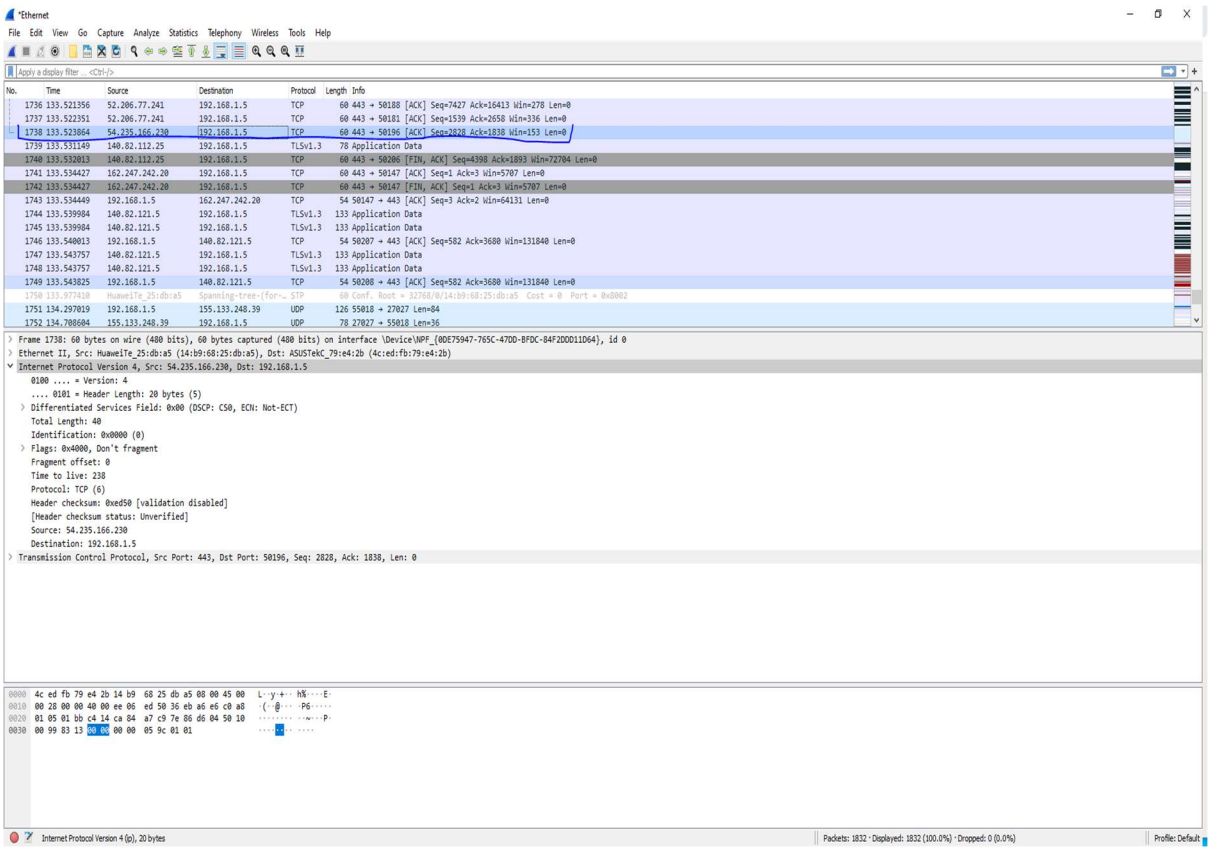
Lab 2

1. Install Wireshark
Wire Shark Installed

2. Capture packet with Wireshark



3. Draw an IP header.

```
Internet Protocol Version 4, Src: 54.235.166.230, Dst: 192.168.1.5
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 40
    Identification: 0x0000 (0)
  > Flags: 0x4000, Don't fragment
    Fragment offset: 0
    Time to live: 238
    Protocol: TCP (6)
    Header checksum: 0xed50 [validation disabled]
    [Header checksum status: Unverified]
    Source: 54.235.166.230
    Destination: 192.168.1.5
> Transmission Control Protocol, Src Port: 443, Dst Port: 50196, Seq: 2828, Ack: 1838, Len: 0
```

4. Explain the fields for a particular IP packet captured. Try to explain the purpose of each field.

- Source IP Address – The address of the host that sent the packet to the destination. The source address is 54.235.166.230

- Destination IP Address – This is the address of the one who received the packet. The destination address is 192.168.1.5
- Version – IP protocol Version. The version is 4
- Header Length -Describes the length of the header and in this case, it is 20 bytes. The size has a minimum of 20 and maximum of 60 bytes.
- Total Length- Describes the total length of the packet and it includes the header in it. Here its 40.
- Identification – describes the fragment.
- Flags- Controls fragments. In this case it doesn't fragment.
- Fragment Offset – Is if a packet is too big to take apart and put together. In this case its 0.
- Time to Live – Sets how long it takes to send and discards if longer than the time to live. Found for a datagram over a number of hops. In this case the time to live is 238.
- Protocol – States the type of protocol that the packet is and in this case its TCP.
- Header Checksum -
- Header Checksum Status – States the status of the header's checksum and here its unverified.

5. Here you find a network trace with fragment bit set in the IP packets. What's the major difference from the packet you described for answering previous questions?

The packets that are here are of the protocol which are of type IPv4 and ICMP in the example and mine is of type TCP for the example that I captured.

https://wiki.wireshark.org/SampleCaptures?action=AttachFile&do=get&target=ipv4frags.pcap

6. List three games you like and list their technical/design highlights.

Halo – This is a first-person shooter that is based in a sci-fi universe and is one of the most popular fps that exists. The main highlights of the game are on the fair gameplay where every player is put into a match with the same gear at first and the players have to fight over the different gear around the map to win. It also limits players to 2 weapons and was one of the first to do it and its now standard in the industry.

Dead Space – Another that is based in a sci-fi universe and this time its third-person shooter that is also a horror game as the player is trapped on a ship and fights to survive and escape the ship. The best feature of the game is the inventory that opens in front of the main character and does not pause the game meaning that you are vulnerable even in the UI for the inventory. Also has narrow corridors that the player moves through that will have jump scares to scare the players and gives a uneasy feeling to players.

Escape from Tarkov (EFT) – EFT is survival game that has players enter a map with others and they have to fight and escape from the map to essentially win. Another FPS this

however is a free for all or Battle Royal that everyone is your enemy except team mates if you enter with them. The best highlight of this game is the fact that you take in gear that you have stashed while playing the game giving it a huge sense of loss if you die. The goal is to kill others and take their gear and escape. However, players can also search for loot like guns and don’t have to fight player or AI giving the game a sense of freedom.