OVERVIEW:

- Investigating IP protocol: IP. Datagram
    - Analyse a trace of IP datagrams sent/received using the traceroute program

1. Capturing packets from an execution of traceroute
    a. Use the traceroute program to send datagrams of different sizes towards a destination
        i. traceroute operates by sending one/or more datagrams with the time-to-live (TTL) field in the IP header set to 1, then sends a series of one/or more datagrams towards the same destination with a TTL value of 2 and so on.
        ii. A router should decrement the TTL in each received datagram by 1 until it reaches 0 for the router to return an ICMP message to the sending host- the datagram with a TTL of 1 will cause the router on hop away from the sender to send an ICMP TTL-exceeded message back to the sender, same goes for a router 2 hops away- through this, the host executing traceroute can learn the identities of the routers between itself and the destination by looking the source IP addresses in the datagrams containing the ICMP TTL-exceeded messages
    b. Start wireshark, begin packet capture
    c. Enter 3 traceroute commands:
        i. 56 bytes
        ii. 2000 bytes
        iii. 3500 bytes

```
%traceroute gaia.cs.umass.edu 2000
```

    d. Stop wireshark tracing

2. Look at the captured trace
    a. See the series of ICMP Echo Request/ UDP segment sent by computer + ICMP TTL-exceeded messages returned to computer by the routers

QUESTIONS

1. What is the IP address of your computer?

172.19.127.72

2. Within the IP packet header, what is the value in the upper layer protocol field?

Protocol: 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.

.... 0101 = Header Length: 20 bytes (5)

Total Length: 56

Total length – header length = Payload
56 – 20 = 36

4. **Has this IP datagram been fragmented? Explain how you determined whether the datagram has been fragmented.**

Fragmentation: breaking up data packets to smaller pieces
...0 0000 0000 0000 = Fragment Offset: 0
- nothing was fragmented

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?

Header checksum and identification
- Sequentially

6.

Which of the fields must stay constant? : Procotol type needs to stay the same (ICMP), IP source and address- so that packets can be received and sent accurately

Which fields must change? : Identification and header checksum: to know the number of packets being received/sent

7. Describe the pattern you see in the values in the Identification field of the IP datagram

Header checksum and identification
- Sequentially

8. What is the value in the Identification field and the time to live (TTL) field?

Identification: 0xb45f (46175)
Time to Live: 64

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?

They don’t remain the same, both identification and time to live changes to learn the identities of the identities of the routers

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?

2000 – limit exceeded (1500): 2 fragments: showcasing there's another fragment

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?

010. .... = Flags: 0x2, Don't fragment

By filtering through source: you can see the first fragment

IP datagram length: 1500, the first split fragment

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?

IP datagram length: 500, since it's the remaining bytes from the fragmented packet

13. What fields change in the IP header between the first and second fragment?

Frame number, identification, [Time since reference or first frame: 2.706371000 seconds], packet length

14. How many fragments were created from the original datagram?

With the 2000, there are two fragmented packets created from the original datagram

15. What fields change in the IP header among the fragments?

- fragment offset, and checksum.
- Total packet length
  - First fragmented packet: 1500
  - Second fragmented packet: 500
- Flags