Jason Xin
ECS 152A

Programming 1: Wireshark IP Lab

I used the given example files in the lab, from http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip, as I had a hard time getting pingplotter to function correctly with 2000 byte datagrams.

```
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)
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 Address: 192.168.1.102
    Destination Address: 128.59.23.100
```

1. The IP address of the source is 192.168.1.102, and this should be my computer's IP. (I used the example files so this could be different).
2. The value in the upper layer of the protocol field is ICMP (1).
3. There are 20 bytes in the IP header. Given our packet size of 56, that means the payload was 56 - 20 = 36 bytes.
4. There is no fragmentation, and the fragmentation offset of the packets that follow is 0.

```
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)
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: 0x01
    Fragment Offset: 2960
    Time to Live: 13
    Protocol: ICMP (1)
    Header Checksum: 0x1d5c [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.102
    Destination Address: 128.59.23.100
  > [3 IPv4 Fragments (3508 bytes): #366(1480), #367(1480), #368(548)]
```

5. The Identification, Time to Live, and Header Checksum fields change.
6. I found that the Version, Header Length, Source Address, Destination Address, Differentiated Services Field, and Protocol stayed the same throughout the IP datagrams. All of these fields must stay constant. The version is consistent, because it was set to IPv4. Header length stayed consistent because header length for IPv4 does

not change. Source Address and Destination Address stay constant because our source and destination for these datagrams stayed the same throughout the process, and the IPs used didn't change. Differentiated Services and (Upper Layer) Protocol stayed the same because the same protocol was used for every one of these trials. As listed above, the Identification and Header Checksum fields must change. The IP Datagrams all have a unique ID, so the Identification field is different. The header changes for each datagram, so the header checksum also changes. However, Time to Live doesn't always change, (this may be due to time to live for each datagram sometimes being insignificantly small) but does more often than not.

7. The Identification field increments with each ICMP request.

```
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)
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 Address: 67.99.58.194
    Destination Address: 192.168.1.102
```

8. The Identification field had a value of 0xa60b (42507), while the TTL field was 244.
9. The Identification field changes, as the replies all have unique values. However, the Time to Live is constant across all of the replies. I think this is because Time to Live is the same for replies to the same first router, but Identification has to be unique across these replies, or else they would be considered part of the same datagram.

```
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: 548
    Identification: 0x32f9 (13049)
  > Flags: 0x00
    Fragment Offset: 1480
  > Time to Live: 1
    Protocol: ICMP (1)
    Header Checksum: 0x2a7a [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.102
    Destination Address: 128.59.23.100
  > [2 IPv4 Fragments (2008 bytes): #92(1480), #93(528)]
```

10. Yes, the bottom part lists that the datagram has been broken into 1 IPv4 fragments.

```
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: 1500
    Identification: 0x32f9 (13049)
  > Flags: 0x20, More fragments
    Fragment Offset: 0
  > Time to Live: 1
    Protocol: ICMP (1)
    Header Checksum: 0x077b [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.102
    Destination Address: 128.59.23.100
    [Reassembled IPv4 in frame: 93]
```

11. The Flags section is set to 0x20, and wireshark tells us that this meansdata has been fragmented. We know that this is the first of the fragments because the fragmentation offset field is set to 0, whereas if it was a later fragment, this field would be some non-zero number. The IP datagram has a length of 1500.

```
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: 548
    Identification: 0x32f9 (13049)
  > Flags: 0x00
    Fragment Offset: 1480
  > Time to Live: 1
    Protocol: ICMP (1)
    Header Checksum: 0x2a7a [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.102
    Destination Address: 128.59.23.100
  v [2 IPv4 Fragments (2008 bytes): #92(1480), #93(528)]
```

12. We know this fragment is the second because the fragmentation offset is 1480, meaning that there was some fragment before it. This is the last fragment of the datagram, as this packet's Flags section is 0x00, which indicates no more fragments.
13. The IP header fields that change between these two fragments are the total length, the Flags, the fragmentation offset, and the checksum.

```
Frame 216: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 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)
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: 1500
    Identification: 0x3323 (13091)
  > Flags: 0x20, More fragments
    Fragment Offset: 0
  > Time to Live: 1
    Protocol: ICMP (1)
    Header Checksum: 0x0751 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.102
    Destination Address: 128.59.23.100
    [Reassembled IPv4 in frame: 218]
```

```
Frame 217: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 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)
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: 1500
    Identification: 0x3323 (13091)
  > Flags: 0x20, More fragments
    Fragment Offset: 1480
  > Time to Live: 1
    Protocol: ICMP (1)
    Header Checksum: 0x0698 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.102
    Destination Address: 128.59.23.100
    [Reassembled IPv4 in frame: 218]
```

```
Frame 218: 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)
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: 0x3323 (13091)
  > Flags: 0x01
    Fragment Offset: 2960
  > Time to Live: 1
    Protocol: ICMP (1)
    Header Checksum: 0x2983 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.102
    Destination Address: 128.59.23.100
  v [3 IPv4 Fragments (3508 bytes): #216(1480), #217(1480), #218(548)]
```

14. With a datagram size of 3500, there were 3 packets that the datagram was fragmented and is sent as. We see this in the third picture above in the last field.
15. The IP header fields that change between all these three fragments are the fragmentation offset, and the checksum. The first two packets have the same total length (1500), but the last is different (568). This difference is also seen in the Flags field: the

first two packets have a value set of 0x20 that means more fragments, while the last one does not.