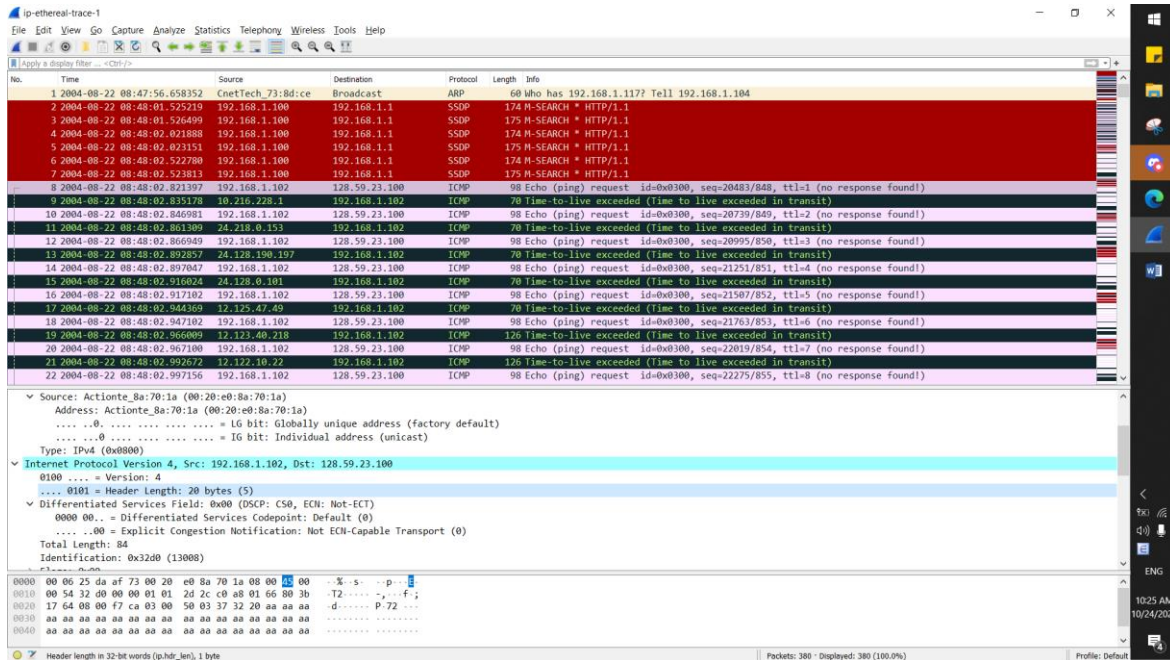
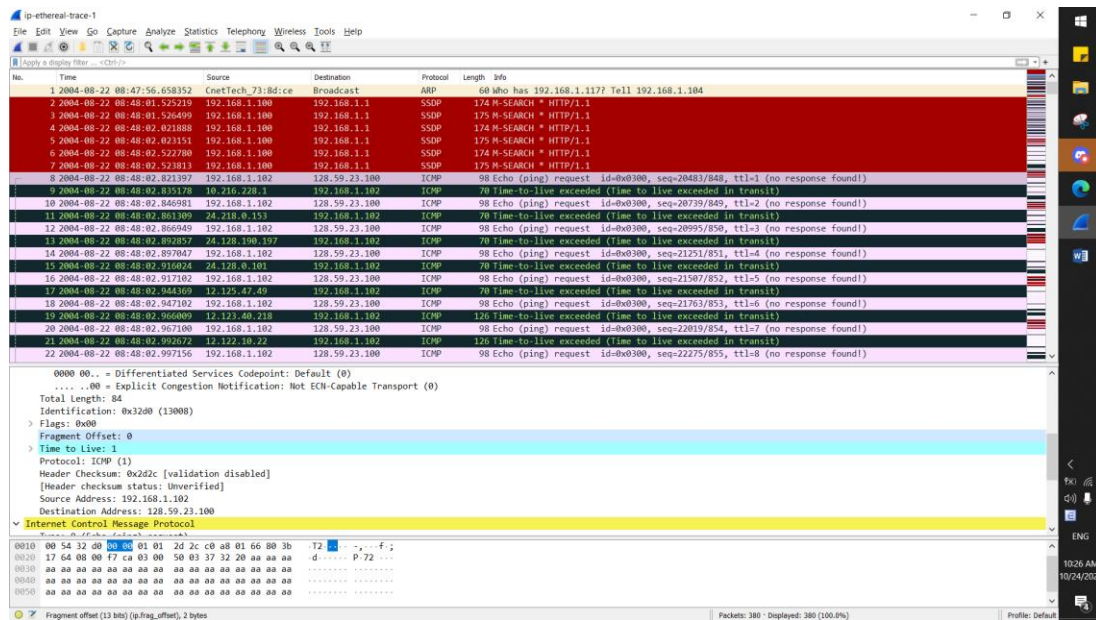


2. ICMP (1)



3. Header: 20 bytes, total 84 bytes, payload = total – header = 64 bytes

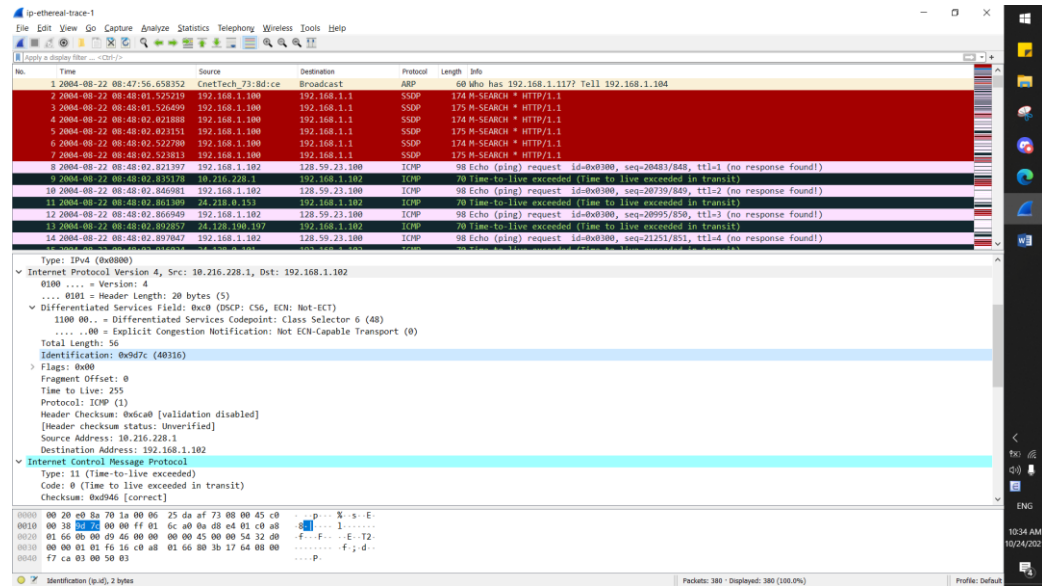


4. The fragment offset is set to 0, therefore, the packet has not been fragmented

5. The header checksum and the identification changes from each datagram to the next

6. Fields that stay constant: Version (IPv4), Length of header, Source IP, Destination IP, Upper layer protocol. Fields that must stay constant is same as above. Fields must change are the header checksum and identification

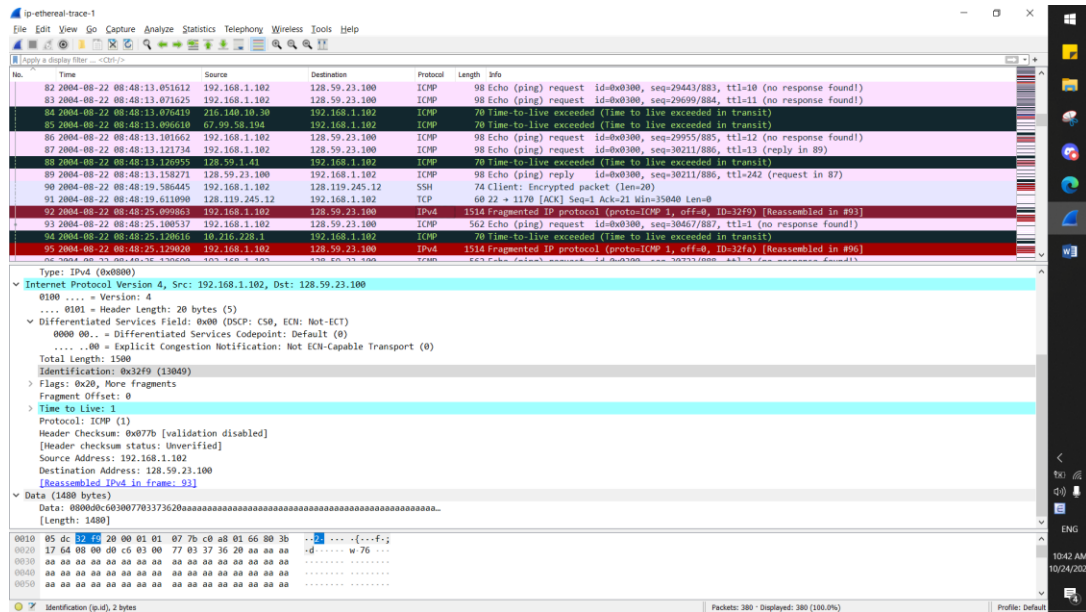
7. The pattern in the identification field is that the field increases by one in each stand of echo requests



8. Identification: 0x9d7c (40316), TTL : 255

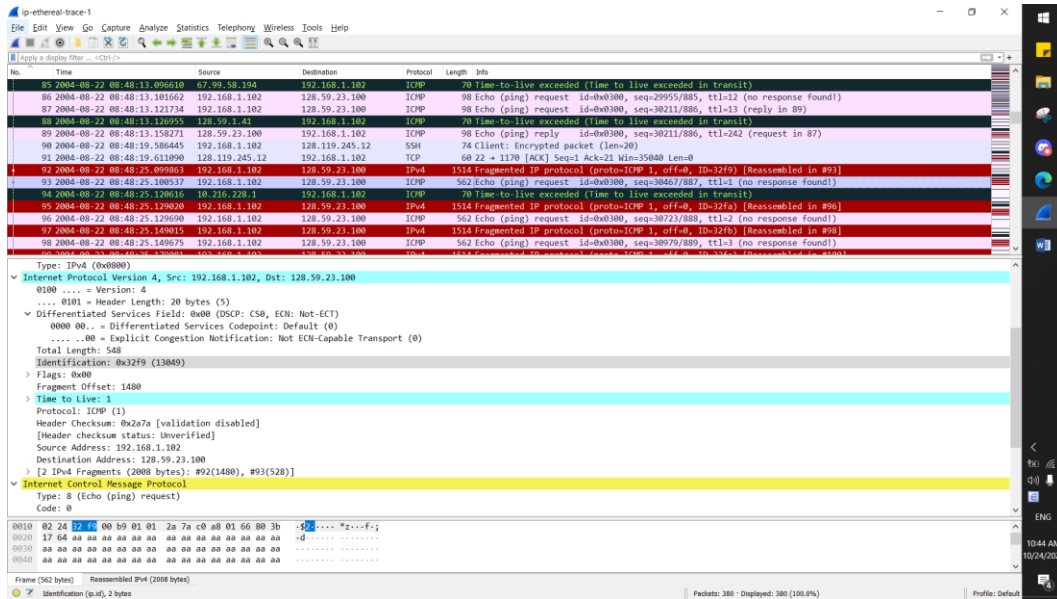
9. The identification field changes from all of the replies because this field has to have a unique value. If they (2 or more replies) have the same value then the replies must be fragments of a bigger packet

The TTL field does not change because the time to live to the first hop router is always the same.



10. Yes, that message has been fragmented across more than one IP datagram (0x20 More Fragments)

11. The fact that the flag is set for more segments shows that the datagram has been fragmented. The fragment offset is 0



12. The fragment offset is 1480. There are no more fragments because it no longer has a flag set for more fragments.

13. The fields that change are: Length, Flags Set, Fragment offset, header checksum

14. After switching to 3500 bytes, 3 fragments are created.

15. 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 (540) and does not have a flag set

