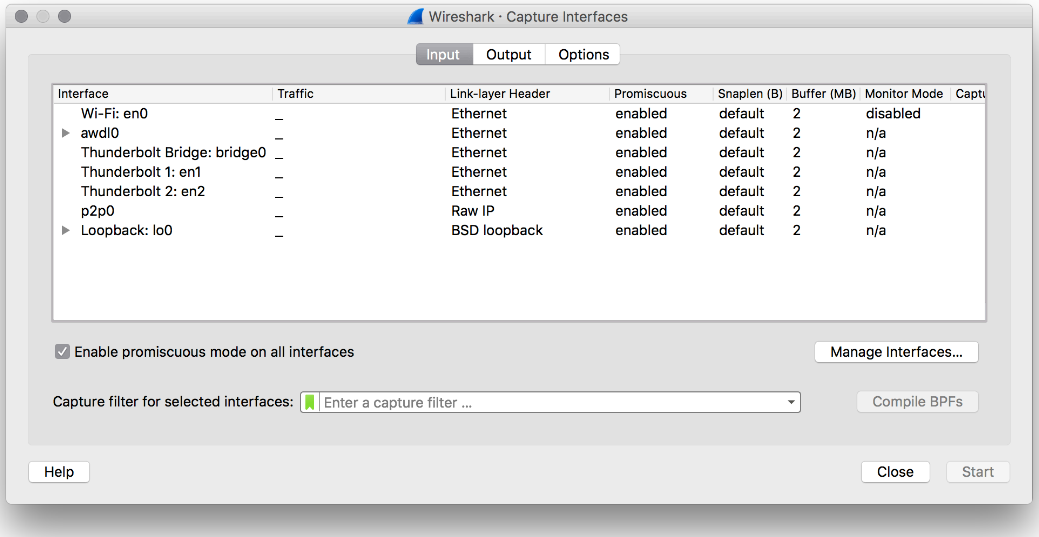
Using Wireshark to capture DHCP & DNS message

> **Author: Victoria Mengqi LIU 刘梦琪**
>
> **ClassID: 2013215105**
>
> **StudentID: 2013213062**

1. Configuration of Wireshark

Before we make the lab, there are several steps to take before starting the capture procedure. The system of my computer is window & old version of Wireshark. Firstly, install the Wireshark. Because I can't login the `https://www.wireshark.org/download.html` so I install another vision.In the menu, select **Capture-Interfaces**, selects the interface, then select **Options**.



Interface	Traffic	Link-layer Header	Promiscuous	Snaplen (B)	Buffer (MB)	Monitor Mode	Captu
Wi-Fi: en0	_	Ethernet	enabled	default	2	disabled	
▸ awdl0	_	Ethernet	enabled	default	2	n/a	
Thunderbolt Bridge: bridge0	_	Ethernet	enabled	default	2	n/a	
Thunderbolt 1: en1	_	Ethernet	enabled	default	2	n/a	
Thunderbolt 2: en2	_	Ethernet	enabled	default	2	n/a	
p2p0	_	Raw IP	enabled	default	2	n/a	
▸ Loopback: lo0	_	BSD loopback	enabled	default	2	n/a	

☑ Enable promiscuous mode on all interfaces

Capture filter for selected interfaces: Enter a capture filter ...

2. Procedure of capture

For DHCP

1. Select the **Option** for the capturing, input the Capture Filter condition "udp port 67", then press "Start".
2. Open CLI, input `ipconfig /release` to release the address.
3. Input `ipconfig /renew` in CLI.

For DNS

1. Select the **Options** for the capturing, input the Capture Filter condition `udp port 53` , then press **Start**
2. Input `nslookup -qt=A/MX bupt.edu.cn` in CLI

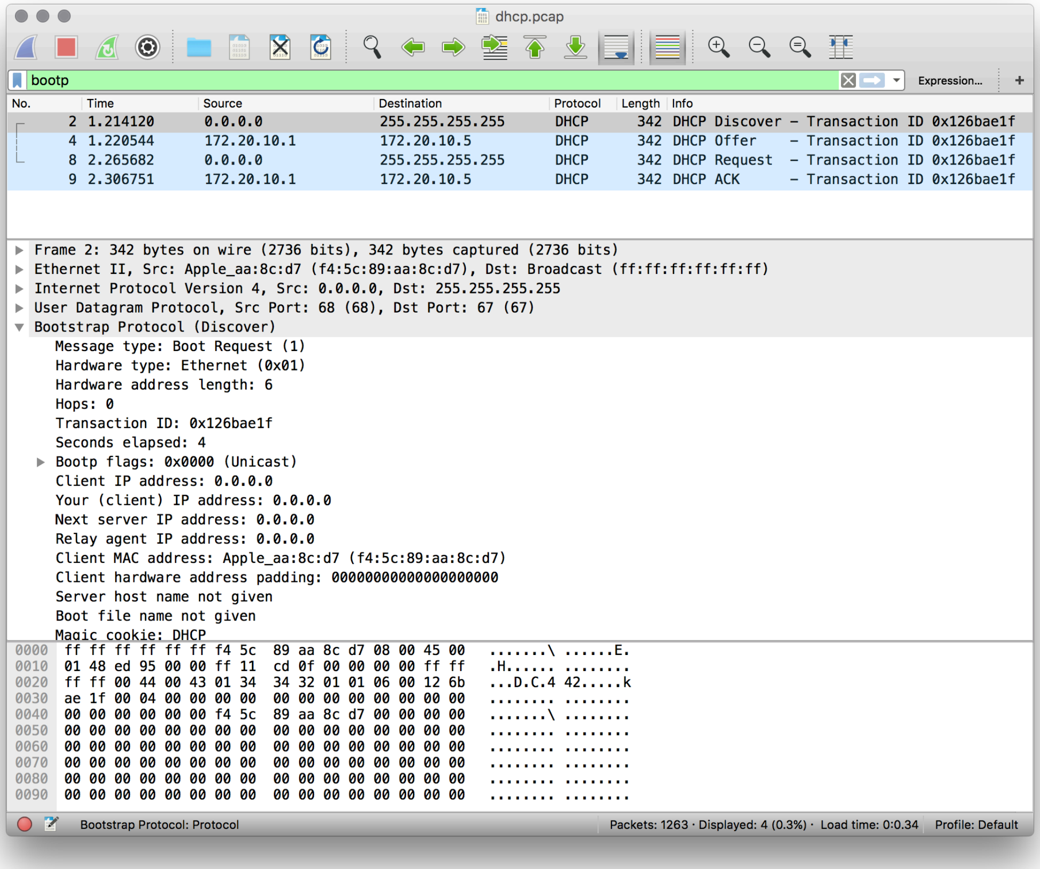
3. For DHCP Capture

List the value

Discover

After the client cancels the remaining lease of the IP address with DHCP server,it has no IP address.Then the IP address acquisition process begins. First DHCP client sends out the discover message to discover all DHCP servers in local area or other subnets(if relay agent is used).

By selecting the DHCP Discover message,the detailed information of the message is shown in the packet details pane.The following figure shows the detailed information:



bootp

```
No.   Time      Source       Destination      Protocol  Length  Info
    2 1.214120  0.0.0.0      255.255.255.255  DHCP      342  DHCP Discover  - Transaction ID 0x126bae1f
    4 1.220544  172.20.10.1  172.20.10.5      DHCP      342  DHCP Offer     - Transaction ID 0x126bae1f
    8 2.265682  0.0.0.0      255.255.255.255  DHCP      342  DHCP Request   - Transaction ID 0x126bae1f
    9 2.306751  172.20.10.1  172.20.10.5      DHCP      342  DHCP ACK       - Transaction ID 0x126bae1f
```

```
▶ Frame 2: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
▶ Ethernet II, Src: Apple_aa:8c:d7 (f4:5c:89:aa:8c:d7), 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)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x126bae1f
    Seconds elapsed: 4
  ▶ 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_aa:8c:d7 (f4:5c:89:aa:8c:d7)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
```

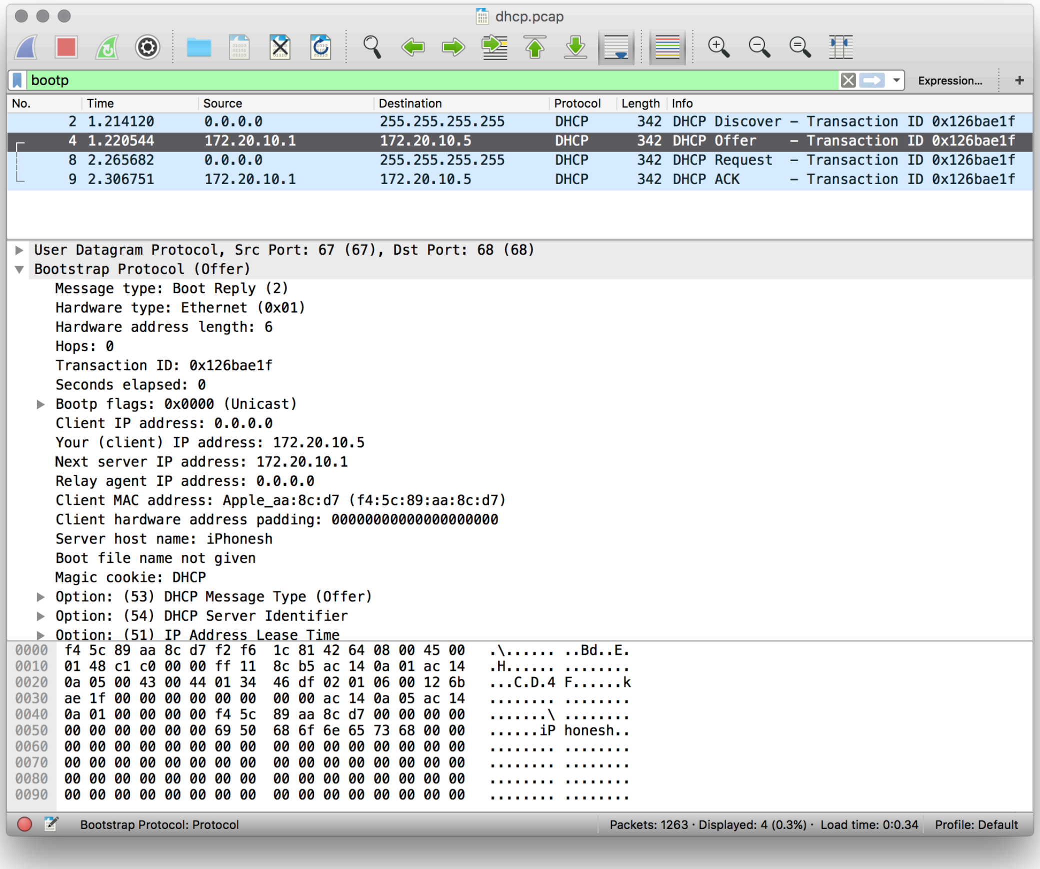
```
0000  ff ff ff ff ff ff f4 5c  89 aa 8c d7 08 00 45 00   .......\ ......E.
0010  01 48 ed 95 00 00 ff 11  cd 0f 00 00 00 00 ff ff   .H...... ........
0020  ff ff 00 44 00 43 01 34  34 32 01 01 06 00 12 6b   ...D.C.4 42.....k
0030  ae 1f 00 04 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0040  00 00 00 00 00 00 f4 5c  89 aa 8c d7 00 00 00 00   .......\ ........
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
```

Bootstrap Protocol: Protocol   Packets: 1263 · Displayed: 4 (0.3%) · Load time: 0:0.34   Profile: Default

```
Bootstrap Protocol (Discover)
Message type: Boot Request (1)
Transaction ID: 0x126bae1f
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
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
Frame address:
    Source: 0.0.0.0
    Destination: 255.255.255.255
```

Offer

After DHCP servers receive discover message from a client,they will send back an offer message to offer the client an available IP address from the address pool or simply offer the requested IP address in the discover message. The following 2 figures below show the detailed information in the heading of DHCP Offer Message:



```
No.  Time      Source       Destination      Protocol  Length  Info
  2  1.214120  0.0.0.0      255.255.255.255  DHCP      342     DHCP Discover - Transaction ID 0x126bae1f
  4  1.220544  172.20.10.1  172.20.10.5      DHCP      342     DHCP Offer    - Transaction ID 0x126bae1f
  8  2.265682  0.0.0.0      255.255.255.255  DHCP      342     DHCP Request  - Transaction ID 0x126bae1f
  9  2.306751  172.20.10.1  172.20.10.5      DHCP      342     DHCP ACK      - Transaction ID 0x126bae1f
```

```
▶ User Datagram Protocol, Src Port: 67 (67), Dst Port: 68 (68)
▼ Bootstrap Protocol (Offer)
     Message type: Boot Reply (2)
     Hardware type: Ethernet (0x01)
     Hardware address length: 6
     Hops: 0
     Transaction ID: 0x126bae1f
     Seconds elapsed: 0
   ▶ Bootp flags: 0x0000 (Unicast)
     Client IP address: 0.0.0.0
     Your (client) IP address: 172.20.10.5
     Next server IP address: 172.20.10.1
     Relay agent IP address: 0.0.0.0
     Client MAC address: Apple_aa:8c:d7 (f4:5c:89:aa:8c:d7)
     Client hardware address padding: 00000000000000000000
     Server host name: iPhonesh
     Boot file name not given
     Magic cookie: DHCP
   ▶ Option: (53) DHCP Message Type (Offer)
   ▶ Option: (54) DHCP Server Identifier
   ▶ Option: (51) IP Address Lease Time
```

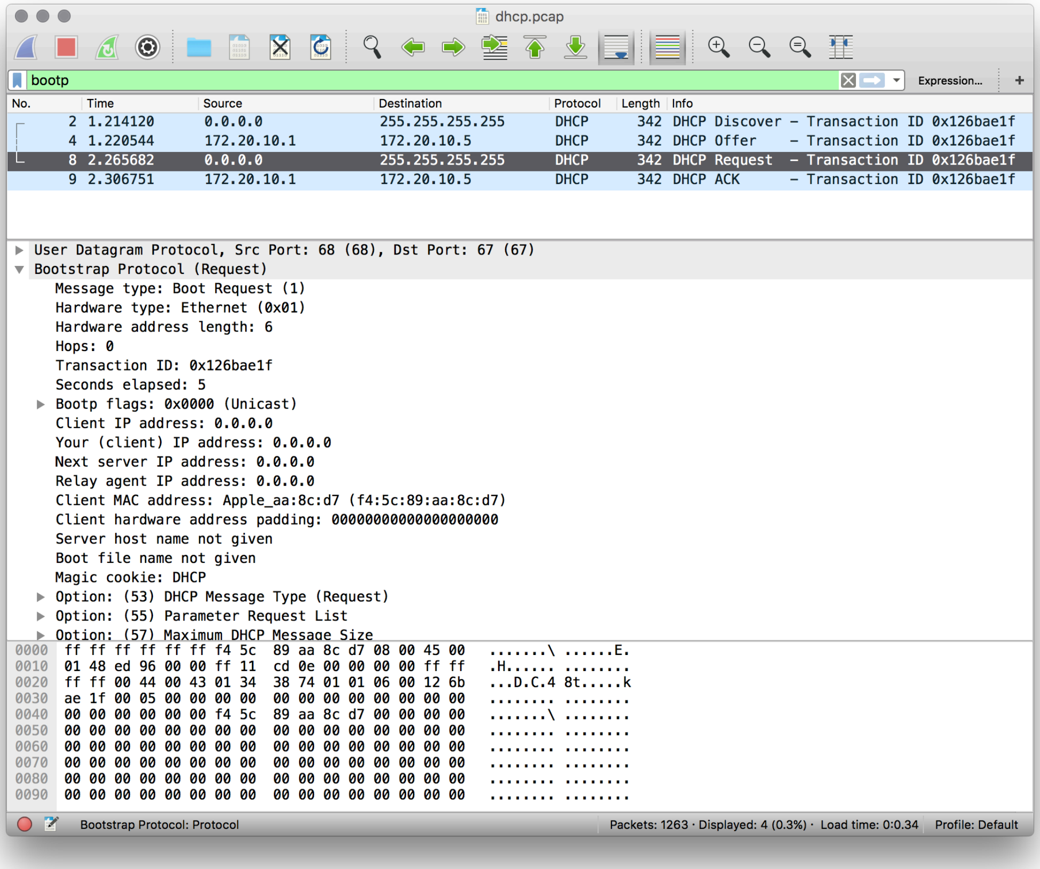
```
0000  f4 5c 89 aa 8c d7 f2 f6  1c 81 42 64 08 00 45 00   .\...... ..Bd..E.
0010  01 48 c1 c0 00 00 ff 11  8c b5 ac 14 0a 01 ac 14   .H...... ........
0020  0a 05 00 43 00 44 01 34  46 df 02 01 06 00 12 6b   ...C.D.4 F......k
0030  ae 1f 00 00 00 00 00 00  00 00 ac 14 0a 05 ac 14   ........ ........
0040  0a 01 00 00 00 00 f4 5c  89 aa 8c d7 00 00 00 00   .......\ ........
0050  00 00 00 00 00 00 69 50  68 6f 6e 65 73 68 00 00   ......iP honesh..
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
```

Bootstrap Protocol: Protocol   Packets: 1263 · Displayed: 4 (0.3%) · Load time: 0:0.34   Profile: Default

```
Bootstrap Protocol (Offer)
Message type: Boot Reply (2)
Transaction ID: 0x126bae1f
Client IP address: 0.0.0.0
Your (client) IP address: 172.20.10.5
Next server IP address: 172.20.10.1
Relay agent IP address: 0.0.0.0
Option: (53) DHCP Message Type (Offer)
Option: (54) DHCP Server Identifier
Option: (51) IP Address Lease Time
Option: (1) Subnet Mask
Option: (3) Router
Option: (6) Domain Name Server
Option: (255) End
Frame address:
    Source: 172.20.10.1
    Destination: 172.20.10.5
```

Request

After the client receives offers from different DHCP servers,it selects one offer by sending request message to the selected server and at the same time to decline other servers' offers.In this lab,since only one server gives offer to the client,there's no selection process.



bootp

```
No.  Time      Source       Destination      Protocol Length Info
   2 1.214120  0.0.0.0      255.255.255.255  DHCP     342 DHCP Discover - Transaction ID 0x126bae1f
   4 1.220544  172.20.10.1  172.20.10.5      DHCP     342 DHCP Offer    - Transaction ID 0x126bae1f
   8 2.265682  0.0.0.0      255.255.255.255  DHCP     342 DHCP Request  - Transaction ID 0x126bae1f
   9 2.306751  172.20.10.1  172.20.10.5      DHCP     342 DHCP ACK      - Transaction ID 0x126bae1f
```

```
▶ User Datagram Protocol, Src Port: 68 (68), Dst Port: 67 (67)
▼ Bootstrap Protocol (Request)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x126bae1f
    Seconds elapsed: 5
  ▶ 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_aa:8c:d7 (f4:5c:89:aa:8c:d7)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  ▶ Option: (53) DHCP Message Type (Request)
  ▶ Option: (55) Parameter Request List
  ▶ Option: (57) Maximum DHCP Message Size
```

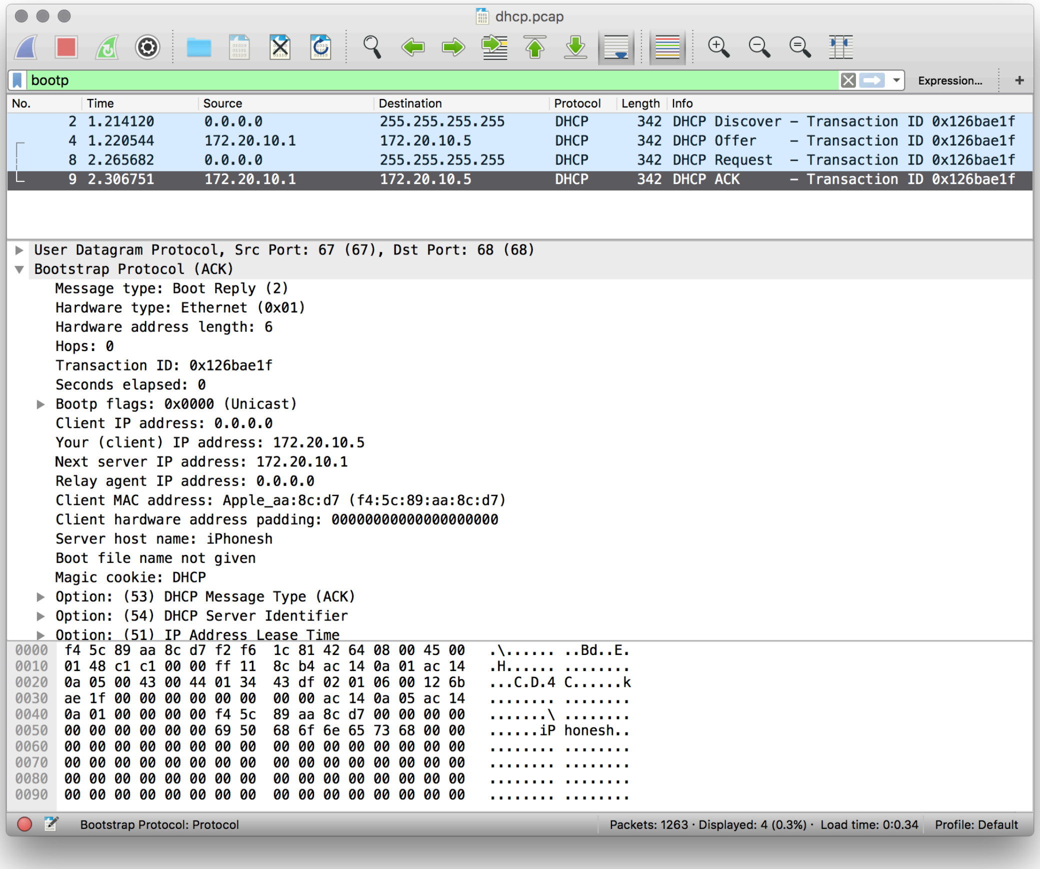
```
0000  ff ff ff ff ff ff f4 5c  89 aa 8c d7 08 00 45 00   .......\ ......E.
0010  01 48 ed 96 00 00 ff 11  cd 0e 00 00 00 00 ff ff   .H...... ........
0020  ff ff 00 44 00 43 01 34  38 74 01 01 06 00 12 6b   ...D.C.4 8t.....k
0030  ae 1f 00 05 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0040  00 00 00 00 00 00 f4 5c  89 aa 8c d7 00 00 00 00   .......\ ........
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
```

Bootstrap Protocol: Protocol   Packets: 1263 · Displayed: 4 (0.3%) · Load time: 0:0.34   Profile: Default

```
Bootstrap Protocol (Request)
Message type: Boot Request (1)
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
Option: (53) DHCP Message Type (Request)
Option: (55) Parameter Request List
Option: (57) Maximum DHCP Message Size
Option: (61) Client identifier
Option: (50) Requested IP Address
Option: (54) DHCP Server Identifier
Option: (12) Host Name
Option: (255) End
Frame address:
    Source: 0.0.0.0
    Destination: 255.255.255.255
```

ACK

After the selected server receives the request message from the client,it sends out an **ACK** message to acknowledge that the offered IP address is assigned to the client.



```
No.   Time       Source       Destination      Protocol  Length  Info
   2  1.214120   0.0.0.0      255.255.255.255  DHCP      342     DHCP Discover - Transaction ID 0x126bae1f
   4  1.220544   172.20.10.1  172.20.10.5      DHCP      342     DHCP Offer    - Transaction ID 0x126bae1f
   8  2.265682   0.0.0.0      255.255.255.255  DHCP      342     DHCP Request  - Transaction ID 0x126bae1f
   9  2.306751   172.20.10.1  172.20.10.5      DHCP      342     DHCP ACK      - Transaction ID 0x126bae1f
```

```
▶ User Datagram Protocol, Src Port: 67 (67), Dst Port: 68 (68)
▼ Bootstrap Protocol (ACK)
     Message type: Boot Reply (2)
     Hardware type: Ethernet (0x01)
     Hardware address length: 6
     Hops: 0
     Transaction ID: 0x126bae1f
     Seconds elapsed: 0
   ▶ Bootp flags: 0x0000 (Unicast)
     Client IP address: 0.0.0.0
     Your (client) IP address: 172.20.10.5
     Next server IP address: 172.20.10.1
     Relay agent IP address: 0.0.0.0
     Client MAC address: Apple_aa:8c:d7 (f4:5c:89:aa:8c:d7)
     Client hardware address padding: 00000000000000000000
     Server host name: iPhonesh
     Boot file name not given
     Magic cookie: DHCP
   ▶ Option: (53) DHCP Message Type (ACK)
   ▶ Option: (54) DHCP Server Identifier
   ▶ Option: (51) IP Address Lease Time
```

```
0000  f4 5c 89 aa 8c d7 f2 f6  1c 81 42 64 08 00 45 00   .\...... ..Bd..E.
0010  01 48 c1 c1 00 00 ff 11  8c b4 ac 14 0a 01 ac 14   .H...... ........
0020  0a 05 00 43 00 44 01 34  43 df 02 01 06 00 12 6b   ...C.D.4 C......k
0030  ae 1f 00 00 00 00 00 00  00 00 ac 14 0a 05 ac 14   ........ ........
0040  0a 01 00 00 00 00 f4 5c  89 aa 8c d7 00 00 00 00   .......\ ........
0050  00 00 00 00 00 00 69 50  68 6f 6e 65 73 68 00 00   ......iP honesh..
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
```

Bootstrap Protocol: Protocol
Packets: 1263 · Displayed: 4 (0.3%) · Load time: 0:0.34
Profile: Default

```
Bootstrap Protocol (ACK)
Message type: Boot Reply (2)
Transaction ID: 0x126bae1f
Client IP address: 0.0.0.0
Your (client) IP address: 172.20.10.5
Next server IP address: 172.20.10.1
Relay agent IP address: 0.0.0.0
Option: (53) DHCP Message Type (ACK)
Option: (54) DHCP Server Identifier
Option: (51) IP Address Lease Time
Option: (1) Subnet Mask
Option: (3) Router
Option: (6) Domain Name Server
Option: (255) End
Frame address:
    Source: 172.20.10.1
    Destination: 172.20.10.5
```

Explain for the Parameters

We can find that the message type may be different because thesetwo values have different meanings, which type ‘1’ means boot request from c to server and ‘2’ means boot reply from server to client.

Next, we may find that IP address which the client has may be changed. Thismeans that when laptop sends DHCP REQUEST source destination in the packet header, which here all 0s means communicate from client to the serverneed not to through the router.

```
Option:(1) Subnet Mask
Option:(3) Router
Option:(6) Domain Name Server
Option:(12) Host name
Option:(50) Request IP address
Option:(51) IP address lease time
Option:(53) DCHP Message Type
Option:(54) DCHP Server Identifier
Option:(55) Parameter Request List
```

Frame Addres: i.e. MAC address

Compared with the example

Tabel 1: DHCP-discover comparison

parameter	example	Capture
Transaction ID	12	0x126bae1f
Your IP Address	12	0.0.0.0
Destination IP	255.255.255.255	255.255.255.255

Tabel 2: DHCP-offer comparison

parameter	example	Capture
Transaction ID	12	0x126bae1f
Your IP Address	192.168.10.98	172.20.10.1
Destination IP	255.255.255.255	172.20.10.5

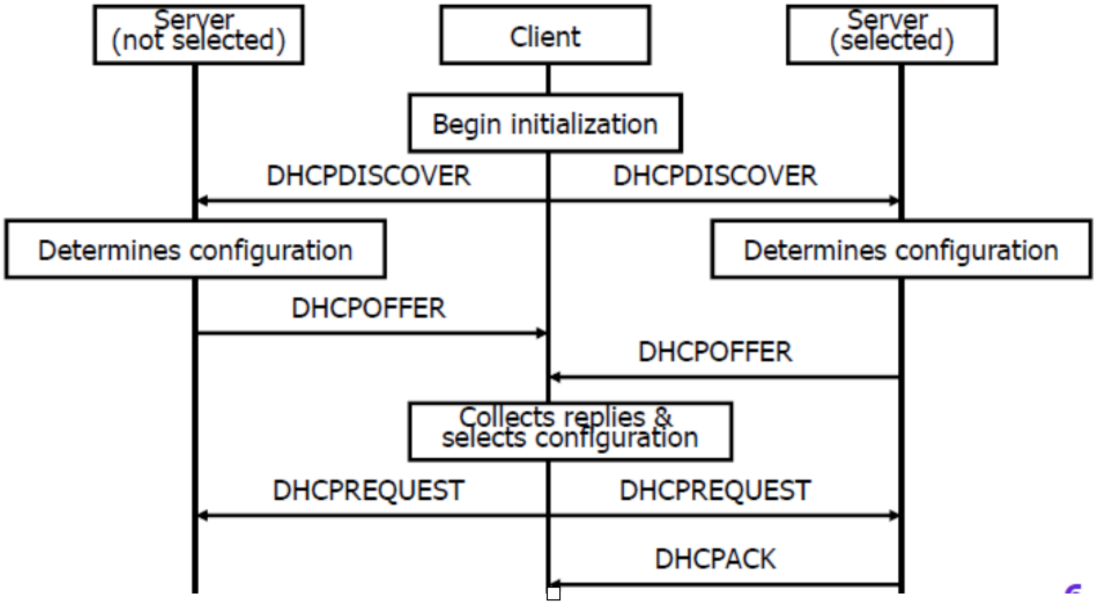
Table 3: DHCP-request comparson

parameter	example	Capture
Transaction ID	12	0x126bae1f
Your IP Address	192.168.10.97	0.0.0.0

Table 4: DHCP-ACK comparison

parameter	example	Capture
Transaction ID	12	0x126bae1f
Your IP Address	192.168.10.98	172.20.10.5

MSC

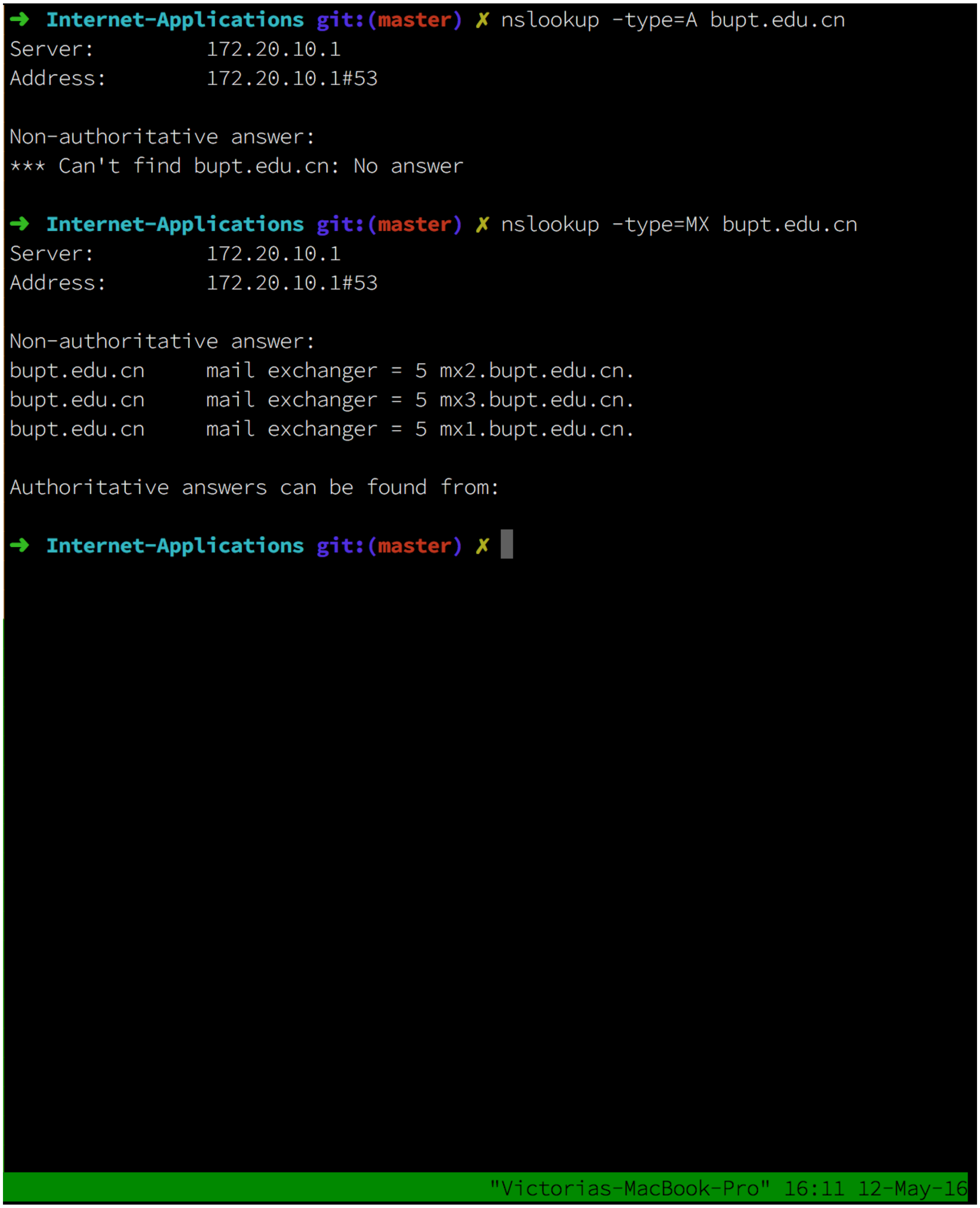


4. For DNS Capture

Including DNS QUERY and DNS Query RESPONSE. Analyze the captured packets in*field-level* and explain the meaning and result of each field value. Capture your screen and show the result.

List the command with shell, enter the `nslookup –qt=A bupt.edu.cn`

This command is used to query the system



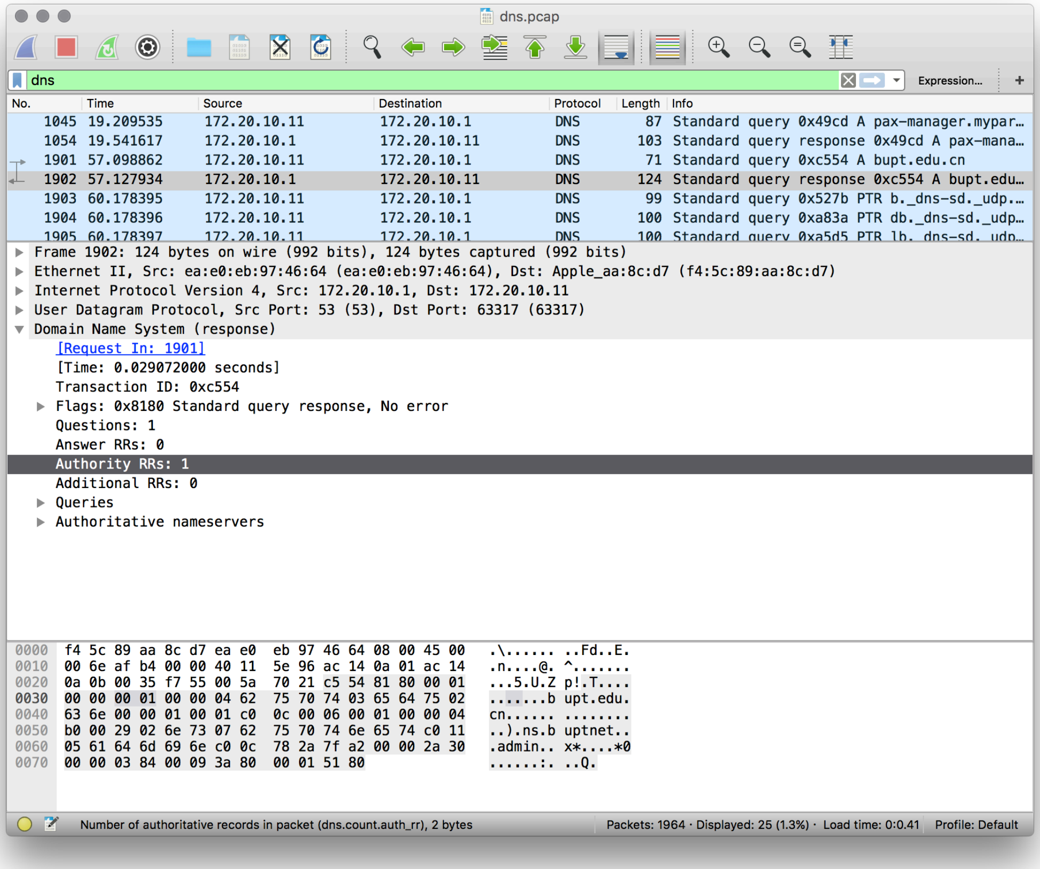
```
➜  Internet-Applications git:(master) ✗ nslookup -type=A bupt.edu.cn
Server:         172.20.10.1
Address:        172.20.10.1#53

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

➜  Internet-Applications git:(master) ✗ nslookup -type=MX bupt.edu.cn
Server:         172.20.10.1
Address:        172.20.10.1#53

Non-authoritative answer:
bupt.edu.cn     mail exchanger = 5 mx2.bupt.edu.cn.
bupt.edu.cn     mail exchanger = 5 mx3.bupt.edu.cn.
bupt.edu.cn     mail exchanger = 5 mx1.bupt.edu.cn.

Authoritative answers can be found from:

➜  Internet-Applications git:(master) ✗ 
```

```
                                       "Victorias-MacBook-Pro" 16:11 12-May-16
```

List the command with shell, enter the `nslookup –qt=MX bupt.edu.cn`

DNS Standard Query Packet (`nslookup type=A`)

By selecting the DNS Standard Query message,detailed information of this packet’s is shown in the figure below:



dns.pcap

dns

```
No.     Time        Source         Destination    Protocol  Length  Info
   1045 19.209535   172.20.10.11   172.20.10.1    DNS          87  Standard query 0x49cd A pax-manager.mypar…
   1054 19.541617   172.20.10.1    172.20.10.11   DNS         103  Standard query response 0x49cd A pax-mana…
   1901 57.098862   172.20.10.11   172.20.10.1    DNS          71  Standard query 0xc554 A bupt.edu.cn
   1902 57.127934   172.20.10.1    172.20.10.11   DNS         124  Standard query response 0xc554 A bupt.edu…
   1903 60.178395   172.20.10.11   172.20.10.1    DNS          99  Standard query 0x527b PTR b._dns-sd._udp.…
   1904 60.178396   172.20.10.11   172.20.10.1    DNS         100  Standard query 0xa83a PTR db._dns-sd._udp…
   1905 60.178397   172.20.10.11   172.20.10.1    DNS         100  Standard query 0xa5d5 PTR lb._dns-sd._udp…
```

```
▶ Frame 1902: 124 bytes on wire (992 bits), 124 bytes captured (992 bits)
▶ Ethernet II, Src: ea:e0:eb:97:46:64 (ea:e0:eb:97:46:64), Dst: Apple_aa:8c:d7 (f4:5c:89:aa:8c:d7)
▶ Internet Protocol Version 4, Src: 172.20.10.1, Dst: 172.20.10.11
▶ User Datagram Protocol, Src Port: 53 (53), Dst Port: 63317 (63317)
▼ Domain Name System (response)
    [Request In: 1901]
    [Time: 0.029072000 seconds]
    Transaction ID: 0xc554
  ▶ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 0
    Authority RRs: 1
    Additional RRs: 0
  ▶ Queries
  ▶ Authoritative nameservers
```

```
0000  f4 5c 89 aa 8c d7 ea e0  eb 97 46 64 08 00 45 00   .\...... ..Fd..E.
0010  00 6e af b4 00 00 40 11  5e 96 ac 14 0a 01 ac 14   .n....@. ^.......
0020  0a 0b 00 35 f7 55 00 5a  70 21 c5 54 81 80 00 01   ...5.U.Z p!.T....
0030  00 00 00 01 00 00 04 62  75 70 74 03 65 64 75 02   .......b upt.edu.
0040  63 6e 00 00 01 00 01 c0  0c 00 06 00 01 00 00 04   cn...... ........
0050  b0 00 29 02 6e 73 07 62  75 70 74 6e 65 74 c0 11   ..).ns.b uptnet..
0060  05 61 64 6d 69 6e c0 0c  78 2a 7f a2 00 00 2a 30   .admin.. x*....*0
0070  00 00 03 84 00 09 3a 80  00 01 51 80               ......:. ..Q.
```

Number of authoritative records in packet (dns.count.auth_rr), 2 bytes

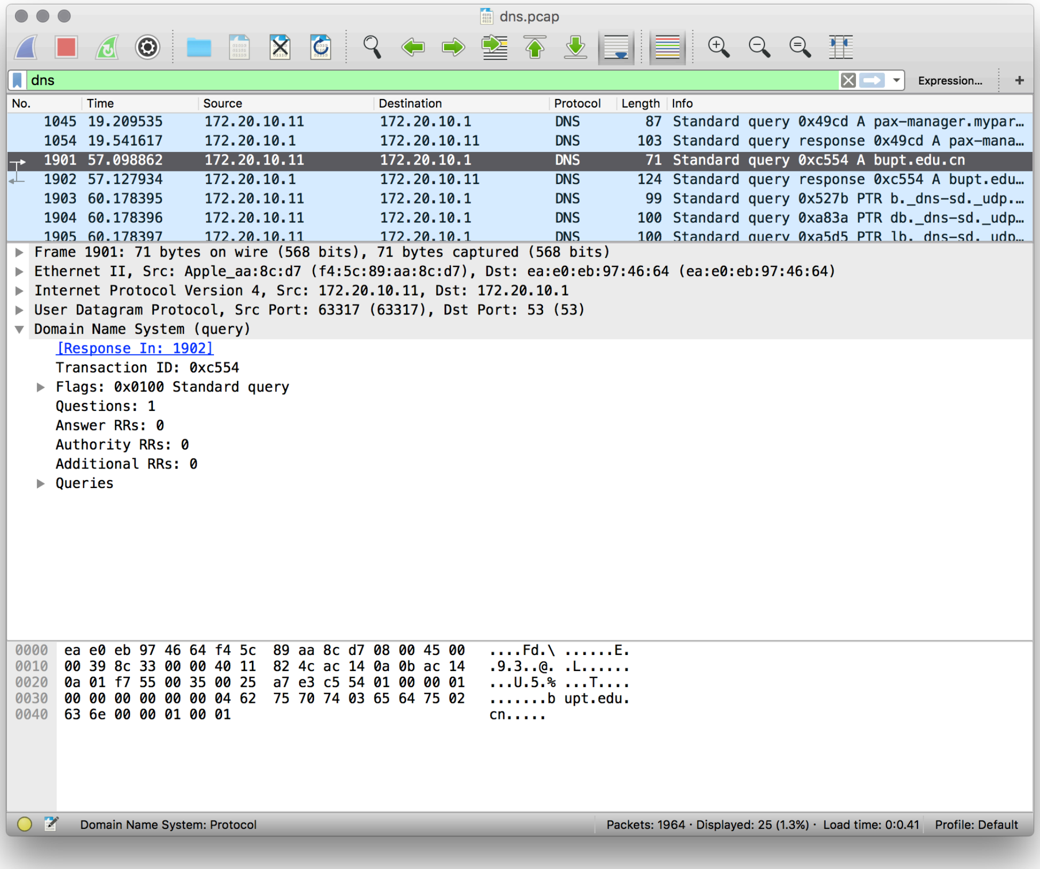
Packets: 1964 · Displayed: 25 (1.3%) · Load time: 0:0.41 Profile: Default

Detailed information in DNS Query Packet (`nslookup type=A`)

> The form below lists the values of fields and corresponding explanations:
>
> Transaction ID=0x16fc This field is used to match queries and corresponding responses.Here,the transaction ID of this DNS query packet is 0x16fc. The response packet to this query should have the same transaction ID.
>
> Queries Name= `bupt.edu.cn` The first field of the question section.
>
> `Opcode=0000` A field used to specify the domain name which is used to do the query. Here, “0000” indicates thatthis query is a standardquery which is used to map adomain name to its IP address. A 4-bit field which describes the type of a query. Here, “0000” indicates thatthis query is a standardquery which is used to map adomain name to its IP address.

DNS Standard Response Packet (`nslookup type=A`)

By selecting the DNS Standard Query message,detailed information of this packet’s is shown in the figure below:



```
No.     Time        Source          Destination     Protocol  Length  Info
   1045 19.209535   172.20.10.11    172.20.10.1     DNS           87  Standard query 0x49cd A pax-manager.mypar…
   1054 19.541617   172.20.10.1     172.20.10.11    DNS          103  Standard query response 0x49cd A pax-mana…
   1901 57.098862   172.20.10.11    172.20.10.1     DNS           71  Standard query 0xc554 A bupt.edu.cn
   1902 57.127934   172.20.10.1     172.20.10.11    DNS          124  Standard query response 0xc554 A bupt.edu…
   1903 60.178395   172.20.10.11    172.20.10.1     DNS           99  Standard query 0x527b PTR b._dns-sd._udp.…
   1904 60.178396   172.20.10.11    172.20.10.1     DNS          100  Standard query 0xa83a PTR db._dns-sd._udp…
   1905 60.178397   172.20.10.11    172.20.10.1     DNS          100  Standard query 0xa5d5 PTR lb._dns-sd._udp…
```

```
▶ Frame 1901: 71 bytes on wire (568 bits), 71 bytes captured (568 bits)
▶ Ethernet II, Src: Apple_aa:8c:d7 (f4:5c:89:aa:8c:d7), Dst: ea:e0:eb:97:46:64 (ea:e0:eb:97:46:64)
▶ Internet Protocol Version 4, Src: 172.20.10.11, Dst: 172.20.10.1
▶ User Datagram Protocol, Src Port: 63317 (63317), Dst Port: 53 (53)
▼ Domain Name System (query)
    [Response In: 1902]
    Transaction ID: 0xc554
  ▶ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▶ Queries
```

```
0000  ea e0 eb 97 46 64 f4 5c  89 aa 8c d7 08 00 45 00   ....Fd.\ ......E.
0010  00 39 8c 33 00 00 40 11  82 4c ac 14 0a 0b ac 14   .9.3..@. .L......
0020  0a 01 f7 55 00 35 00 25  a7 e3 c5 54 01 00 00 01   ...U.5.% ...T....
0030  00 00 00 00 00 00 04 62  75 70 74 03 65 64 75 02   .......b upt.edu.
0040  63 6e 00 00 01 00 01                               cn.....
```

Domain Name System: Protocol   Packets: 1964 · Displayed: 25 (1.3%) · Load time: 0:0.41   Profile: Default

Detailed information in DNS Response Packet (nslookup type=A)

lists the values of fields and corresponding explanations:

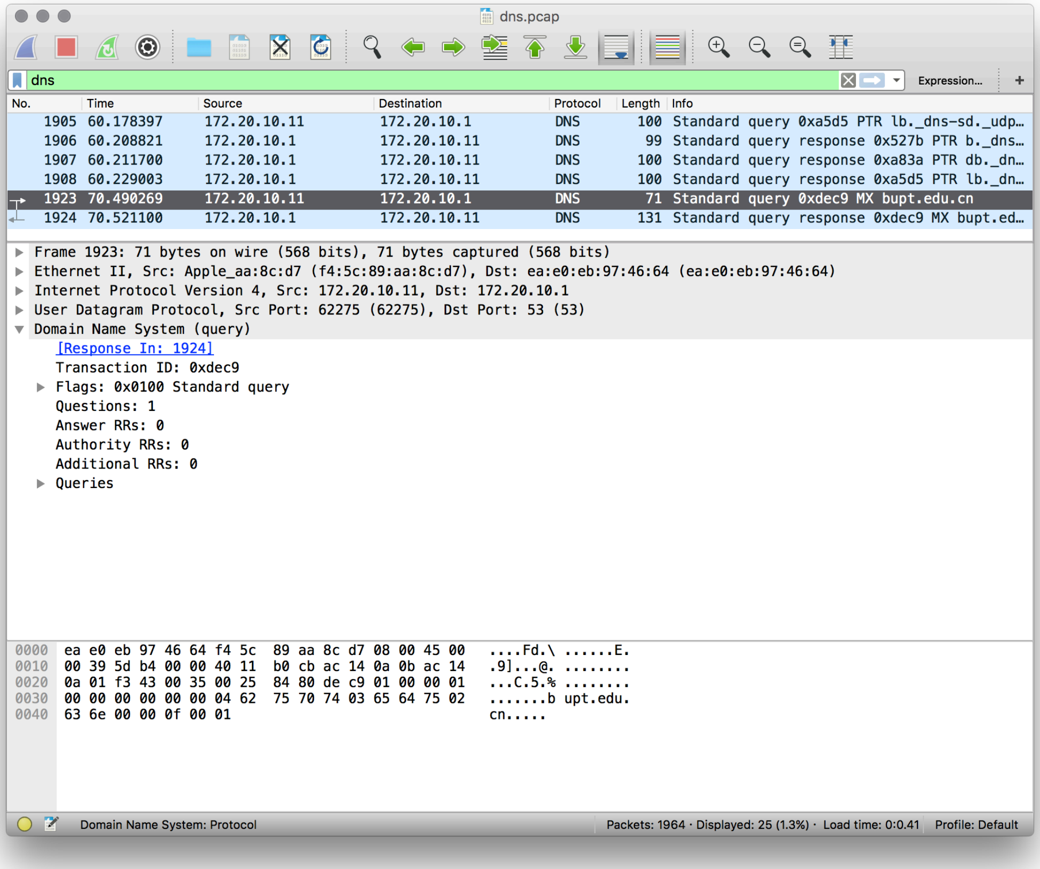
`Transaction ID=0x16fc` This field is used to match queries and corresponding responses. Here,the transaction ID of this DNS response packet is 0x16fc. The response packet to this query should have the same transaction ID with query packet.

`Query type=A` The second field of the question section.A 16-bit field is used tospecify the type of the query. Asking for a resource record with a particular type Here, “A” indicates this query asks for the host IP address for the given domain name.

`Resource Record 1 (Primary name server)= ns.buptnet.edu.cn` This field defines the Primary name server in the resource data in bytes. In this resource record, the record shows that primary name server is `ns.buptnet.edu.cn`

DNS Standard Query Packet (`nslookup type=MX`)

By selecting the DNS Standard Query message,detailed information of this packet’s is shown in the figure below:



dns.pcap

dns

```
No.    Time       Source        Destination   Protocol Length Info
  1905 60.178397  172.20.10.11  172.20.10.1   DNS        100 Standard query 0xa5d5 PTR lb._dns-sd._udp…
  1906 60.208821  172.20.10.1   172.20.10.11  DNS         99 Standard query response 0x527b PTR b._dns…
  1907 60.211700  172.20.10.1   172.20.10.11  DNS        100 Standard query response 0xa83a PTR db._dn…
  1908 60.229003  172.20.10.1   172.20.10.11  DNS        100 Standard query response 0xa5d5 PTR lb._dn…
  1923 70.490269  172.20.10.11  172.20.10.1   DNS         71 Standard query 0xdec9 MX bupt.edu.cn
  1924 70.521100  172.20.10.1   172.20.10.11  DNS        131 Standard query response 0xdec9 MX bupt.ed…
```

```
▶ Frame 1923: 71 bytes on wire (568 bits), 71 bytes captured (568 bits)
▶ Ethernet II, Src: Apple_aa:8c:d7 (f4:5c:89:aa:8c:d7), Dst: ea:e0:eb:97:46:64 (ea:e0:eb:97:46:64)
▶ Internet Protocol Version 4, Src: 172.20.10.11, Dst: 172.20.10.1
▶ User Datagram Protocol, Src Port: 62275 (62275), Dst Port: 53 (53)
▼ Domain Name System (query)
    [Response In: 1924]
    Transaction ID: 0xdec9
  ▶ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▶ Queries
```

```
0000  ea e0 eb 97 46 64 f4 5c  89 aa 8c d7 08 00 45 00   ....Fd.\ ......E.
0010  00 39 5d b4 00 00 40 11  b0 cb ac 14 0a 0b ac 14   .9]...@. ........
0020  0a 01 f3 43 00 35 00 25  84 80 de c9 01 00 00 01   ...C.5.% ........
0030  00 00 00 00 00 00 04 62  75 70 74 03 65 64 75 02   .......b upt.edu.
0040  63 6e 00 00 0f 00 01                               cn.....
```

Domain Name System: Protocol   Packets: 1964 · Displayed: 25 (1.3%) · Load time: 0:0.41   Profile: Default

Detailed information in DNS Query Packet (`nslookup type=MX`)

Lists the values of fields and corresponding explanations:

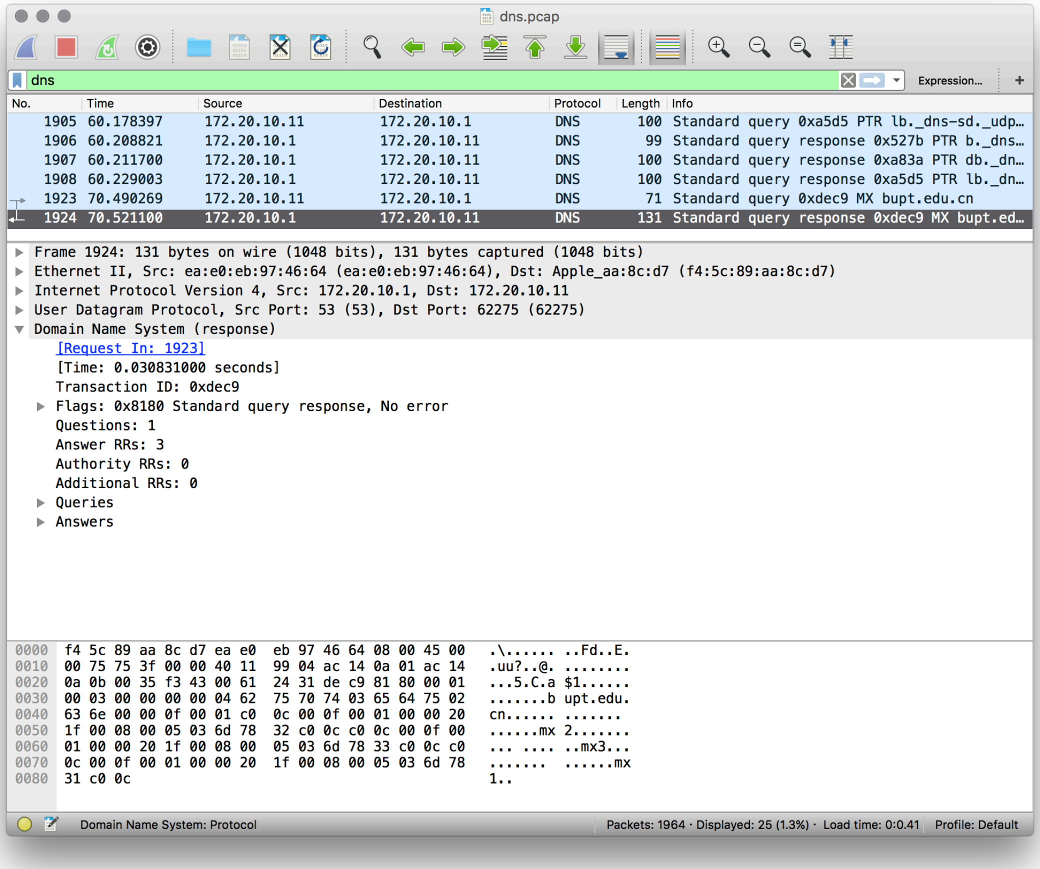
`Transaction ID=0xc1f9` This field is used to match queries and corresponding responses. Here,the transaction ID of this DNS query packet is 0xc1f9. The response packet to this query should have the same transaction ID.

`Queries Name= bupt.edu.cn` The first field of the question section.

A field used to specify the domain name which is used to do the query.

DNS Standard Response Packet (`nslookup type=MX)

By selecting the DNS Standard Query message,detailed information of this packet’s is shown in the figure below:



```
No.    Time        Source        Destination   Protocol  Length  Info
  1905 60.178397   172.20.10.11  172.20.10.1   DNS         100   Standard query 0xa5d5 PTR lb._dns-sd._udp…
  1906 60.208821   172.20.10.1   172.20.10.11  DNS          99   Standard query response 0x527b PTR b._dns…
  1907 60.211700   172.20.10.1   172.20.10.11  DNS         100   Standard query response 0xa83a PTR db._dn…
  1908 60.229003   172.20.10.1   172.20.10.11  DNS         100   Standard query response 0xa5d5 PTR lb._dn…
  1923 70.490269   172.20.10.11  172.20.10.1   DNS          71   Standard query 0xdec9 MX bupt.edu.cn
  1924 70.521100   172.20.10.1   172.20.10.11  DNS         131   Standard query response 0xdec9 MX bupt.ed…
```

```
▶ Frame 1924: 131 bytes on wire (1048 bits), 131 bytes captured (1048 bits)
▶ Ethernet II, Src: ea:e0:eb:97:46:64 (ea:e0:eb:97:46:64), Dst: Apple_aa:8c:d7 (f4:5c:89:aa:8c:d7)
▶ Internet Protocol Version 4, Src: 172.20.10.1, Dst: 172.20.10.11
▶ User Datagram Protocol, Src Port: 53 (53), Dst Port: 62275 (62275)
▼ Domain Name System (response)
    [Request In: 1923]
    [Time: 0.030831000 seconds]
    Transaction ID: 0xdec9
  ▶ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 0
  ▶ Queries
  ▶ Answers
```

```
0000  f4 5c 89 aa 8c d7 ea e0  eb 97 46 64 08 00 45 00   .\...... ..Fd..E.
0010  00 75 75 3f 00 00 40 11  99 04 ac 14 0a 01 ac 14   .uu?..@. ........
0020  0a 0b 00 35 f3 43 00 61  24 31 de c9 81 80 00 01   ...5.C.a $1......
0030  00 03 00 00 00 00 04 62  75 70 74 03 65 64 75 02   .......b upt.edu.
0040  63 6e 00 00 0f 00 01 c0  0c 00 0f 00 01 00 00 20   cn...... .......
0050  1f 00 08 00 05 03 6d 78  32 c0 0c c0 0c 00 0f 00   ......mx 2.......
0060  01 00 00 20 1f 00 08 00  05 03 6d 78 33 c0 0c c0   ... .... ..mx3...
0070  0c 00 0f 00 01 00 00 20  1f 00 08 00 05 03 6d 78   .......  ......mx
0080  31 c0 0c                                           1..
```

```
Domain Name System: Protocol          Packets: 1964 · Displayed: 25 (1.3%) · Load time: 0:0.41    Profile: Default
```

Detailed infomation in DNS Response Packet (`nklookup type=MX`)

lists the values of fields and corresponding explanations:

`Transaction ID=0xc1f9` This field is used to match queries and corresponding responses. Here,the transaction ID of this DNS response packet is 0xc1f9. The response packet to this query should have the same transaction ID with query packet.

`Query type=MX` The second field of the question section.MX 16-bit field is used to specify the type of the query. Asking for a resource record with a particular type Here, “MX” indicates this query asks for the host IP address for the give server of the email server.

`Resource Record 1 Mail exchange)= mx1.bupt.edu.cn`

This field defines the Mail exchange. In this resource record, the record shows that mx1.bupt.edu.cn is mail exchange

Comparisons of DNS Examples in Lecture notes.

lecture notes,the “Z” field in the DNS message should be a 3-bit field which is reserved for future use and must be set to 0.However,in the caputred packet,only the first bit is identified as “Z” field.The remaining two bits are used to indicate the answer’s authentication and data’s authentication.