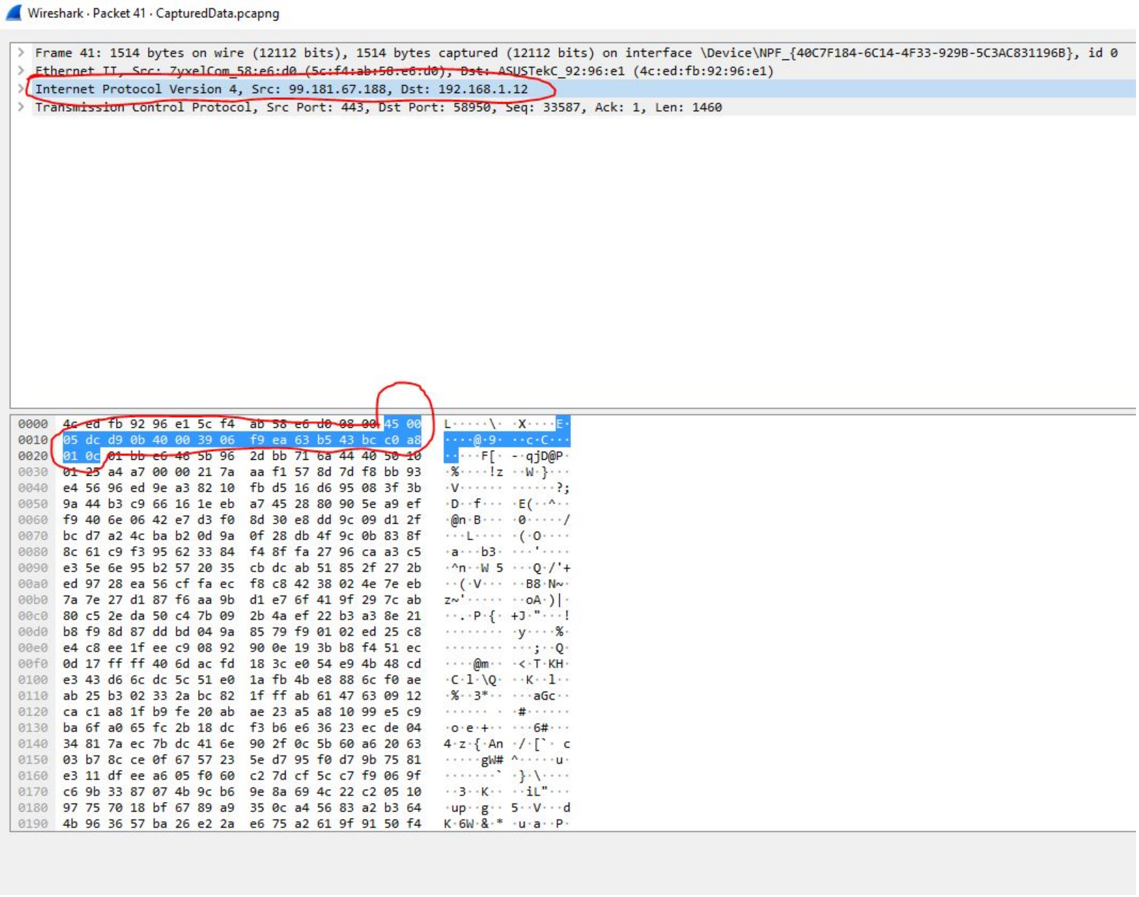
Lab 2

Question 3:

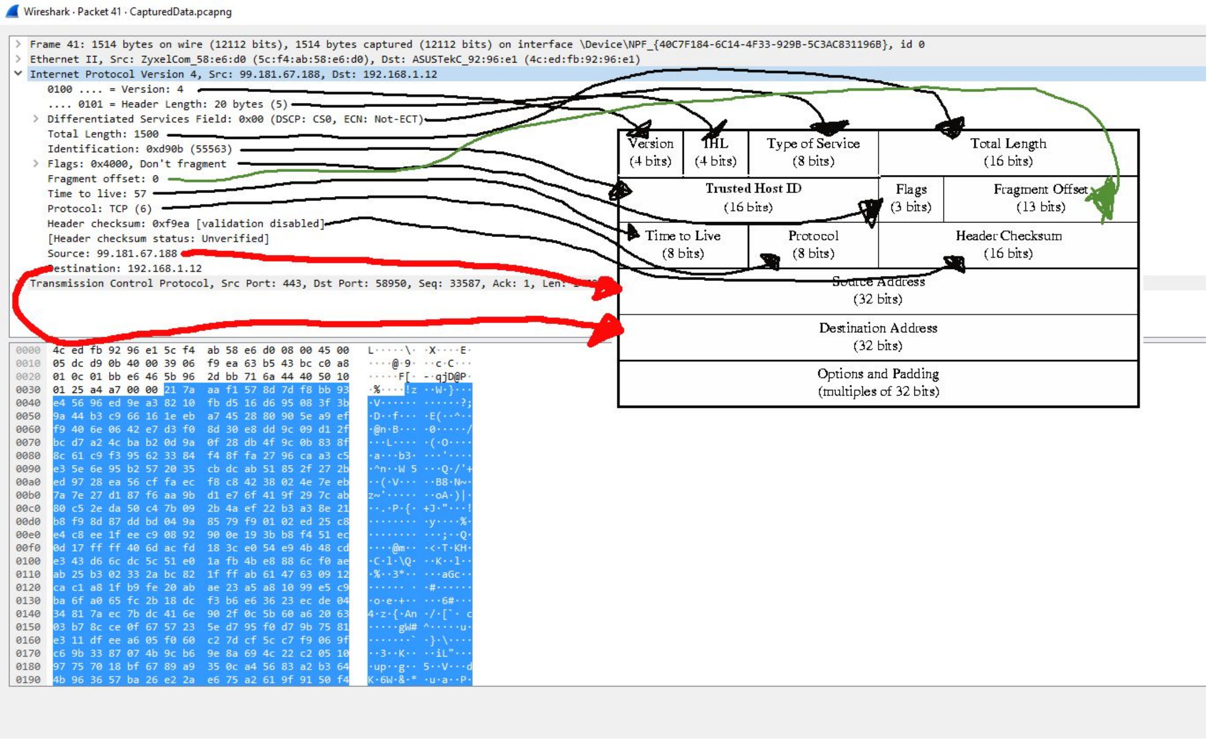


Wireshark · Packet 41 · CapturedData.pcapng

```
> Frame 41: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF_{40C7F184-6C14-4F33-929B-5C3AC831196B}, id 0
> Ethernet II, Src: ZyxelCom_58:e6:d0 (5c:f4:ab:58:e6:d0), Dst: ASUSTekC_92:96:e1 (4c:ed:fb:92:96:e1)
> Internet Protocol Version 4, Src: 99.181.67.188, Dst: 192.168.1.12
> Transmission Control Protocol, Src Port: 443, Dst Port: 58950, Seq: 33587, Ack: 1, Len: 1460
```

```
0000  4c ed fb 92 96 e1 5c f4  ab 58 e6 d0 08 00 45 00   L·····\· ·X····E·
0010  05 dc d9 0b 40 00 39 06  f9 ea 63 b5 43 bc c0 a8   ····@·9· ··c·C···
0020  01 0c 01 bb e6 46 5b 96  2d bb 71 6a 44 40 50 10   ·····F[· -·qjD@P·
0030  01 25 a4 a7 00 00 21 7a  aa f1 57 8d 7d f8 bb 93   ·%····!z ··W·}···
0040  e4 56 96 ed 9e a3 82 10  fb d5 16 d6 95 08 3f 3b   ·V······ ······?;
0050  9a 44 b3 c9 66 16 1e eb  a7 45 28 80 90 5e a9 ef   ·D··f··· ·E(··^··
0060  f9 40 6e 06 42 e7 d3 f0  8d 30 e8 dd 9c 09 d1 2f   ·@n·B··· ·0·····/
0070  bc d7 a2 4c ba b2 0d 9a  0f 28 db 4f 9c 0b 83 8f   ···L···· ·(·O····
0080  8c 61 c9 f3 95 62 33 84  f4 8f fa 27 96 ca a3 c5   ·a···b3· ···'····
0090  e3 5e 6e 95 b2 57 20 35  cb dc ab 51 85 2f 27 2b   ·^n··W 5 ···Q·/'+
00a0  ed 97 28 ea 56 cf fa ec  f8 c8 42 38 02 4e 7e eb   ··(·V··· ··B8·N~·
00b0  7a 7e 27 d1 87 f6 aa 9b  d1 e7 6f 41 9f 29 7c ab   z~'····· ··oA·)|·
00c0  80 c5 2e da 50 c4 7b 09  2b 4a ef 22 b3 a3 8e 21   ··.·P·{· +J·"···!
00d0  b8 f9 8d 87 dd bd 04 9a  85 79 f9 01 02 ed 25 c8   ········ ·y····%·
00e0  e4 c8 ee 1f ee c9 08 92  90 0e 19 3b b8 f4 51 ec   ········ ···;··Q·
00f0  0d 17 ff ff 40 6d ac fd  18 3c e0 54 e9 4b 48 cd   ····@m·· ·<·T·KH·
0100  e3 43 d6 6c dc 5c 51 e0  1a fb 4b e8 88 6c f0 ae   ·C·l·\Q· ··K··l··
0110  ab 25 b3 02 33 2a bc 82  1f ff ab 61 47 63 09 12   ·%··3*·· ···aGc··
0120  ca c1 a8 1f b9 fe 20 ab  ae 23 a5 a8 10 99 e5 c9   ······ · ·#······
0130  ba 6f a0 65 fc 2b 18 dc  f3 b6 e6 36 23 ec de 04   ·o·e·+·· ···6#···
0140  34 81 7a ec 7b dc 41 6e  90 2f 0c 5b 60 a6 20 63   4·z·{·An ·/·[`· c
0150  03 b7 8c ce 0f 67 57 23  5e d7 95 f0 d7 9b 75 81   ·····gW# ^·····u·
0160  e3 11 df ee a6 05 f0 60  c2 7d cf 5c c7 f9 06 9f   ·······` ·}·\····
0170  c6 9b 33 87 07 4b 9c b6  9e 8a 69 4c 22 c2 05 10   ··3··K·· ··iL"···
0180  97 75 70 18 bf 67 89 a9  35 0c a4 56 83 a2 b3 64   ·up··g·· 5··V···d
0190  4b 96 36 57 ba 26 e2 2a  e6 75 a2 61 9f 91 50 f4   K·6W·&·* ·u·a··P·
```

Question 4:



Wireshark · Packet 41 · CapturedData.pcapng

```
> Frame 41: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF_{40C7F184-6C14-4F33-929B-5C3AC831196B}, id 0
> Ethernet II, Src: ZyxelCom_58:e6:d0 (5c:f4:ab:58:e6:d0), Dst: ASUSTekC_92:96:e1 (4c:ed:fb:92:96:e1)
v Internet Protocol Version 4, Src: 99.181.67.188, Dst: 192.168.1.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1500
    Identification: 0xd90b (55563)
  > Flags: 0x4000, Don't fragment
    Fragment offset: 0
    Time to live: 57
    Protocol: TCP (6)
    Header checksum: 0xf9ea [validation disabled]
    [Header checksum status: Unverified]
    Source: 99.181.67.188
    Destination: 192.168.1.12
> Transmission Control Protocol, Src Port: 443, Dst Port: 58950, Seq: 33587, Ack: 1, Len: 1460
```

```
0000  4c ed fb 92 96 e1 5c f4  ab 58 e6 d0 08 00 45 00   L·····\· ·X····E·
0010  05 dc d9 0b 40 00 39 06  f9 ea 63 b5 43 bc c0 a8   ····@·9· ··c·C···
0020  01 0c 01 bb e6 46 5b 96  2d bb 71 6a 44 40 50 10   ·····F[· -·qjD@P·
0030  01 25 a4 a7 00 00 21 7a  aa f1 57 8d 7d f8 bb 93   ·%····!z ··W·}···
0040  e4 56 96 ed 9e a3 82 10  fb d5 16 d6 95 08 3f 3b   ·V······ ······?;
0050  9a 44 b3 c9 66 16 1e eb  a7 45 28 80 90 5e a9 ef   ·D··f··· ·E(··^··
0060  f9 40 6e 06 42 e7 d3 f0  8d 30 e8 dd 9c 09 d1 2f   ·@n·B··· ·0·····/
0070  bc d7 a2 4c ba b2 0d 9a  0f 28 db 4f 9c 0b 83 8f   ···L···· ·(·O····
0080  8c 61 c9 f3 95 62 33 84  f4 8f fa 27 96 ca a3 c5   ·a···b3· ···'····
0090  e3 5e 6e 95 b2 57 20 35  cb dc ab 51 85 2f 27 2b   ·^n··W 5 ···Q·/'+
00a0  ed 97 28 ea 56 cf fa ec  f8 c8 42 38 02 4e 7e eb   ··(·V··· ··B8·N~·
00b0  7a 7e 27 d1 87 f6 aa 9b  d1 e7 6f 41 9f 29 7c ab   z~'····· ··oA·)|·
00c0  80 c5 2e da 50 c4 7b 09  2b 4a ef 22 b3 a3 8e 21   ··.·P·{· +J·"···!
00d0  b8 f9 8d 87 dd bd 04 9a  85 79 f9 01 02 ed 25 c8   ········ ·y····%·
00e0  e4 c8 ee 1f ee c9 08 92  90 0e 19 3b b8 f4 51 ec   ········ ···;··Q·
00f0  0d 17 ff ff 40 6d ac fd  18 3c e0 54 e9 4b 48 cd   ····@m·· ·<·T·KH·
0100  e3 43 d6 6c dc 5c 51 e0  1a fb 4b e8 88 6c f0 ae   ·C·l·\Q· ··K··l··
0110  ab 25 b3 02 33 2a bc 82  1f ff ab 61 47 63 09 12   ·%··3*·· ···aGc··
0120  ca c1 a8 1f b9 fe 20 ab  ae 23 a5 a8 10 99 e5 c9   ······ · ·#······
0130  ba 6f a0 65 fc 2b 18 dc  f3 b6 e6 36 23 ec de 04   ·o·e·+·· ···6#···
0140  34 81 7a ec 7b dc 41 6e  90 2f 0c 5b 60 a6 20 63   4·z·{·An ·/·[`· c
0150  03 b7 8c ce 0f 67 57 23  5e d7 95 f0 d7 9b 75 81   ·····gW# ^·····u·
0160  e3 11 df ee a6 05 f0 60  c2 7d cf 5c c7 f9 06 9f   ·······` ·}·\····
0170  c6 9b 33 87 07 4b 9c b6  9e 8a 69 4c 22 c2 05 10   ··3··K·· ··iL"···
0180  97 75 70 18 bf 67 89 a9  35 0c a4 56 83 a2 b3 64   ·up··g·· 5··V···d
0190  4b 96 36 57 ba 26 e2 2a  e6 75 a2 61 9f 91 50 f4   K·6W·&·* ·u·a··P·
```

Lab 2

Version – This is the version for the IP protocol
Header length – The length of the header the minimum length is 20 bytes and the max is 60 bytes.
Type of Service – Specifies how the data should be handled.
Total length – The length of the entire packet that is sent which includes header and data. The smallest length is 20 bytes and the longest is 65,536 bytes.
Identification – Used to differentiate fragmented packets from different datagrams.
Flags – This is used to control/identify fragments.
Fragmented offset – This is used for when the packet is too big for a frame to break it apart and then put it back together.
Time to live – Limits a datagram's lifetime by setting the maximum number of hops. If the packet doesn't get to its destination before the TTL expires, it is discarded.
Protocol – Describes the protocol that is to be used in the data portion of the IP datagram. For example, TCP is represented by the number 6 and UDP by 17.
Header checksum – Used for error-checking of the header. If the packet reaches a router and the checksum calculated by the router does not match, the packet is discarded.
Source IP address – The IP address of the host that sent the packet.
Destination IP address – The IP address of the host that should receive the packet.
Options – This is used for network testing, debugging, security, and more. This field is usually empty.

Question 5: The major difference is that the packet that I have captured was sent through the network using a TCP protocol while the one you have provided has been sent using the ICMP protocol which in this case was used to locally ping through the network.

Question 6: The game I like are:

Risk of Rain 2: This is a 3D roguelike that has an interesting porch to the items you receive by giving the ability to stack the majority of the items unlike other roguelike games where you get the item once and that is it. The game is made in unity and for the amount of AI creatures that are created on each level it is surprisingly well optimized, with the exception when the player is 2 hours in and starts breaking the game.

Hades: Another roguelike which unlike other roguelikes focuses on delivering concrete story and integrating the story to the reasoning for replayility unlike most other roguelikes that give you a definitive ending once you complete the games the first time.

Crusader Kings 3: An excellent management game in which you get to control a county/duchy/kingdom/empire. The primary focus of this game is to expand your dynasty through marrying well educated spouses with good traits and political background and teaches the player how important it is to marry your young daughter to an old king to secure alliance with England. Its strongest design feature is how many various interactions the player can have with other rulers and how it manages to show the harsh brutality of the medieval ages while being on the age of acceptability for today's standards.

Lab 2