

## Foundation of Computer Networks - Wireshark Project

### Bhavin Oza (bo2115)

No.	Time	Source	Destination	Protocol	Length	Info
8	21:48:02.821397	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20483/848, ttl=1 (no response found!)
9	21:48:02.835178	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
10	21:48:02.846981	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20739/849, ttl=2 (no response found!)
11	21:48:02.861309	24.218.0.153	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
12	21:48:02.866949	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20995/850, ttl=3 (no response found!)
13	21:48:02.892857	24.128.190.197	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

▼ Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
▼ Destination: LinksysG_da:af:73 (00:06:25:da:af:73)
Address: LinksysG_da:af:73 (00:06:25:da:af:73)
.... 0. .... = LG bit: Globally unique address (factory default)
.... 0. .... = IG bit: Individual address (unicast)
▼ Source: Actionte_8a:70:1a (00:20:e0:8a:70:1a)
Address: Actionte_8a:70:1a (00:20:e0:8a:70:1a)
.... 0. .... = LG bit: Globally unique address (factory default)
.... 0. .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
▼ 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
0... .... = Reserved bit: Not set
.0.. .... = Don't fragment: Not set
..0. .... = More fragments: Not set
...0 0000 0000 = Fragment Offset: 0
> Time to Live: 1
Protocol: ICMP (1)
Header Checksum: 0x2d2c [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.1.102
Destination Address: 128.59.23.100
> Internet Control Message Protocol

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 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	.....
0040	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	.....
0060	aa aa		..

1). 192.168.1.102

2). ICMP (1)

3). Header length = 20 bytes

Total length = 84 bytes.

Hence,  $84 - 20 = 64$  bytes in payload of IP datagram.

4). No. More fragmented bits set to 0.

5). Identification, Time to Live and Header checksum.

6). The fields that stay constant are:

Version, Header Length, Differentiated Services, Upper layer protocol, Source address and Destination address.

These fields need to be constant as:

Version -> All packets are IPv4

Header Length -> All are ICMP packets

Differentiated Services -> All use same type of service class

## Foundation of Computer Networks - Wireshark Project

### Bhavin Oza (bo2115)

Upper layer protocol -> All are ICMP packets

Source address -> All packets are sent from same source IP

Destination address -> All packets are sent to same destination IP

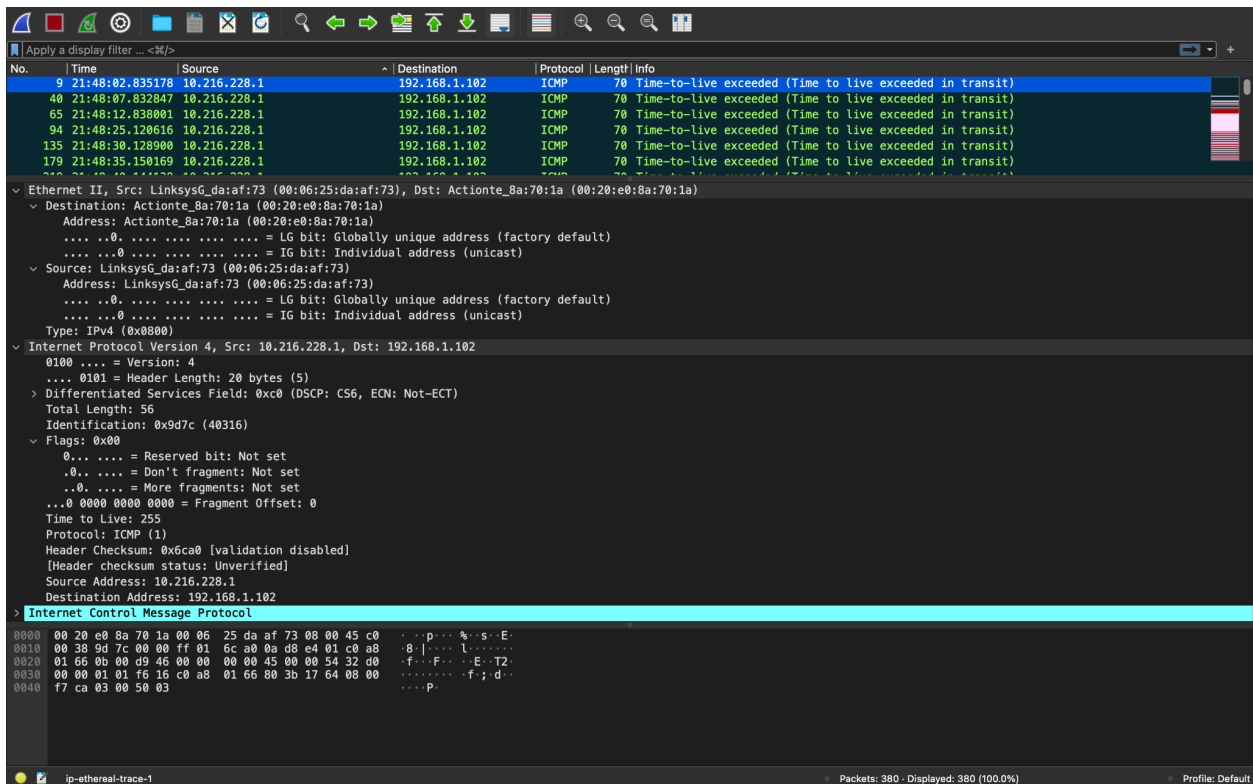
These fields need to change as:

Identification -> Each of the IP packets should have a different id

Time to live -> Each subsequent packet is incremented by the traceroute

Header checksum -> As the header changes, so does the header checksum

#### 7). TTL increases



#### 8). Identification ID -> 40316

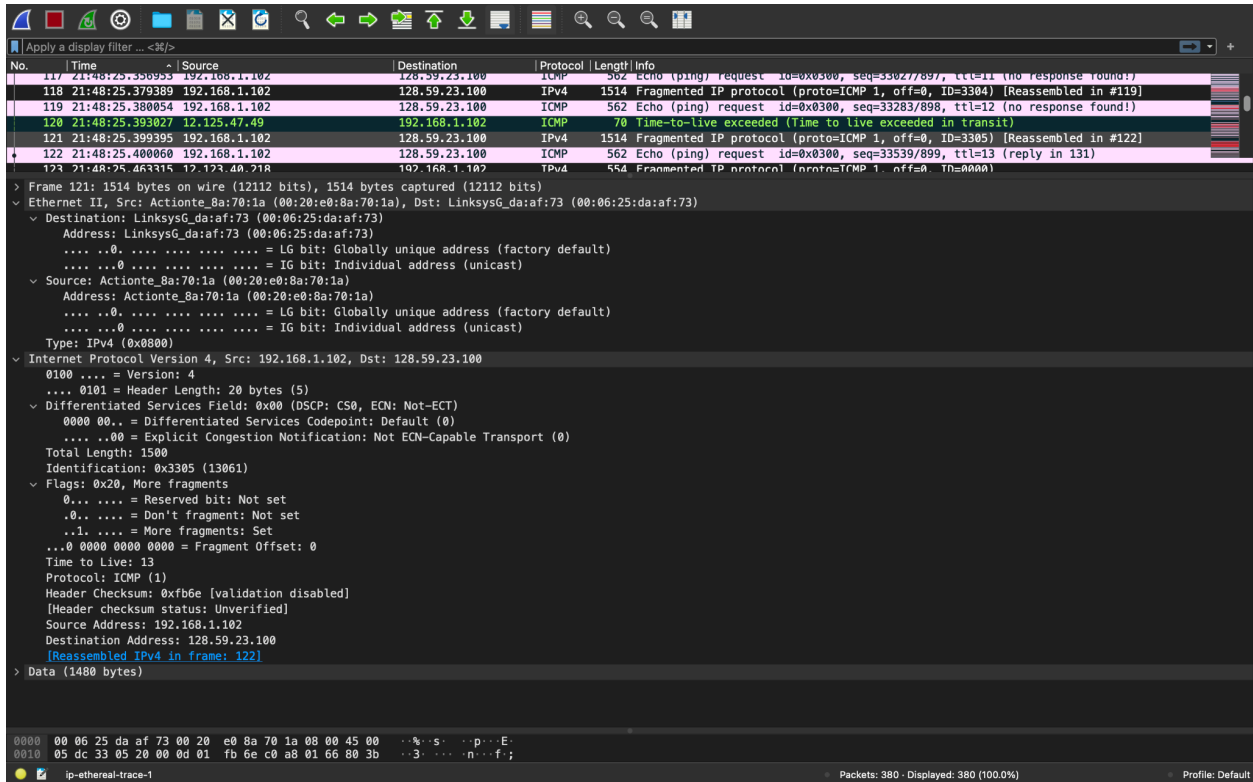
TTL-exceeded value -> 255

#### 9). TTL-exceeded value always remains the same for first hop routers.

Identification field changes as it is always different for each IP datagram.

# Foundation of Computer Networks - Wireshark Project

## Bhavin Oza (bo2115)

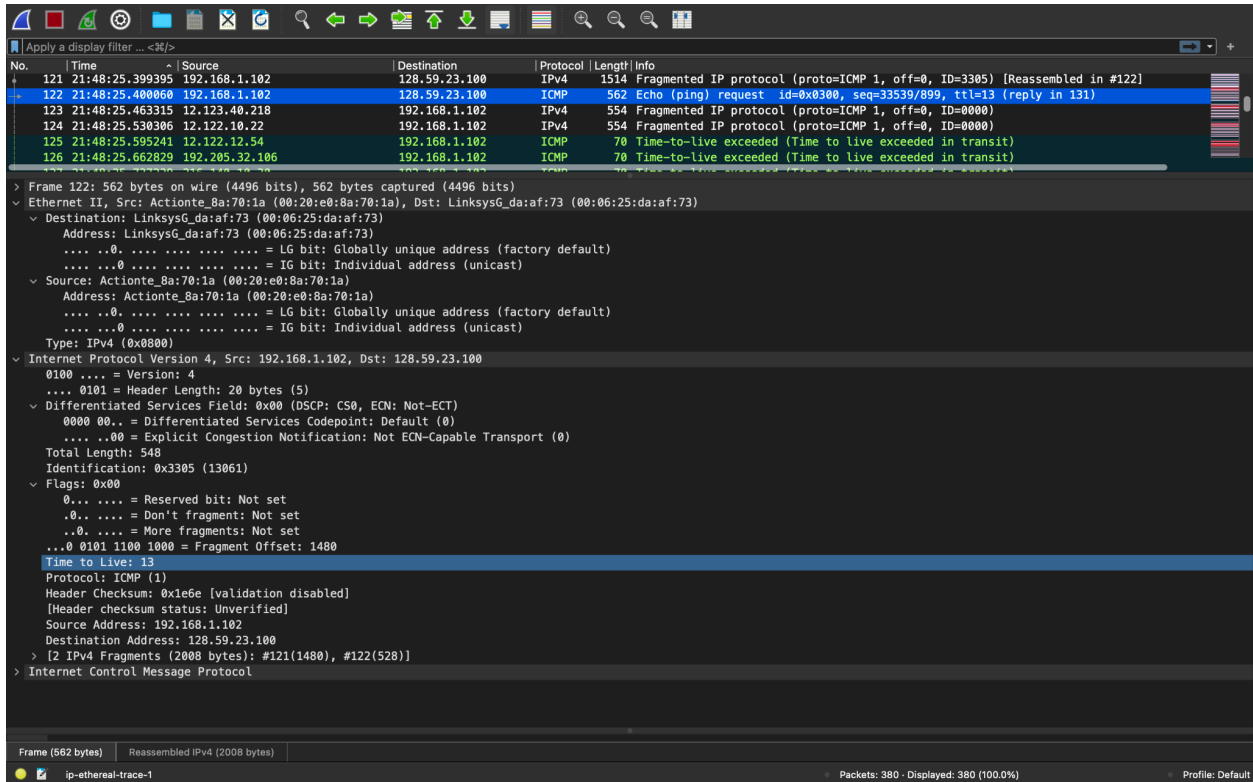


10). Yes

11). Flag for more fragments is set, indicating the datagram is fragmented.  
Fragment offset is 0, indicating this is the first fragment.  
Total length of first datagram -> 1500 bytes, including 20 bytes of header.

## Foundation of Computer Networks - Wireshark Project

### Bhavin Oza (bo2115)



12). Fragment offset if set to 1480, indicating this is not the first fragment.

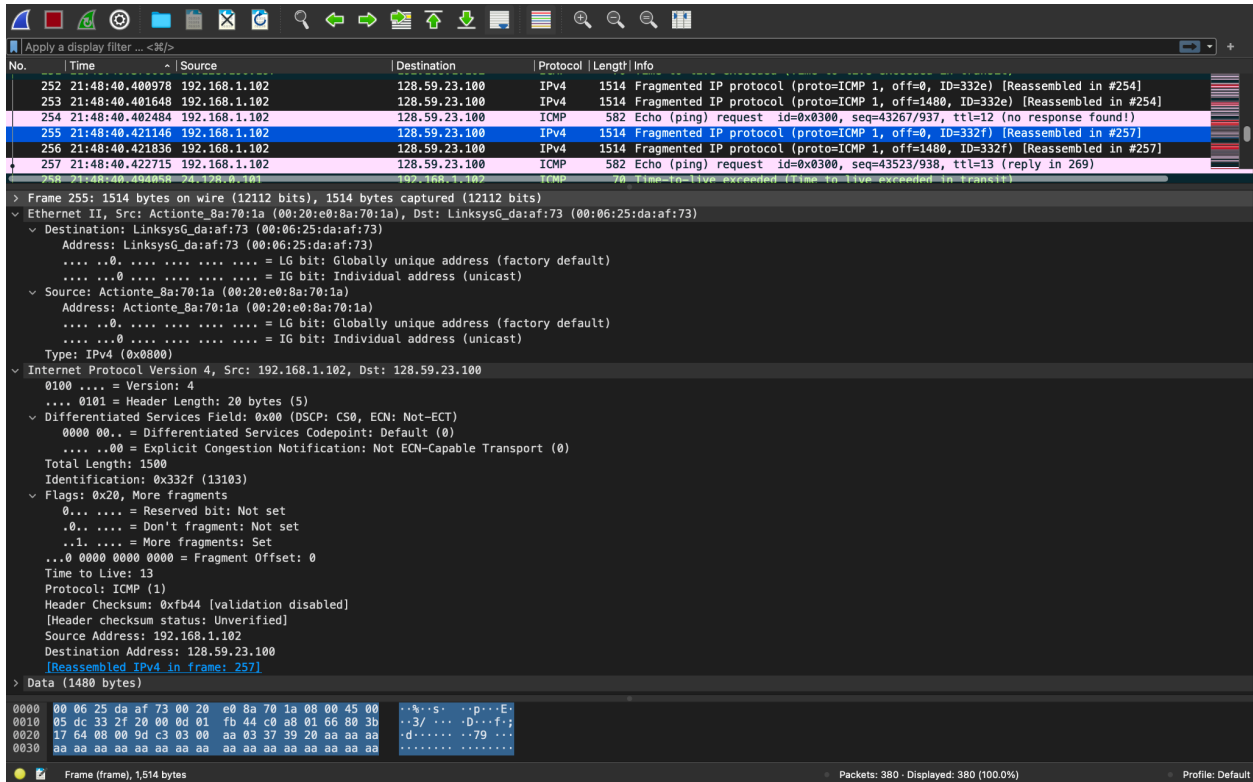
No, there are no more fragments, hence this is the last fragment.

Flag for more fragments is not set, indicating this is the last fragment.

13). Total length, checksum, flags and fragment offset.

# Foundation of Computer Networks - Wireshark Project

## Bhavin Oza (bo2115)



14). 3

15). Fragment offset, More fragment flag, Header checksum and total length.

The first two fragments have a total length as 1500 and the last fragment has a total length as 568.

The first two fragments have more fragment flags set, whereas the last fragment does not have it.

All three fragments have differences in header checksum and fragment offset.