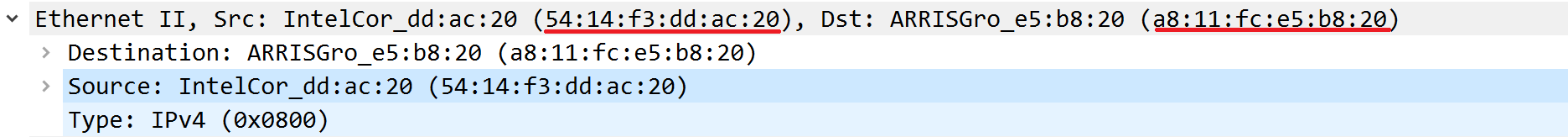
**Protocol Analysis Questions**

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.

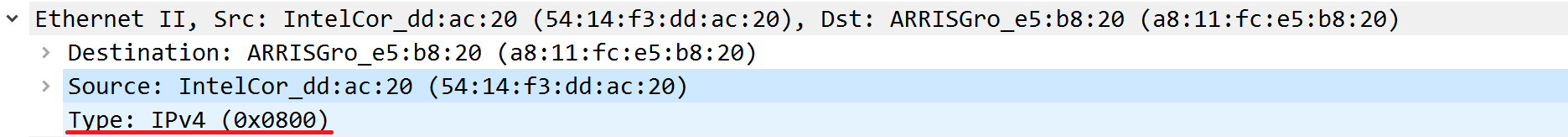
1. Examine the Ethernet
2. What is the Ethernet address of the source and destination?



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?



IPv4 (0x0800)

(2) Examine the Internet Protocol

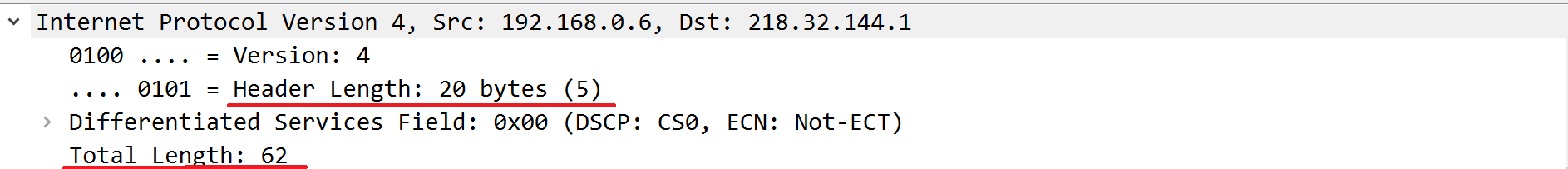
a. What is the IP address of the source and destination?



Source: 192.168.0.6

Destination: 218.32.144.1

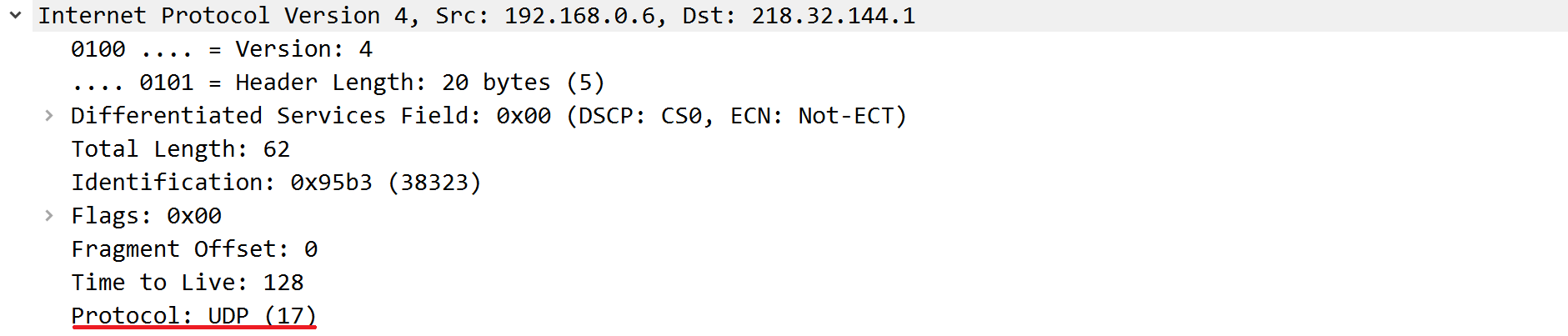
b. What is the header length? What is the total packet length?



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?



UDP (17)

(3) Examine the User Datagram Protocol

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



Client Port: 57454,

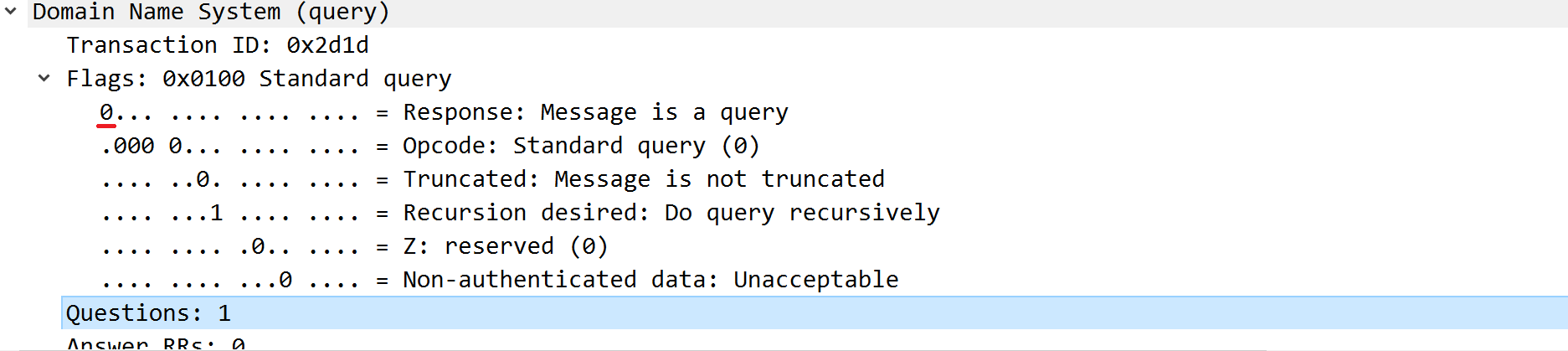
Server Port: 53

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?



第一個bit說明message是query或response，

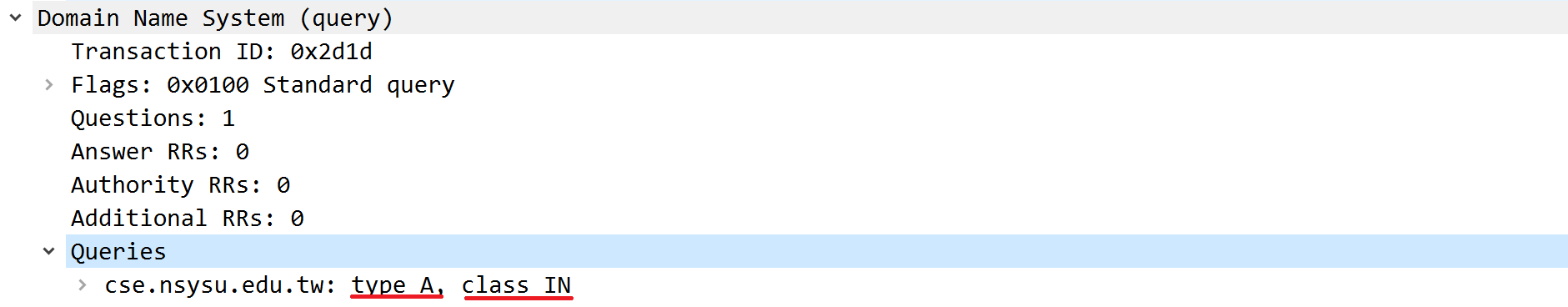
0 為query，而 1 則是 response。

b. What is the query transaction ID?



Transaction ID: 0X2d1d

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



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

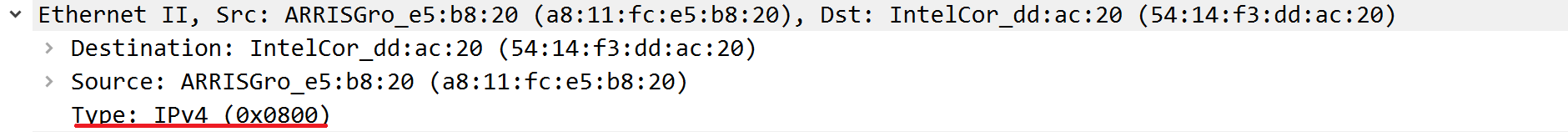
a. What is the Ethernet address of the source and destination?



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

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

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



IPv4 (0x0800)

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

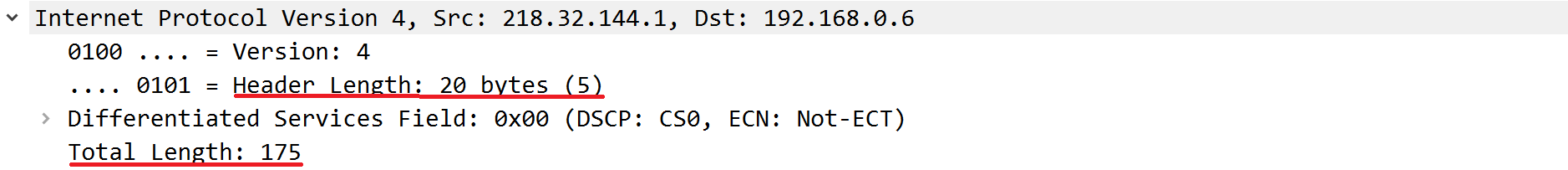
a. What is the IP address of the source and destination?



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?

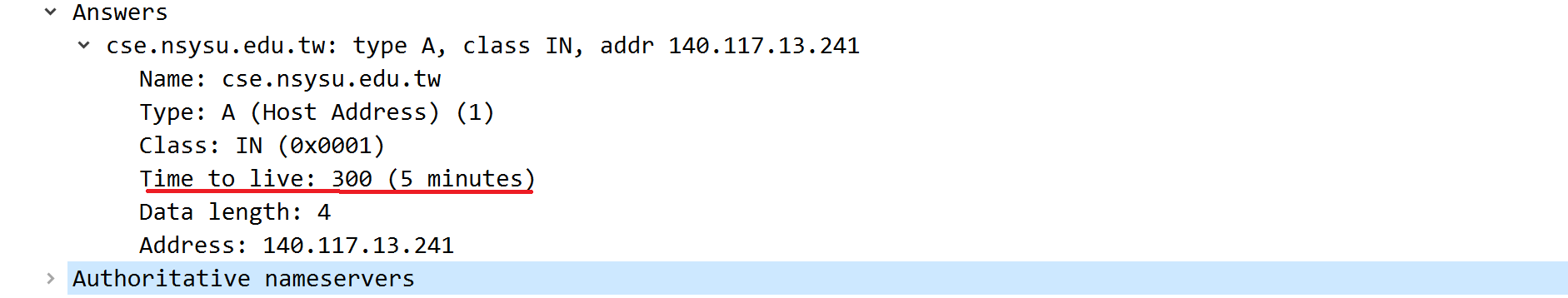


Header length: 20 bytes

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.



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

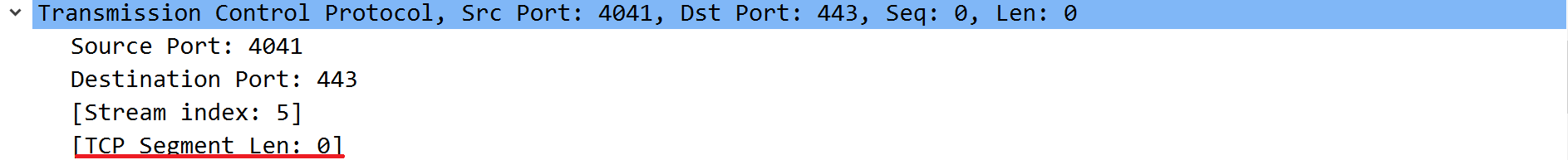
1. What are the ephemeral port number used by the client and the well-known port number used by the server?



Client port: 4041

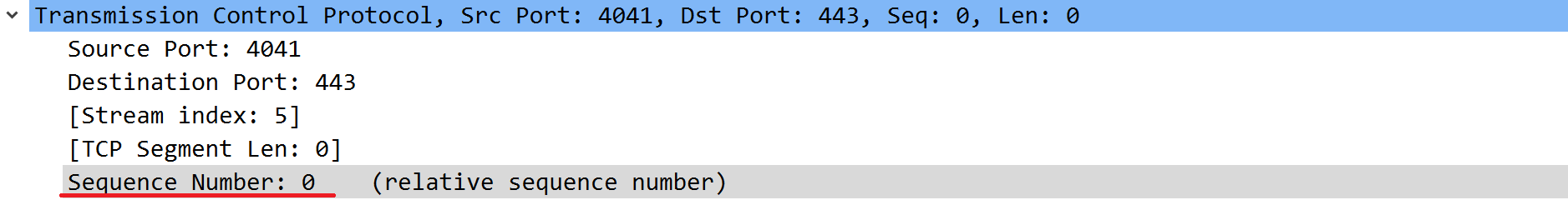
Server port: 443

1. What is the length of the TCP segment?



Length: 0

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



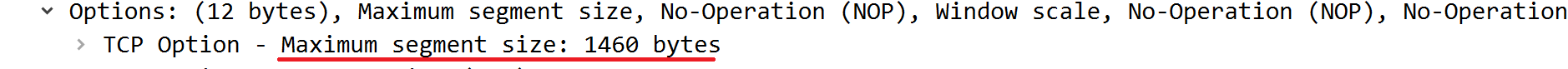
Sequence number: 0

1. What is the initial window size?



Window size: 64240 bytes

1. What is the maximum segment size?



Maximum segment size: 1460 bytes

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



Hex character: 0x002

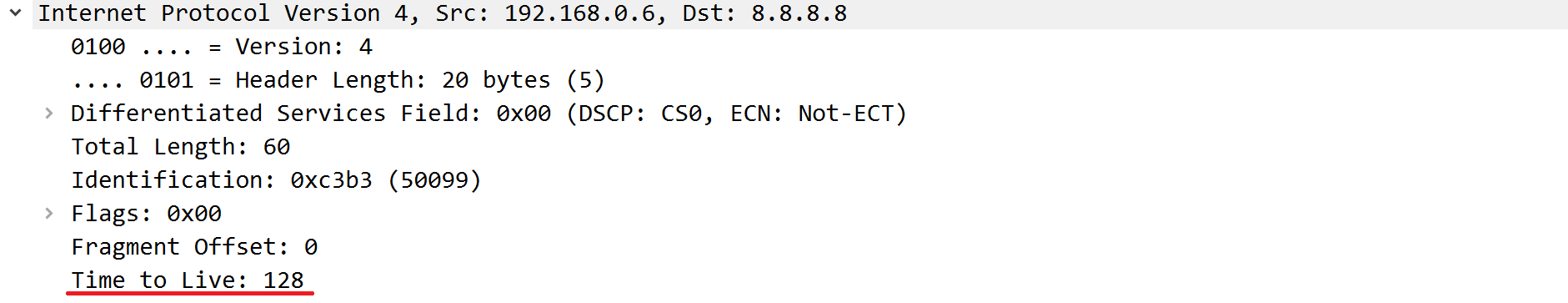
**Part 2 Probing the Internet (ICMP, PING, Traceroute)**

**Objective**

**1. Ping Captured.**

(1) Find the first ICMP Echo Request packet.

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



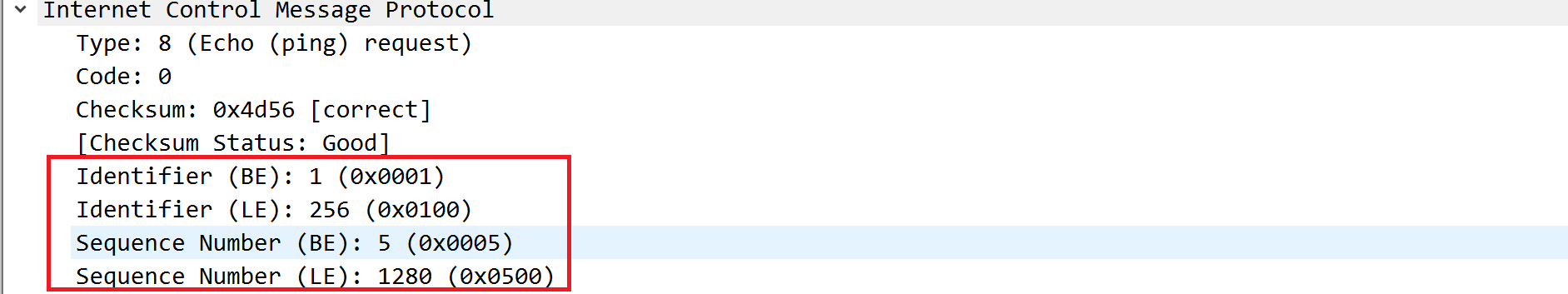
128 seconds

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



Type: 8 (Echo (ping) request)

1. What is the message identifier and sequence number?



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?



Type: 0 (Echo (ping) reply)

**2. Traceroute Captured.**

(1) Find the first ICMP Echo Request packet.

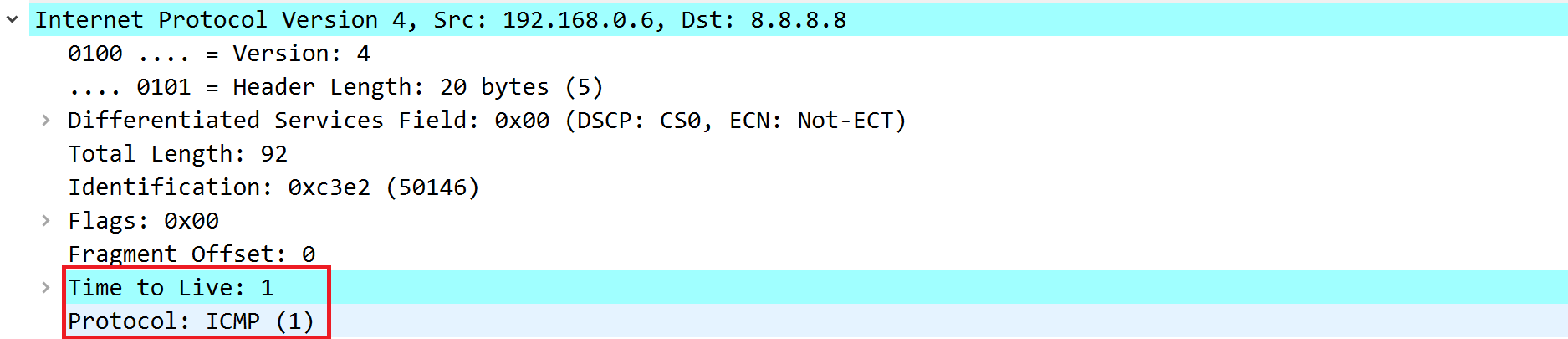
a. Examine the Internet Protocol. What are the source and destination addresses?



Source: 192.168.0.6

Destination: 8.8.8.8

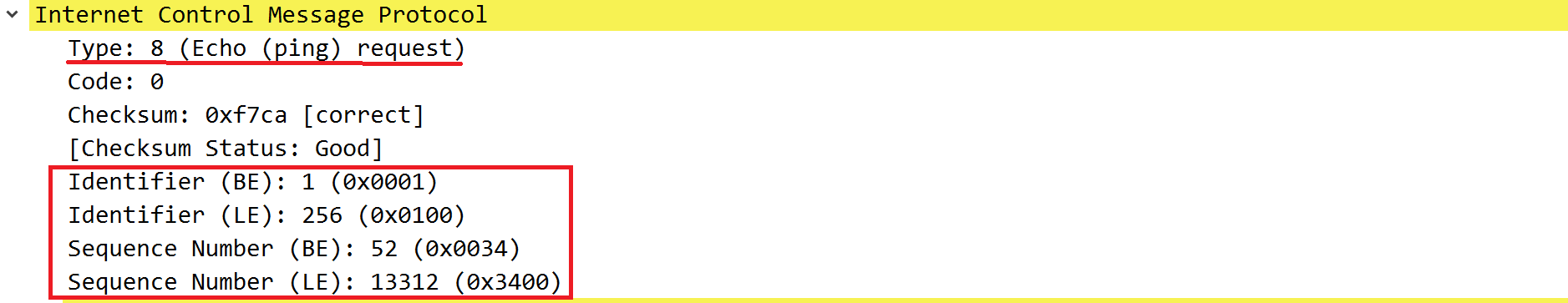
b. What are the protocol type and the Time-to-Live in the IP packet?



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?



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.

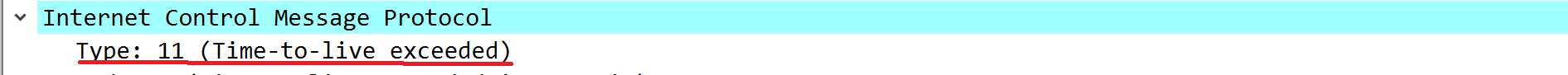
a. Examine the Internet Protocol. What are the source and destination addresses?



Source: 192.168.0.1

Destination: 192.168.0.6

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



Type: 11 (Time-to-live exceeded)

**Part 3 Measuring Network Bandwidth**

**Objective**

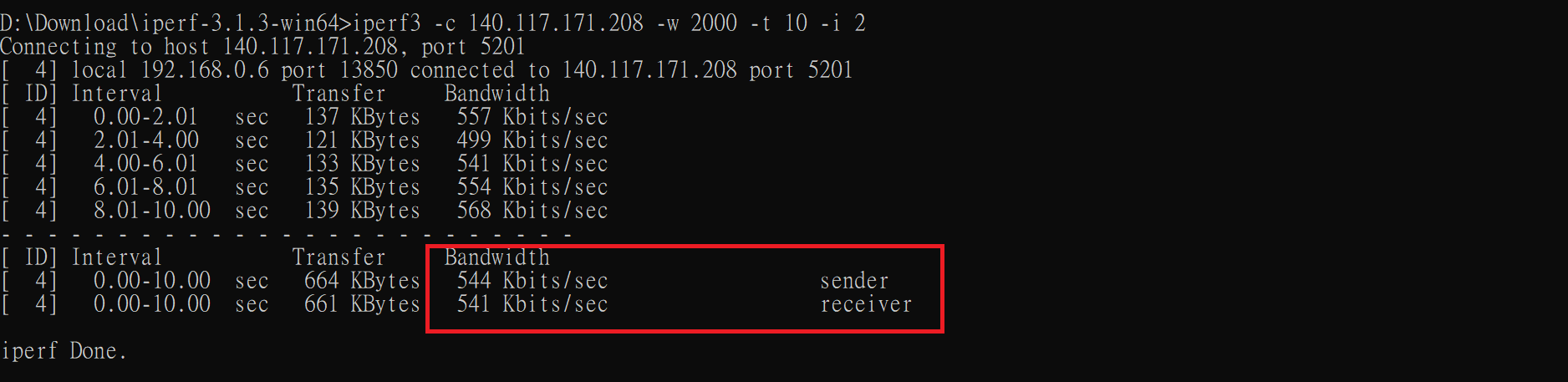
1. Measure the bandwidth for Transmission Control Protocol Type “iperf3 -c 140.117.171.208 -t 10 -i 2”



Sender bandwidth: 1.05 Mbits/sec

Receiver bandwidth: 969 Kbits/sec

1. 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”

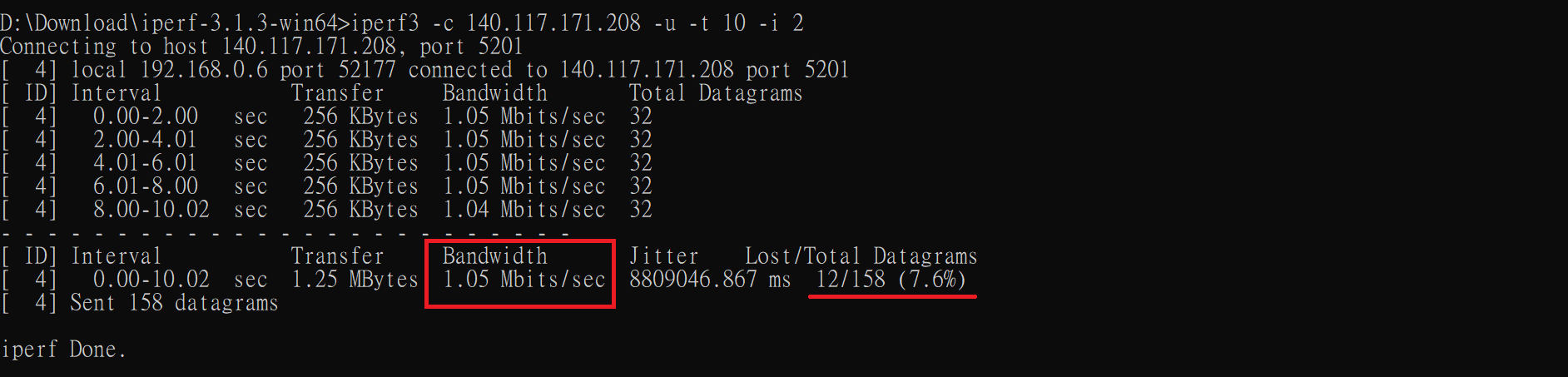


Sender bandwidth: 544 Kbits/sec

Receiver bandwidth: 541 Kbits/sec

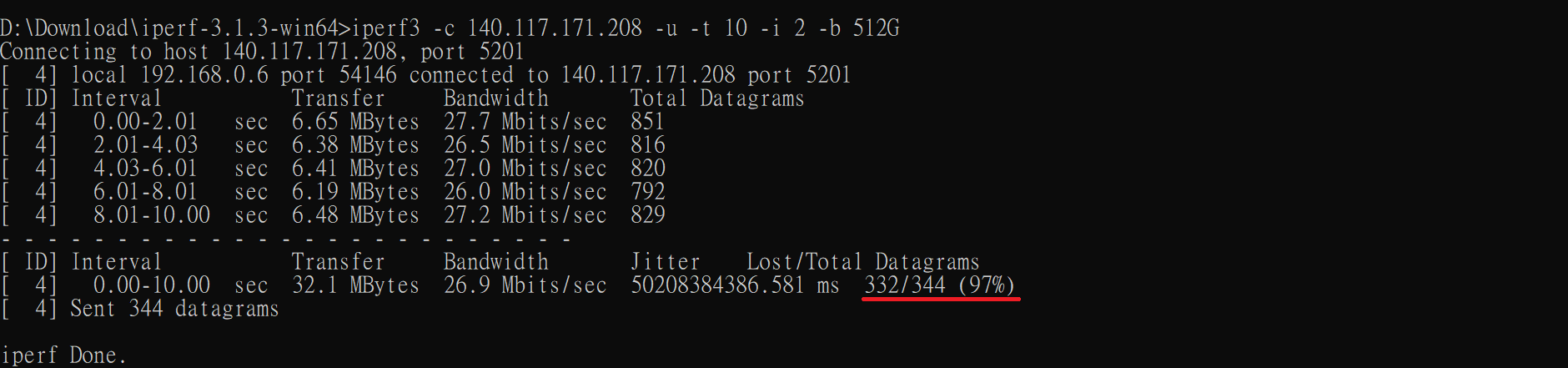
調整 window size 後，頻寬大約少了一半

1. Measure the bandwidth for User Datagram Protocol Type “iperf3 -c 140.117.171.208 -u -t 10 -i 2”



Bandwidth: 1.05 Mbits/sec

1. 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”



封包丟失率從原本 7.6% 上升到 97%