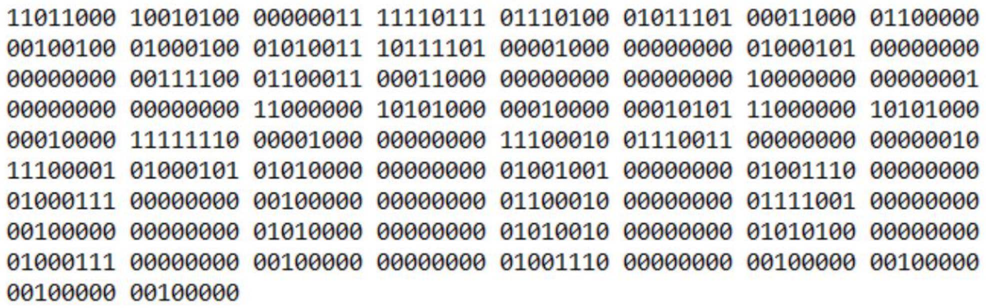
Wireshark Packet Analyze

NOTE: 1 Bytes = 8 Bits



```
11011000 10010100 00000011 11110111 01110100 01011101 00011000 01100000
00100100 01000100 01010011 10111101 00001000 00000000 01000101 00000000
00000000 00111100 01100011 00011000 00000000 00000000 10000000 00000001
00000000 00000000 11000000 10101000 00010000 00010101 11000000 10101000
00010000 11111110 00001000 00000000 11100010 01110011 00000000 00000010
11100001 01000101 01010000 00000000 01001001 00000000 01001110 00000000
01000111 00000000 00100000 00000000 01100010 00000000 01111001 00000000
00100000 00000000 01010000 00000000 01010010 00000000 01010100 00000000
01000111 00000000 00100000 00000000 01001110 00000000 00100000 00100000
00100000 00100000
```

i. What are the source and Destination IP addresses? (2 marks)

DST - D8-94-03-F7-74-5D

SR-CC-30-12-24-53-BD

ii. What are the source and Destination MAC addresses? (2 marks)

SRC - 192.168.16.21
DST - 192.168.16.254

iii. What is the TTL? (1 marks)

128

iv. iv. What is the IP Packet total length? (1 marks)

60

v. What is layer 4 protocol? (2 marks)

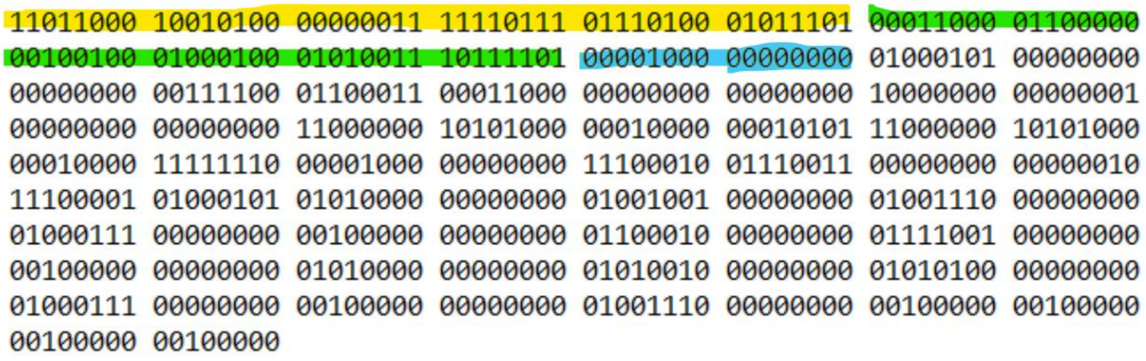
ICMP

vi. Briefly explain about the above communication. (2 marks)

ICMP PACKET BROADCASTING

STARTING WITH ETHERNET FRAME

14 Bytes



```
11011000 10010100 00000011 11110111 01110100 01011101 00011000 01100000
00100100 01000100 01010011 10111101 00001000 00000000 01000101 00000000
00000000 00111100 01100011 00011000 00000000 00000000 10000000 00000001
00000000 00000000 11000000 10101000 00010000 00010101 11000000 10101000
00010000 11111110 00001000 00000000 11100010 01110011 00000000 00000010
11100001 01000101 01010000 00000000 01001001 00000000 01001110 00000000
01000111 00000000 00100000 00000000 01100010 00000000 01111001 00000000
00100000 00000000 01010000 00000000 01010010 00000000 01010100 00000000
01000111 00000000 00100000 00000000 01001110 00000000 00100000 00100000
00100000 00100000
```

First 6 Bytes in YELLOW = Destination Mac Address

- 11011000 10010100 00000011 11110111 01110100 01011101
- D8-94-03-F7-74-5D

Second 6 Bytes in GREEN = Source Mac Address

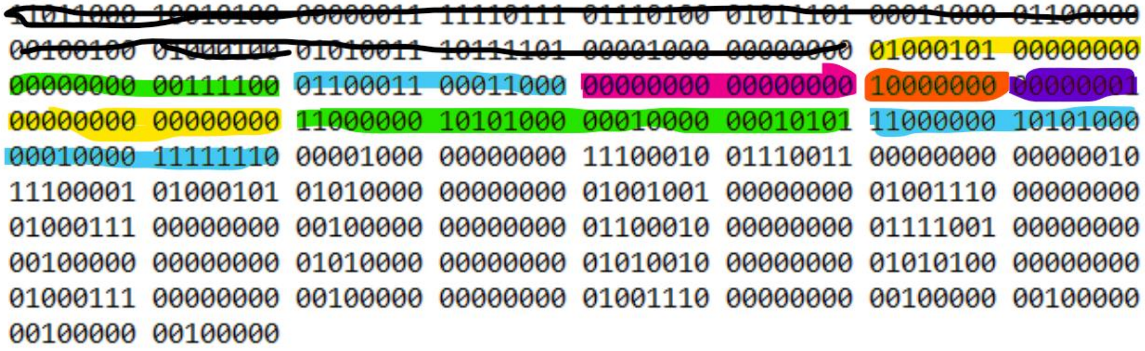
- 00011000 01100000 00100100 01000100 01010011 10111101
- 18-60-24-48-53-BD

Third 2 Bytes in BLUE = Protocol Type

- 8 = EGP

NEXT WITH IP PACKET

20 Bytes



```
~~11011000 10010100 00000011 11110111 01110100 01011101 00011000 01100000~~
~~00100100 01000100 01010011 10111101 00001000 00000000~~ 01000101 00000000
00000000 00111100 01100011 00011000 00000000 00000000 10000000 00000001
00000000 00000000 11000000 10101000 00010000 00010101 11000000 10101000
00010000 11111110 00001000 00000000 11100010 01110011 00000000 00000010
11100001 01000101 01010000 00000000 01001001 00000000 01001110 00000000
01000111 00000000 00100000 00000000 01100010 00000000 01111001 00000000
00100000 00000000 01010000 00000000 01010010 00000000 01010100 00000000
01000111 00000000 00100000 00000000 01001110 00000000 00100000 00100000
00100000 00100000
```

First 2 Bytes in YELLOW = IHL and Type of Service

Second 2 Bytes in GREEN = Total Length

- 00000000.00111100
- 60

Third 2 Bytes in BLUE = Identification

2 Bytes in PINK = Fragments

1 Bytes in ORANGE = TTL

- 10000000
- 128

1 Bytes in PURPLE = PROTOCOL

2 Bytes in YELLOW = Header Checksum

4 Bytes in GREEN = Source Ip Add

- 11000000 10101000 00010000 00010101
- 192.168.16.21

4 Bytes in BLUE = Destination Ip Add

- 11000000 10101000 00010000 11111110
- 192.168.16.254