes   969 Kbits/sec                  receiver

iperf Done.
```

Sender bandwidth: 1.05 Mbits/sec

Receiver bandwidth: 969 Kbits/sec

2. Adjust the window size for Transmission Control Protocol. See what's different. Type "iperf3 -c 140.117.171.208 -w 2000 -t 10 -i 2"



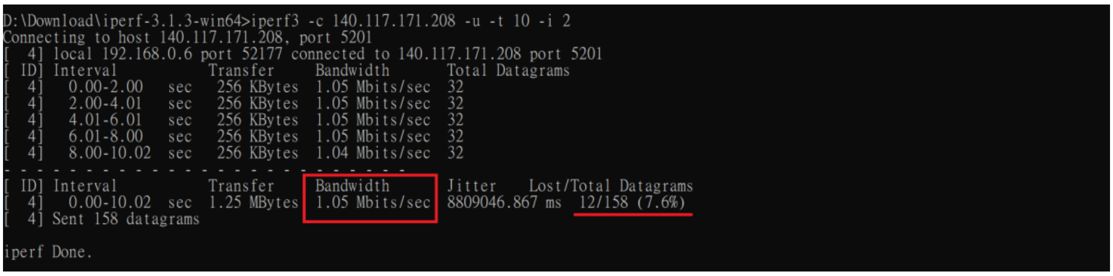
```
D:\Download\iperf-3.1.3-win64>iperf3 -c 140.117.171.208 -w 2000 -t 10 -i 2
Connecting to host 140.117.171.208, port 5201
[  4] local 192.168.0.6 port 13850 connected to 140.117.171.208 port 5201
[ ID] Interval           Transfer     Bandwidth
[  4]   0.00-2.01   sec   137 KBytes   557 Kbits/sec
[  4]   2.01-4.00   sec   121 KBytes   499 Kbits/sec
[  4]   4.00-6.01   sec   133 KBytes   541 Kbits/sec
[  4]   6.01-8.01   sec   135 KBytes   554 Kbits/sec
[  4]   8.01-10.00  sec   139 KBytes   568 Kbits/sec
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bandwidth
[  4]   0.00-10.00  sec   664 KBytes   544 Kbits/sec                  sender
[  4]   0.00-10.00  sec   661 KBytes   541 Kbits/sec                  receiver

iperf Done.
```

Sender bandwidth: 544 Kbits/sec

Receiver bandwidth: 541 Kbits/sec

調整 window size 後，頻寬大約少了一半

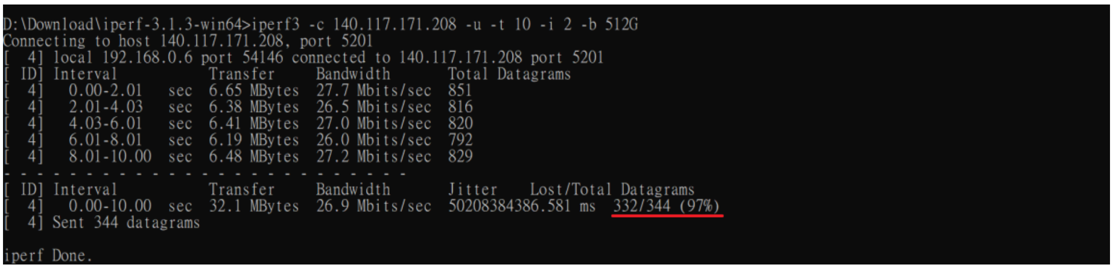
3. Measure the bandwidth for User Datagram Protocol Type "iperf3 -c 140.117.171.208 -u -t 10 -i 2"



```
D:\Download\iperf-3.1.3-win64>iperf3 -c 140.117.171.208 -u -t 10 -i 2
Connecting to host 140.117.171.208, port 5201
[  4] local 192.168.0.6 port 52177 connected to 140.117.171.208 port 5201
[ ID] Interval           Transfer     Bandwidth       Total Datagrams
[  4]   0.00-2.00   sec   256 KBytes  1.05 Mbits/sec  32
[  4]   2.00-4.01   sec   256 KBytes  1.05 Mbits/sec  32
[  4]   4.01-6.01   sec   256 KBytes  1.05 Mbits/sec  32
[  4]   6.01-8.00   sec   256 KBytes  1.05 Mbits/sec  32
[  4]   8.00-10.02  sec   256 KBytes  1.04 Mbits/sec  32
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bandwidth       Jitter    Lost/Total Datagrams
[  4]   0.00-10.02  sec  1.25 MBytes  1.05 Mbits/sec  8809046.867 ms  12/158 (7.6%)
[  4] Sent 158 datagrams

iperf Done.
```

Bandwidth: 1.05 Mbits/sec

4. Adjust the bandwidth for User Datagram Protocol. Measure the package lost rate or any else happened. Type "iperf3 -c 140.117.171.208 -u -t 10 -i 2 -b 512G"



```
D:\Download\iperf-3.1.3-win64>iperf3 -c 140.117.171.208 -u -t 10 -i 2 -b 512G
Connecting to host 140.117.171.208, port 5201
[  4] local 192.168.0.6 port 54146 connected to 140.117.171.208 port 5201
[ ID] Interval           Transfer     Bandwidth       Total Datagrams
[  4]   0.00-2.01   sec  6.65 MBytes  27.7 Mbits/sec  851
[  4]   2.01-4.03   sec  6.38 MBytes  26.5 Mbits/sec  816
[  4]   4.03-6.01   sec  6.41 MBytes  27.0 Mbits/sec  820
[  4]   6.01-8.01   sec  6.19 MBytes  26.0 Mbits/sec  792
[  4]   8.01-10.00  sec  6.48 MBytes  27.2 Mbits/sec  829
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bandwidth       Jitter    Lost/Total Datagrams
[  4]   0.00-10.00  sec  32.1 MBytes  26.9 Mbits/sec  50208384386.581 ms  332/344 (97%)
[  4] Sent 344 datagrams

iperf Done.
```

封包丟失率從原本 7.6% 上升到 97%