Διαχείριση Δικτύων Βασισμένων στο Λογισμικό
4ο εργαστήριο: “IP-DHCP”

ΟΝΟΜΑΤΕΠΩΝΥΜΟ:	Νικόλας Μαυρόπουλος
Α.Μ.:	it21865

IP lab

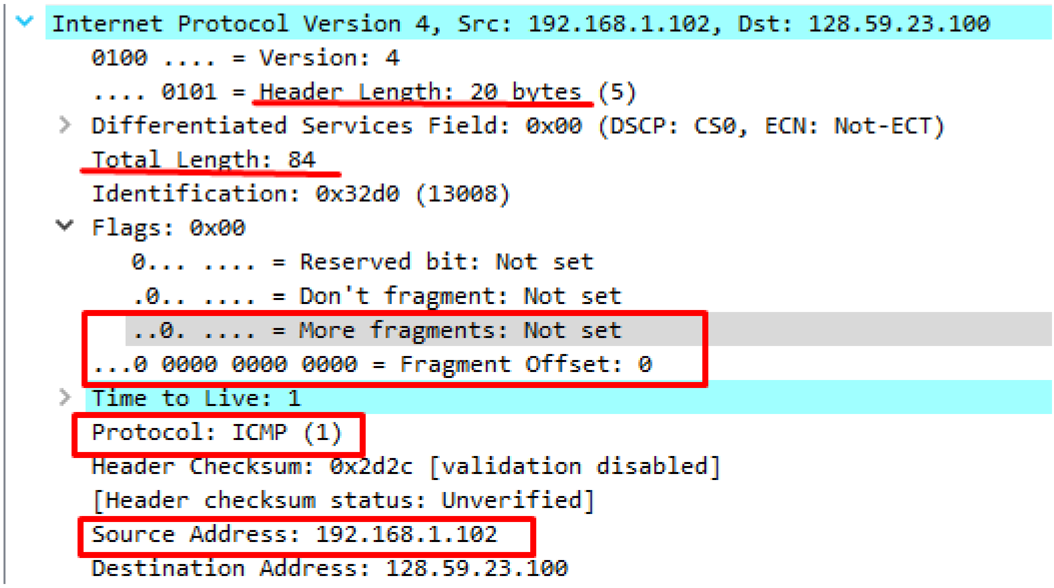
Please provide screenshots to justify your answers to the following questions (the minimum number of screenshots needed – and “to the point” data from these screenshots):

1. What is the IP address of your computer?
   IP address: 192.168.1.102

2. Within the IP packet header, what is the value in the upper layer protocol field?
   Protocol field: ICMP 0x01

3. How many bytes are in the IP header? How many bytes are in the payload *of the IP datagram*? Explain how you determined the number of payload bytes.
   IP header bytes: 20 bytes. Total length is 84 bytes, in order to find the payload I need to do Total length – IP header = 84 – 20 = 64 bytes. Payload of the IP datagram: 64 bytes

4. Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented.
   This IP datagram has **not** been fragmented. Under Flags field More fragments is not set and also Frament Offset is 0

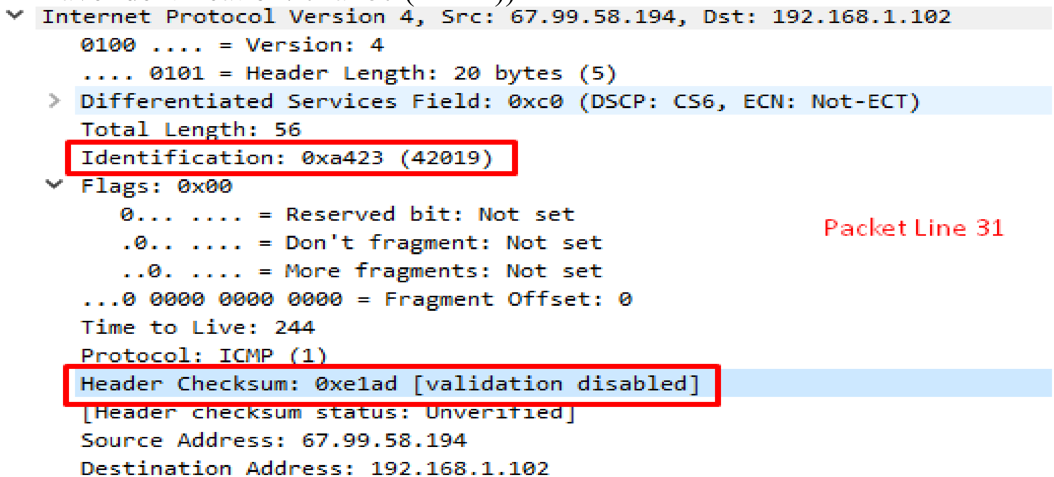


```
Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0x32d0 (13008)
  ∨ Flags: 0x00
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
    ...0 0000 0000 0000 = Fragment Offset: 0
  > Time to Live: 1
    Protocol: ICMP (1)
    Header Checksum: 0x2d2c [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.102
    Destination Address: 128.59.23.100
```

5. Which fields in the IP datagram *always* change from one datagram to the next within this series of ICMP messages sent by your computer?
   The Header Checksum and the Identification always change from one datagram to the next

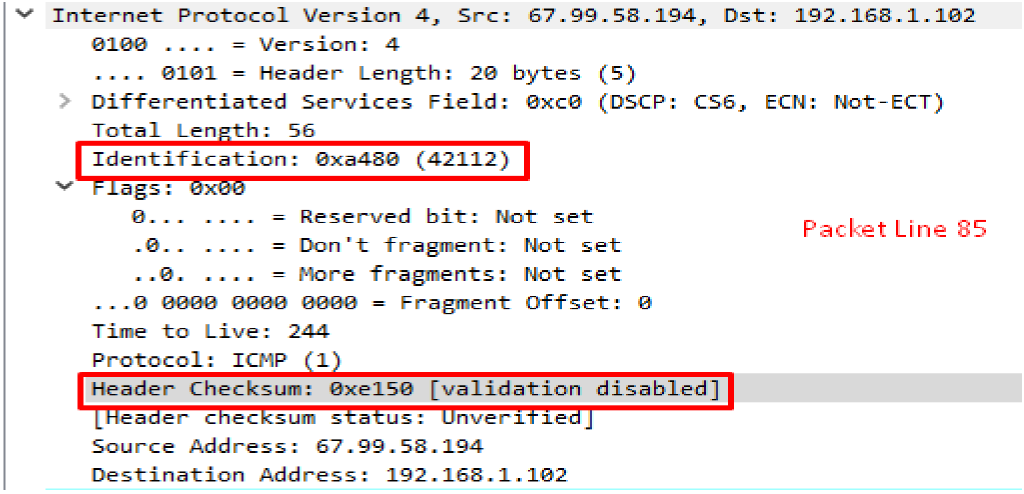
6. Which fields stay constant? Which of the fields *must* stay constant? Which fields must change? Why?
   Fields that stay constant
      Version: because IPv4 is always used
      Header Length: because all packets are ICMP packets
      Total Length
      Source IP: sending all packets from my computer
      Destination IP: contacting same destination
      Flags: same protocol
      Upper Layer Protocol: same protocol
   Fields that must stay constant
      Same as above
   Fields that must change
      Header Checksum: because header changes
      Identification: because packets have different IDs

7. Describe the pattern you see in the values in the Identification field of the IP datagram
   The Identification field increases with each datagram(From packet line 31 we have Identification: 0xa423 (42019) and then to the next packet on line 85 we have Identification: 0xa480 (42112))



```
Internet Protocol Version 4, Src: 67.99.58.194, Dst: 192.168.1.102
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
    Total Length: 56
    Identification: 0xa423 (42019)
  v Flags: 0x00
        0... .... = Reserved bit: Not set
        .0.. .... = Don't fragment: Not set
        ..0. .... = More fragments: Not set
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 244
    Protocol: ICMP (1)
    Header Checksum: 0xe1ad [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 67.99.58.194
    Destination Address: 192.168.1.102
```

Packet Line 31

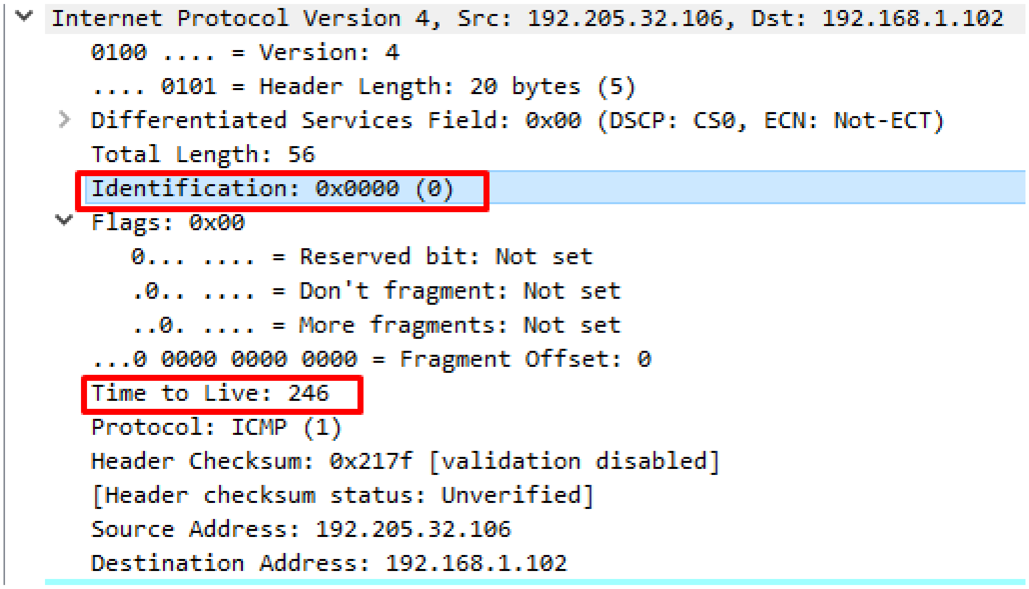


```
Internet Protocol Version 4, Src: 67.99.58.194, Dst: 192.168.1.102
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
    Total Length: 56
    Identification: 0xa480 (42112)
  v Flags: 0x00
        0... .... = Reserved bit: Not set
        .0.. .... = Don't fragment: Not set
        ..0. .... = More fragments: Not set
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 244
    Protocol: ICMP (1)
    Header Checksum: 0xe150 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 67.99.58.194
    Destination Address: 192.168.1.102
```

Packet Line 85

8. What is the value in the Identification field and the TTL field?
   My nearest first hop router is 192.205.32.106
   Identification field: 0x0000   TTL field: 246

9. Do these values remain unchanged for all of the ICMP TTL-exceeded replies sent to your computer by the nearest (first hop) router? Why?
   The TTL field remains unchanged since the TTL for the first hop router is always the same



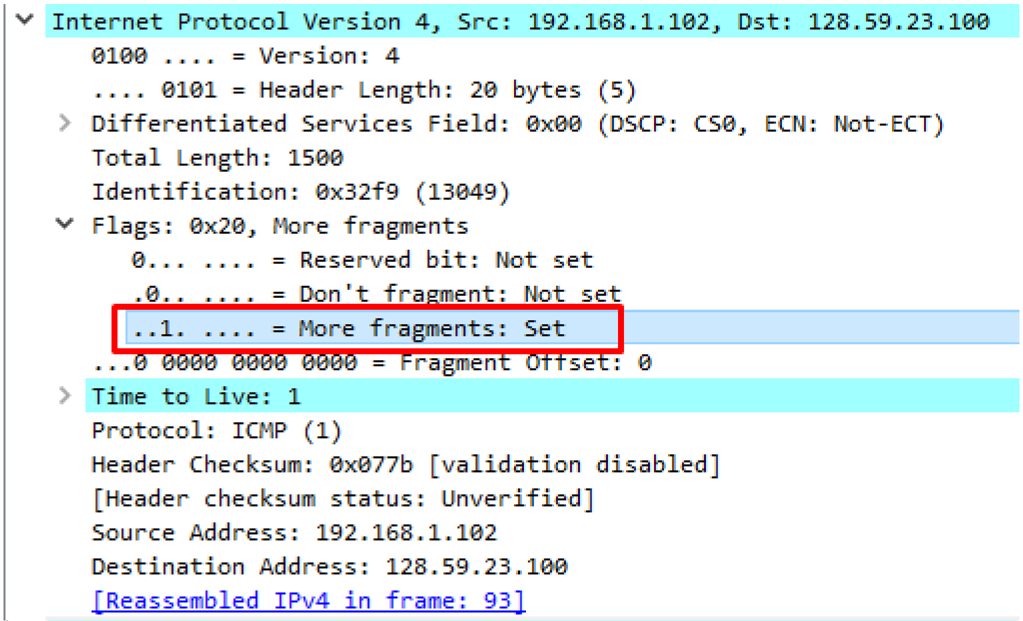
```
v Internet Protocol Version 4, Src: 192.205.32.106, Dst: 192.168.1.102
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 56
    Identification: 0x0000 (0)
  v Flags: 0x00
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 246
    Protocol: ICMP (1)
    Header Checksum: 0x217f [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.205.32.106
    Destination Address: 192.168.1.102
```

10. Find the first ICMP Echo Request message that was sent by your computer after you changed the *Packet Size* in *pingplotter* to be 2000. Has that message been fragmented across more than one IP datagram?
    Yes, this packet has been fragmented across more than one IP datagram

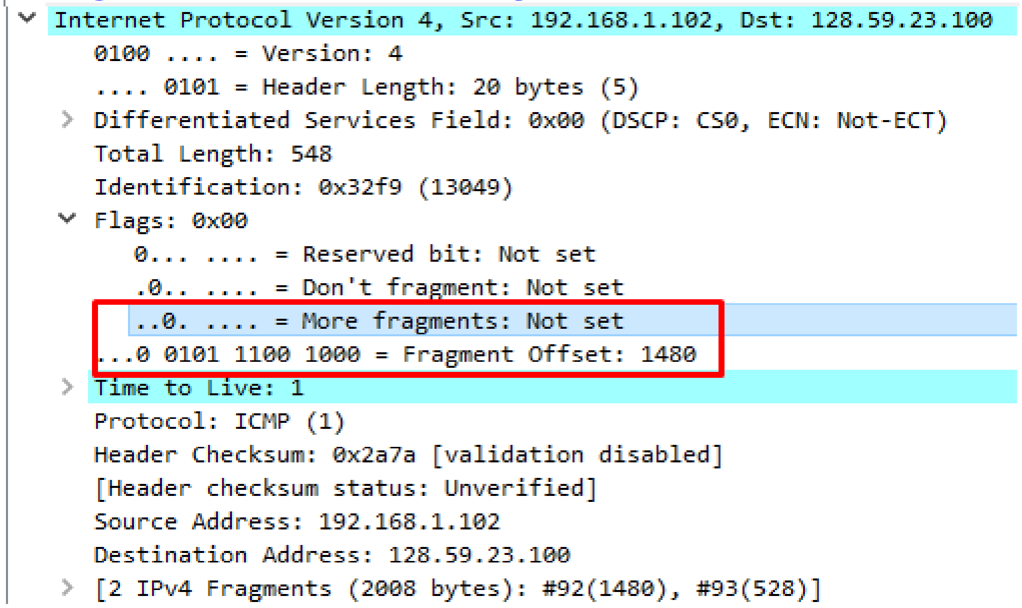
11. Print out the first fragment of the fragmented IP datagram. What information in the IP header indicates that the datagram been fragmented? What information in the IP header indicates whether this is the first fragment versus a latter fragment? How long is this IP datagram?
    In the Flags field More Fragments is set as a result the datagram has been fragmented. Fragment Offset is set to 0, so we know this is the first fragment. The length of the first datagram is 1480, with the header we have 1500.

12. Print out the second fragment of the fragmented IP datagram. What information in the IP header indicates that this is not the first datagram fragment? Are the more fragments? How can you tell?
    Fragment Offset is set to 1480 so this is not the first fragment. Since the More Fragments is not set, this is the last fragment

13. What fields change in the IP header between the first and second fragment?
    Total Length, Flags, Fragment Offset and Header Checksum



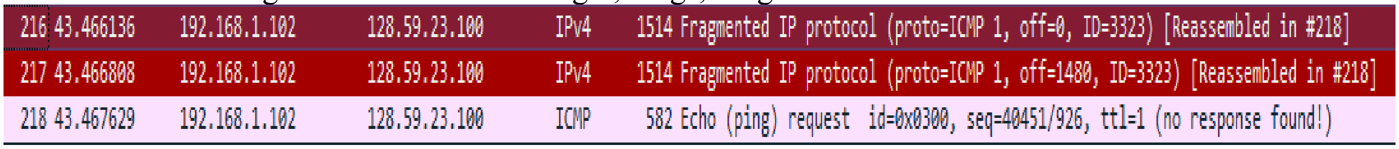
```
∨ Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1500
    Identification: 0x32f9 (13049)
  ∨ Flags: 0x20, More fragments
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..1. .... = More fragments: Set
    ...0 0000 0000 0000 = Fragment Offset: 0
  > Time to Live: 1
    Protocol: ICMP (1)
    Header Checksum: 0x077b [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.102
    Destination Address: 128.59.23.100
    [Reassembled IPv4 in frame: 93]
```



```
∨ Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 548
    Identification: 0x32f9 (13049)
  ∨ Flags: 0x00
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
    ...0 0101 1100 1000 = Fragment Offset: 1480
  > Time to Live: 1
    Protocol: ICMP (1)
    Header Checksum: 0x2a7a [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.102
    Destination Address: 128.59.23.100
  > [2 IPv4 Fragments (2008 bytes): #92(1480), #93(528)]
```

14. How many fragments were created from the original datagram?
    3 packets were created from the original datagram

15. What fields change in the IP header among the fragments?
    Fragment 1 → 2: Fragment Offset and Header Checksum
    Fragment 2 → 3: Total Length, Flags, Fragment Offset and Header Checksum



```
216 43.466136   192.168.1.102   128.59.23.100   IPv4   1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=3323) [Reassembled in #218]
217 43.466808   192.168.1.102   128.59.23.100   IPv4   1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3323) [Reassembled in #218]
218 43.467629   192.168.1.102   128.59.23.100   ICMP    582 Echo (ping) request  id=0x0300, seq=40451/926, ttl=1 (no response found!)
```

DHCP lab

Please respond to the following questions and add respective screenshot(s):

1. Are DHCP messages sent over UDP or TCP?
   They are sent over UDP

2. What is the link-layer (e.g., Ethernet) address of your host?
   Address of my host: Dell_4f:36:23 (00:08:74:4f:36:23)

3. What values in the DHCP discover message differentiate this message from the DHCP request message?
   DHCP Message Type, which is 1 for discover message and 3 for request packet

4. What is the value of the Transaction-ID in each of the first four (Discover/Offer/Request/ACK) DHCP messages? What are the values of the Transaction-ID in the second set (Request/ACK) set of DHCP messages? What is the purpose of the Transaction-ID field?
   First four messages Transaction ID: 0x3e5e0ce3
   Second set messages Transaction ID: 0x257e55a3
   The Transaction ID field determines if a message is part of a group of messages related to a single transaction

5. A host uses DHCP to obtain an IP address, among other things. But a host's IP address is not confirmed until the end of the four-message exchange! If the IP address is not set until the end of the four-message exchange, then what values are used in the IP datagrams in the four-message exchange? For each of the four DHCP messages (Discover/Offer/Request/ACK DHCP), indicate the source and destination IP addresses that are carried in the encapsulating IP datagram.
   If the IP address is not set, then DHCP host and server both use 255.255.255.255 as destination address. The host uses 0.0.0.0 as source address and the server uses its own IP address as source.
   Discover: Source: 0.0.0.0 Destination: 255.255.255.255
   Offer: Source: 192.168.1.1 Destination: 255.255.255.255
   Request: Source: 0.0.0.0 Destination: 255.255.255.255
   ACK DHCP: Source:192.168.1.1 Destination: 255.255.255.255

6. What is the IP address of your DHCP server?
   IP address: 192.168.1.1

7. What IP address is the DHCP server offering to your host in the DHCP Offer message? Indicate which DHCP message contains the offered DHCP address.
   It is offering me the IP address 192.168.1.101 The Offer message contains the offered DHCP address

8. In the example screenshot in this assignment, there is no relay agent between the host and the DHCP server. What values in the trace indicate the absence of a relay agent? Is there a relay agent in your experiment? If so what is the IP address of the agent?
   The value that indicates the absence of a relay agent is 0.0.0.0 In my experiment there is **not** a relay agent.

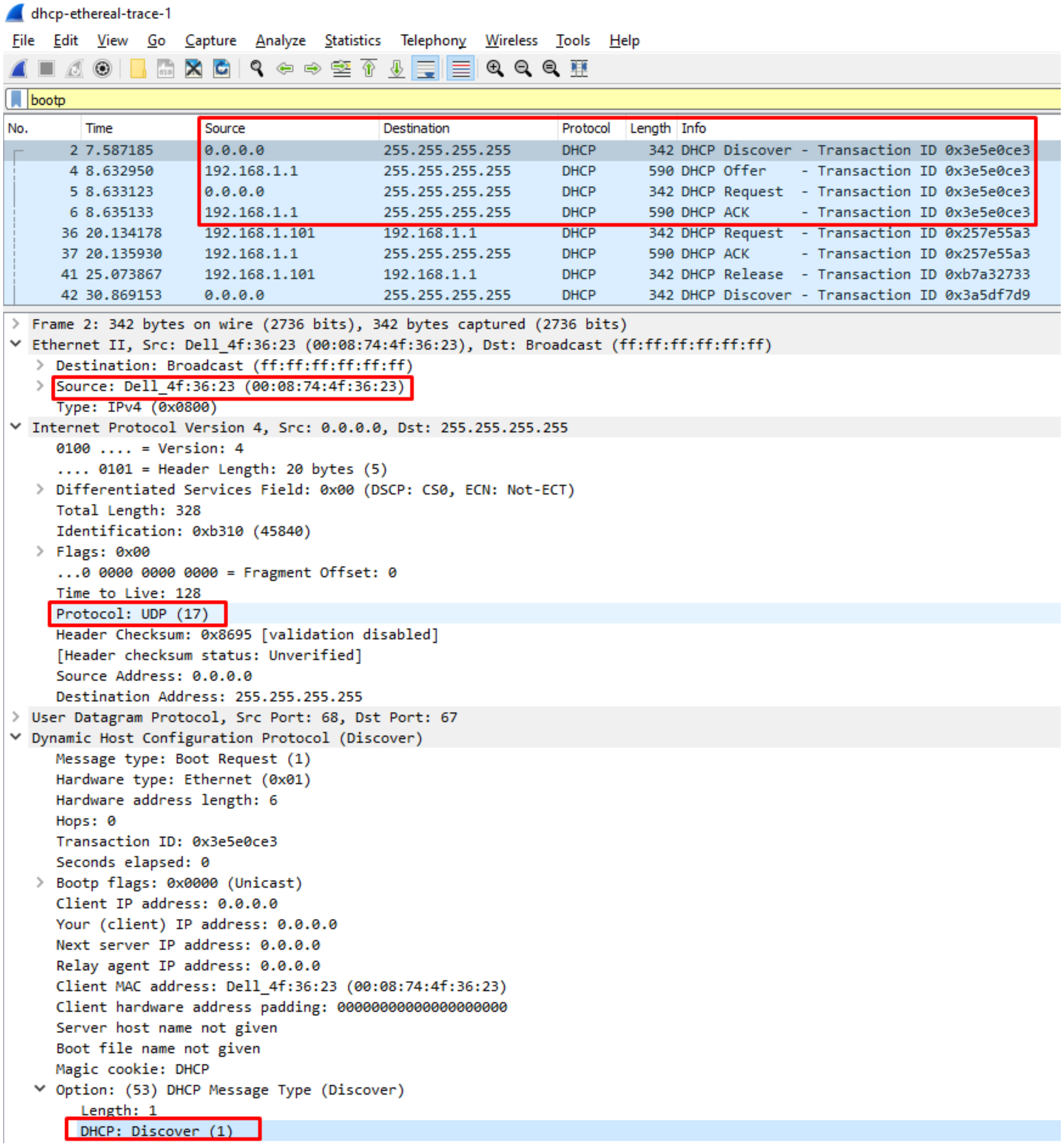
9. Explain the purpose of the router and subnet mask lines in the DHCP offer message.
   The router line specifies where the client should deliver messages by default. The subnet mask line tells the client which subnet mask to use.

10. In the DHCP trace file noted in footnote 2, the DHCP server offers a specific IP address to the client (see also question 7. above). In the client's response to the first server OFFER message, does the client accept this IP address? Where in the client's RESPONSE is the client's requested address?
    The client accepts the IP address. Having been offered the IP address 192.168.1.101, the client sends Requested IP Address message further requesting this IP address

11. Explain the purpose of the lease time. How long is the lease time in your experiment?
    Lease time tells the client for how long they can use this IP address assigned by the DHCP server. In my experiment the lease time is 1 day

12. What is the purpose of the DHCP release message? Does the DHCP server issue an acknowledgment of receipt of the client's DHCP request? What would happen if the client's DHCP release message is lost?
    The DHCP release message is to release the IP address back to the server. The server does **not** issue an acknowledgment of receipt. If the release message is lost, then the server would have to wait for the lease time to expire for that IP address in order to reassign it.

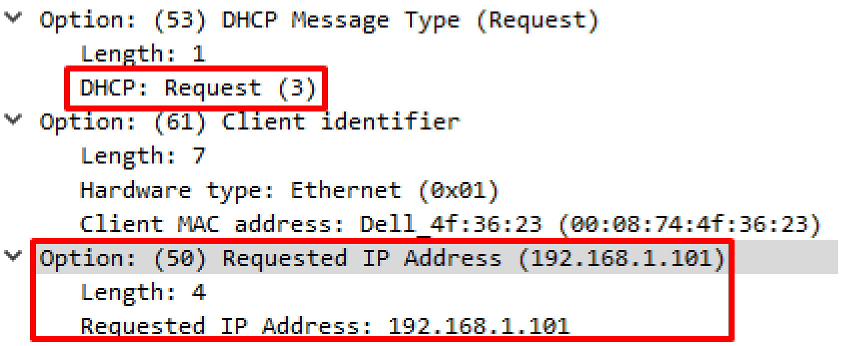
13. Clear the *bootp* filter from your Wireshark window. Were any ARP packets sent or received during the DHCP packet-exchange period? If so, explain the purpose of those ARP packets.
    Yes, ARP packets were sent and received in order to assist the identification of the MAC and IP addresses.


dhcp-ethereal-trace-1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

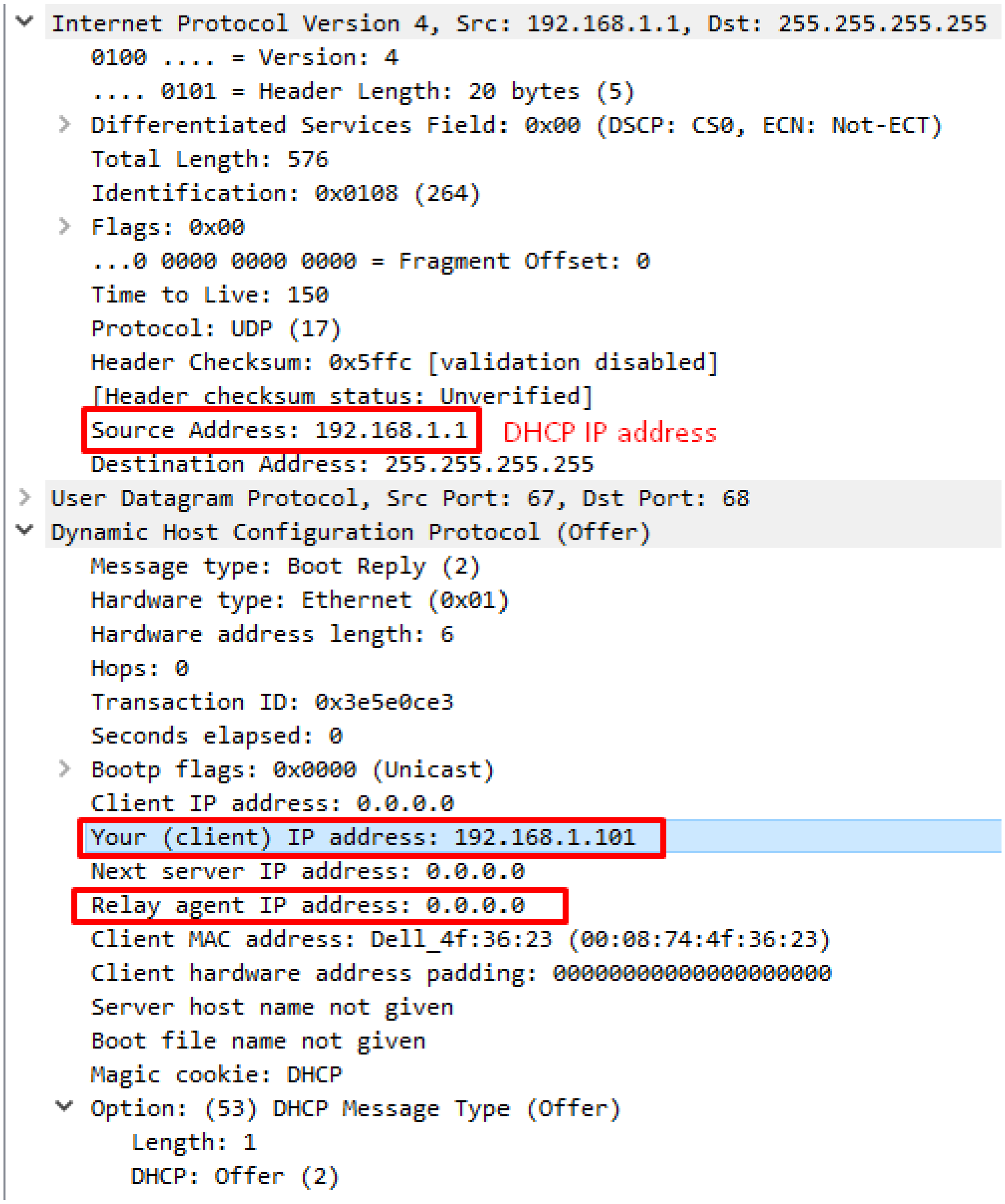
bootp

No.	Time	Source	Destination	Protocol	Length	Info
2	7.587185	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x3e5e0ce3
4	8.632950	192.168.1.1	255.255.255.255	DHCP	590	DHCP Offer - Transaction ID 0x3e5e0ce3
5	8.633123	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x3e5e0ce3
6	8.635133	192.168.1.1	255.255.255.255	DHCP	590	DHCP ACK - Transaction ID 0x3e5e0ce3
36	20.134178	192.168.1.101	192.168.1.1	DHCP	342	DHCP Request - Transaction ID 0x257e55a3
37	20.135930	192.168.1.1	255.255.255.255	DHCP	590	DHCP ACK - Transaction ID 0x257e55a3
41	25.073867	192.168.1.101	192.168.1.1	DHCP	342	DHCP Release - Transaction ID 0xb7a32733
42	30.869153	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x3a5df7d9

```
> Frame 2: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
v Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  > Source: Dell_4f:36:23 (00:08:74:4f:36:23)
    Type: IPv4 (0x0800)
v Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 328
    Identification: 0xb310 (45840)
  > Flags: 0x00
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0x8695 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 0.0.0.0
    Destination Address: 255.255.255.255
> User Datagram Protocol, Src Port: 68, Dst Port: 67
v Dynamic Host Configuration Protocol (Discover)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x3e5e0ce3
    Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 0.0.0.0
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: Dell_4f:36:23 (00:08:74:4f:36:23)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  v Option: (53) DHCP Message Type (Discover)
      Length: 1
      DHCP: Discover (1)
```



```
v Option: (53) DHCP Message Type (Request)
    Length: 1
    DHCP: Request (3)
v Option: (61) Client identifier
    Length: 7
    Hardware type: Ethernet (0x01)
    Client MAC address: Dell_4f:36:23 (00:08:74:4f:36:23)
v Option: (50) Requested IP Address (192.168.1.101)
    Length: 4
    Requested IP Address: 192.168.1.101
```



```
⌄ Internet Protocol Version 4, Src: 192.168.1.1, Dst: 255.255.255.255
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 576
    Identification: 0x0108 (264)
  > Flags: 0x00
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 150
    Protocol: UDP (17)
    Header Checksum: 0x5ffc [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.1
    Destination Address: 255.255.255.255
> User Datagram Protocol, Src Port: 67, Dst Port: 68
⌄ Dynamic Host Configuration Protocol (Offer)
    Message type: Boot Reply (2)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x3e5e0ce3
    Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 192.168.1.101
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: Dell_4f:36:23 (00:08:74:4f:36:23)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  ⌄ Option: (53) DHCP Message Type (Offer)
      Length: 1
      DHCP: Offer (2)
```

DHCP IP address