Sri Sai Anusha Gandu, Student ID: 16230560

Assignment 2

Network Architecture-I, Fall-2016

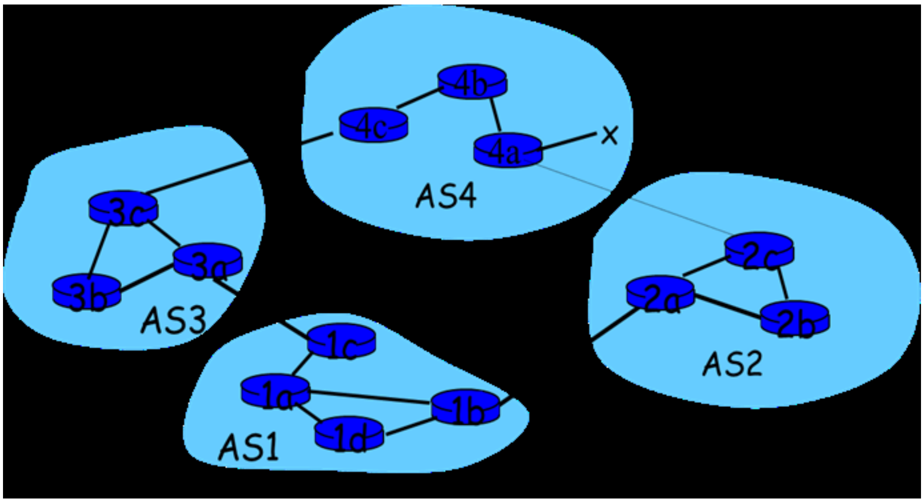
1. Consider the network shown below. Suppose AS2 and AS3 are running OSPF for their intra-AS routing protocol. Suppose AS1 and AS4 are running RIP for their intra-AS routing protocol. Suppose eBGP and iBGP are used for the inter-AS routing protocol. Initially suppose there is no physical link between AS2 and AS4.

(a) Router 3c learns about prefix x from which routing protocol: OSPF, RIP, eBGP or iBGP?

(b) Router 3a learns about prefix x from which routing protocol?

(c) Router 1c learns about prefix x from which routing protocol?

(d) Router 1d learns about prefix x from which routing protocol?



Ans:

Given that AS2 and AS3 are running OSPF for their intra-AS routing protocol, AS1 and AS4 are running RIP for their intra-AS routing protocol and eBGP and iBGP are used for the inter-AS routing protocol and there is no link between AS2 and AS4.

(a)

Router 3c learns about prefix x from eBGP routing protocol. x is connected to AS4 and it is close to AS3 and is the only path to know about the prefix. Hence the Router 3c learns about x from eBGP protocol.

(b)

Router 3a learns about prefix x from iBGP routing protocol. As Router 3c learns about x from eBGP inter-AS routing protocol from AS4, Router 3a which is internally connected to Router 3c learns from iBGP inter-AS routing protocol.

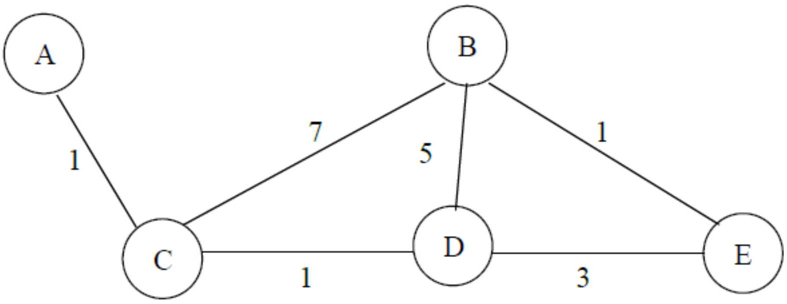
(c)

Router 1c learns about prefix x from eBGP routing protocol. AS3 learns about x from AS4 through eBGP inter-AS routing protocol and in turn Router 1c which is a gateway router learns from AS3 through eBGP routing protocol.

(d)

Router 1d learns about prefix x from iBGP routing protocol. Though x is close to 1d through AS2, since there is no physical connection between AS2 and AS4, it routes through AS4 to AS3 and then to AS1. Router 1d learns about x from gateway router 1c through iBGP routing protocol.

2. Consider the network shown below (the labels are the delay on the links).

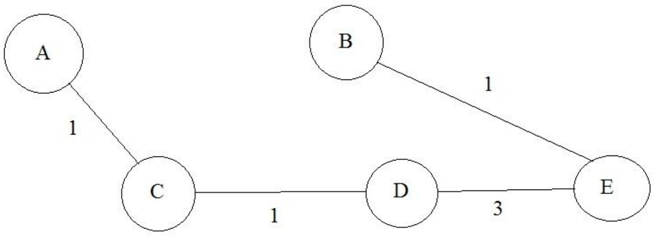


Show the operation of Dijkstra's (Link State) algorithm for computing the shortest path from C to all destinations.

Ans:

Step	N`	D(A) = p(A)	D(B) = p(B)	D(D) = p(D)	D(E) = p(E)
0	C	1,A	7,B	1,D	∞
1	CD	1,A	6,D	--	4,D
2	CDA	--	6,D	--	4,D
3	CDAE	--	5,E	--	--
4	CDAEB	--	--	--	--

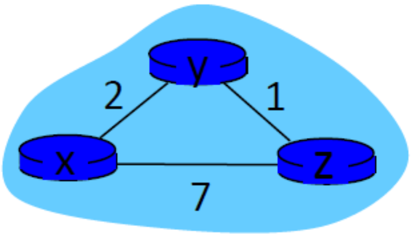
The shortest path from C to all destinations is depicted as below.



Forwarding table in C:

Destination	Link
A	(C,A)
B	(C,D)
D	(C,D)
E	(C,D)

3. Consider the network shown below (the labels are the delay on the links)



(a) Show the operation of Distance Vector algorithm for computing the shortest path from node X, node Y, node Z to all destinations.

(b) Show the distance table that would be computed by the distance vector algorithm.

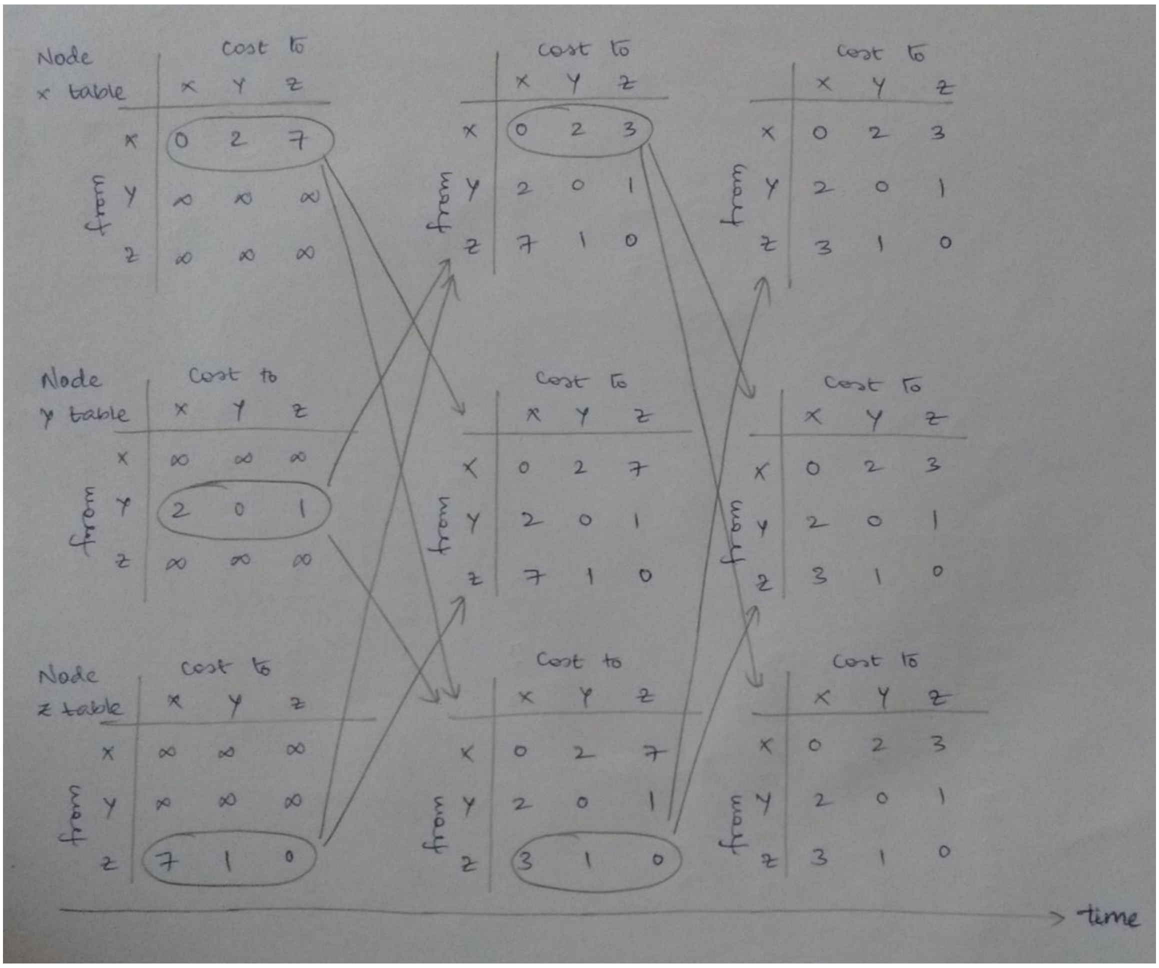
Ans:

(a)

We know

$D_x(y) = \min\{c(x,y) + D_y(y), c(x,z) + D_z(y)\} = \min\{2+0 , 7+1\} = 2$

$D_x(z) = \min\{c(x,y) + D_y(z), c(x,z) + D_z(z)\} = \min\{2+1 , 7+0\} = 3$



Node x table

cost to

from

	x	y	z
x	0	2	7
y	∞	∞	∞
z	∞	∞	∞

Node y table

Cost to

from

	x	y	z
x	∞	∞	∞
y	2	0	1
z	∞	∞	∞

Node z table

cost to

from

	x	y	z
x	∞	∞	∞
y	∞	∞	∞
z	7	1	0

cost to

from

	x	y	z
x	0	2	3
y	2	0	1
z	7	1	0

Cost to

from

	x	y	z
x	0	2	7
y	2	0	1
z	7	1	0

Cost to

from

	x	y	z
x	0	2	7
y	2	0	1
z	3	1	0

cost to

from

	x	y	z
x	0	2	3
y	2	0	1
z	3	1	0

Cost to

from

	x	y	z
x	0	2	3
y	2	0	1
z	3	1	0

Cost to

from

	x	y	z
x	0	2	3
y	2	0	1
z	3	1	0

(b)

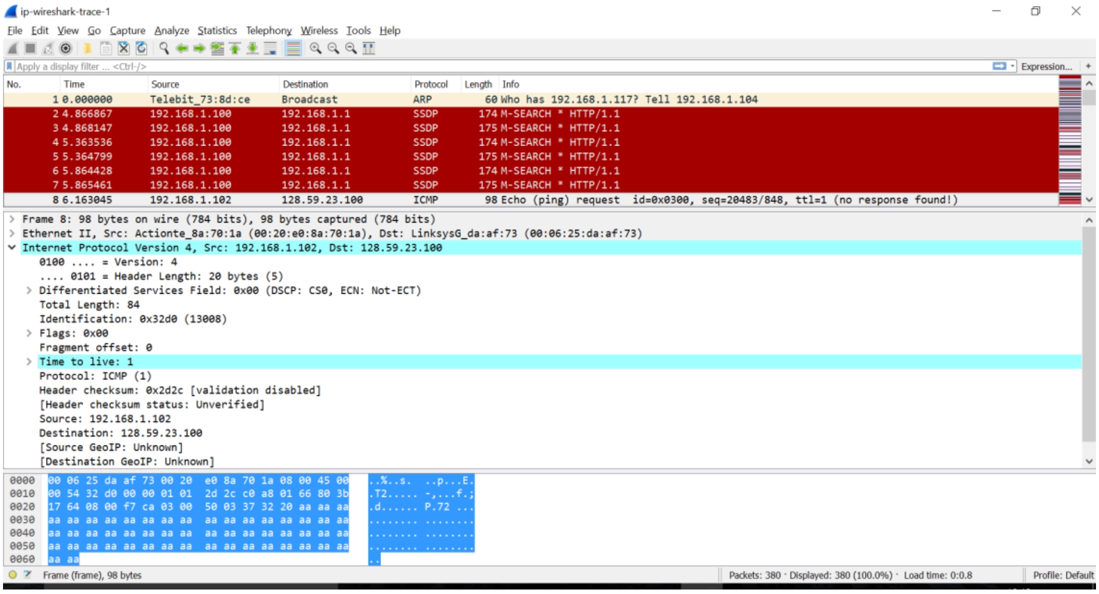
Node	To x	To y	To z
From x	0	2	3
From y	2	0	1
From z	3	1	0

Laboratory Homework

1. Select the first ICMP Echo Request message sent by the computer, and expand the Internet Protocol part of the packet in the packet details window. What is the IP address of the user's computer?

Ans:

The IP address of the user’s computer is given by 192.168.1.102


ip-wireshark-trace-1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...

```
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    SSDP      174 M-SEARCH * HTTP/1.1
   3 4.868147   192.168.1.100     192.168.1.1    SSDP      175 M-SEARCH * HTTP/1.1
   4 5.363536   192.168.1.100     192.168.1.1    SSDP      174 M-SEARCH * HTTP/1.1
   5 5.364799   192.168.1.100     192.168.1.1    SSDP      175 M-SEARCH * HTTP/1.1
   6 5.864428   192.168.1.100     192.168.1.1    SSDP      174 M-SEARCH * HTTP/1.1
   7 5.865461   192.168.1.100     192.168.1.1    SSDP      175 M-SEARCH * HTTP/1.1
   8 6.163045   192.168.1.102     128.59.23.100  ICMP       98 Echo (ping) request  id=0x0300, seq=20483/848, ttl=1 (no response found!)
```

```
> 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, Dst: 128.59.23.100
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0x32d0 (13008)
  > Flags: 0x00
    Fragment offset: 0
  > Time to live: 1
    Protocol: ICMP (1)
    Header checksum: 0x2d2c [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.102
    Destination: 128.59.23.100
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
```

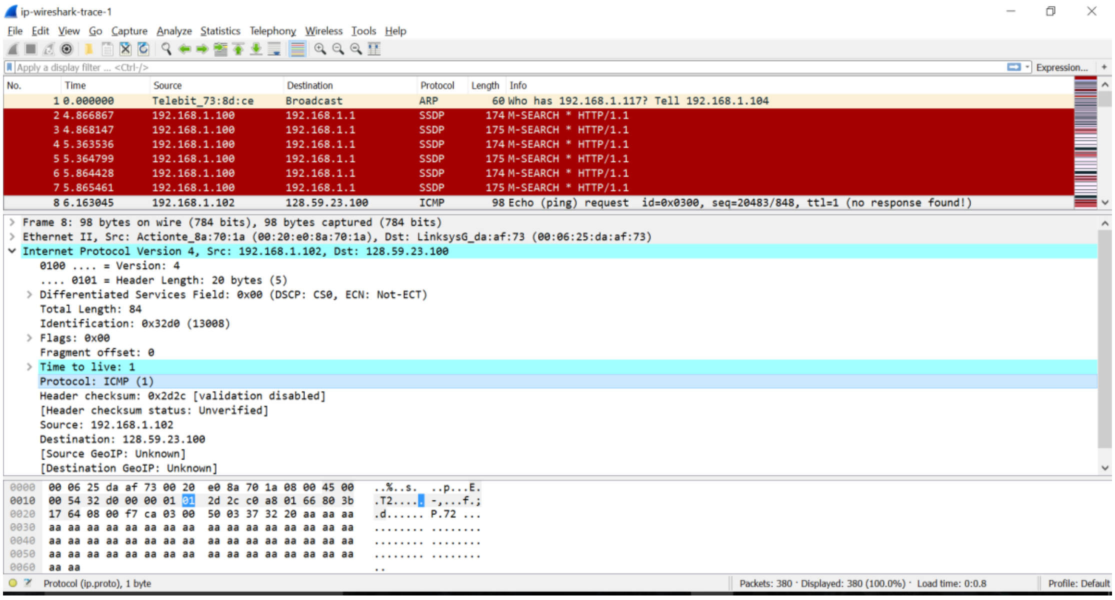
```
0000  00 06 25 da af 73 00 20  e0 8a 70 1a 08 00 45 00   ..%..s.  ..p...E.
0010  00 54 32 d0 00 00 01 01  2d 2c c0 a8 01 66 80 3b   .T2..... -,...f.;
0020  17 64 08 00 f7 ca 03 00  50 03 37 32 20 aa aa aa   .d...... P.72 ...
0030  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ........ ........
0040  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ........ ........
0050  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ........ ........
0060  aa aa                                              ..
```

```
Frame (frame), 98 bytes      Packets: 380 · Displayed: 380 (100.0%) · Load time: 0:0.8      Profile: Default
```

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

Ans:

Within the IP packet header, the value in the upper layer protocol field is 1.


ip-wireshark-trace-1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...

```
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    SSDP      174 M-SEARCH * HTTP/1.1
   3 4.868147   192.168.1.100     192.168.1.1    SSDP      175 M-SEARCH * HTTP/1.1
   4 5.363536   192.168.1.100     192.168.1.1    SSDP      174 M-SEARCH * HTTP/1.1
   5 5.364799   192.168.1.100     192.168.1.1    SSDP      175 M-SEARCH * HTTP/1.1
   6 5.864428   192.168.1.100     192.168.1.1    SSDP      174 M-SEARCH * HTTP/1.1
   7 5.865461   192.168.1.100     192.168.1.1    SSDP      175 M-SEARCH * HTTP/1.1
   8 6.163045   192.168.1.102     128.59.23.100  ICMP       98 Echo (ping) request  id=0x0300, seq=20483/848, ttl=1 (no response found!)
```

```
> 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, Dst: 128.59.23.100
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0x32d0 (13008)
  > Flags: 0x00
    Fragment offset: 0
  > Time to live: 1
    Protocol: ICMP (1)
    Header checksum: 0x2d2c [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.102
    Destination: 128.59.23.100
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
```

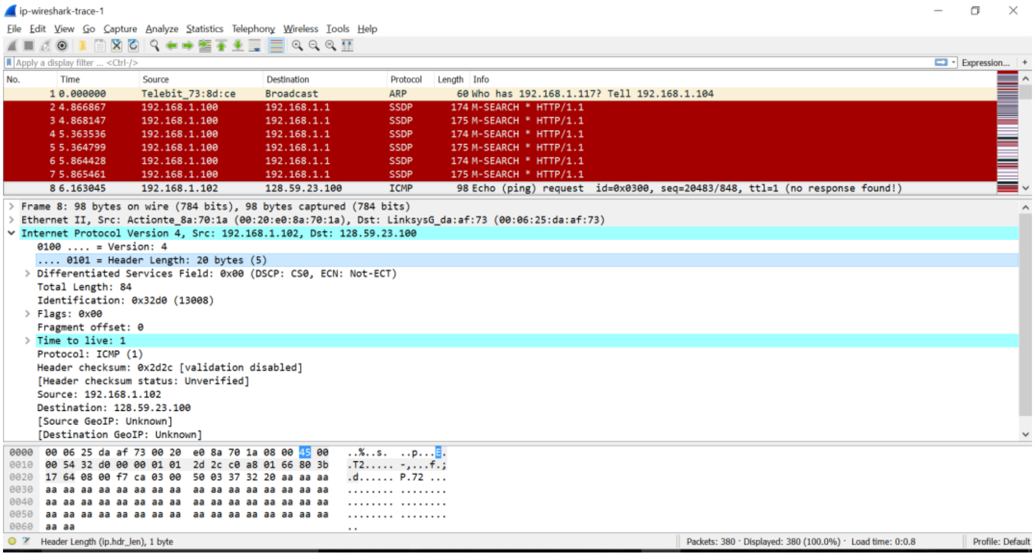
```
0000  00 06 25 da af 73 00 20  e0 8a 70 1a 08 00 45 00   ..%..s.  ..p...E.
0010  00 54 32 d0 00 00 01 01  2d 2c c0 a8 01 66 80 3b   .T2..... -,...f.;
0020  17 64 08 00 f7 ca 03 00  50 03 37 32 20 aa aa aa   .d...... P.72 ...
0030  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ........ ........
0040  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ........ ........
0050  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ........ ........
0060  aa aa                                              ..
```

```
Protocol (ip.proto), 1 byte      Packets: 380 · Displayed: 380 (100.0%) · Load time: 0:0.8      Profile: Default
```

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 header length is 20 bytes. The payload of the IP datagram is of length 84 bytes. The number of payload bytes is given by the difference between the payload of IP datagram and the header length = 84-20 = 64 bytes.


ip-wireshark-trace-1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...

```
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    SSDP       174 M-SEARCH * HTTP/1.1
   3 4.868147   192.168.1.100   192.168.1.1    SSDP       175 M-SEARCH * HTTP/1.1
   4 5.363536   192.168.1.100   192.168.1.1    SSDP       174 M-SEARCH * HTTP/1.1
   5 5.364799   192.168.1.100   192.168.1.1    SSDP       175 M-SEARCH * HTTP/1.1
   6 5.864428   192.168.1.100   192.168.1.1    SSDP       174 M-SEARCH * HTTP/1.1
   7 5.865461   192.168.1.100   192.168.1.1    SSDP       175 M-SEARCH * HTTP/1.1
   8 6.163045   192.168.1.102   128.59.23.100  ICMP        98 Echo (ping) request  id=0x0300, seq=20483/848, ttl=1 (no response found!)
```

```
> 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, Dst: 128.59.23.100
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0x32d0 (13008)
  > Flags: 0x00
    Fragment offset: 0
  > Time to live: 1
    Protocol: ICMP (1)
    Header checksum: 0x2d2c [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.102
    Destination: 128.59.23.100
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
```

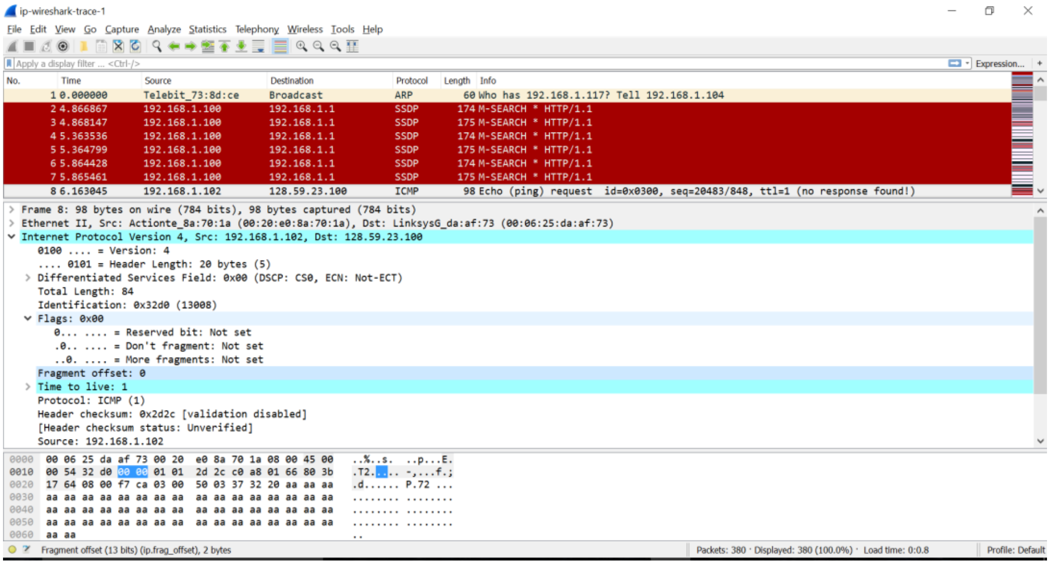
```
0000  00 06 25 da af 73 00 20  e0 8a 70 1a 08 00 45 00   ..%..s.  ..p...E.
0010  00 54 32 d0 00 00 01 01  2d 2c c0 a8 01 66 80 3b   .T2..... -,...f.;
0020  17 64 08 00 f7 ca 03 00  50 03 37 32 20 aa aa aa   .d...... P.72 ...
0030  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ........ ........
0040  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ........ ........
0050  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ........ ........
0060  aa aa                                              ..
```

```
Header Length (ip.hdr_len), 1 byte    Packets: 380 · Displayed: 380 (100.0%) · Load time: 0:0.8    Profile: Default
```

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

Ans:

The IP datagram is not fragmented. This is known by the flags value of 0x00.


ip-wireshark-trace-1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...

```
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    SSDP       174 M-SEARCH * HTTP/1.1
   3 4.868147   192.168.1.100   192.168.1.1    SSDP       175 M-SEARCH * HTTP/1.1
   4 5.363536   192.168.1.100   192.168.1.1    SSDP       174 M-SEARCH * HTTP/1.1
   5 5.364799   192.168.1.100   192.168.1.1    SSDP       175 M-SEARCH * HTTP/1.1
   6 5.864428   192.168.1.100   192.168.1.1    SSDP       174 M-SEARCH * HTTP/1.1
   7 5.865461   192.168.1.100   192.168.1.1    SSDP       175 M-SEARCH * HTTP/1.1
   8 6.163045   192.168.1.102   128.59.23.100  ICMP        98 Echo (ping) request  id=0x0300, seq=20483/848, ttl=1 (no response found!)
```

```
> 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, Dst: 128.59.23.100
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0x32d0 (13008)
  v Flags: 0x00
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
    Fragment offset: 0
  > Time to live: 1
    Protocol: ICMP (1)
    Header checksum: 0x2d2c [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.102
```

```
0000  00 06 25 da af 73 00 20  e0 8a 70 1a 08 00 45 00   ..%..s.  ..p...E.
0010  00 54 32 d0 00 00 01 01  2d 2c c0 a8 01 66 80 3b   .T2..... -,...f.;
0020  17 64 08 00 f7 ca 03 00  50 03 37 32 20 aa aa aa   .d...... P.72 ...
0030  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ........ ........
0040  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ........ ........
0050  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ........ ........
0060  aa aa                                              ..
```

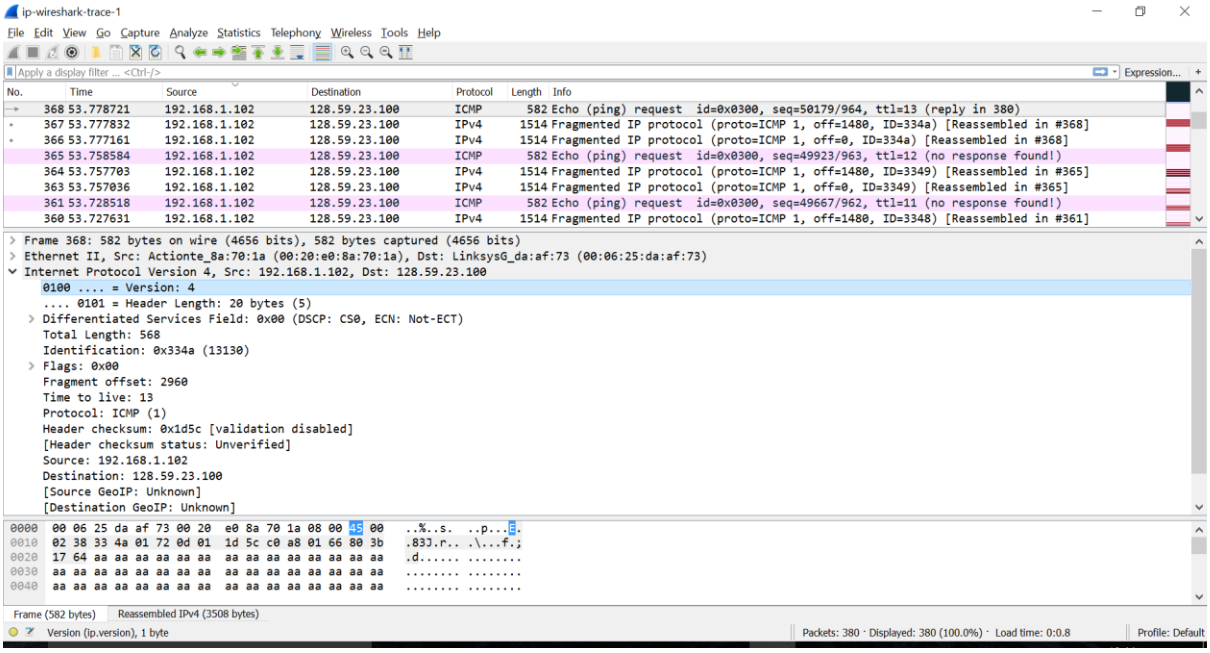
```
Fragment offset (13 bits) (ip.frag_offset), 2 bytes    Packets: 380 · Displayed: 380 (100.0%) · Load time: 0:0.8    Profile: Default
```

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

Ans:

Let us consider the datagrams 368, 365 and 361

Datagram 368


ip-wireshark-trace-1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Expression…
+

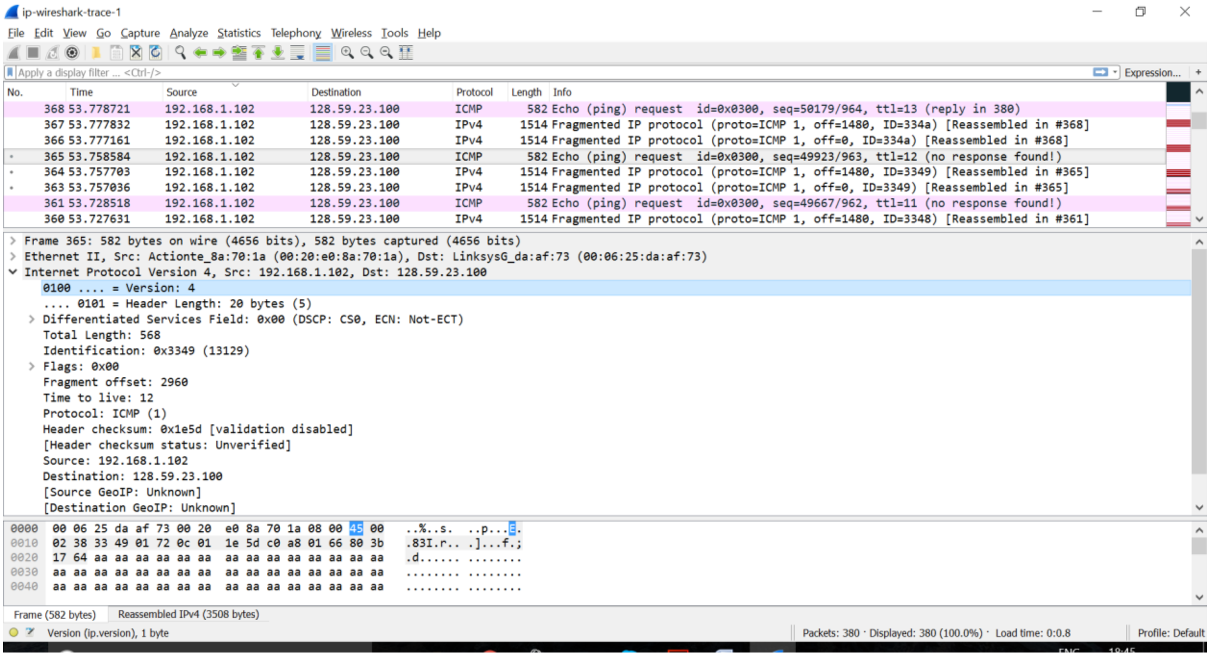
```
No.   Time       Source         Destination    Protocol Length Info
  368 53.778721  192.168.1.102  128.59.23.100  ICMP      582 Echo (ping) request  id=0x0300, seq=50179/964, ttl=13 (reply in 380)
  367 53.777832  192.168.1.102  128.59.23.100  IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=334a) [Reassembled in #368]
  366 53.777161  192.168.1.102  128.59.23.100  IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=334a) [Reassembled in #368]
  365 53.758584  192.168.1.102  128.59.23.100  ICMP      582 Echo (ping) request  id=0x0300, seq=49923/963, ttl=12 (no response found!)
  364 53.757703  192.168.1.102  128.59.23.100  IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3349) [Reassembled in #365]
  363 53.757036  192.168.1.102  128.59.23.100  IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=3349) [Reassembled in #365]
  361 53.728518  192.168.1.102  128.59.23.100  ICMP      582 Echo (ping) request  id=0x0300, seq=49667/962, ttl=11 (no response found!)
  360 53.727631  192.168.1.102  128.59.23.100  IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3348) [Reassembled in #361]
```

```
> Frame 368: 582 bytes on wire (4656 bits), 582 bytes captured (4656 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, Dst: 128.59.23.100
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 568
    Identification: 0x334a (13130)
  > Flags: 0x00
    Fragment offset: 2960
    Time to live: 13
    Protocol: ICMP (1)
    Header checksum: 0x1d5c [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.102
    Destination: 128.59.23.100
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
```

```
0000  00 06 25 da af 73 00 20  e0 8a 70 1a 08 00 45 00   ..%..s.  ..p...E.
0010  02 38 33 4a 01 72 0d 01  1d 5c c0 a8 01 66 80 3b   .83J.r.. .\...f.;
0020  17 64 aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   .d...... ........
0030  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ........ ........
0040  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ........ ........
```

Frame (582 bytes)
Reassembled IPv4 (3508 bytes)
Version (ip.version), 1 byte
Packets: 380 · Displayed: 380 (100.0%) · Load time: 0:0.8
Profile: Default

Datagram 365


ip-wireshark-trace-1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Expression…
+

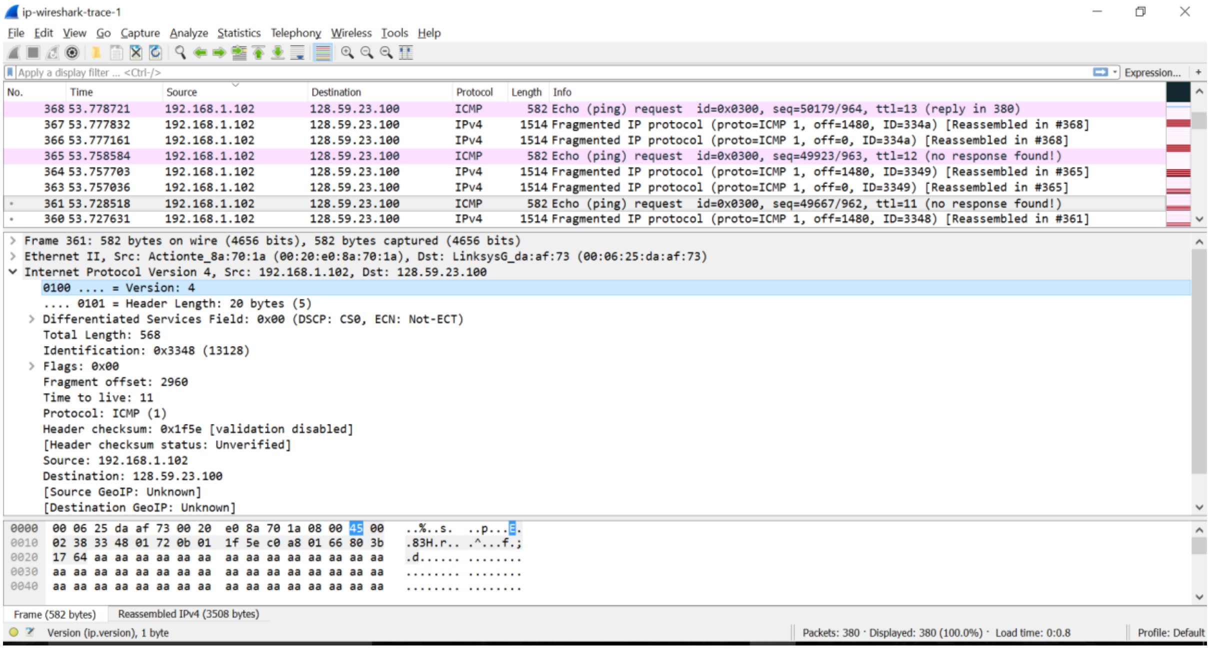
```
No.   Time       Source         Destination    Protocol Length Info
  368 53.778721  192.168.1.102  128.59.23.100  ICMP      582 Echo (ping) request  id=0x0300, seq=50179/964, ttl=13 (reply in 380)
  367 53.777832  192.168.1.102  128.59.23.100  IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=334a) [Reassembled in #368]
  366 53.777161  192.168.1.102  128.59.23.100  IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=334a) [Reassembled in #368]
  365 53.758584  192.168.1.102  128.59.23.100  ICMP      582 Echo (ping) request  id=0x0300, seq=49923/963, ttl=12 (no response found!)
  364 53.757703  192.168.1.102  128.59.23.100  IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3349) [Reassembled in #365]
  363 53.757036  192.168.1.102  128.59.23.100  IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=3349) [Reassembled in #365]
  361 53.728518  192.168.1.102  128.59.23.100  ICMP      582 Echo (ping) request  id=0x0300, seq=49667/962, ttl=11 (no response found!)
  360 53.727631  192.168.1.102  128.59.23.100  IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3348) [Reassembled in #361]
```

```
> Frame 365: 582 bytes on wire (4656 bits), 582 bytes captured (4656 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, Dst: 128.59.23.100
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 568
    Identification: 0x3349 (13129)
  > Flags: 0x00
    Fragment offset: 2960
    Time to live: 12
    Protocol: ICMP (1)
    Header checksum: 0x1e5d [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.102
    Destination: 128.59.23.100
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
```

```
0000  00 06 25 da af 73 00 20  e0 8a 70 1a 08 00 45 00   ..%..s.  ..p...E.
0010  02 38 33 49 01 72 0c 01  1e 5d c0 a8 01 66 80 3b   .83I.r.. .]...f.;
0020  17 64 aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   .d...... ........
0030  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ........ ........
0040  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ........ ........
```

Frame (582 bytes)
Reassembled IPv4 (3508 bytes)
Version (ip.version), 1 byte
Packets: 380 · Displayed: 380 (100.0%) · Load time: 0:0.8
Profile: Default

Datagram 361


ip-wireshark-trace-1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...

```
No.    Time         Source          Destination     Protocol  Length Info
   368 53.778721    192.168.1.102   128.59.23.100   ICMP       582 Echo (ping) request  id=0x0300, seq=50179/964, ttl=13 (reply in 380)
   367 53.777832    192.168.1.102   128.59.23.100   IPv4      1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=334a) [Reassembled in #368]
   366 53.777161    192.168.1.102   128.59.23.100   IPv4      1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=334a) [Reassembled in #368]
   365 53.758584    192.168.1.102   128.59.23.100   ICMP       582 Echo (ping) request  id=0x0300, seq=49923/963, ttl=12 (no response found!)
   364 53.757703    192.168.1.102   128.59.23.100   IPv4      1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3349) [Reassembled in #365]
   363 53.757036    192.168.1.102   128.59.23.100   IPv4      1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=3349) [Reassembled in #365]
   361 53.728518    192.168.1.102   128.59.23.100   ICMP       582 Echo (ping) request  id=0x0300, seq=49667/962, ttl=11 (no response found!)
   360 53.727631    192.168.1.102   128.59.23.100   IPv4      1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3348) [Reassembled in #361]
```

```
> Frame 361: 582 bytes on wire (4656 bits), 582 bytes captured (4656 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, Dst: 128.59.23.100
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 568
    Identification: 0x3348 (13128)
  > Flags: 0x00
    Fragment offset: 2960
    Time to live: 11
    Protocol: ICMP (1)
    Header checksum: 0x1f5e [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.102
    Destination: 128.59.23.100
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
```

```
0000  00 06 25 da af 73 00 20  e0 8a 70 1a 08 00 45 00   ..%..s.  ..p...E.
0010  02 38 33 48 01 72 0b 01  1f 5e c0 a8 01 66 80 3b   .83H.r..  .^...f.;
0020  17 64 aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   .d......  ........
0030  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ........  ........
0040  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ........  ........
```

Frame (582 bytes) | Reassembled IPv4 (3508 bytes)

Version (ip.version), 1 byte | Packets: 380 · Displayed: 380 (100.0%) · Load time: 0:0.8 | Profile: Default

With the series of ICMP messages sent by the computer, the fields in the IP datagram that always change are identification, time to live and header checksum.

For datagram 368:

Identification: 0x334a (13130)
Time to Live: 13
Header Checksum: 0x1d5c

For datagram 365:

Identification: 0x3349 (13129)
Time to Live: 12
Header Checksum: 0x1e5d

For datagram 361:

Identification: 0x3348 (13128)
Time to Live: 11
Header Checksum: 0x1f5e

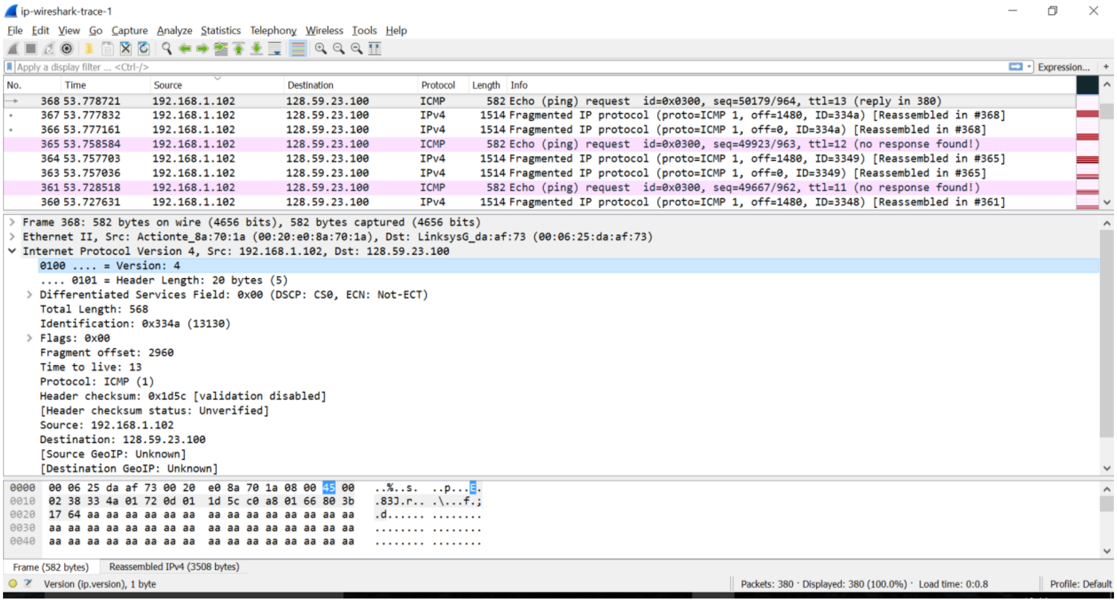
6. Which fields stay constant? Which of the fields *must* stay constant? Which fields must change? Why?

Ans:

The header length, payload length, flags, fragment offset, source address and destination address remain constant and must stay constant with the series of ICMP messages sent by the computer as the webpage is being accessed is the same.

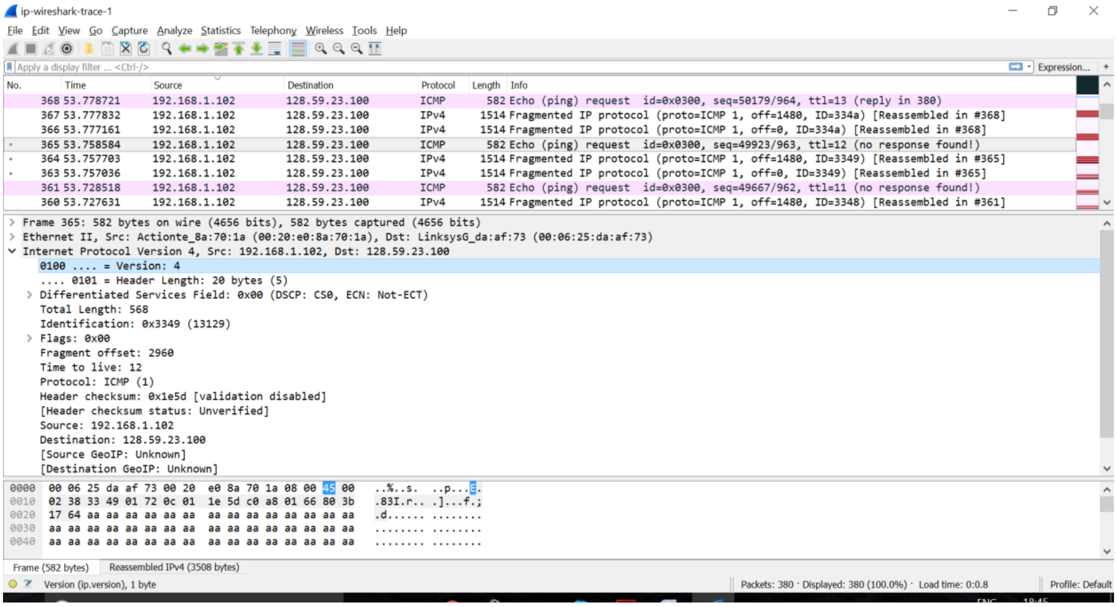
The fields like identification, time to live and header checksum change with the series of ICMP messages sent to the computer as each packet should have a unique identification.

Datagram 368


ip-wireshark-trace-1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
Frame (582 bytes)
Reassembled IPv4 (3508 bytes)
Version (ip.version), 1 byte
Packets: 380 · Displayed: 380 (100.0%) · Load time: 0:0.8
Profile: Default

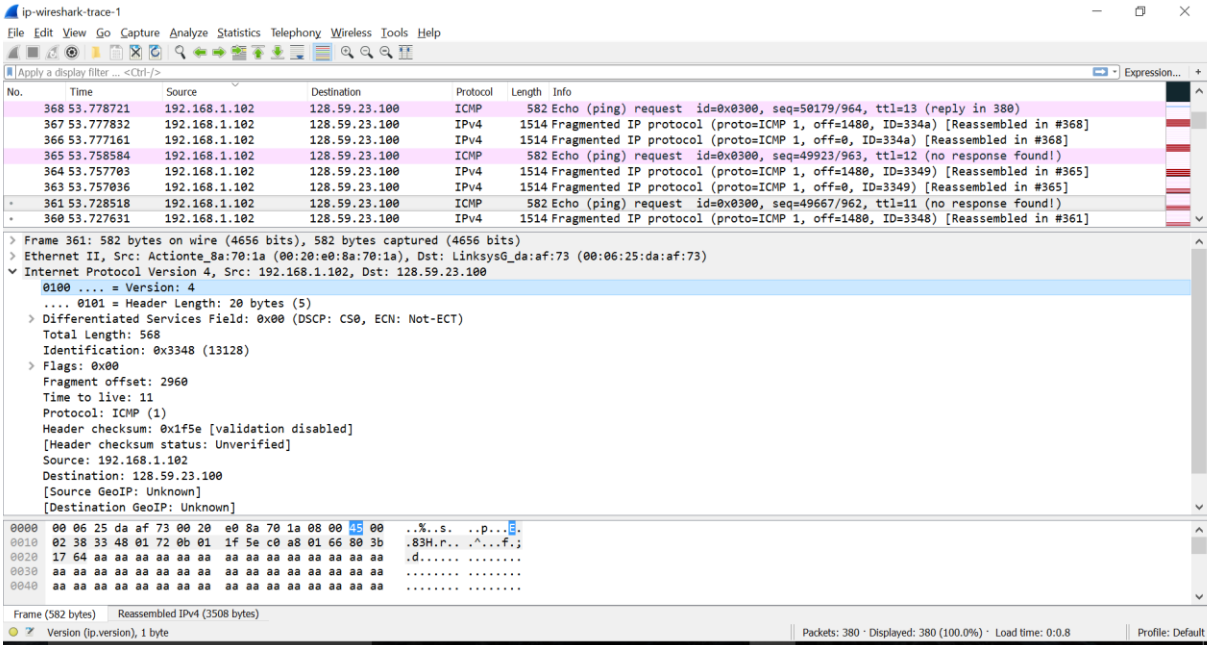
```
No.   Time        Source         Destination    Protocol Length Info
  368 53.778721   192.168.1.102  128.59.23.100  ICMP      582 Echo (ping) request  id=0x0300, seq=50179/964, ttl=13 (reply in 380)
  367 53.777832   192.168.1.102  128.59.23.100  IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=334a) [Reassembled in #368]
  366 53.777161   192.168.1.102  128.59.23.100  IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=334a) [Reassembled in #368]
  365 53.758584   192.168.1.102  128.59.23.100  ICMP      582 Echo (ping) request  id=0x0300, seq=49923/963, ttl=12 (no response found!)
  364 53.757703   192.168.1.102  128.59.23.100  IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3349) [Reassembled in #365]
  363 53.757036   192.168.1.102  128.59.23.100  IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=3349) [Reassembled in #365]
  361 53.728518   192.168.1.102  128.59.23.100  ICMP      582 Echo (ping) request  id=0x0300, seq=49667/962, ttl=11 (no response found!)
  360 53.727631   192.168.1.102  128.59.23.100  IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3348) [Reassembled in #361]

> Frame 368: 582 bytes on wire (4656 bits), 582 bytes captured (4656 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, Dst: 128.59.23.100
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 568
    Identification: 0x334a (13130)
  > Flags: 0x00
    Fragment offset: 2960
    Time to live: 13
    Protocol: ICMP (1)
    Header checksum: 0x1d5c [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.102
    Destination: 128.59.23.100
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]

0000  00 06 25 da af 73 00 20  e0 8a 70 1a 08 00 45 00   ..%..s.  ..p...E.
0010  02 38 33 4a 01 72 0d 01  1d 5c c0 a8 01 66 80 3b   .83J.r.. .\...f.;
0020  17 64 aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   .d...... ........
0030  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ........ ........
0040  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ........ ........
```

Datagram 365


ip-wireshark-trace-1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
Frame (582 bytes)
Reassembled IPv4 (3508 bytes)
Version (ip.version), 1 byte
Packets: 380 · Displayed: 380 (100.0%) · Load time: 0:0.8
Profile: Default

```
No.   Time        Source         Destination    Protocol Length Info
  368 53.778721   192.168.1.102  128.59.23.100  ICMP      582 Echo (ping) request  id=0x0300, seq=50179/964, ttl=13 (reply in 380)
  367 53.777832   192.168.1.102  128.59.23.100  IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=334a) [Reassembled in #368]
  366 53.777161   192.168.1.102  128.59.23.100  IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=334a) [Reassembled in #368]
  365 53.758584   192.168.1.102  128.59.23.100  ICMP      582 Echo (ping) request  id=0x0300, seq=49923/963, ttl=12 (no response found!)
  364 53.757703   192.168.1.102  128.59.23.100  IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3349) [Reassembled in #365]
  363 53.757036   192.168.1.102  128.59.23.100  IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=3349) [Reassembled in #365]
  361 53.728518   192.168.1.102  128.59.23.100  ICMP      582 Echo (ping) request  id=0x0300, seq=49667/962, ttl=11 (no response found!)
  360 53.727631   192.168.1.102  128.59.23.100  IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3348) [Reassembled in #361]

> Frame 365: 582 bytes on wire (4656 bits), 582 bytes captured (4656 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, Dst: 128.59.23.100
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 568
    Identification: 0x3349 (13129)
  > Flags: 0x00
    Fragment offset: 2960
    Time to live: 12
    Protocol: ICMP (1)
    Header checksum: 0x1e5d [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.102
    Destination: 128.59.23.100
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]

0000  00 06 25 da af 73 00 20  e0 8a 70 1a 08 00 45 00   ..%..s.  ..p...E.
0010  02 38 33 49 01 72 0c 01  1e 5d c0 a8 01 66 80 3b   .83I.r.. .]...f.;
0020  17 64 aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   .d...... ........
0030  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ........ ........
0040  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ........ ........
```

Datagram 361


ip-wireshark-trace-1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...

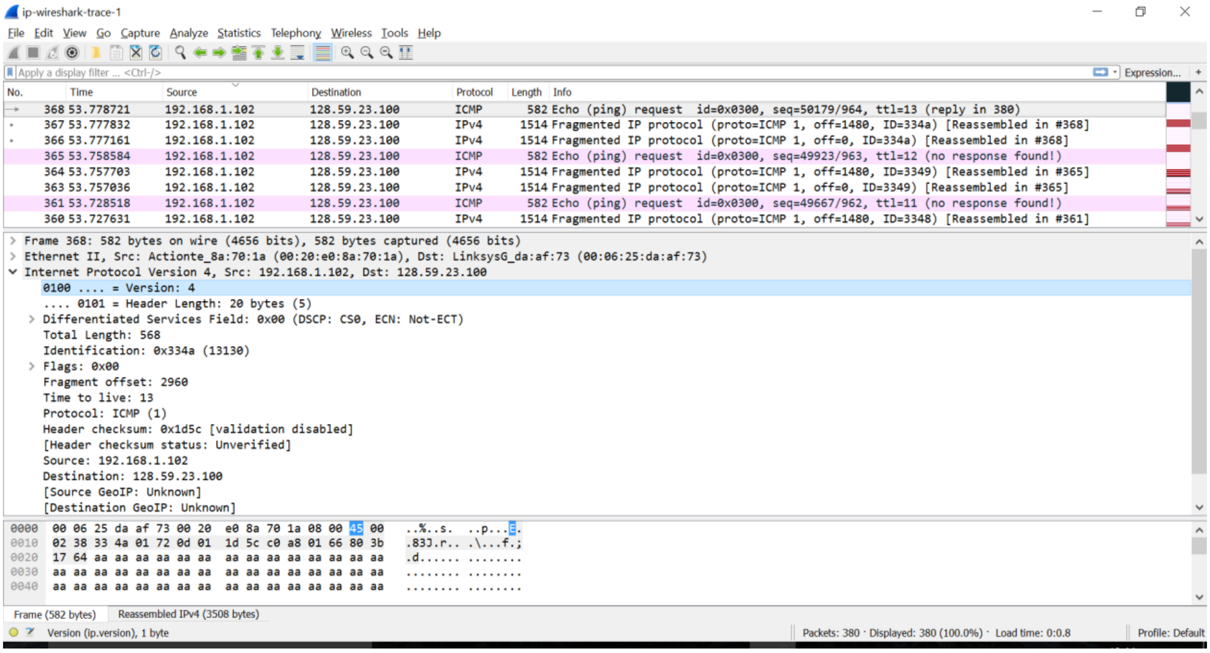
```
No.  Time          Source          Destination     Protocol  Length Info
  368 53.778721    192.168.1.102   128.59.23.100   ICMP       582 Echo (ping) request  id=0x0300, seq=50179/964, ttl=13 (reply in 380)
  367 53.777832    192.168.1.102   128.59.23.100   IPv4      1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=334a) [Reassembled in #368]
  366 53.777161    192.168.1.102   128.59.23.100   IPv4      1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=334a) [Reassembled in #368]
  365 53.758584    192.168.1.102   128.59.23.100   ICMP       582 Echo (ping) request  id=0x0300, seq=49923/963, ttl=12 (no response found!)
  364 53.757703    192.168.1.102   128.59.23.100   IPv4      1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3349) [Reassembled in #365]
  363 53.757036    192.168.1.102   128.59.23.100   IPv4      1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=3349) [Reassembled in #365]
  361 53.728518    192.168.1.102   128.59.23.100   ICMP       582 Echo (ping) request  id=0x0300, seq=49667/962, ttl=11 (no response found!)
  360 53.727631    192.168.1.102   128.59.23.100   IPv4      1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3348) [Reassembled in #361]

> Frame 361: 582 bytes on wire (4656 bits), 582 bytes captured (4656 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, Dst: 128.59.23.100
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 568
    Identification: 0x3348 (13128)
  > Flags: 0x00
    Fragment offset: 2960
    Time to live: 11
    Protocol: ICMP (1)
    Header checksum: 0x1f5e [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.102
    Destination: 128.59.23.100
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]

0000  00 06 25 da af 73 00 20  e0 8a 70 1a 08 00 45 00   ..%..s.  ..p...E.
0010  02 38 33 48 01 72 0b 01  1f 5e c0 a8 01 66 80 3b   .83H.r.. .^...f.;
0020  17 64 aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   .d...... ........
0030  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ........ ........
0040  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ........ ........

Frame (582 bytes)   Reassembled IPv4 (3508 bytes)
Version (ip.version), 1 byte        Packets: 380 · Displayed: 380 (100.0%) · Load time: 0:0.8        Profile: Default
```

7. Describe the pattern you see in the values in the Identification field of the IP datagram Next (with the packets still sorted by source address) find the series of ICMP TTL exceeded replies sent to the computer by the nearest (first hop) router.

Ans:

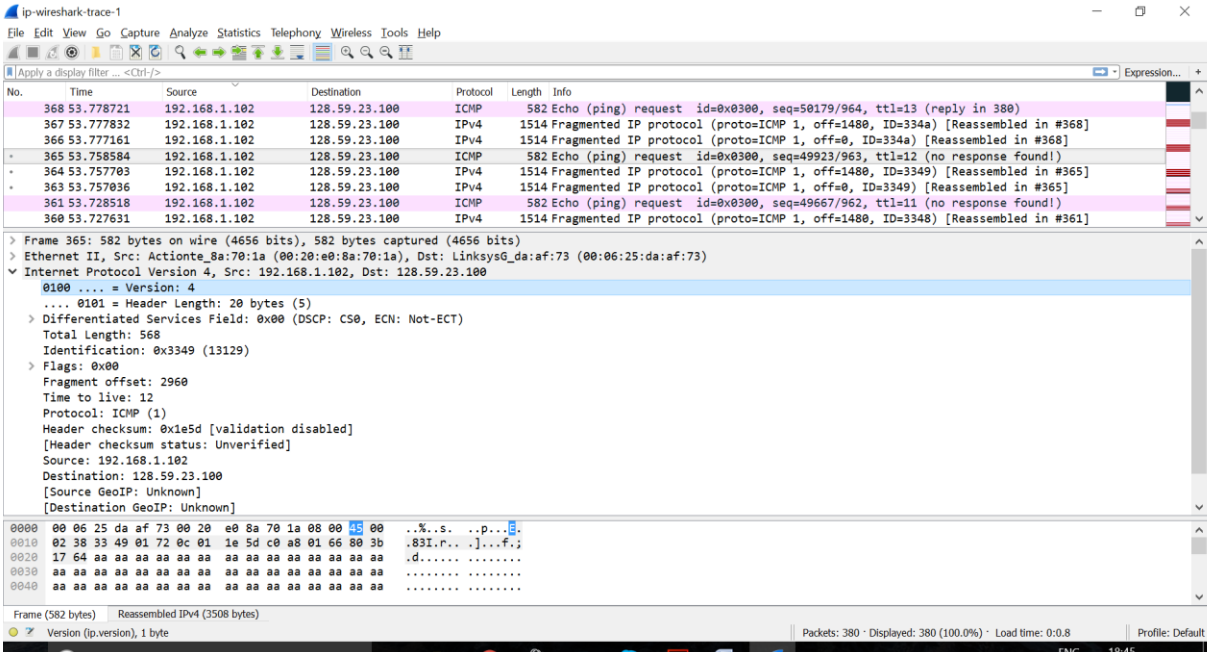
The value in the identification field of the IP datagram decreases by 1 as we move down.

Datagram 368


ip-wireshark-trace-1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...

```
No.  Time          Source          Destination     Protocol  Length Info
  368 53.778721    192.168.1.102   128.59.23.100   ICMP       582 Echo (ping) request  id=0x0300, seq=50179/964, ttl=13 (reply in 380)
  367 53.777832    192.168.1.102   128.59.23.100   IPv4      1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=334a) [Reassembled in #368]
  366 53.777161    192.168.1.102   128.59.23.100   IPv4      1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=334a) [Reassembled in #368]
  365 53.758584    192.168.1.102   128.59.23.100   ICMP       582 Echo (ping) request  id=0x0300, seq=49923/963, ttl=12 (no response found!)
  364 53.757703    192.168.1.102   128.59.23.100   IPv4      1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3349) [Reassembled in #365]
  363 53.757036    192.168.1.102   128.59.23.100   IPv4      1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=3349) [Reassembled in #365]
  361 53.728518    192.168.1.102   128.59.23.100   ICMP       582 Echo (ping) request  id=0x0300, seq=49667/962, ttl=11 (no response found!)
  360 53.727631    192.168.1.102   128.59.23.100   IPv4      1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3348) [Reassembled in #361]

> Frame 368: 582 bytes on wire (4656 bits), 582 bytes captured (4656 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, Dst: 128.59.23.100
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 568
    Identification: 0x334a (13130)
  > Flags: 0x00
    Fragment offset: 2960
    Time to live: 13
    Protocol: ICMP (1)
    Header checksum: 0x1d5c [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.102
    Destination: 128.59.23.100
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]

0000  00 06 25 da af 73 00 20  e0 8a 70 1a 08 00 45 00   ..%..s.  ..p...E.
0010  02 38 33 4a 01 72 0d 01  1d 5c c0 a8 01 66 80 3b   .83J.r.. .\...f.;
0020  17 64 aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   .d...... ........
0030  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ........ ........
0040  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ........ ........

Frame (582 bytes)   Reassembled IPv4 (3508 bytes)
Version (ip.version), 1 byte        Packets: 380 · Displayed: 380 (100.0%) · Load time: 0:0.8        Profile: Default
```

Datagram 365


ip-wireshark-trace-1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...

```
No.   Time        Source          Destination     Protocol  Length Info
  368 53.778721   192.168.1.102   128.59.23.100   ICMP       582 Echo (ping) request  id=0x0300, seq=50179/964, ttl=13 (reply in 380)
  367 53.777832   192.168.1.102   128.59.23.100   IPv4      1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=334a) [Reassembled in #368]
  366 53.777161   192.168.1.102   128.59.23.100   IPv4      1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=334a) [Reassembled in #368]
  365 53.758584   192.168.1.102   128.59.23.100   ICMP       582 Echo (ping) request  id=0x0300, seq=49923/963, ttl=12 (no response found!)
  364 53.757703   192.168.1.102   128.59.23.100   IPv4      1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3349) [Reassembled in #365]
  363 53.757036   192.168.1.102   128.59.23.100   IPv4      1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=3349) [Reassembled in #365]
  361 53.728518   192.168.1.102   128.59.23.100   ICMP       582 Echo (ping) request  id=0x0300, seq=49667/962, ttl=11 (no response found!)
  360 53.727631   192.168.1.102   128.59.23.100   IPv4      1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3348) [Reassembled in #361]
```

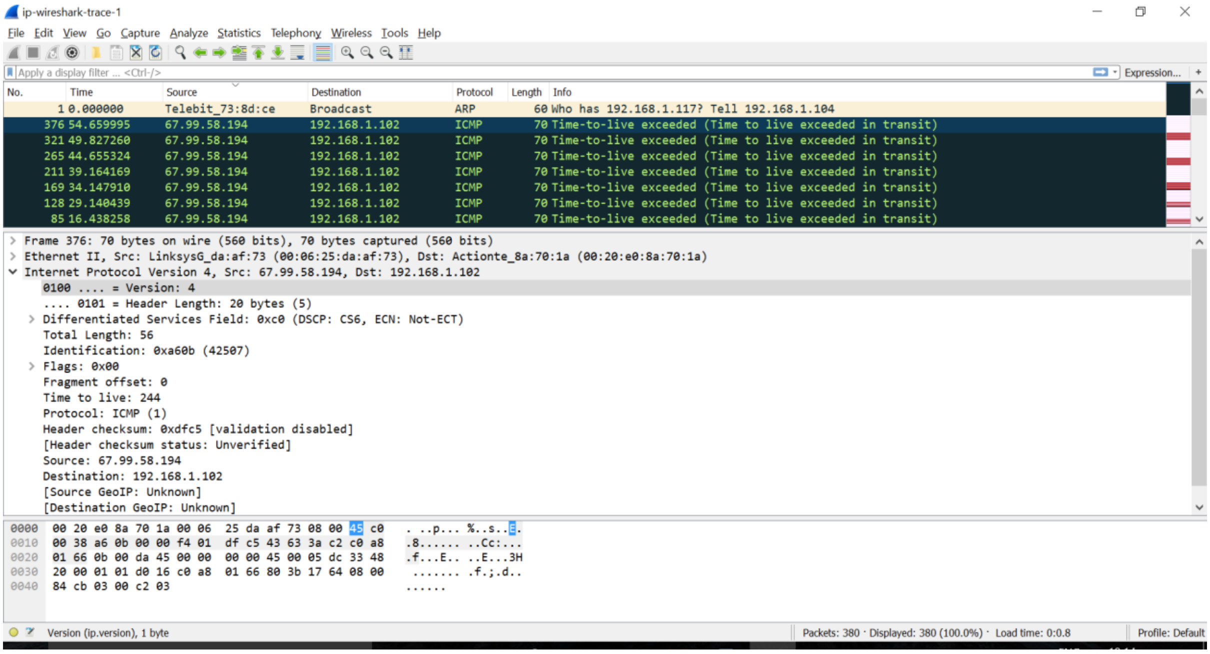
```
> Frame 365: 582 bytes on wire (4656 bits), 582 bytes captured (4656 bits)
> Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
v Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 568
    Identification: 0x3349 (13129)
  > Flags: 0x00
    Fragment offset: 2960
    Time to live: 12
    Protocol: ICMP (1)
    Header checksum: 0x1e5d [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.102
    Destination: 128.59.23.100
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
```

```
0000  00 06 25 da af 73 00 20  e0 8a 70 1a 08 00 45 00   ..%..s.  ..p...E.
0010  02 38 33 49 01 72 0c 01  1e 5d c0 a8 01 66 80 3b   .83I.r.. .]...f.;
0020  17 64 aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   .d...... ........
0030  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ........ ........
0040  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ........ ........
```

Frame (582 bytes) | Reassembled IPv4 (3508 bytes)

Version (ip.version), 1 byte | Packets: 380 · Displayed: 380 (100.0%) · Load time: 0:0.8 | Profile: Default

Series of ICMP TTL exceeded replies sent to the computer


ip-wireshark-trace-1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...

```
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
  376 54.659995   67.99.58.194       192.168.1.102   ICMP        70 Time-to-live exceeded (Time to live exceeded in transit)
  321 49.827260   67.99.58.194       192.168.1.102   ICMP        70 Time-to-live exceeded (Time to live exceeded in transit)
  265 44.655324   67.99.58.194       192.168.1.102   ICMP        70 Time-to-live exceeded (Time to live exceeded in transit)
  211 39.164169   67.99.58.194       192.168.1.102   ICMP        70 Time-to-live exceeded (Time to live exceeded in transit)
  169 34.147910   67.99.58.194       192.168.1.102   ICMP        70 Time-to-live exceeded (Time to live exceeded in transit)
  128 29.140439   67.99.58.194       192.168.1.102   ICMP        70 Time-to-live exceeded (Time to live exceeded in transit)
   85 16.438258   67.99.58.194       192.168.1.102   ICMP        70 Time-to-live exceeded (Time to live exceeded in transit)
```

```
> Frame 376: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)
> Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: Actionte_8a:70:1a (00:20:e0:8a:70:1a)
v Internet Protocol Version 4, Src: 67.99.58.194, Dst: 192.168.1.102
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
    Total Length: 56
    Identification: 0xa60b (42507)
  > Flags: 0x00
    Fragment offset: 0
    Time to live: 244
    Protocol: ICMP (1)
    Header checksum: 0xdfc5 [validation disabled]
    [Header checksum status: Unverified]
    Source: 67.99.58.194
    Destination: 192.168.1.102
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
```

```
0000  00 20 e0 8a 70 1a 00 06  25 da af 73 08 00 45 c0   . ..p... %..s..E.
0010  00 38 a6 0b 00 00 f4 01  df c5 43 63 3a c2 c0 a8   .8...... ..Cc:...
0020  01 66 0b 00 da 45 00 00  00 00 45 00 05 dc 33 48   .f...E.. ..E...3H
0030  20 00 01 01 d0 16 c0 a8  01 66 80 3b 17 64 08 00    ....... .f.;.d..
0040  84 cb 03 00 c2 03                                  ......
```

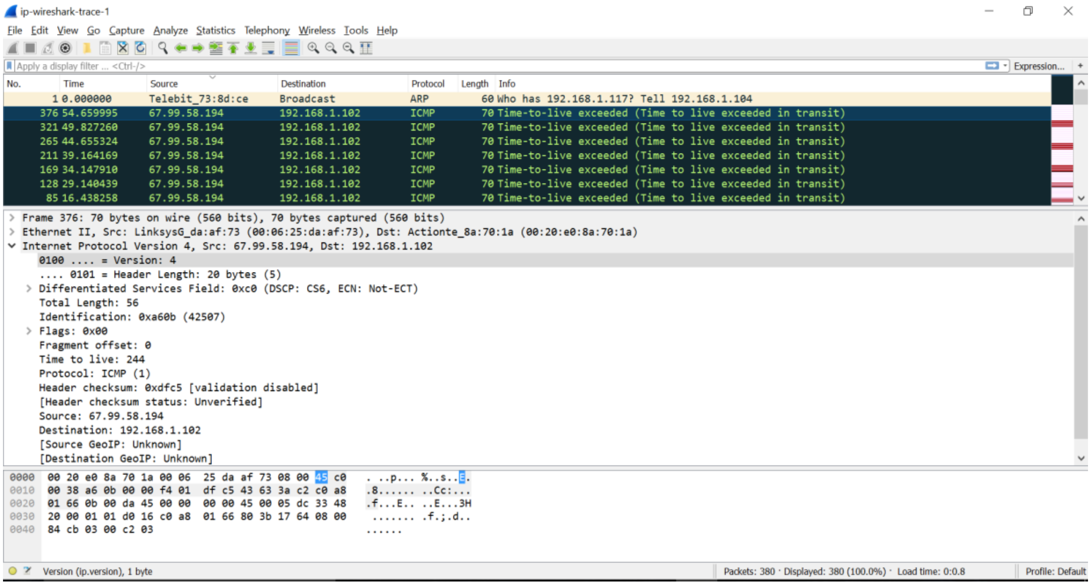
Version (ip.version), 1 byte | Packets: 380 · Displayed: 380 (100.0%) · Load time: 0:0.8 | Profile: Default

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

Ans:

Identification: 0xa60b (42507)

Time to Live: 244


ip-wireshark-trace-1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
Version (ip.version), 1 byte
Packets: 380 · Displayed: 380 (100.0%) · Load time: 0:0.8
Profile: Default

```
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
    376 54.659995   67.99.58.194      192.168.1.102   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
    321 49.827260   67.99.58.194      192.168.1.102   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
    265 44.655324   67.99.58.194      192.168.1.102   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
    211 39.164169   67.99.58.194      192.168.1.102   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
    169 34.147910   67.99.58.194      192.168.1.102   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
    128 29.140439   67.99.58.194      192.168.1.102   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
     85 16.438258   67.99.58.194      192.168.1.102   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
```

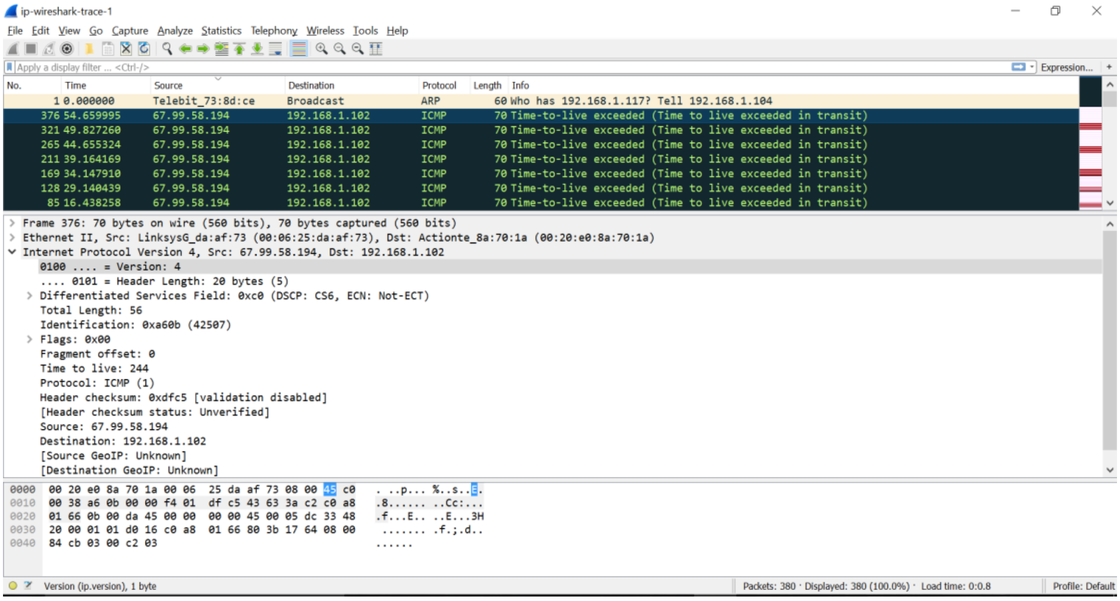
```
> Frame 376: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)
> Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: Actionte_8a:70:1a (00:20:e0:8a:70:1a)
v Internet Protocol Version 4, Src: 67.99.58.194, Dst: 192.168.1.102
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
    Total Length: 56
    Identification: 0xa60b (42507)
  > Flags: 0x00
    Fragment offset: 0
    Time to live: 244
    Protocol: ICMP (1)
    Header checksum: 0xdfc5 [validation disabled]
    [Header checksum status: Unverified]
    Source: 67.99.58.194
    Destination: 192.168.1.102
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
```

```
0000  00 20 e0 8a 70 1a 00 06  25 da af 73 08 00 45 c0   . ..p... %..s..E.
0010  00 38 a6 0b 00 00 f4 01  df c5 43 63 3a c2 c0 a8   .8...... ..Cc:...
0020  01 66 0b 00 da 45 00 00  00 00 45 00 05 dc 33 48   .f...E.. ..E...3H
0030  20 00 01 01 d0 16 c0 a8  01 66 80 3b 17 64 08 00    ....... .f.;.d..
0040  84 cb 03 00 c2 03                                   ......
```

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

Ans:

The identification value changes from one packet to another as each packet has unique identification, but the TTL values remain the same for the series of ICMP TTL exceeded replies sent to the computer as no datagram is sent to the computer.

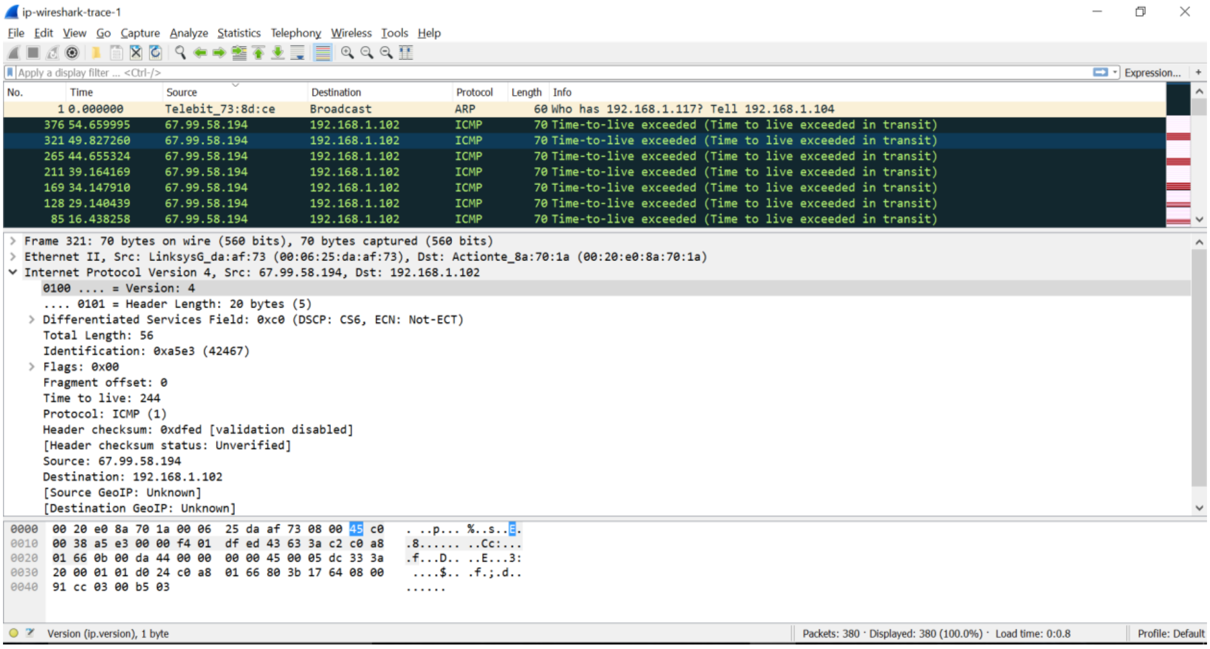


```
No.     Time        Source            Destination     Protocol  Length  Info
      1 0.000000    Telebit_73:8d:ce  Broadcast       ARP       60 Who has 192.168.1.117? Tell 192.168.1.104
    376 54.659995   67.99.58.194      192.168.1.102   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
    321 49.827260   67.99.58.194      192.168.1.102   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
    265 44.655324   67.99.58.194      192.168.1.102   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
    211 39.164169   67.99.58.194      192.168.1.102   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
    169 34.147910   67.99.58.194      192.168.1.102   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
    128 29.140439   67.99.58.194      192.168.1.102   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
     85 16.438258   67.99.58.194      192.168.1.102   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
```

```
> Frame 376: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)
> Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: Actionte_8a:70:1a (00:20:e0:8a:70:1a)
v Internet Protocol Version 4, Src: 67.99.58.194, Dst: 192.168.1.102
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
    Total Length: 56
    Identification: 0xa60b (42507)
  > Flags: 0x00
    Fragment offset: 0
    Time to live: 244
    Protocol: ICMP (1)
    Header checksum: 0xdfc5 [validation disabled]
    [Header checksum status: Unverified]
    Source: 67.99.58.194
    Destination: 192.168.1.102
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
```

```
0000  00 20 e0 8a 70 1a 00 06  25 da af 73 08 00 45 c0   . ..p... %..s..E.
0010  00 38 a6 0b 00 00 f4 01  df c5 43 63 3a c2 c0 a8   .8...... ..Cc:...
0020  01 66 0b 00 da 45 00 00  00 00 45 00 05 dc 33 48   .f...E.. ..E...3H
0030  20 00 01 01 d0 16 c0 a8  01 66 80 3b 17 64 08 00    ....... .f.;.d..
0040  84 cb 03 00 c2 03                                   ......
```

ip-wireshark-trace-1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
Version (ip.version), 1 byte
Packets: 380 · Displayed: 380 (100.0%) · Load time: 0:0.8
Profile: Default

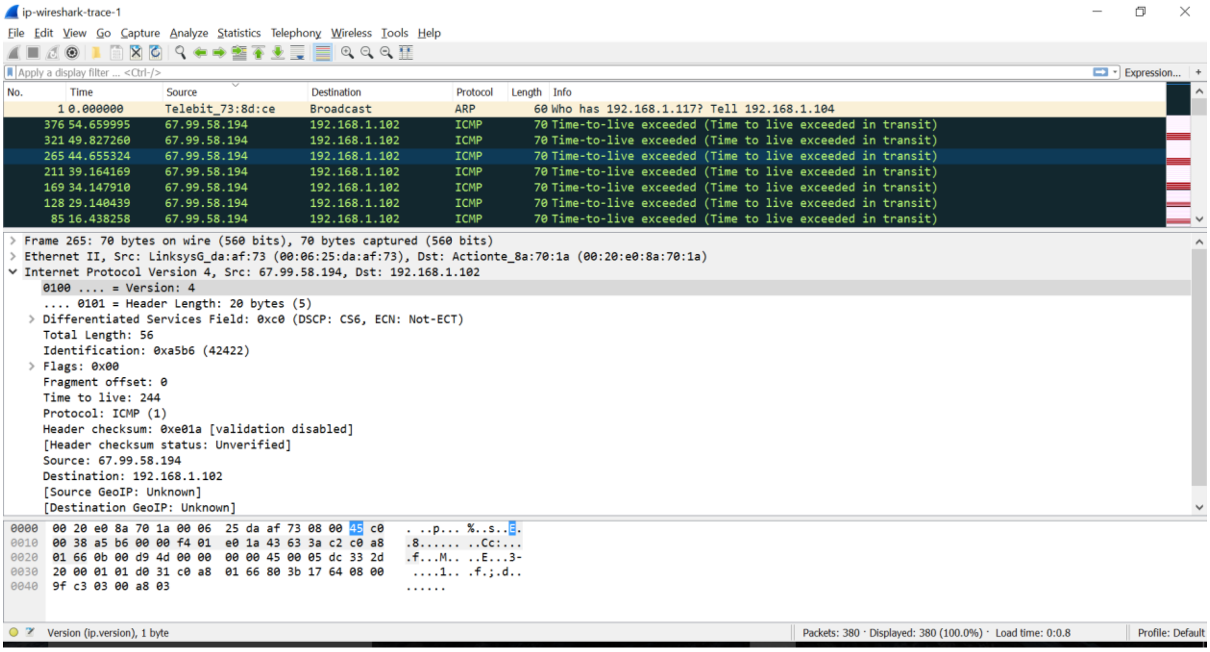

ip-wireshark-trace-1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
+

```
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
  376  54.659995   67.99.58.194      192.168.1.102   ICMP          70  Time-to-live exceeded (Time to live exceeded in transit)
  321  49.827260   67.99.58.194      192.168.1.102   ICMP          70  Time-to-live exceeded (Time to live exceeded in transit)
  265  44.655324   67.99.58.194      192.168.1.102   ICMP          70  Time-to-live exceeded (Time to live exceeded in transit)
  211  39.164169   67.99.58.194      192.168.1.102   ICMP          70  Time-to-live exceeded (Time to live exceeded in transit)
  169  34.147910   67.99.58.194      192.168.1.102   ICMP          70  Time-to-live exceeded (Time to live exceeded in transit)
  128  29.140439   67.99.58.194      192.168.1.102   ICMP          70  Time-to-live exceeded (Time to live exceeded in transit)
   85  16.438258   67.99.58.194      192.168.1.102   ICMP          70  Time-to-live exceeded (Time to live exceeded in transit)
```

```
> Frame 321: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)
> Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: Actionte_8a:70:1a (00:20:e0:8a:70:1a)
v Internet Protocol Version 4, Src: 67.99.58.194, Dst: 192.168.1.102
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
    Total Length: 56
    Identification: 0xa5e3 (42467)
  > Flags: 0x00
    Fragment offset: 0
    Time to live: 244
    Protocol: ICMP (1)
    Header checksum: 0xdfed [validation disabled]
    [Header checksum status: Unverified]
    Source: 67.99.58.194
    Destination: 192.168.1.102
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
```

```
0000  00 20 e0 8a 70 1a 00 06  25 da af 73 08 00 45 c0   . ..p... %..s..E.
0010  00 38 a5 e3 00 00 f4 01  df ed 43 63 3a c2 c0 a8   .8...... ..Cc:...
0020  01 66 0b 00 da 44 00 00  00 00 45 00 05 dc 33 3a   .f...D.. ..E...3:
0030  20 00 01 01 d0 24 c0 a8  01 66 80 3b 17 64 08 00    ....$.. .f.;.d..
0040  91 cc 03 00 b5 03                                  ......
```

Version (ip.version), 1 byte
Packets: 380 · Displayed: 380 (100.0%) · Load time: 0:0.8
Profile: Default


ip-wireshark-trace-1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
+

```
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
  376  54.659995   67.99.58.194      192.168.1.102   ICMP          70  Time-to-live exceeded (Time to live exceeded in transit)
  321  49.827260   67.99.58.194      192.168.1.102   ICMP          70  Time-to-live exceeded (Time to live exceeded in transit)
  265  44.655324   67.99.58.194      192.168.1.102   ICMP          70  Time-to-live exceeded (Time to live exceeded in transit)
  211  39.164169   67.99.58.194      192.168.1.102   ICMP          70  Time-to-live exceeded (Time to live exceeded in transit)
  169  34.147910   67.99.58.194      192.168.1.102   ICMP          70  Time-to-live exceeded (Time to live exceeded in transit)
  128  29.140439   67.99.58.194      192.168.1.102   ICMP          70  Time-to-live exceeded (Time to live exceeded in transit)
   85  16.438258   67.99.58.194      192.168.1.102   ICMP          70  Time-to-live exceeded (Time to live exceeded in transit)
```

```
> Frame 265: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)
> Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: Actionte_8a:70:1a (00:20:e0:8a:70:1a)
v Internet Protocol Version 4, Src: 67.99.58.194, Dst: 192.168.1.102
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
    Total Length: 56
    Identification: 0xa5b6 (42422)
  > Flags: 0x00
    Fragment offset: 0
    Time to live: 244
    Protocol: ICMP (1)
    Header checksum: 0xe01a [validation disabled]
    [Header checksum status: Unverified]
    Source: 67.99.58.194
    Destination: 192.168.1.102
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
```

```
0000  00 20 e0 8a 70 1a 00 06  25 da af 73 08 00 45 c0   . ..p... %..s..E.
0010  00 38 a5 b6 00 00 f4 01  e0 1a 43 63 3a c2 c0 a8   .8...... ..Cc:...
0020  01 66 0b 00 d9 4d 00 00  00 00 45 00 05 dc 33 2d   .f...M.. ..E...3-
0030  20 00 01 01 d0 31 c0 a8  01 66 80 3b 17 64 08 00    ....1.. .f.;.d..
0040  9f c3 03 00 a8 03                                  ......
```

Version (ip.version), 1 byte
Packets: 380 · Displayed: 380 (100.0%) · Load time: 0:0.8
Profile: Default