

COMP-3670 Lab 3- Wireshark Lab: IP v7.0 Questions 8-15

Donovan Longo

105011200

8. The identification field has a value of: 39108

The TTL field has a value of: 250

2140	143.333805	154.54.89.85	192.168.0.80	ICMP	110 Time-to-live exceeded (Time to live exceeded in transit)
2069	142.340137	154.54.89.85	192.168.0.80	ICMP	110 Time-to-live exceeded (Time to live exceeded in transit)
1997	141.332162	154.54.89.85	192.168.0.80	ICMP	110 Time-to-live exceeded (Time to live exceeded in transit)

>	Frame 2140: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface \Device\NPF_{940CBB90-F1E1-4F69-A185-E3812C8CFF51}, id 0
>	Ethernet II, Src: 02:00:00:00:00:04 (02:00:00:00:00:04), Dst: HonHaiPr_06:e7:09 (90:32:4b:06:e7:09)
▼	Internet Protocol Version 4, Src: 154.54.89.85, Dst: 192.168.0.80
	0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
>	Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
	Total Length: 96
	Identification: 0x98c4 (39108)
>	Flags: 0x00
	Fragment Offset: 0
	Time to Live: 250
	Protocol: ICMP (1)
	Header Checksum: 0x7354 [validation disabled]
	[Header checksum status: Unverified]
	Source Address: 154.54.89.85
	Destination Address: 192.168.0.80
>	Internet Control Message Protocol

9. The identification field does not remain unchanged for all the ICMP TTL-exceeded replies to sent to our computer. This is because the identification field is a unique value given to all datagrams. The only time an IP datagram has the same identification value is when the datagram has been fragmented. The Time to Live field does remain unchanged, keeping the value of 250 for all the TTL-exceeded replies to the computer. Below is a screenshot of another ICMP TTL-exceeded reply to prove my answer. TTL is still 250 but the identification field has the value of 38980.

2140	143.333805	154.54.89.85	192.168.0.80	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
2069	142.340137	154.54.89.85	192.168.0.80	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
1997	141.332162	154.54.89.85	192.168.0.80	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
1925	140.340322	154.54.89.85	192.168.0.80	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
1854	139.339714	154.54.89.85	192.168.0.80	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
1774	138.332036	154.54.89.85	192.168.0.80	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
1701	137.332675	154.54.89.85	192.168.0.80	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
1634	136.085451	154.54.89.85	192.168.0.80	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
1540	121.950317	154.54.89.85	192.168.0.80	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
1485	120.950831	154.54.89.85	192.168.0.80	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
1432	119.948084	154.54.89.85	192.168.0.80	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
1379	118.952623	154.54.89.85	192.168.0.80	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
1327	117.947131	154.54.89.85	192.168.0.80	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
1275	116.948878	154.54.89.85	192.168.0.80	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
1222	115.952523	154.54.89.85	192.168.0.80	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)

```

> Frame 2069: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface \Device\NPF_{940CBB90-F1E1-4F69-A185-E3812C8CFF51}
> Ethernet II, Src: 02:00:00:00:00:04 (02:00:00:00:00:04), Dst: HonHaiPr_06:e7:09 (90:32:4b:06:e7:09)
▼ Internet Protocol Version 4, Src: 154.54.89.85, Dst: 192.168.0.80
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        Total Length: 96
        Identification: 0x9844 (38980)
    > Flags: 0x00
        Fragment Offset: 0
        Time to Live: 250
        Protocol: ICMP (1)
        Header Checksum: 0x73d4 [validation disabled]
        [Header checksum status: Unverified]
        Source Address: 154.54.89.85
        Destination Address: 192.168.0.80
> Internet Control Message Protocol

```

Fragmentation

10. Yes, the first ICMP Echo request sent from our computer with a large size was fragmented across more than one IP datagram.

797	108.553135	192.168.0.80	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=0046) [Reassembled in #798]
798	108.553135	192.168.0.80	128.119.245.12	ICMP	534	Echo (ping) request id=0x0001, seq=3911/18191, ttl=255 (reply in 809)

```

> Frame 797: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF_{940CBB90-F1E1-4F69-A185-E3812C8CFF51}, id 0
> Ethernet II, Src: HonHaiPr_06:e7:09 (90:32:4b:06:e7:09), Dst: 02:00:00:00:00:04 (02:00:00:00:00:04)
▼ Internet Protocol Version 4, Src: 192.168.0.80, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        Total Length: 1500
        Identification: 0x0046 (70)
    > Flags: 0x20, More fragments
        Fragment Offset: 0
        Time to Live: 255
        Protocol: ICMP (1)
        Header Checksum: 0x5f5e [validation disabled]
        [Header checksum status: Unverified]
        Source Address: 192.168.0.80
        Destination Address: 128.119.245.12
        [Reassembled IPv4 in frame: 798]
> Data (1480 bytes)

```

11. Using the screenshot above we can tell this datagram has been fragmented since the Flags field is set for more fragments. To determine whether this is the first fragment versus a latter fragment we can use the Fragment Offset field which the value is 0. This indicates this is the first fragment. Lastly the IP datagram has a length of 1480 bytes from the data and 20 bytes from the header totaling to 1500 bytes.

12. The Fragment Offset field in the IP deafer indicates that it is not the first fragment. This is because the value of fragment offset is 1480, not zero resulting this fragment is not the first datagram fragment. Since the Flags value is not set to more fragments, we can conclude this is the last fragment. Screenshot included below.

```
> 798 108.553135      192.168.0.80        128.119.245.12     ICMP               534 [Echo (ping) request id=0x0001, seq=3911/18191, ttl=255 (reply in 809)]
```

```
> Frame 798: 534 bytes on wire (4272 bits), 534 bytes captured (4272 bits) on interface \Device\NPF_{940CB890-F1E1-4F69-A185-E3B12C8CF5F1}, id 0  
Ethernet II, Src: HonHaiPr_06:e7:09 (90:32:4b:06:e7:09), Dst: 02:00:00:00:00:04 (02:00:00:00:00:04)  
Internet Protocol Version 4, Src: 192.168.0.80, Dst: 128.119.245.12  
    0100 .... = Version: 4  
    .... 0101 = Header Length: 20 bytes (5)  
    > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  
    Total Length: 520  
    Identification: 0x0046 (70)  
    Flags: 0x00  
        0... .... = Reserved bit: Not set  
        .0.. .... = Don't fragment: Not set  
        ..0. .... = More fragments: Not set  
    Fragment Offset: 1480  
    Time to Live: 255  
    Protocol: ICMP (1)  
    Header Checksum: 0x8279 [validation disabled]  
    [Header checksum status: Unverified]  
    Source Address: 192.168.0.80  
    Destination Address: 128.119.245.12  
    > [2 IPv4 Fragments (1980 bytes): #797(1480), #798(500)]  
        [Frame: 797, payload: 0-1479 (1480 bytes)]  
        [Frame: 798, payload: 1480-1979 (500 bytes)]  
        [Fragment count: 2]  
        [Reassembled IPv4 length: 1980]  
        [Reassembled IPv4 data: 08002cfc00010f4720202020202020202020202020202020202020202020.]  
> Internet Control Message Protocol
```