

1) My IP: 10.0.0.143

The screenshot shows a Wireshark packet capture on a Wi-Fi interface. The packet list on the left shows a series of DNS and ICMP messages. Packet 13 is highlighted in red, showing an ICMP Echo (ping) request from 10.0.0.143 to 23.47.144.10. The packet details pane on the right shows the Ethernet II header, Internet Protocol Version 4 header, and ICMP Echo (ping) request details. The packet bytes pane at the bottom shows the raw data of the packet.

Frame 13: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
> Ethernet II, Src: HonHaiPr_5b:aec:9 (08:ed:b9:5b:aec:9), Dst: Arrisdro_70:0f:2f (10:86:8c:70:0f:2f)
Internet Protocol Version 4, Src: 10.0.0.143, Dst: 23.47.144.10
0100 = Version: 4
... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 56
Identification: 0x368b (13963)
Flags: 0x00
Fragment offset: 0
Time to live: 255
Protocol: ICMP (1)
Header checksum: 0xd371 [validation disabled]
[Header checksum status: Unverified]
Source: 10.0.0.143
Destination: 23.47.144.10
[Source GeoIP: Unknown]

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

The screenshot shows a Wireshark packet capture on a Wi-Fi interface. The packet list on the left shows a series of DNS and ICMP messages. Packet 13 is highlighted in red, showing an ICMP Echo (ping) request from 10.0.0.143 to 23.47.144.10. The packet details pane on the right shows the Ethernet II header, Internet Protocol Version 4 header, and ICMP Echo (ping) request details. The packet bytes pane at the bottom shows the raw data of the packet.

Frame 13: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
> Ethernet II, Src: HonHaiPr_5b:aec:9 (08:ed:b9:5b:aec:9), Dst: Arrisdro_70:0f:2f (10:86:8c:70:0f:2f)
Internet Protocol Version 4, Src: 10.0.0.143, Dst: 23.47.144.10
0100 = Version: 4
... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 56
Identification: 0x368b (13963)
Flags: 0x00
Fragment offset: 0
Time to live: 255
Protocol: ICMP (1)
Header checksum: 0xd371 [validation disabled]
[Header checksum status: Unverified]
Source: 10.0.0.143

3) There are 20 Bytes in the header; the total length is 56 Bytes; this makes the payload 56 - 20 = 36 Bytes

Wireshark packet capture showing an ICMP Echo (ping) request. The packet list shows a ping request from 10.0.0.136 to 10.0.0.1. The packet details pane shows the IP header with a total length of 56 bytes and the ICMP header with a sequence number of 266656. The packet bytes pane shows the raw data of the packet.

4) It was not fragmented: the more fragments flag was set to 0.

Wireshark packet capture showing an ICMP Echo (ping) request. The packet list shows a ping request from 10.0.0.136 to 10.0.0.1. The packet details pane shows the IP header with a total length of 56 bytes and the ICMP header with a sequence number of 266656. The packet bytes pane shows the raw data of the packet.

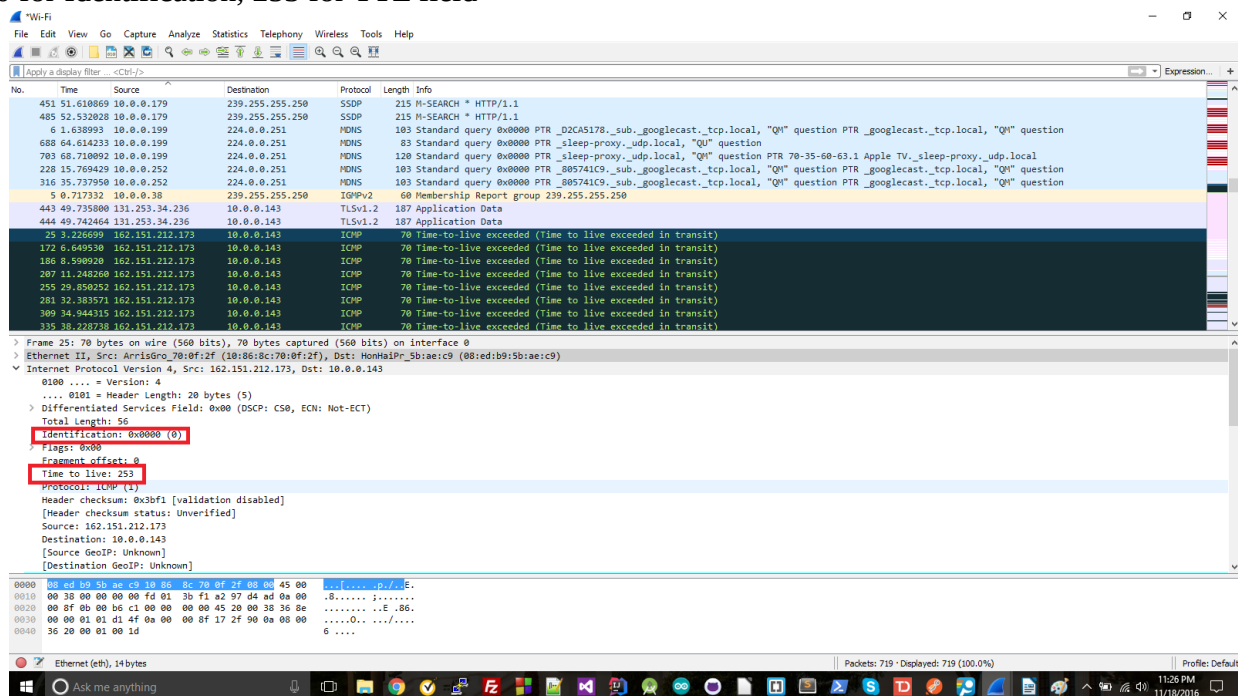
5) The fields that always change are Identification, checksum, and Time to live.

6) The fields that stay constant are Version, Header Length, Differentiated Services Field, Total Length, Protocol, Source, Destination. These must all stay the same, because Version determines what IP version the two hosts are using to communicate, Header Length must stay the same for ICMP, Differentiated Services must stay the same for all of the same protocol, Source since all packets are coming from the same place, destination since all packets are going to the same place.

The fields that must change are Identification since each packet needs its own individual ID, checksum since each datagram will have its own content that needs to be checked, and time to live since each TTL gets incremented.

7) The Identification field is incrementing with each packet that is part of the sequence (13963, 13964, etc)

8) 0 for Identification, 253 for TTL field



9) They do stay the same. The reason for this is that the hop is always the same distance away.

10) It has. I know this because it says the fragmentation flag was set.

Wireshark packet capture showing an ICMP Echo (ping) request. The packet is fragmented, with the first fragment highlighted in green. The packet details pane shows the IP header with the fragmentation flag set (More Fragments bit). The packet bytes pane shows the raw data of the first fragment.

Frame 247: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0

Ethernet II, Src: NonHdPr_Sb:ae:c9 (08:ed:b9:5b:ae:c9), Dst: ArrisGro_70:f2f (10:86:8c:70:f2f)

Internet Protocol Version 4, Src: 10.0.0.143, Dst: 23.47.144.10

0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 1500
Identification: 0x36e1 (14049)
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: 1
[Expert Info (Note/Sequence): "Time To Live" only 1]
Protocol: ICMP (1)
Header checksum: 0xab78 [validation disabled]
[Header checksum status: Unverified]

11) The fragment flag is set so we know it's a fragment (red box). We know it's the first because the fragment offset is 0 (yellow box). The datagram is 1500 Bytes (blue box).

Wireshark packet capture showing an ICMP Echo (ping) request. The packet is fragmented, with the first fragment highlighted in green. The packet details pane shows the IP header with the fragmentation flag set (More Fragments bit). The packet bytes pane shows the raw data of the first fragment.

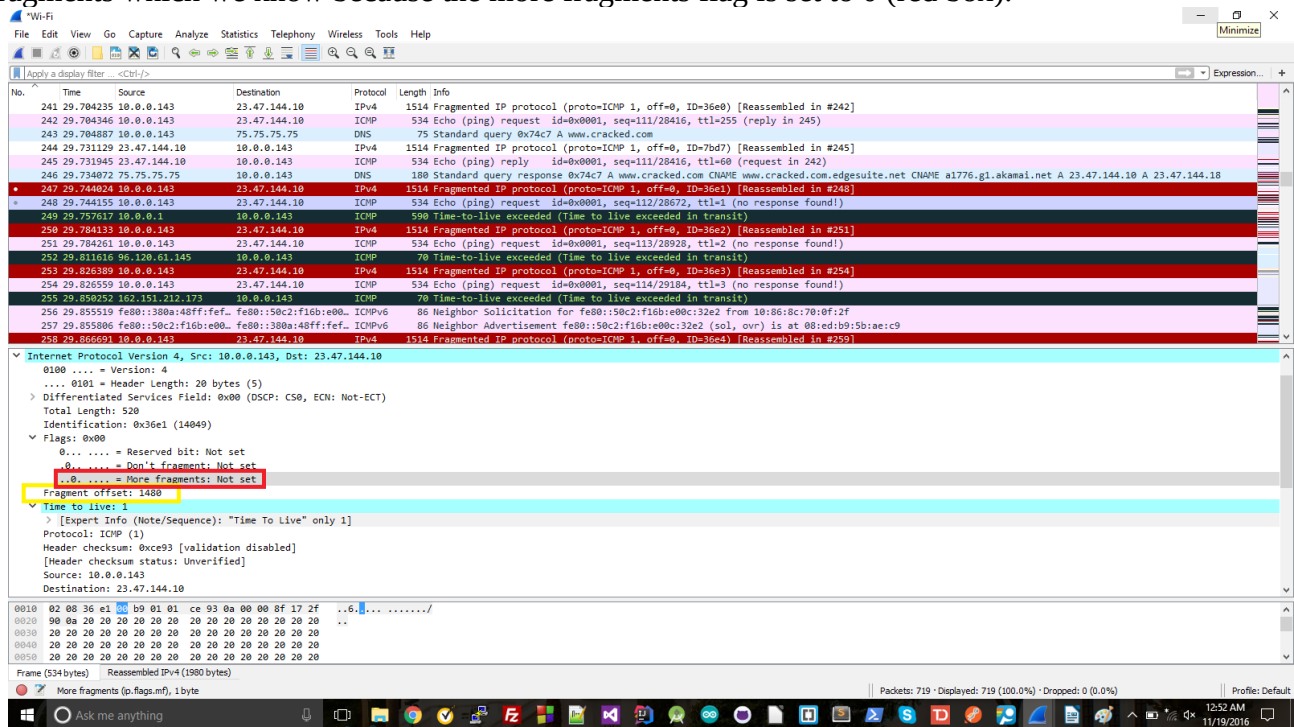
Frame 247: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0

Ethernet II, Src: NonHdPr_Sb:ae:c9 (08:ed:b9:5b:ae:c9), Dst: ArrisGro_70:f2f (10:86:8c:70:f2f)

Internet Protocol Version 4, Src: 10.0.0.143, Dst: 23.47.144.10

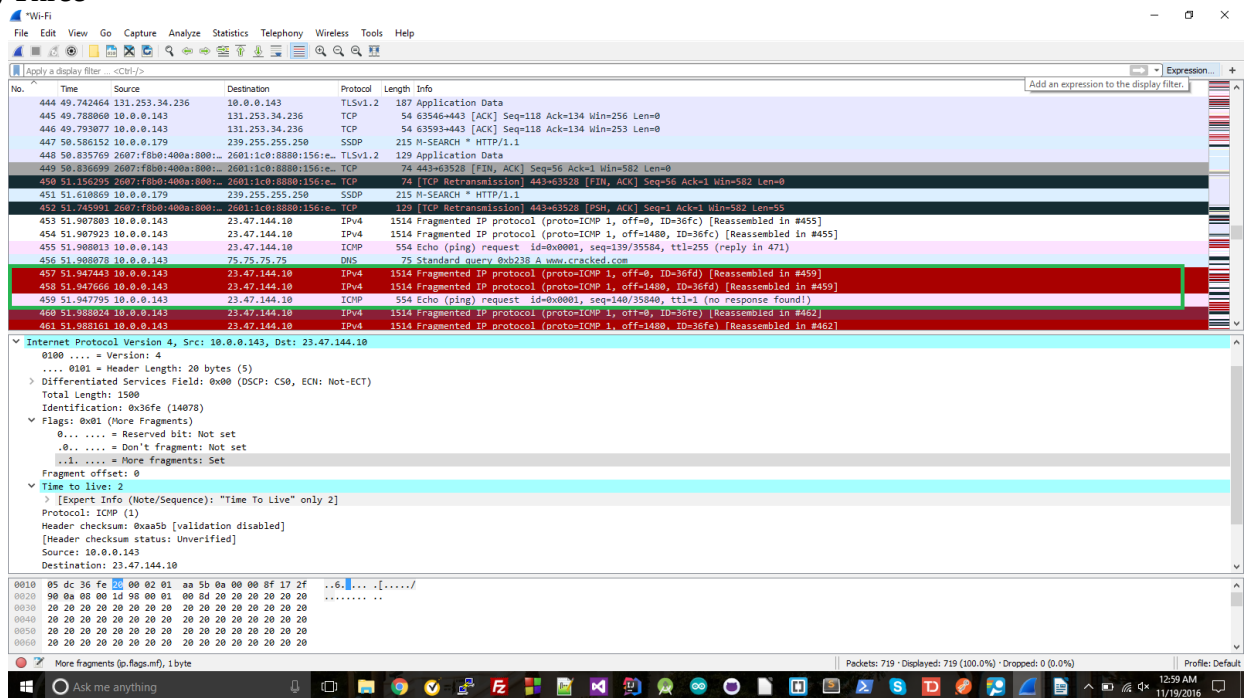
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 1500
Identification: 0x36e1 (14049)
Flags: 0x01 (More Fragments)
0... = Reserved bit: Not set
.0... = Don't fragment: Not set
..1... = More fragments: Set
Fragment offset: 0
Time to live: 1
[Expert Info (Note/Sequence): "Time To Live" only 1]
Protocol: ICMP (1)
Header checksum: 0xab78 [validation disabled]
[Header checksum status: Unverified]

12) I know this is not the first datagram because the offset is not 0 (yellow box). There are no more fragments which we know because the more fragments flag is set to 0 (red box).



13) The header fields that change are length, identification, more fragments flag, offset, and checksum.

14) Three



15) The header fields that change are the length, ID, more fragments flag, fragment offset, and checksum.