Computer Science Department - ITU	
Computer Networks Lab	
Course Instructor: Anam Zahid	**Dated: 12/11/2024**
Lab Engineer: Nasir Amjad & Ghulam Ruqia	**Semester: Fall 2024**
Session: 2023-2027	**Batch: BSCS2023 & BSAI2023**

Lab 12. Introduction of IP

Name	Roll number	Report Marks(10)	Viva Marks(5)	Total Marks (15)
Hassan Usman	BSAI23047			

Checked on: ______________________________

Signature: ______________________________

Objective

The objective of this lab is to do some networking commands to help us better understand networking and, in its troubleshooting, as well as its administration.

Equipment and Component

Component Description	Value	Quantity
Computer	Available in lab	1

Conduct of Lab

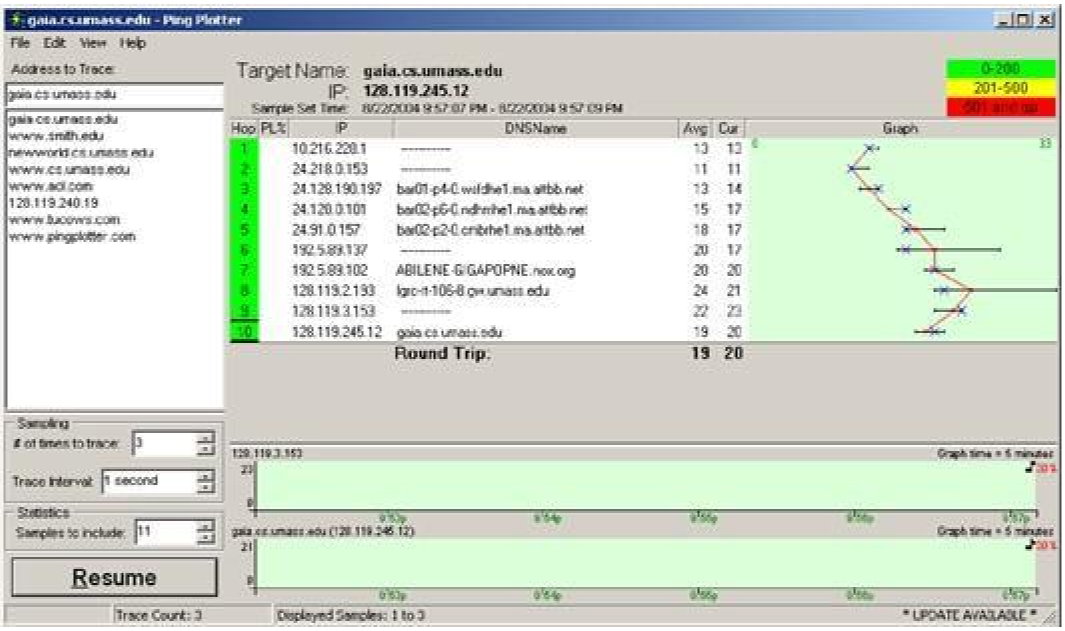
1. Students have to perform this experiment on Wireshark.
2. Students are required to perform this experiment individually.
3. In case the lab experiment is not understood, the students are advised to seek help from the course instructor, lab engineers and assigned teaching assistants (TAs)
4. At the end of the lab, every student is required to save the completed lab manual in PDF format and submit this single PDF file on Google Classroom at the submission link created for this lab..

Theory and Background

An **Internet Protocol** address is a numerical label such as 192.0.2.1 that is connected to a computer network that uses the Internet Protocol for communication. They establish the framework for data exchange, with key examples including TCP/IP for internet communication and HTTP/DNS for web-related functions.

Lab Tasks

- Start up Wireshark and begin packet capture *(Capture->Start)* and then press *OK* on the Wireshark Packet Capture Options screen (we'll not need to select any options here).
- Start up *pingplotter* and enter the name of a target destination in the "Address to Trace Window." Select the menu item *Edit>Options->Packet Options* and enter a value of 56 in the *Packet Size* field and then press OK. Then press the Trace button. You should see a *pingplotter* window that looks something like this:



Target Name: gaia.cs.umass.edu
IP: 128.119.245.12
Sample Set Time: 8/22/2004 9:57:07 PM - 8/22/2004 9:57:09 PM

Hop	PL%	IP	DNSName	Avg	Cur
1		10.216.228.1	----------	13	13
2		24.218.0.153	----------	11	11
3		24.128.190.197	bar01-p4-0.wlfdhe1.ma.attbb.net	13	14
4		24.128.0.101	bar02-p6-0.ndhmhe1.ma.attbb.net	15	17
5		24.91.0.157	bar02-p2-0.cmbrhe1.ma.attbb.net	18	17
6		192.5.89.137	----------	20	17
7		192.5.89.102	ABILENE-GIGAPOPNE.nox.org	20	20
8		128.119.2.193	lgrc-rt-106-8.gw.umass.edu	24	21
9		128.119.3.153	----------	22	23
10		128.119.245.12	gaia.cs.umass.edu	19	20
			Round Trip:	19	20

Sampling
# of times to trace: 3
Trace Interval: 1 second

Statistics
Samples to include: 11

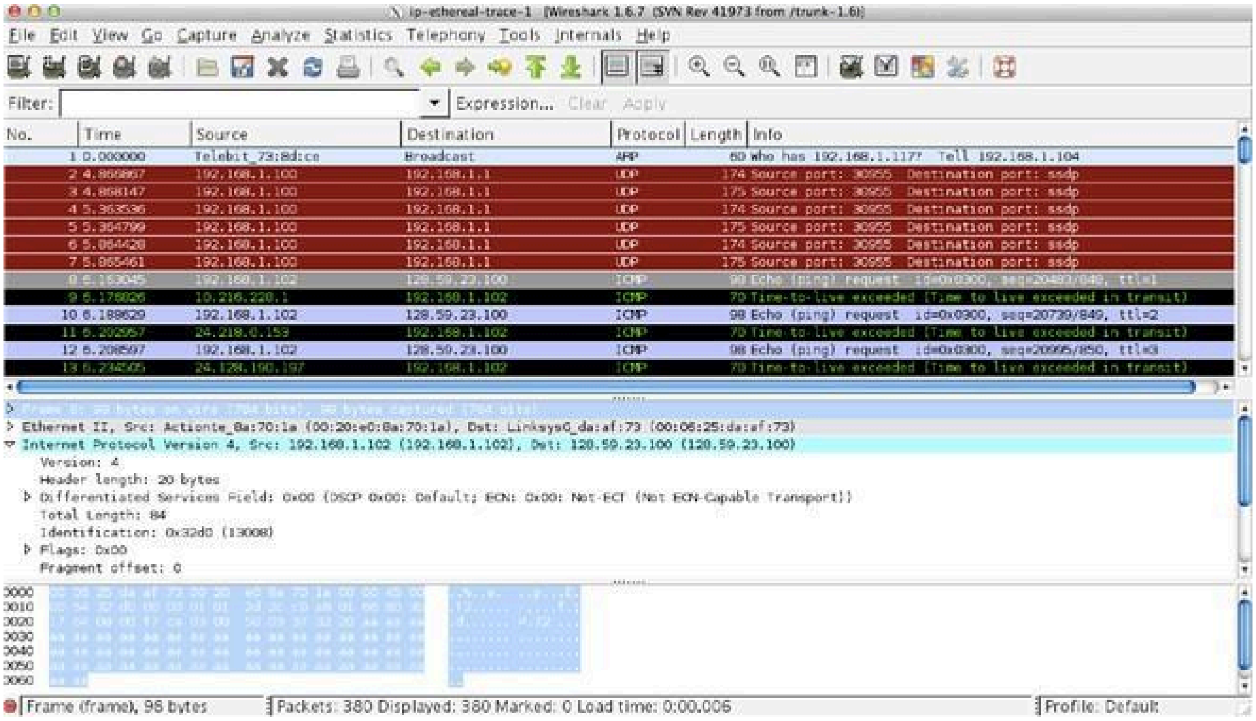
Trace Count: 3
Displayed Samples: 1 to 3

- Next, send a set of datagrams with a longer length, by selecting *Edit->Options->Packet Options* and enter a value of 2000 in the *Packet Size* field and then press OK. Then press the Resume button.
- Finally, send a set of datagrams with a longer length, by selecting *Edit->Advanced Options->Packet Options* and enter a value of 3500 in the *Packet Size* field and then press OK. Then press the Resume button.
- Stop Wireshark tracing.

A look at the captured trace

In your trace, you should be able to see the series of ICMP Echo Request (in the case of Windows machine) or the UDP segment (in the case of Unix) sent by your computer and the ICMP TTL-exceeded messages returned to your computer by the intermediate routers. In the questions below, we'll assume you are using a Windows machine; the corresponding questions for the case of a Unix machine should be clear. Whenever possible, when answering a question below you should hand in a printout of the packet(s) within the trace that you used to answer the question asked.

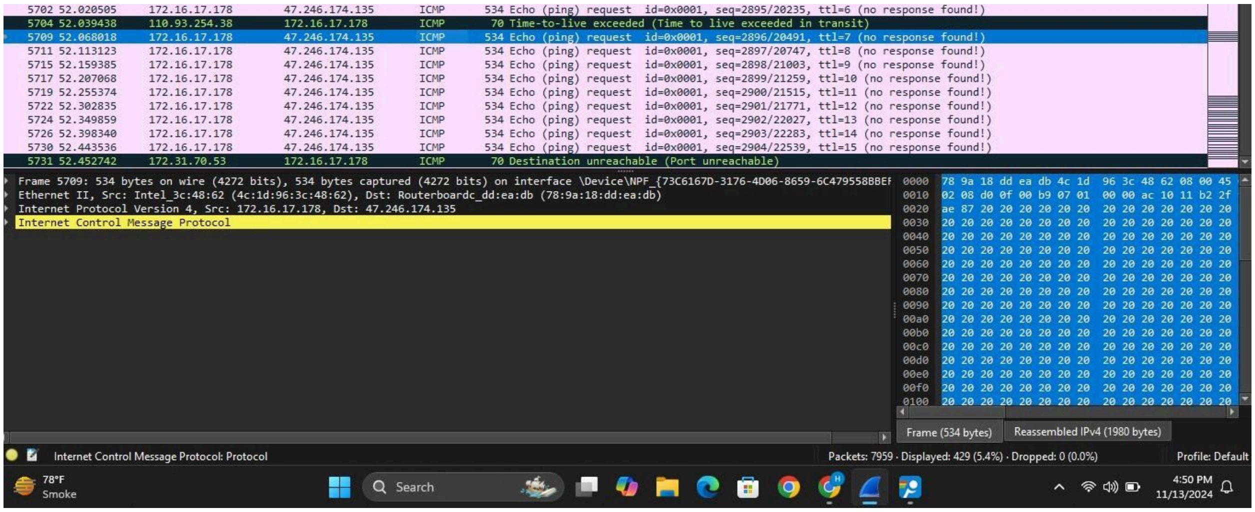
Select the first ICMP Echo Request message sent by your computer, and expand the Internet Protocol part of the packet in the packet details window.


ip-ethereal-trace-1 [Wireshark 1.6.7 (SVN Rev 41973 from /trunk-1.6)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply

```
No.  Time        Source            Destination      Protocol Length Info
   1 0.000000    Telebit_73:8d:ce  Broadcast        ARP       60 Who has 192.168.1.117?  Tell 192.168.1.104
   2 4.866867    192.168.1.100     192.168.1.1      UDP      174 Source port: 30955  Destination port: ssdp
   3 4.868147    192.168.1.100     192.168.1.1      UDP      175 Source port: 30955  Destination port: ssdp
   4 5.363536    192.168.1.100     192.168.1.1      UDP      174 Source port: 30955  Destination port: ssdp
   5 5.364799    192.168.1.100     192.168.1.1      UDP      175 Source port: 30955  Destination port: ssdp
   6 5.864428    192.168.1.100     192.168.1.1      UDP      174 Source port: 30955  Destination port: ssdp
   7 5.865461    192.168.1.100     192.168.1.1      UDP      175 Source port: 30955  Destination port: ssdp
   8 6.163045    192.168.1.102     128.59.23.100    ICMP      98 Echo (ping) request  id=0x0300, seq=20483/848, ttl=1
   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
  11 6.202967    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
  13 6.234505    24.128.190.197    192.168.1.102    ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
```

```
> Frame 8: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
> Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
v Internet Protocol Version 4, Src: 192.168.1.102 (192.168.1.102), Dst: 128.59.23.100 (128.59.23.100)
    Version: 4
    Header length: 20 bytes
  > Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 84
    Identification: 0x32d0 (13008)
  > Flags: 0x00
    Fragment offset: 0
```

1. **What is the IP address of your computer?**



```
5702 52.020505   172.16.17.178   47.246.174.135   ICMP   534 Echo (ping) request  id=0x0001, seq=2895/20235, ttl=6 (no response found!)
5704 52.039438   110.93.254.38   172.16.17.178    ICMP    70 Time-to-live exceeded (Time to live exceeded in transit)
5709 52.068018   172.16.17.178   47.246.174.135   ICMP   534 Echo (ping) request  id=0x0001, seq=2896/20491, ttl=7 (no response found!)
5711 52.113123   172.16.17.178   47.246.174.135   ICMP   534 Echo (ping) request  id=0x0001, seq=2897/20747, ttl=8 (no response found!)
5715 52.159385   172.16.17.178   47.246.174.135   ICMP   534 Echo (ping) request  id=0x0001, seq=2898/21003, ttl=9 (no response found!)
5717 52.207068   172.16.17.178   47.246.174.135   ICMP   534 Echo (ping) request  id=0x0001, seq=2899/21259, ttl=10 (no response found!)
5719 52.255374   172.16.17.178   47.246.174.135   ICMP   534 Echo (ping) request  id=0x0001, seq=2900/21515, ttl=11 (no response found!)
5722 52.302835   172.16.17.178   47.246.174.135   ICMP   534 Echo (ping) request  id=0x0001, seq=2901/21771, ttl=12 (no response found!)
5724 52.349859   172.16.17.178   47.246.174.135   ICMP   534 Echo (ping) request  id=0x0001, seq=2902/22027, ttl=13 (no response found!)
5726 52.398340   172.16.17.178   47.246.174.135   ICMP   534 Echo (ping) request  id=0x0001, seq=2903/22283, ttl=14 (no response found!)
5730 52.443536   172.16.17.178   47.246.174.135   ICMP   534 Echo (ping) request  id=0x0001, seq=2904/22539, ttl=15 (no response found!)
5731 52.452742   172.31.70.53    172.16.17.178    ICMP    70 Destination unreachable (Port unreachable)
```

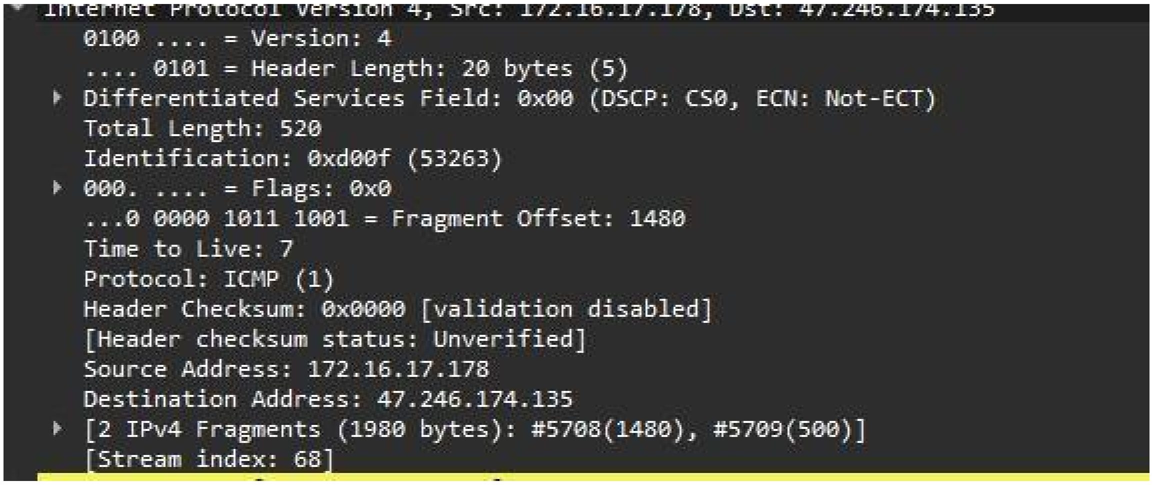
```
Frame 5709: 534 bytes on wire (4272 bits), 534 bytes captured (4272 bits) on interface \Device\NPF_{73C6167D-3176-4D06-8659-6C479558BBEF
Ethernet II, Src: Intel_3c:48:62 (4c:1d:96:3c:48:62), Dst: Routerboardc_dd:ea:db (78:9a:18:dd:ea:db)
Internet Protocol Version 4, Src: 172.16.17.178, Dst: 47.246.174.135
Internet Control Message Protocol
```

```
0000  78 9a 18 dd ea db 4c 1d  96 3c 48 62 08 00 45
0010  02 08 d0 0f 00 b9 07 01  00 00 ac 10 11 b2 2f
0020  ae 87 20 20 20 20 20 20  20 20 20 20 20 20 20
0030  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20
0040  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20
0050  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20
0060  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20
0070  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20
0080  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20
0090  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20
00a0  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20
00b0  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20
00c0  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20
00d0  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20
00e0  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20
00f0  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20
0100  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20
```

Frame (534 bytes)
Reassembled IPv4 (1980 bytes)
Internet Control Message Protocol: Protocol
Packets: 7959 · Displayed: 429 (5.4%) · Dropped: 0 (0.0%)
Profile: Default
78°F
Smoke
Search
4:50 PM
11/13/2024

source:172.16.17.178

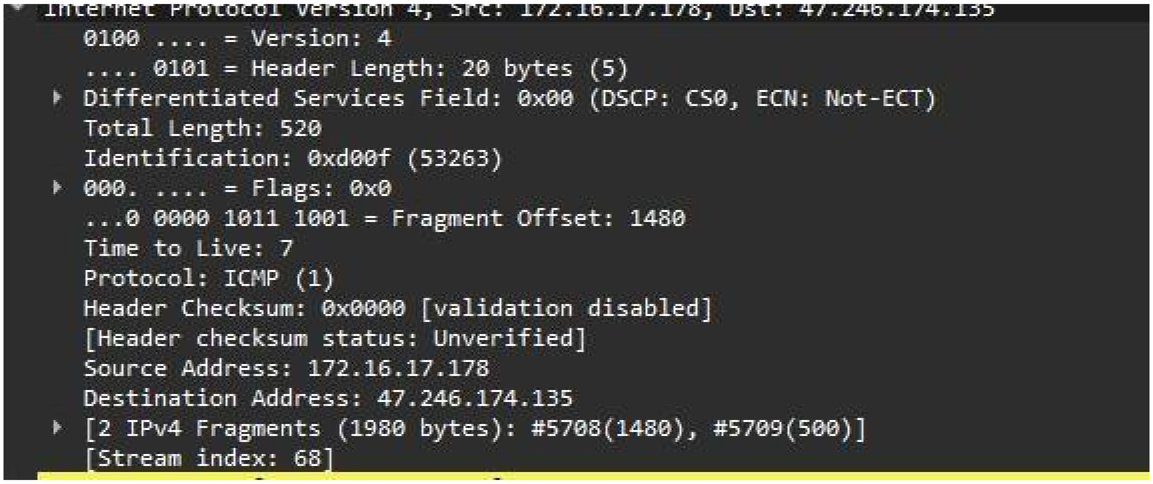
2. **Within the IP packet header, what is the value in the upper layer protocol field?**



```
Internet Protocol Version 4, Src: 172.16.17.178, Dst: 47.246.174.135
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 520
    Identification: 0xd00f (53263)
  ▸ 000. .... = Flags: 0x0
    ...0 0000 1011 1001 = Fragment Offset: 1480
    Time to Live: 7
    Protocol: ICMP (1)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 172.16.17.178
    Destination Address: 47.246.174.135
  ▸ [2 IPv4 Fragments (1980 bytes): #5708(1480), #5709(500)]
    [Stream index: 68]
```

ICMP 1

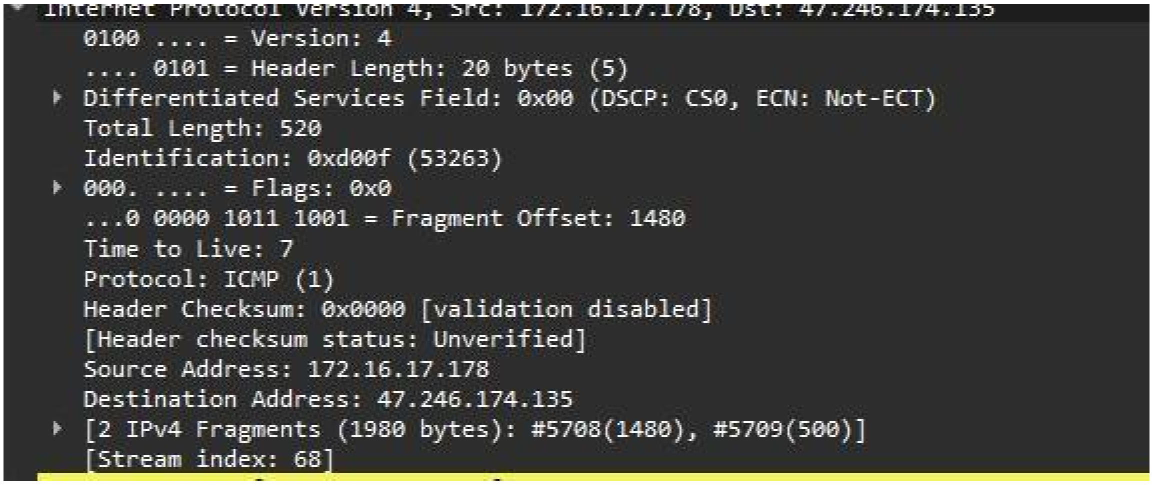
3. **How many bytes are in the IP header? How many bytes are in the payload *of the IP datagram*? Explain how you determined the number of payload bytes.**



```
Internet Protocol Version 4, Src: 172.16.17.178, Dst: 47.246.174.135
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 520
    Identification: 0xd00f (53263)
  > 000. .... = Flags: 0x0
    ...0 0000 1011 1001 = Fragment Offset: 1480
    Time to Live: 7
    Protocol: ICMP (1)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 172.16.17.178
    Destination Address: 47.246.174.135
  > [2 IPv4 Fragments (1980 bytes): #5708(1480), #5709(500)]
    [Stream index: 68]
```

20 bytes in header 520-20=500 in payload we subtract total length and the bytes in header

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

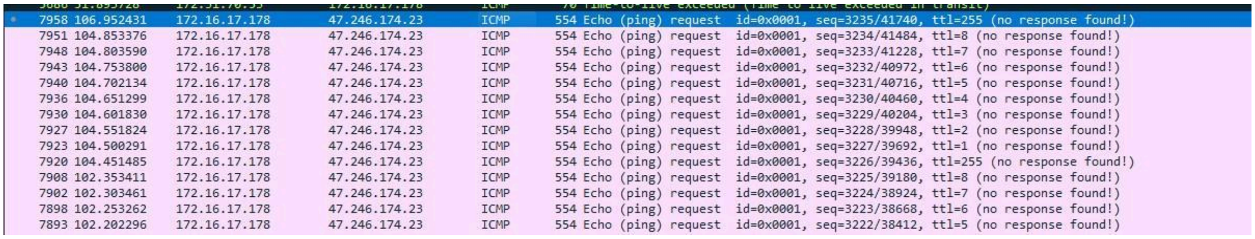


```
Internet Protocol Version 4, Src: 172.16.17.178, Dst: 47.246.174.135
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 520
    Identification: 0xd00f (53263)
  > 000. .... = Flags: 0x0
    ...0 0000 1011 1001 = Fragment Offset: 1480
    Time to Live: 7
    Protocol: ICMP (1)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 172.16.17.178
    Destination Address: 47.246.174.135
  > [2 IPv4 Fragments (1980 bytes): #5708(1480), #5709(500)]
    [Stream index: 68]
```

yes it has been fragmented, we can see that through the fragment offset

Next, sort the traced packets according to IP source address by clicking on the *Source* column header; a small downward pointing arrow should appear next to the word *Source*. If the arrow points up, click on the *Source* column header again. Select the first ICMP Echo Request message sent by your computer, and expand the Internet Protocol portion in the "details of selected packet header" window. In the "listing of captured packets" window, you should see all of the subsequent ICMP messages (perhaps with additional interspersed packets sent by other protocols running on your computer) below this first ICMP. Use the down arrow to move through the ICMP messages sent by your computer.

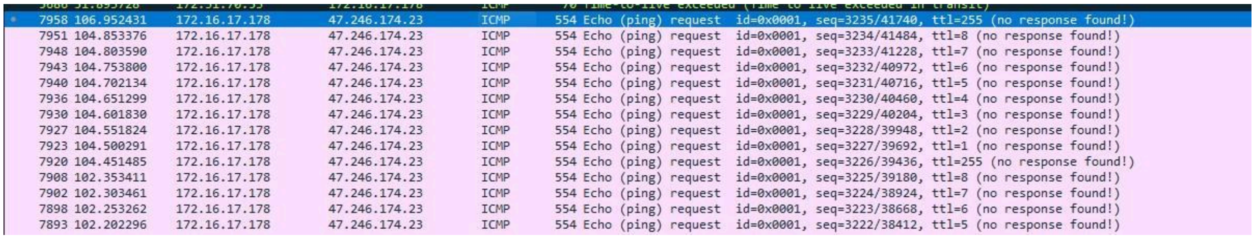
5. **Which fields in the IP datagram *always* change from one datagram to the next within this series of ICMP messages sent by your computer?**



```
5080 51.895728    172.31.70.33     172.16.17.178    ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
7958 106.952431   172.16.17.178    47.246.174.23    ICMP     554 Echo (ping) request  id=0x0001, seq=3235/41740, ttl=255 (no response found!)
7951 104.853376   172.16.17.178    47.246.174.23    ICMP     554 Echo (ping) request  id=0x0001, seq=3234/41484, ttl=8 (no response found!)
7948 104.803590   172.16.17.178    47.246.174.23    ICMP     554 Echo (ping) request  id=0x0001, seq=3233/41228, ttl=7 (no response found!)
7943 104.753800   172.16.17.178    47.246.174.23    ICMP     554 Echo (ping) request  id=0x0001, seq=3232/40972, ttl=6 (no response found!)
7940 104.702134   172.16.17.178    47.246.174.23    ICMP     554 Echo (ping) request  id=0x0001, seq=3231/40716, ttl=5 (no response found!)
7936 104.651299   172.16.17.178    47.246.174.23    ICMP     554 Echo (ping) request  id=0x0001, seq=3230/40460, ttl=4 (no response found!)
7930 104.601830   172.16.17.178    47.246.174.23    ICMP     554 Echo (ping) request  id=0x0001, seq=3229/40204, ttl=3 (no response found!)
7927 104.551824   172.16.17.178    47.246.174.23    ICMP     554 Echo (ping) request  id=0x0001, seq=3228/39948, ttl=2 (no response found!)
7923 104.500291   172.16.17.178    47.246.174.23    ICMP     554 Echo (ping) request  id=0x0001, seq=3227/39692, ttl=1 (no response found!)
7920 104.451485   172.16.17.178    47.246.174.23    ICMP     554 Echo (ping) request  id=0x0001, seq=3226/39436, ttl=255 (no response found!)
7908 102.353411   172.16.17.178    47.246.174.23    ICMP     554 Echo (ping) request  id=0x0001, seq=3225/39180, ttl=8 (no response found!)
7902 102.303461   172.16.17.178    47.246.174.23    ICMP     554 Echo (ping) request  id=0x0001, seq=3224/38924, ttl=7 (no response found!)
7898 102.253262   172.16.17.178    47.246.174.23    ICMP     554 Echo (ping) request  id=0x0001, seq=3223/38668, ttl=6 (no response found!)
7893 102.202296   172.16.17.178    47.246.174.23    ICMP     554 Echo (ping) request  id=0x0001, seq=3222/38412, ttl=5 (no response found!)
```

ttl, checksum and identification change

6. **Which fields stay constant? Which of the fields *must* stay constant? Which fields must change? Why?**

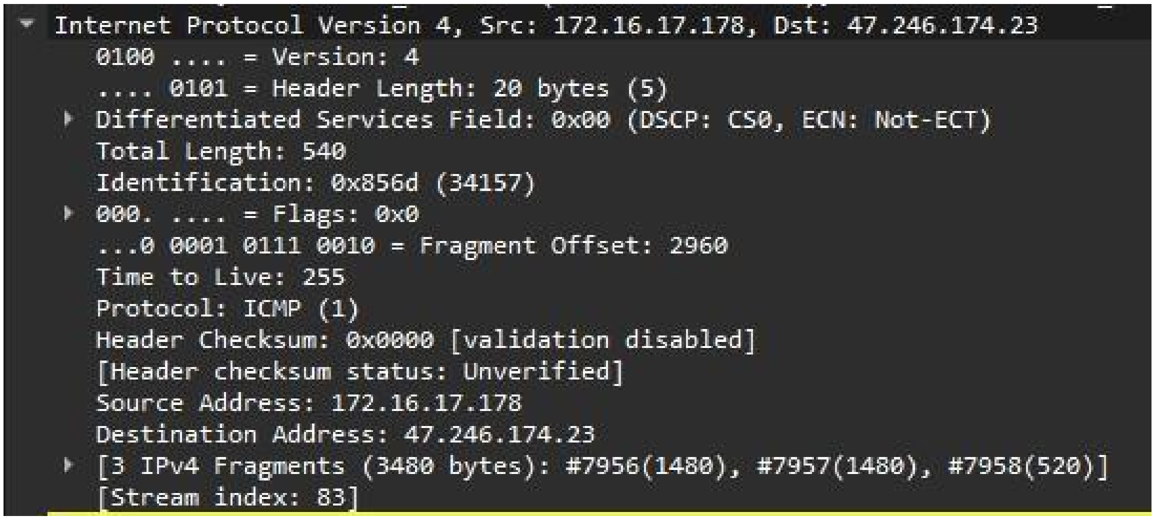


```
5080 51.895728    172.31.70.33     172.16.17.178    ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
7958 106.952431   172.16.17.178    47.246.174.23    ICMP     554 Echo (ping) request  id=0x0001, seq=3235/41740, ttl=255 (no response found!)
7951 104.853376   172.16.17.178    47.246.174.23    ICMP     554 Echo (ping) request  id=0x0001, seq=3234/41484, ttl=8 (no response found!)
7948 104.803590   172.16.17.178    47.246.174.23    ICMP     554 Echo (ping) request  id=0x0001, seq=3233/41228, ttl=7 (no response found!)
7943 104.753800   172.16.17.178    47.246.174.23    ICMP     554 Echo (ping) request  id=0x0001, seq=3232/40972, ttl=6 (no response found!)
7940 104.702134   172.16.17.178    47.246.174.23    ICMP     554 Echo (ping) request  id=0x0001, seq=3231/40716, ttl=5 (no response found!)
7936 104.651299   172.16.17.178    47.246.174.23    ICMP     554 Echo (ping) request  id=0x0001, seq=3230/40460, ttl=4 (no response found!)
7930 104.601830   172.16.17.178    47.246.174.23    ICMP     554 Echo (ping) request  id=0x0001, seq=3229/40204, ttl=3 (no response found!)
7927 104.551824   172.16.17.178    47.246.174.23    ICMP     554 Echo (ping) request  id=0x0001, seq=3228/39948, ttl=2 (no response found!)
7923 104.500291   172.16.17.178    47.246.174.23    ICMP     554 Echo (ping) request  id=0x0001, seq=3227/39692, ttl=1 (no response found!)
7920 104.451485   172.16.17.178    47.246.174.23    ICMP     554 Echo (ping) request  id=0x0001, seq=3226/39436, ttl=255 (no response found!)
7908 102.353411   172.16.17.178    47.246.174.23    ICMP     554 Echo (ping) request  id=0x0001, seq=3225/39180, ttl=8 (no response found!)
7902 102.303461   172.16.17.178    47.246.174.23    ICMP     554 Echo (ping) request  id=0x0001, seq=3224/38924, ttl=7 (no response found!)
7898 102.253262   172.16.17.178    47.246.174.23    ICMP     554 Echo (ping) request  id=0x0001, seq=3223/38668, ttl=6 (no response found!)
7893 102.202296   172.16.17.178    47.246.174.23    ICMP     554 Echo (ping) request  id=0x0001, seq=3222/38412, ttl=5 (no response found!)
```

source address and destination address and ICMP stay constant. source and destination needs to stay constant. however when data is fragmented, the identification, ttl and checksum change.

Next (with the packets still sorted by source address) find the series of ICMP TTL exceeded replies sent to your computer by the nearest (first hop) router.

7. **What is the value in the Identification field and the TTL field?**



```
▾ Internet Protocol Version 4, Src: 172.16.17.178, Dst: 47.246.174.23
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 540
    Identification: 0x856d (34157)
  ▸ 000. .... = Flags: 0x0
    ...0 0001 0111 0010 = Fragment Offset: 2960
    Time to Live: 255
    Protocol: ICMP (1)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 172.16.17.178
    Destination Address: 47.246.174.23
  ▸ [3 IPv4 Fragments (3480 bytes): #7956(1480), #7957(1480), #7958(520)]
    [Stream index: 83]
```

identification field:34157
ttl:255