THE UNIVERSITY OF DODOMA

COLLEGE OF INFORMATICS AND VIRTUAL EDUCATION

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING (CSE)

WIRESHARK LABS PRESENTATION.

PROGRAM: BSc-CNISE

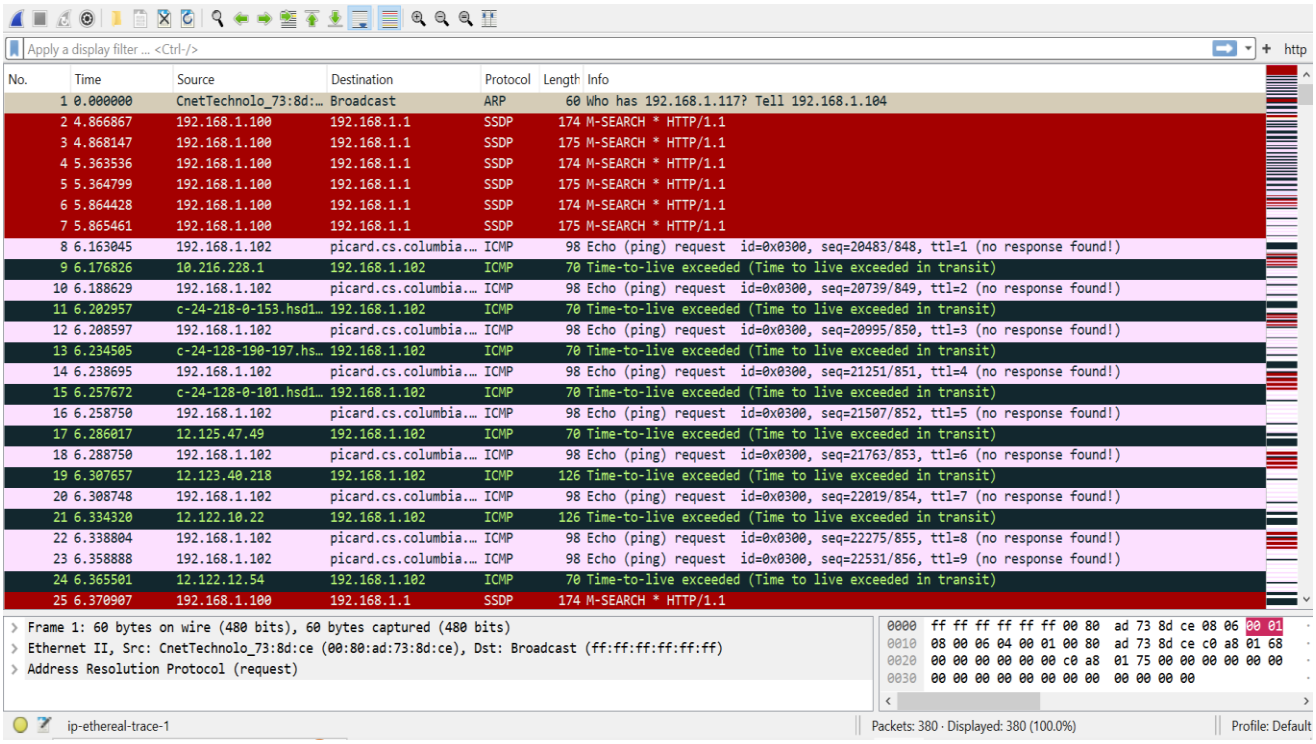
COURSE: IA 311

GROUP PARTICIPANTS

NAMES	REGISTRATION NUMBER
HENRY SELEMAN	T22-03-00295
JIMSON MAHENGE	T22-03-08372
PUDENCIANA KIYEGA	T22-03-11584
PETRO MOHERE	T22-03-02116
GEORGE KALAMU	T22-03-08400

➢ Capturing packets from an execution of traceroute.

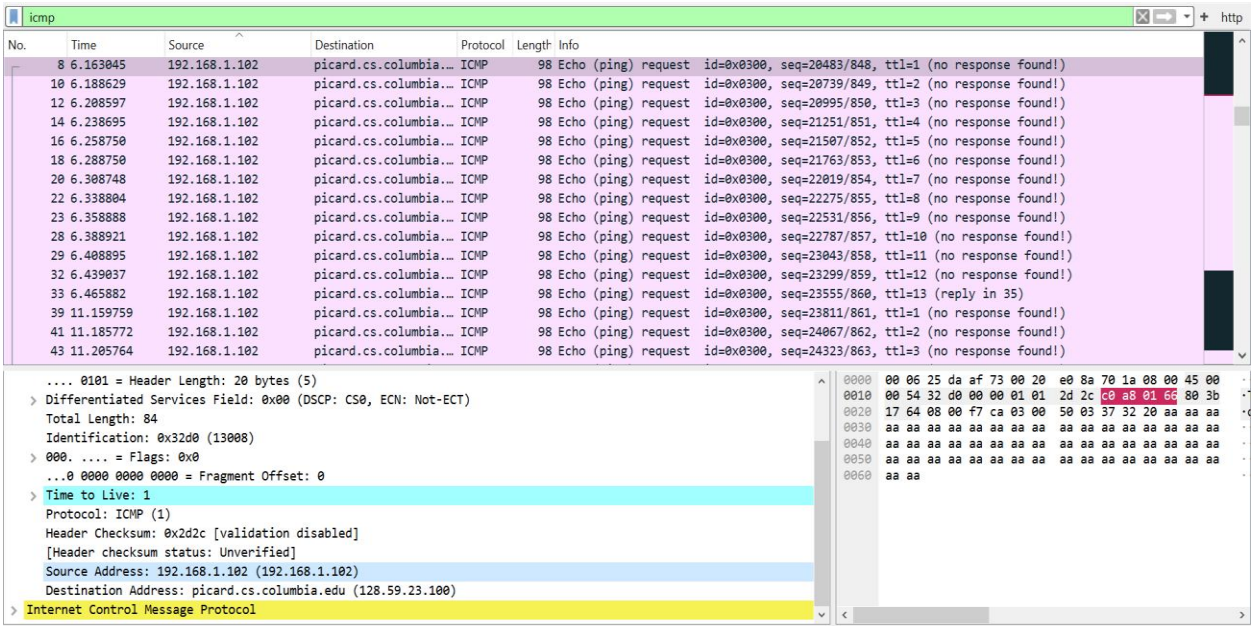
Answer:



➢ A look at the captured trace.

1. Select the first ICMP Echo Request message sent by your computer, and expand the Internet Protocol part of the packet in the packet details window.

   Answer:



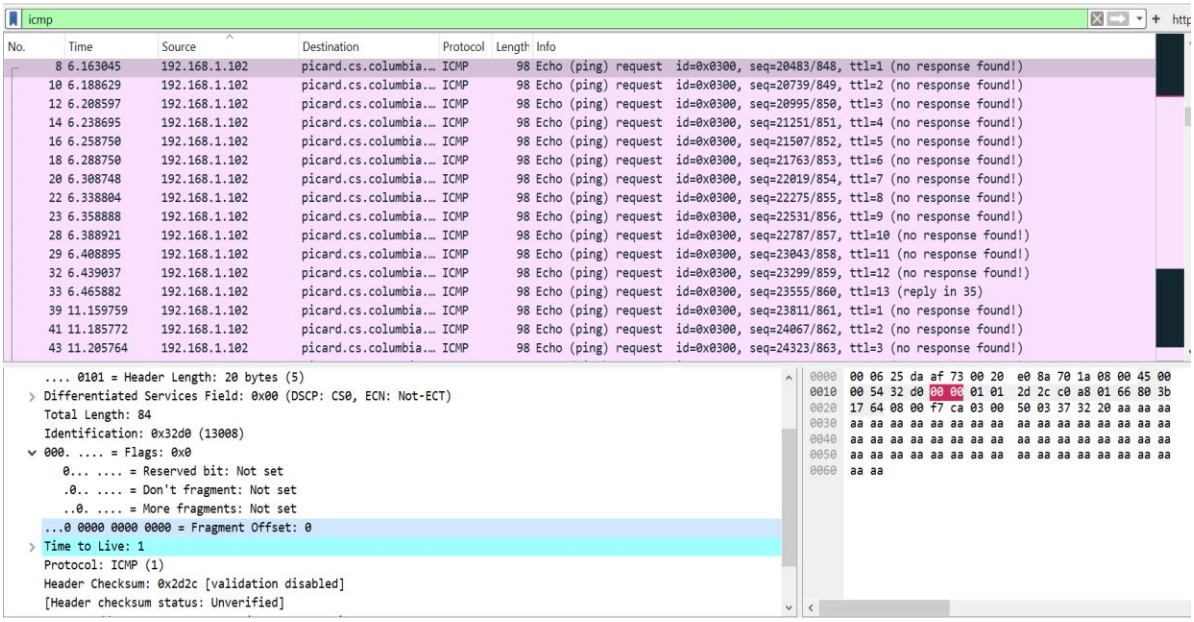
What is the IP address of your computer?

Answer: From the figure above the IP address of the computer is the Source Address that is **192.168.1.102.**

2. Within the IP packet header, what is the value in the upper layer protocol field?
   Answer:
   From the figure above**, t**he Value in the upper layer protocol field is **ICMP (1).**

3. How many bytes are in the IP header? How many bytes are in the payload of the IP datagram? Explain how you determined the number of payload bytes.
   Answer:
   From the diagram above there are **20 bytes in the IP header**. There are **64 bytes in the payload of the IP datagram.** The number of payload is determined by substracting **Header length(20 bytes) from Total length(84 bytes).**

4. Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented.
   Answer:
   Yes, the Ip datagram has been **fragmented**.Because the value of **fragment offset is 0**.

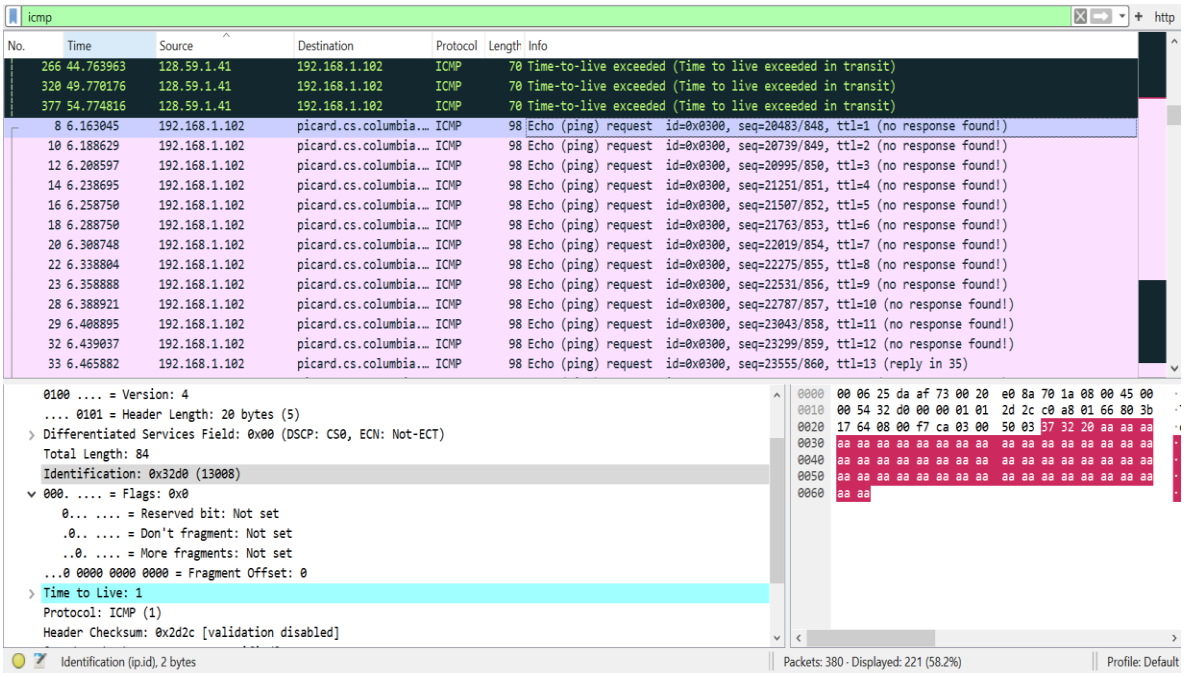


5. Which fields in the IP datagram always change from one datagram to the next within this series of ICMP messages sent by your computer?
   Answer:
   The field in IP datagram that always change from one datagram to another are **Identification and Header Checksum**.

6. Which fields stay constant? Which of the fields must stay constant? Which fields must change? Why?
   Answer:
   The fields that stay constant are usually **the source and destination IP addresses**, as well as the **protocol type (ICMP)**. **The Identification field and Header Checksum** must change to uniquely identify each datagram, as it helps in reassembling fragmented packets.

7. Describe the pattern you see in the values in the Identification field of the IP datagram.
   Answer:
   The IP header Identification fields increment in sequence with each ICMP Echo (ping) request.

8. What is the value in the Identification field and the TTL field?
   Answer:
   The value of identification field is **0x32d0 (13008) and** TTL field is **1**.



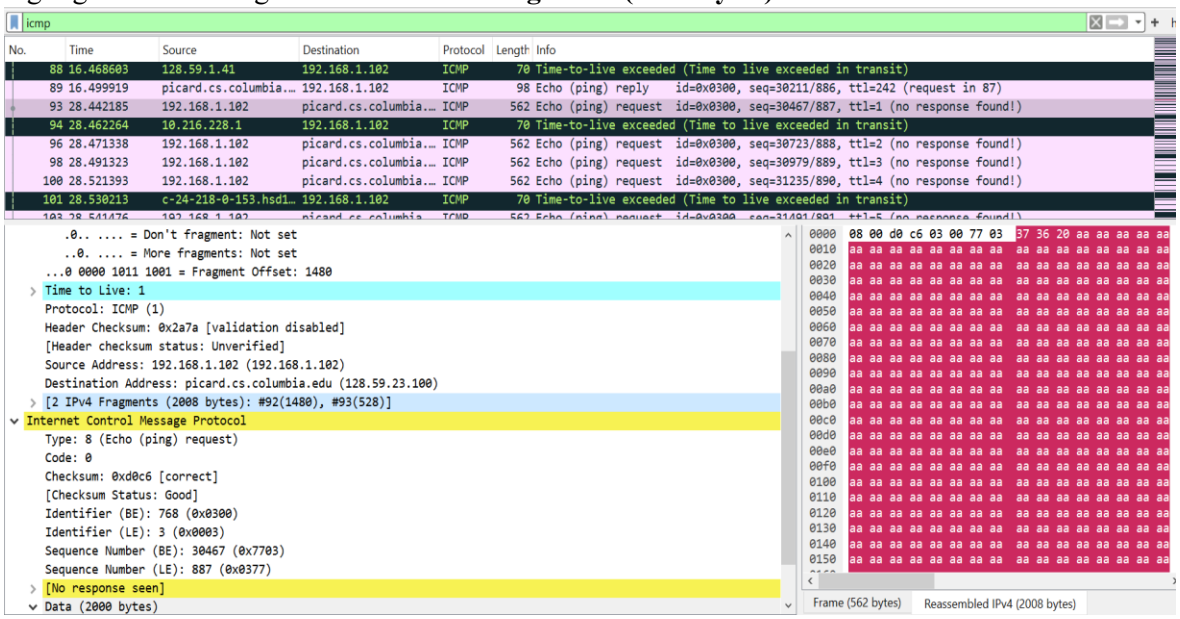
9. Do these values remain unchanged for all of the ICMP TTL-exceeded replies sent to your computer by the nearest (first hop) router? Why?
   Answer:
   TTL field is unchanged, because the TTL for the first hop router is always the same. But the identification number is different even if the TTL for the first hop router is always the same.

➢ Fragmentation.

10. Find the first ICMP Echo Request message that was sent by your computer after you changed the Packet Size in pingplotter to be 2000. Has that message been fragmented across more than one IP datagram? [Note: if you find your packet has not been fragmented, you should download the zip file http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip and extract the ipethereal-trace-1packet trace. If your computer has an Ethernet interface, a packet size of 2000 should cause fragmentation.3].

    Answer:

    Yes, that message has been **fragmented** across two IP datagram **1480 and 528** as highlighted in the diagram below **2 IPv4 fragments (2008 bytes).**



11. Print out the first fragment of the fragmented IP datagram. What information in the IP header indicates that the datagram been fragmented? What information in the IP header indicates whether this is the first fragment versus a latter fragment? How long is this IP datagram?

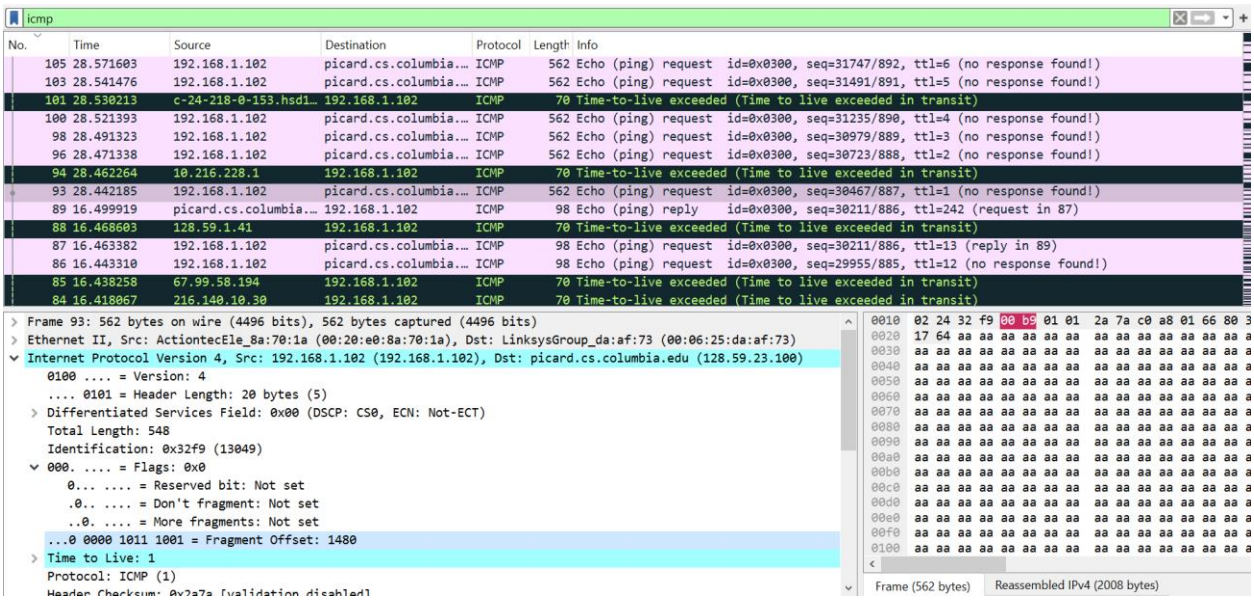
Answer:

The fact that the flag is set for more segments shows that the the datagram has been fragmented (see above).The fragment offset is set to 0 indicating that this is the first fragment rather than a latter fragment where that value is set to (1480). The datagram has a total length of 1500.

12. Print out the second fragment of the fragmented IP datagram. What information in the IP header indicates that this is not the first datagram fragment? Are the more fragments? How can you tell?

    Answer:

    The second fragment is obvious because it now has a a fragment offset of **1480**. There are no more fragments because it no longer has a flag set for more fragments.



13. What fields change in the IP header between the first and second fragment?
    Answer:
    The fields that change are **Total Length** and **Flags Set.**

14. How many fragments were created from the original datagram?
    Answer:
    After switching **to 3500 bytes**, **3 fragements** are created.

15. What fields change in the IP header among the fragments
    Answer:
    The fields that change are the fragment offset **(0, 1480, 2960) and checksum.** The first 2 packets also have lengths of 1500 and more fragments flags set, while the last fragment is shorter **(548) and** does not have a flag set.

