**Part.I**

**1.**



**(1) Examine the Ethernet**

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

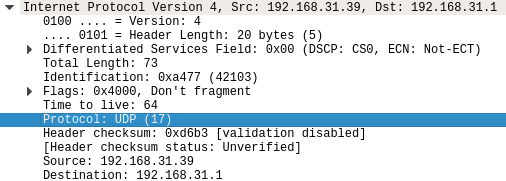
Source: 00:0c:29:b8:1b:52

Destination: 40:31:3c:22:3d:1b

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

0x0800 (IPv4)

**(2) Examine the Internet Protocol**



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

Source: 192.168.31.39

Destination: 192.168.31.1

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

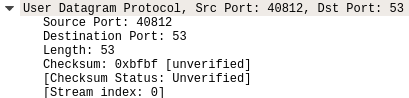
Header length = 20 Bytes

Package length = 73 Bytes

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

17 UDP

**(3) Examine the User Datagram Protocol**



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

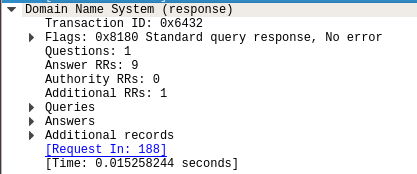
Client port: 40812

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?**

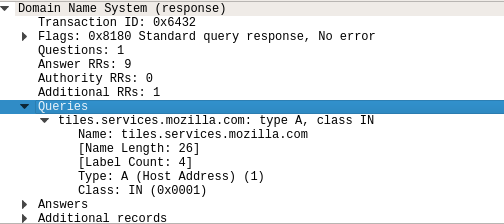
Flags

**b. What is the query transaction ID?**

0x6432

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

Queries



**2.**



**(1) Examine the Ethernet**



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

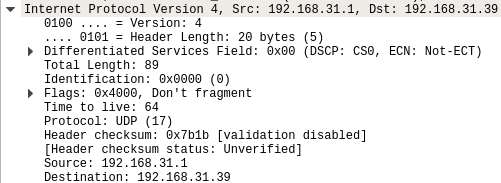
Source: 40:31:3c:22:3d:1b

Destination: 00:0c:29:b8:1b:52

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

IPv4

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



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

Source: 192.168.31.1

Destination: 192.168.31.39

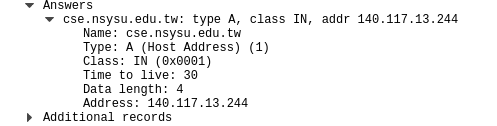
**b. What is the header length? What is the total packet length? Is it longer than the query?**

Header length: 20 Bytes

Total length: 89 Bytes

It’s longer than query packet (73 Bytes).

**c. How many answers are provided in the response message?**

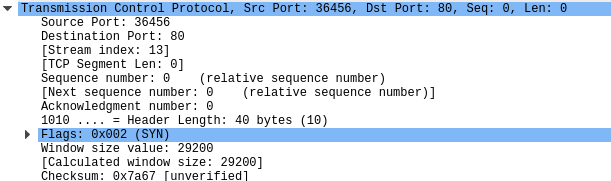
**Compare the answers and their time-to-live values.** 

1 answer, time-to-live: 30

**3.**



**(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?**

Client port: 36456

Server port: 80

**b. What is the length of the TCP segment?**

0

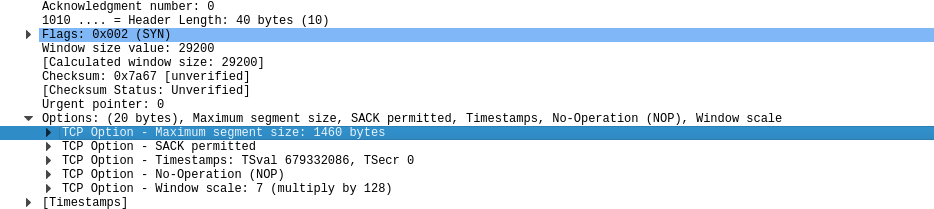
**c. What is the initial sequence number for the segments from the client to the server?**

0

**d. What is the initial window size?**

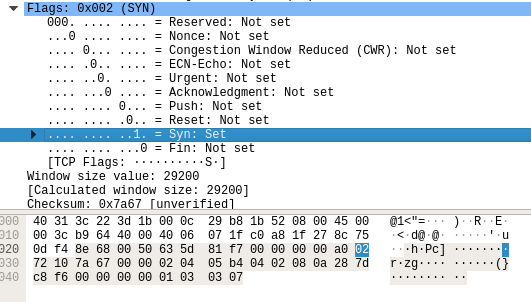
29200

**e. What is the maximum segment size?**



1460 Bytes

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



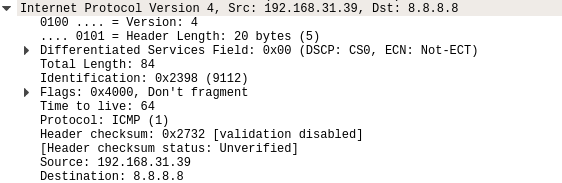
**Part.II**

**1.**

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

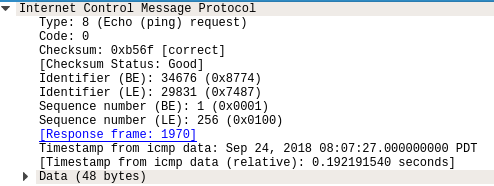


**a. First, examine the Internet Protocol. What is the Time-to-Live?**



Time-to-live: 64

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



Echo (ping) request

**c. What is the message identifier and sequence number?**

Identifier (BE): 34676 (0x8774)

Identifier (LE): 29831 (0x7487)

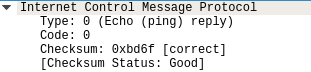
Sequence number (BE): 1 (0x0001)

Sequence number (LE): 256 (0x0100)

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



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



Echo (ping) reply

**2.**

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

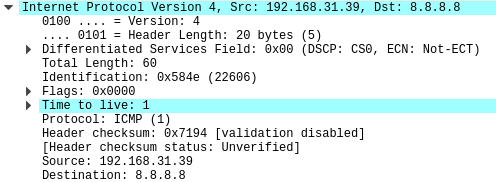


**a. Examine the Internet Protocol. What are the source and destination addresses?**

Source: 192.168.31.39

Destination: 8.8.8.8

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

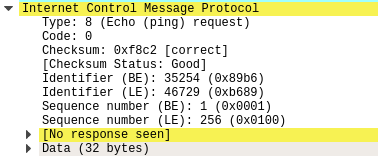


Protocol type: ICMP

Time-to-live: 1

**c. Next, examine the Internet Control Message Protocol.**

**What is the ICMP message type? What are the message identifier and sequence number?**



Type: Echo (ping) request

Identifier (BE): 35254 (0x89b6)

Identifier (LE): 46729 (0xb689)

Sequence number (BE): 1 (0x0001)

Sequence number (LE): 256 (0x0100)

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



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

Source: 192.168.31.1

Destination: 192.168.31.39

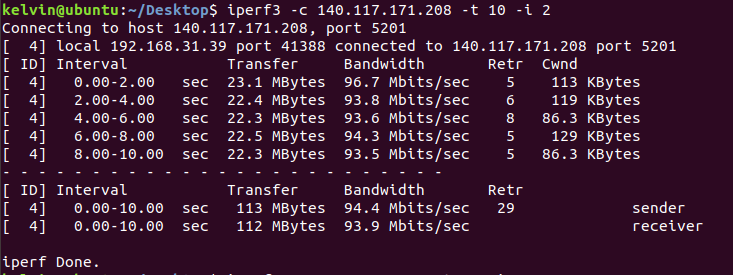
**b. Next, examine the Internet Control Message Protocol. What is the ICMP message type?**



Time-to-live exceeded

**Part.III**

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

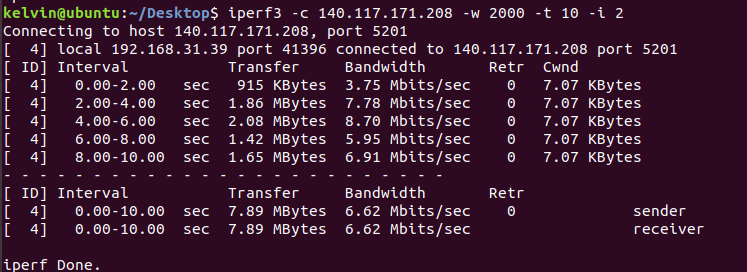


Uplink Bandwidth: 94.4Mb

Downlink Bandwidth: 93.9Mb

**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”**

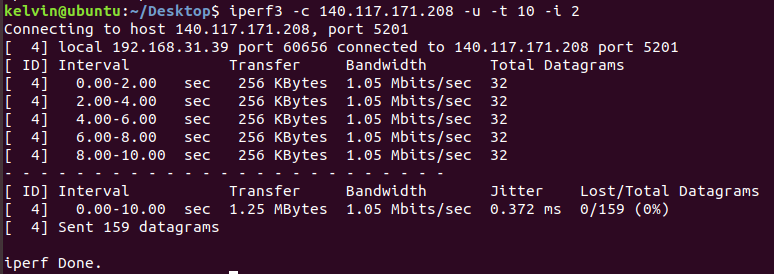


Uplink Bandwidth: 6.62Mb

Downlink Bandwidth: 6.62Mb

速度遠低於正常狀態。

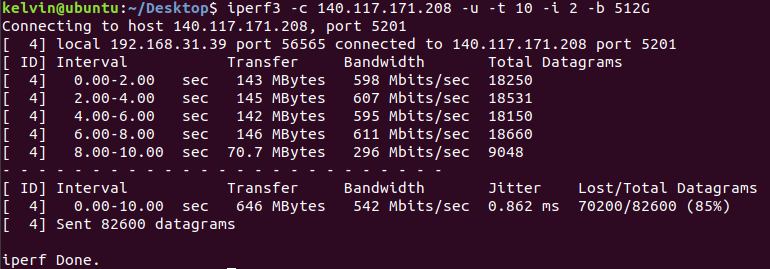
**3. Measure the bandwidth for User Datagram Protocol Type “iperf3 –c 140.117.171.208 -u -t 10 -i 2”**



Bandwidth: 1.05Mb

**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”**



Bandwidth: 542Mb

Lost/Total Datagrams: 70200/82600 (85%)

封包大量遺失。