

# Student Information

Full Name: Furkan Göksel

Id Number: 2237436

## Screenshots

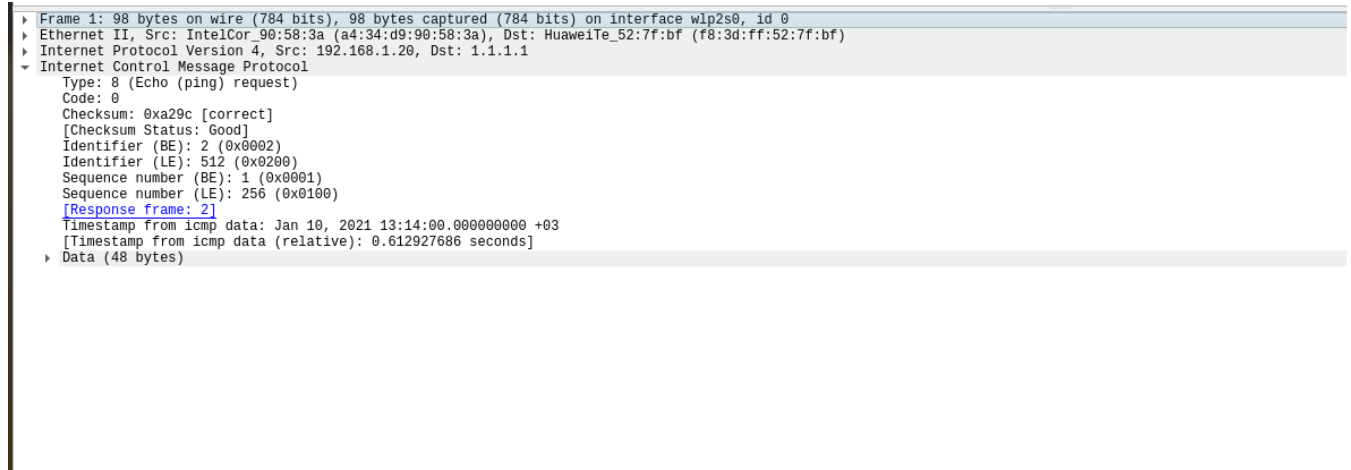


Figure 1: ICMP Request

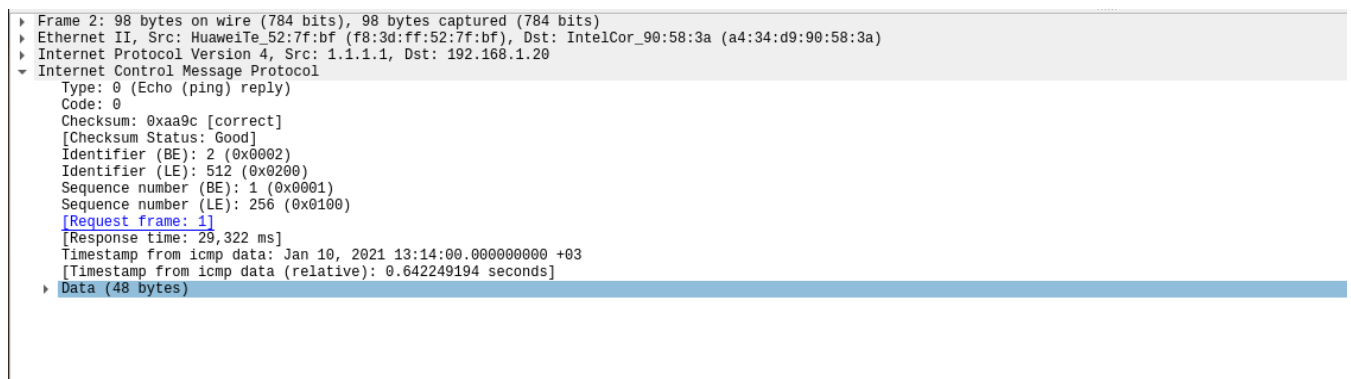


Figure 2: ICMP Reply

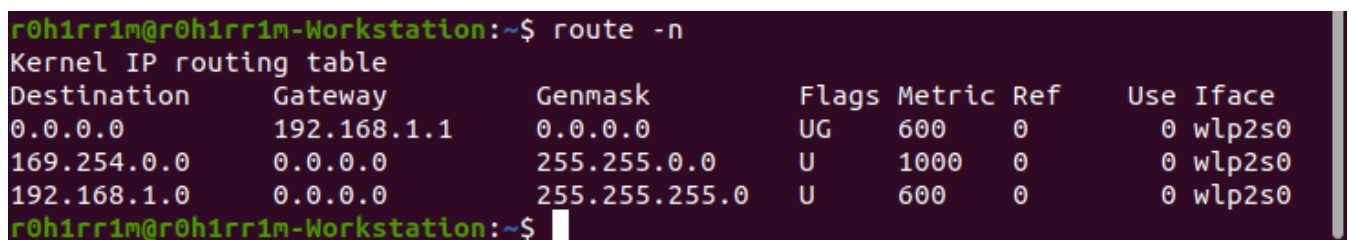


Figure 3: Route Table

# Answers

## 1. (10 Points)

For the request packet, the source host IP address is 192.168.1.20, and the destination host IP address is 1.1.1.1

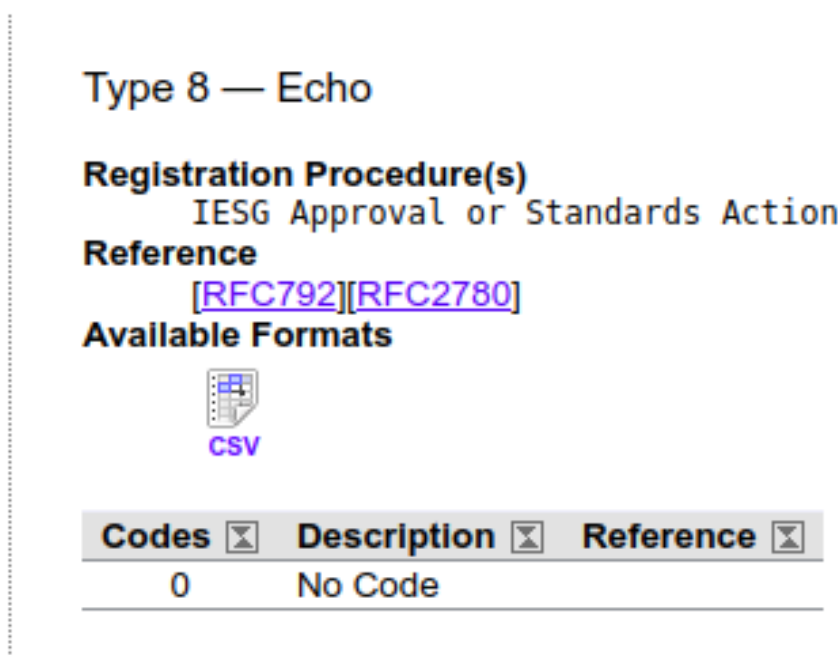
For the reply packet, the source host IP address is 1.1.1.1, and the destination host IP address is 192.168.1.20

## 2. (20 Points)

Port numbers are used in the transport layer for the process to process communication. However ICMP is a network layer protocol, and it doesn't use the transport layer. This is why it doesn't have a port number. ICMP needs just host to host communication, and it is carried inside IP datagram.

## 3a. (15 Points)

The combination of those two fields (type and code) gives the specific message type and information. Using the type field, the message type is identified. Moreover, for some types of messages, the code field is used to give more specific information about the type of message. More specifically, ICMP has two types of codes which are error and query, and the query messages don't require any additional information, thus their code values are 0. However, for the error messages, it further specifies the current condition (like a subtype). For example from the IANA website in the ICMP parameters page we can see that Echo Request and Echo Reply (Figure 4 and Figure 5) uses just code 0, but Destination Unreachable type has some code values that indicate different information (Figure 6).




Type 8 — Echo		
Registration Procedure(s)		
IESG Approval or Standards Action		
Reference		
<a href="#">[RFC792]</a> <a href="#">[RFC2780]</a>		
Available Formats		
 CSV		
Codes	Description	Reference
0	No Code	

Figure 4: Echo Request Type and Code

## Type 0 — Echo Reply

### Registration Procedure(s)

IESG Approval or Standards Action

### Reference

[\[RFC792\]](#)[\[RFC2780\]](#)

### Available Formats



CSV

Codes	Description	Reference
0	No Code	

Figure 5: Echo Reply Type and Code

## Type 3 — Destination Unreachable

### Registration Procedure(s)

IESG Approval or Standards Action

### Reference

[\[RFC792\]](#)[\[RFC2780\]](#)

### Available Formats



CSV

Codes	Description	Reference
0	Net Unreachable	<a href="#">[RFC792]</a>
1	Host Unreachable	<a href="#">[RFC792]</a>
2	Protocol Unreachable	<a href="#">[RFC792]</a>
3	Port Unreachable	<a href="#">[RFC792]</a>
4	Fragmentation Needed and Don't Fragment was Set	<a href="#">[RFC792]</a>
5	Source Route Failed	<a href="#">[RFC792]</a>
6	Destination Network Unknown	<a href="#">[RFC1122]</a>
7	Destination Host Unknown	<a href="#">[RFC1122]</a>
8	Source Host Isolated	<a href="#">[RFC1122]</a>
9	Communication with Destination Network is Administratively Prohibited	<a href="#">[RFC1122]</a>
10	Communication with Destination Host is Administratively Prohibited	<a href="#">[RFC1122]</a>
11	Destination Network Unreachable for Type of Service	<a href="#">[RFC1122]</a>
12	Destination Host Unreachable for Type of Service	<a href="#">[RFC1122]</a>
13	Communication Administratively Prohibited	<a href="#">[RFC1812]</a>
14	Host Precedence Violation	<a href="#">[RFC1812]</a>
15	Precedence cutoff in effect	<a href="#">[RFC1812]</a>

Figure 6: Destination Unreachable Type and Code

### 3b. (15 Points)

In the ICMP Echo Request, the type field value is 8 and the code field value is 0.

In the ICMP Echo Reply, the type field value is 0 and the code field value is 0.

Again from Figure 4 and Figure 5, they indicate the packet type. According to RFC, it says the type field value is 8 for the echo request message and 0 for the echo reply message. For both message types, the code field value is 0. For both packet type, code 0 means no code because they are query messages. As I said above, the combination of those two identifies our types.

### 4. (20 Points)

Total packet length is **98**. From this length, **14** bytes of them belongs to the protocol Ethernet II header. From the last homework, we know that **20** bytes are used for the protocol IPv4 headers. Let's look at the protocol ICMP headers. **1** byte is used for type value, **1** byte is used for code value, **2** byte is used for checksum, **2** byte is used for identifier, **2** byte is used for sequence number (according to RFC 792, sequence number and identifier can be used to aid matching echos and replies), **8** byte timestamp value (Although Wireshark parses this field separately from data, it is not an original header (by the way, the original header size is 8 bytes) according to RFC. According to Wikipedia and some forum posts, Linux ping adds this information. A direct quote from Wikipedia is "The payload may include a timestamp indicating the time of transmission and a sequence number, which are not found in this example. This allows ping to compute the round trip time in a stateless manner without needing to record the time of transmission of each packet."), and **48** bytes for the data. Overall:

14 (Ethernet II) + 20 (IPv4) + 1 (Type) + 1 (Code) + 2 (Checksum) + 2 (Identifier) + 2 (Sequence number) + 8 (Timestamp) + 48 (Data) = 98

Some extra information that I found for these fields:

- Type and Code are used for determining message type and information as explained above
- Checksum is used for error detection purposes. It provides integrity for whole ICMP Message.
- Further information about Identifier and Sequence Number is that we may use identifier as a session number, and sequence numbers as a packet number in this session such that it is incremented by one after each sending the same type of message.
- BE and LE abbreviations are used to indicate Big Endian and Little Endian forms of these values by Wireshark. Because this representation may differ from operating system to operating system.

### 5. (20 Points)

Based on my route table, I have three entries. In a normal routing process, the destination of a sending packet will be anded bit wisely with the Genmask of an entry since it is the netmask for the destination network. Then, it is checked whether it is equal or not to the destination field of the entry. This operation is repeated for all entries in the route table, and the best matching is determined (longest prefix matching rule). Also, there are some special values in the routing table (they are also in my route table). 0.0.0.0 for gateway field means "no gateway, none needed". In other words, IP that is matched with this entry is in my local network, and directly available. Furthermore, Destination 0.0.0.0, and Genmask 0.0.0.0 entry is my default route, and it specifies

my default gateway which is my router. Any outgoing packets, whose destination host is in the remote network, use this entry, and it is sent to my router (because my router connects me to the Internet). Therefore, if I remove this rule (first entry in my route table) outgoing packets will be dropped and we cannot send any ping request to **remote hosts**.