Assignment 6 - Wireshark Lab: IP v6.0

Packet trace taken from author

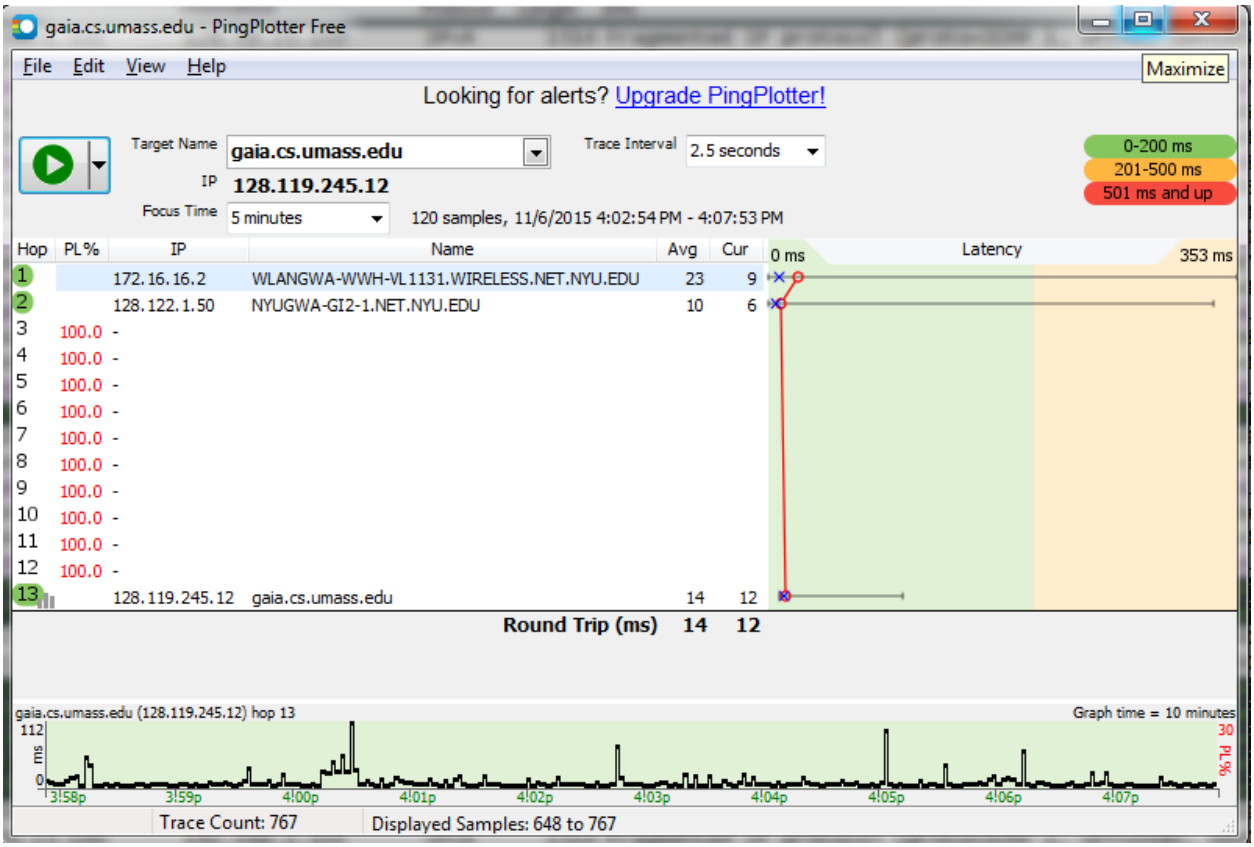

Figure 1 – Ping Plot to gaia.cs.umass.edu

Answer 1:

```
No.     Time                           Source                Destination           Protocol Length Info
      8 2004-08-22 01:48:02.821397     192.168.1.102         128.59.23.100         ICMP     98     Echo (ping) reque
st  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)
Internet Protocol Version 4, Src: 192.168.1.102 (192.168.1.102), Dst: 128.59.23.100 (128.59.23.100)
  Version: 4
  Header Length: 20 bytes
```

The IP address of the computer is **192.168.1.102**

Answer 2:

```
Internet Protocol Version 4, Src: 192.168.1.102 (192.168.1.102), Dst: 128.59.23.100 (128.59.23.100)
  Version: 4
  Header Length: 20 bytes
  Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
  Total Length: 84
  Identification: 0x32d0 (13008)
  Flags: 0x00
  Fragment offset: 0
  Time to live: 1
  Protocol: ICMP (1)
  Header checksum: 0x2d2c [validation disabled]
  Source: 192.168.1.102 (192.168.1.102)
  Destination: 128.59.23.100 (128.59.23.100)
  [Source GeoIP: Unknown]
  [Destination GeoIP: Unknown]
```

Within the IP packet header, the value in the upper layer protocol field is **1 (ICMP)**

Answer 3:

```
Internet Protocol Version 4, Src: 192.168.1.102 (192.168.1.102), Dst: 128.59.23.100 (128.59.23.100)
  Version: 4
  Header Length: 20 bytes
  Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
  Total Length: 84
  Identification: 0x32d0 (13008)
  Flags: 0x00
```

The number of bytes in IP Header is **20bytes**. The size of the payload is **64bytes** since the header length is 20 bytes and the Total length is 84bytes. Total Length - Header length gives Payload length.

Answer 4:

```
Internet Protocol Version 4, Src: 192.168.1.102 (192.168.1.102), Dst: 128.59.23.100 (128.59.23.100)
  Version: 4
  Header Length: 20 bytes
  Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
  Total Length: 84
  Identification: 0x32d0 (13008)
  Flags: 0x00
  Fragment offset: 0
```

The flags otherwise indicate that there is **no fragmentation**. Also the fragment offset is 0 indicating that this is the final datagram.

Answer 5:

The fields that always change from one datagram to the next with in this series

1. **Total Length**
2. **Time to live**
3. **Identification**
4. **Header Checksum**

Answer 6:

The fields that stay constant are:-

1. **Source IP**
2. **Destination IP**
3. **Version**
4. **Protocol**
5. **Flags**

The fields that must stay constant are:-

1. **Source IP**
2. **Identification**
3. **Protocol**

Since source is sending the fragments, the source must be the same otherwise it signals different fragments. The destination can change as the source might be able to ping another destination

Identification is the way in which the destination keeps track about from which sender do these packets belong and help in building the fragments.

Protocol is always ICMP Here since ICMP messages are sent across.

Answer 7:

Yes there is a clear pattern in the Identification field of the IP Datagram. Every ICMP request has identification number incremented by 1 from the previous identification number.

Answer 8:

The first hop is **10.216.228.1** and the lists of ICMP Time to live exceeded messages are shown below:-

330	2004-08-22 01:48:50.159434	10.216.228.1	192.168.1.102	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
274	2004-08-22 01:48:45.151425	10.216.228.1	192.168.1.102	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
219	2004-08-22 01:48:40.144138	10.216.228.1	192.168.1.102	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
179	2004-08-22 01:48:35.150169	10.216.228.1	192.168.1.102	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
135	2004-08-22 01:48:30.128900	10.216.228.1	192.168.1.102	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
94	2004-08-22 01:48:25.120616	10.216.228.1	192.168.1.102	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
65	2004-08-22 01:48:12.838001	10.216.228.1	192.168.1.102	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
40	2004-08-22 01:48:07.832847	10.216.228.1	192.168.1.102	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
9	2004-08-22 01:48:02.835178	10.216.228.1	192.168.1.102	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)

The value of the Identification field = **0x9ebb (40635)** and Time to live = **255**

```
Internet Protocol Version 4, Src: 10.216.228.1 (10.216.228.1), Dst: 192.168.1.102 (192.168.1.102)
  Version: 4
  Header Length: 20 bytes
⊞ Differentiated Services Field: 0xc0 (DSCP 0x30: Class Selector 6; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
  Total Length: 56
  Identification: 0x9ebb (40635)
⊞ Flags: 0x00
  Fragment offset: 0
  Time to live: 255
```

Answer 9:

No the Identification field is not the same for all the ICMP TTL-exceeded replies since each timeout is intended for one particular IP datagram.

Time to live however has not changed indicating the sender always sends a predefined value for timeout.

Answer 10:

The first ICMP Echo request after packet size changed to 2000 is shown below. Yes the message is fragmented across more than one IP datagram as shown below.

```
Internet Protocol Version 4, Src: 192.168.1.102 (192.168.1.102), Dst: 128.59.23.100 (128.59.23.100)
  Version: 4
  Header Length: 20 bytes
⊟ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    0000 00.. = Differentiated Services Codepoint: Default (0x00)
    .... ..00 = Explicit Congestion Notification: Not-ECT (Not ECN-Capable Transport) (0x00)
  Total Length: 1500
  Identification: 0x32f9 (13049)
⊞ Flags: 0x01 (More Fragments)
  Fragment offset: 0

Internet Protocol Version 4, Src: 192.168.1.102 (192.168.1.102), Dst: 128.59.23.100 (128.59.23.100)
  Version: 4
  Header Length: 20 bytes
⊟ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    0000 00.. = Differentiated Services Codepoint: Default (0x00)
    .... ..00 = Explicit Congestion Notification: Not-ECT (Not ECN-Capable Transport) (0x00)
  Total Length: 548
  Identification: 0x32f9 (13049)
⊞ Flags: 0x00
  Fragment offset: 1480
⊟ Time to live: 1
```

Answer 11:

The print out of the first Fragment of the Fragmented IP Datagram is shown below. The **Flags field(0<<1)** and the **fragment offset(0)** indicate that this is a fragment with offset at 0th Byte which means it's fragmented. The information that indicates this is the first fragment is **Fragment Offset = 0**. The length of the IP Datagram is **1500 bytes** which is equivalent to MTU of Ethernet link layer frame**.**

```
No.     Time                        Source                Destination           Protocol Length Info
     92 2004-08-22 01:48:25.099863 192.168.1.102         128.59.23.100         IPv4     1514   Fragmented IP pro
tocol (proto=ICMP 1, off=0, ID=32f9) [Reassembled in #93]

Frame 92: 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 (192.168.1.102), Dst: 128.59.23.100 (128.59.23.100)
  Version: 4
  Header Length: 20 bytes
  Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    0000 00.. = Differentiated Services Codepoint: Default (0x00)
    .... ..00 = Explicit Congestion Notification: Not-ECT (Not ECN-Capable Transport) (0x00)
  Total Length: 1500
  Identification: 0x32f9 (13049)
  Flags: 0x01 (More Fragments)
  Fragment offset: 0
  Time to live: 1
    [Expert Info (Note/Sequence): "Time To Live" only 1]
      ["Time To Live" only 1]
      [Severity level: Note]
      [Group: Sequence]
  Protocol: ICMP (1)
  Header checksum: 0x077b [validation disabled]
```

Fig 2 – Packet Print

Answer 12:

The print of the second fragment is shown below. The offset field indicates that this is 1480th byte location which succeeds the last byte (1479th) of the first fragment which concludes this is the second fragment. No, there are no more fragments as the flags field is reset to 0 indicating this is the last fragment.

```
No.     Time                        Source                Destination           Protocol Length Info
     93 2004-08-22 01:48:25.100537 192.168.1.102         128.59.23.100         ICMP     562    Echo (ping) reque
st  id=0x0300, seq=30467/887, ttl=1 (no response found!)

Frame 93: 562 bytes on wire (4496 bits), 562 bytes captured (4496 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 (192.168.1.102), Dst: 128.59.23.100 (128.59.23.100)
  Version: 4
  Header Length: 20 bytes
  Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    0000 00.. = Differentiated Services Codepoint: Default (0x00)
    .... ..00 = Explicit Congestion Notification: Not-ECT (Not ECN-Capable Transport) (0x00)
  Total Length: 548
  Identification: 0x32f9 (13049)
  Flags: 0x00
  Fragment offset: 1480
  Time to live: 1
```

Fig 3- Packet Print

Answer 13:

The fields that change between the first and the second fragment are **Total length, Flags, offset & header checksum**.

Answer 14: For the ICMP Echo Request for packet size = 3500, the numbers of fragments created are **3** from the original datagram**.**

Fragment 1

```
No.     Time                        Source                Destination           Protocol Length Info
    216 2004-08-22 01:48:40.124488 192.168.1.102         128.59.23.100         IPv4     1514   Fragmented IP pro
tocol (proto=ICMP 1, off=0, ID=3323) [Reassembled in #218]

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 (192.168.1.102), Dst: 128.59.23.100 (128.59.23.100)
  Version: 4
  Header Length: 20 bytes
  Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    0000 00.. = Differentiated Services Codepoint: Default (0x00)
    .... ..00 = Explicit Congestion Notification: Not-ECT (Not ECN-Capable Transport) (0x00)
  Total Length: 1500
  Identification: 0x3323 (13091)
  Flags: 0x01 (More Fragments)
  Fragment offset: 0
  Time to live: 1
```

Fragment 2

```
No.     Time                        Source                Destination           Protocol Length Info
    217 2004-08-22 01:48:40.125160 192.168.1.102         128.59.23.100         IPv4     1514   Fragmented IP pro
tocol (proto=ICMP 1, off=1480, ID=3323) [Reassembled in #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 (192.168.1.102), Dst: 128.59.23.100 (128.59.23.100)
  Version: 4
  Header Length: 20 bytes
  Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    0000 00.. = Differentiated Services Codepoint: Default (0x00)
    .... ..00 = Explicit Congestion Notification: Not-ECT (Not ECN-Capable Transport) (0x00)
  Total Length: 1500
  Identification: 0x3323 (13091)
  Flags: 0x01 (More Fragments)
  Fragment offset: 1480
  Time to live: 1
```

Fragment 3

```
No.     Time                        Source                Destination           Protocol Length Info
    218 2004-08-22 01:48:40.125981 192.168.1.102         128.59.23.100         ICMP     582    Echo (ping) reque
st  id=0x0300, seq=40451/926, ttl=1 (no response found!)

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 (192.168.1.102), Dst: 128.59.23.100 (128.59.23.100)
  Version: 4
  Header Length: 20 bytes
  Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    0000 00.. = Differentiated Services Codepoint: Default (0x00)
    .... ..00 = Explicit Congestion Notification: Not-ECT (Not ECN-Capable Transport) (0x00)
  Total Length: 568
  Identification: 0x3323 (13091)
  Flags: 0x00
  Fragment offset: 2960
  Time to live: 1
```

Answer 15:

The fields that change between the first and the second fragment are **Total length, Flags, offset & header checksum**.