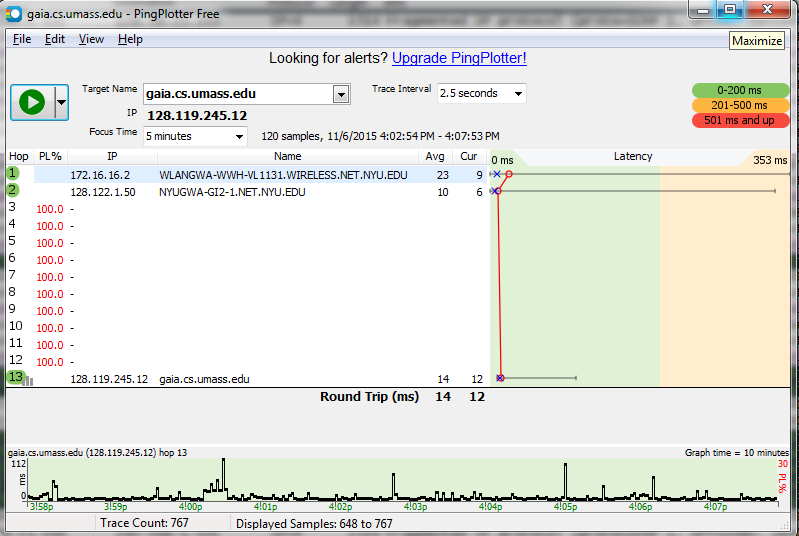
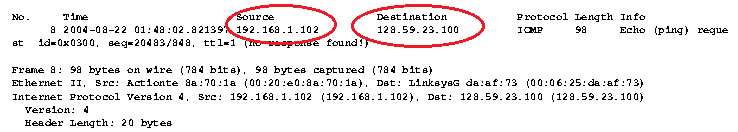
**Assignment 6 - Wireshark Lab: IP v6.0**

**Packet trace taken from author**

****

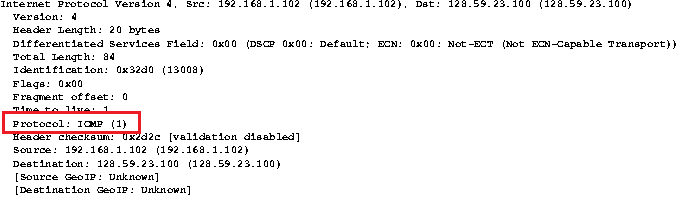
**Figure 1** – Ping Plot to gaia.cs.umass.edu

**Answer 1:**

****

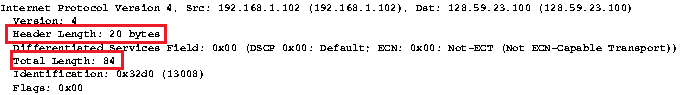
The IP address of the computer is **192.168.1.102**

**Answer 2:**



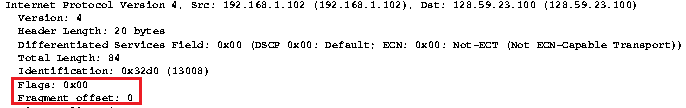
Within the IP packet header, the value in the upper layer protocol field is **1 (ICMP)**

**Answer 3:**

****

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:**

****

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.

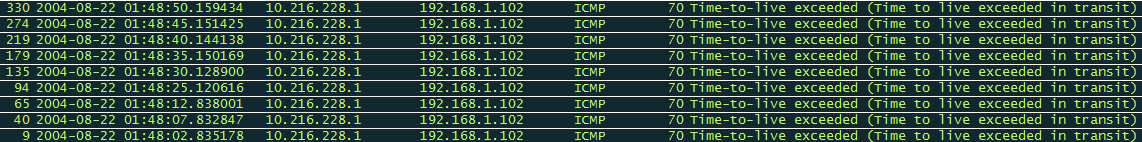
Protocol is always ICMP Here since ICMP messages are sent across.

**Answer 7:**

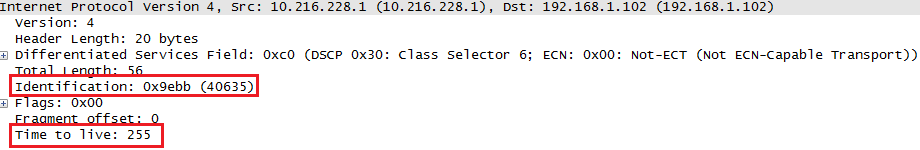
Yes there is a clear pattern in the Identification field of the IP Datagram. Every ICMP request has identification number incremented by 1 from the previous identification number.

**Answer 8:**

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



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



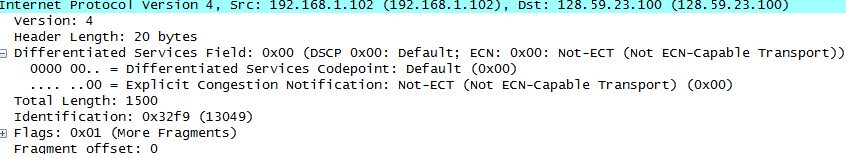
**Answer 9:**

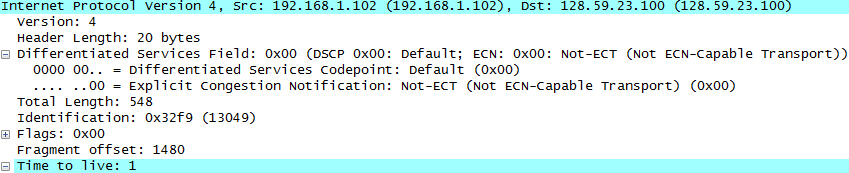
No the Identification field is not the same for all the ICMP TTL-exceeded replies since each timeout is intended for one particular IP datagram.

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

**Answer 10:**

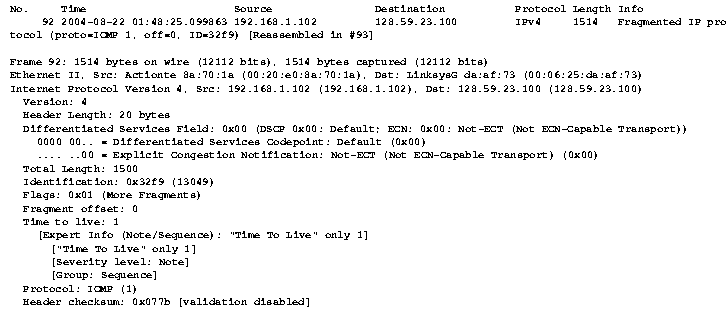
The first ICMP Echo request after packet size changed to 2000 is shown below. Yes the message is fragmented across more than one IP datagram as shown below.

****

****

**Answer 11:**

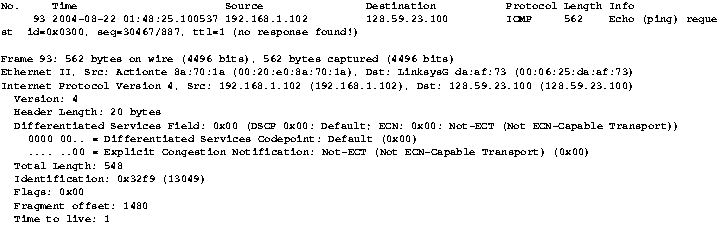
The print out of the first Fragment of the Fragmented IP Datagram is shown below. The **Flags field(0<<1)** and the **fragment offset(0)** indicate that this is a fragment with offset at 0th Byte which means it’s fragmented. The information that indicates this is the first fragment is **Fragment Offset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

****

**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.



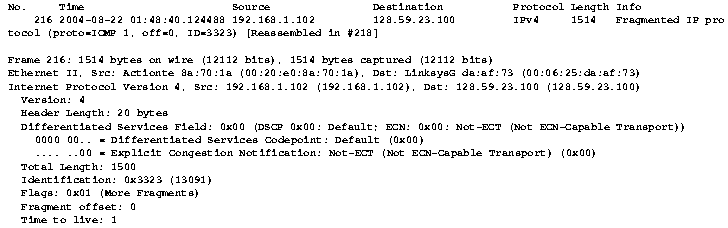
**Fig 3**- Packet Print

**Answer 13:**

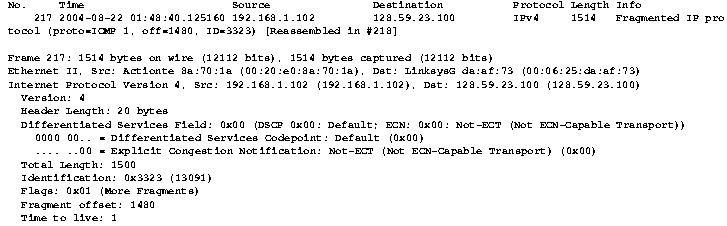
The fields that change between the first and the second fragment are **Total length, Flags, offset & header checksum**.

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

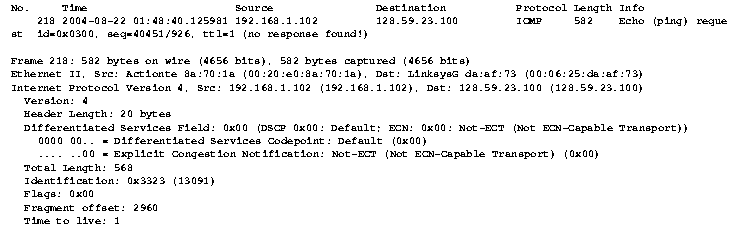
Fragment 1



Fragment 2



Fragment 3



**Answer 15:**

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