Sheridan College		
Course	**Data Network Design and Configuration – Routers and Switches**	
Professor	**Ida Leung**	
Student Name/ID	**Kunjan Patel/991535676**	
Table number		
Lab 1: Wireshark Practise		
Performed Date	**19/5/2019**	
Instructor's Sign		(marks)

OBJECTIVES:

- Review the use of wireshark and how to use the captured data

Step 1: Use Wireshark to capture the following protocols in complete set (include sender and receiver both direction full conversation(:

1. DHCP
2. DNS

Step 2: Printscreen and document your capture for each data flow for the protocol

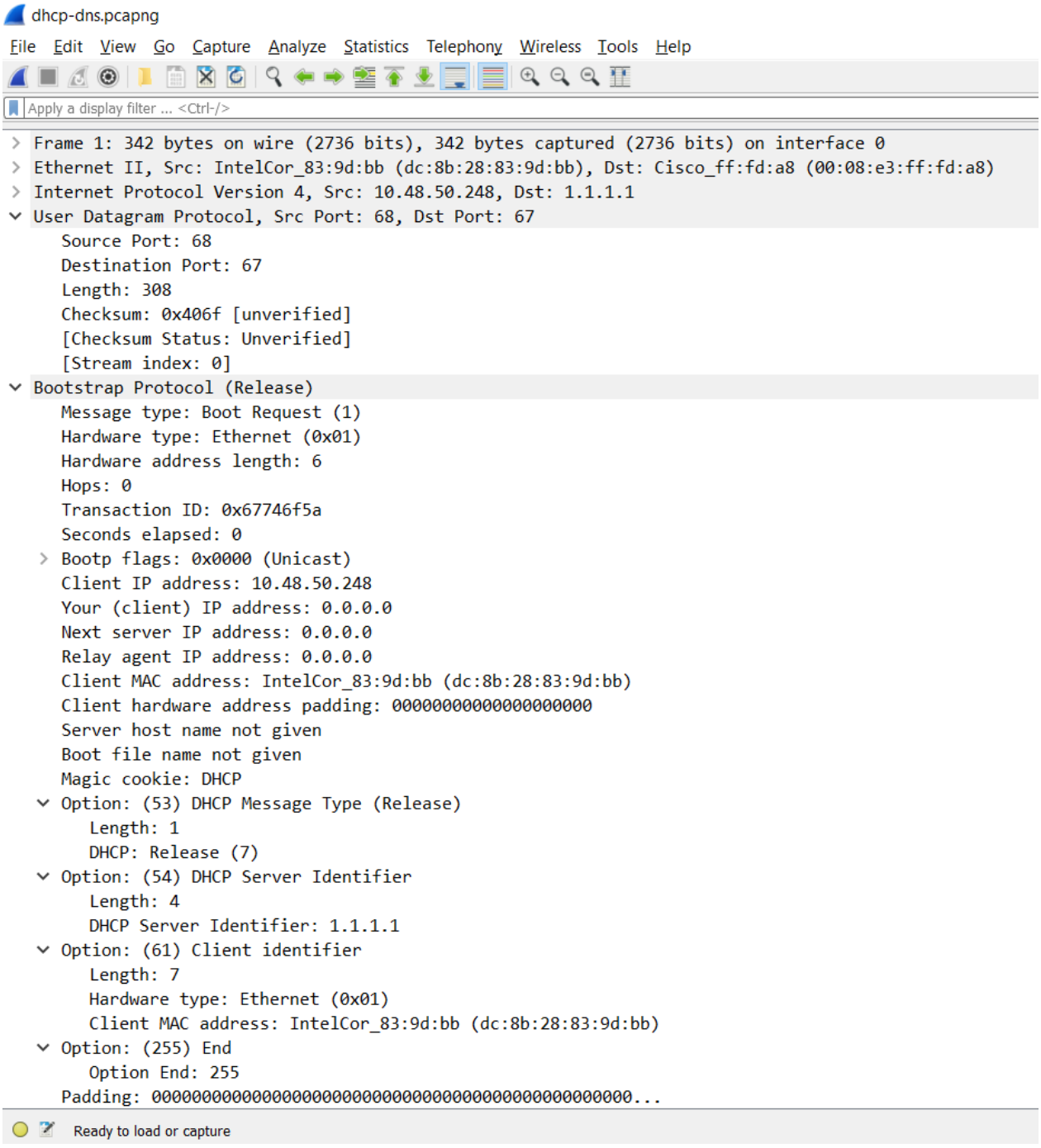

Fig 1.1 DHCP release

Wireshark · Packet 44 · dhcp-dns.pcapng

```
> Frame 44: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
> Ethernet II, Src: IntelCor_83:9d:bb (dc:8b:28:83:9d:bb), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
v User Datagram Protocol, Src Port: 68, Dst Port: 67
    Source Port: 68
    Destination Port: 67
    Length: 308
    Checksum: 0x5807 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 11]
v Bootstrap Protocol (Discover)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xad0d7c67
    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: IntelCor_83:9d:bb (dc:8b:28:83:9d:bb)
    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: (61) Client identifier
      Length: 7
      Hardware type: Ethernet (0x01)
      Client MAC address: IntelCor_83:9d:bb (dc:8b:28:83:9d:bb)
  v Option: (50) Requested IP Address
      Length: 4
      Requested IP Address: 10.48.50.248
  v Option: (12) Host Name
      Length: 3
      Host Name: MSI
  v Option: (60) Vendor class identifier
```

Fig 1.2 DHCP discover

Wireshark · Packet 44 · dhcp-dns.pcapng

```
    Relay agent IP address: 0.0.0.0
    Client MAC address: IntelCor_83:9d:bb (dc:8b:28:83:9d:bb)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  ⌄ Option: (53) DHCP Message Type (Discover)
       Length: 1
       DHCP: Discover (1)
  ⌄ Option: (61) Client identifier
       Length: 7
       Hardware type: Ethernet (0x01)
       Client MAC address: IntelCor_83:9d:bb (dc:8b:28:83:9d:bb)
  ⌄ Option: (50) Requested IP Address
       Length: 4
       Requested IP Address: 10.48.50.248
  ⌄ Option: (12) Host Name
       Length: 3
       Host Name: MSI
  ⌄ Option: (60) Vendor class identifier
       Length: 8
       Vendor class identifier: MSFT 5.0
  ⌄ Option: (55) Parameter Request List
       Length: 14
       Parameter Request List Item: (1) Subnet Mask
       Parameter Request List Item: (3) Router
       Parameter Request List Item: (6) Domain Name Server
       Parameter Request List Item: (15) Domain Name
       Parameter Request List Item: (31) Perform Router Discover
       Parameter Request List Item: (33) Static Route
       Parameter Request List Item: (43) Vendor-Specific Information
       Parameter Request List Item: (44) NetBIOS over TCP/IP Name Server
       Parameter Request List Item: (46) NetBIOS over TCP/IP Node Type
       Parameter Request List Item: (47) NetBIOS over TCP/IP Scope
       Parameter Request List Item: (119) Domain Search
       Parameter Request List Item: (121) Classless Static Route
       Parameter Request List Item: (249) Private/Classless Static Route (Microsoft)
       Parameter Request List Item: (252) Private/Proxy autodiscovery
  ⌄ Option: (255) End
       Option End: 255
    Padding: 00000000000000000000
```

Fig 1.3 DHCP discover options

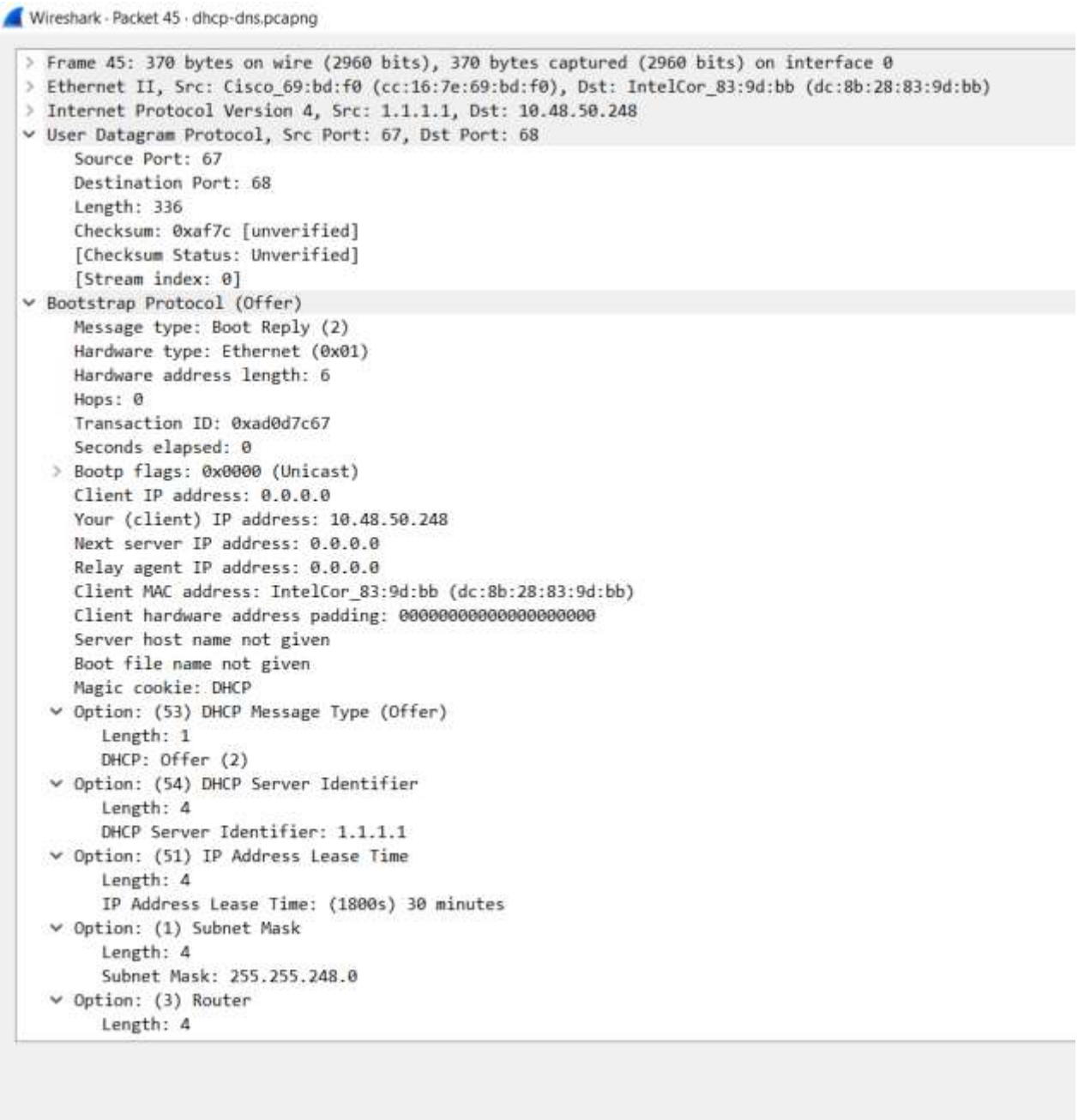

Fig 1.4 DHCP offer

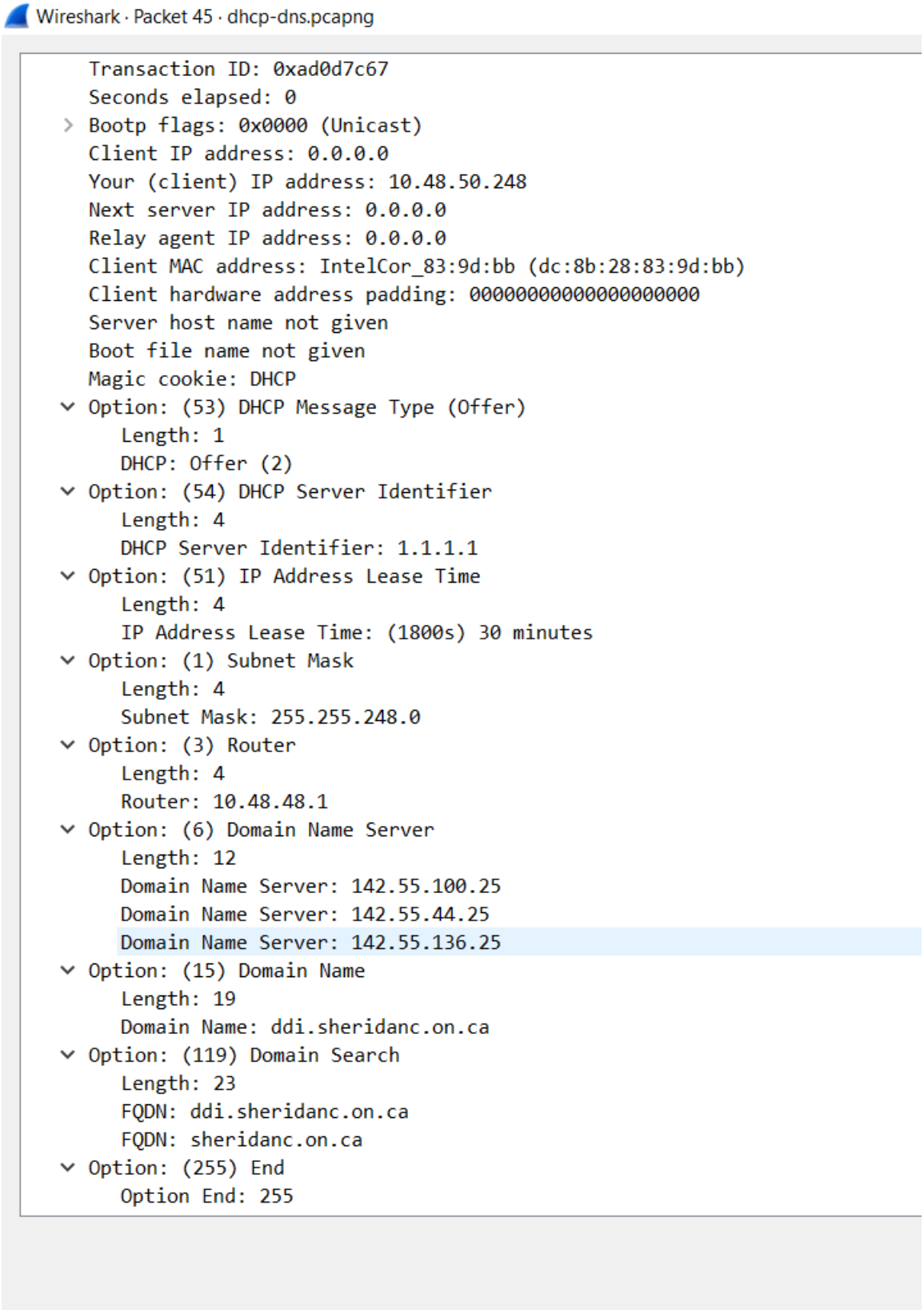

Fig 1.5 DHCP offer options

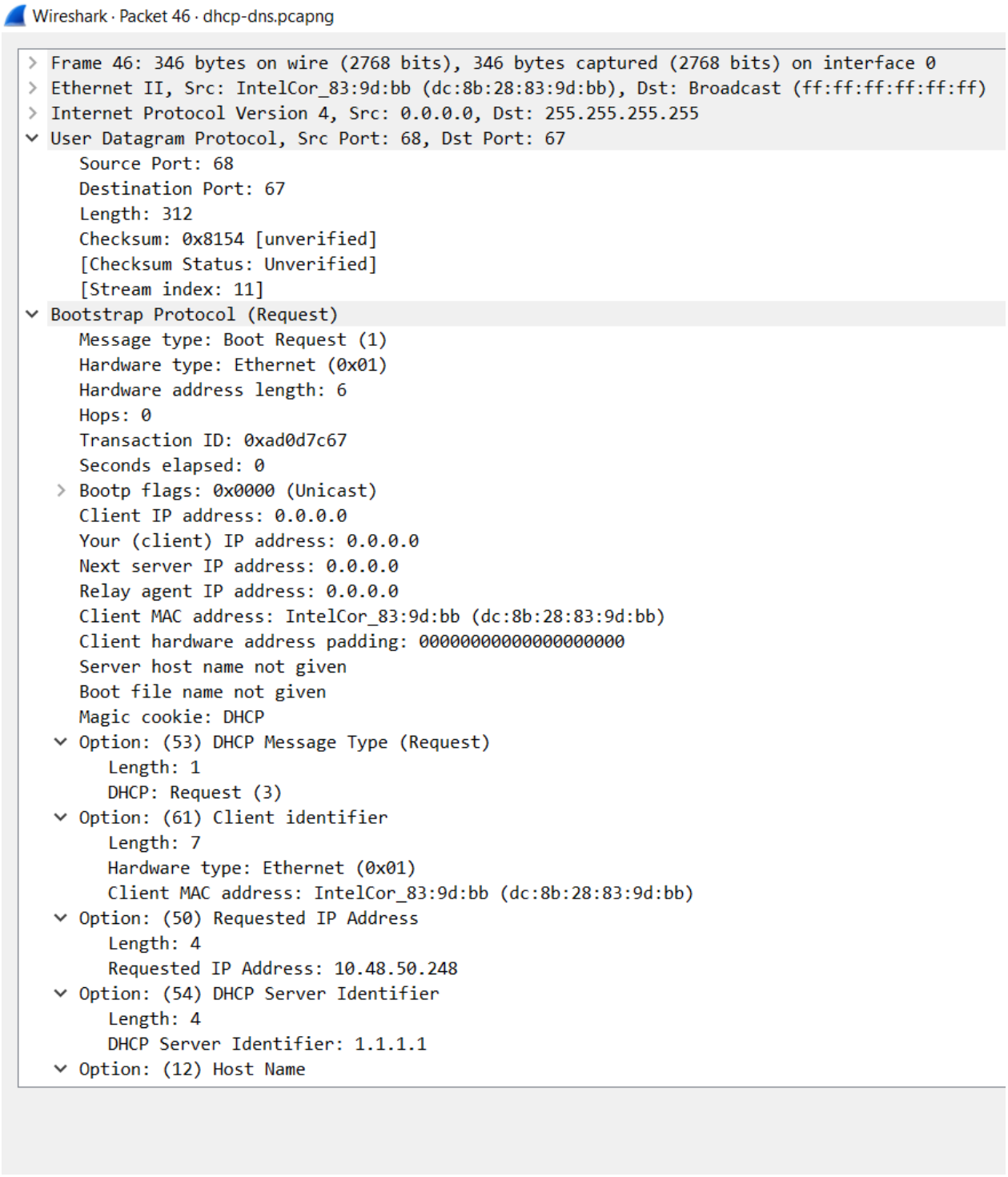

Fig 1.6 DHCP request

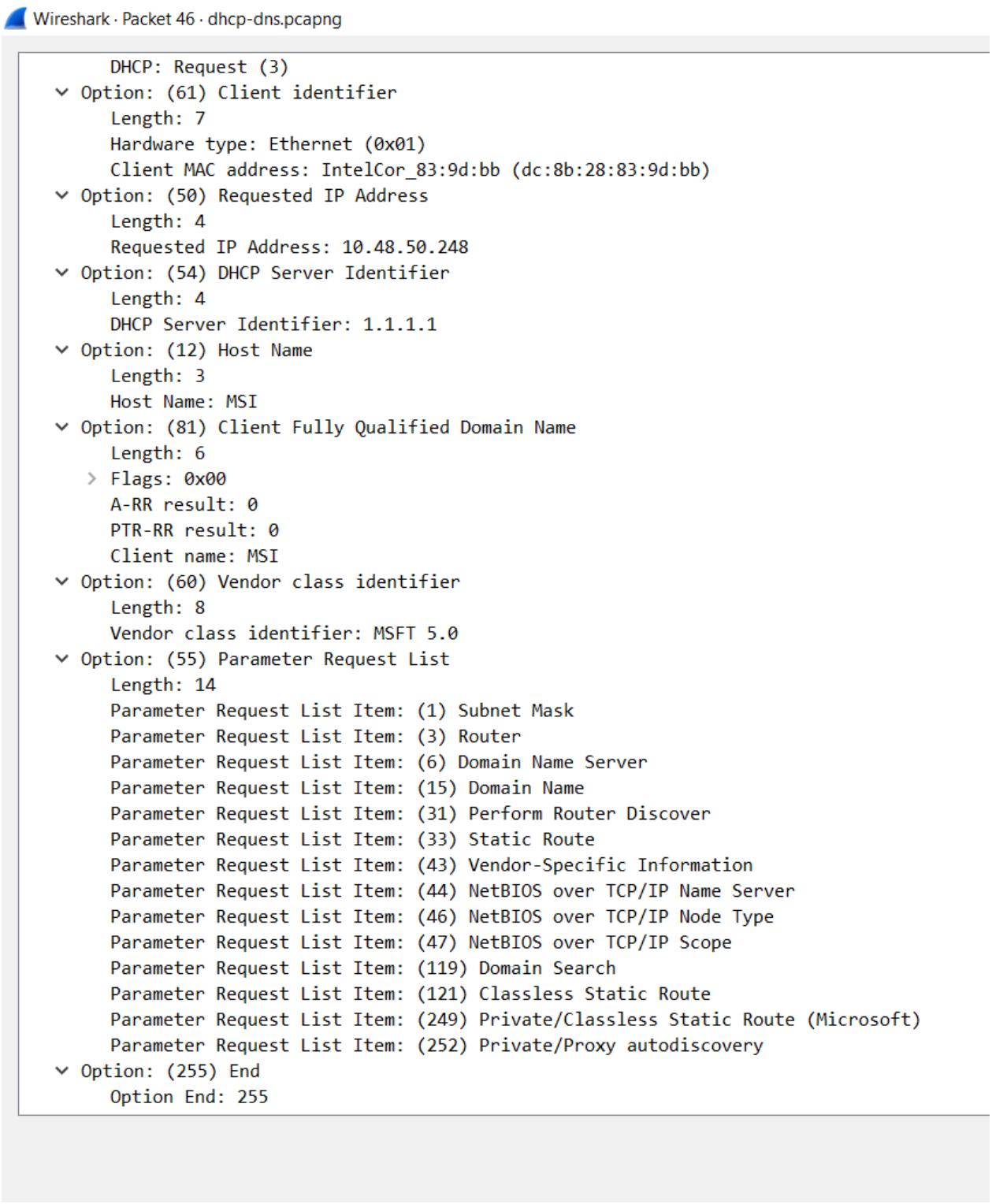

Fig 1.7 DHCP offer options

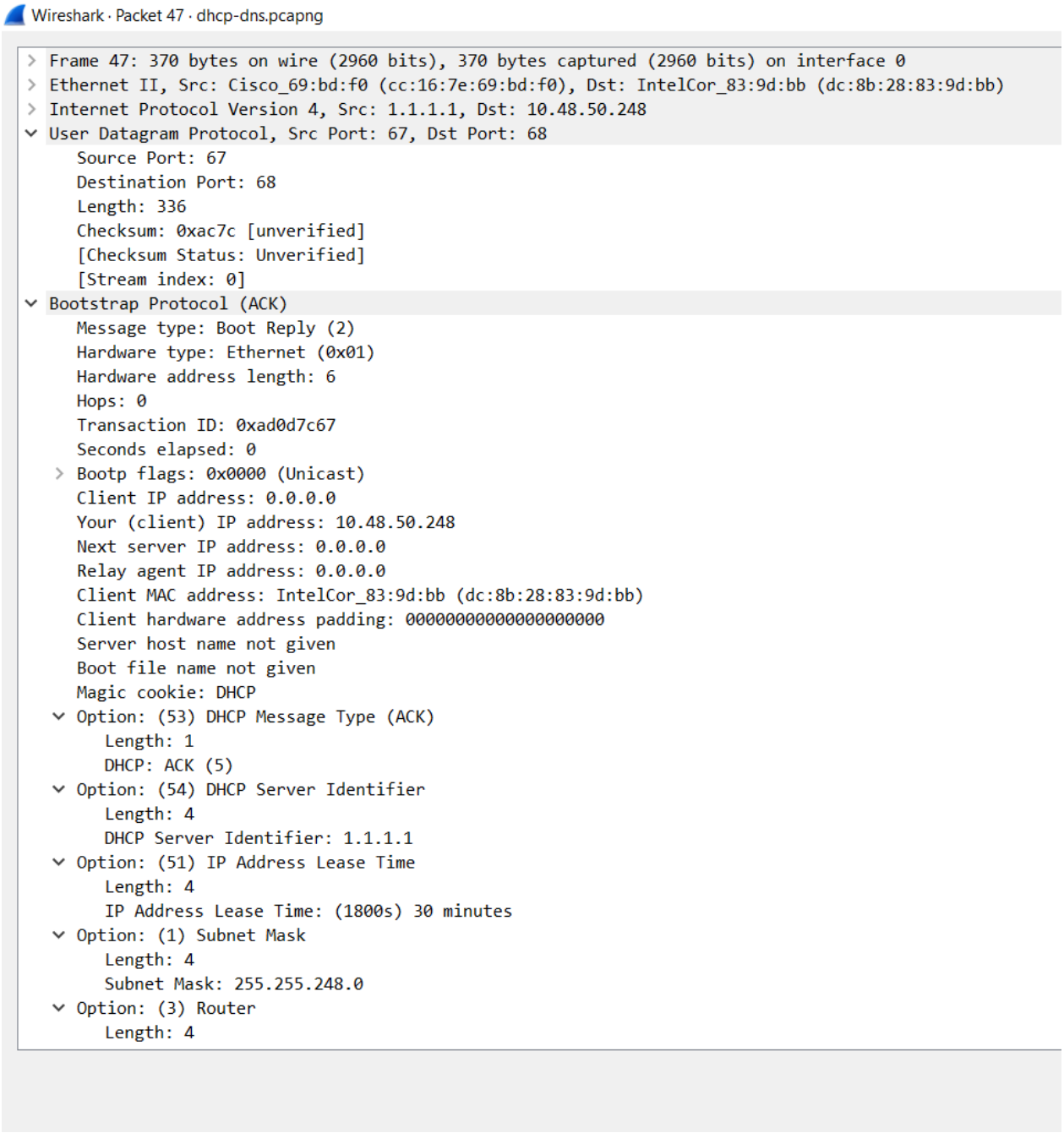

Fig 1.8 DHCP acknowledge

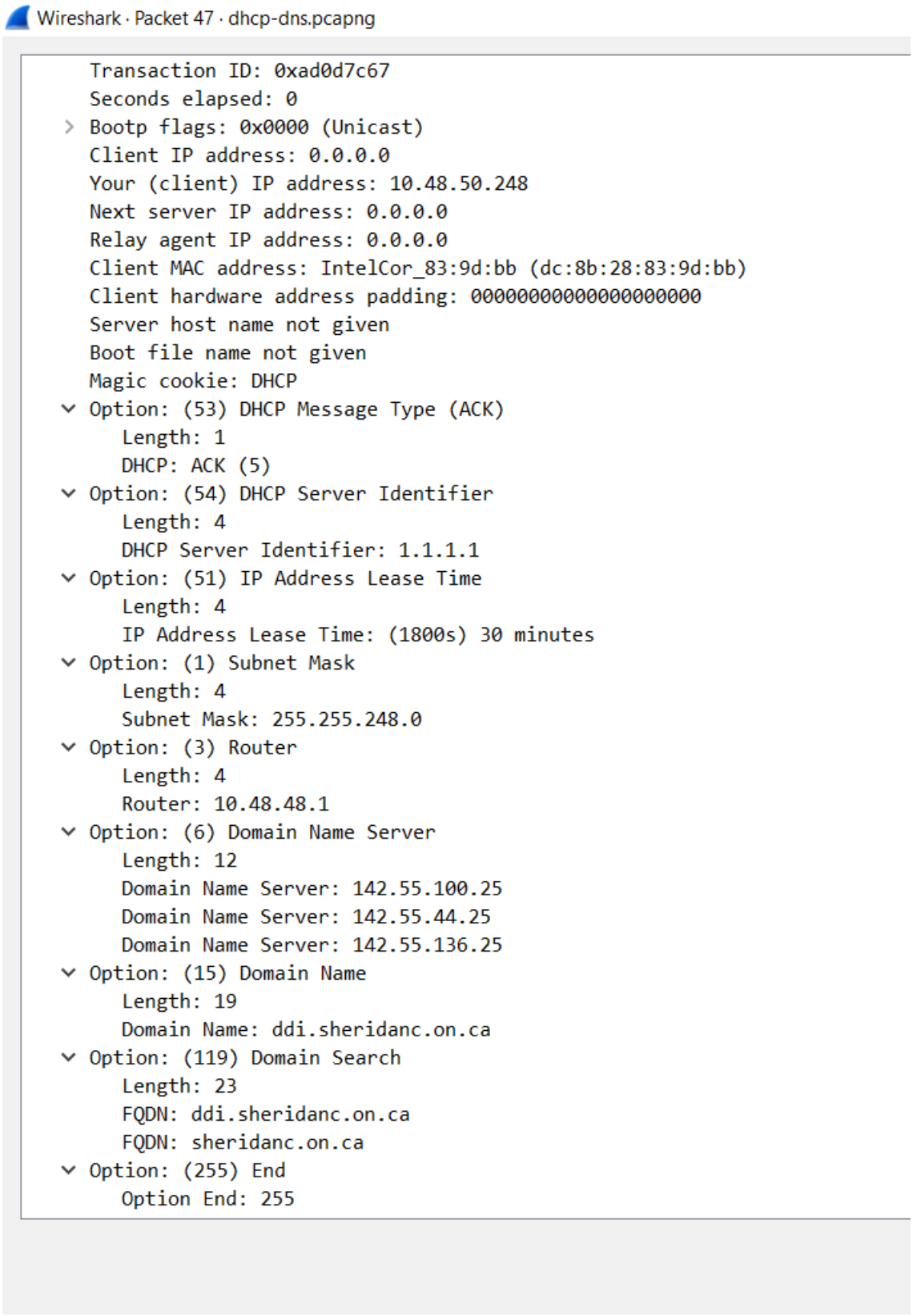

Fig 1.9 DHCP acknowledge options

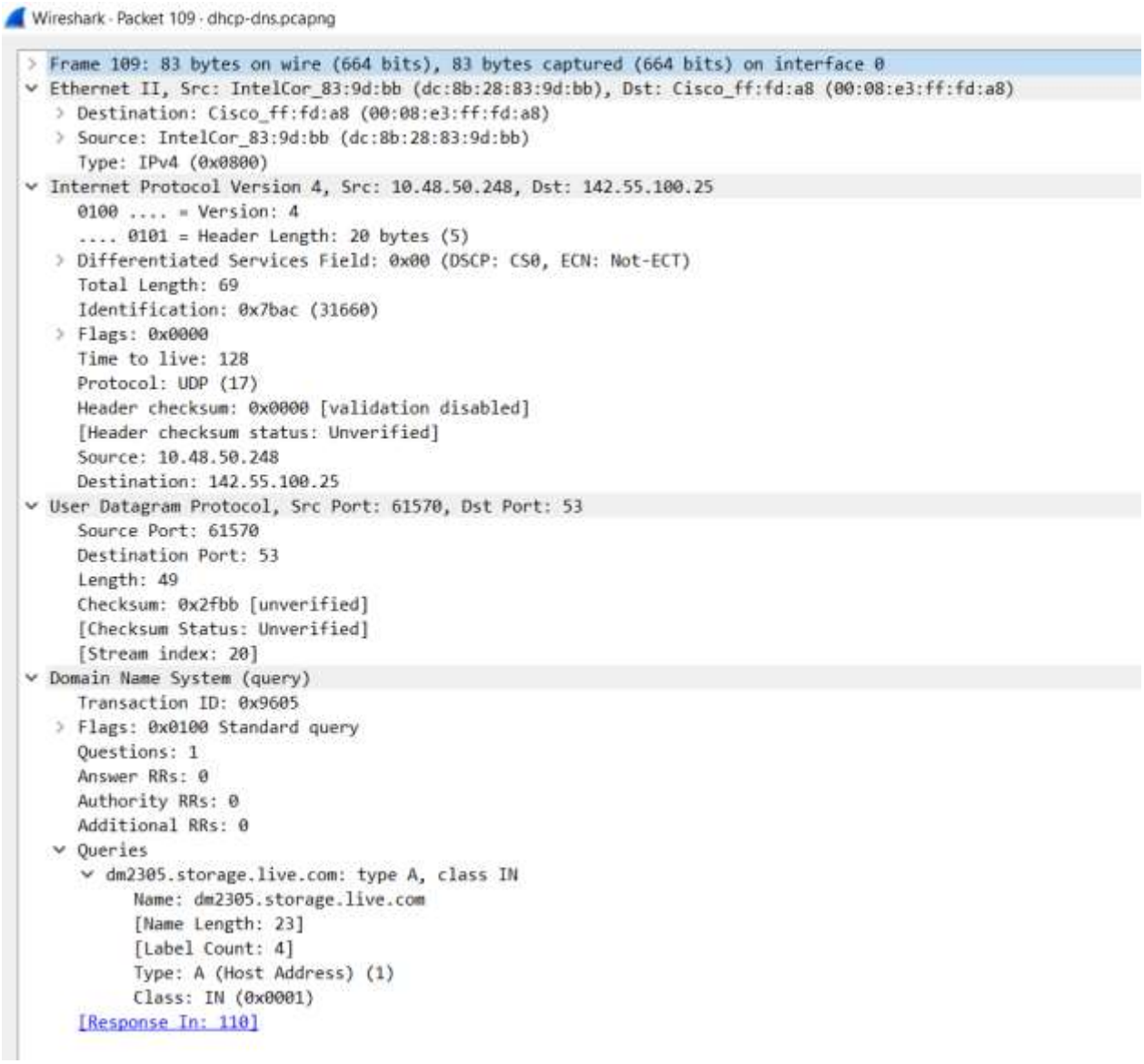

Fig 1.10 DNS request

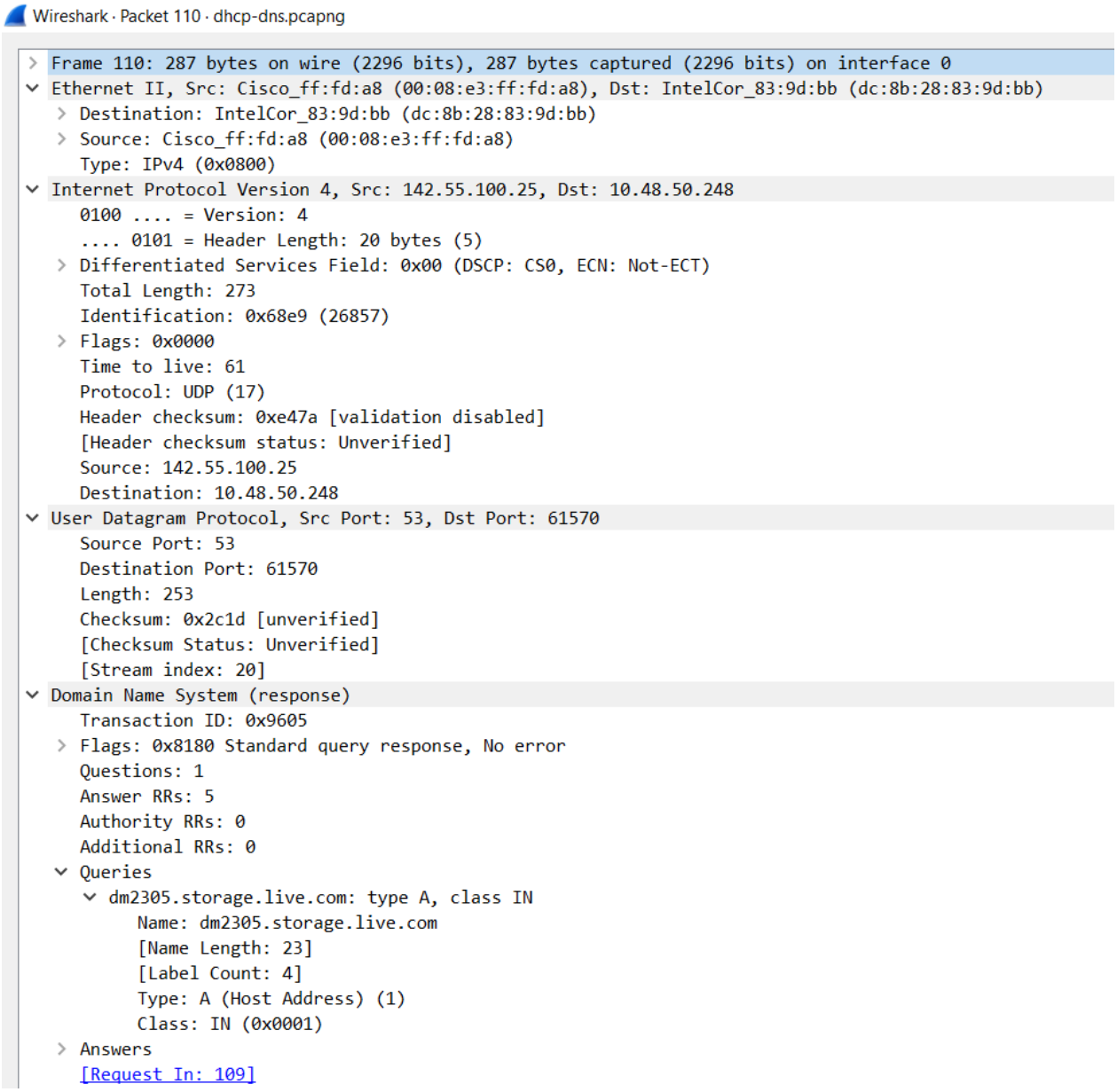

Fig 1.11 DNS response

Step 3: Answer the following questions based on your finding.

DHCP Protocol

1. What address is being used for DHCP request as source? Why it is being used? What address is being used for the DHCP rekmZquest as destination? Why it is being used?

Source address : 0.0.0.0
Destination address: 255.255.255.255

When every network follows same standards then we don't need to remember settings for each network connection. So, by default when you are trying to connect network, your system send request using first IP. Same for destination address. It sends request using broadcast network address.

2. What is the lease timer for your IP? In which DHCP option you can locate it?

Option(51) : IP Address Lease Time
Duration : (1800s) 30 minutes

3. What do the four basic information require for your laptop to access to Internet? Where can you locate that information from the DHCPOFFER? (i.e. which option)

Option(3) Router : 10.48.48.1
Option(6) Domain Name Server : 142.55.100.25
Client IP address : 10.48.50.248
Option(51) IP Address Lease Time : 30 minutes

4. What is the port number for the server end?

Port number : 67

DNS Protocol

1. What is the DNS server IP? Where do you obtain the DNS server IP?

   Obtain it from DHCP server when you request for new IP address
   IP address : 142.55.100.25
   142.55.44.25
   142.55.136.25

2. What is the destination mac address on your DNS request? How do your laptop find out the mac address?

   Destination MAC address : 00:08:e3:ff:fd:a8
   Laptop find that mac address using ARP and RARP which discovers from IP address given by DHCP server.

3. Disable the wireless/wireline connection, do nslookup www.youtube.com in command prompt. Keep the wireshark running. Do you able to resolve the youtube.com domain name? If so, how? If not, what happen after the first DNS request out without response?

   No, unable to resolve server for youtube.com. Basically, you don't get response from server. Since DNS request follows UDP protocol, it doesn't care to wait for DNS response.

4. What is in common for DHCP and DNS request (in terms of transport layer)? Why? What are the differences? (in terms of delivery methodology such as unicast, multicast, broadcast) Why?

   Common : none
   Difference :
   - Destination port for DHCP is 67 and DNS is 53
   - DHCP request uses TCP protocol and DNS uses UDP protocol

5. What is the port number for the server end?

   Port : 53