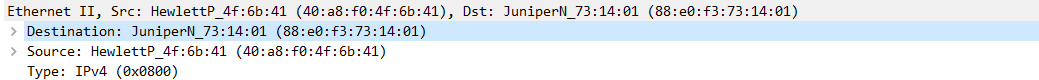
**Part1: Web Browsing (DNS, TCP)**

**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. 

(1) Examine the Ethernet 

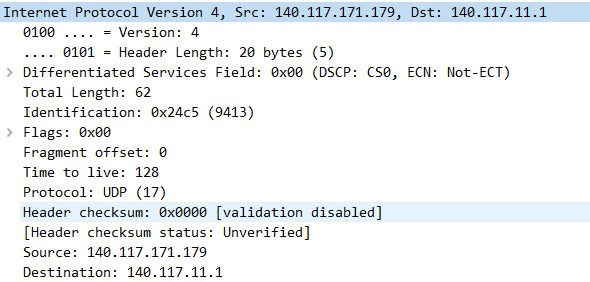
a. What is the Ethernet address of the source and destination?

Source: HewlettP\_4f:6b:41 (40:a8:f0:4f:6b:41)

Destination: JuniperN\_73:14:01 (88:e0:f3:73:14:01)

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

Type: IPv4 (0x0800)

(2) Examine the Internet Protocol 

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

source: 140.117.171.179

destination: 140.117.11.1

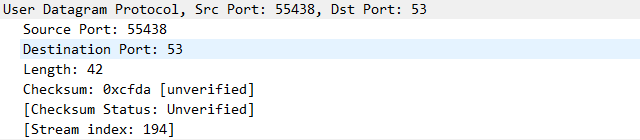
b. What is the header length? What is the total packet length?

Header Length: 20 bytes

Total Length: 62 bytes

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

Protocol: UDP (17)

(3) Examine the User Datagram Protocol 

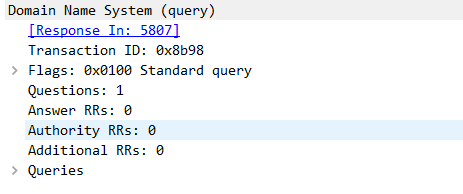
a. Identify the client ephemeral port number and the server well-known port number .

client:55438

Server:53

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

UDP

(4) Examine the Domain Name System (query) 

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

Domain Name System (query)

b. What is the query transaction ID?

Transaction ID: 0x8b98

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

Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

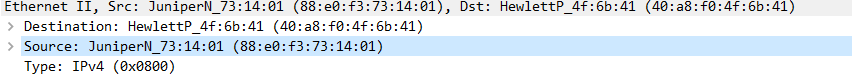
Authority RRs: 0

Additional RRs: 0

**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. 

1. Examine the Ethernet.



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

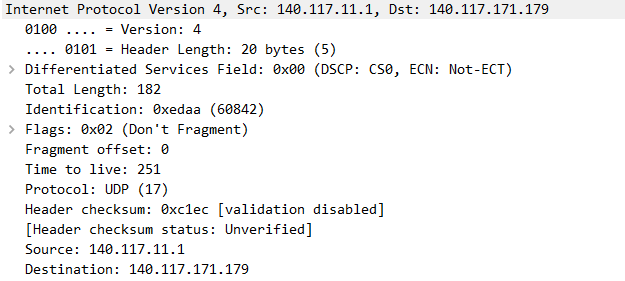
Source: JuniperN\_73:14:01 (88:e0:f3:73:14:01)

Destination: HewlettP\_4f:6b:41 (40:a8:f0:4f:6b:41)

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

Type: IPv4 (0x0800)

1. Examine the Internet Protocol & Domain Name System (response)



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

Source: 140.117.11.1

Destination: 140.117.171.179

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

Header Length: 20 bytes (5)

Total Length: 182 bytes

Yes，response比query長

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

One，time to live:3

**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.

(1) 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?

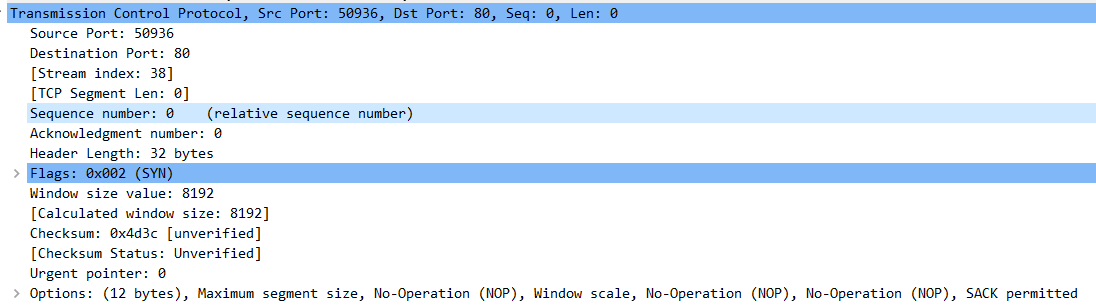
client :50936

server:80

1. What is the length of the TCP segment?

Len:0

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

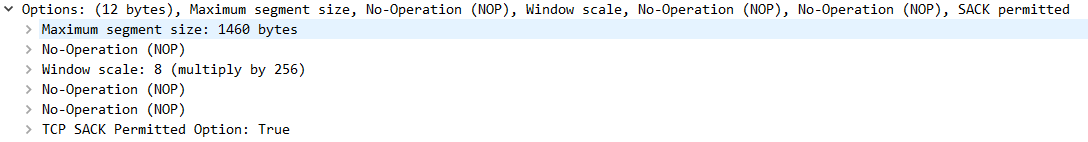


Sequence number: 0 (relative sequence number)

1. What is the initial window size?

Window size value: 8192

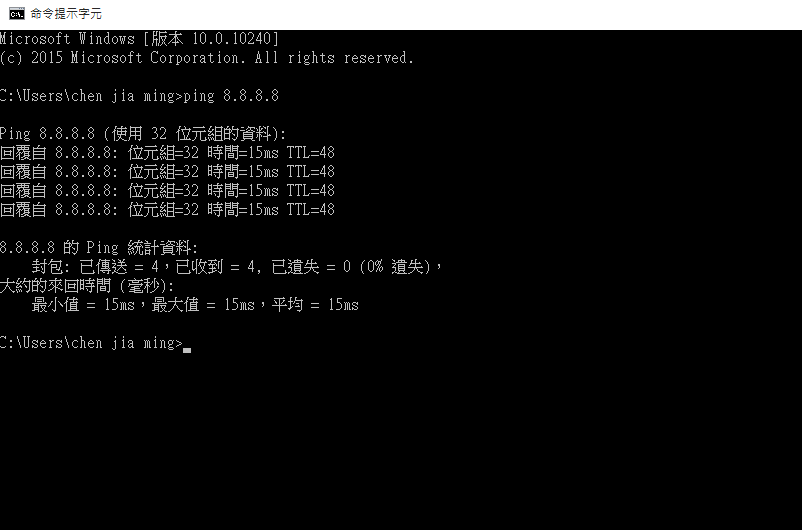
1. What is the maximum segment size?

Maximum segment size: 1460 bytes

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

Flags: 0x002 (SYN)

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

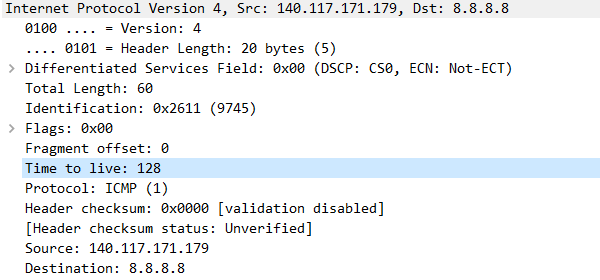


**1.** Ping Captured.

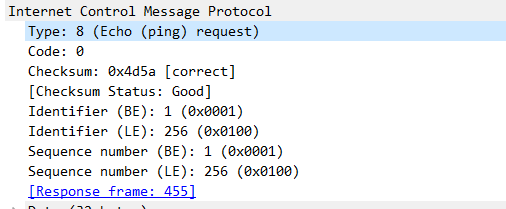
(1) Find the first ICMP Echo Request packet. 

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

Time to live: 128



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

Type: 8 (Echo (ping) request)

c. What is the message identifier and sequence number?

Identifier (BE): 1 (0x0001)

Identifier (LE): 256 (0x0100)

Sequence number (BE): 1 (0x0001)

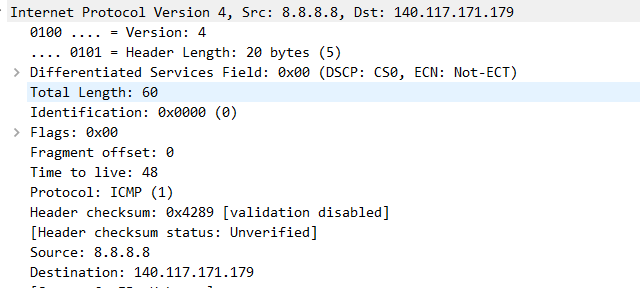
Sequence number (LE): 256 (0x0100)

(2) Find the first ICMP Echo Reply packet.



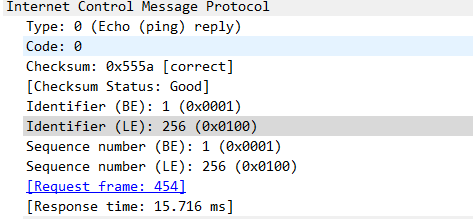
1. Examine the Internet Protocol. What are the source and destination addresses?

Source: 8.8.8.8

Destination: 140.117.171.179 

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

Type: 0 (Echo (ping) reply)



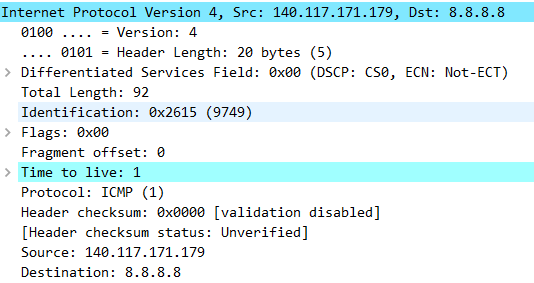
**2.** Traceroute Captured.



(1) Find the first ICMP Echo Request packet. 

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

Src: 140.117.171.179, Dst: 8.8.8.8



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

Time to live: 1

Protocol: ICMP (1)

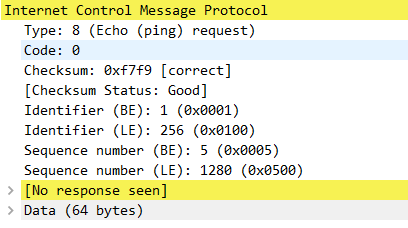
1. Next, examine the Internet Control Message Protocol. What is the ICMP message type? What are the message identifier and sequence number?

Identifier (BE): 1 (0x0001)

Identifier (LE): 256 (0x0100)

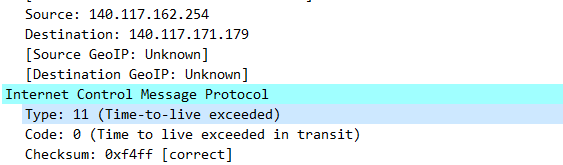
Sequence number (BE): 5 (0x0005)

Sequence number (LE): 1280 (0x0500)



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



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

Source: 140.117.162.254

Destination: 140.117.171.179

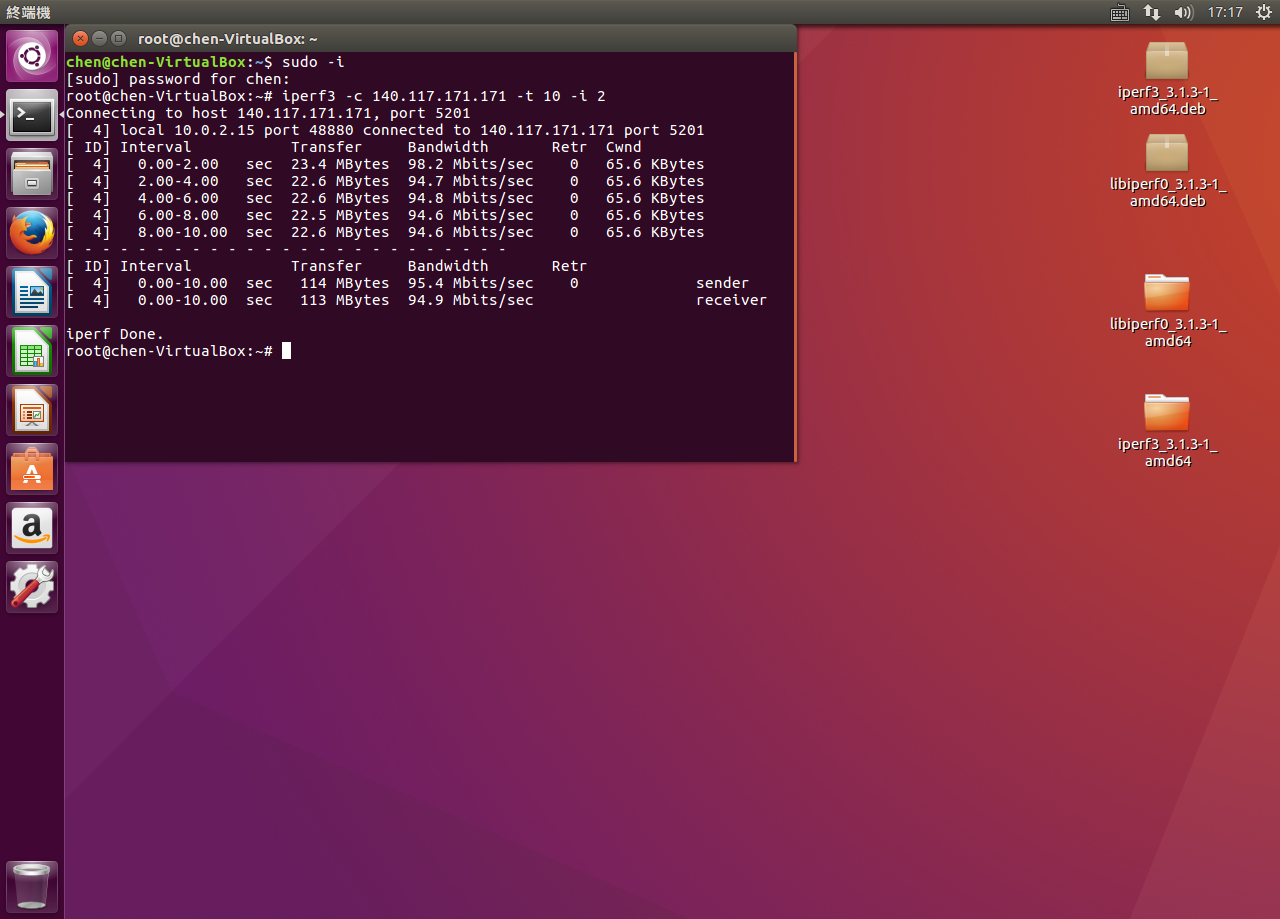
1. Next, examine the Internet Control Message Protocol. What is the ICMP message type?

Type: 11 (Time-to-live exceeded)

**Part 3 Measuring Network Bandwidth**

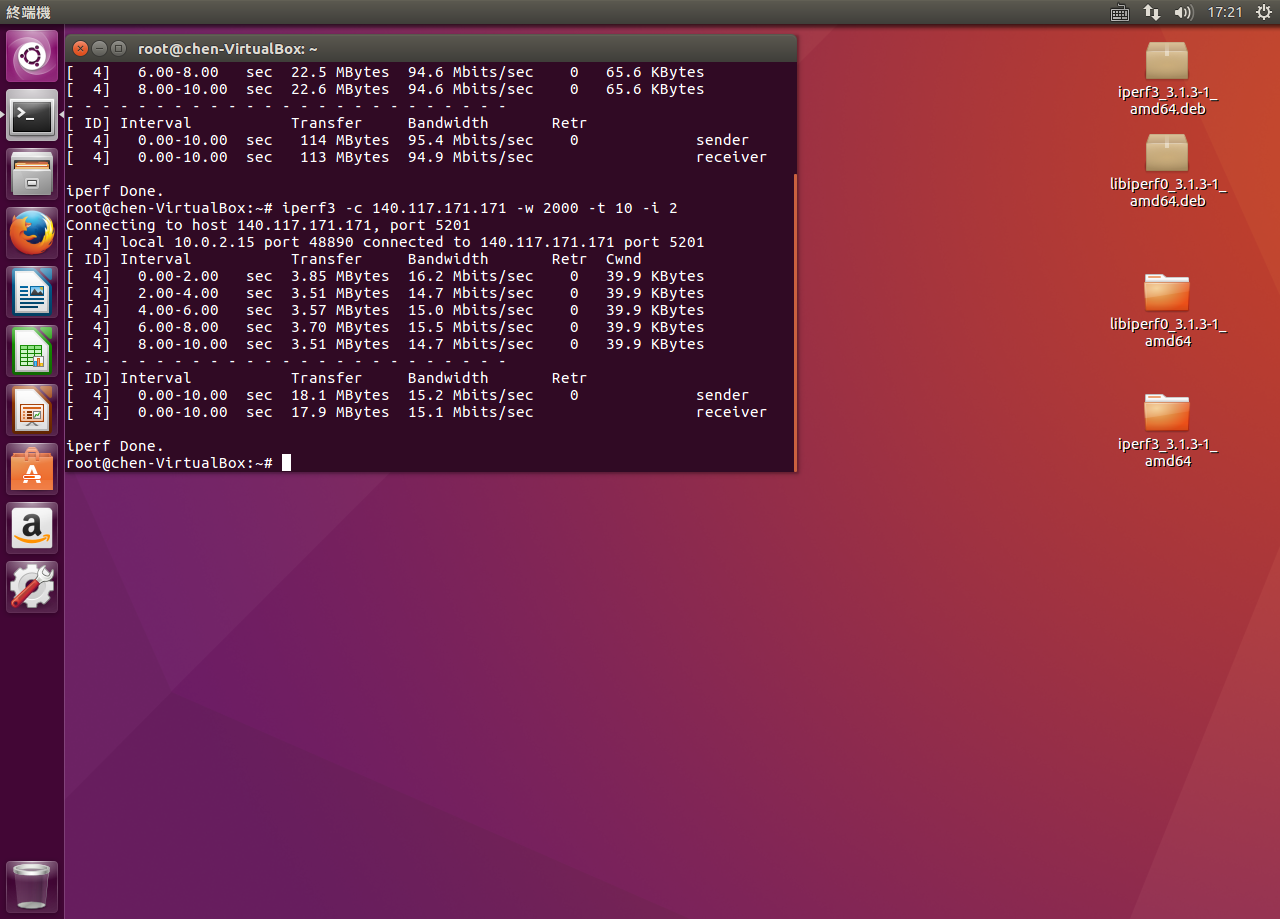
1. Measure the bandwidth for Transmission Control Protocol

Type “iperf3 -c 140.117.171.171 -t 10 -i 2”



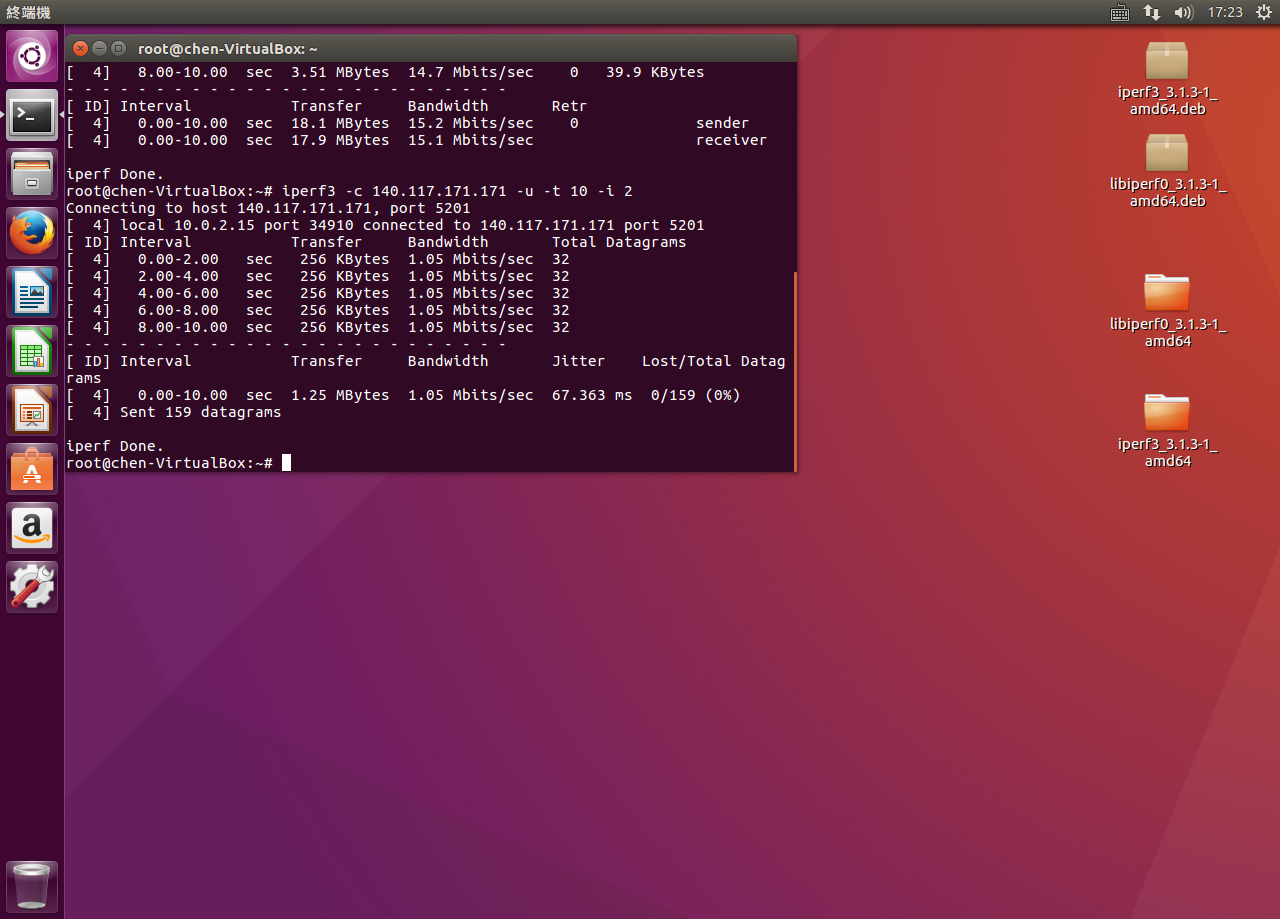
2. Adjust the window size for Transmission Control Protocol. See what’s different.

Type “iperf3 -c 140.117.171.171 -w 2000 -t 10 -i 2”



3. Measure the bandwidth for User Datagram Protocol

Type “iperf3 -c 140.117.171.171 -u -t 10 -i 2”



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

Type “iperf3 -c 140.117.171.171 -u -t 10 -i 2 -b 512G”

