LAB-6

1.Pick an IP message from Wireshark capture for ICMP (from ping/ traceroute). What is the value of the upper layer protocol field? What is the IP address of your computer shown?

Value of the upper layer protocol field = 1

IP address of my computer = 192.168.0.7

```
PS C:\Users\gurus> ping google.com

Pinging google.com [142.250.76.78] with 32 bytes of data:
Reply from 142.250.76.78: bytes=32 time=60ms TTL=111
Reply from 142.250.76.78: bytes=32 time=53ms TTL=111
Reply from 142.250.76.78: bytes=32 time=85ms TTL=111
Reply from 142.250.76.78: bytes=32 time=55ms TTL=111

Ping statistics for 142.250.76.78:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 53ms, Maximum = 85ms, Average = 63ms
PS C:\Users\gurus>
```

No.	Time	Source	Destination	Protocol	Length	Info
8508	17.011655	192.168.0.7	142.250.76.78	ICMP	74	Echo (ping) request id=0x0001, seq=20/5120, ttl=128 (reply in 8509)
8509	17.072078	142.250.76.78	192.168.0.7	ICMP	74	Echo (ping) reply id=0x0001, seq=20/5120, ttl=111 (request in 8508)
8526	18.016051	192.168.0.7	142.250.76.78	ICMP	74	Echo (ping) request id=0x0001, seq=21/5376, ttl=128 (reply in 8527)
8527	18.069741	142.250.76.78	192.168.0.7	ICMP	74	Echo (ping) reply id=0x0001, seq=21/5376, ttl=111 (request in 8526)
8528	19.025128	192.168.0.7	142.250.76.78	ICMP	74	Echo (ping) request id=0x0001, seq=22/5632, ttl=128 (reply in 8529)
8529	19.110229	142.250.76.78	192.168.0.7	ICMP	74	Echo (ping) reply id=0x0001, seq=22/5632, ttl=111 (request in 8528)
8532	20.029766	192.168.0.7	142.250.76.78	ICMP	74	Echo (ping) request id=0x0001, seq=23/5888, ttl=128 (reply in 8533)
8533	20.085436	142.250.76.78	192.168.0.7	ICMP	74	Echo (ping) reply id=0x0001, seq=23/5888, ttl=111 (request in 8532)

```
> Frame 8508: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{309848B1-796F-4478-94CE-2AE7C9DA600A}, id 0
> Ethernet II, Src: IntelCor_8a:c8:39 (5c:87:9c:8a:c8:39), Dst: D-LinkIn_a7:c6:ab (f4:8c:eb:a7:c6:ab)
v Internet Protocol Version 4, Src: 192.168.0.7, Dst: 142.250.76.78
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0x8cd7 (36055)
  > Flags: 0x0000
    Fragment offset: 0
    Time to live: 128
    Protocol: ICMP (1)
    Header checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
```

IP Address

Protocol Number

2. How many bytes are there in the IP datagram? How did you determine this value?

Header Length= 20 bytes

IP datagram length= (total length-header length) = 60-20=40 bytes

No.	Time	Source	Destination	Protocol	Length	Info
8508	17.011655	192.168.0.7	142.250.76.78	ICMP	74	Echo (ping) request id=0x0001, seq=20/5120, ttl=128 (reply in 8509)
8509	17.072078	142.250.76.78	192.168.0.7	ICMP	74	Echo (ping) reply id=0x0001, seq=20/5120, ttl=111 (request in 8508)
8526	18.016051	192.168.0.7	142.250.76.78	ICMP	74	Echo (ping) request id=0x0001, seq=21/5376, ttl=128 (reply in 8527)
8527	18.069741	142.250.76.78	192.168.0.7	ICMP	74	Echo (ping) reply id=0x0001, seq=21/5376, ttl=111 (request in 8526)
8528	19.025128	192.168.0.7	142.250.76.78	ICMP	74	Echo (ping) request id=0x0001, seq=22/5632, ttl=128 (reply in 8529)
8529	19.110229	142.250.76.78	192.168.0.7	ICMP	74	Echo (ping) reply id=0x0001, seq=22/5632, ttl=111 (request in 8528)
8532	20.029766	192.168.0.7	142.250.76.78	ICMP	74	Echo (ping) request id=0x0001, seq=23/5888, ttl=128 (reply in 8533)
8533	20.085436	142.250.76.78	192.168.0.7	ICMP	74	Echo (ping) reply id=0x0001, seq=23/5888, ttl=111 (request in 8532)

```
> Frame 8508: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{309848B1-796F-4478-94CE-2AE7C9DA600A}, id 0
> Ethernet II, Src: IntelCor_8a:c8:39 (5c:87:9c:8a:c8:39), Dst: D-LinkIn_a7:c6:ab (f4:8c:eb:a7:c6:ab)
v Internet Protocol Version 4, Src: 192.168.0.7, Dst: 142.250.76.78
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0x8cd7 (36055)
  > Flags: 0x0000
    Fragment offset: 0
    Time to live: 128
    Protocol: ICMP (1)
    Header checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
```

3. IS the datagram fragmented? How did you know?

No, the fragment offset is set to zero

No.	Time	Source	Destination	Protocol	Length	Info
8508	17.011655	192.168.0.7	142.250.76.78	ICMP	74	Echo (ping) request id=0x0001, seq=20/5120, ttl=128 (reply in 8509)
8509	17.072078	142.250.76.78	192.168.0.7	ICMP	74	Echo (ping) reply id=0x0001, seq=20/5120, ttl=111 (request in 8508)
8526	18.016051	192.168.0.7	142.250.76.78	ICMP	74	Echo (ping) request id=0x0001, seq=21/5376, ttl=128 (reply in 8527)
8527	18.069741	142.250.76.78	192.168.0.7	ICMP	74	Echo (ping) reply id=0x0001, seq=21/5376, ttl=111 (request in 8526)
8528	19.025128	192.168.0.7	142.250.76.78	ICMP	74	Echo (ping) request id=0x0001, seq=22/5632, ttl=128 (reply in 8529)
8529	19.110229	142.250.76.78	192.168.0.7	ICMP	74	Echo (ping) reply id=0x0001, seq=22/5632, ttl=111 (request in 8528)
8532	20.029766	192.168.0.7	142.250.76.78	ICMP	74	Echo (ping) request id=0x0001, seq=23/5888, ttl=128 (reply in 8533)
8533	20.085436	142.250.76.78	192.168.0.7	ICMP	74	Echo (ping) reply id=0x0001, seq=23/5888, ttl=111 (request in 8532)


```
> Frame 8508: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{309848B1-796F-4478-94CE-2AE7C9DA600A}, id 0
> Ethernet II, Src: IntelCor_8a:c8:39 (5c:87:9c:8a:c8:39), Dst: D-LinkIn_a7:c6:ab (f4:8c:eb:a7:c6:ab)
v Internet Protocol Version 4, Src: 192.168.0.7, Dst: 142.250.76.78
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0x8cd7 (36055)
  > Flags: 0x0000
    Fragment offset: 0
    Time to live: 128
    Protocol: ICMP (1)
    Header checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
```

4. Which fields stay constant between IP datagrams? Which do not?

From the screenshots below we can say that,

Constant fields:

Version, Header length, Source IP, Destination IP, differentiated service, Protocol number, Header checksum,

Fields that change: Identification, TTL (Here TTL Remains unchanged)

No.	Time	Source	Destination	Protocol	Length	Info
8508	17.011655	192.168.0.7	142.250.76.78	ICMP	74	Echo (ping) request id=0x0001, seq=20/5120, ttl=128 (reply in 8509)
8509	17.072078	142.250.76.78	192.168.0.7	ICMP	74	Echo (ping) reply id=0x0001, seq=20/5120, ttl=111 (request in 8508)
8526	18.016051	192.168.0.7	142.250.76.78	ICMP	74	Echo (ping) request id=0x0001, seq=21/5376, ttl=128 (reply in 8527)
8527	18.069741	142.250.76.78	192.168.0.7	ICMP	74	Echo (ping) reply id=0x0001, seq=21/5376, ttl=111 (request in 8526)
8528	19.025128	192.168.0.7	142.250.76.78	ICMP	74	Echo (ping) request id=0x0001, seq=22/5632, ttl=128 (reply in 8529)
8529	19.110229	142.250.76.78	192.168.0.7	ICMP	74	Echo (ping) reply id=0x0001, seq=22/5632, ttl=111 (request in 8528)
8532	20.029766	192.168.0.7	142.250.76.78	ICMP	74	Echo (ping) request id=0x0001, seq=23/5888, ttl=128 (reply in 8533)
8533	20.085436	142.250.76.78	192.168.0.7	ICMP	74	Echo (ping) reply id=0x0001, seq=23/5888, ttl=111 (request in 8532)

```
> Frame 8508: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{309848B1-796F-4478-94CE-2AE7C9DA600A}, id 0
> Ethernet II, Src: IntelCor_8a:c8:39 (5c:87:9c:8a:c8:39), Dst: D-LinkIn_a7:c6:ab (f4:8c:eb:a7:c6:ab)
v Internet Protocol Version 4, Src: 192.168.0.7, Dst: 142.250.76.78
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0x8cd7 (36055)
  > Flags: 0x0000
    Fragment offset: 0
    Time to live: 128
    Protocol: ICMP (1)
    Header checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.0.7
    Destination: 142.250.76.78
> Internet Control Message Protocol
```

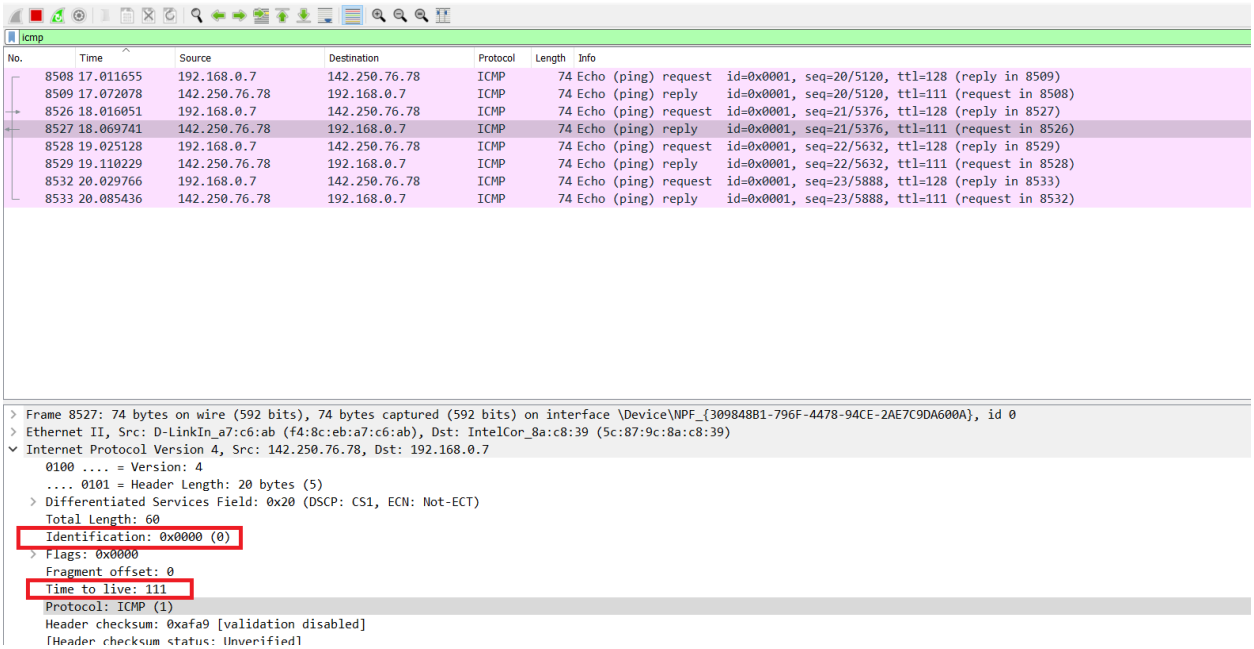
No.	Time	Source	Destination	Protocol	Length	Info
8508	17.011655	192.168.0.7	142.250.76.78	ICMP	74	Echo (ping) request id=0x0001, seq=20/5120, ttl=128 (reply in 8509)
8509	17.072078	142.250.76.78	192.168.0.7	ICMP	74	Echo (ping) reply id=0x0001, seq=20/5120, ttl=111 (request in 8508)
8526	18.016051	192.168.0.7	142.250.76.78	ICMP	74	Echo (ping) request id=0x0001, seq=21/5376, ttl=128 (reply in 8527)
8527	18.069741	142.250.76.78	192.168.0.7	ICMP	74	Echo (ping) reply id=0x0001, seq=21/5376, ttl=111 (request in 8526)
8528	19.025128	192.168.0.7	142.250.76.78	ICMP	74	Echo (ping) request id=0x0001, seq=22/5632, ttl=128 (reply in 8529)
8529	19.110229	142.250.76.78	192.168.0.7	ICMP	74	Echo (ping) reply id=0x0001, seq=22/5632, ttl=111 (request in 8528)
8532	20.029766	192.168.0.7	142.250.76.78	ICMP	74	Echo (ping) request id=0x0001, seq=23/5888, ttl=128 (reply in 8533)
8533	20.085436	142.250.76.78	192.168.0.7	ICMP	74	Echo (ping) reply id=0x0001, seq=23/5888, ttl=111 (request in 8532)

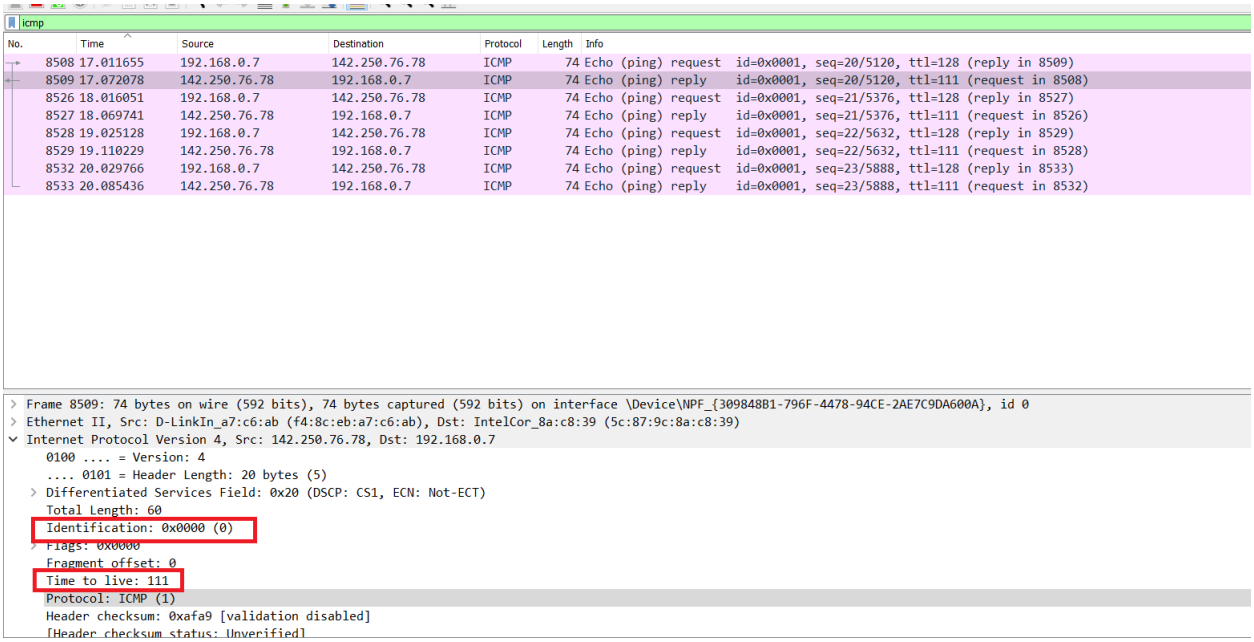
```
> Frame 8526: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{309848B1-796F-4478-94CE-2AE7C9DA600A}, id 0
> Ethernet II, Src: IntelCor_8a:c8:39 (5c:87:9c:8a:c8:39), Dst: D-LinkIn_a7:c6:ab (f4:8c:eb:a7:c6:ab)
v Internet Protocol Version 4, Src: 192.168.0.7, Dst: 142.250.76.78
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0x8cd8 (36056)
  > Flags: 0x0000
    Fragment offset: 0
    Time to live: 128
    Protocol: ICMP (1)
    Header checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.0.7
    Destination: 142.250.76.78
```

5. What is the value of the identification and time to live fields of the datagram you picked? Do they remain unchanged for the TTL exceeded replies from the first router?

Identification number =0, TTL=111.

In my test, these fields unchanged and shown below





icmp

No.	Time	Source	Destination	Protocol	Length	Info
8508	17.011655	192.168.0.7	142.250.76.78	ICMP	74	Echo (ping) request id=0x0001, seq=20/5120, ttl=128 (reply in 8509)
8509	17.072078	142.250.76.78	192.168.0.7	ICMP	74	Echo (ping) reply id=0x0001, seq=20/5120, ttl=111 (request in 8508)
8526	18.016051	192.168.0.7	142.250.76.78	ICMP	74	Echo (ping) request id=0x0001, seq=21/5376, ttl=128 (reply in 8527)
8527	18.069741	142.250.76.78	192.168.0.7	ICMP	74	Echo (ping) reply id=0x0001, seq=21/5376, ttl=111 (request in 8526)
8528	19.025128	192.168.0.7	142.250.76.78	ICMP	74	Echo (ping) request id=0x0001, seq=22/5632, ttl=128 (reply in 8529)
8529	19.110229	142.250.76.78	192.168.0.7	ICMP	74	Echo (ping) reply id=0x0001, seq=22/5632, ttl=111 (request in 8528)
8532	20.029766	192.168.0.7	142.250.76.78	ICMP	74	Echo (ping) request id=0x0001, seq=23/5888, ttl=128 (reply in 8533)
8533	20.085436	142.250.76.78	192.168.0.7	ICMP	74	Echo (ping) reply id=0x0001, seq=23/5888, ttl=111 (request in 8532)

```
> Frame 8529: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{309848B1-796F-4478-94CE-2AE7C9DA600A}, id 0
> Ethernet II, Src: D-LinkIn_a7:c6:ab (f4:8c:eb:a7:c6:ab), Dst: IntelCor_8a:c8:39 (5c:87:9c:8a:c8:39)
v Internet Protocol Version 4, Src: 142.250.76.78, Dst: 192.168.0.7
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x20 (DSCP: CS1, ECN: Not-ECT)
    Total Length: 60
    Identification: 0x0000 (0)
  > Flags: 0x0000
    Fragment offset: 0
    Time to live: 111
    Protocol: ICMP (1)
    Header checksum: 0xafa9 [validation disabled]
    [Header checksum status: Unverified]
```