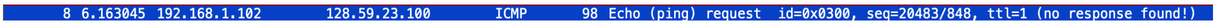
Computer Networks

LAB 5a

Author: Tran Dinh Dang Khoa
2211649

November 2, 2024

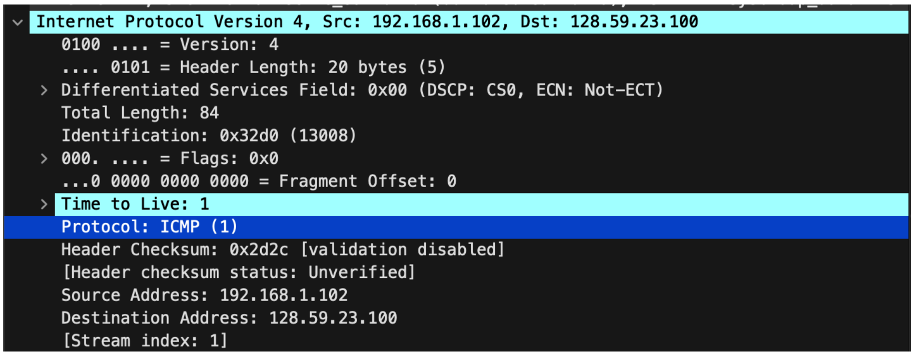
1. Select the first ICMP Echo Request message sent by your computer, and expand the Internet Protocol part of the packet in the packet details window.What is the IP address of your computer?



```
  8 6.163045  192.168.1.102         128.59.23.100         ICMP       98  Echo (ping) request  id=0x0300, seq=20483/848, ttl=1 (no response found!)
```

IP address: `192.168.1.102`

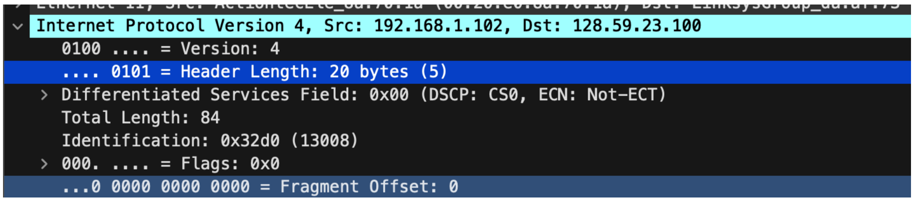
2. Within the IP packet header, what is the value in the upper layer protocol field?



```
v Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0x32d0 (13008)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
  > Time to Live: 1
    Protocol: ICMP (1)
    Header Checksum: 0x2d2c [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.102
    Destination Address: 128.59.23.100
    [Stream index: 1]
```

The value is `ICMP (1)`.

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.

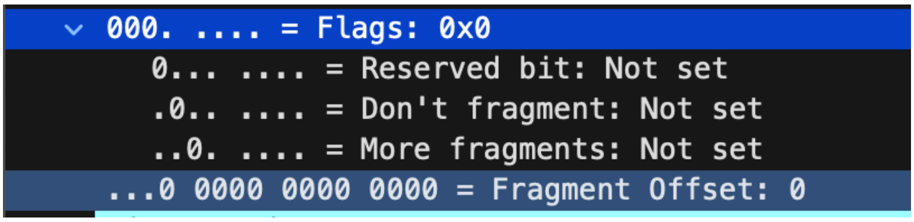


```
v Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0x32d0 (13008)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
```

Header length is 20 bytes

- There are 64 (84 - 20) bytes in the payload of the IP datagram.

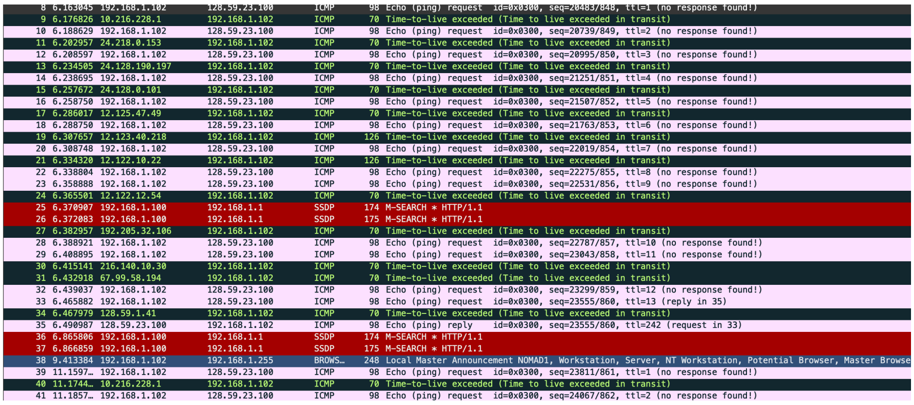
4. Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented.



```
  v 000. .... = Flags: 0x0
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
    ...0 0000 0000 0000 = Fragment Offset: 0
```

This IP datagram is not fragmented. Because the fragment flag is 0.

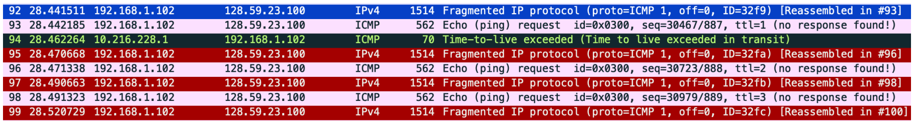
5. Which fields in the IP datagram always change from one datagram to the next within this series of ICMP messages sent by your computer?



```
 8 6.163045 192.168.1.102   128.59.23.100   ICMP     98 Echo (ping) request  id=0x0300, seq=20483/848, ttl=1 (no response found!)
 9 6.176826 10.216.228.1    192.168.1.102   ICMP     70 Time-to-live exceeded (Time to live exceeded in transit)
10 6.188629 192.168.1.102   128.59.23.100   ICMP     98 Echo (ping) request  id=0x0300, seq=20739/849, ttl=2 (no response found!)
11 6.202957 24.218.0.153    192.168.1.102   ICMP     70 Time-to-live exceeded (Time to live exceeded in transit)
12 6.208597 192.168.1.102   128.59.23.100   ICMP     98 Echo (ping) request  id=0x0300, seq=20995/850, ttl=3 (no response found!)
13 6.234505 24.128.190.197  192.168.1.102   ICMP     70 Time-to-live exceeded (Time to live exceeded in transit)
14 6.238695 192.168.1.102   128.59.23.100   ICMP     98 Echo (ping) request  id=0x0300, seq=21251/851, ttl=4 (no response found!)
15 6.257672 24.128.0.101    192.168.1.102   ICMP     70 Time-to-live exceeded (Time to live exceeded in transit)
16 6.258750 192.168.1.102   128.59.23.100   ICMP     98 Echo (ping) request  id=0x0300, seq=21507/852, ttl=5 (no response found!)
17 6.286017 12.125.47.49    192.168.1.102   ICMP     70 Time-to-live exceeded (Time to live exceeded in transit)
18 6.288750 192.168.1.102   128.59.23.100   ICMP     98 Echo (ping) request  id=0x0300, seq=21763/853, ttl=6 (no response found!)
19 6.307657 12.123.40.218   192.168.1.102   ICMP    126 Time-to-live exceeded (Time to live exceeded in transit)
20 6.308748 192.168.1.102   128.59.23.100   ICMP     98 Echo (ping) request  id=0x0300, seq=22019/854, ttl=7 (no response found!)
21 6.334320 12.122.10.22    192.168.1.102   ICMP    126 Time-to-live exceeded (Time to live exceeded in transit)
22 6.338804 192.168.1.102   128.59.23.100   ICMP     98 Echo (ping) request  id=0x0300, seq=22275/855, ttl=8 (no response found!)
23 6.358888 192.168.1.102   128.59.23.100   ICMP     98 Echo (ping) request  id=0x0300, seq=22531/856, ttl=9 (no response found!)
24 6.365501 12.122.12.54    192.168.1.102   ICMP     70 Time-to-live exceeded (Time to live exceeded in transit)
25 6.370907 192.168.1.100   192.168.1.1     SSDP    174 M-SEARCH * HTTP/1.1
26 6.372083 192.168.1.100   192.168.1.1     SSDP    175 M-SEARCH * HTTP/1.1
27 6.382957 192.205.32.106  192.168.1.102   ICMP     70 Time-to-live exceeded (Time to live exceeded in transit)
28 6.388921 192.168.1.102   128.59.23.100   ICMP     98 Echo (ping) request  id=0x0300, seq=22787/857, ttl=10 (no response found!)
29 6.408895 192.168.1.102   128.59.23.100   ICMP     98 Echo (ping) request  id=0x0300, seq=23043/858, ttl=11 (no response found!)
30 6.415141 216.140.10.30   192.168.1.102   ICMP     70 Time-to-live exceeded (Time to live exceeded in transit)
31 6.432918 67.99.58.194    192.168.1.102   ICMP     70 Time-to-live exceeded (Time to live exceeded in transit)
32 6.439037 192.168.1.102   128.59.23.100   ICMP     98 Echo (ping) request  id=0x0300, seq=23299/859, ttl=12 (no response found!)
33 6.465882 192.168.1.102   128.59.23.100   ICMP     98 Echo (ping) request  id=0x0300, seq=23555/860, ttl=13 (reply in 35)
34 6.467979 128.59.1.41     192.168.1.102   ICMP     70 Time-to-live exceeded (Time to live exceeded in transit)
35 6.490987 128.59.23.100   192.168.1.102   ICMP     98 Echo (ping) reply    id=0x0300, seq=23555/860, ttl=242 (request in 33)
36 6.865806 192.168.1.100   192.168.1.1     SSDP    174 M-SEARCH * HTTP/1.1
37 6.866859 192.168.1.100   192.168.1.1     SSDP    175 M-SEARCH * HTTP/1.1
38 9.413384 192.168.1.102   192.168.1.255   BROWS…  248 Local Master Announcement NOMAD1, Workstation, Server, NT Workstation, Potential Browser, Master Browse
39 11.1597… 192.168.1.102   128.59.23.100   ICMP     98 Echo (ping) request  id=0x0300, seq=23811/861, ttl=1 (no response found!)
40 11.1744… 10.216.228.1    192.168.1.102   ICMP     70 Time-to-live exceeded (Time to live exceeded in transit)
41 11.1857… 192.168.1.102   128.59.23.100   ICMP     98 Echo (ping) request  id=0x0300, seq=24067/862, ttl=2 (no response found!)
```

The fields in the IP datagram always change from one datagram to the next within this series of ICMP are sequence number and the TTL field.

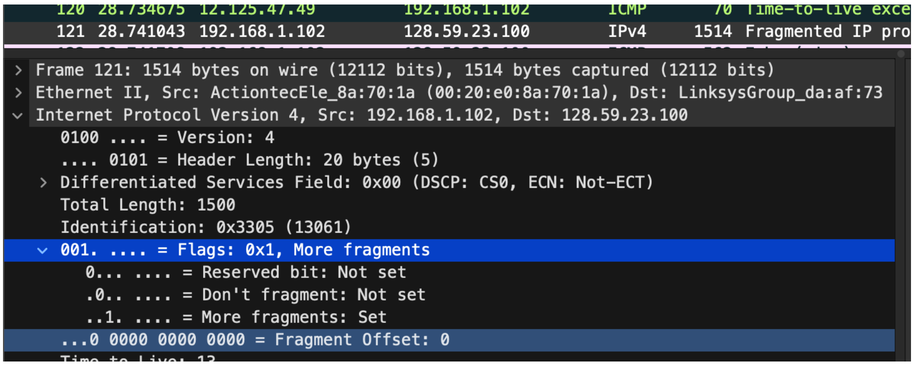
6. Which fields stay constant? Which of the fields must stay constant? Which fields must change? Why?
   - The fields stay constant:
     - Source and Destination IP address
     - Protocol field.
     - ICMP type and code.
   - The fields changes:
     - Sequence number
     - Time to live
7. Describe the pattern you see in the values in the Identification field of the IP datagram
   - The identification field value decrease by 1 in every IP datagram.
8. What is the value in the Identification field and the TTL field?
   - The value in the Identification field: `0x9d7c`
   - The TTL field: `255`
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?
   - The value in the Identification field changes in every IP datagram
   - The TTL field remains unchanged: `255`
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?



```
92 28.441511 192.168.1.102   128.59.23.100   IPv4   1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=32f9) [Reassembled in #93]
93 28.442185 192.168.1.102   128.59.23.100   ICMP    562 Echo (ping) request  id=0x0300, seq=30467/887, ttl=1 (no response found!)
94 28.462264 10.216.228.1    192.168.1.102   ICMP     70 Time-to-live exceeded (Time to live exceeded in transit)
95 28.470668 192.168.1.102   128.59.23.100   IPv4   1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fa) [Reassembled in #96]
96 28.471338 192.168.1.102   128.59.23.100   ICMP    562 Echo (ping) request  id=0x0300, seq=30723/888, ttl=2 (no response found!)
97 28.490663 192.168.1.102   128.59.23.100   IPv4   1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fb) [Reassembled in #98]
98 28.491323 192.168.1.102   128.59.23.100   ICMP    562 Echo (ping) request  id=0x0300, seq=30979/889, ttl=3 (no response found!)
99 28.520729 192.168.1.102   128.59.23.100   IPv4   1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fc) [Reassembled in #100]
```

Yes, the message has been fragmented across more than 1 IP datagram.

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?

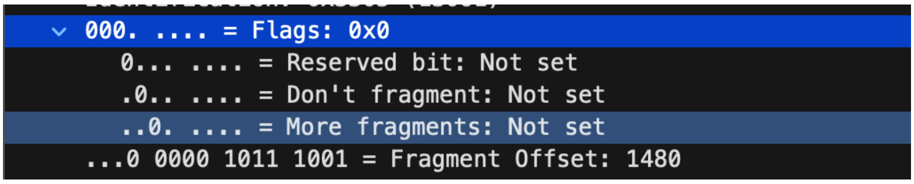


```
  120  28.734675  12.125.47.49    192.168.1.102    ICMP      70  Time-to-live exce
  121  28.741043  192.168.1.102   128.59.23.100    IPv4    1514  Fragmented IP pro

> Frame 121: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
> Ethernet II, Src: ActiontecEle_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysGroup_da:af:73
v Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1500
    Identification: 0x3305 (13061)
  v 001. .... = Flags: 0x1, More fragments
        0... .... = Reserved bit: Not set
        .0.. .... = Don't fragment: Not set
        ..1. .... = More fragments: Set
    ...0 0000 0000 0000 = Fragment Offset: 0
```

The Flags bit for more fragments is set, indicating that the datagram has been fragmented. Since the fragment offset is 0, we know that this is the first fragment. This first datagram has a total length of 1500, including the header

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 the more fragments? How can you tell?



```
  v 000. .... = Flags: 0x0
        0... .... = Reserved bit: Not set
        .0.. .... = Don't fragment: Not set
        ..0. .... = More fragments: Not set
    ...0 0000 1011 1001 = Fragment Offset: 1480
```

We can tell that this is not the first fragment, since the fragment offset is `1480`. It is the last fragment, since the more fragments flag is not set

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

    - The IP header fields that changed between the fragments are: Total Length, Flags, Fragment Offset, and Checksum.

14. How many fragments were created from the original datagram?

    - After switching to 3500, there are 3 packets created from the original datagram.

15. What fields change in the IP header among the fragments?

    - The IP header fields that changed between all of the packets are: fragment offset, and checksum. Between the first two packets and the last packet, we see a change in total length, and also in the flags. The first two packets have a total length of 1500, with the more fragments bit set to 1, and the last packet has a total length of 540, with the more fragments bit set to 0