Capture DHCP&DNS Packets using Wireshark

Name: SHI Yuqi
Class Number: 2013215103
QM Student Number: 130806701
BUPT Student Number: 2013212998

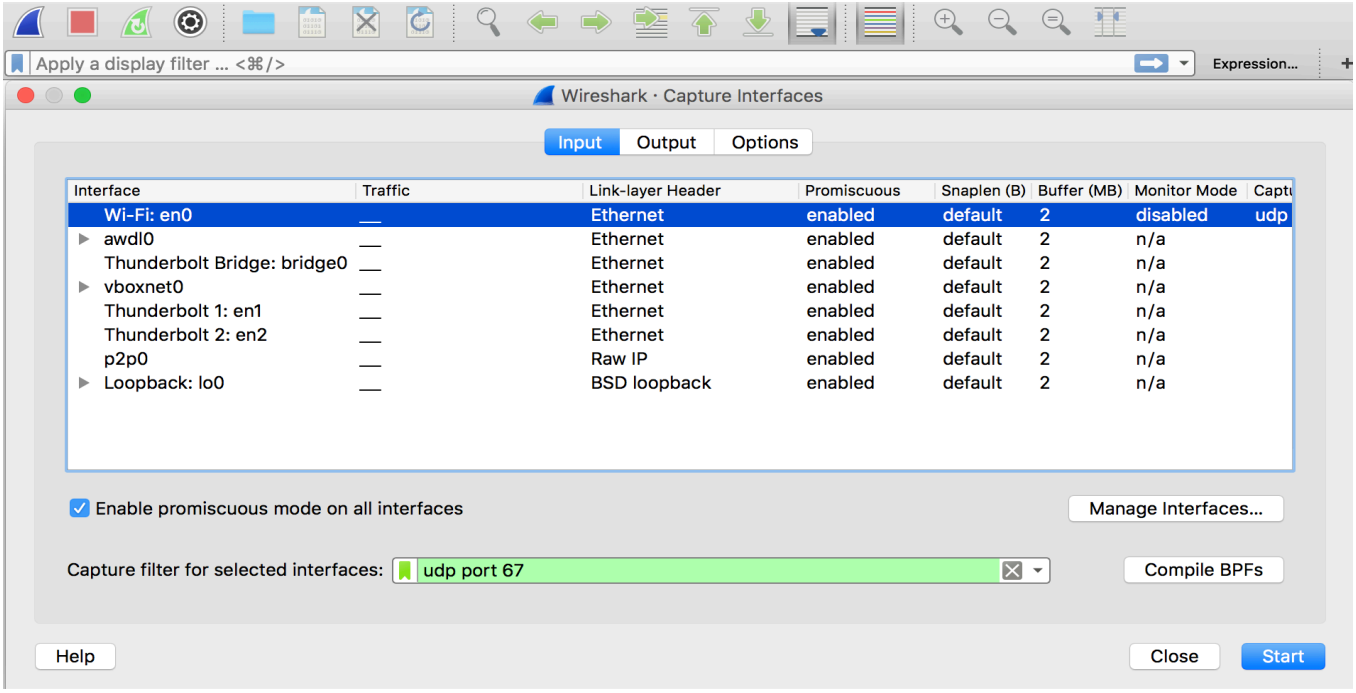
1. Configuration of Wireshark

1.1 Capture Filter Configuration

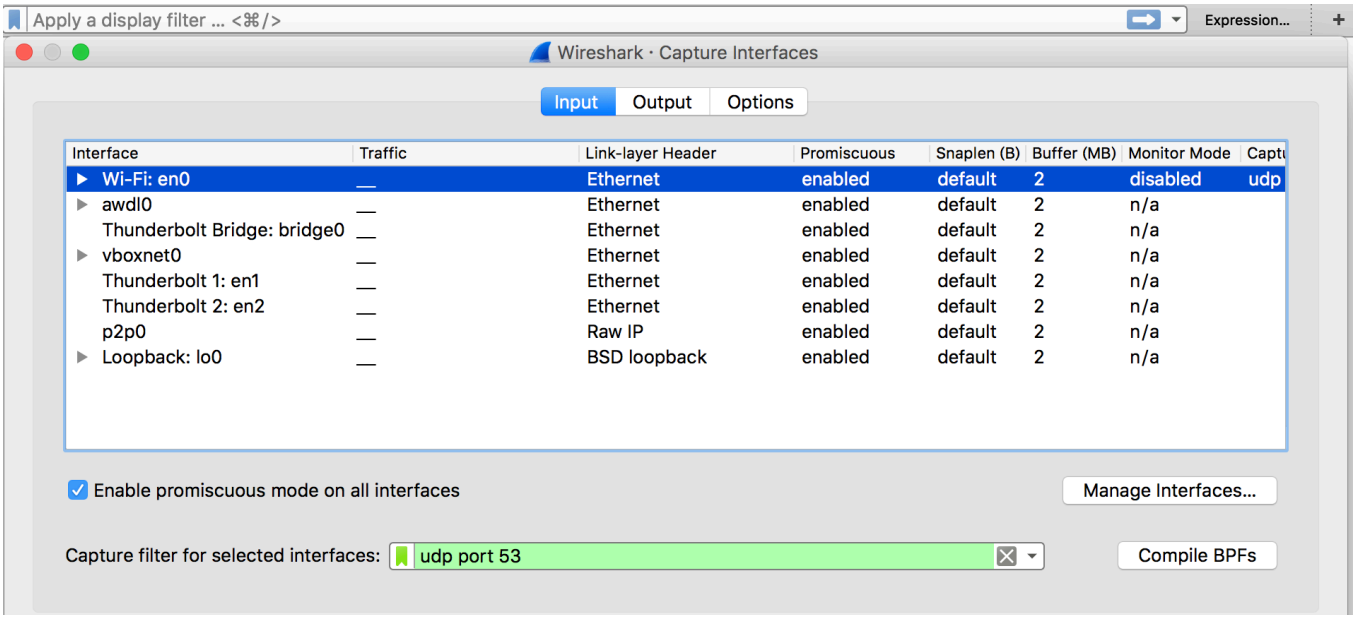
This lab is done in the dormitory 3309 using wireless connection so I choose Wi-Fi: en0 to capture from.

Click the capture options button, then I can set the capture filter.

When we capture DHCP messages, the capture filter is udp port 67.

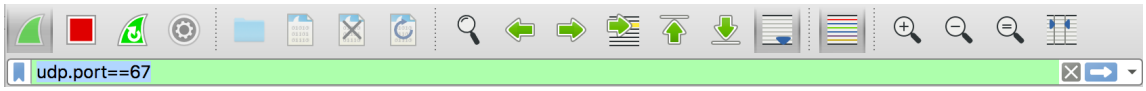


When we capture DNS messages, the capture filter is udp port 53.

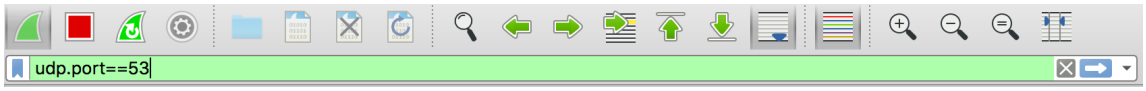


1.2 Display filter configuration

We use udp. port==67 to display only DHCP Packets.



We use udp. port==53 to display only DNS Packets.

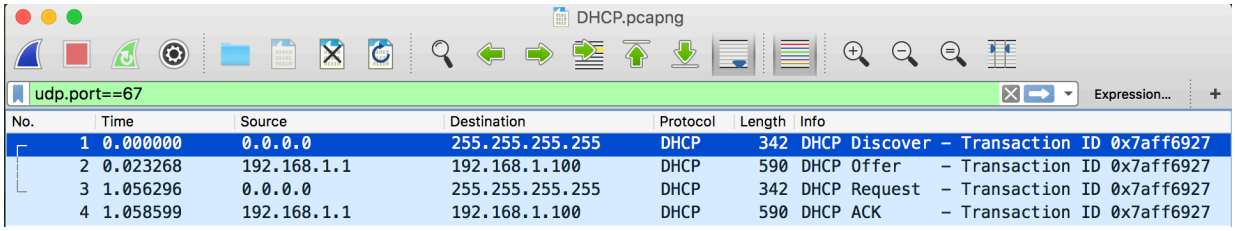


Click the second square button to stop the capturing process, then click the first button to start a new capture process.

2. DHCP Analysis

DHCP provides automatic configuration of remote hosts and it's an extension of BOOTP.

In my MAC, firstly, I start my I Wireshark and configure it to capture and display DHCP packets. Then I follow the step of: Menu -> System Preferences -> Network -> Advanced -> TCP/IP -> Renew DHCP Lease.



The four messages we will analyze are DHCP Discover, Offer, Request and ACK.

They have the same transaction ID 0x7aff6927.

We can learn that the IPv4 address for host is 192.168.1.100

the IPv4 address for DHCP server is 192.168.1.1.

a) DHCP Discover Message

Firstly, client broadcasts to locate available servers, the contents of DHCP discover message are as follows:

```
▶ Frame 1: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
▶ Ethernet II, Src: Apple_a6:ba:49 (ac:bc:32:a6:ba:49), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▶ Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
▶ User Datagram Protocol, Src Port: 68 (68), Dst Port: 67 (67)
▶ Bootstrap Protocol (Discover)
```

- Source frame address: ac:bc:32:a6:ba:49 (client).
- Destination frame address:ff:ff:ff:ff:ff:ff, broadcast to locate available server.
- Source IP address: 0.0.0.0, it hasn't been assigned now.
- Destination IP address: 255.255.255.255,broadcast to locate available server.
- For DHCP protocol, it uses port 68 for client and port 67 for server.

```
▼ Bootstrap Protocol (Discover)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x7aff6927
    Seconds elapsed: 1
  ▶ 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: Apple_a6:ba:49 (ac:bc:32:a6:ba:49)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  ▶ Option: (53) DHCP Message Type (Discover)
  ▶ Option: (55) Parameter Request List
  ▶ Option: (57) Maximum DHCP Message Size
  ▶ Option: (61) Client identifier
  ▶ Option: (51) IP Address Lease Time
  ▶ Option: (12) Host Name
  ▶ Option: (255) End
    Padding: 000000000000000000000000
```

- Message type: Boot Request (1), it is a request message from client to server.
- Transaction ID: 0x7aff6927, an integer used by the client to match responses with requests.
- Client IP address: 0.0.0.0, client doesn't know its IP address now because the server doesn't assign it to client, it is only filled in if client is in BOUND, RENEW or REBIND state.
- Your IP address: 0.0.0.0, it is the client IP address that server wants to assign, it isn't assigned now.
- Next server IP address: 0.0.0.0, client doesn't know the server's IP address, so it is set to 0.
- Relay agent IP address: 0.0.0.0, client doesn't know the relay agent IP address, so it is set to 0

The option 53, 55,51,12 are as follows:

```
▼ Option: (53) DHCP Message Type (Discover)
    Length: 1
    DHCP: Discover (1)
▼ Option: (55) Parameter Request List
    Length: 10
    Parameter Request List Item: (1) Subnet Mask
    Parameter Request List Item: (121) Classless Static Route
    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: (119) Domain Search
    Parameter Request List Item: (252) Private/Proxy autodiscovery
    Parameter Request List Item: (95) LDAP [TODO:RFC3679]
    Parameter Request List Item: (44) NetBIOS over TCP/IP Name Server
    Parameter Request List Item: (46) NetBIOS over TCP/IP Node Type
▶ Option: (57) Maximum DHCP Message Size
▶ Option: (61) Client identifier
▼ Option: (51) IP Address Lease Time
    Length: 4
    IP Address Lease Time: (7776000s) 90 days
▼ Option: (12) Host Name
    Length: 11
    Host Name: serenadeMBP
▶ Option: (255) End
  Padding: 00000000000000000000000
```

The format of option is as follows:

label	length	value

- Option 53: DHCP message type

  This option is used to convey the type of the DHCP message. The code for this option is 53,

  and its length is 1. Legal values for this option are:

  1. DHCPDISCOVER 2. DHCPOFFER 3. DHCPREQUEST

  4. DHCPDECLINE 5. DHCPACK 6. DHCPNAK

  7. DHCPRELEASE 8. DHCPINFORM

  The value is 1 means it is a DHCP Discover message.

- Option 55: Parameter request list

  This option is used by a DHCP client to request values for specified configuration parameters.

  The list of requested parameters is specified as n octets, where each octet is a valid DHCP option code as defined in this document. Its length is 10.

- Option 51: IP address lease time

  The option is used in a client request to allow the client to request a lease time for IP address. The time is in units of seconds, and is specified as a 32-bit unsigned integer.

  Its length is 4 and the value is 90 days.

- Option 12: Host name

  This option specifies the name of the client. Its length is 11 and name is serenadeMBP.

Compared with the example in lecture notes:

All fields are the same except the transaction ID and the MAC address.

What's more the seconds elapsed since client began address acquisition or renewal process changed to 1.

capture				example			
1	1	6	0	1	1	6	0
0x7aff6927				12			
1		flags		0		flags	
0				0			
0				0			
0				0			
0				0			
ac:bc:32:a6:ba:49				aa:ec:f9:23:44:19			

b) DHCP Offer Message

DHCP offer message is from server to client in response to DHCPDISCOVER Message and offer the client with the configuration parameters.

The contents of DHCP offer message are as follows:

```
▶ Frame 2: 590 bytes on wire (4720 bits), 590 bytes captured (4720 bits) on interface 0
▶ Ethernet II, Src: Tp-LinkT_e5:aa:34 (28:2c:b2:e5:aa:34), Dst: Apple_a6:ba:49 (ac:bc:32:a6:ba:49)
▶ Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.100
▶ User Datagram Protocol, Src Port: 67 (67), Dst Port: 68 (68)
▶ Bootstrap Protocol (Offer)
```

- Source frame address: 28:2c:b2:e5:aa:34 (server).
- Destination frame address: ac:bc:32:a6:ba:49(client)
- Source IP address:192.168.1.1, it is the relay agent IP address.
- Destination IP address:192.168.1.100
- For DHCP protocol, it uses port 68 for client and port 67 for server.

```
▼ Bootstrap Protocol (Offer)
    Message type: Boot Reply (2)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x7aff6927
    Seconds elapsed: 0
  ▶ Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 192.168.1.100
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: Apple_a6:ba:49 (ac:bc:32:a6:ba:49)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
```

- Message type: Boot Reply (2), it is a reply message from server to client.
- Transaction ID: 0x7aff6927, an integer used by the client to match responses with requests.
- Client IP address: 0.0.0.0, client doesn't know its IP address now because the server doesn't assign it to the client, it only filled in if client is in BOUND, RENEW or REBIND state.
- Your IP address: 192.168.1.100, it is the client IP address that server wants to assign.
- Next server IP address: 0.0.0.0, server's IP address is in option 54.
- Relay agent IP address: 0.0.0.0, client doesn't know the relay agent IP address, so it is set to 0.

The option 53, 54,51,6,1,3 are as follows:

```
▼ Option: (53) DHCP Message Type (Offer)
    Length: 1
    DHCP: Offer (2)
▼ Option: (54) DHCP Server Identifier
    Length: 4
    DHCP Server Identifier: 192.168.1.1
▼ Option: (51) IP Address Lease Time
    Length: 4
    IP Address Lease Time: (7200s) 2 hours
▼ Option: (6) Domain Name Server
    Length: 8
    Domain Name Server: 221.130.33.60
    Domain Name Server: 221.130.33.52
▼ Option: (1) Subnet Mask
    Length: 4
    Subnet Mask: 255.255.255.0
▼ Option: (3) Router
    Length: 4
    Router: 192.168.1.1
▶ Option: (255) End
  Padding: 0000000000000000000000000000000000000000000000...
```

- Option 53: DHCP message type (offer)
  The value is 2 means it is a DHCP offer message.

- Option 54: DHCP server identifier
  DHCP servers include this option in the DHCPOFFER in order to allow the client to distinguish between lease offers. DHCP clients use the contents of the 'server identifier' field as the destination address for any DHCP messages unicast to the DHCP server. Its length is 4
  and the DHCP server's IP address is 192.168.1.1.

- Option 51: IP address lease time
  In a server reply, a DHCP server uses this option to specify the lease time it is willing to offer.
  The time is in units of seconds, and is specified as a 32-bit unsigned integer. Its length is 4 and the value is 2 hours.

- Option 6: Domain name server
  The domain name server option specifies a list of Domain Name System (STD 13, RFC 1035) name servers available to the client. Servers should be listed in order of preference. Its length is 8 and it has 2 domain name servers.

- Option 1: Subnet mask

  The subnet mask option specifies the client's subnet mask as per RFC 950. If both the subnet mask and the router option are specified in a DHCP reply, the subnet mask option must be first. Its length is 4 and the value is 255.255.255.0.

- Option 3: Router

  The router option specifies a list of IP addresses for routers on the client's subnet. Routers should be listed in order of preference. Its length is 4 and the router's IP address is 192.168.1.1

Compared with the example in lecture notes:

All fields are the same except the transaction ID, your IP address, next server IP address, router IP address and the MAC address of client.

It's quite strange that the router IP address doesn't equal to the relay agent address which confuse me a lot.

capture				example			
2	1	6	0	2	1	6	0
0x7aff6927				12			
0		flags		0		flags	
0				0			
192.168.1.100				192.168.10.35			
192.168.1.1				192.168.10.98			
192.168.1.1				0			
ac:bc:32:a6:ba:49				aa:ec:f9:23:44:19			
53	1	2		53	1	2	

c) DHCP Request Message

1. DHCP request message is from client to server, it can do these things:

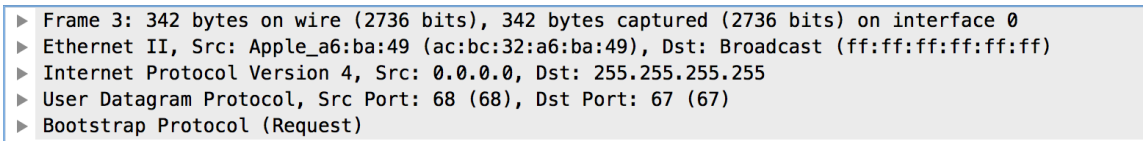
(a) requesting offered parameters from one server and declining offers from all others

(b) confirming correctness of previously allocated address

(c) extending the lease on a particular network address.

The DHCP request message is broadcast so that it can request a lease as well as inform the unselected servers. The client chooses one DHCPOFFER from all the offers it receives, regardless of which subnet the DHCP server is located in. The servers are informed that client accepts whose offer and the unselected servers will withdraw the offers.

The contents of DHCP request message are as follows:



- Source frame address: ac:bc:32:a6:ba:49 (client).
- Destination frame address: ff:ff:ff:ff:ff:ff, broadcast so that it can request a lease as well as inform the unselected servers.
- Source IP address: 0.0.0.0, it hasn't been assigned now.
- Destination IP address: 255.255.255.255, broadcast so that it can requesta lease as well as inform the unselected servers.
- For DHCP protocol, it uses port 68 for client and port 67 for server.

```
▼ Bootstrap Protocol (Request)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x7aff6927
    Seconds elapsed: 3
  ▶ 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: Apple_a6:ba:49 (ac:bc:32:a6:ba:49)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
```

- Message type: Boot Request (1), it is a request message from client to server.
- Transaction ID: 0x7aff6927, an integer used by the client to match responses with requests.
- Client IP address: 0.0.0.0, client doesn't know its IP address now because the server hasn't assign it, it is only filled in if client is in BOUND, RENEW or REBIND state.
- Your IP address: 0.0.0.0, it is the client IP address that server wants to assign, this message is from client to server so it is set 0.
- Next server IP address: 0.0.0.0, the selected server's IP address is in option 54.
- Relay agent IP address: 0.0.0.0, client doesn't know the relay agent IP address so set it 0.

The unfolded contents of option 53, 55, 50, 54, 12 are as follows:

```
▼ Option: (53) DHCP Message Type (Request)
    Length: 1
    DHCP: Request (3)
▼ Option: (55) Parameter Request List
    Length: 10
    Parameter Request List Item: (1) Subnet Mask
    Parameter Request List Item: (121) Classless Static Route
    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: (119) Domain Search
    Parameter Request List Item: (252) Private/Proxy autodiscovery
    Parameter Request List Item: (95) LDAP [TODO:RFC3679]
    Parameter Request List Item: (44) NetBIOS over TCP/IP Name Server
    Parameter Request List Item: (46) NetBIOS over TCP/IP Node Type
▶ Option: (57) Maximum DHCP Message Size
▶ Option: (61) Client identifier
▼ Option: (50) Requested IP Address
    Length: 4
    Requested IP Address: 192.168.1.100
▼ Option: (54) DHCP Server Identifier
    Length: 4
    DHCP Server Identifier: 192.168.1.1
▼ Option: (12) Host Name
    Length: 11
    Host Name: serenadeMBP
▶ Option: (255) End
  Padding: 000000000000
```

- Option 53: DHCP message type

  The value is 3 means it is a DHCP request message.

- Option 55: Parameter request list

  This option is used by a DHCP client to request values for specified configuration parameters.

  The list of requested parameters is specified as n octets, where each octet is a valid DHCP option code as defined in this document. Its length is 10.

- Option 50: Requested IP address

  This option is used in a client request to allow the client to request that a particular IP address be assigned. Its length is 4. It shows the requested IP address is 192.168.1.100, which is the source address in the release message that mentioned above.

- Option 12: Host name

  This option specifies the name of the client. Its length is 11 and name is serenadeMBP.

- Option 54: DHCP server identifier
  DHCP client indicates which of several lease offers is being accepted by including this option in a DHCP request message. The identifier is the IP address of the selected server. Its length is 4 and the selected server's IP address is 192.168.1.1.

  Compared with the example in lecture notes:

  All fields are the same except the transaction ID and the MAC address.

capture				example			
1	1	6	0	1	1	6	0
0x7aff6927				12			
3		flags		0		flags	
0				0			
0				0			
0				0			
0				0			
ac:bc:32:a6:ba:49				aa:ec:f9:23:44:19			
53	1	3		53	1	3	

d) DHCP ACK Message

DHCP ACK message is from server to client with configuration parameters, including committed network address. It is the response of DHCP request message from client to server and after that the IP address is assigned to the client.

The contents of DHCP ACK message are as follows:

```
▶ Frame 4: 590 bytes on wire (4720 bits), 590 bytes captured (4720 bits) on interface 0
▶ Ethernet II, Src: Tp-LinkT_e5:aa:34 (28:2c:b2:e5:aa:34), Dst: Apple_a6:ba:49 (ac:bc:32:a6:ba:49)
▶ Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.100
▶ User Datagram Protocol, Src Port: 67 (67), Dst Port: 68 (68)
▶ Bootstrap Protocol (ACK)
```

- Source frame address: 28:2c:b2:e5:aa:34 (server).
- Destination frame address: ac:bc:32:a6:ba:49broadcast because the client isn't assigned IP address now, so it can't respond the ARP from server.
- Source IP address: 192.168.1.1, it is the relay agent IP address.
- Destination IP address:192.168.1.100
- For DHCP protocol, it uses port 68 for client and port 67 for server

```
▼ Bootstrap Protocol (ACK)
    Message type: Boot Reply (2)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x7aff6927
    Seconds elapsed: 0
  ▶ Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 192.168.1.100
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: Apple_a6:ba:49 (ac:bc:32:a6:ba:49)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
```

- Message type: Boot Reply (2), it is a reply message from server to client.
- Transaction ID: 0x7aff6927, an integer used by the client to match responses with requests.
- Client IP address: 0.0.0.0, client doesn't know its IP address now because the server doesn't assign it, it is only filled in if client is in BOUND, RENEW or REBIND state.
- Your IP address: 192.168.1.100, it is the client IP address that server wants to assign.
- Next server IP address: 0.0.0.0, server's IP address is in option 54.
- Relay agent IP address: 0.0.0.0, it uses a relay agent to pass this message.

The contents of option 53, 54, 51, 6, 1, 3 are as follows:

```
▼ Option: (53) DHCP Message Type (ACK)
    Length: 1
    DHCP: ACK (5)
▼ Option: (54) DHCP Server Identifier
    Length: 4
    DHCP Server Identifier: 192.168.1.1
▼ Option: (51) IP Address Lease Time
    Length: 4
    IP Address Lease Time: (7200s) 2 hours
▼ Option: (6) Domain Name Server
    Length: 8
    Domain Name Server: 221.130.33.60
    Domain Name Server: 221.130.33.52
▼ Option: (1) Subnet Mask
    Length: 4
    Subnet Mask: 255.255.255.0
▼ Option: (3) Router
    Length: 4
    Router: 192.168.1.1
```

- Option 53: DHCP message type
  The value is 5 means it is a DHCP ACK message.

- Option 54: DHCP server identifier
  DHCP servers include this option in the DHCP ACK in order to allow the client to distinguish between lease offers. Its length is 4 and it shows the server's IP address is 192.168.1.1.

- Option 51: IP address lease time
  In a server reply, a DHCP server uses this option to specify the lease time it is willing to offer. The time is in units of seconds, and is specified as a 32-bit unsigned integer. Its length is 4 and the value is 2 hours.

- Option 6: Domain name server
  The domain name server option specifies a list of Domain Name System (STD 13, RFC 1035) name servers available to the client. Servers should be listed in order of preference. Its length is 8 and it has 2 domain name servers.

- Option 1: Subnet mask
  The subnet mask option specifies the client's subnet mask as per RFC 950. If both the subnet mask and the router option are specified in a DHCP reply, the subnet mask option must be first. Its length is 4 and the value is 255.255.255.0.

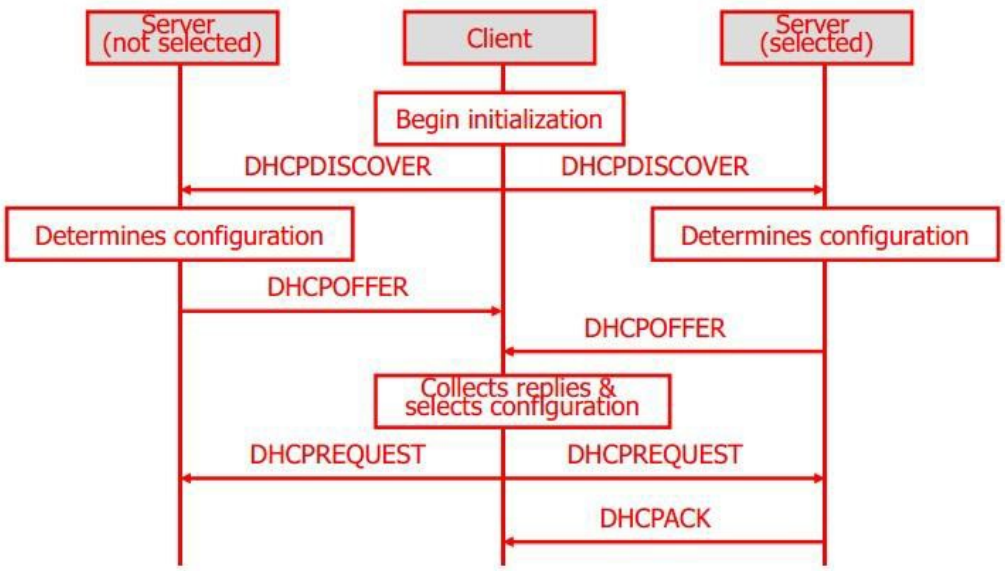
- Option 3: Router
  The routeroption specifies a list of IP addresses for routers on the client's subnet. Routers should be listed in order of preference. Its length is 4 and the router's IP address is 192.168.1.1

Compared with the example in lecture notes:

All fields are the same except the transaction ID, your IP address, next server IP address, relay agent IP address and the MAC address. Use relay agent to pass the message

capture				example			
2	1	6	0	2	1	6	0
0x7aff6927				12			
0		flags		0		flags	
0				0			
192.168.1.100				192.168.10.35			
0				192.168.10.98			
192.168.1.1				0			
ac:bc:32:a6:ba:49				aa:ec:f9:23:44:19			
53	1	5		53	1	5	

DHCP MSC



2. DNS Analysis

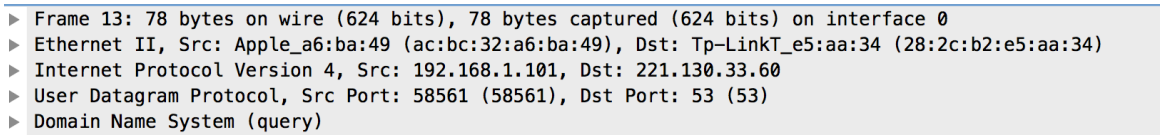
The Domain Name System (DNS) is a hierarchical distributed naming system for computers, services, or any other resources connected to the Internet or a private network. It translates easily memorized domain names to the numerical IP addresses needed for the purpose of locating computer services and devices worldwide.

3.1 Find a pair of A type message

Type a URL www.imperial.ac.uk in my browser, and then type "nslookup www.imperial.ac.uk" in cmd
Then I capture these two A type DNS messages:

The first one is the query message and the second one is the response

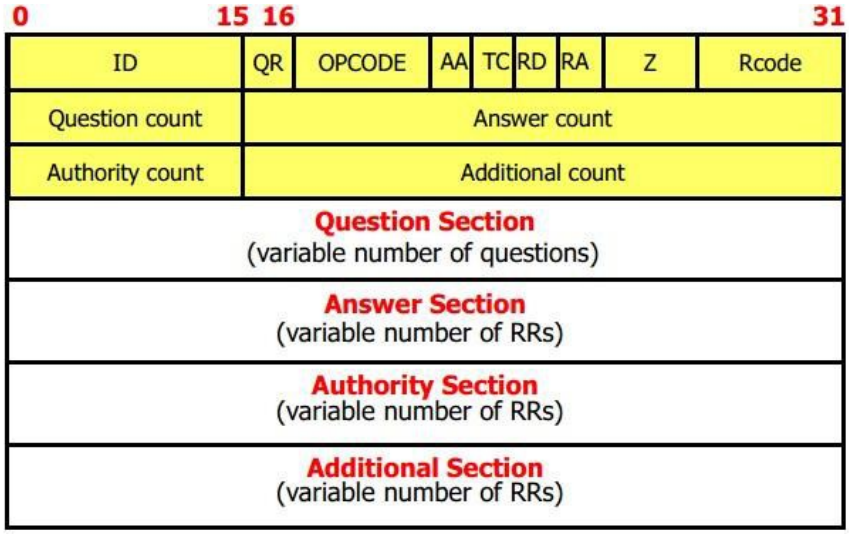
3.1.1 Query message analysis



- Source frame address: ac:bc:32:a6:ba:49(client).
- Destination frame address: 28:2c:b2:e5:aa:34(server).
- Source IP address: 192.168.1.101(client).
- Destination IP address: 221.130.33.60(server).
- For DNS protocol, it uses port 53 for server, the port number of client is assigned randomly from 1024 to 65535, in this case is 58561.

```
▼ Domain Name System (query)
    [Response In: 14]
    Transaction ID: 0x1973
  ▼ Flags: 0x0100 Standard query
      0... .... .... .... = Response: Message is a query
      .000 0... .... .... = Opcode: Standard query (0)
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... .0.. .... = Z: reserved (0)
      .... .... ...0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▼ Queries
    ▼ www.imperial.ac.uk: type A, class IN
        Name: www.imperial.ac.uk
        [Name Length: 18]
        [Label Count: 4]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
```

The query message format is as follows:

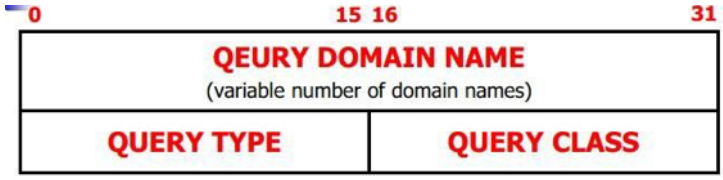


- ID: Transaction ID is 0x1973, it is a 16-bit field used to correlate queries and responses.
- QR: 1-bit field that identifies the message as a query (0) or response (1). This message is a query.
- OPCODE: 4-bit field that describes the type of query:

  0: Standard query (name to address).1: Inverse query (address to name). 2: Server status request. This message is a standard query.
- AA: Only response message has it.
- TC: Truncation. 1-bit field. When set to 1, indicates the message has been truncated due to length greater than that permitted. This message is not truncated.
- RD: Recursion Desired. 1-bit field. Set to 1 by the resolver to request

- RA: Only response message has it.
- Z: 3-bit field. Reserved for future use. Must be set to 0.
- RCODE: Only response message has it.
- Question count: 16-bit field that defines the number of entries in the question section, it is 1 in this message.
- Answer count: 16-bit field that defines the number of resource records in the answer section, it is 0 in this message.
- Authority count: 16-bit field that defines the number of name server resource records in the authority section, it is 0 in this message.
- Additional count: 16-bit field that defines the number of resource records in the additional records section, it is 0 in this message.

The question section format is as follows:



The question domain name is www.imperial.ac.uk . Query type is a 16-bit field used to specify the type of the query. A means host address. Class is a 16-bit field used to specify the class of the query. IN means Internet system.

Compared with the example in lecture notes:

	capture	example
Header	OPCODE=SQUERY	OPCODE=SQUERY
Question Section	QNAME=www.cmu.com QCLASS=IN, QYPE=A	QNAME=SRI-ARPA, QCLASS=IN, QYPE=A
Answer Section	<empty>	<empty>
Authority Section	<empty>	<empty>
Additional Section	<empty>	<empty>

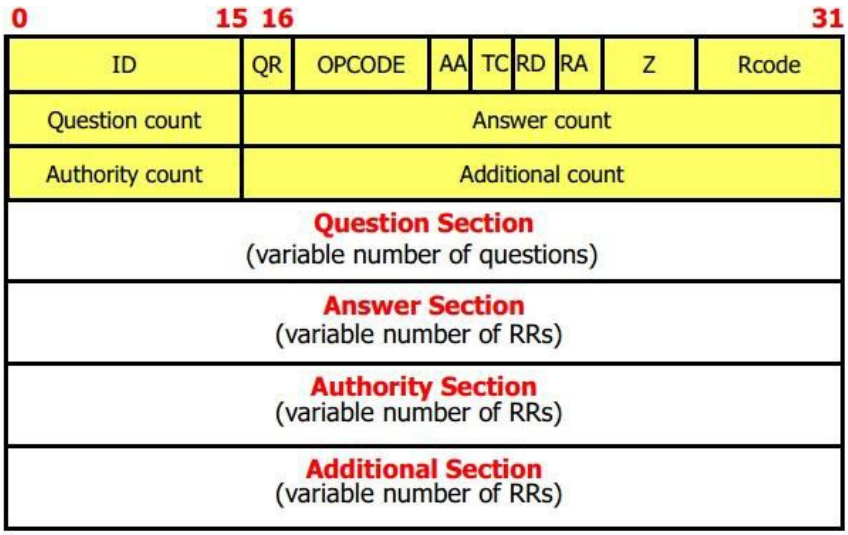
3.1.2 Response message analysis

```
▶ Frame 14: 123 bytes on wire (984 bits), 123 bytes captured (984 bits) on interface 0
▶ Ethernet II, Src: Tp-LinkT_e5:aa:34 (28:2c:b2:e5:aa:34), Dst: Apple_a6:ba:49 (ac:bc:32:a6:ba:49)
▶ Internet Protocol Version 4, Src: 221.130.33.60, Dst: 192.168.1.101
▶ User Datagram Protocol, Src Port: 53 (53), Dst Port: 58561 (58561)
▶ Domain Name System (response)
```

- Source frame address: 28:2c:b2:e5:aa:34 (server).
- Destination frame address: ac:bc:32:a6:ba:49 (client).
- Source IP address: 221.130.33.60(server).
- Destination IP address: 192.168.1.101(client)
- For DNS protocol, it uses port 53 for server, the port number of client is assigned randomly from 1024 to 65535, in this case is 58561 same as the query message

```
▼ Domain Name System (response)
    [Request In: 13]
    [Time: 0.807841000 seconds]
    Transaction ID: 0x1973
  ▼ Flags: 0x8180 Standard query response, No error
      1... .... .... .... = Response: Message is a response
      .000 0... .... .... = Opcode: Standard query (0)
      .... .0.. .... .... = Authoritative: Server is not an authority for domain
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... 1... .... = Recursion available: Server can do recursive queries
      .... .... .0.. .... = Z: reserved (0)
      .... .... ..0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server
      .... .... ...0 .... = Non-authenticated data: Unacceptable
      .... .... .... 0000 = Reply code: No error (0)
    Questions: 1
    Answer RRs: 2
    Authority RRs: 0
    Additional RRs: 0
```

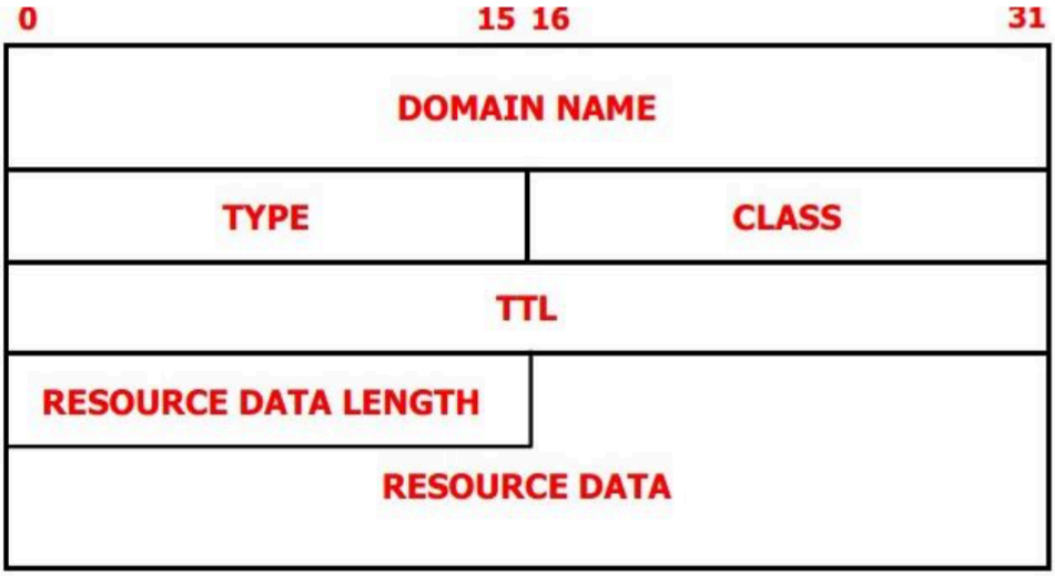
The response message format is follows:



- ID: Transaction ID is 0x1973, it is a 16-bit field used to correlate queries and responses.
- QR: 1-bit field that identifies the message as a query (0) or response (1). This message is a response.
- OPCODE: This message is a standard query.
- AA: Only response message has it.
- TC: This message is not truncated.
- RD: Recursion Desired. 1-bit field. Set to 1 by the resolver to request recursive service by the name server. It wants to do query recursively.
- RA: Only response message has it it's set to 1.
- Z: 3-bit field. Reserved for future use. Must be set to 0.
- RCODE: Only response message has it.
- Question count: 16-bit field that defines the number of entries in the question section, it is 1 in this message.
- Answer count: 16-bit field that defines the number of resource records in the answer section, it is 2 in this message.
- Authority count: 16-bit field that defines the number of name server resource records in the authority section, it is 0 in this message.
- Additional count: 16-bit field that defines the number of resource records in the additional records section, it is 0 in this message.

```
▼ Queries
  ▼ www.imperial.ac.uk: type A, class IN
      Name: www.imperial.ac.uk
      [Name Length: 18]
      [Label Count: 4]
      Type: A (Host Address) (1)
      Class: IN (0x0001)
▼ Answers
  ▼ www.imperial.ac.uk: type CNAME, class IN, cname wrp.cc.gslb.ic.ac.uk
      Name: www.imperial.ac.uk
      Type: CNAME (Canonical NAME for an alias) (5)
      Class: IN (0x0001)
      Time to live: 300
      Data length: 17
      CNAME: wrp.cc.gslb.ic.ac.uk
  ▼ wrp.cc.gslb.ic.ac.uk: type A, class IN, addr 155.198.64.24
      Name: wrp.cc.gslb.ic.ac.uk
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 30
      Data length: 4
      Address: 155.198.64.24
```

We can see the non-authoritative answer from the cmd that the answer address is 155.198.64.24 same as the packet that caught.



First resource record's type is CNAME, it maps an alias name to the true canonical name. The official name of www.imperial.ac.uk is wrp.cc.gslb.ic.ac.uk.

The second record type is A, it maps the name of a system to its address. If a system has several addresses, then there will be a separate record for each.

```
serenadeMacBook-Pro:~ serenashi$ nslookup www.imperial.ac.uk
Server:         221.130.33.60
Address:        221.130.33.60#53

Non-authoritative answer:
www.imperial.ac.uk      canonical name = wrp.cc.gslb.ic.ac.uk.
Name:   wrp.cc.gslb.ic.ac.uk
Address: 155.198.64.24
```

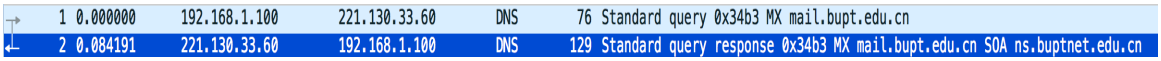
Compared with the example in lecture notes:

	capture	example
Header	OPCODE=SQUERY, RESPONSE, AA	OPCODE=SQUERY, RESPONSE, AA
Question Section	www.imperial.ac.uk QCLASS=IN, QYPE=A	QNAME=SRI-ARPA, QCLASS=IN, QYPE=A
Answer Section	2 records as mentioned before	SRI-NIC,ARPA, 86400 IN A 26.0.0.73 86400 IN A 26.0.0.51
Authority Section	0 records as mentioned before	<empty>
Additional Section	0 records as mentioned before	<empty>

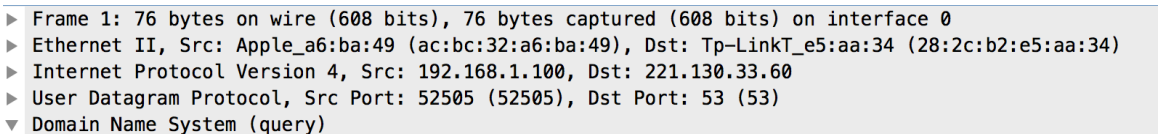
3.2 Find a pair of MX type message

Deliver an e-mail from the website mail.bupt.edu.cn, and then type "nslookup –type=MX mail.bupt.edu.cn" in cmd

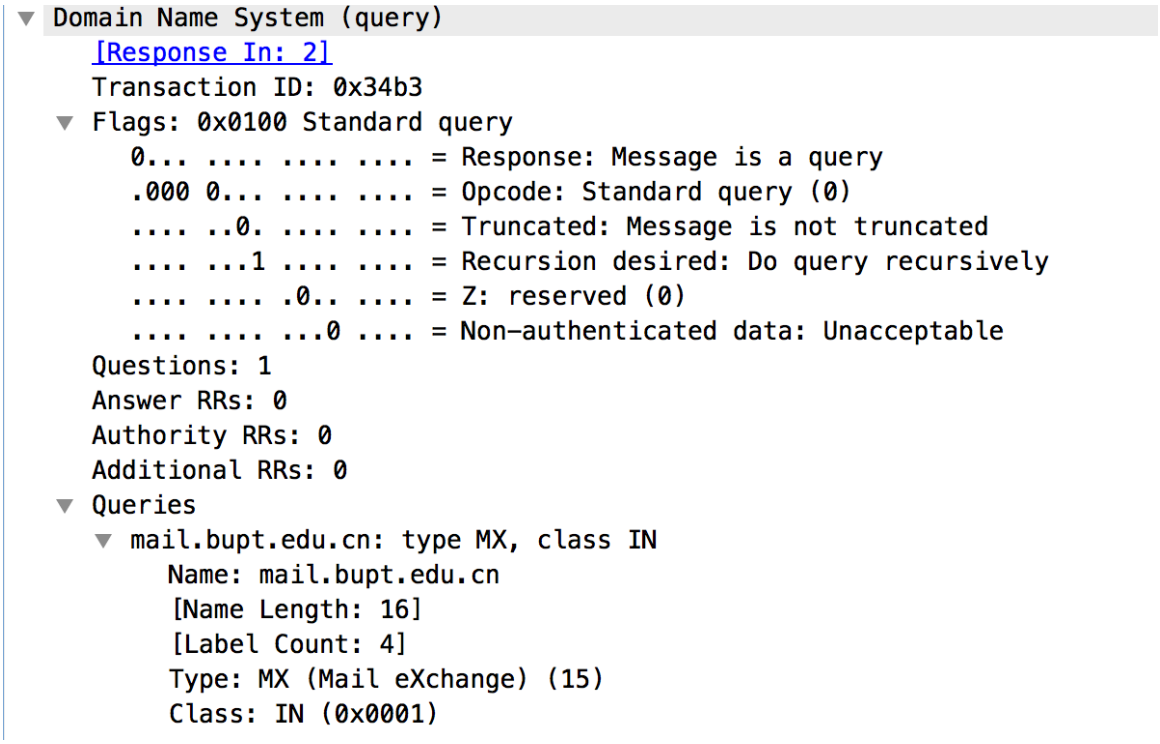
Then I capture these two MX type DNS messages:



3.2.1 Query message analysis



- Source frame address: ac:bc:32:a6:ba:49(client).
- Destination frame address: 28:2c:b2:e5:aa:34(server).
- Source IP address: 192.168.1.100(client).
- Destination IP address: 221.130.33.60(server).
- For DNS protocol, it uses port 53 for server, the port number of client is assigned randomly from 1024 to 65535, in this case is 52505.



- ID: Transaction ID is 0x34b3, it is a 16-bit field used to correlate queries and responses.
- QR: This message is a query.
- OPCODE: This message is a standard query.
- AA: Only response message has it.
- TC: Truncation. 1-bit field. When set to 1, indicates the message has been truncated due to length greater than that permitted. This message is not truncated.
- RD: Recursion Desired. 1-bit field. Set to 1 by the resolver to request recursive service by the name server. It wants to do query recursively.
- RA: Only response message has it.
- Z: 3-bit field. Reserved for future use. Must be set to 0.
- RCODE: Only response message has it.
- Question count: 16-bit field that defines the number of entries in the question section, it is 1 in this message.
- Answer count: 16-bit field that defines the number of resource records in the answer section, it is 0 in this message.
- Authority count: 16-bit field that defines the number of name server resource records in the authority section, it is 0 in this message.
- Additional count: 16-bit field that defines the number of resource records in the additional records section, it is 0 in this message.

The question domain name is mail.bupt.edu.cn. Query type is a 16-bit field used to specify the type of the query. MX means mail exchange. Class is a 16-bit field used to specify the class of the query. IN means Internet system.

Compared with the example in lecture notes:

	capture	example
Header	OPCODE=SQUERY	OPCODE=SQUERY
Question Section	mail.bupt.edu.cn QCLASS=IN, QYPQE=MX	QNAME=SRI-ARPA, QCLASS=IN, QYPE=A
Answer Section	<empty>	<empty>
Authority Section	<empty>	<empty>
Additional Section	<empty>	<empty>

3.2.2 Response message analysis

```
▶ Frame 2: 129 bytes on wire (1032 bits), 129 bytes captured (1032 bits) on interface 0
▶ Ethernet II, Src: Tp-LinkT_e5:aa:34 (28:2c:b2:e5:aa:34), Dst: Apple_a6:ba:49 (ac:bc:32:a6:ba:49)
▶ Internet Protocol Version 4, Src: 221.130.33.60, Dst: 192.168.1.100
▶ User Datagram Protocol, Src Port: 53 (53), Dst Port: 52505 (52505)
▶ Domain Name System (response)
```

- Source frame address: 28:2c:b2:e5:aa:34 (server).
- Destination frame address: ac:bc:32:a6:ba:49 (client).
- Source IP address: 221.130.33.60(server).
- Destination IP address: 192.168.1.101(client)
- For DNS protocol, it uses port 53 for server, the port number of client is assigned randomly from 1024 to 65535, in this case is 52505 same as the query message

```
▼ Domain Name System (response)
    [Request In: 1]
    [Time: 0.084191000 seconds]
    Transaction ID: 0x34b3
  ▼ Flags: 0x8180 Standard query response, No error
      1... .... .... .... = Response: Message is a response
      .000 0... .... .... = Opcode: Standard query (0)
      .... .0.. .... .... = Authoritative: Server is not an authority for domain
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... 1... .... = Recursion available: Server can do recursive queries
      .... .... .0.. .... = Z: reserved (0)
      .... .... ..0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server
      .... .... ...0 .... = Non-authenticated data: Unacceptable
      .... .... .... 0000 = Reply code: No error (0)
    Questions: 1
    Answer RRs: 0
    Authority RRs: 1
    Additional RRs: 0
```

I'm quite confused about the authoritative answer that I got in my cmd because I can't find answer in the packets that I caught as the answer RRS is zero.

```
▼ Queries
  ▼ mail.bupt.edu.cn: type MX, class IN
      Name: mail.bupt.edu.cn
      [Name Length: 16]
      [Label Count: 4]
      Type: MX (Mail eXchange) (15)
      Class: IN (0x0001)
▼ Authoritative nameservers
  ▼ bupt.edu.cn: type SOA, class IN, mname ns.buptnet.edu.cn
      Name: bupt.edu.cn
      Type: SOA (Start Of a zone of Authority) (6)
      Class: IN (0x0001)
      Time to live: 10800
      Data length: 41
      Primary name server: ns.buptnet.edu.cn
      Responsible authority's mailbox: admin.bupt.edu.cn
      Serial Number: 2016051102
      Refresh Interval: 10800 (3 hours)
      Retry Interval: 900 (15 minutes)
      Expire limit: 604800 (7 days)
      Minimum TTL: 86400 (1 day)
```

An authoritative name server provides actual answer to your DNS queries such as – mail server IP address. It provides original and definitive answers to DNS queries. It does not provide just cached answers that were obtained from another name server. Therefore, it only returns answers to queries about domain names that are installed in its configuration system. This is what we get from the cmd response.

```
serenadeMacBook-Pro:~ serenashi$ nslookup -type=MX mail.bupt.edu.cn
Server:         221.130.33.60
Address:        221.130.33.60#53

Non-authoritative answer:
*** Can't find mail.bupt.edu.cn: No answer

Authoritative answers can be found from:
bupt.edu.cn
        origin = ns.buptnet.edu.cn
        mail addr = admin.bupt.edu.cn
        serial = 2016051102
        refresh = 10800
        retry = 900
        expire = 604800
        minimum = 86400
```