

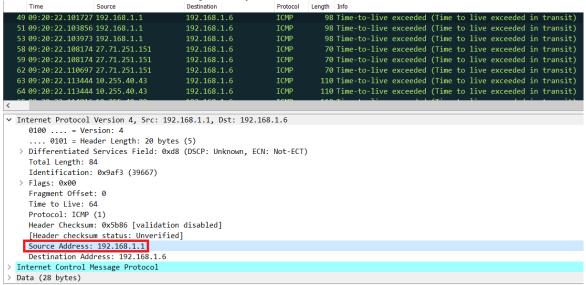
COMPUTER NETWORK Lab 4a

Student name: Nguyễn Minh Tâm

ID: 1952968

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?

Ans: The IP address of my computer: 192.168.1.1



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

Ans: The upper layer protocol field: ICMP(1)

```
Protocol Length Info
  51 09:20:22.103856 192.168.1.1
                                                                          98 Time-to-live exceeded (Time to live exceeded in transit)
  53 09:20:22.103973 192.168.1.1
                                         192.168.1.6
                                                                          98 Time-to-live exceeded (Time to live exceeded in transit)
  58 09:20:22.108174 27.71.251.151
                                                                          70 Time-to-live exceeded (Time to live exceeded in transit)
  59 09:20:22.108174 27.71.251.151
                                         192.168.1.6
                                                                          70 Time-to-live exceeded (Time to live exceeded in transit)
                                                                          70 Time-to-live exceeded (Time to live exceeded in transit)
                                         192.168.1.6
 63 09:20:22.113444 10.255.40.43
                                         192.168.1.6
                                                                         110 Time-to-live exceeded (Time to live exceeded in transit)
                                                                         110 Time-to-live exceeded (Time to live exceeded in transit)
                                         192.168.1.6
 Ethernet II, Src: DASANNet_c9:2d:cf (9c:65:ee:c9:2d:cf), Dst: IntelCor_5e:45:34 (dc:fb:48:5e:45:34)
Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.6
    0100 .... = Version: 4
       .. 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0xd8 (DSCP: Unknown, ECN: Not-ECT)
    Total Length: 84
    Identification: 0x9af3 (39667)
  > Flags: 0x00
    Fragment Offset: 0
     Time to Live: 6
   Protocol: ICMP (1)
    Header Checksum: 0x5b86 [validation disabled]
    [Header checksum status: Unverified]
     Source Address: 192.168.1.1
    Destination Address: 192.168.1.6
> Internet Control Message Protocol
```

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.

Ans:



The IP header: 20 bytes.

The payload = total length – header bytes = 84 - 20 = 64 bytes.

```
Protocol Length Info
  49 09:20:22.101727 192.168.1.1
                                            192.168.1.6
 51 09:20:22.103856 192.168.1.1
                                                                             98 Time-to-live exceeded (Time to live exceeded in transit)
                                           192.168.1.6
                                                                 ICMP
  53 09:20:22.103973 192.168.1.1
                                                                             98 Time-to-live exceeded (Time to live exceeded in transit)
                                           192.168.1.6
                                                                 ICMP
                                                                             70 Time-to-live exceeded (Time to live exceeded in transit)
 58 09:20:22.108174 27.71.251.151
                                           192.168.1.6
                                                                 ICMP
 59 09:20:22.108174 27.71.251.151
                                                                             70 Time-to-live exceeded (Time to live exceeded in transit)
                                           192.168.1.6
                                                                  ICMP
 62 09:20:22.110697 27.71.251.151
                                                                            70 Time-to-live exceeded (Time to live exceeded in transit) 110 Time-to-live exceeded (Time to live exceeded in transit)
                                           192.168.1.6
 63 09:20:22.113444 10.255.40.43
                                           192.168.1.6
                                                                  ICMP
 64 09:20:22.113444 10.255.40.43

✓ Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.6

    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0xd8 (DSCP: Unknown, ECN: Not-ECT)
    Total Length: 84
     Identification: 0x9af3 (39667)
  > Flags: 0x00
    Fragment Offset: 0
    Time to Live: 64
    Protocol: ICMP (1)
    Header Checksum: 0x5b86 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.1
    Destination Address: 192.168.1.6
> Internet Control Message Protocol
> Data (28 bytes)
```

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

Ans: As you can see the fragment offset = 0, so this IP datagram has not been fragmented yet.

```
19 09:20:22.101727 192.168.1.1
  51 09:20:22.103856 192.168.1.1
                                         192.168.1.6
                                                               ICMP
                                                                         98 Time-to-live exceeded (Time to live exceeded in transit)
  53 09:20:22.103973 192.168.1.1
                                                               ICMP
                                                                          98 Time-to-live exceeded (Time to live exceeded in transit)
                                                                          70 Time-to-live exceeded (Time to live exceeded in transit)
  58 09:20:22.108174 27.71.251.151
                                         192.168.1.6
  59 09:20:22.108174 27.71.251.151
                                                               ICMP
                                                                          70 Time-to-live exceeded (Time to live exceeded in transit)
                                                                          70 Time-to-live exceeded (Time to live exceeded in transit)
 62 09:20:22.110697 27.71.251.151
                                                               ICMP
  63 09:20:22.113444 10.255.40.43
                                                               ICMP
  64 09:20:22.113444 10.255.40.43
                                                                         110 Time-to-live exceeded (Time to live exceeded in transit)
Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.6
    0100 .... = Version: 4
     .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0xd8 (DSCP: Unknown, ECN: Not-ECT)
    Total Length: 84
    Identification: 0x9af3 (39667)
    Flags: 0x00
   Fragment Offset: 0
    Time to Live: 64
    Protocol: ICMP (1)
    Header Checksum: 0x5b86 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.1
    Destination Address: 192.168.1.6
> Internet Control Message Protocol
> Data (28 bytes)
```

- 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: Identification, Time to live and Header checksum always change from one datagram to the next.
- 6. Which fields stay constant? Which of the fields must stay constant? Which fields must change? Why?
 Ans:

The fields that stay constant:

- Version (since we are using IPv4 for all packets)



- header length (since these are ICMP packets)
- source IP (since we are sending from the same source)
- destination IP (since we are sending to the same destination)
- Differentiated Services (since all packets are ICMP they use the same type of Service class)
- Upper Layer Protocol (sinice these are ICMP packets)

The fields that must stay constant is the same to the fields that stay constant.

The fields that must change:

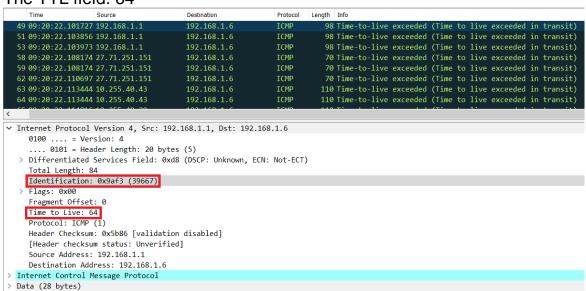
- Identification (IP packets must have different IDs)
- Time to live (traceroute increments each subsequent packet)
- Header checksum (since header changes, so the checksum must change)
- 7. Describe the pattern you see in the values in the Identification field of the IP datagram

Ans: The pattern I see in the values in the Identification field is that the IP header Identification fields increment with each ICMP request.

8. What is the value in the Identification field and the TTL field? Ans:

The Identification field: 39667

The TTL field: 64



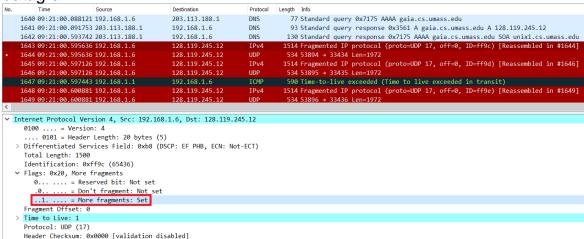
9. Do these values remain unchanged for all of the ICMP TTL-exceeded replies sent to your computer by the nearest (first hop) router? Why? Ans:

The Identification field changes for all the ICMP TTL-exceeded replies because the Identification field is a unique value. When two or more IP datagrams have the same identification value, then it means that these IP datagrams are fragments of a single large IP datagram.



The TTL field remains unchanged because the TTL for the first hop router is always the same.

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? Ans: Yes, the message has been fragmented across more than one IP datagram.



11. 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 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.

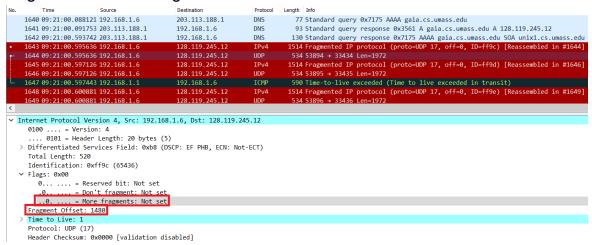
```
1640 09:21:00.088121 192.168.1.6
                                                                    203.113.188.1
                                                                                                                 93 Standard query response 0x3561 A gaia.cs.umass.edu A 128.119.245.12
130 Standard query response 0x7175 AAAA gaia.cs.umass.edu SOA unix1.cs.umass.edu
1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=ff9c) [Reassembled in #1644]
      1641 09:21:00.091753 203.113.188.1
1642 09:21:00.593742 203.113.188.1
                                                                   192.168.1.6
                                                                   128.119.245.12
                                                                                                                  534 53894 → 33434 Len=1972
                                                                                                                 1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=ff9d) [Reassembled in #1646
Internet Protocol Version 4, Src: 192.168.1.6, Dst: 128.119.245.12
       0100 .... = Version: 4
      ... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0xb8 (DSCP: EF PHB, ECN: Not-ECT)
Total Length: 1500
Identification: 0xff9c (65436)
    ✓ Flags: 0x20, More fragments
0... = Reserved bit: Not set
            .0.. ... = Don't fragment: Not
     ..1. .... = More fragments: Set
Fragment Offset: 0
       Time to Live: 1
       Protocol: UDP (17)
       Header Checksum: 0x0000 [validation disabled]
```

12. What information in the IP header indicates that this is not the first datagram fragment? Are the more fragments? How can you tell? Ans:

Because the Fragment Offset = 1480, it indicates that this is the last datagram fragment.



You can see that the More Fragments is not set, so there are no more fragments in this datagram.

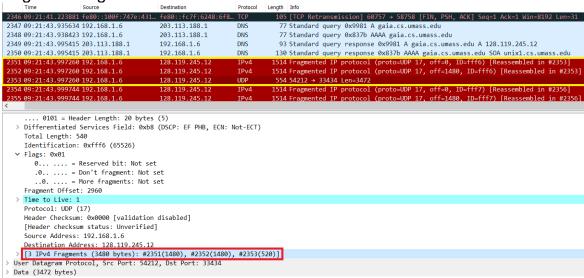


13. What fields change in the IP header between the first and second fragment?

Ans: The IP header fields that changed between the fragments are: total length, flags, fragment offset. You can see two screenshots above to see the differences.

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

The first ICMP Echo Request message has 3 fragments cretaed from the original datagram.



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

Between the first and the second fragment, the Fragment Offset changes.

Faculty of Computer Science and Engineering – HCMC University of Technology

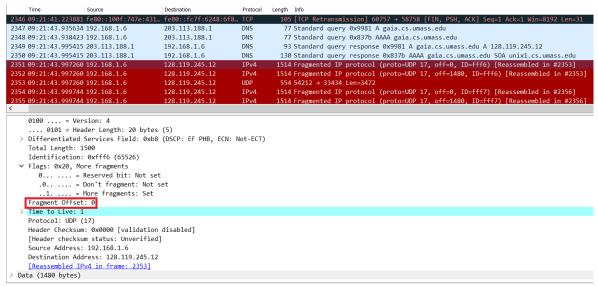


Figure 1: First fragment

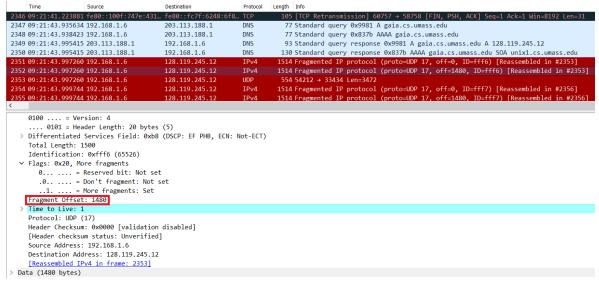


Figure 2: Second fragment

Between the second and the third fragment, the Total Length, the Flags and the Fragment Offset change.



Faculty of Computer Science and Engineering – HCMC University of Technology

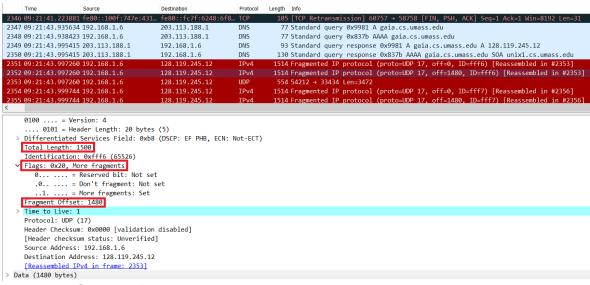


Figure 3: Second fragment

Time	Source	Destination	Protocol	Length Info
2346 09:21:41.22	881 fe80::100f:747e:431	fe80::fc7f:6248:6f	8 TCP	105 [TCP Retransmission] 60757 → 58758 [FIN, PSH, ACK] Seq=1 Ack=1 Win=8192 Len=31
2347 09:21:43.93	634 192.168.1.6	203.113.188.1	DNS	77 Standard query 0x9981 A gaia.cs.umass.edu
2348 09:21:43.938	3423 192.168.1.6	203.113.188.1	DNS	77 Standard query 0x837b AAAA gaia.cs.umass.edu
2349 09:21:43.99	415 203.113.188.1	192.168.1.6	DNS	93 Standard query response 0x9981 A gaia.cs.umass.edu A 128.119.245.12
2350 09:21:43.99	415 203.113.188.1	192.168.1.6	DNS	130 Standard query response 0x837b AAAA gaia.cs.umass.edu SOA unix1.cs.umass.edu
2351 09:21:43.99	260 192.168.1.6	128.119.245.12	IPv4	1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=fff6) [Reassembled in #2353]
2352 09:21:43.99	260 192.168.1.6	128.119.245.12	IPv4	1514 Fragmented IP protocol (proto=UDP 17, off=1480, ID=fff6) [Reassembled in #2353]
2353 09:21:43.99	260 192.168.1.6	128.119.245.12	UDP	554 54212 → 33434 Len=3472
2354 09:21:43.99	744 192.168.1.6	128.119.245.12	IPv4	1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=fff7) [Reassembled in #2356]
2355 09:21:43.999	744 192.168.1.6	128.119.245.12	IPv4	1514 Fragmented IP protocol (proto=UDP 17, off=1480, ID=fff7) [Reassembled in #2356]
<				
0100 =	Version: 4			
0101 = Header Length: 20 bytes (5)				
> <u>Differentiated Services Field: 0xb8 (DSCP: EF PHB, ECN: Not-ECT)</u>				
Total Length: 540				
<u>Identificati</u> on: 0xfff6 (65526)				
v Flags: 0x01				
0 = Reserved bit: Not set				
.0 = Don't fragment: Not set				
0 = More fragments: Not set				
Fragment Offset: 2960				
> Time to Live: 1				
Protocol: UDP (17)				
Header Checksum: 0x0000 [validation disabled]				
[Header checksum status: Unverified]				
Source Address: 192.168.1.6				
Destination Address: 128.119.245.12				
> [3 IPv4 Fragments (3480 bytes): #2351(1480), #2352(1480), #2353(520)]				
> User Datagram Protocol, Src Port: 54212, Dst Port: 33434				
	T 1 1 6			

Figure 4: Third fragment