Online Gaming Technologies - Lab 2

3.

Version 0100	IHL 20 bytes	Types Of Service 0x48 (DSCP, ECN)	Total Length 52
Identification 0xda79	IP Flags 0x00	Fragment Offset 0	
Time to live 123	Protocol TCP	Header Checksum 0x134f (validation disabled)	
Source Address 52.114.92.97			
Destination Address 192.168.0.56			
Option 12 bytes, No-Operation, No-Operation, Sack			

4. Version: This is a 4-bit version indicator.

Internet header length: This is used to show how many 32 bit words are present in the header.

Type of Service: This field is provided features related to the quality of service for data streaming or VoIP calls. It is also used for specifying handle Datagram.

Total length: The total length is measured in bytes. The minimum size is 20 bytes and the maximum is 65535 bytes.

Identification: This is a packet that is used to identify fragments of an IP datagram uniquely.

IP Flags: This is a 3-bit field that helps to control the possible fragments. This can be their possible configuration.
   Bit 0: Reserved and has to be set to zero.
   Bit 1: Means do not fragment.
   Bit 2: Means more fragments.

Fragment offset: This represents the number of data bytes ahead of the particular fragment in the specific datagram.

Time to live: This is an 8 bit field that indicates the maximum

time the datagram will be live in the internet system. The time duration is measured in seconds, and when it reaches zero, the datagram will be erased.

Protocol: This IPv4 header is reserved to denote the internet protocol that is used in the latter portion of the datagram.

Header Checksum: This is a 16 bit header checksum field, which is used to check the header for any errors.

Source Address: The source address is a 32-bit address of the source used for the IPv4 packet.

Destination Address: The destination address is a 32-bit address that stores the address of the receiver.

IP options: This is an optional field of the IPv4 header used when the value of the IHL is greater than 5. It contains values and settings related with security, record route and time stamp.

Data: This stores the data from the protocol layer, which has handed over the data to the IP layer.

5. The flags is set to more fragments is the example as well as having a different identification. The time to live is the example is shorter than is the packet that I looked at. It also uses the ICMP protocol instead of TCP. The example doesn't have the same header checksum as mine and it's source address and destination address are only 1 apart compared to the packet I looked at where they were quite different.