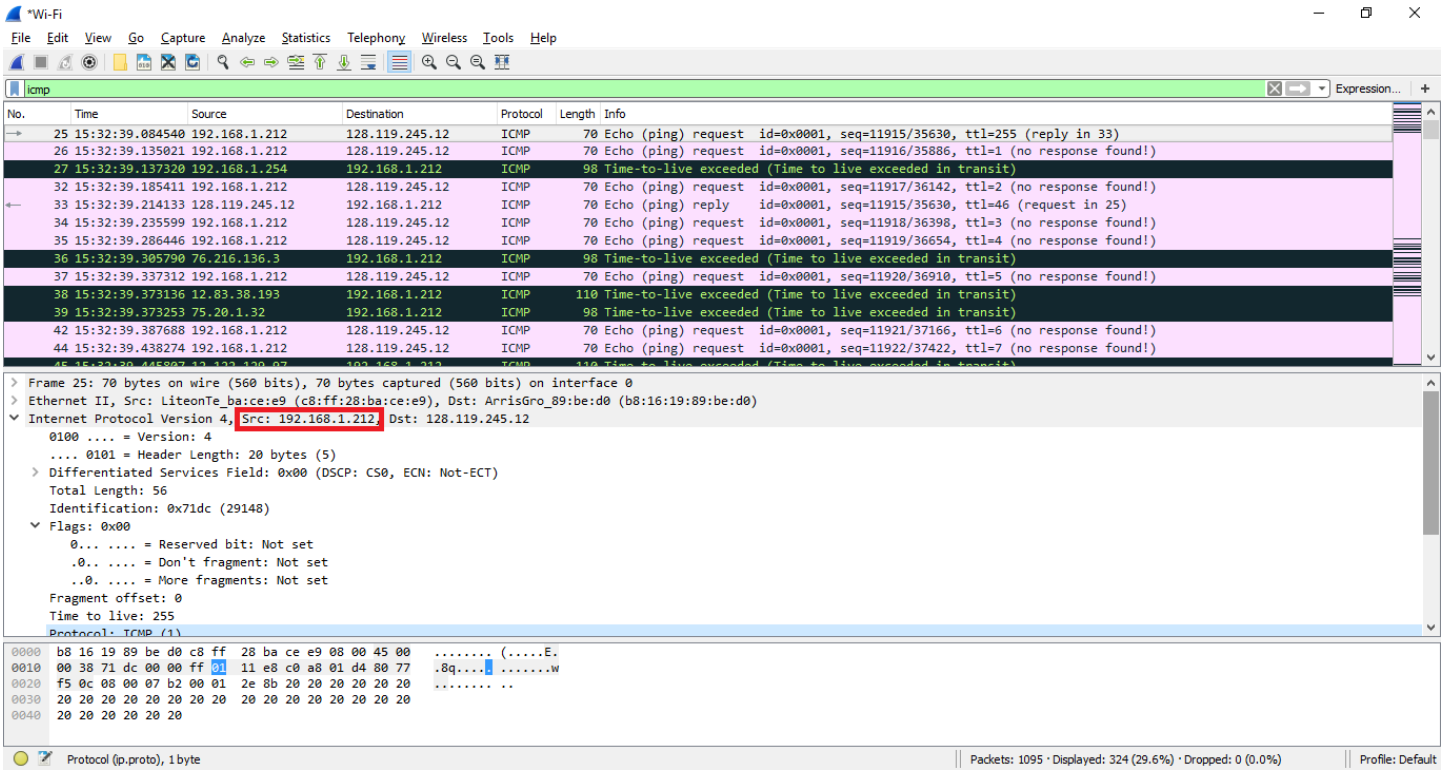
Jessica Spokoyny
Nov 19, 2016
CS 372 – Lab 4

Lab 4

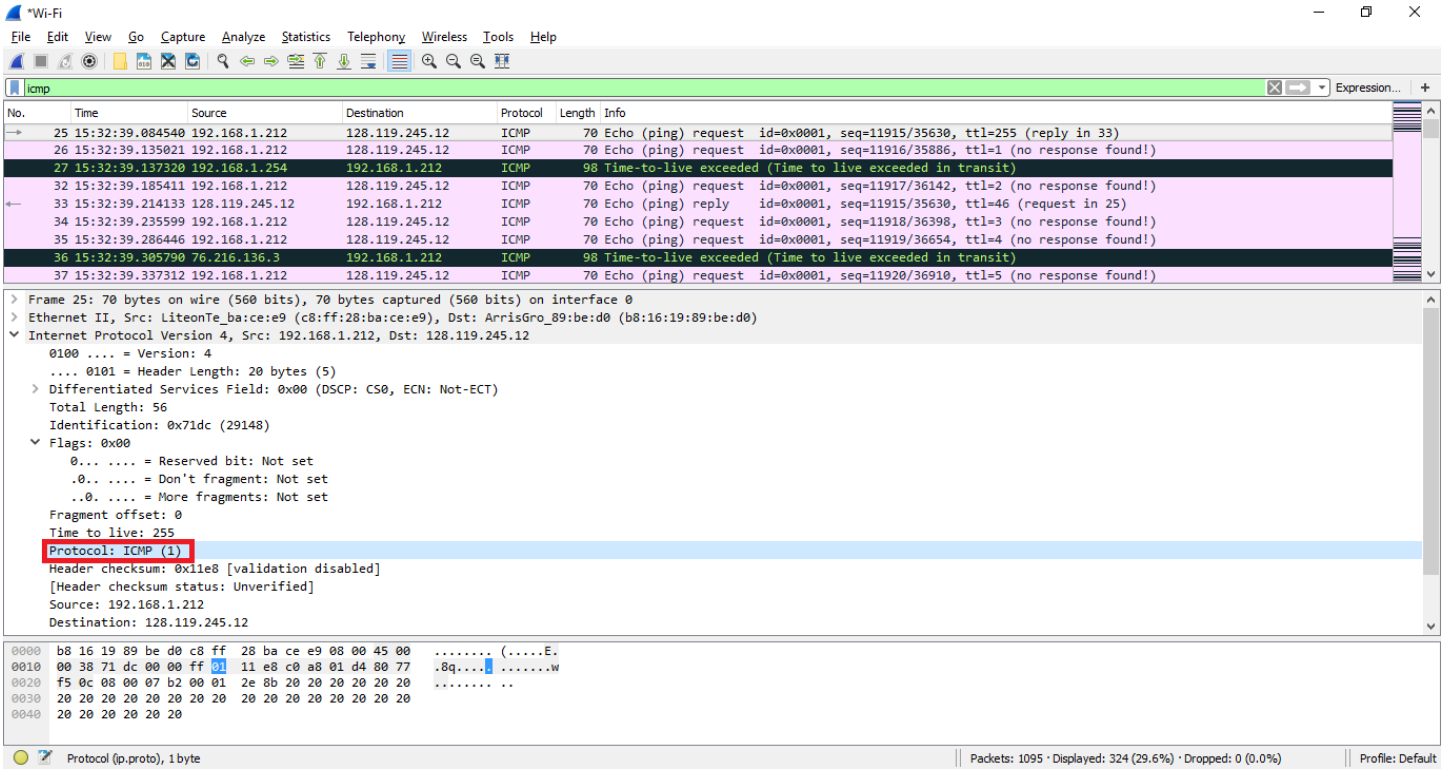
1. **What is the IP address of your computer?**

My computer's IP address is 192.168.1.212



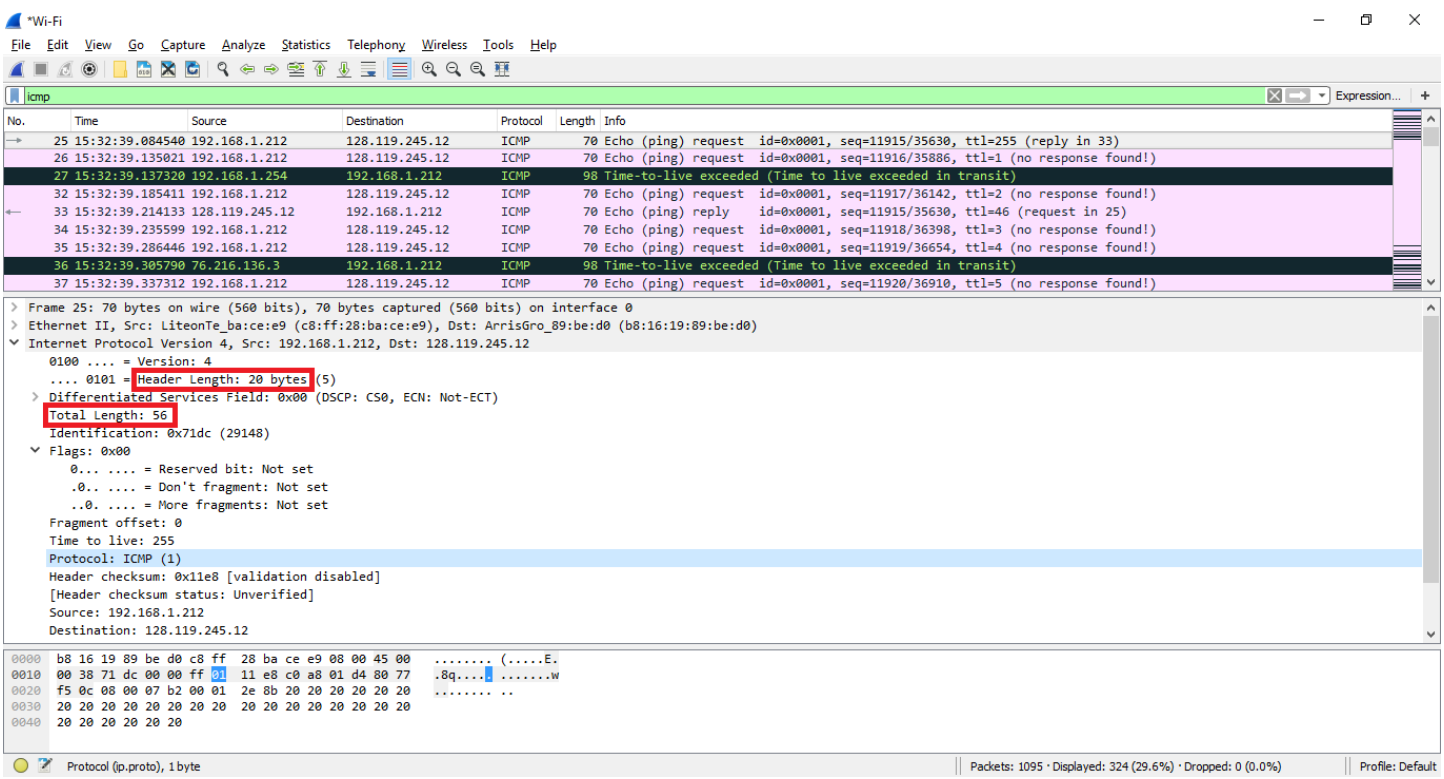
2. **Within the IP packet header, what is the value in the upper layer protocol field?**

The value in the upper layer protocol field is ICMP (1)



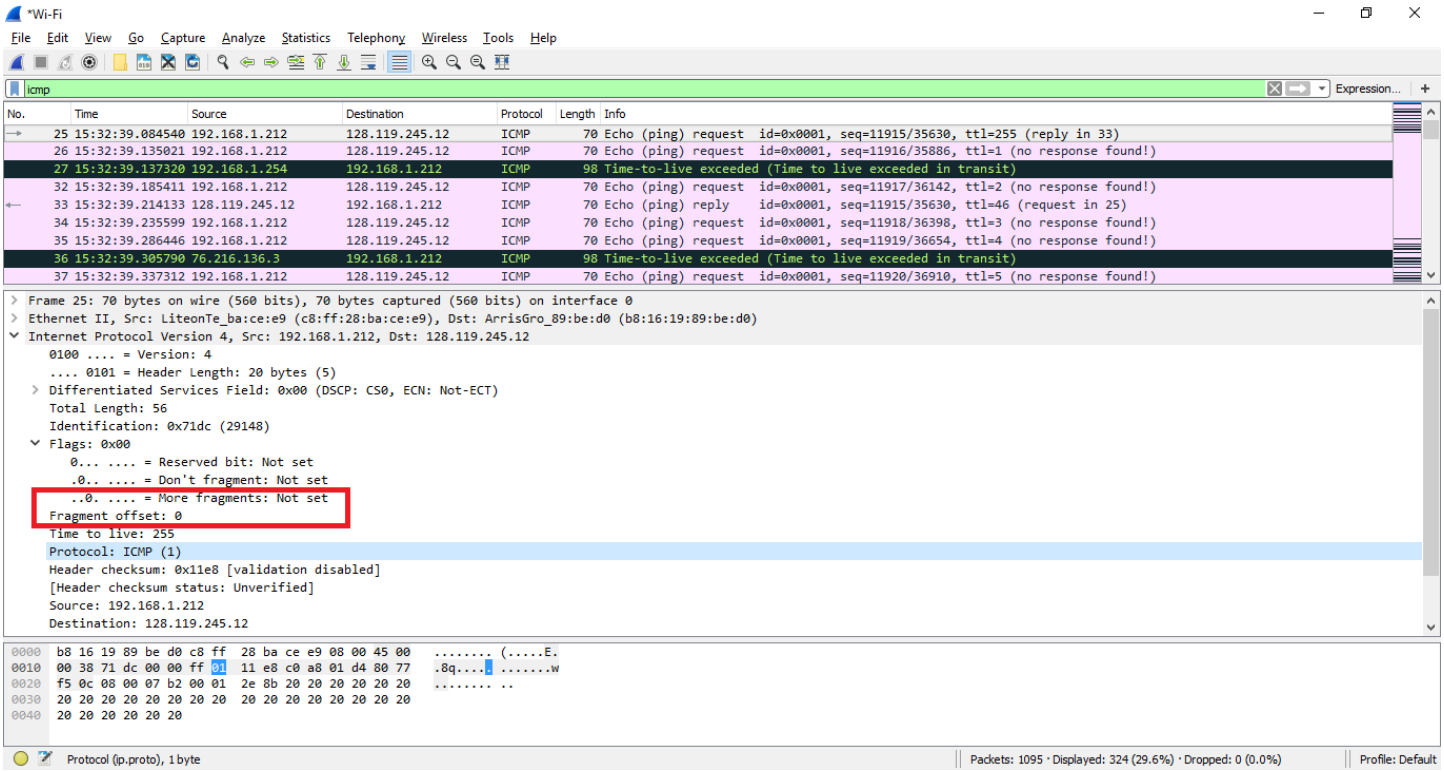
3. **How many bytes are in the IP header? How many bytes are in the payload *of the IP datagram*? Explain how you determined the number of payload bytes.**

There are 20 bytes in the IP header, and total length is 56 bytes which leaves 36 bytes in the payload of the IP datagram



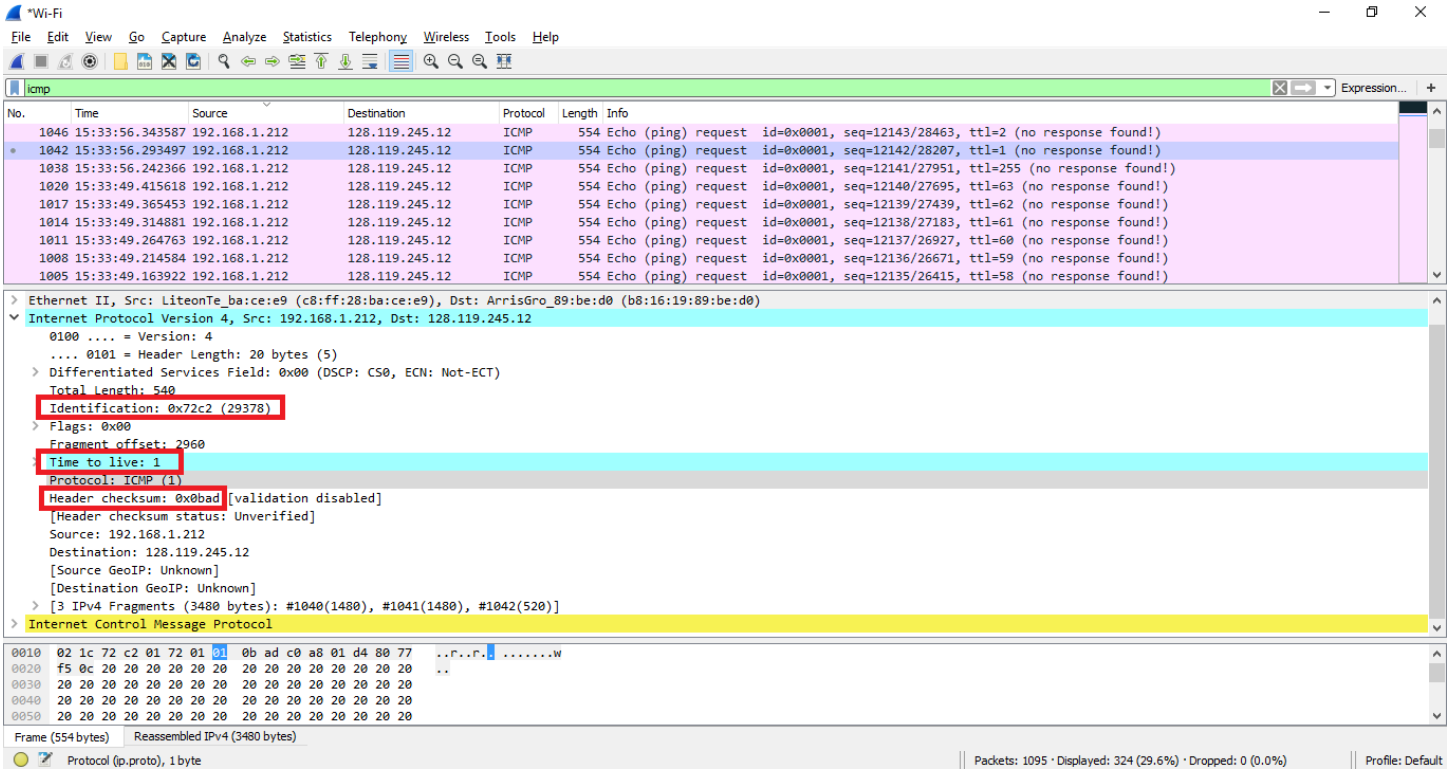
4. **Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented.**

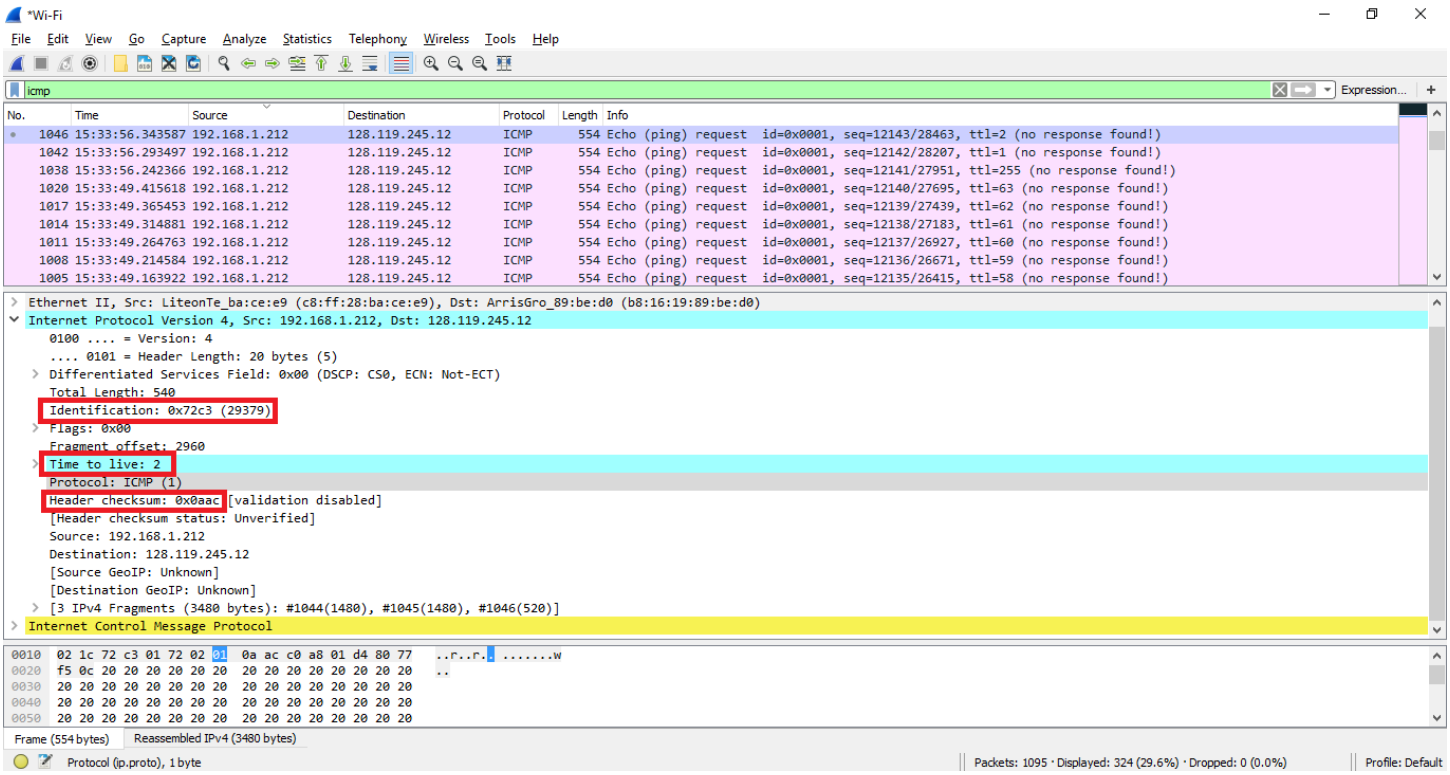
No, this IP datagram has not been fragmented. We can see that the ‘More fragments’ flag as well as the ‘fragment offset’ are zero which indicate that it is not fragmented. (more fragments set to zero indicates that this is the last packet and fragment offset set to zero means that this packet contains the beginning of the datagram)



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?**

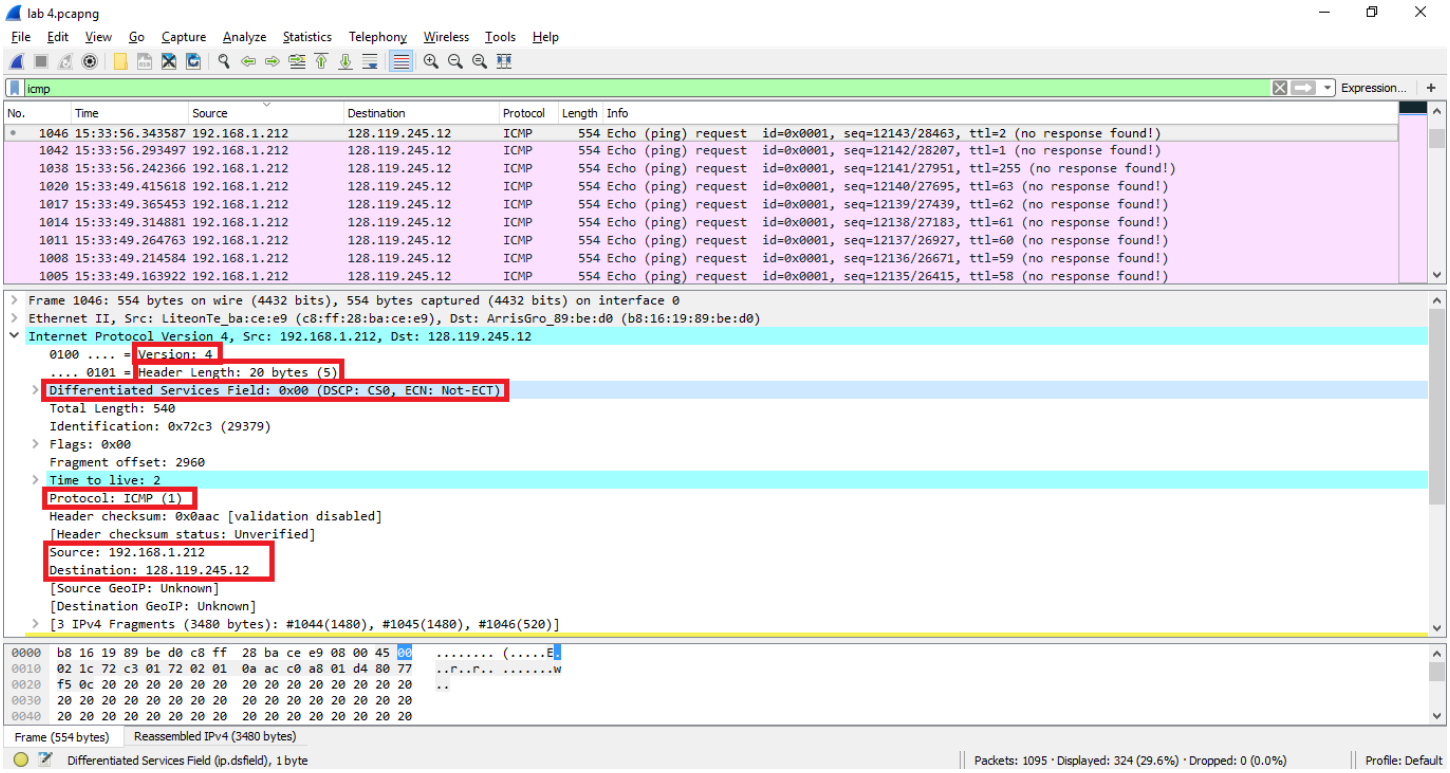
Within this series of ICMP messages sent by my computer, the ‘Identification’, ‘Time to live’, and ‘Header checksum’ fields always change from one datagram to the next.

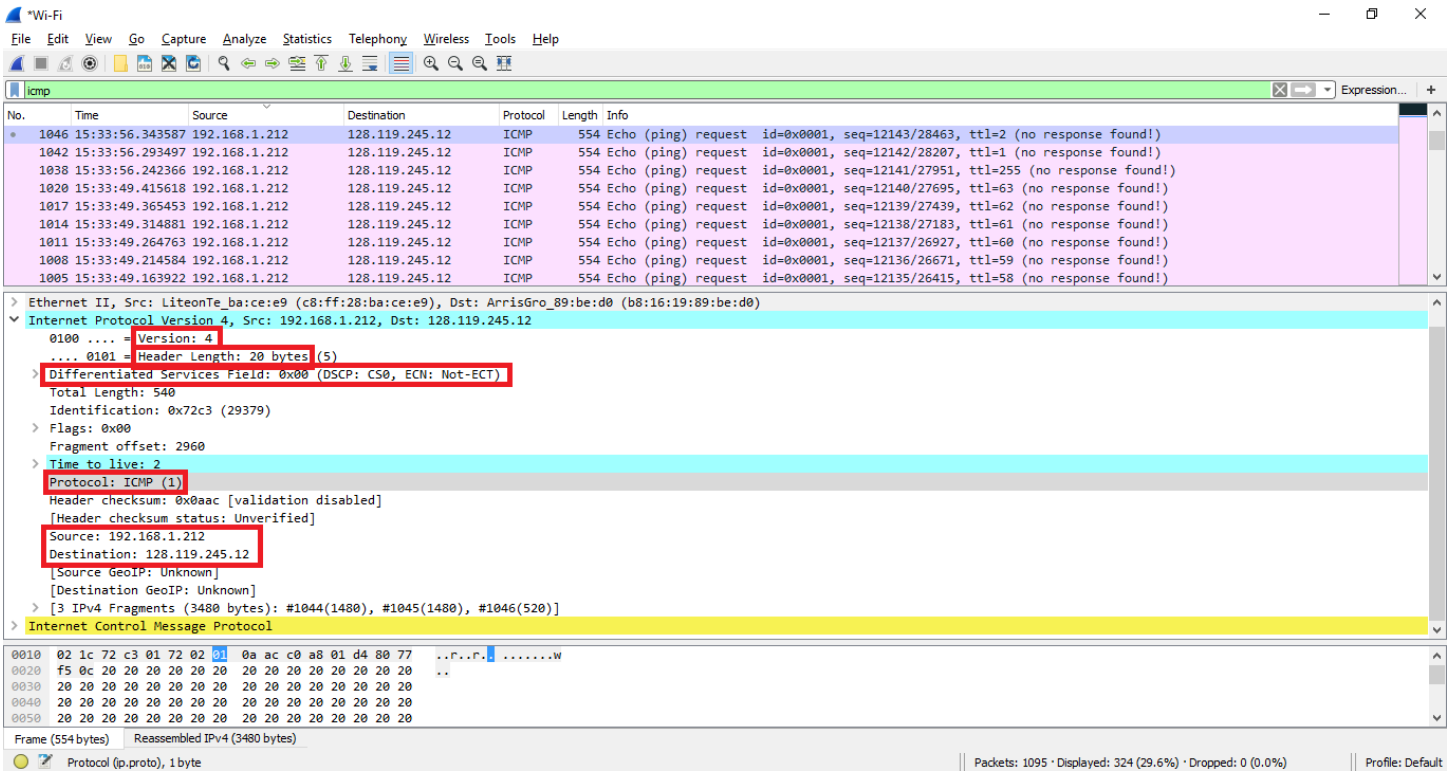




6. Which fields stay constant? Which of the fields *must* stay constant? Which fields must change? Why?

The fields that stay constant are Version, Header Length, Source, Destination, Differentiated Services Field, and Protocol





The fields that *must* stay constant are:

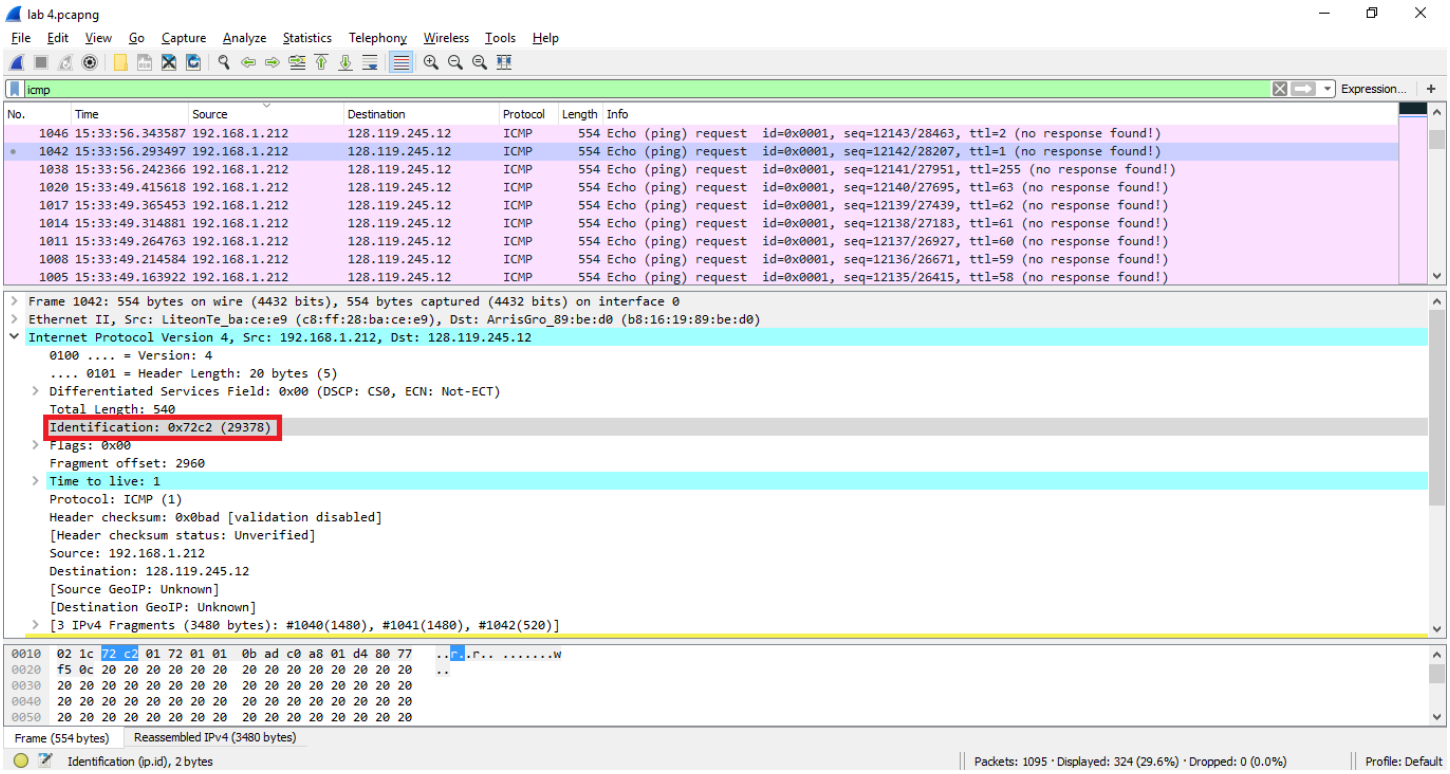
- Version: all packets use IPv4
- Header Length: all ICMP packets have the same header length
- Source: all packets are being sent from the same source
- Destination: all packets are being sent to the same destination
- Differentiated Services Field: all ICMP packets use the same type of service class
- Protocol: all ICMP packets use the same protocol

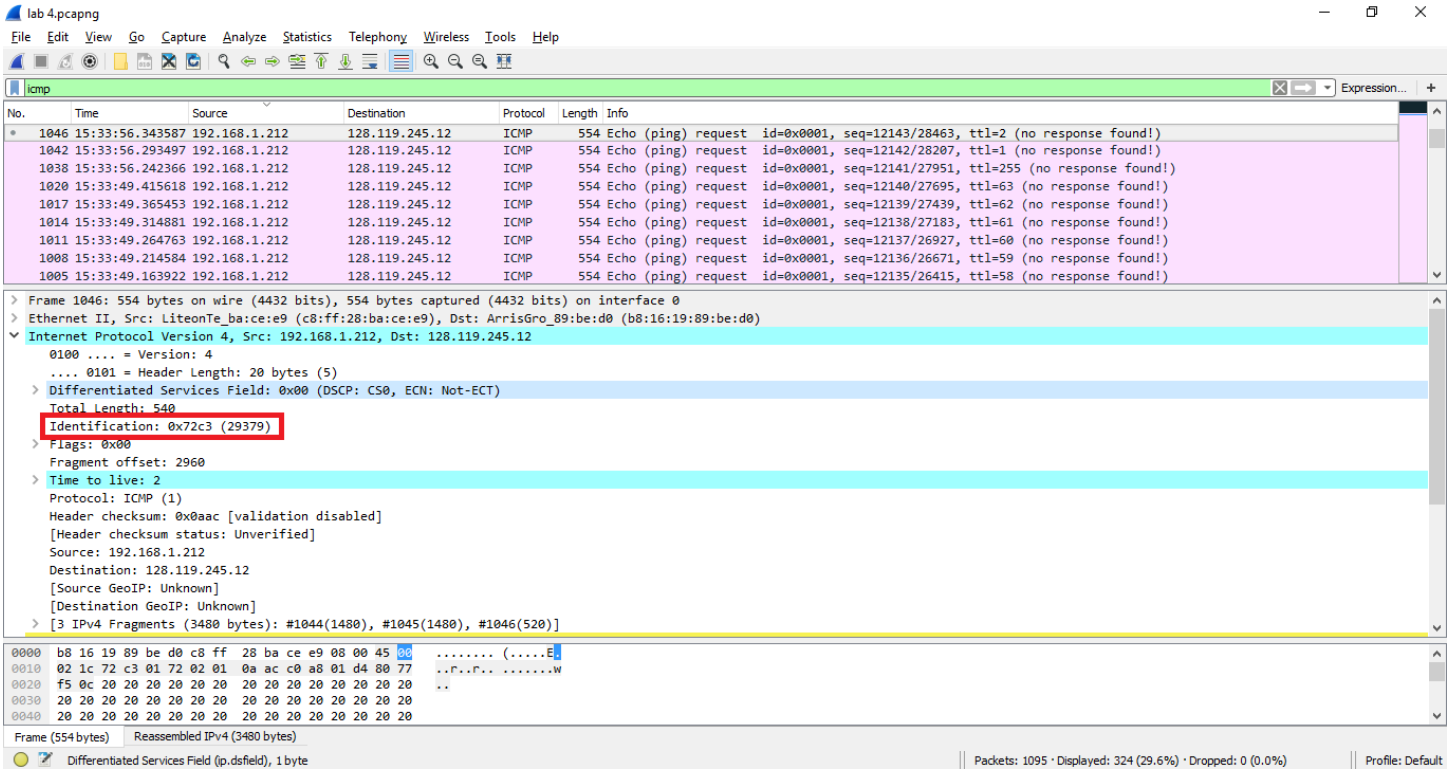
The fields that *must* change are:

- Identification: each packet must have a unique id
- Time to live: ttl is incremented with every packet
- Header checksum: the header changes so the checksum must as well

7. Describe the pattern you see in the values in the Identification field of the IP datagram

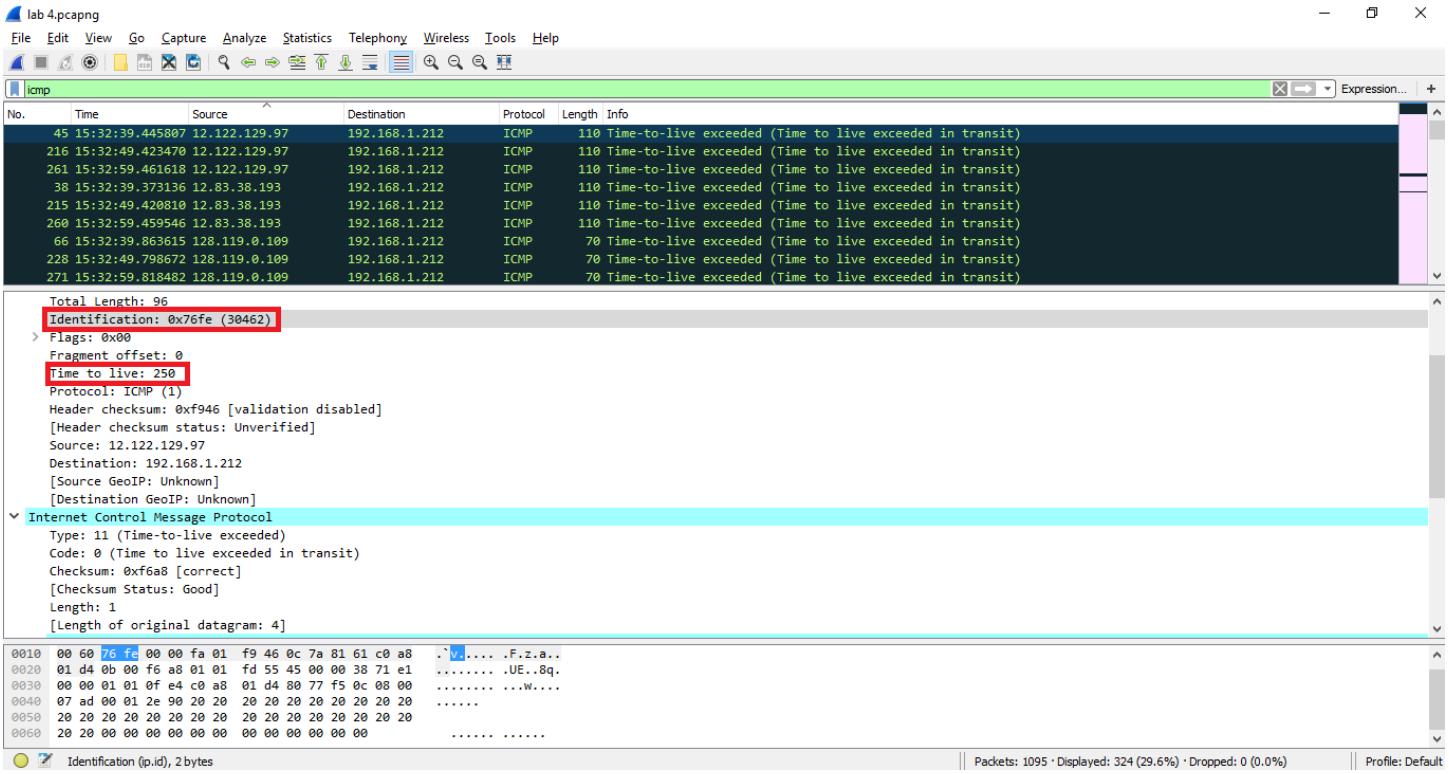
The Identification field of the IP datagram increments each time an ICMP Echo Request message is sent.





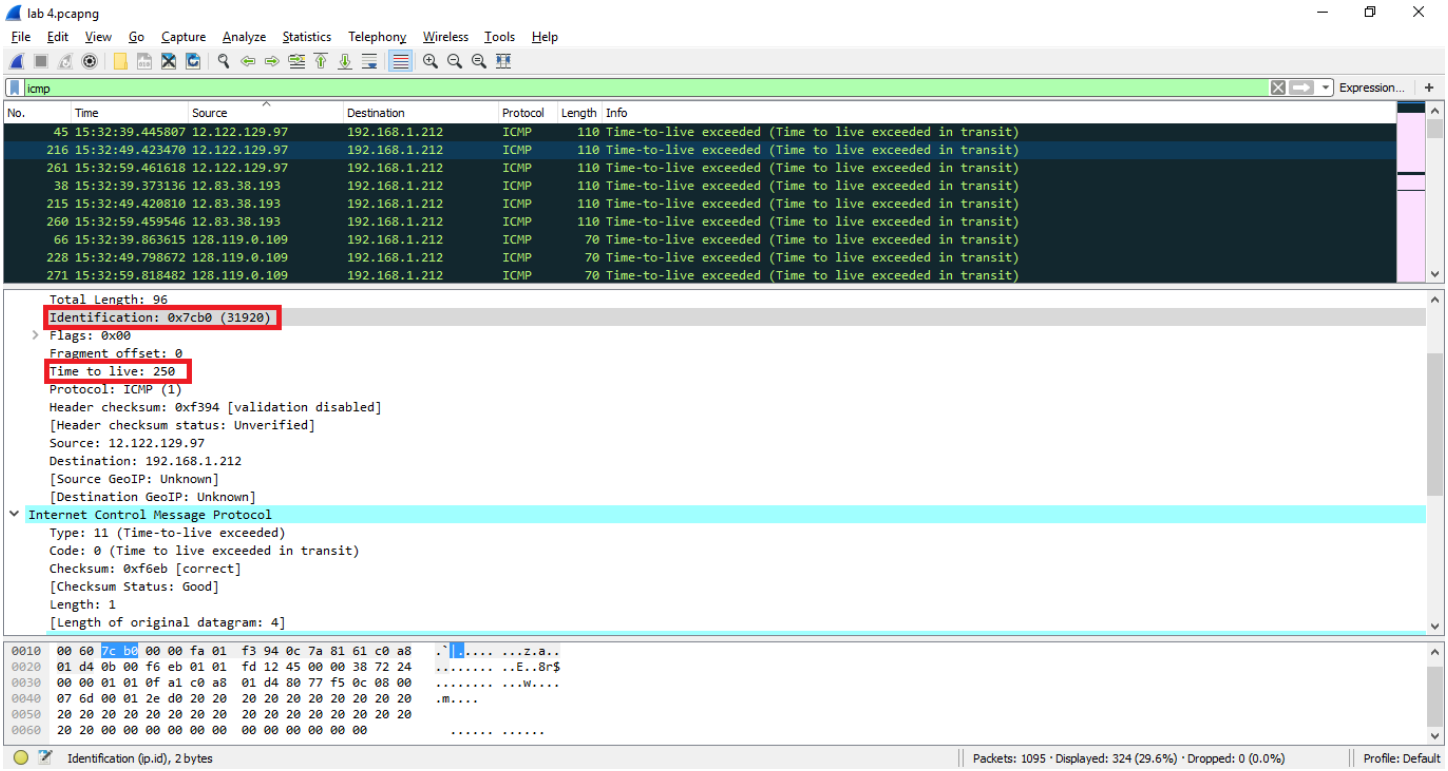
8. **What is the value in the Identification field and the TTL field?**

Identification: 0x76fe 30462
TTL: 250



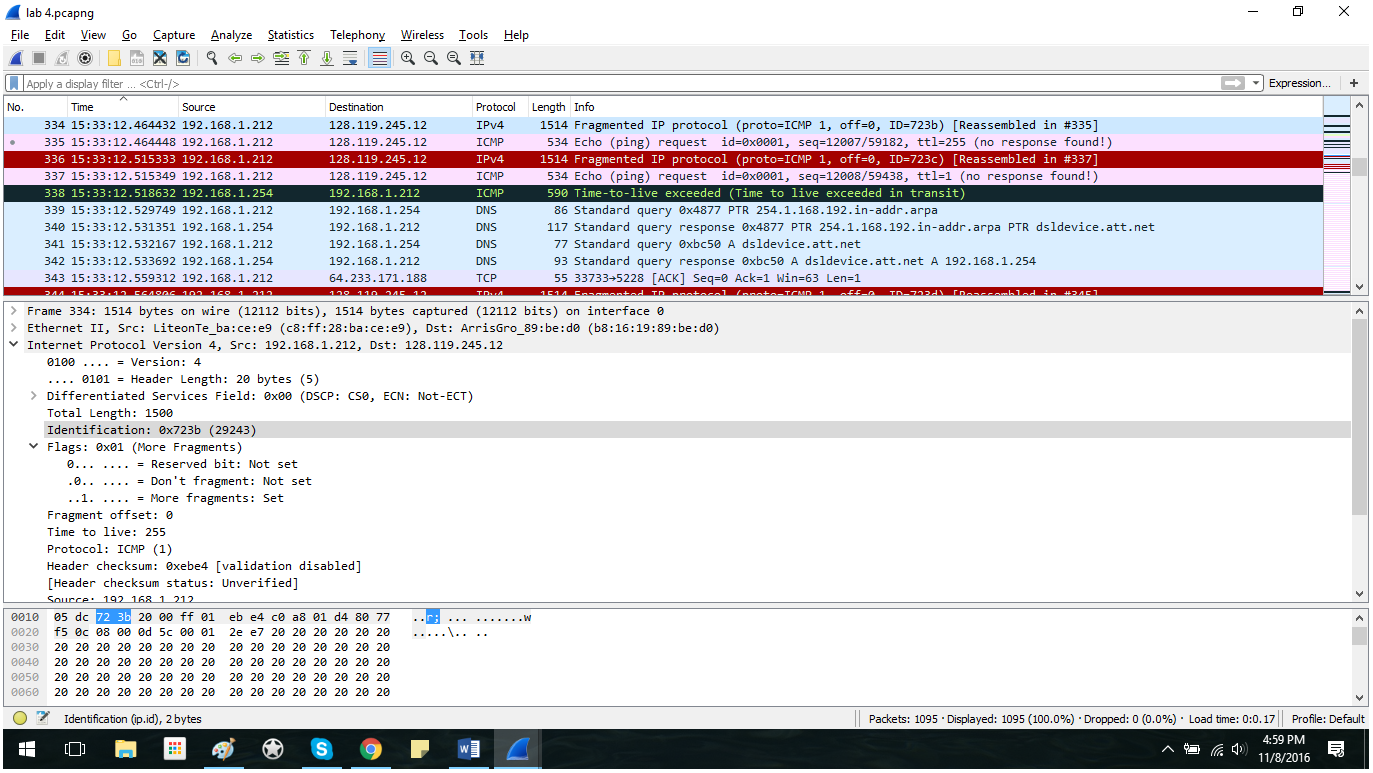
9. **Do these values remain unchanged for all of the ICMP TTL-exceeded replies sent to your computer by the nearest (first hop) router? Why?**

Each of the ICMP TTL-exceeded replies has a unique identification number. (if the identification numbers were the same it would suggest that the datagrams are actually fragments of the same datagram). The TTL field stays constant because the time to live 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?

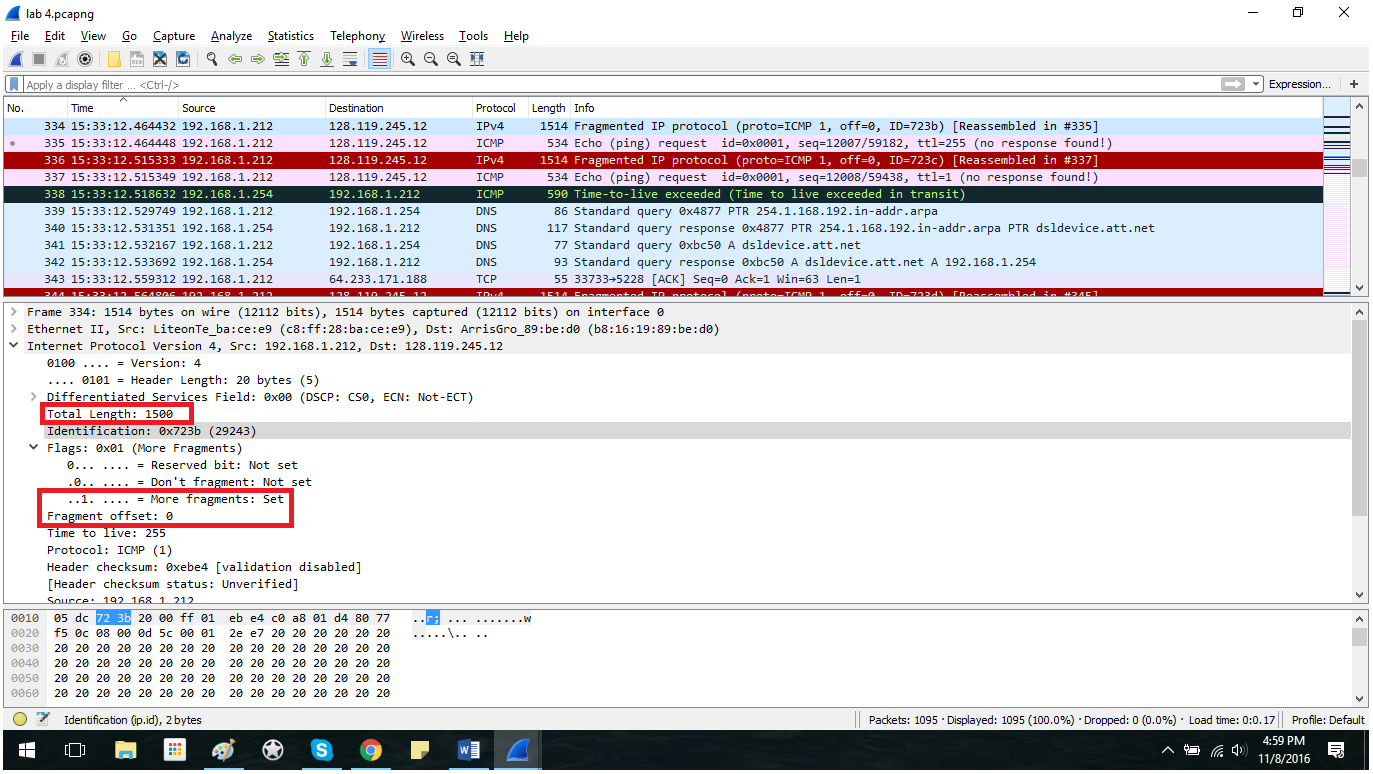
Yes, that message has been fragmented across more than one IP datagram.



11. Screenshot the first fragment of the fragmented IP datagram (with sufficient details to answer these questions). What information in the IP header indicates that the datagram

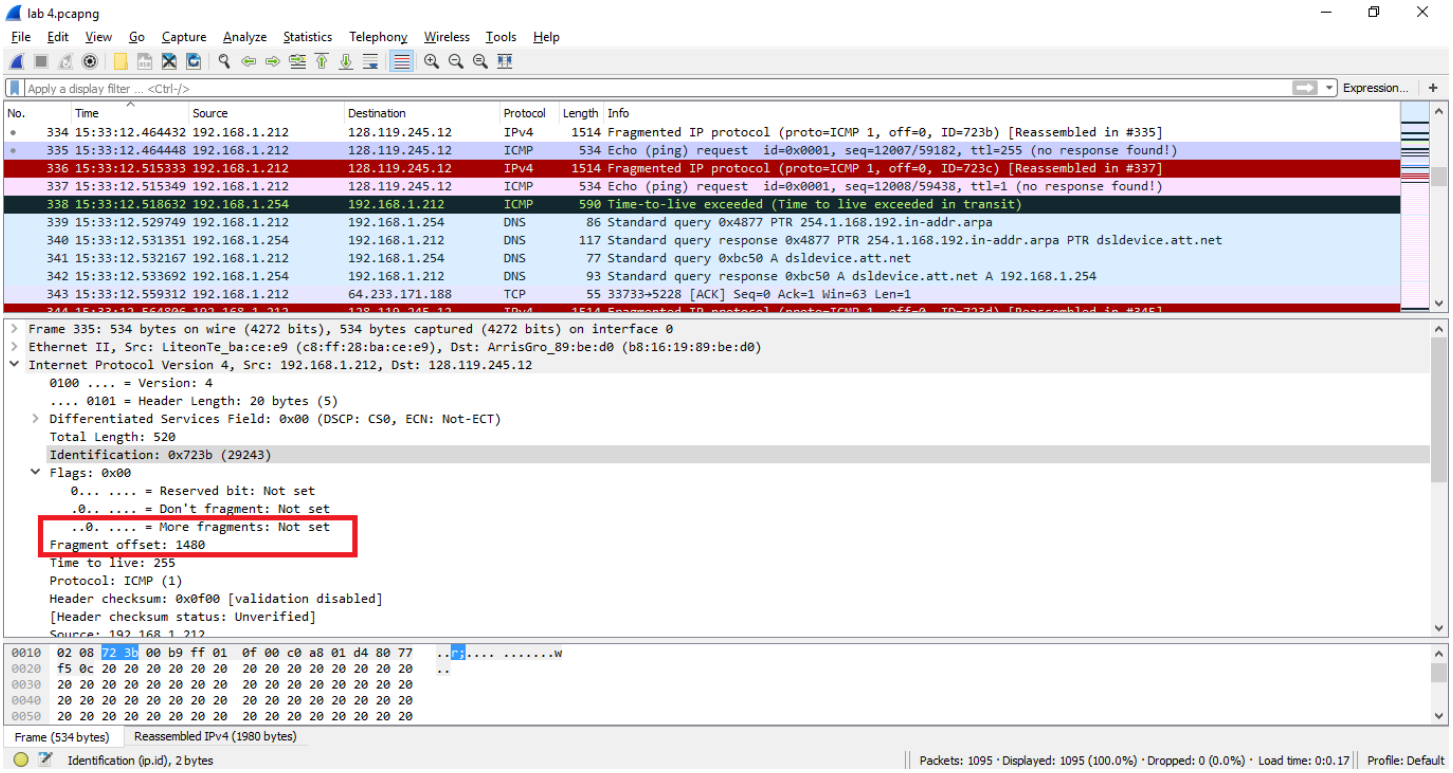
been fragmented? What information in the IP header indicates whether this is the first fragment versus a latter fragment? How long is this IP datagram?

Because the 'More fragments' flag is set, we know that the datagram has been fragmented. The Fragment offset = 0 which indicates that this is the first fragment. This IP datagram is 1500 bytes long.



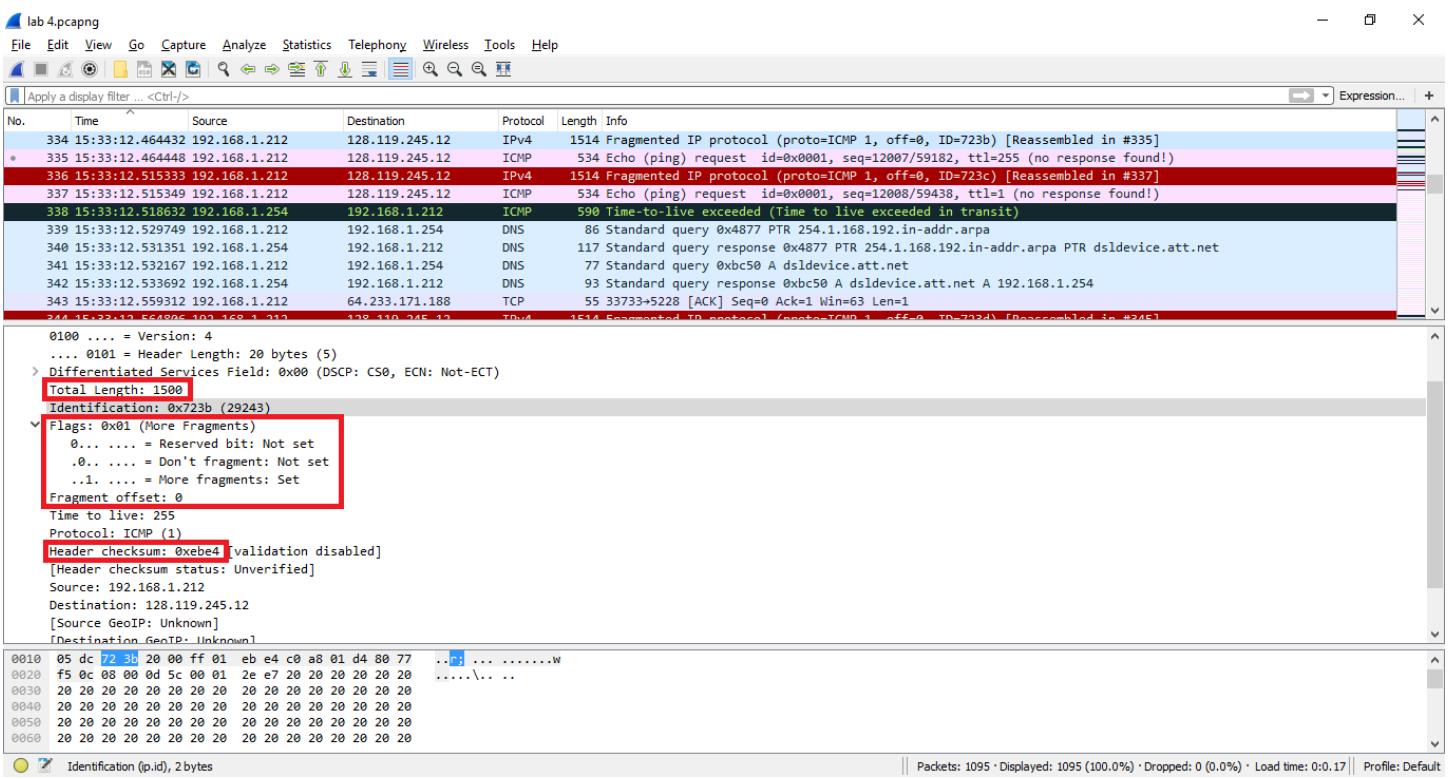
12. Screenshot the second fragment of the fragmented IP datagram (with sufficient details to answer these questions). What information in the IP header indicates that this is not the first datagram fragment? Are the more fragments? How can you tell?

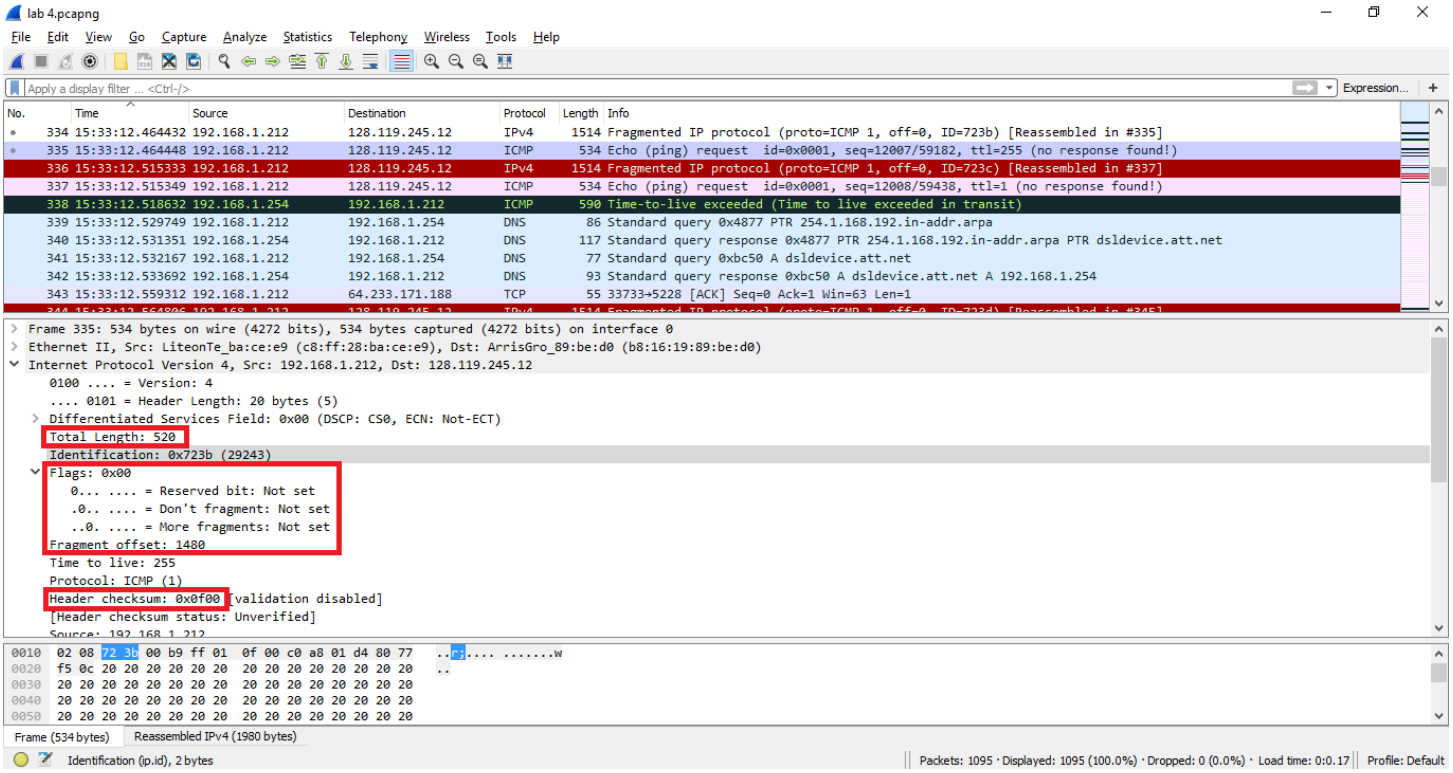
The Fragment offset = 1480 which indicates that this is not the first datagram fragment. The 'More fragments' flag is not set which indicated that there aren't any more fragments.



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

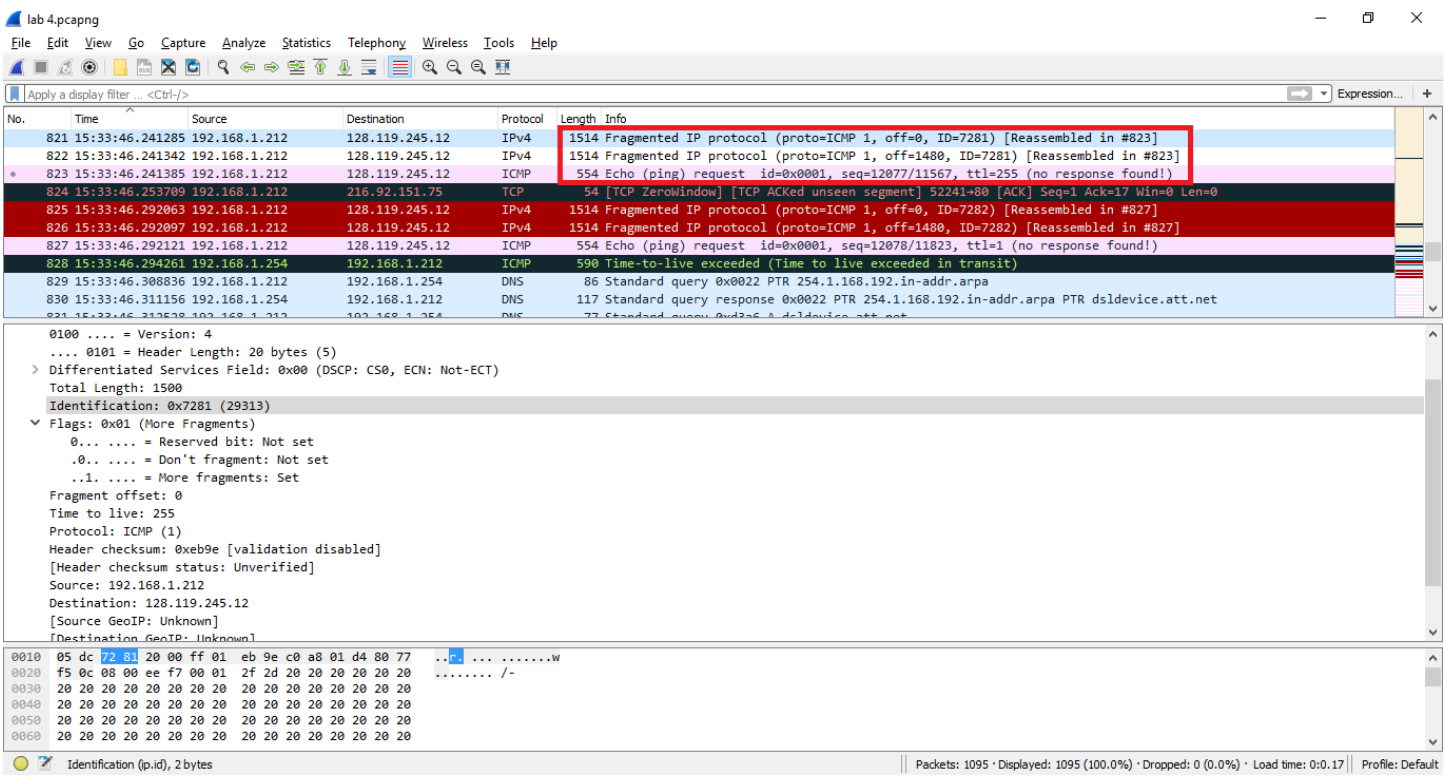
The fields that change in the IP header between the first and second fragments are: total length, flags, fragment offset, and checksum.





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

There were three fragments created from the original datagram



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

The fields that change are flags, fragment offset, checksum, and total length. Each of the three packets has a unique fragment offset and checksum. The first two packets have the same total length and flags but the third has different values in those fields.

lab 4.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression...

No.	Time	Source	Destination	Protocol	Length	Info
821	15:33:46.241285	192.168.1.212	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=7281) [Reassembled in #823]
822	15:33:46.241342	192.168.1.212	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=7281) [Reassembled in #823]
823	15:33:46.241385	192.168.1.212	128.119.245.12	ICMP	554	Echo (ping) request id=0x0001, seq=12077/11567, ttl=255 (no response found!)
824	15:33:46.253709	192.168.1.212	216.92.151.75	TCP	54	[TCP ZeroWindow] [TCP ACKed unseen segment] 52241→80 [ACK] Seq=1 Ack=17 Win=0 Len=0
825	15:33:46.292063	192.168.1.212	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=7282) [Reassembled in #827]
826	15:33:46.292097	192.168.1.212	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=7282) [Reassembled in #827]
827	15:33:46.292121	192.168.1.212	128.119.245.12	ICMP	554	Echo (ping) request id=0x0001, seq=12078/11823, ttl=1 (no response found!)
828	15:33:46.294261	192.168.1.254	192.168.1.212	ICMP	590	Time-to-live exceeded (Time to live exceeded in transit)
829	15:33:46.308836	192.168.1.212	192.168.1.254	DNS	86	Standard query 0x0022 PTR 254.1.168.192.in-addr.arpa
830	15:33:46.311156	192.168.1.254	192.168.1.212	DNS	117	Standard query response 0x0022 PTR 254.1.168.192.in-addr.arpa PTR dsldevice.att.net

```
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1500
    Identification: 0x7281 (29313)
  v Flags: 0x01 (More Fragments)
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..1. .... = More fragments: Set
    Fragment offset: 0
    Time to live: 255
    Protocol: ICMP (1)
    Header checksum: 0xeb9e [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.212
    Destination: 128.119.245.12
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
```

```
0010  05 dc 72 81 20 00 ff 01  eb 9e c0 a8 01 d4 80 77   ..r. ... .......w
0020  f5 0c 08 00 ee f7 00 01  2f 2d 20 20 20 20 20 20   ........ /-
0030  20 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 20
0050  20 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 20
```

Identification (ip.id), 2 bytes | Packets: 1095 · Displayed: 1095 (100.0%) · Dropped: 0 (0.0%) · Load time: 0:0.17 | Profile: Default

lab 4.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression...

No.	Time	Source	Destination	Protocol	Length	Info
821	15:33:46.241285	192.168.1.212	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=7281) [Reassembled in #823]
822	15:33:46.241342	192.168.1.212	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=7281) [Reassembled in #823]
823	15:33:46.241385	192.168.1.212	128.119.245.12	ICMP	554	Echo (ping) request id=0x0001, seq=12077/11567, ttl=255 (no response found!)
824	15:33:46.253709	192.168.1.212	216.92.151.75	TCP	54	[TCP ZeroWindow] [TCP ACKed unseen segment] 52241→80 [ACK] Seq=1 Ack=17 Win=0 Len=0
825	15:33:46.292063	192.168.1.212	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=7282) [Reassembled in #827]
826	15:33:46.292097	192.168.1.212	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=7282) [Reassembled in #827]
827	15:33:46.292121	192.168.1.212	128.119.245.12	ICMP	554	Echo (ping) request id=0x0001, seq=12078/11823, ttl=1 (no response found!)
828	15:33:46.294261	192.168.1.254	192.168.1.212	ICMP	590	Time-to-live exceeded (Time to live exceeded in transit)
829	15:33:46.308836	192.168.1.212	192.168.1.254	DNS	86	Standard query 0x0022 PTR 254.1.168.192.in-addr.arpa
830	15:33:46.311156	192.168.1.254	192.168.1.212	DNS	117	Standard query response 0x0022 PTR 254.1.168.192.in-addr.arpa PTR dsldevice.att.net

```
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1500
    Identification: 0x7281 (29313)
  v Flags: 0x01 (More Fragments)
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..1. .... = More fragments: Set
    Fragment offset: 1480
    Time to live: 255
    Protocol: ICMP (1)
    Header checksum: 0xeae5 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.212
    Destination: 128.119.245.12
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
```

```
0010  05 dc 72 81 20 b9 ff 01  ea e5 c0 a8 01 d4 80 77   ..r. ... .......w
0020  f5 0c 20 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 20
0040  20 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 20
0060  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
```

Identification (ip.id), 2 bytes | Packets: 1095 · Displayed: 1095 (100.0%) · Dropped: 0 (0.0%) · Load time: 0:0.17 | Profile: Default

lab 4.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression...

No.	Time	Source	Destination	Protocol	Length	Info
821	15:33:46.241285	192.168.1.212	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=7281) [Reassembled in #823]
822	15:33:46.241342	192.168.1.212	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=7281) [Reassembled in #823]
823	15:33:46.241385	192.168.1.212	128.119.245.12	ICMP	554	Echo (ping) request id=0x0001, seq=12077/11567, ttl=255 (no response found!)
824	15:33:46.253709	192.168.1.212	216.92.151.75	TCP	54	[TCP ZeroWindow] [TCP ACKed unseen segment] 52241→80 [ACK] Seq=1 Ack=17 Win=0 Len=0
825	15:33:46.292063	192.168.1.212	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=7282) [Reassembled in #827]
826	15:33:46.292097	192.168.1.212	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=7282) [Reassembled in #827]
827	15:33:46.292121	192.168.1.212	128.119.245.12	ICMP	554	Echo (ping) request id=0x0001, seq=12078/11823, ttl=1 (no response found!)
828	15:33:46.294261	192.168.1.254	192.168.1.212	ICMP	590	Time-to-live exceeded (Time to live exceeded in transit)
829	15:33:46.308836	192.168.1.212	192.168.1.254	DNS	86	Standard query 0x0022 PTR 254.1.168.192.in-addr.arpa
830	15:33:46.311156	192.168.1.254	192.168.1.212	DNS	117	Standard query response 0x0022 PTR 254.1.168.192.in-addr.arpa PTR dsldevice.att.net

```
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 540
    Identification: 0x7281 (29313)
  v Flags: 0x00
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
    Fragment offset: 2960
    Time to live: 255
    Protocol: ICMP (1)
    Header checksum: 0x0ded [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.212
    Destination: 128.119.245.12
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
```

```
0010  02 1c 72 81 01 72 ff 01  0d ed c0 a8 01 d4 80 77   ..r..r.. .......w
0020  f5 0c 20 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 20
0040  20 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 20
```

Frame (554 bytes) | Reassembled IPv4 (3480 bytes)

Identification (ip.id), 2 bytes | Packets: 1095 · Displayed: 1095 (100.0%) · Dropped: 0 (0.0%) · Load time: 0:0.17 | Profile: Default