

ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC BÁCH KHOA
KHOA KHOA HỌC VÀ KỸ THUẬT MÁY TÍNH



MẠNG MÁY TÍNH THỰC HÀNH - CO3094

Báo cáo:

Lab4a

Giảng viên hướng dẫn: Vũ Thành Tài

Sinh viên: Lê Đức Cường

Thành phố Hồ Chí Minh, tháng 3 năm 2025



1 Question 1

Select the first ICMP Echo Request message sent by your computer, and expand the Internet Protocol part of the packet in the packet details window.

What is the IP address of your computer?

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.230.19.125	128.119.245.12	ICMP	70	Echo (ping) request id=0x0001, seq=2124/19464, ttl=7 (no response found!)
2	0.062552	10.230.19.125	128.119.245.12	ICMP	70	Echo (ping) request id=0x0001, seq=2125/19720, ttl=8 (no response found!)
3	0.086936	113.171.45.30	10.230.19.125	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit)
4	0.086936	113.171.31.33	10.230.19.125	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
5	0.125337	10.230.19.125	128.119.245.12	ICMP	70	Echo (ping) request id=0x0001, seq=2126/19976, ttl=9 (no response found!)
6	0.188010	10.230.19.125	128.119.245.12	ICMP	70	Echo (ping) request id=0x0001, seq=2127/20232, ttl=10 (no response found!)
7	0.250541	10.230.19.125	128.119.245.12	ICMP	70	Echo (ping) request id=0x0001, seq=2128/20488, ttl=11 (no response found!)
8	0.312976	10.230.19.125	128.119.245.12	ICMP	70	Echo (ping) request id=0x0001, seq=2129/20744, ttl=12 (no response found!)
9	0.370899	63.218.212.5	10.230.19.125	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
10	0.376382	10.230.19.125	128.119.245.12	ICMP	70	Echo (ping) request id=0x0001, seq=2130/21000, ttl=13 (no response found!)
11	0.396429	154.54.25.149	10.230.19.125	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
12	0.439745	10.230.19.125	128.119.245.12	ICMP	70	Echo (ping) request id=0x0001, seq=2131/21256, ttl=14 (no response found!)
13	0.447543	154.54.45.161	10.230.19.125	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
14	0.502616	10.230.19.125	128.119.245.12	ICMP	70	Echo (ping) request id=0x0001, seq=2132/21512, ttl=15 (no response found!)
15	0.527057	154.54.166.69	10.230.19.125	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
16	0.566577	10.230.19.125	128.119.245.12	ICMP	70	Echo (ping) request id=0x0001, seq=2133/21768, ttl=16 (no response found!)
17	0.605221	154.54.165.29	10.230.19.125	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)

Ans: The IP address of my computer is 10.230.19.125

2 Question 2

Within the IP packet header, what is the value in the upper layer protocol field?

Ans: The value of the upper layer protocol field is ICMP (1)

```
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 168
    Identification: 0x0000 (0)
  010. .... = Flags: 0x2, Don't fragment
...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 249
    Protocol: ICMP (1)
    Header Checksum: 0xc428 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 113.171.45.30
    Destination Address: 10.230.19.125
    [Stream index: 1]
```

3 Question 3

How many bytes are in the IP header? How many bytes are in the payload of the IP datagram? Explain how you determined the number of payload bytes.



```
▼ Internet Protocol Version 4, Src: 113.171.31.33, Dst: 10.230.19.125
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 56
    Identification: 0xe10f (57615)
  ▶ 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 247
    Protocol: ICMP (1)
    Header Checksum: 0xf385 [validation disabled]
    [Header checksum status: Unverified]
```

Ans: Header length: 20 bytes

Payload = Total Length: 56 – header length:20 = 36 bytes.

4 Question 4

Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented.

Ans: This IP datagram has not been fragmented. I know this because the more fragments bit has not been set.

5 Question 5

Which fields in the IP datagram always change from one datagram to the next within this series of ICMP messages sent by your computer?

Ans: The checksum always changes and so does the sequence number.

6 Question 6

Which fields stay constant? Which of the fields must stay constant? Which fields must change? Why?

Ans: Header length and time to live stay constant because these are preset. The fragment number, sequence number, flags, total length and checksum vary from each segment so they change.

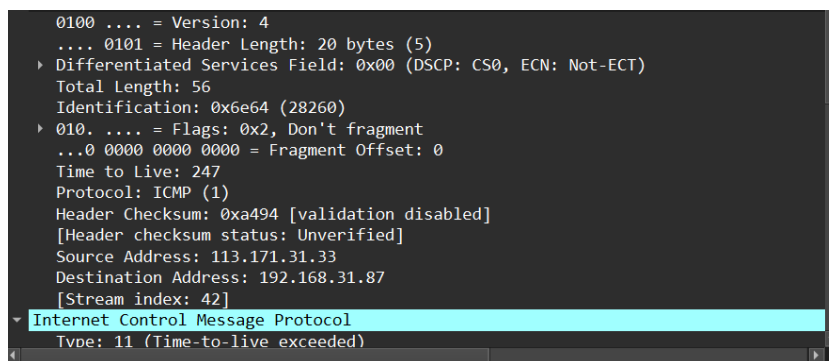
7 Question 7

What is the value in the Identification field and the TTL field?

Ans: The value of the identification field is incremented by 1 on every new outgoing message.

8 Question 8

What is the value in the Identification field and the TTL field?



```
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 56
    Identification: 0x6e64 (28260)
  ▸ 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 247
    Protocol: ICMP (1)
    Header Checksum: 0xa494 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 113.171.31.33
    Destination Address: 192.168.31.87
    [Stream index: 42]
  ▾ Internet Control Message Protocol
    Type: 11 (Time-to-live exceeded)
```

Ans: Identification: 0x6e64 (28260)

Time to live: 247

9 Question 9

Do these values remain unchanged for all of the ICMP TTL-exceeded replies sent to your computer by the nearest (first hop) router? Why?

Ans: The Identification field in ICMP TTL-exceeded reply packets changes because it needs to be unique to distinguish different packets during transmission. Meanwhile, the Time to Live (TTL) value remains the same because it is a constant and does not change when the reply is sent. TTL is used to limit the lifetime of a packet, preventing it from looping indefinitely in the network. When a router receives a packet with a TTL of 1 and decrements it to 0, it discards the packet and sends an ICMP TTL-exceeded message back to the source. During this process, the TTL of the ICMP message does not change but simply reflects the state of the original packet when it was discarded.



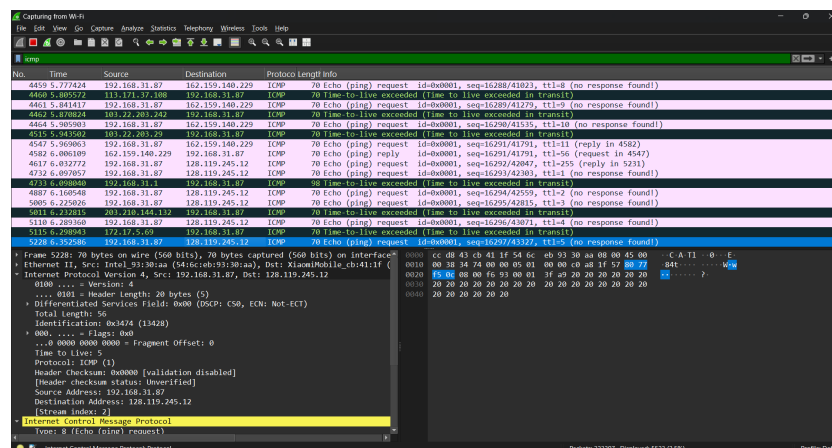
10 Question 10

Find the first ICMP Echo Request message that was sent by your computer after you changed the Packet Size in pingplotter to be 2000. Has that message been fragmented across more than one IP datagram? [Note: if you find your packet has not been fragmented, you should download the zip file <http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip> and extract the ip ethereal-trace-1packet trace. If your computer has an Ethernet interface, a packet size of 2000 should cause fragmentation.

Ans: Yes, it has been fragmented.

11 Question 11

Print out the first fragment of the fragmented IP datagram. What information in the IP header indicates that the datagram been fragmented? What information in the IP header indicates whether this is the first fragment versus a latter fragment? How long is this IP datagram?



Ans: The fact that the flag is set for more segments shows that the the datagram has been fragmented (see above).The fragment offset is set to 0 indicating that this is the first fragment rather than a latter fragment where that value is is set to 96. The datagram has a total length of 56.



12 Question 12

Print out the second fragment of the fragmented IP datagram. What information in the IP header indicates that this is not the first datagram fragment? Are there more fragments? How can you tell?

Ans: Since fragment offset is set to 1480 this shows that it is not the first fragment. Since the more fragments bit is set to zero this indicates there are no more fragments.

13 Question 13

What fields change in the IP header between the first and second fragment?

Ans: The fields that change are:

- Length
- Flags Set
- Fragment offset
- header checksum

14 Question 14

How many fragments were created from the original datagram?

Ans: 3 fragments were created from the original datagram.

15 Question 15

What fields change in the IP header among the fragments?

Ans: Fragment offset, total length, more fragments bit, TTL and the checksum.