## 學號：M083040017

## 姓名：蘇品瑜

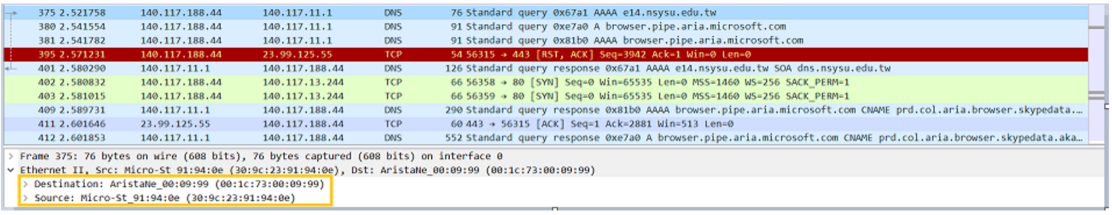
# Part 1: Web Browsing (DNS, TCP)

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?

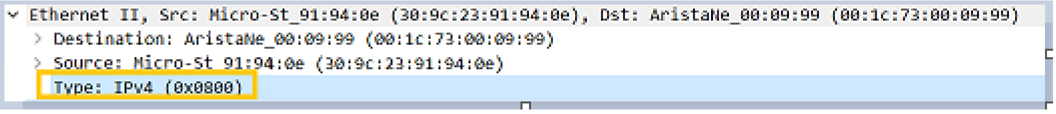


```
375 2.521758   140.117.188.44   140.117.11.1     DNS    76 Standard query 0x67a1 AAAA e14.nsysu.edu.tw
380 2.541554   140.117.188.44   140.117.11.1     DNS    91 Standard query 0xe7a0 A browser.pipe.aria.microsoft.com
381 2.541782   140.117.188.44   140.117.11.1     DNS    91 Standard query 0x81b0 AAAA browser.pipe.aria.microsoft.com
395 2.571231   140.117.188.44   23.99.125.55     TCP    54 56315 → 443 [RST, ACK] Seq=3942 Ack=1 Win=0 Len=0
401 2.580290   140.117.11.1     140.117.188.44   DNS   126 Standard query response 0x67a1 AAAA e14.nsysu.edu.tw SOA dns.nsysu.edu.tw
402 2.580832   140.117.188.44   140.117.13.244   TCP    66 56358 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
403 2.581015   140.117.188.44   140.117.13.244   TCP    66 56359 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
409 2.589731   140.117.11.1     140.117.188.44   DNS   290 Standard query response 0x81b0 AAAA browser.pipe.aria.microsoft.com CNAME prd.col.aria.browser.skypedata.…
411 2.601646   23.99.125.55     140.117.188.44   TCP    60 443 → 56315 [ACK] Seq=1 Ack=2881 Win=513 Len=0
412 2.601853   140.117.11.1     140.117.188.44   DNS   552 Standard query response 0xe7a0 A browser.pipe.aria.microsoft.com CNAME prd.col.aria.browser.skypedata.aka…

> Frame 375: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface 0
v Ethernet II, Src: Micro-St_91:94:0e (30:9c:23:91:94:0e), Dst: AristaNe_00:09:99 (00:1c:73:00:09:99)
  > Destination: AristaNe_00:09:99 (00:1c:73:00:09:99)
  > Source: Micro-St_91:94:0e (30:9c:23:91:94:0e)
```

Source: Micro-St_91:94:0e (30:9c:23:91:94:0e)

Destination:AristaNe_00:09:99(00:1c:73:00:09:99)

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

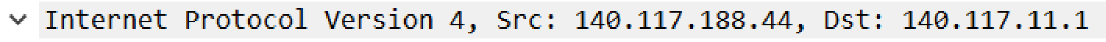


```
v Ethernet II, Src: Micro-St_91:94:0e (30:9c:23:91:94:0e), Dst: AristaNe_00:09:99 (00:1c:73:00:09:99)
  > Destination: AristaNe_00:09:99 (00:1c:73:00:09:99)
  > Source: Micro-St_91:94:0e (30:9c:23:91:94:0e)
    Type: IPv4 (0x0800)
```

Type field: IPv4

(2) Examine the Internet Protocol

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

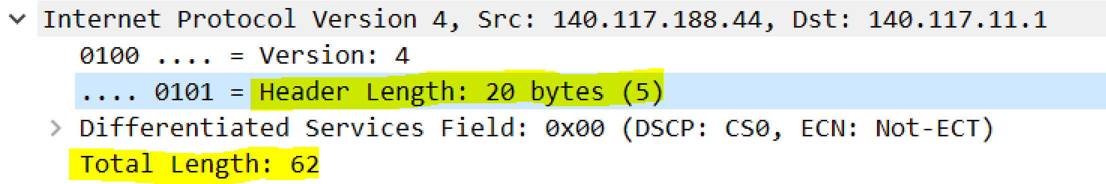


```
v Internet Protocol Version 4, Src: 140.117.188.44, Dst: 140.117.11.1
```

Source : 140.117.188.44

Destination: 140.117.11.1

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

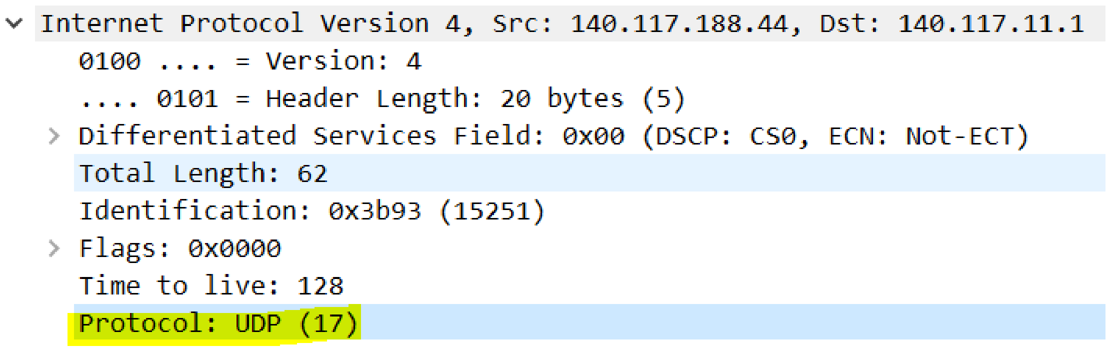


```
v Internet Protocol Version 4, Src: 140.117.188.44, Dst: 140.117.11.1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 62
```

header length:20bytes

total packet length:62bytes

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



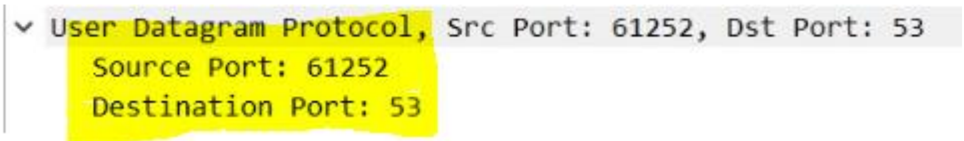
```
v Internet Protocol Version 4, Src: 140.117.188.44, Dst: 140.117.11.1
     0100 .... = Version: 4
     .... 0101 = Header Length: 20 bytes (5)
   > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
     Total Length: 62
     Identification: 0x3b93 (15251)
   > Flags: 0x0000
     Time to live: 128
     Protocol: UDP (17)
```

Type : UDP

Number : 17

(3) Examine the User Datagram Protocol

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

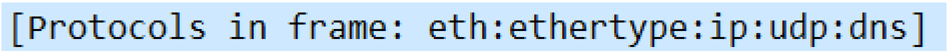


```
v User Datagram Protocol, Src Port: 61252, Dst Port: 53
     Source Port: 61252
     Destination Port: 53
```

client ephemeral port number: 61252

server well-known port number: 53

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

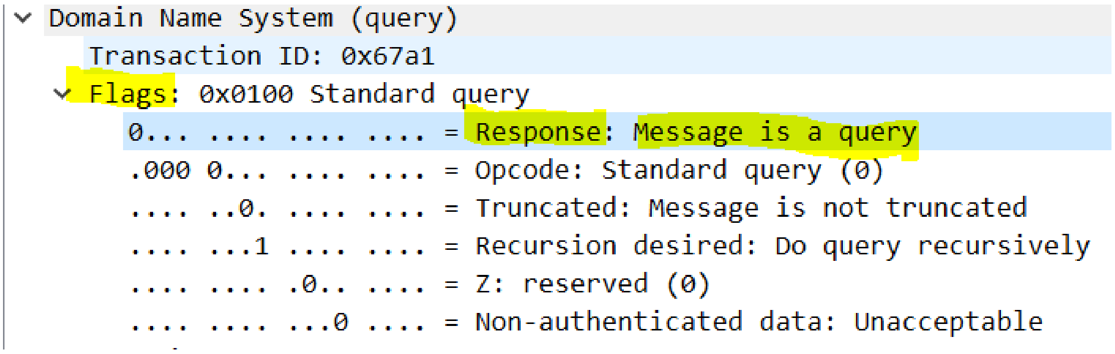


```
[Protocols in frame: eth:ethertype:ip:udp:dns]
```

DNS

(4) Examine the Domain Name System (query)

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



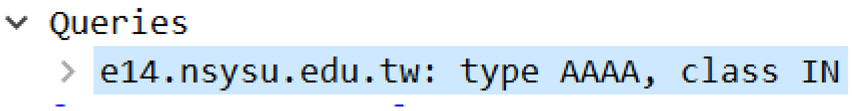
```
v Domain Name System (query)
     Transaction ID: 0x67a1
   v Flags: 0x0100 Standard query
        0... .... .... .... = Response: Message is a query
        .000 0... .... .... = Opcode: Standard query (0)
        .... ..0. .... .... = Truncated: Message is not truncated
        .... ...1 .... .... = Recursion desired: Do query recursively
        .... .... .0.. .... = Z: reserved (0)
        .... .... ...0 .... = Non-authenticated data: Unacceptable
```

Field : Response

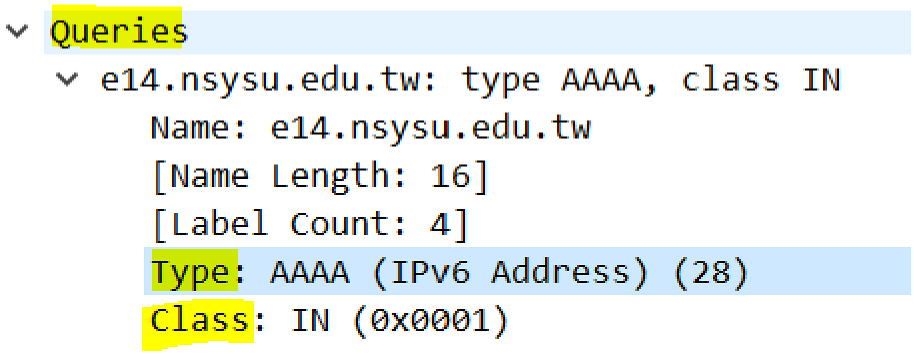
b. What is the query transaction ID?

transaction ID : 0x67a1

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



```
v Queries
   > e14.nsysu.edu.tw: type AAAA, class IN
```



```
⌄ Queries
    ⌄ e14.nsysu.edu.tw: type AAAA, class IN
        Name: e14.nsysu.edu.tw
        [Name Length: 16]
        [Label Count: 4]
        Type: AAAA (IPv6 Address) (28)
        Class: IN (0x0001)
```

Queries > Type

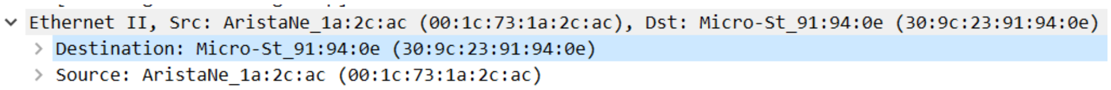
Queries > Class

**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?

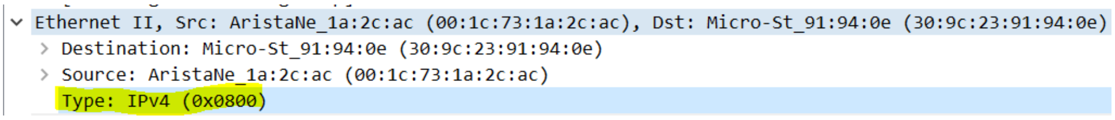


```
⌄ Ethernet II, Src: AristaNe_1a:2c:ac (00:1c:73:1a:2c:ac), Dst: Micro-St_91:94:0e (30:9c:23:91:94:0e)
  > Destination: Micro-St_91:94:0e (30:9c:23:91:94:0e)
  > Source: AristaNe_1a:2c:ac (00:1c:73:1a:2c:ac)
```

Source : AristaNe_1a:2c:ac

Destination: Micro-St_91:94:0e

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

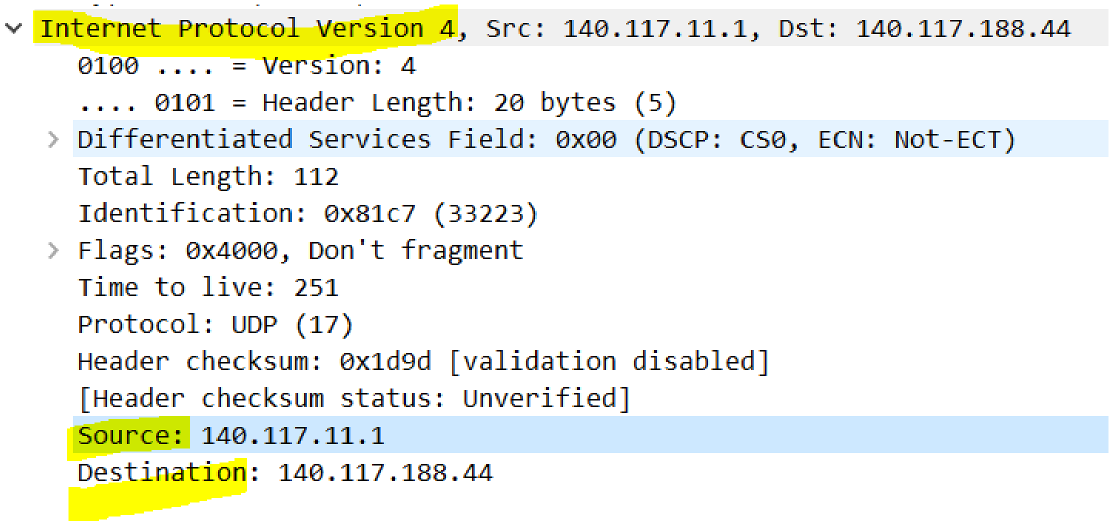


```
⌄ Ethernet II, Src: AristaNe_1a:2c:ac (00:1c:73:1a:2c:ac), Dst: Micro-St_91:94:0e (30:9c:23:91:94:0e)
  > Destination: Micro-St_91:94:0e (30:9c:23:91:94:0e)
  > Source: AristaNe_1a:2c:ac (00:1c:73:1a:2c:ac)
    Type: IPv4 (0x0800)
```

Ans : IPv4

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

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

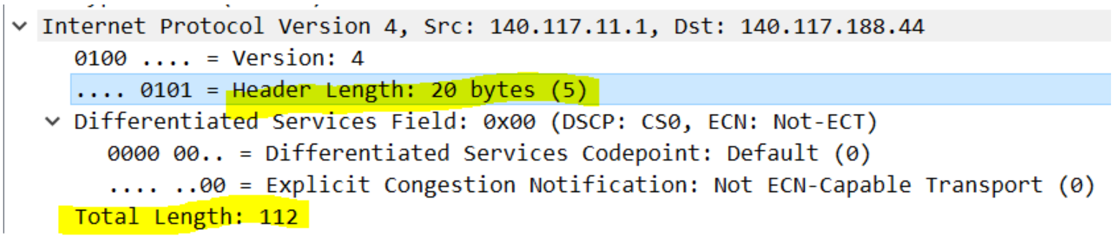


```
v Internet Protocol Version 4, Src: 140.117.11.1, Dst: 140.117.188.44
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 112
    Identification: 0x81c7 (33223)
  > Flags: 0x4000, Don't fragment
    Time to live: 251
    Protocol: UDP (17)
    Header checksum: 0x1d9d [validation disabled]
    [Header checksum status: Unverified]
    Source: 140.117.11.1
    Destination: 140.117.188.44
```

Source : 140.117.11.1

Destination: 140.117.188.44

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



```
v Internet Protocol Version 4, Src: 140.117.11.1, Dst: 140.117.188.44
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  v Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 112
```

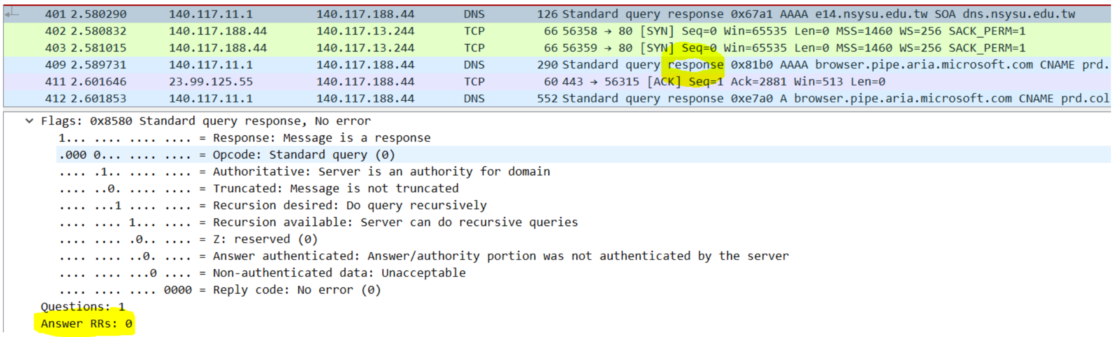
header length:20 bytes

packet length:112

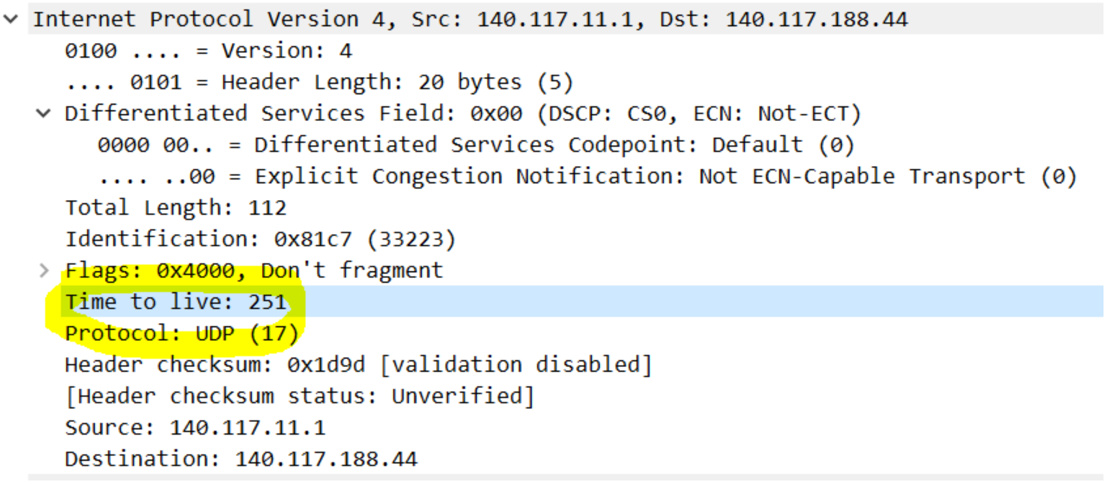
For header length is equal.

For total packet length is longer.

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



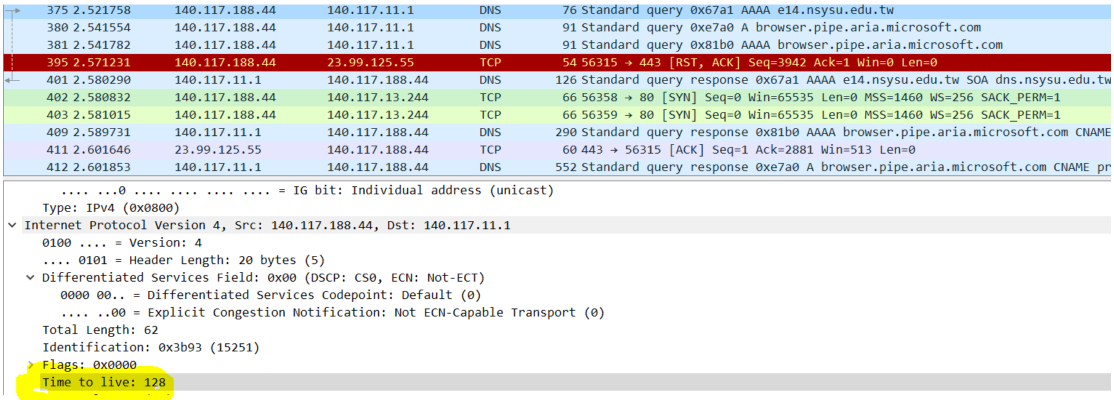
```
401 2.580290   140.117.11.1     140.117.188.44   DNS   126 Standard query response 0x67a1 AAAA e14.nsysu.edu.tw SOA dns.nsysu.edu.tw
402 2.580832   140.117.188.44   140.117.13.244   TCP    66 56358 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
403 2.581015   140.117.188.44   140.117.13.244   TCP    66 56359 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
409 2.589731   140.117.11.1     140.117.188.44   DNS   290 Standard query response 0x81b0 AAAA browser.pipe.aria.microsoft.com CNAME prd.
411 2.601646   23.99.125.55     140.117.188.44   TCP    60 443 → 56315 [ACK] Seq=1 Ack=2881 Win=513 Len=0
412 2.601853   140.117.11.1     140.117.188.44   DNS   552 Standard query response 0xe7a0 A browser.pipe.aria.microsoft.com CNAME prd.col

v Flags: 0x8580 Standard query response, No error
    1... .... .... .... = Response: Message is a response
    .000 0... .... .... = Opcode: Standard query (0)
    .... .1.. .... .... = Authoritative: Server is an authority for domain
    .... ..0. .... .... = Truncated: Message is not truncated
    .... ...1 .... .... = Recursion desired: Do query recursively
    .... .... 1... .... = Recursion available: Server can do recursive queries
    .... .... .0.. .... = Z: reserved (0)
    .... .... ..0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server
    .... .... ...0 .... = Non-authenticated data: Unacceptable
    .... .... .... 0000 = Reply code: No error (0)
  Questions: 1
  Answer RRs: 0
```



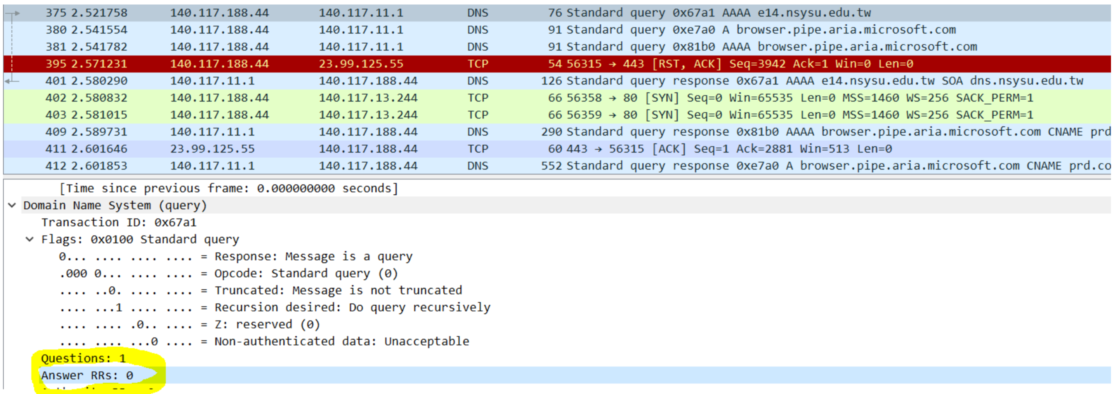
```
v Internet Protocol Version 4, Src: 140.117.11.1, Dst: 140.117.188.44
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  v Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 112
    Identification: 0x81c7 (33223)
  > Flags: 0x4000, Don't fragment
    Time to live: 251
    Protocol: UDP (17)
    Header checksum: 0x1d9d [validation disabled]
    [Header checksum status: Unverified]
    Source: 140.117.11.1
    Destination: 140.117.188.44
```

Response :

- Ans: 0
- Time to live: 251



```
375 2.521758   140.117.188.44   140.117.11.1     DNS    76 Standard query 0x67a1 AAAA e14.nsysu.edu.tw
380 2.541554   140.117.188.44   140.117.11.1     DNS    91 Standard query 0xe7a0 A browser.pipe.aria.microsoft.com
381 2.541782   140.117.188.44   140.117.11.1     DNS    91 Standard query 0x81b0 AAAA browser.pipe.aria.microsoft.com
395 2.571231   140.117.188.44   23.99.125.55     TCP    54 56315 → 443 [RST, ACK] Seq=3942 Ack=1 Win=0 Len=0
401 2.580290   140.117.11.1     140.117.188.44   DNS   126 Standard query response 0x67a1 AAAA e14.nsysu.edu.tw SOA dns.nsysu.edu.tw
402 2.580832   140.117.188.44   140.117.13.244   TCP    66 56358 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
403 2.581015   140.117.188.44   140.117.13.244   TCP    66 56359 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
409 2.589731   140.117.11.1     140.117.188.44   DNS   290 Standard query response 0x81b0 AAAA browser.pipe.aria.microsoft.com CNAME
411 2.601646   23.99.125.55     140.117.188.44   TCP    60 443 → 56315 [ACK] Seq=1 Ack=2881 Win=513 Len=0
412 2.601853   140.117.11.1     140.117.188.44   DNS   552 Standard query response 0xe7a0 A browser.pipe.aria.microsoft.com CNAME pr

      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
v Internet Protocol Version 4, Src: 140.117.188.44, Dst: 140.117.11.1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  v Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 62
    Identification: 0x3b93 (15251)
  > Flags: 0x0000
    Time to live: 128
```



```
375 2.521758   140.117.188.44   140.117.11.1     DNS    76 Standard query 0x67a1 AAAA e14.nsysu.edu.tw
380 2.541554   140.117.188.44   140.117.11.1     DNS    91 Standard query 0xe7a0 A browser.pipe.aria.microsoft.com
381 2.541782   140.117.188.44   140.117.11.1     DNS    91 Standard query 0x81b0 AAAA browser.pipe.aria.microsoft.com
395 2.571231   140.117.188.44   23.99.125.55     TCP    54 56315 → 443 [RST, ACK] Seq=3942 Ack=1 Win=0 Len=0
401 2.580290   140.117.11.1     140.117.188.44   DNS   126 Standard query response 0x67a1 AAAA e14.nsysu.edu.tw SOA dns.nsysu.edu.tw
402 2.580832   140.117.188.44   140.117.13.244   TCP    66 56358 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
403 2.581015   140.117.188.44   140.117.13.244   TCP    66 56359 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
409 2.589731   140.117.11.1     140.117.188.44   DNS   290 Standard query response 0x81b0 AAAA browser.pipe.aria.microsoft.com CNAME prd
411 2.601646   23.99.125.55     140.117.188.44   TCP    60 443 → 56315 [ACK] Seq=1 Ack=2881 Win=513 Len=0
412 2.601853   140.117.11.1     140.117.188.44   DNS   552 Standard query response 0xe7a0 A browser.pipe.aria.microsoft.com CNAME prd.co

      [Time since previous frame: 0.000000000 seconds]
v Domain Name System (query)
    Transaction ID: 0x67a1
  v 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
```

Request:

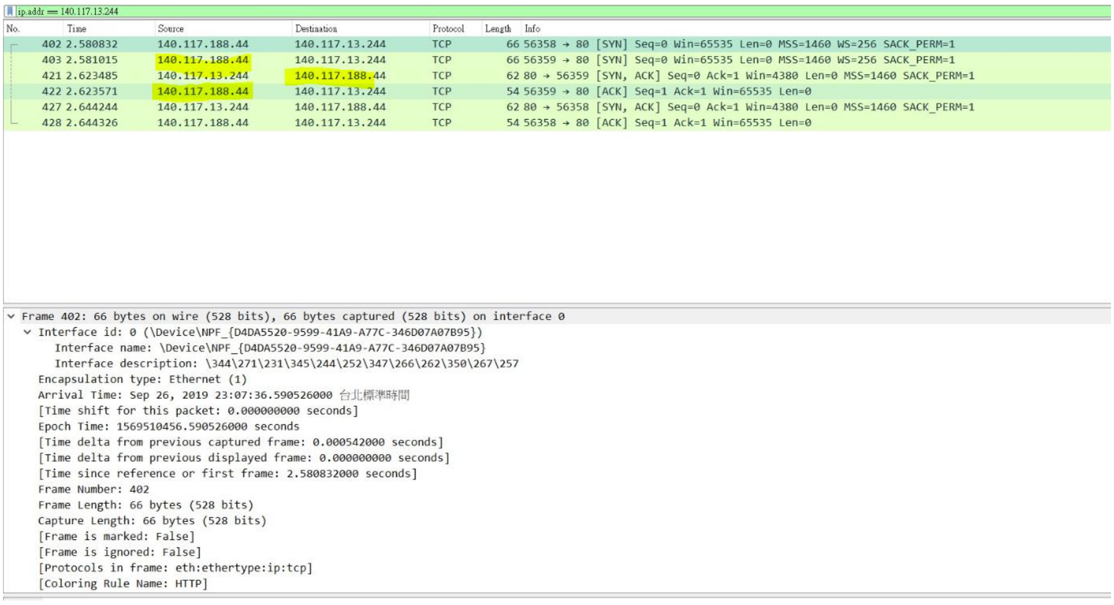
- Ans:
- Time to live:

| | Request | Response |
|---|---|---|
| Answer number | 0 | 0 |
| Time to live | 128 | 251 |

**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.**

Figure: TCP three-way handshake

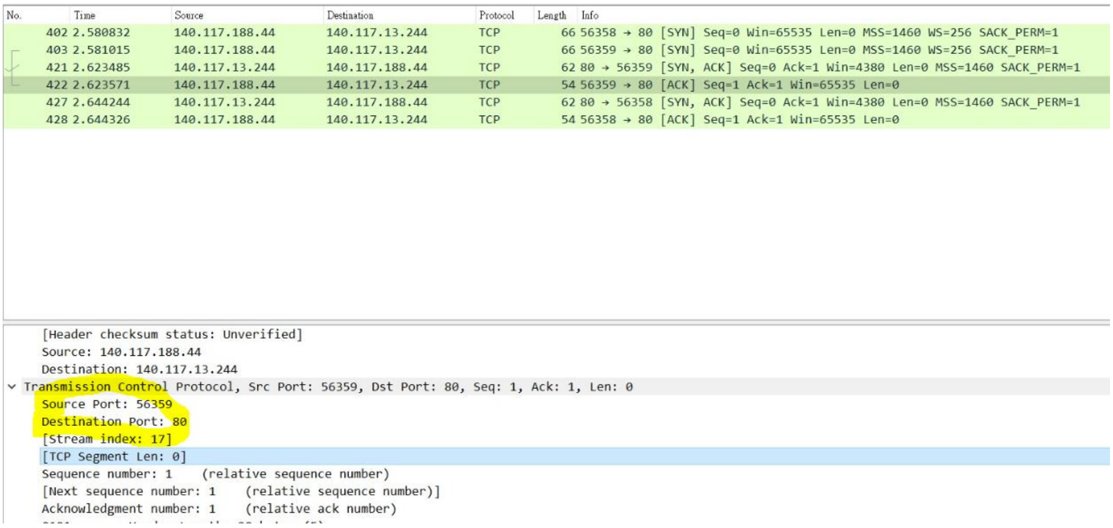


```
ip.addr == 140.117.13.244

No.   Time       Source           Destination      Protocol  Length  Info
  402 2.580832   140.117.188.44   140.117.13.244   TCP       66 56358 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
  403 2.581015   140.117.188.44   140.117.13.244   TCP       66 56359 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
  421 2.623485   140.117.13.244   140.117.188.44   TCP       62 80 → 56359 [SYN, ACK] Seq=0 Ack=1 Win=4380 Len=0 MSS=1460 SACK_PERM=1
  422 2.623571   140.117.188.44   140.117.13.244   TCP       54 56359 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0
  427 2.644244   140.117.13.244   140.117.188.44   TCP       62 80 → 56358 [SYN, ACK] Seq=0 Ack=1 Win=4380 Len=0 MSS=1460 SACK_PERM=1
  428 2.644326   140.117.188.44   140.117.13.244   TCP       54 56358 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0
```

```
v Frame 402: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
  v Interface id: 0 (\Device\NPF_{D4DA5520-9599-41A9-A77C-346D07A07B95})
      Interface name: \Device\NPF_{D4DA5520-9599-41A9-A77C-346D07A07B95}
      Interface description: \344\271\231\345\244\252\347\266\262\350\267\257
    Encapsulation type: Ethernet (1)
    Arrival Time: Sep 26, 2019 23:07:36.590526000 台北標準時間
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1569510456.590526000 seconds
    [Time delta from previous captured frame: 0.000542000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 2.580832000 seconds]
    Frame Number: 402
    Frame Length: 66 bytes (528 bits)
    Capture Length: 66 bytes (528 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp]
    [Coloring Rule Name: HTTP]
```

(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?



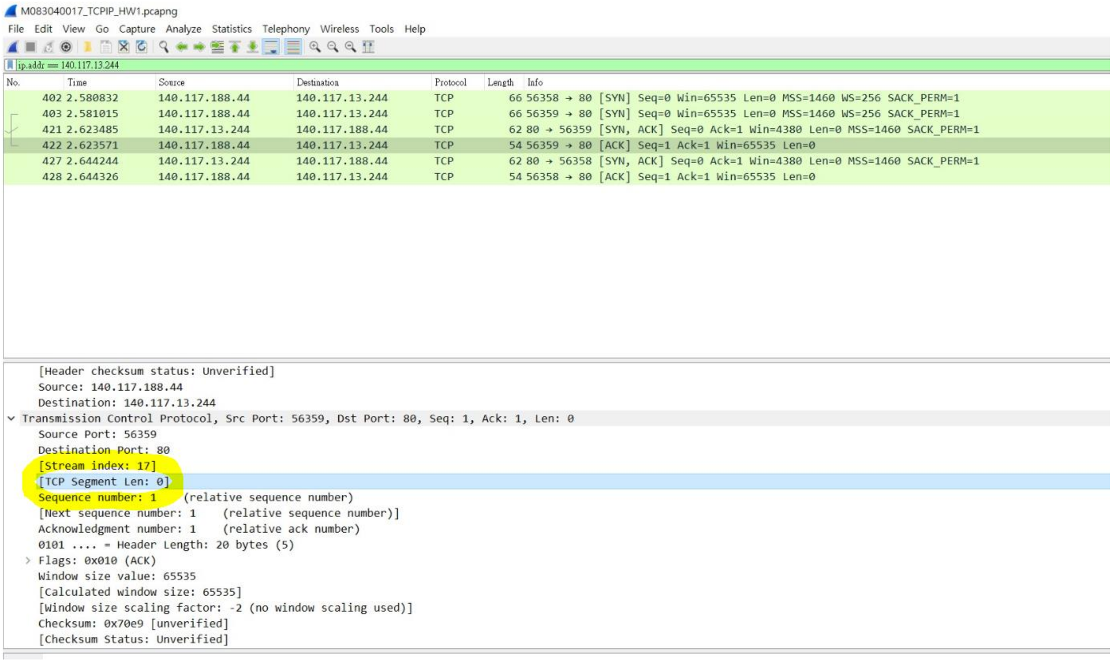
```
No.   Time       Source           Destination      Protocol  Length  Info
  402 2.580832   140.117.188.44   140.117.13.244   TCP       66 56358 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
  403 2.581015   140.117.188.44   140.117.13.244   TCP       66 56359 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
  421 2.623485   140.117.13.244   140.117.188.44   TCP       62 80 → 56359 [SYN, ACK] Seq=0 Ack=1 Win=4380 Len=0 MSS=1460 SACK_PERM=1
  422 2.623571   140.117.188.44   140.117.13.244   TCP       54 56359 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0
  427 2.644244   140.117.13.244   140.117.188.44   TCP       62 80 → 56358 [SYN, ACK] Seq=0 Ack=1 Win=4380 Len=0 MSS=1460 SACK_PERM=1
  428 2.644326   140.117.188.44   140.117.13.244   TCP       54 56358 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0
```

```
    [Header checksum status: Unverified]
    Source: 140.117.188.44
    Destination: 140.117.13.244
v Transmission Control Protocol, Src Port: 56359, Dst Port: 80, Seq: 1, Ack: 1, Len: 0
    Source Port: 56359
    Destination Port: 80
    [Stream index: 17]
    [TCP Segment Len: 0]
    Sequence number: 1    (relative sequence number)
    [Next sequence number: 1    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
```

ephemeral port number: 56359

well-known port number: 80

b. What is the length of the TCP segment?



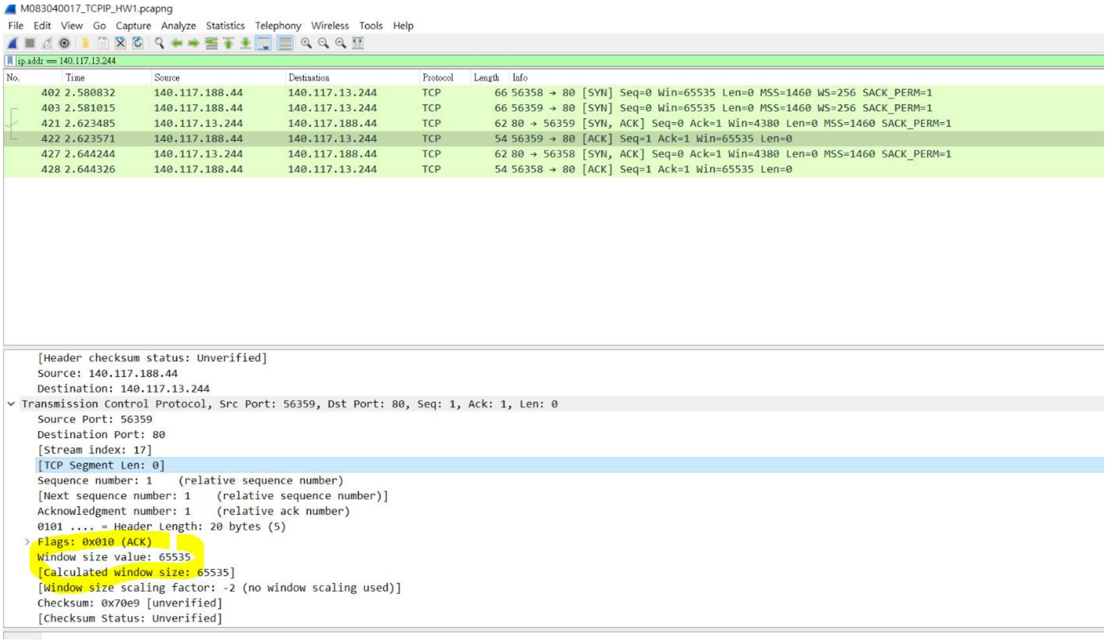
```
M083040017_TCPIP_HW1.pcapng
File  Edit  View  Go  Capture  Analyze  Statistics  Telephony  Wireless  Tools  Help
ip.addr == 140.117.13.244
No.     Time         Source           Destination      Protocol  Length  Info
    402 2.580832     140.117.188.44   140.117.13.244   TCP         66 56358 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
    403 2.581015     140.117.188.44   140.117.13.244   TCP         66 56359 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
    421 2.623485     140.117.13.244   140.117.188.44   TCP         62 80 → 56359 [SYN, ACK] Seq=0 Ack=1 Win=4380 Len=0 MSS=1460 SACK_PERM=1
    422 2.623571     140.117.188.44   140.117.13.244   TCP         54 56359 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0
    427 2.644244     140.117.13.244   140.117.188.44   TCP         62 80 → 56358 [SYN, ACK] Seq=0 Ack=1 Win=4380 Len=0 MSS=1460 SACK_PERM=1
    428 2.644326     140.117.188.44   140.117.13.244   TCP         54 56358 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0

    [Header checksum status: Unverified]
    Source: 140.117.188.44
    Destination: 140.117.13.244
v Transmission Control Protocol, Src Port: 56359, Dst Port: 80, Seq: 1, Ack: 1, Len: 0
    Source Port: 56359
    Destination Port: 80
    [Stream index: 17]
    [TCP Segment Len: 0]
    Sequence number: 1    (relative sequence number)
    [Next sequence number: 1    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x010 (ACK)
    Window size value: 65535
    [Calculated window size: 65535]
    [Window size scaling factor: -2 (no window scaling used)]
    Checksum: 0x70e9 [unverified]
    [Checksum Status: Unverified]
```

the length of the TCP segment: 0

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

initial sequence number:1

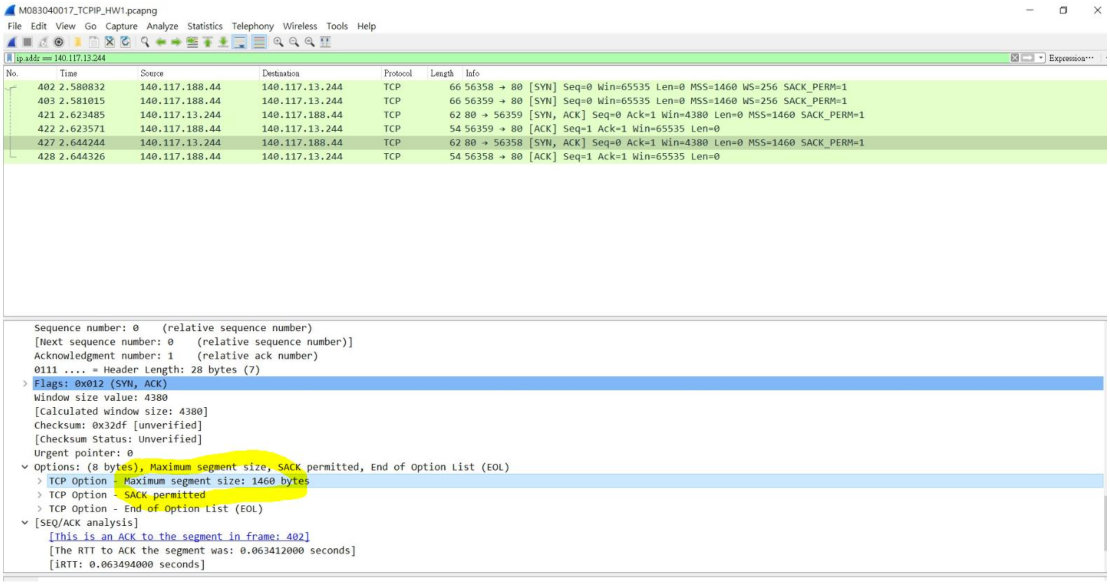
d. What is the initial window size?



```
M083040017_TCPIP_HW1.pcapng
File  Edit  View  Go  Capture  Analyze  Statistics  Telephony  Wireless  Tools  Help
ip.addr == 140.117.13.244
No.     Time         Source           Destination      Protocol  Length  Info
    402 2.580832     140.117.188.44   140.117.13.244   TCP         66 56358 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
    403 2.581015     140.117.188.44   140.117.13.244   TCP         66 56359 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
    421 2.623485     140.117.13.244   140.117.188.44   TCP         62 80 → 56359 [SYN, ACK] Seq=0 Ack=1 Win=4380 Len=0 MSS=1460 SACK_PERM=1
    422 2.623571     140.117.188.44   140.117.13.244   TCP         54 56359 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0
    427 2.644244     140.117.13.244   140.117.188.44   TCP         62 80 → 56358 [SYN, ACK] Seq=0 Ack=1 Win=4380 Len=0 MSS=1460 SACK_PERM=1
    428 2.644326     140.117.188.44   140.117.13.244   TCP         54 56358 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0

    [Header checksum status: Unverified]
    Source: 140.117.188.44
    Destination: 140.117.13.244
v Transmission Control Protocol, Src Port: 56359, Dst Port: 80, Seq: 1, Ack: 1, Len: 0
    Source Port: 56359
    Destination Port: 80
    [Stream index: 17]
    [TCP Segment Len: 0]
    Sequence number: 1    (relative sequence number)
    [Next sequence number: 1    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x010 (ACK)
    Window size value: 65535
    [Calculated window size: 65535]
    [Window size scaling factor: -2 (no window scaling used)]
    Checksum: 0x70e9 [unverified]
    [Checksum Status: Unverified]
```

initial window size : 65535

e. What is the maximum segment size?

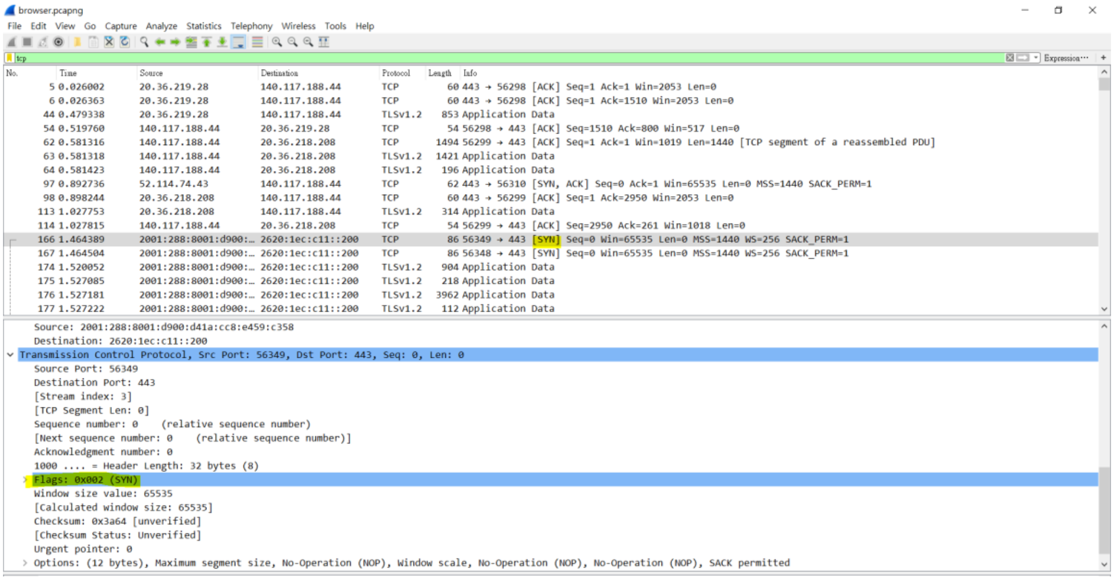

M083040017_TCPIP_HW1.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression…

```
ip.addr == 140.117.13.244

No.    Time          Source            Destination       Protocol  Length  Info
   402 2.580832      140.117.188.44    140.117.13.244    TCP         66 56358 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
   403 2.581015      140.117.188.44    140.117.13.244    TCP         66 56359 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
   421 2.623485      140.117.13.244    140.117.188.44    TCP         62 80 → 56359 [SYN, ACK] Seq=0 Ack=1 Win=4380 Len=0 MSS=1460 SACK_PERM=1
   422 2.623571      140.117.188.44    140.117.13.244    TCP         54 56359 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0
   427 2.644244      140.117.13.244    140.117.188.44    TCP         62 80 → 56358 [SYN, ACK] Seq=0 Ack=1 Win=4380 Len=0 MSS=1460 SACK_PERM=1
   428 2.644326      140.117.188.44    140.117.13.244    TCP         54 56358 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0
```

```
    Sequence number: 0    (relative sequence number)
    [Next sequence number: 0    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    0111 .... = Header Length: 28 bytes (7)
  > Flags: 0x012 (SYN, ACK)
    Window size value: 4380
    [Calculated window size: 4380]
    Checksum: 0x32df [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  v Options: (8 bytes), Maximum segment size, SACK permitted, End of Option List (EOL)
      > TCP Option - Maximum segment size: 1460 bytes
      > TCP Option - SACK permitted
      > TCP Option - End of Option List (EOL)
  v [SEQ/ACK analysis]
      [This is an ACK to the segment in frame: 402]
      [The RTT to ACK the segment was: 0.063412000 seconds]
      [iRTT: 0.063494000 seconds]
```

maximum segment size: 1460bytes

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


browser.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression…

```
tcp

No.    Time          Source               Destination        Protocol  Length  Info
     5 0.026002      20.36.219.28         140.117.188.44     TCP         60 443 → 56298 [ACK] Seq=1 Ack=1 Win=2053 Len=0
     6 0.026363      20.36.219.28         140.117.188.44     TCP         60 443 → 56298 [ACK] Seq=1 Ack=1510 Win=2053 Len=0
    44 0.479338      20.36.219.28         140.117.188.44     TLSv1.2    853 Application Data
    54 0.519760      140.117.188.44       20.36.219.28       TCP         54 56298 → 443 [ACK] Seq=1510 Ack=800 Win=517 Len=0
    62 0.581316      140.117.188.44       20.36.218.208      TCP       1494 56299 → 443 [ACK] Seq=1 Ack=1 Win=1019 Len=1440 [TCP segment of a reassembled PDU]
    63 0.581318      140.117.188.44       20.36.218.208      TLSv1.2   1421 Application Data
    64 0.581423      140.117.188.44       20.36.218.208      TLSv1.2    196 Application Data
    97 0.892736      52.114.74.43         140.117.188.44     TCP         62 443 → 56310 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 SACK_PERM=1
    98 0.898244      20.36.218.208        140.117.188.44     TCP         60 443 → 56299 [ACK] Seq=1 Ack=2950 Win=2053 Len=0
   113 1.027753      20.36.218.208        140.117.188.44     TLSv1.2    314 Application Data
   114 1.027815      140.117.188.44       20.36.218.208      TCP         54 56299 → 443 [ACK] Seq=2950 Ack=261 Win=1018 Len=0
   166 1.464389      2001:288:8001:d900:… 2620:1ec:c11::200  TCP         86 56349 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM=1
   167 1.464504      2001:288:8001:d900:… 2620:1ec:c11::200  TCP         86 56348 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM=1
   174 1.520052      2001:288:8001:d900:… 2620:1ec:c11::200  TLSv1.2    904 Application Data
   175 1.527085      2001:288:8001:d900:… 2620:1ec:c11::200  TLSv1.2    218 Application Data
   176 1.527181      2001:288:8001:d900:… 2620:1ec:c11::200  TLSv1.2   3962 Application Data
   177 1.527222      2001:288:8001:d900:… 2620:1ec:c11::200  TLSv1.2    112 Application Data
```

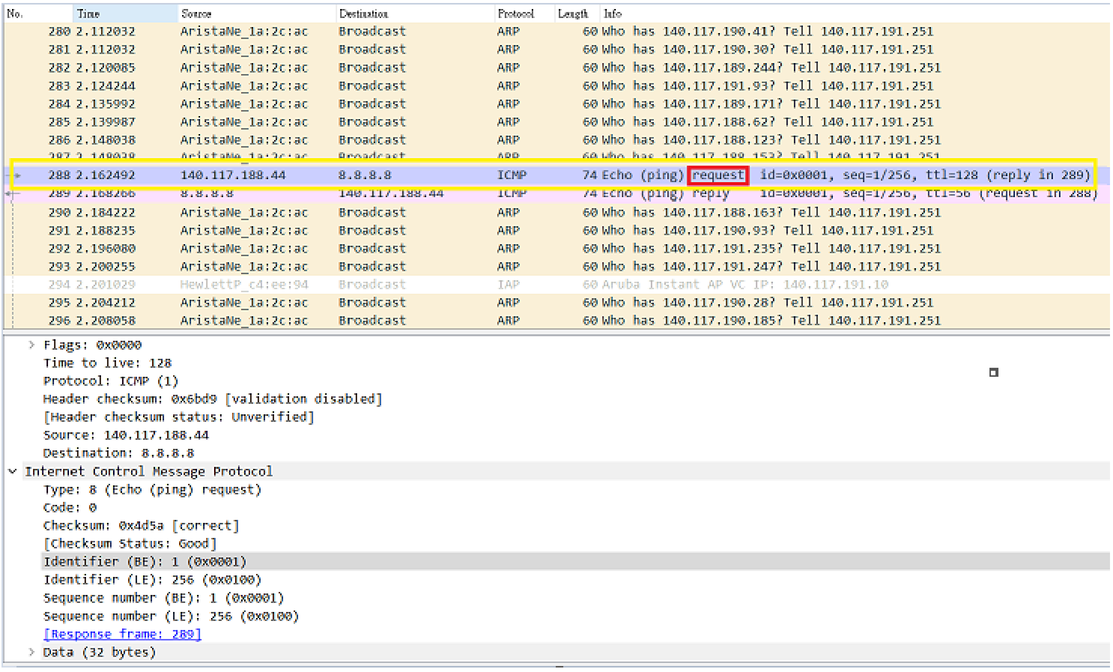
```
    Source: 2001:288:8001:d900:d41a:cc8:e459:c358
    Destination: 2620:1ec:c11::200
v Transmission Control Protocol, Src Port: 56349, Dst Port: 443, Seq: 0, Len: 0
    Source Port: 56349
    Destination Port: 443
    [Stream index: 3]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    [Next sequence number: 0    (relative sequence number)]
    Acknowledgment number: 0
    1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x002 (SYN)
    Window size value: 65535
    [Calculated window size: 65535]
    Checksum: 0x3a64 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  > Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP), SACK permitted
```

Ans : 0x002

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

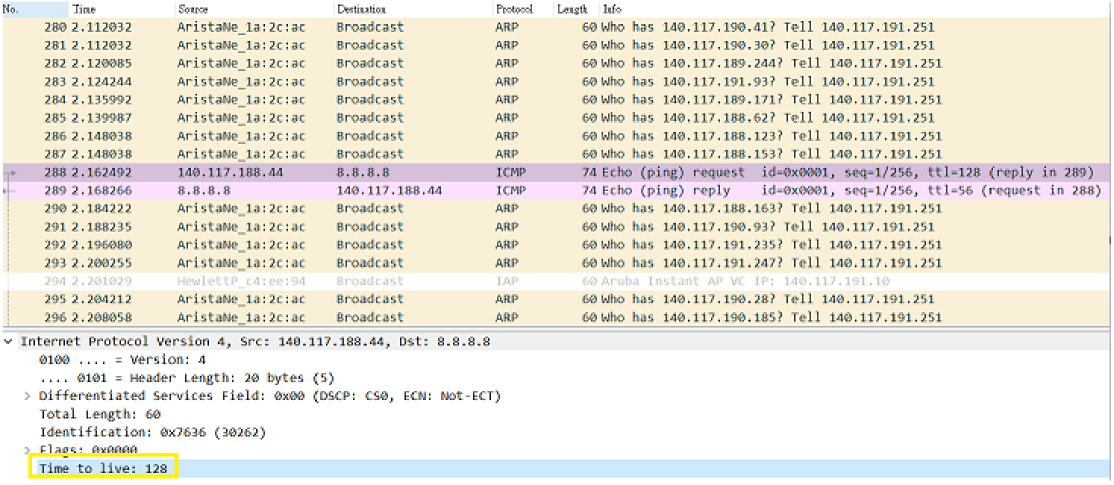
## 1. Ping Captured.

(1) Find the first ICMP Echo Request packet.



```
No.   Time       Source              Destination       Protocol  Length  Info
  280 2.112032   AristaNe_1a:2c:ac   Broadcast         ARP         60 Who has 140.117.190.41? Tell 140.117.191.251
  281 2.112032   AristaNe_1a:2c:ac   Broadcast         ARP         60 Who has 140.117.190.30? Tell 140.117.191.251
  282 2.120085   AristaNe_1a:2c:ac   Broadcast         ARP         60 Who has 140.117.189.244? Tell 140.117.191.251
  283 2.124244   AristaNe_1a:2c:ac   Broadcast         ARP         60 Who has 140.117.191.93? Tell 140.117.191.251
  284 2.135992   AristaNe_1a:2c:ac   Broadcast         ARP         60 Who has 140.117.189.171? Tell 140.117.191.251
  285 2.139987   AristaNe_1a:2c:ac   Broadcast         ARP         60 Who has 140.117.188.62? Tell 140.117.191.251
  286 2.148038   AristaNe_1a:2c:ac   Broadcast         ARP         60 Who has 140.117.188.123? Tell 140.117.191.251
  287 2.148038   AristaNe_1a:2c:ac   Broadcast         ARP         60 Who has 140.117.188.153? Tell 140.117.191.251
  288 2.162492   140.117.188.44      8.8.8.8           ICMP        74 Echo (ping) request  id=0x0001, seq=1/256, ttl=128 (reply in 289)
  289 2.168266   8.8.8.8             140.117.188.44    ICMP        74 Echo (ping) reply    id=0x0001, seq=1/256, ttl=56 (request in 288)
  290 2.184222   AristaNe_1a:2c:ac   Broadcast         ARP         60 Who has 140.117.188.163? Tell 140.117.191.251
  291 2.188235   AristaNe_1a:2c:ac   Broadcast         ARP         60 Who has 140.117.190.93? Tell 140.117.191.251
  292 2.196080   AristaNe_1a:2c:ac   Broadcast         ARP         60 Who has 140.117.191.235? Tell 140.117.191.251
  293 2.200255   AristaNe_1a:2c:ac   Broadcast         ARP         60 Who has 140.117.191.247? Tell 140.117.191.251
  294 2.201029   HewlettP_c4:ee:94   Broadcast         IAP         60 Aruba Instant AP VC IP: 140.117.191.10
  295 2.204212   AristaNe_1a:2c:ac   Broadcast         ARP         60 Who has 140.117.190.28? Tell 140.117.191.251
  296 2.208058   AristaNe_1a:2c:ac   Broadcast         ARP         60 Who has 140.117.190.185? Tell 140.117.191.251

  > Flags: 0x0000
    Time to live: 128
    Protocol: ICMP (1)
    Header checksum: 0x6bd9 [validation disabled]
    [Header checksum status: Unverified]
    Source: 140.117.188.44
    Destination: 8.8.8.8
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4d5a [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 1 (0x0001)
    Sequence number (LE): 256 (0x0100)
    [Response frame: 289]
  > Data (32 bytes)
```

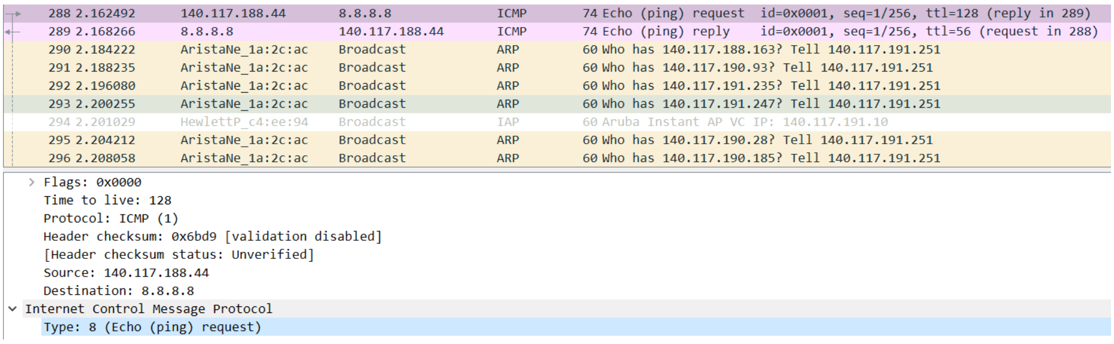
a. First, examine the Internet Protocol. What is the Time-to-Live?



```
No.   Time       Source              Destination       Protocol  Length  Info
  280 2.112032   AristaNe_1a:2c:ac   Broadcast         ARP         60 Who has 140.117.190.41? Tell 140.117.191.251
  281 2.112032   AristaNe_1a:2c:ac   Broadcast         ARP         60 Who has 140.117.190.30? Tell 140.117.191.251
  282 2.120085   AristaNe_1a:2c:ac   Broadcast         ARP         60 Who has 140.117.189.244? Tell 140.117.191.251
  283 2.124244   AristaNe_1a:2c:ac   Broadcast         ARP         60 Who has 140.117.191.93? Tell 140.117.191.251
  284 2.135992   AristaNe_1a:2c:ac   Broadcast         ARP         60 Who has 140.117.189.171? Tell 140.117.191.251
  285 2.139987   AristaNe_1a:2c:ac   Broadcast         ARP         60 Who has 140.117.188.62? Tell 140.117.191.251
  286 2.148038   AristaNe_1a:2c:ac   Broadcast         ARP         60 Who has 140.117.188.123? Tell 140.117.191.251
  287 2.148038   AristaNe_1a:2c:ac   Broadcast         ARP         60 Who has 140.117.188.153? Tell 140.117.191.251
  288 2.162492   140.117.188.44      8.8.8.8           ICMP        74 Echo (ping) request  id=0x0001, seq=1/256, ttl=128 (reply in 289)
  289 2.168266   8.8.8.8             140.117.188.44    ICMP        74 Echo (ping) reply    id=0x0001, seq=1/256, ttl=56 (request in 288)
  290 2.184222   AristaNe_1a:2c:ac   Broadcast         ARP         60 Who has 140.117.188.163? Tell 140.117.191.251
  291 2.188235   AristaNe_1a:2c:ac   Broadcast         ARP         60 Who has 140.117.190.93? Tell 140.117.191.251
  292 2.196080   AristaNe_1a:2c:ac   Broadcast         ARP         60 Who has 140.117.191.235? Tell 140.117.191.251
  293 2.200255   AristaNe_1a:2c:ac   Broadcast         ARP         60 Who has 140.117.191.247? Tell 140.117.191.251
  294 2.201029   HewlettP_c4:ee:94   Broadcast         IAP         60 Aruba Instant AP VC IP: 140.117.191.10
  295 2.204212   AristaNe_1a:2c:ac   Broadcast         ARP         60 Who has 140.117.190.28? Tell 140.117.191.251
  296 2.208058   AristaNe_1a:2c:ac   Broadcast         ARP         60 Who has 140.117.190.185? Tell 140.117.191.251

v Internet Protocol Version 4, Src: 140.117.188.44, 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: 0x7636 (30262)
  > Flags: 0x0000
    Time to live: 128
```

Ans: 128 (sec)

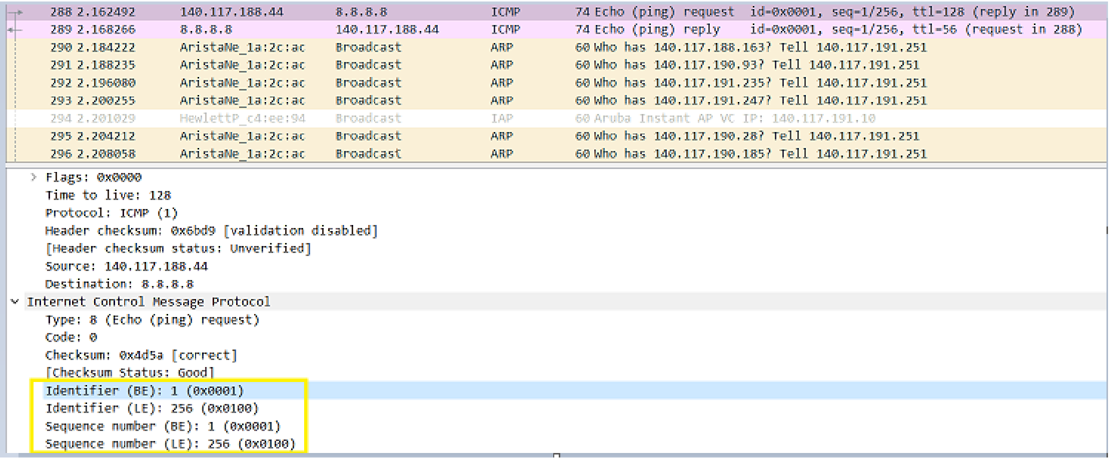
b. Next examine the Internet Control Message Protocol. What is the ICMP message type?



```
288 2.162492   140.117.188.44    8.8.8.8          ICMP   74 Echo (ping) request  id=0x0001, seq=1/256, ttl=128 (reply in 289)
289 2.168266   8.8.8.8           140.117.188.44   ICMP   74 Echo (ping) reply    id=0x0001, seq=1/256, ttl=56 (request in 288)
290 2.184222   AristaNe_1a:2c:ac Broadcast        ARP    60 Who has 140.117.188.163? Tell 140.117.191.251
291 2.188235   AristaNe_1a:2c:ac Broadcast        ARP    60 Who has 140.117.190.93? Tell 140.117.191.251
292 2.196080   AristaNe_1a:2c:ac Broadcast        ARP    60 Who has 140.117.191.235? Tell 140.117.191.251
293 2.200255   AristaNe_1a:2c:ac Broadcast        ARP    60 Who has 140.117.191.247? Tell 140.117.191.251
294 2.201029   HewlettP_c4:ee:94 Broadcast        IAP    60 Aruba Instant AP VC IP: 140.117.191.10
295 2.204212   AristaNe_1a:2c:ac Broadcast        ARP    60 Who has 140.117.190.28? Tell 140.117.191.251
296 2.208058   AristaNe_1a:2c:ac Broadcast        ARP    60 Who has 140.117.190.185? Tell 140.117.191.251

  > Flags: 0x0000
    Time to live: 128
    Protocol: ICMP (1)
    Header checksum: 0x6bd9 [validation disabled]
    [Header checksum status: Unverified]
    Source: 140.117.188.44
    Destination: 8.8.8.8
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
```

Ans:8(Echo (ping) request)

c. What is the message identifier and sequence number?



```
288 2.162492   140.117.188.44    8.8.8.8          ICMP   74 Echo (ping) request  id=0x0001, seq=1/256, ttl=128 (reply in 289)
289 2.168266   8.8.8.8           140.117.188.44   ICMP   74 Echo (ping) reply    id=0x0001, seq=1/256, ttl=56 (request in 288)
290 2.184222   AristaNe_1a:2c:ac Broadcast        ARP    60 Who has 140.117.188.163? Tell 140.117.191.251
291 2.188235   AristaNe_1a:2c:ac Broadcast        ARP    60 Who has 140.117.190.93? Tell 140.117.191.251
292 2.196080   AristaNe_1a:2c:ac Broadcast        ARP    60 Who has 140.117.191.235? Tell 140.117.191.251
293 2.200255   AristaNe_1a:2c:ac Broadcast        ARP    60 Who has 140.117.191.247? Tell 140.117.191.251
294 2.201029   HewlettP_c4:ee:94 Broadcast        IAP    60 Aruba Instant AP VC IP: 140.117.191.10
295 2.204212   AristaNe_1a:2c:ac Broadcast        ARP    60 Who has 140.117.190.28? Tell 140.117.191.251
296 2.208058   AristaNe_1a:2c:ac Broadcast        ARP    60 Who has 140.117.190.185? Tell 140.117.191.251

  > Flags: 0x0000
    Time to live: 128
    Protocol: ICMP (1)
    Header checksum: 0x6bd9 [validation disabled]
    [Header checksum status: Unverified]
    Source: 140.117.188.44
    Destination: 8.8.8.8
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4d5a [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 1 (0x0001)
    Sequence number (LE): 256 (0x0100)
```

Ans:

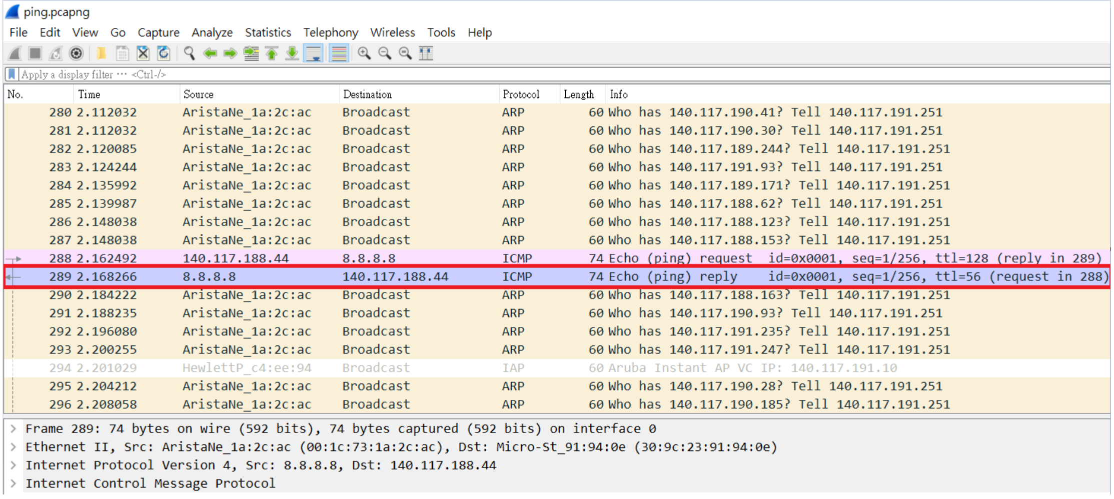
Identifier (BE): 1(0x0001)

Identifier (LE): 256(0x0100)

Sequence number (BE): 1 (0x0001)

Sequence number (LE): 256(0x0100)

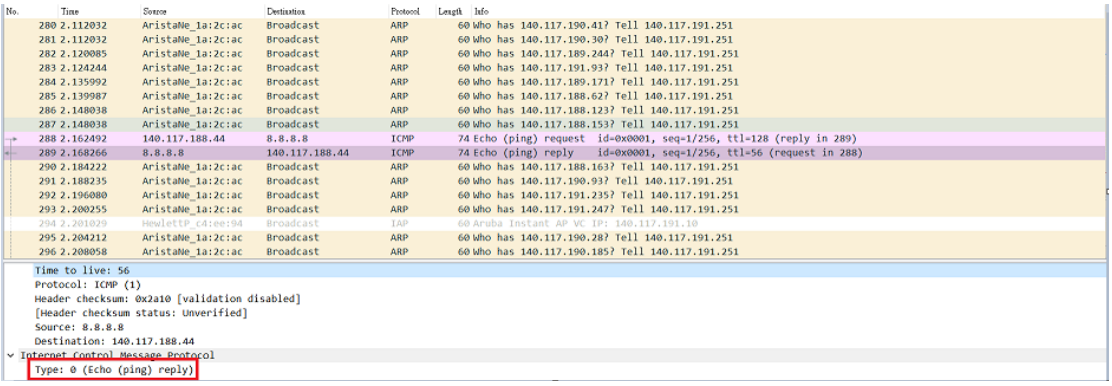
(2) Find the first ICMP Echo Reply packet.



ping.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ··· <Ctrl-/>

```
No.  Time       Source            Destination      Protocol Length Info
280 2.112032   AristaNe_1a:2c:ac Broadcast        ARP    60 Who has 140.117.190.41? Tell 140.117.191.251
281 2.112032   AristaNe_1a:2c:ac Broadcast        ARP    60 Who has 140.117.190.30? Tell 140.117.191.251
282 2.120085   AristaNe_1a:2c:ac Broadcast        ARP    60 Who has 140.117.189.244? Tell 140.117.191.251
283 2.124244   AristaNe_1a:2c:ac Broadcast        ARP    60 Who has 140.117.191.93? Tell 140.117.191.251
284 2.135992   AristaNe_1a:2c:ac Broadcast        ARP    60 Who has 140.117.189.171? Tell 140.117.191.251
285 2.139987   AristaNe_1a:2c:ac Broadcast        ARP    60 Who has 140.117.188.62? Tell 140.117.191.251
286 2.148038   AristaNe_1a:2c:ac Broadcast        ARP    60 Who has 140.117.188.123? Tell 140.117.191.251
287 2.148038   AristaNe_1a:2c:ac Broadcast        ARP    60 Who has 140.117.191.153? Tell 140.117.191.251
288 2.162492   140.117.188.44    8.8.8.8          ICMP   74 Echo (ping) request  id=0x0001, seq=1/256, ttl=128 (reply in 289)
289 2.168266   8.8.8.8           140.117.188.44   ICMP   74 Echo (ping) reply    id=0x0001, seq=1/256, ttl=56 (request in 288)
290 2.184222   AristaNe_1a:2c:ac Broadcast        ARP    60 Who has 140.117.188.163? Tell 140.117.191.251
291 2.188235   AristaNe_1a:2c:ac Broadcast        ARP    60 Who has 140.117.190.93? Tell 140.117.191.251
292 2.196080   AristaNe_1a:2c:ac Broadcast        ARP    60 Who has 140.117.191.235? Tell 140.117.191.251
293 2.200255   AristaNe_1a:2c:ac Broadcast        ARP    60 Who has 140.117.191.247? Tell 140.117.191.251
294 2.201029   HewlettP_c4:ee:94 Broadcast        IAP    60 Aruba Instant AP VC IP: 140.117.191.10
295 2.204212   AristaNe_1a:2c:ac Broadcast        ARP    60 Who has 140.117.190.28? Tell 140.117.191.251
296 2.208058   AristaNe_1a:2c:ac Broadcast        ARP    60 Who has 140.117.190.185? Tell 140.117.191.251

> Frame 289: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
> Ethernet II, Src: AristaNe_1a:2c:ac (00:1c:73:1a:2c:ac), Dst: Micro-St_91:94:0e (30:9c:23:91:94:0e)
> Internet Protocol Version 4, Src: 8.8.8.8, Dst: 140.117.188.44
> Internet Control Message Protocol
```

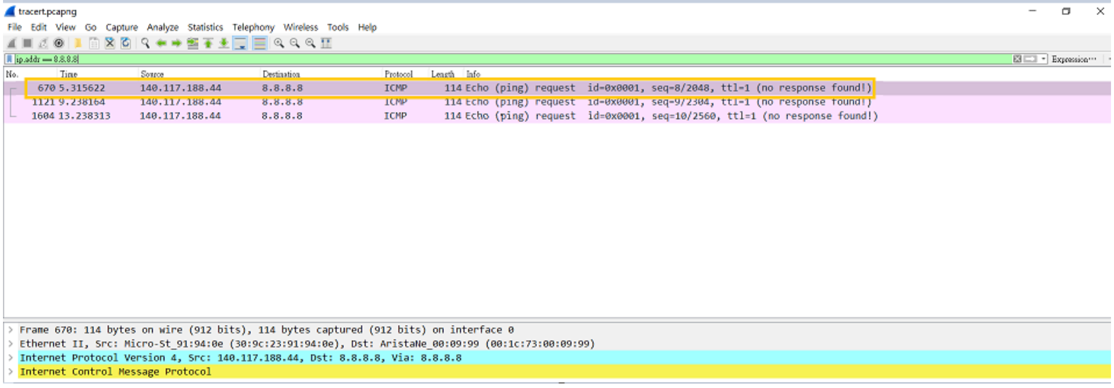
a. Now examine the Internet Control Message Protocol. What is the ICMP message type?



```
No.     Time       Source              Destination      Protocol Length Info
    280 2.112032   AristaNe_1a:2c:ac   Broadcast        ARP      60 Who has 140.117.190.41? Tell 140.117.191.251
    281 2.112032   AristaNe_1a:2c:ac   Broadcast        ARP      60 Who has 140.117.190.30? Tell 140.117.191.251
    282 2.120085   AristaNe_1a:2c:ac   Broadcast        ARP      60 Who has 140.117.189.244? Tell 140.117.191.251
    283 2.124244   AristaNe_1a:2c:ac   Broadcast        ARP      60 Who has 140.117.191.93? Tell 140.117.191.251
    284 2.135992   AristaNe_1a:2c:ac   Broadcast        ARP      60 Who has 140.117.189.171? Tell 140.117.191.251
    285 2.139987   AristaNe_1a:2c:ac   Broadcast        ARP      60 Who has 140.117.188.62? Tell 140.117.191.251
    286 2.148038   AristaNe_1a:2c:ac   Broadcast        ARP      60 Who has 140.117.188.123? Tell 140.117.191.251
    287 2.148038   AristaNe_1a:2c:ac   Broadcast        ARP      60 Who has 140.117.188.153? Tell 140.117.191.251
    288 2.162492   140.117.188.44      8.8.8.8          ICMP     74 Echo (ping) request  id=0x0001, seq=1/256, ttl=128 (reply in 289)
    289 2.168266   8.8.8.8             140.117.188.44   ICMP     74 Echo (ping) reply    id=0x0001, seq=1/256, ttl=56 (request in 288)
    290 2.184222   AristaNe_1a:2c:ac   Broadcast        ARP      60 Who has 140.117.188.163? Tell 140.117.191.251
    291 2.188235   AristaNe_1a:2c:ac   Broadcast        ARP      60 Who has 140.117.190.93? Tell 140.117.191.251
    292 2.196080   AristaNe_1a:2c:ac   Broadcast        ARP      60 Who has 140.117.191.235? Tell 140.117.191.251
    293 2.200255   AristaNe_1a:2c:ac   Broadcast        ARP      60 Who has 140.117.191.247? Tell 140.117.191.251
    294 2.201029   HewlettP_c4:ee:94   Broadcast        IAP      60 Aruba Instant AP VC IP: 140.117.191.10
    295 2.204212   AristaNe_1a:2c:ac   Broadcast        ARP      60 Who has 140.117.190.28? Tell 140.117.191.251
    296 2.208058   AristaNe_1a:2c:ac   Broadcast        ARP      60 Who has 140.117.190.185? Tell 140.117.191.251

    Time to live: 56
    Protocol: ICMP (1)
    Header checksum: 0x2a10 [validation disabled]
    [Header checksum status: Unverified]
    Source: 8.8.8.8
    Destination: 140.117.188.44
v Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
```

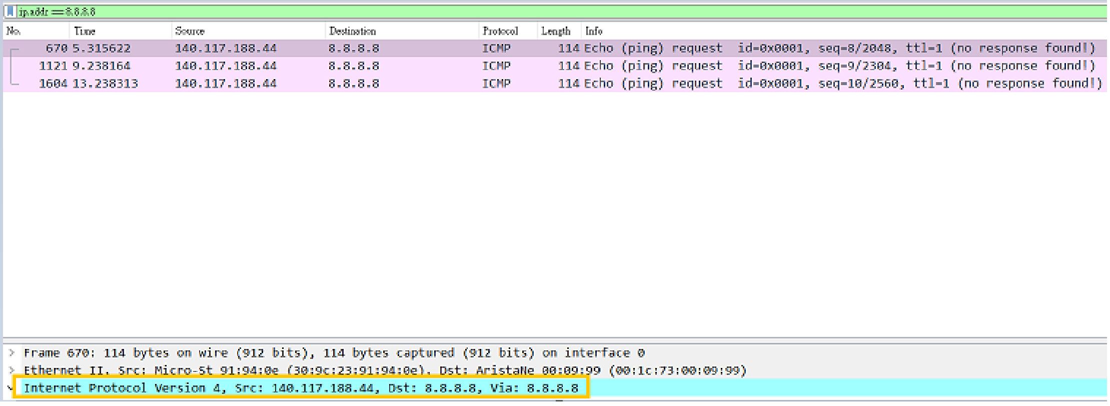
## 2. Traceroute Captured.

(1) Find the first ICMP Echo Request packet.


tracert.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression…

```
ip.addr == 8.8.8.8

No.     Time        Source           Destination  Protocol Length Info
    670 5.315622    140.117.188.44   8.8.8.8      ICMP     114 Echo (ping) request  id=0x0001, seq=8/2048, ttl=1 (no response found!)
   1121 9.238164    140.117.188.44   8.8.8.8      ICMP     114 Echo (ping) request  id=0x0001, seq=9/2304, ttl=1 (no response found!)
   1604 13.238313   140.117.188.44   8.8.8.8      ICMP     114 Echo (ping) request  id=0x0001, seq=10/2560, ttl=1 (no response found!)

> Frame 670: 114 bytes on wire (912 bits), 114 bytes captured (912 bits) on interface 0
> Ethernet II, Src: Micro-St_91:94:0e (30:9c:23:91:94:0e), Dst: AristaNe_00:09:99 (00:1c:73:00:09:99)
> Internet Protocol Version 4, Src: 140.117.188.44, Dst: 8.8.8.8, Via: 8.8.8.8
> Internet Control Message Protocol
```

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

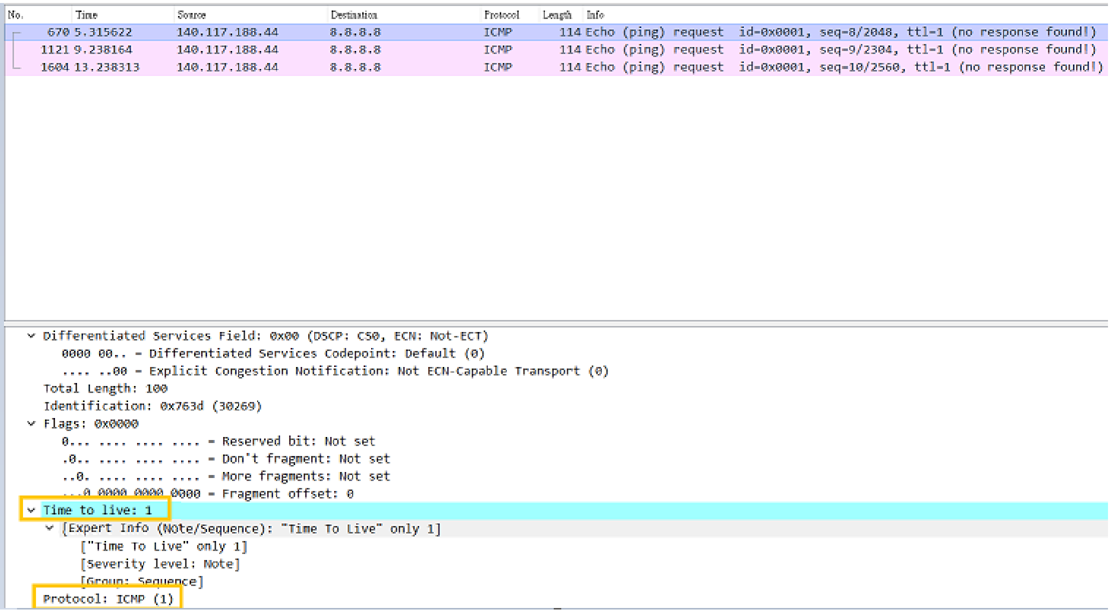


```
ip.addr == 8.8.8.8

No.     Time        Source           Destination  Protocol Length Info
    670 5.315622    140.117.188.44   8.8.8.8      ICMP     114 Echo (ping) request  id=0x0001, seq=8/2048, ttl=1 (no response found!)
   1121 9.238164    140.117.188.44   8.8.8.8      ICMP     114 Echo (ping) request  id=0x0001, seq=9/2304, ttl=1 (no response found!)
   1604 13.238313   140.117.188.44   8.8.8.8      ICMP     114 Echo (ping) request  id=0x0001, seq=10/2560, ttl=1 (no response found!)

> Frame 670: 114 bytes on wire (912 bits), 114 bytes captured (912 bits) on interface 0
> Ethernet II, Src: Micro-St_91:94:0e (30:9c:23:91:94:0e), Dst: AristaNe_00:09:99 (00:1c:73:00:09:99)
v Internet Protocol Version 4, Src: 140.117.188.44, Dst: 8.8.8.8, Via: 8.8.8.8
```

Source : 140.117.188.44

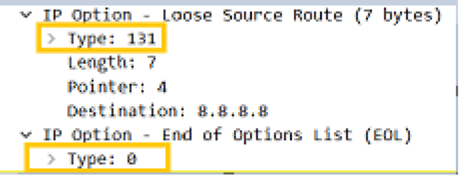
Destination : 8.8.8.8

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



```
No.     Time        Source           Destination  Protocol  Length  Info
  670   5.315622    140.117.188.44   8.8.8.8      ICMP      114 Echo (ping) request  id=0x0001, seq=8/2048, ttl=1 (no response found!)
 1121   9.238164    140.117.188.44   8.8.8.8      ICMP      114 Echo (ping) request  id=0x0001, seq=9/2304, ttl=1 (no response found!)
 1604   13.238313   140.117.188.44   8.8.8.8      ICMP      114 Echo (ping) request  id=0x0001, seq=10/2560, ttl=1 (no response found!)
```

```
v Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    0000 00.. = Differentiated Services Codepoint: Default (0)
    .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 100
  Identification: 0x763d (30269)
v Flags: 0x0000
    0... .... .... .... = Reserved bit: Not set
    .0.. .... .... .... = Don't fragment: Not set
    ..0. .... .... .... = More fragments: Not set
    ...0 0000 0000 0000 = Fragment offset: 0
v Time to live: 1
  v [Expert Info (Note/Sequence): "Time To Live" only 1]
      ["Time To Live" only 1]
      [Severity level: Note]
      [Group: Sequence]
  Protocol: ICMP (1)
```

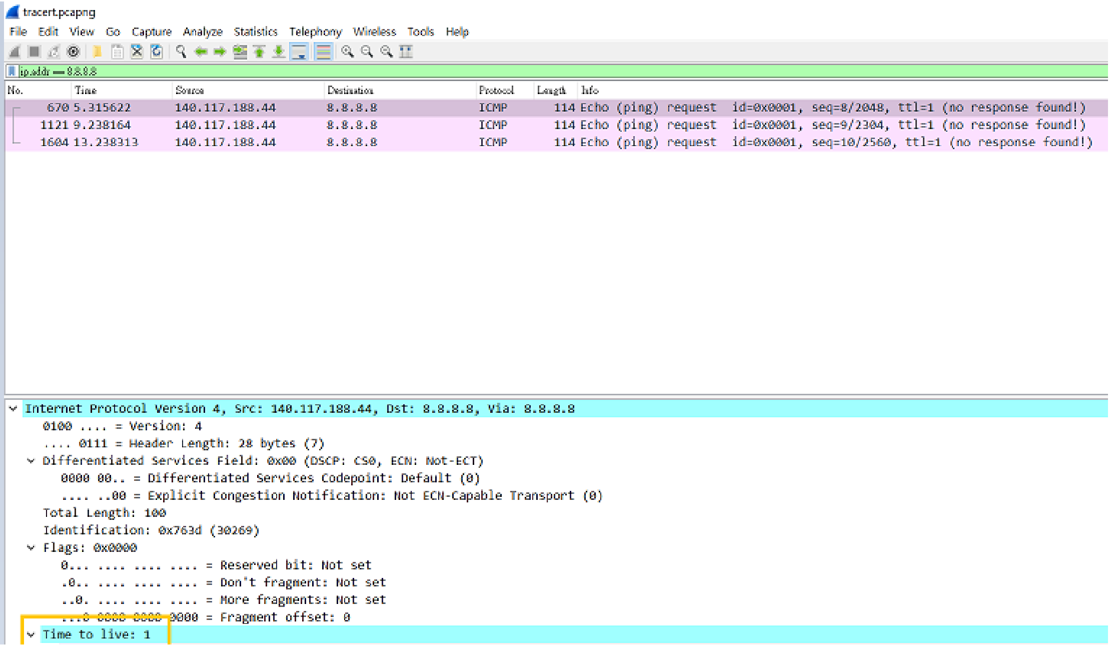


```
v IP Option - Loose Source Route (7 bytes)
  > Type: 131
    Length: 7
    Pointer: 4
    Destination: 8.8.8.8
v IP Option - End of Options List (EOL)
  > Type: 0
```

protocol type:

Loose Source Route → 131

End of Options List → 0


tracert.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

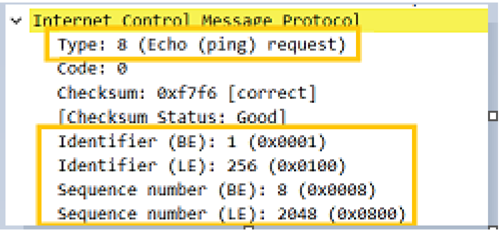
```
ip.addr == 8.8.8.8
```

```
No.     Time        Source           Destination  Protocol  Length  Info
  670   5.315622    140.117.188.44   8.8.8.8      ICMP      114 Echo (ping) request  id=0x0001, seq=8/2048, ttl=1 (no response found!)
 1121   9.238164    140.117.188.44   8.8.8.8      ICMP      114 Echo (ping) request  id=0x0001, seq=9/2304, ttl=1 (no response found!)
 1604   13.238313   140.117.188.44   8.8.8.8      ICMP      114 Echo (ping) request  id=0x0001, seq=10/2560, ttl=1 (no response found!)
```

```
v Internet Protocol Version 4, Src: 140.117.188.44, Dst: 8.8.8.8, Via: 8.8.8.8
    0100 .... = Version: 4
    .... 0111 = Header Length: 28 bytes (7)
  v Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 100
    Identification: 0x763d (30269)
  v Flags: 0x0000
      0... .... .... .... = Reserved bit: Not set
      .0.. .... .... .... = Don't fragment: Not set
      ..0. .... .... .... = More fragments: Not set
      ...0 0000 0000 0000 = Fragment offset: 0
  v Time to live: 1
```

Time-to-Live: 1 (sec)

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: 0xf7f6 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 8 (0x0008)
    Sequence number (LE): 2048 (0x0800)
```

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

message identifier:

(BE) : 1 (0x0001)

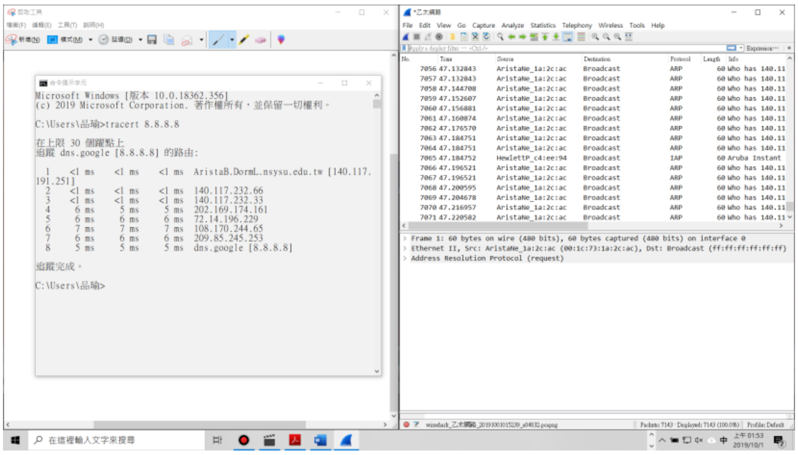
(LE) : 256 (0x0100)

sequence number:

(BE) : 8 (0x0008)

(LE) : 2048 (0x0800)

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



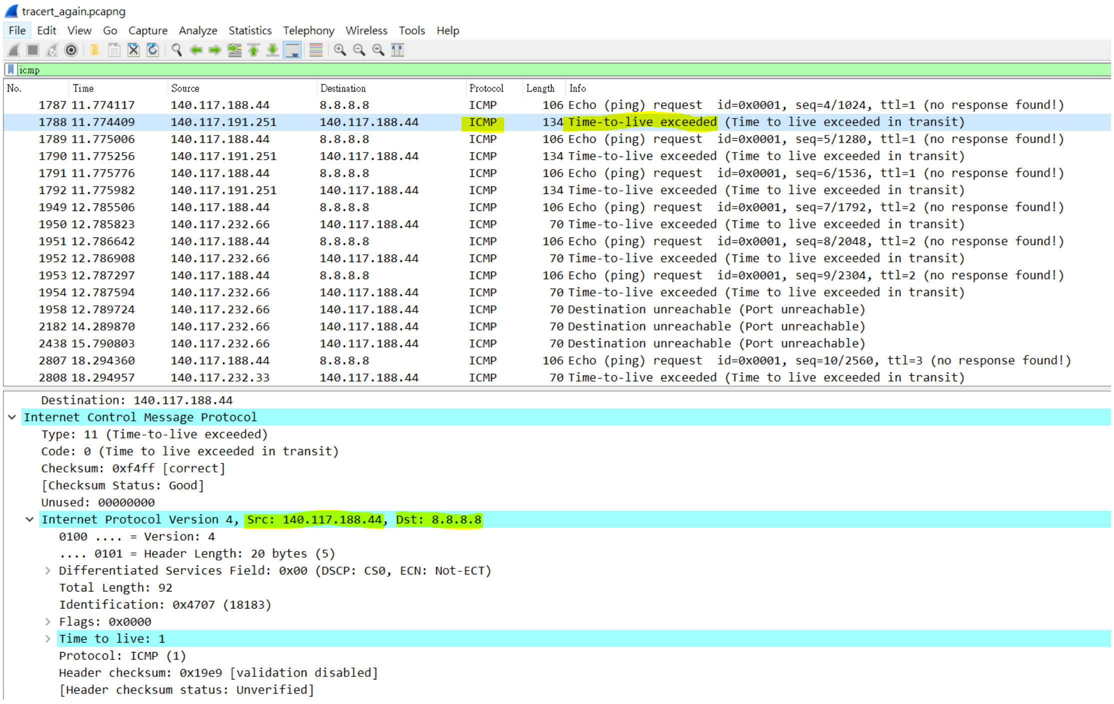
```
Microsoft Windows [版本 10.0.18362.356]
(c) 2019 Microsoft Corporation. 著作權所有，並保留一切權利。

C:\Users\品瑜>tracert 8.8.8.8

在上限 30 個躍點上
追蹤 dns.google [8.8.8.8] 的路由:

  1    <1 ms    <1 ms    <1 ms  AristaB.DormL.nsysu.edu.tw [140.117.
191.251]
  2    <1 ms    <1 ms    <1 ms  140.117.232.66
  3    <1 ms    <1 ms    <1 ms  140.117.232.33
  4     6 ms     5 ms     5 ms  202.169.174.161
  5     6 ms     6 ms     6 ms  72.14.196.229
  6     7 ms     7 ms     7 ms  108.170.244.65
  7     6 ms     6 ms     6 ms  209.85.245.253
  8     5 ms     5 ms     5 ms  dns.google [8.8.8.8]

追蹤完成。

C:\Users\品瑜>
```

```
No.   Time       Source                Destination  Protocol  Length  Info
7056  47.132843  AristaNe_1a:2c:ac     Broadcast    ARP       60 Who has 140.11
7057  47.132843  AristaNe_1a:2c:ac     Broadcast    ARP       60 Who has 140.11
7058  47.144708  AristaNe_1a:2c:ac     Broadcast    ARP       60 Who has 140.11
7059  47.152607  AristaNe_1a:2c:ac     Broadcast    ARP       60 Who has 140.11
7060  47.156881  AristaNe_1a:2c:ac     Broadcast    ARP       60 Who has 140.11
7061  47.160874  AristaNe_1a:2c:ac     Broadcast    ARP       60 Who has 140.11
7062  47.176570  AristaNe_1a:2c:ac     Broadcast    ARP       60 Who has 140.11
7063  47.184751  AristaNe_1a:2c:ac     Broadcast    ARP       60 Who has 140.11
7064  47.184751  AristaNe_1a:2c:ac     Broadcast    ARP       60 Who has 140.11
7065  47.184752  HewlettP_c4:ee:94     Broadcast    IAP       60 Aruba Instant
7066  47.196521  AristaNe_1a:2c:ac     Broadcast    ARP       60 Who has 140.11
7067  47.196521  AristaNe_1a:2c:ac     Broadcast    ARP       60 Who has 140.11
7068  47.200595  AristaNe_1a:2c:ac     Broadcast    ARP       60 Who has 140.11
7069  47.204678  AristaNe_1a:2c:ac     Broadcast    ARP       60 Who has 140.11
7070  47.216957  AristaNe_1a:2c:ac     Broadcast    ARP       60 Who has 140.11
7071  47.220582  AristaNe_1a:2c:ac     Broadcast    ARP       60 Who has 140.11

> Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
> Ethernet II, Src: AristaNe_1a:2c:ac (00:1c:73:1a:2c:ac), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Address Resolution Protocol (request)
```

*乙太網路
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Expression…

ICMP Time-to-live exceeded packet ‘s TTL is equal to 0.

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


tracert_again.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp

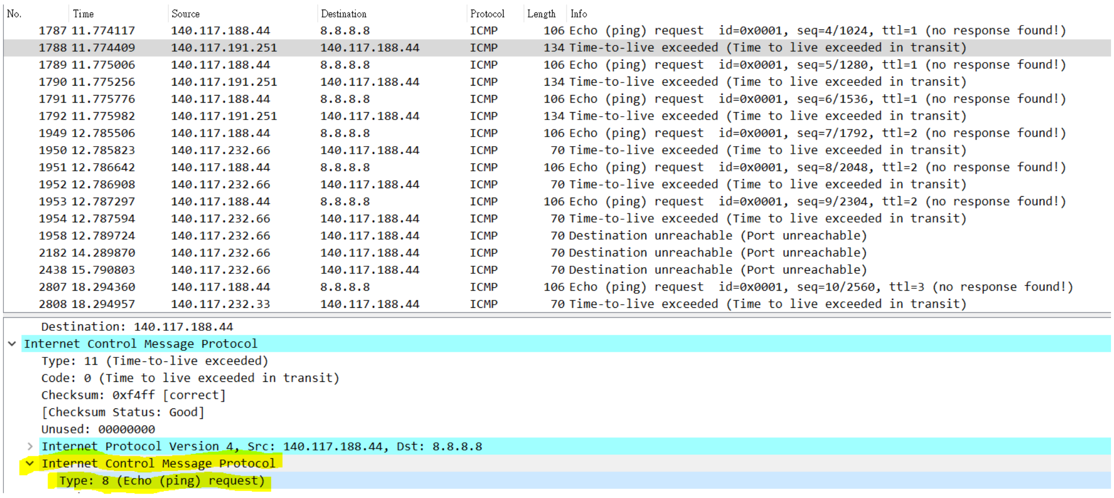
```
No.       Time        Source              Destination         Protocol  Length  Info
     1787 11.774117   140.117.188.44      8.8.8.8             ICMP      106 Echo (ping) request  id=0x0001, seq=4/1024, ttl=1 (no response found!)
     1788 11.774409   140.117.191.251     140.117.188.44      ICMP      134 Time-to-live exceeded (Time to live exceeded in transit)
     1789 11.775006   140.117.188.44      8.8.8.8             ICMP      106 Echo (ping) request  id=0x0001, seq=5/1280, ttl=1 (no response found!)
     1790 11.775256   140.117.191.251     140.117.188.44      ICMP      134 Time-to-live exceeded (Time to live exceeded in transit)
     1791 11.775776   140.117.188.44      8.8.8.8             ICMP      106 Echo (ping) request  id=0x0001, seq=6/1536, ttl=1 (no response found!)
     1792 11.775982   140.117.191.251     140.117.188.44      ICMP      134 Time-to-live exceeded (Time to live exceeded in transit)
     1949 12.785506   140.117.188.44      8.8.8.8             ICMP      106 Echo (ping) request  id=0x0001, seq=7/1792, ttl=2 (no response found!)
     1950 12.785823   140.117.232.66      140.117.188.44      ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
     1951 12.786642   140.117.188.44      8.8.8.8             ICMP      106 Echo (ping) request  id=0x0001, seq=8/2048, ttl=2 (no response found!)
     1952 12.786908   140.117.232.66      140.117.188.44      ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
     1953 12.787297   140.117.188.44      8.8.8.8             ICMP      106 Echo (ping) request  id=0x0001, seq=9/2304, ttl=2 (no response found!)
     1954 12.787594   140.117.232.66      140.117.188.44      ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
     1958 12.789724   140.117.232.66      140.117.188.44      ICMP       70 Destination unreachable (Port unreachable)
     2182 14.289870   140.117.232.66      140.117.188.44      ICMP       70 Destination unreachable (Port unreachable)
     2438 15.790803   140.117.232.66      140.117.188.44      ICMP       70 Destination unreachable (Port unreachable)
     2807 18.294360   140.117.188.44      8.8.8.8             ICMP      106 Echo (ping) request  id=0x0001, seq=10/2560, ttl=3 (no response found!)
     2808 18.294957   140.117.232.33      140.117.188.44      ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
```

```
    Destination: 140.117.188.44
v Internet Control Message Protocol
    Type: 11 (Time-to-live exceeded)
    Code: 0 (Time to live exceeded in transit)
    Checksum: 0xf4ff [correct]
    [Checksum Status: Good]
    Unused: 00000000
  v Internet Protocol Version 4, Src: 140.117.188.44, 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: 0x4707 (18183)
    > Flags: 0x0000
    > Time to live: 1
      Protocol: ICMP (1)
      Header checksum: 0x19e9 [validation disabled]
      [Header checksum status: Unverified]
```

Src : 140.117.188.44

Dst : 8.8.8.8

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



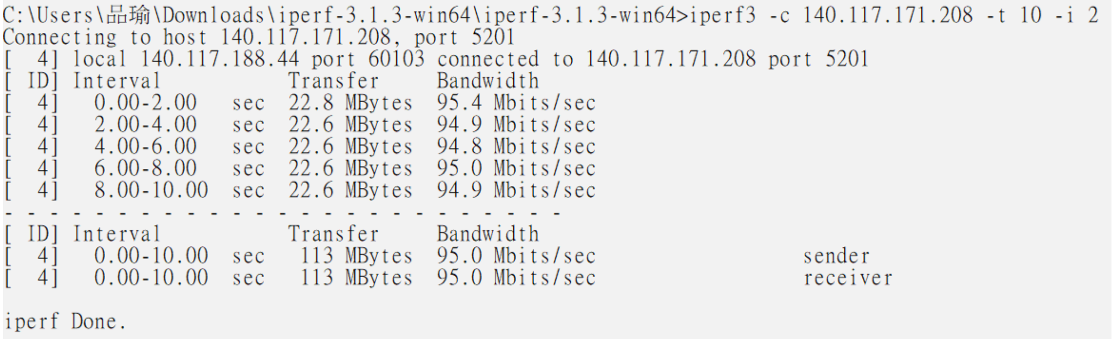
```
No.       Time        Source              Destination         Protocol  Length  Info
     1787 11.774117   140.117.188.44      8.8.8.8             ICMP      106 Echo (ping) request  id=0x0001, seq=4/1024, ttl=1 (no response found!)
     1788 11.774409   140.117.191.251     140.117.188.44      ICMP      134 Time-to-live exceeded (Time to live exceeded in transit)
     1789 11.775006   140.117.188.44      8.8.8.8             ICMP      106 Echo (ping) request  id=0x0001, seq=5/1280, ttl=1 (no response found!)
     1790 11.775256   140.117.191.251     140.117.188.44      ICMP      134 Time-to-live exceeded (Time to live exceeded in transit)
     1791 11.775776   140.117.188.44      8.8.8.8             ICMP      106 Echo (ping) request  id=0x0001, seq=6/1536, ttl=1 (no response found!)
     1792 11.775982   140.117.191.251     140.117.188.44      ICMP      134 Time-to-live exceeded (Time to live exceeded in transit)
     1949 12.785506   140.117.188.44      8.8.8.8             ICMP      106 Echo (ping) request  id=0x0001, seq=7/1792, ttl=2 (no response found!)
     1950 12.785823   140.117.232.66      140.117.188.44      ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
     1951 12.786642   140.117.188.44      8.8.8.8             ICMP      106 Echo (ping) request  id=0x0001, seq=8/2048, ttl=2 (no response found!)
     1952 12.786908   140.117.232.66      140.117.188.44      ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
     1953 12.787297   140.117.188.44      8.8.8.8             ICMP      106 Echo (ping) request  id=0x0001, seq=9/2304, ttl=2 (no response found!)
     1954 12.787594   140.117.232.66      140.117.188.44      ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
     1958 12.789724   140.117.232.66      140.117.188.44      ICMP       70 Destination unreachable (Port unreachable)
     2182 14.289870   140.117.232.66      140.117.188.44      ICMP       70 Destination unreachable (Port unreachable)
     2438 15.790803   140.117.232.66      140.117.188.44      ICMP       70 Destination unreachable (Port unreachable)
     2807 18.294360   140.117.188.44      8.8.8.8             ICMP      106 Echo (ping) request  id=0x0001, seq=10/2560, ttl=3 (no response found!)
     2808 18.294957   140.117.232.33      140.117.188.44      ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
```

```
    Destination: 140.117.188.44
v Internet Control Message Protocol
    Type: 11 (Time-to-live exceeded)
    Code: 0 (Time to live exceeded in transit)
    Checksum: 0xf4ff [correct]
    [Checksum Status: Good]
    Unused: 00000000
  > Internet Protocol Version 4, Src: 140.117.188.44, Dst: 8.8.8.8
  v Internet Control Message Protocol
      Type: 8 (Echo (ping) request)
```

Type : 8 (Echo (ping) request)

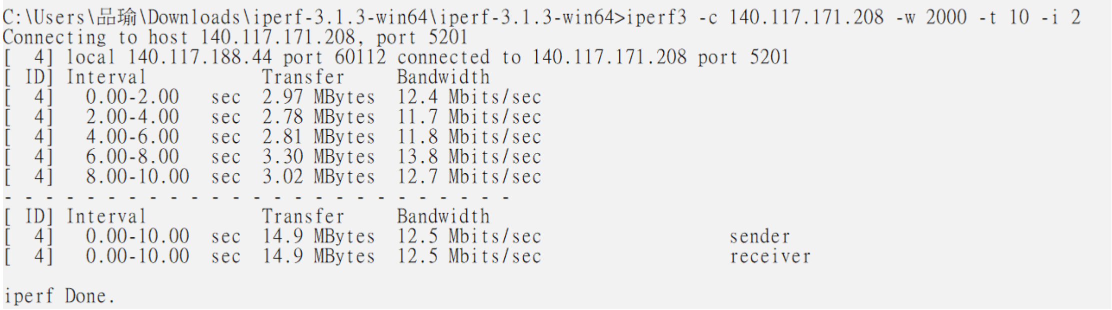
## Part 3 Measuring Network Bandwidth

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



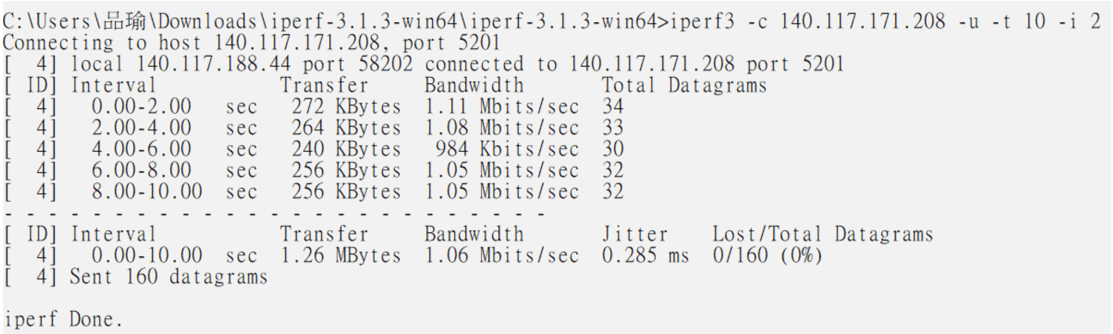
```
C:\Users\品瑜\Downloads\iperf-3.1.3-win64\iperf-3.1.3-win64>iperf3 -c 140.117.171.208 -t 10 -i 2
Connecting to host 140.117.171.208, port 5201
[  4] local 140.117.188.44 port 60103 connected to 140.117.171.208 port 5201
[ ID] Interval           Transfer     Bandwidth
[  4]   0.00-2.00   sec  22.8 MBytes  95.4 Mbits/sec
[  4]   2.00-4.00   sec  22.6 MBytes  94.9 Mbits/sec
[  4]   4.00-6.00   sec  22.6 MBytes  94.8 Mbits/sec
[  4]   6.00-8.00   sec  22.6 MBytes  95.0 Mbits/sec
[  4]   8.00-10.00  sec  22.6 MBytes  94.9 Mbits/sec
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bandwidth
[  4]   0.00-10.00  sec   113 MBytes  95.0 Mbits/sec                  sender
[  4]   0.00-10.00  sec   113 MBytes  95.0 Mbits/sec                  receiver

iperf Done.
```

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”



```
C:\Users\品瑜\Downloads\iperf-3.1.3-win64\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 140.117.188.44 port 60112 connected to 140.117.171.208 port 5201
[ ID] Interval           Transfer     Bandwidth
[  4]   0.00-2.00   sec  2.97 MBytes  12.4 Mbits/sec
[  4]   2.00-4.00   sec  2.78 MBytes  11.7 Mbits/sec
[  4]   4.00-6.00   sec  2.81 MBytes  11.8 Mbits/sec
[  4]   6.00-8.00   sec  3.30 MBytes  13.8 Mbits/sec
[  4]   8.00-10.00  sec  3.02 MBytes  12.7 Mbits/sec
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bandwidth
[  4]   0.00-10.00  sec  14.9 MBytes  12.5 Mbits/sec                  sender
[  4]   0.00-10.00  sec  14.9 MBytes  12.5 Mbits/sec                  receiver

iperf Done.
```

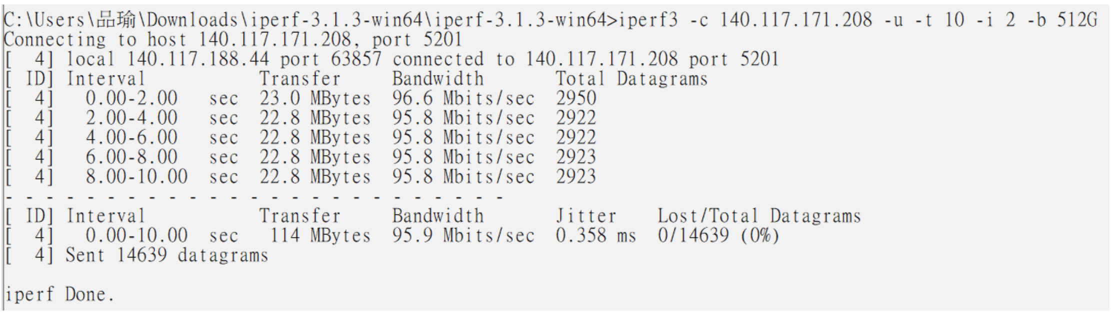
3. Measure the bandwidth for User Datagram Protocol Type “iperf3 -c 140.117.171.208 -u -t 10 -i 2”



```
C:\Users\品瑜\Downloads\iperf-3.1.3-win64\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 140.117.188.44 port 58202 connected to 140.117.171.208 port 5201
[ ID] Interval           Transfer     Bandwidth       Total Datagrams
[  4]   0.00-2.00   sec   272 KBytes  1.11 Mbits/sec  34
[  4]   2.00-4.00   sec   264 KBytes  1.08 Mbits/sec  33
[  4]   4.00-6.00   sec   240 KBytes   984 Kbits/sec  30
[  4]   6.00-8.00   sec   256 KBytes  1.05 Mbits/sec  32
[  4]   8.00-10.00  sec   256 KBytes  1.05 Mbits/sec  32
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bandwidth       Jitter    Lost/Total Datagrams
[  4]   0.00-10.00  sec  1.26 MBytes  1.06 Mbits/sec  0.285 ms  0/160 (0%)
[  4] Sent 160 datagrams

iperf Done.
```

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”



```
C:\Users\品瑜\Downloads\iperf-3.1.3-win64\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 140.117.188.44 port 63857 connected to 140.117.171.208 port 5201
[ ID] Interval           Transfer     Bandwidth       Total Datagrams
[  4]   0.00-2.00   sec  23.0 MBytes  96.6 Mbits/sec  2950
[  4]   2.00-4.00   sec  22.8 MBytes  95.8 Mbits/sec  2922
[  4]   4.00-6.00   sec  22.8 MBytes  95.8 Mbits/sec  2922
[  4]   6.00-8.00   sec  22.8 MBytes  95.8 Mbits/sec  2923
[  4]   8.00-10.00  sec  22.8 MBytes  95.8 Mbits/sec  2923
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bandwidth       Jitter    Lost/Total Datagrams
[  4]   0.00-10.00  sec   114 MBytes  95.9 Mbits/sec  0.358 ms  0/14639 (0%)
[  4] Sent 14639 datagrams

iperf Done.
```