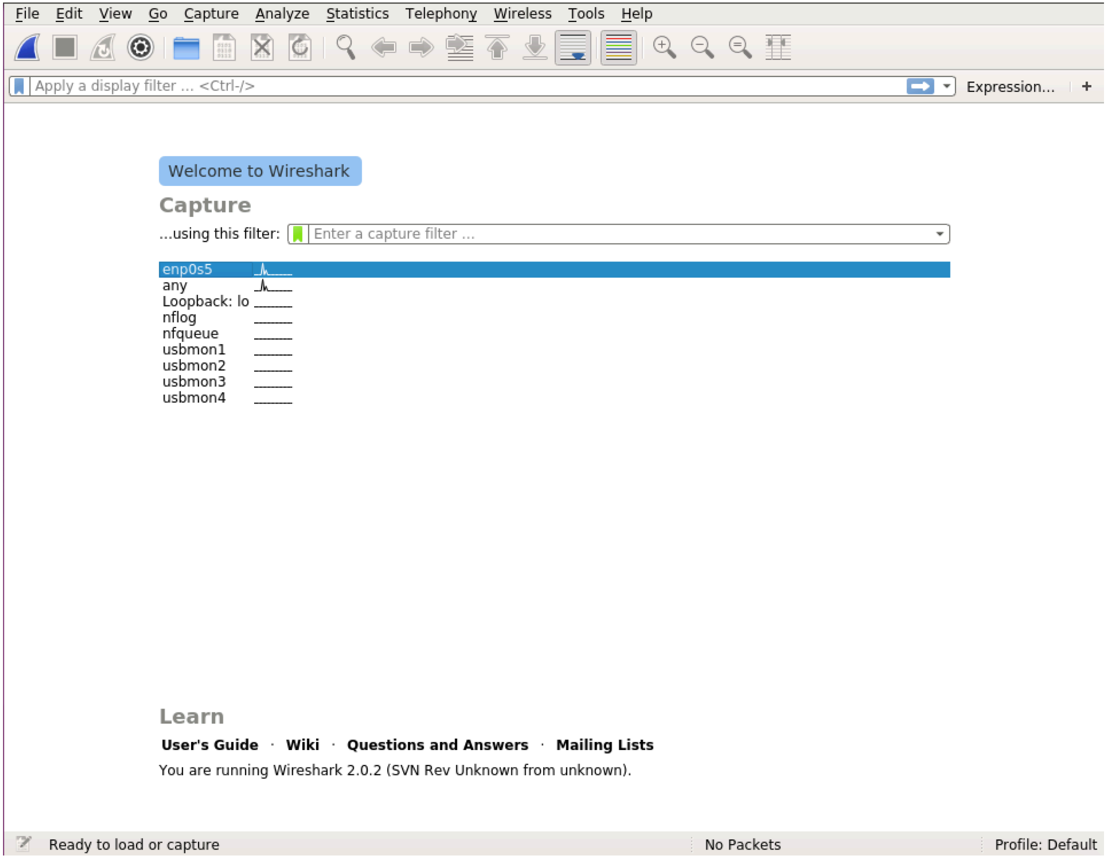
Capture DHCP&DNS Packets and Analysis

Name: Ou Yihang
Class: 2014215104
BUPT Student ID: 2014212948
QM Student ID: 140919433

1. The configuration of Wireshark

1.1 Using the command "scp –X student@192.168.56.101" to connect the physical machine and virtual machine.

1.2 Using the command "sudo wireshark" then input the password to start the wireshark, then this will be show in the screen.



Welcome to Wireshark

Capture

...using this filter: Enter a capture filter …

enp0s5
any
Loopback: lo
nflog
nfqueue
usbmon1
usbmon2
usbmon3
usbmon4

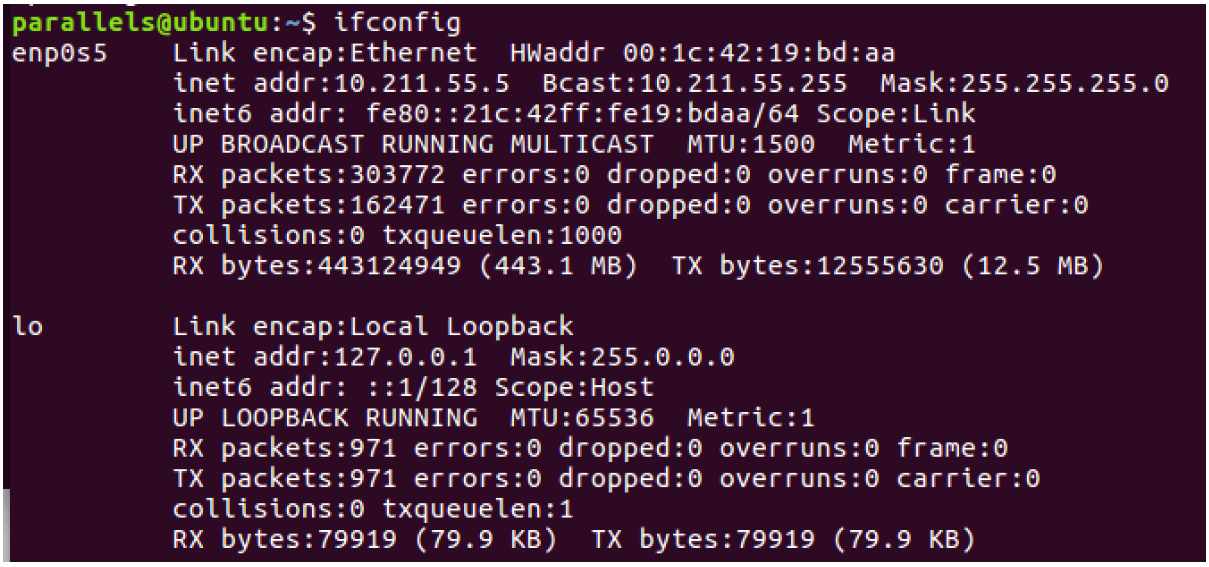
Learn

User's Guide · Wiki · Questions and Answers · Mailing Lists

You are running Wireshark 2.0.2 (SVN Rev Unknown from unknown).

Ready to load or capture | No Packets | Profile: Default

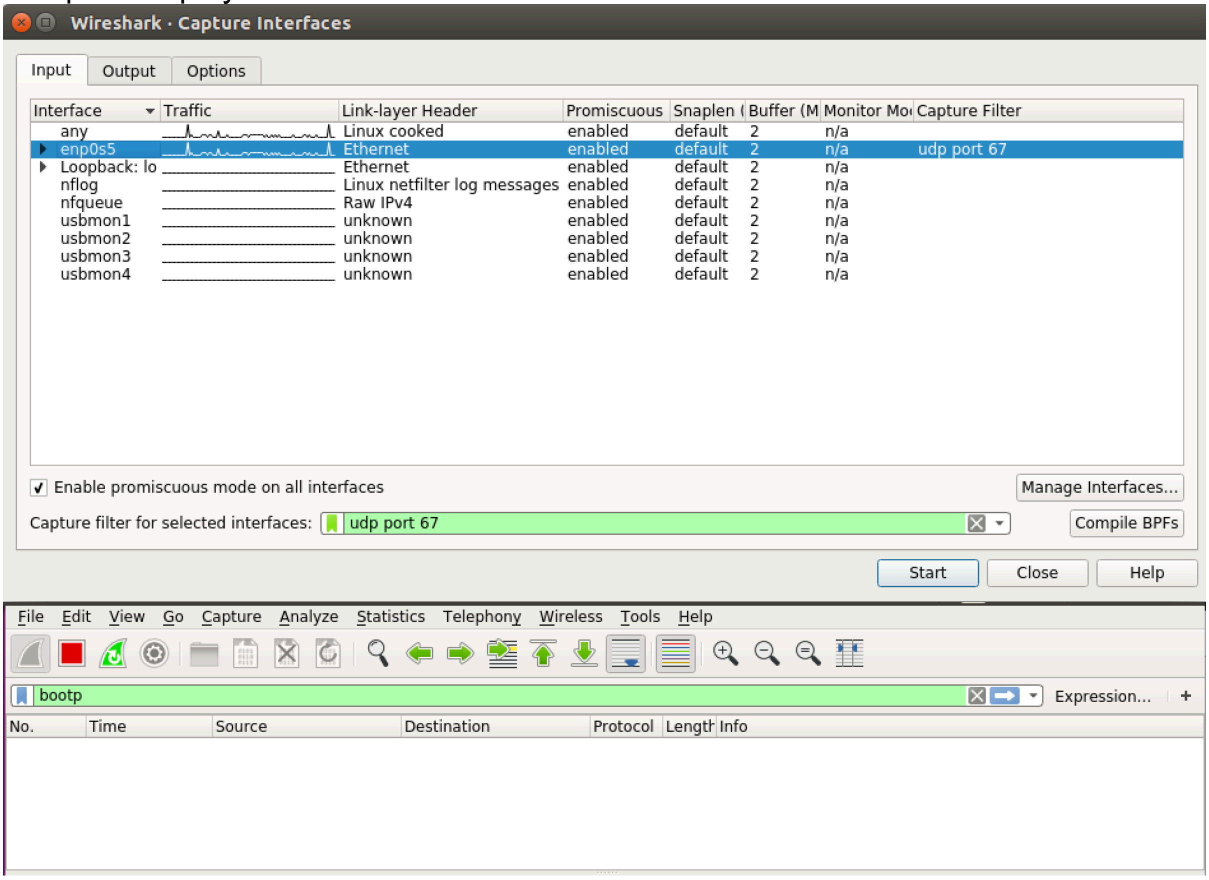
from this picture, there are 2 network is available.
Using the "ifconfig" to check the network status, then you could know the network "enp0s5" could use for capture packet.



```
parallels@ubuntu:~$ ifconfig
enp0s5    Link encap:Ethernet  HWaddr 00:1c:42:19:bd:aa
          inet addr:10.211.55.5  Bcast:10.211.55.255  Mask:255.255.255.0
          inet6 addr: fe80::21c:42ff:fe19:bdaa/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:303772 errors:0 dropped:0 overruns:0 frame:0
          TX packets:162471 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:443124949 (443.1 MB)  TX bytes:12555630 (12.5 MB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:971 errors:0 dropped:0 overruns:0 frame:0
          TX packets:971 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:79919 (79.9 KB)  TX bytes:79919 (79.9 KB)
```

1.3 Capture DHCP packet

To capture DHCP packet, use “udp port 67” as capture filter, click “click”, use” bootp” to display filter.



Interface	Traffic	Link-layer Header	Promiscuous	Snaplen (	Buffer (M	Monitor Mo	Capture Filter
any		Linux cooked	enabled	default	2	n/a	
enp0s5		Ethernet	enabled	default	2	n/a	udp port 67
Loopback: lo		Ethernet	enabled	default	2	n/a	
nflog		Linux netfilter log messages	enabled	default	2	n/a	
nfqueue		Raw IPv4	enabled	default	2	n/a	
usbmon1		unknown	enabled	default	2	n/a	
usbmon2		unknown	enabled	default	2	n/a	
usbmon3		unknown	enabled	default	2	n/a	
usbmon4		unknown	enabled	default	2	n/a	

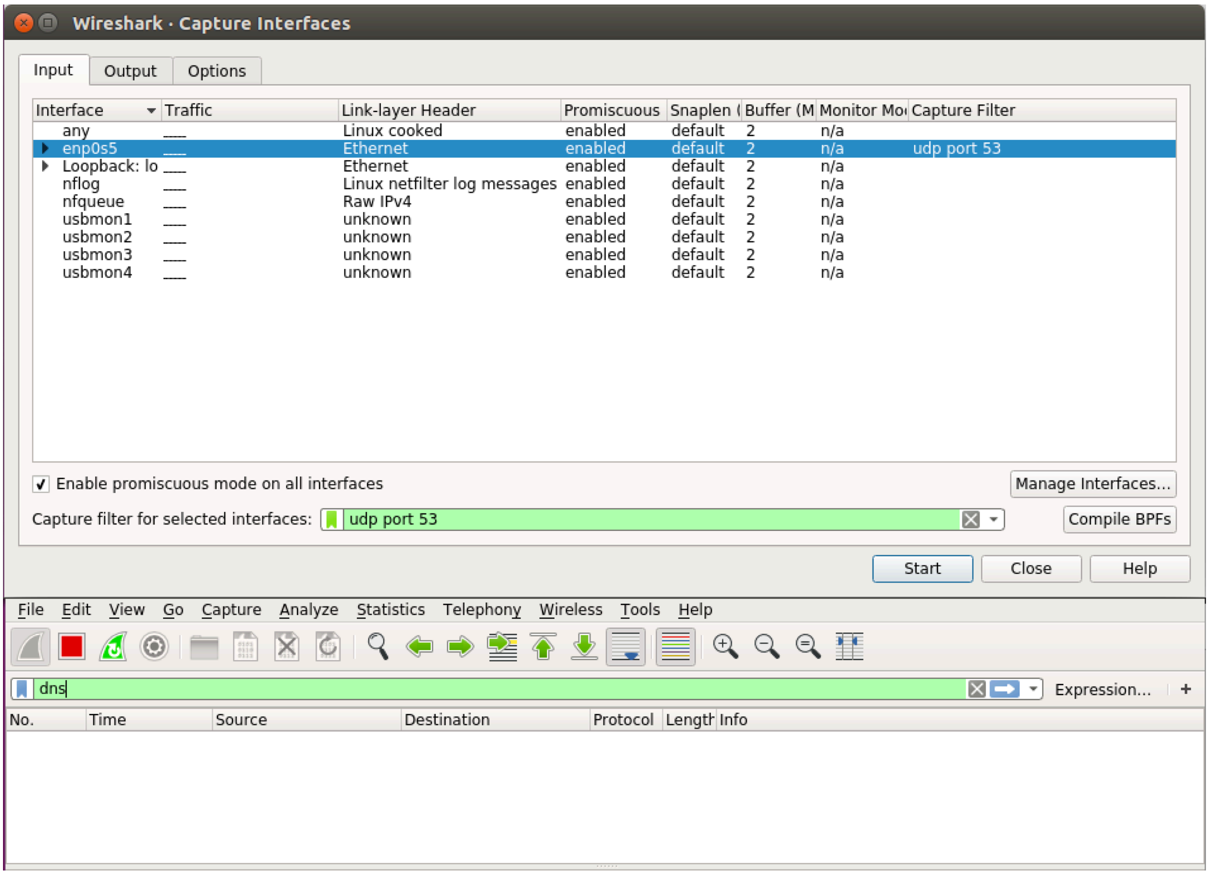
☑ Enable promiscuous mode on all interfaces

Capture filter for selected interfaces: udp port 67

bootp

1.4 Capture DNS packet

To capture DNS packet, use “udp port 53” as capture filter, use “dns” to display filter.



Interface	Traffic	Link-layer Header	Promiscuous	Snaplen (	Buffer (M	Monitor Mo	Capture Filter
any		Linux cooked	enabled	default	2	n/a	
enp0s5		Ethernet	enabled	default	2	n/a	udp port 53
Loopback: lo		Ethernet	enabled	default	2	n/a	
nflog		Linux netfilter log messages	enabled	default	2	n/a	
nfqueue		Raw IPv4	enabled	default	2	n/a	
usbmon1		unknown	enabled	default	2	n/a	
usbmon2		unknown	enabled	default	2	n/a	
usbmon3		unknown	enabled	default	2	n/a	
usbmon4		unknown	enabled	default	2	n/a	

☑ Enable promiscuous mode on all interfaces

Capture filter for selected interfaces: udp port 53

dns

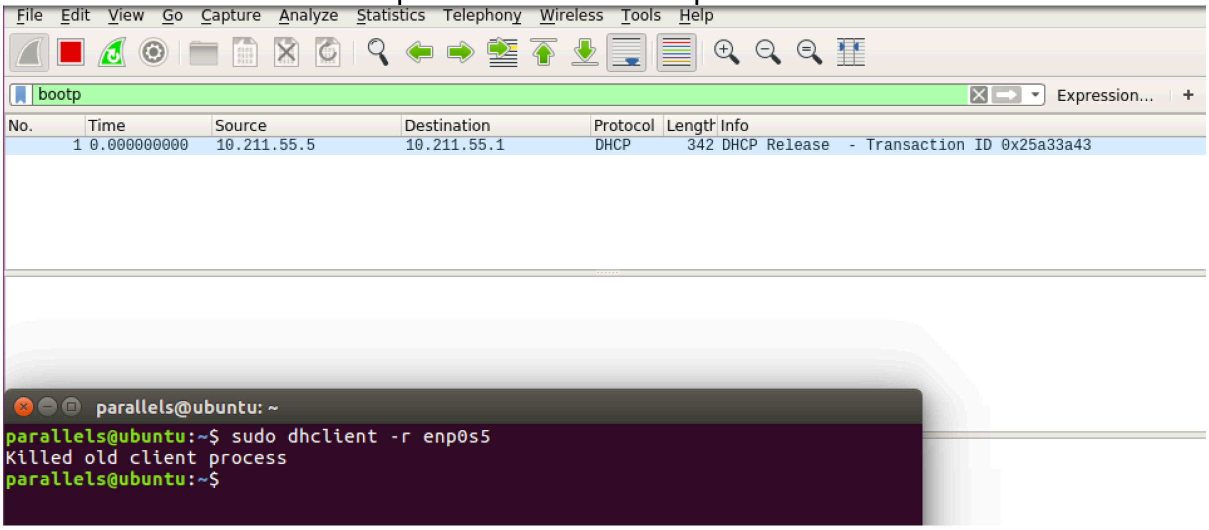
No.	Time	Source	Destination	Protocol	Length	Info

2. The result of DHCP capture and packet analysis

2.1 Capture packet

After configure the wireshark, we start the DHCP packet capture.

Use the “sudo dhclient -r enp0s5”to kill old client process.



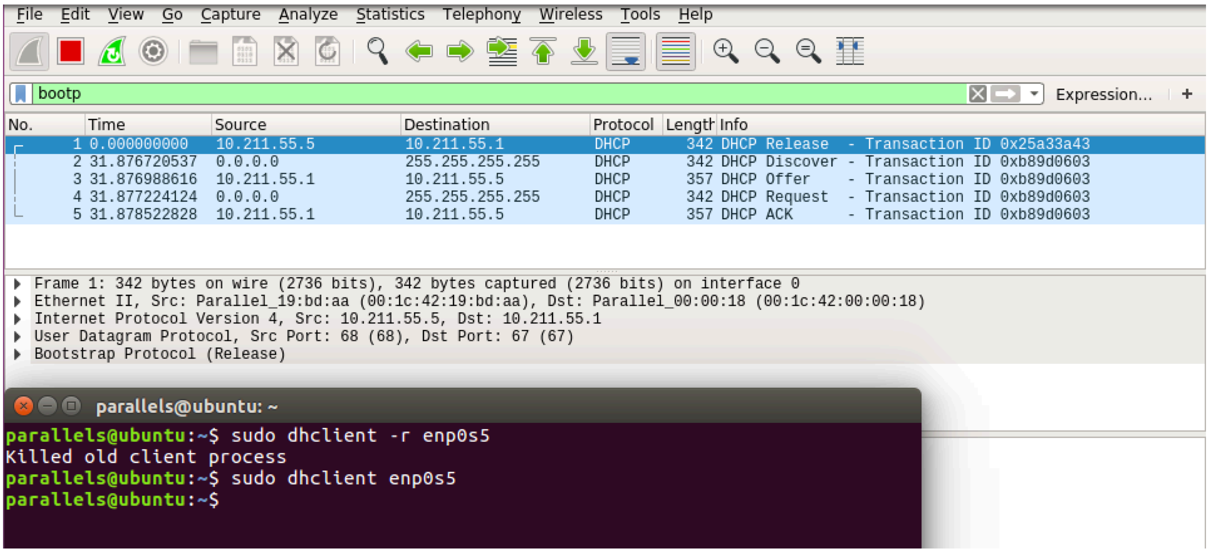
bootp

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.211.55.5	10.211.55.1	DHCP	342	DHCP Release - Transaction ID 0x25a33a43

```
parallels@ubuntu:~$ sudo dhclient -r enp0s5
Killed old client process
parallels@ubuntu:~$
```

from this picture, we get the DHCP Release packet.

Use the “sudo dhclient enp0s5”to initial the DHCP connection.



```
No.  Time          Source         Destination      Protocol Length Info
   1 0.000000000   10.211.55.5    10.211.55.1      DHCP     342 DHCP Release  - Transaction ID 0x25a33a43
   2 31.876720537  0.0.0.0        255.255.255.255  DHCP     342 DHCP Discover - Transaction ID 0xb89d0603
   3 31.876988616  10.211.55.1    10.211.55.5      DHCP     357 DHCP Offer    - Transaction ID 0xb89d0603
   4 31.877224124  0.0.0.0        255.255.255.255  DHCP     342 DHCP Request  - Transaction ID 0xb89d0603
   5 31.878522828  10.211.55.1    10.211.55.5      DHCP     357 DHCP ACK      - Transaction ID 0xb89d0603
```

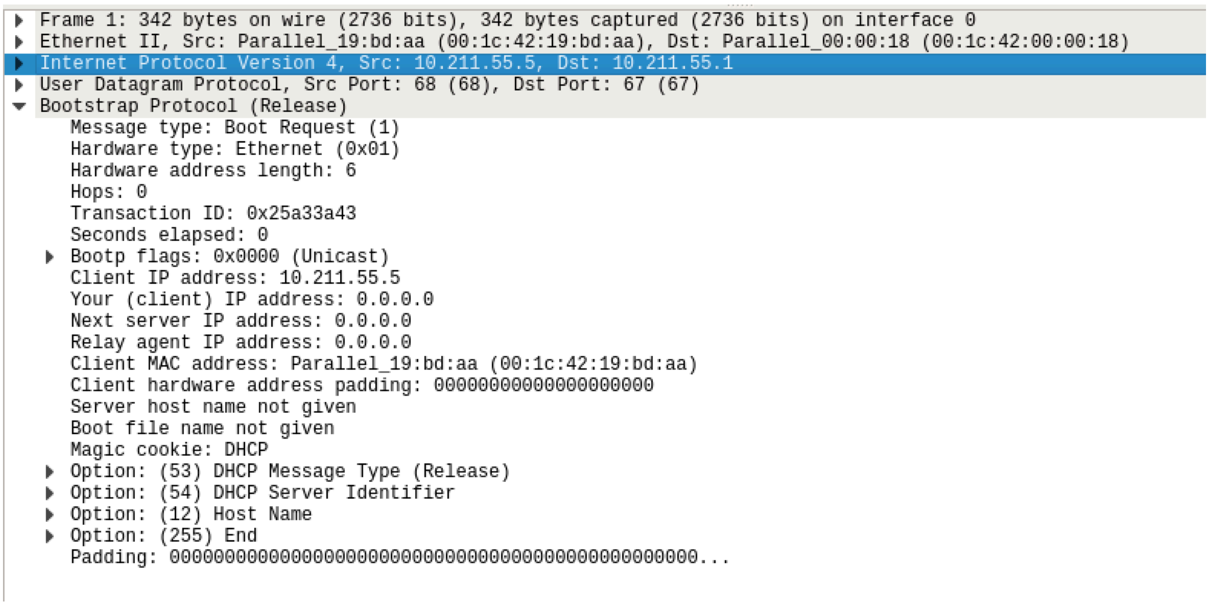
```
▸ Frame 1: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
▸ Ethernet II, Src: Parallel_19:bd:aa (00:1c:42:19:bd:aa), Dst: Parallel_00:00:18 (00:1c:42:00:00:18)
▸ Internet Protocol Version 4, Src: 10.211.55.5, Dst: 10.211.55.1
▸ User Datagram Protocol, Src Port: 68 (68), Dst Port: 67 (67)
▸ Bootstrap Protocol (Release)
```

```
parallels@ubuntu:~$ sudo dhclient -r enp0s5
Killed old client process
parallels@ubuntu:~$ sudo dhclient enp0s5
parallels@ubuntu:~$
```

From this picture, we get the 4 packets, DHCP Discover, DHCP offer, DHCP Request, DHCP ACK.

2.2 Packet analysis

- DHCP release Packet



```
▸ Frame 1: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
▸ Ethernet II, Src: Parallel_19:bd:aa (00:1c:42:19:bd:aa), Dst: Parallel_00:00:18 (00:1c:42:00:00:18)
▸ Internet Protocol Version 4, Src: 10.211.55.5, Dst: 10.211.55.1
▸ User Datagram Protocol, Src Port: 68 (68), Dst Port: 67 (67)
▾ Bootstrap Protocol (Release)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x25a33a43
    Seconds elapsed: 0
  ▸ Bootp flags: 0x0000 (Unicast)
    Client IP address: 10.211.55.5
    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: Parallel_19:bd:aa (00:1c:42:19:bd:aa)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  ▸ Option: (53) DHCP Message Type (Release)
  ▸ Option: (54) DHCP Server Identifier
  ▸ Option: (12) Host Name
  ▸ Option: (255) End
    Padding: 000000000000000000000000000000000000000000000000...
```

1) Critical parameters and explanation

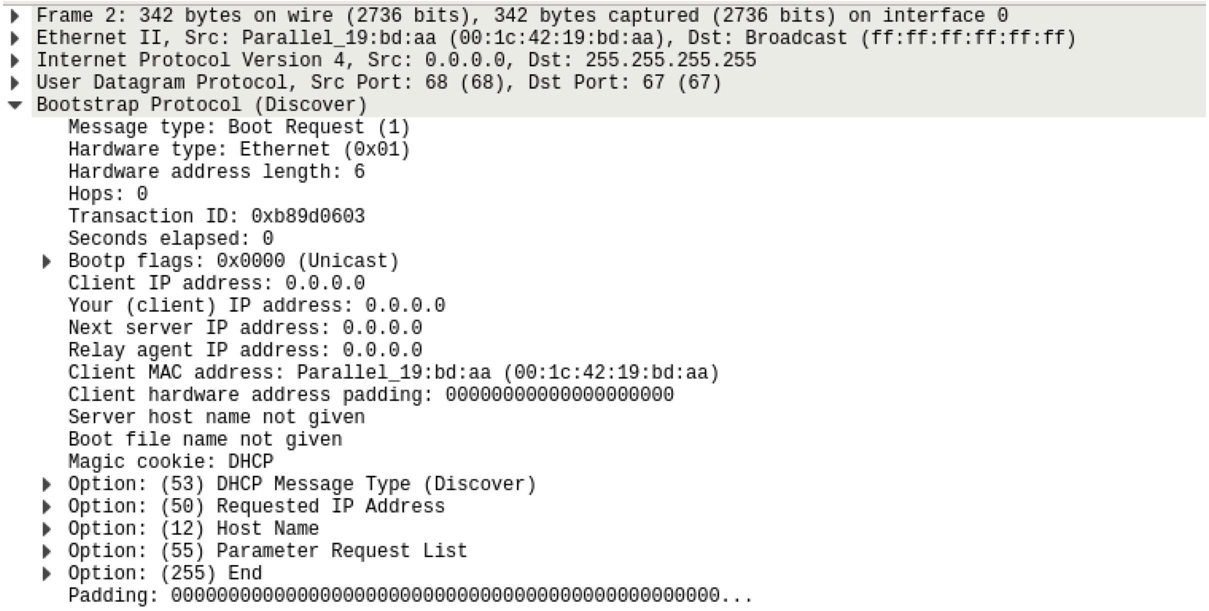
Field	Parameter	Explanation
Message type	Boot Request (1)	This is a request message.
Transaction ID	0x25a33a43	It's used by the client to match responses with requests.
Hops	0	If the data packet transmission via router, each stand adds 1. If in the same network, then0
Client IP address	10.211.55.5	The client has no IP address after release. This filed in only when

		the client definitely knows its IP addresses.
Your IP address	0.0.0.0	This is the IP address the server wants to allocate to the client and it’s filled by the server.
Server IP address	0.0.0.0	This is filled with server’s IP address when it sends DHCPOFFER, DHCPACK and DHCPNACK packets.
Router IP address	0.0.0.0	This is filled with relay agent’s IP address.
Option=53	Length 1	DHCP Message Type, Discover (1)
Option=54	Length 4	DHCP Server Identifier: 10.211.55.1
Option=12	Length 15	Host Name: ubuntu

2) Address

	Frame address	IP Address	Port Number
Source	Parallel_19:bd:aa (00:1c:42:19:bd:aa),	10.211.55.5	68
Destination	Parallel_00:00:18 (00:1c:42:00:00:18)	10.211.55.1	67

- DHCP Discover Packet



```
▶ Frame 2: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
▶ Ethernet II, Src: Parallel_19:bd:aa (00:1c:42:19:bd:aa), 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: 0xb89d0603
    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: Parallel_19:bd:aa (00:1c:42:19:bd:aa)
    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: (50) Requested IP Address
  ▶ Option: (12) Host Name
  ▶ Option: (55) Parameter Request List
  ▶ Option: (255) End
    Padding: 000000000000000000000000000000000000000000000000...
```

1) Critical parameters and explanation

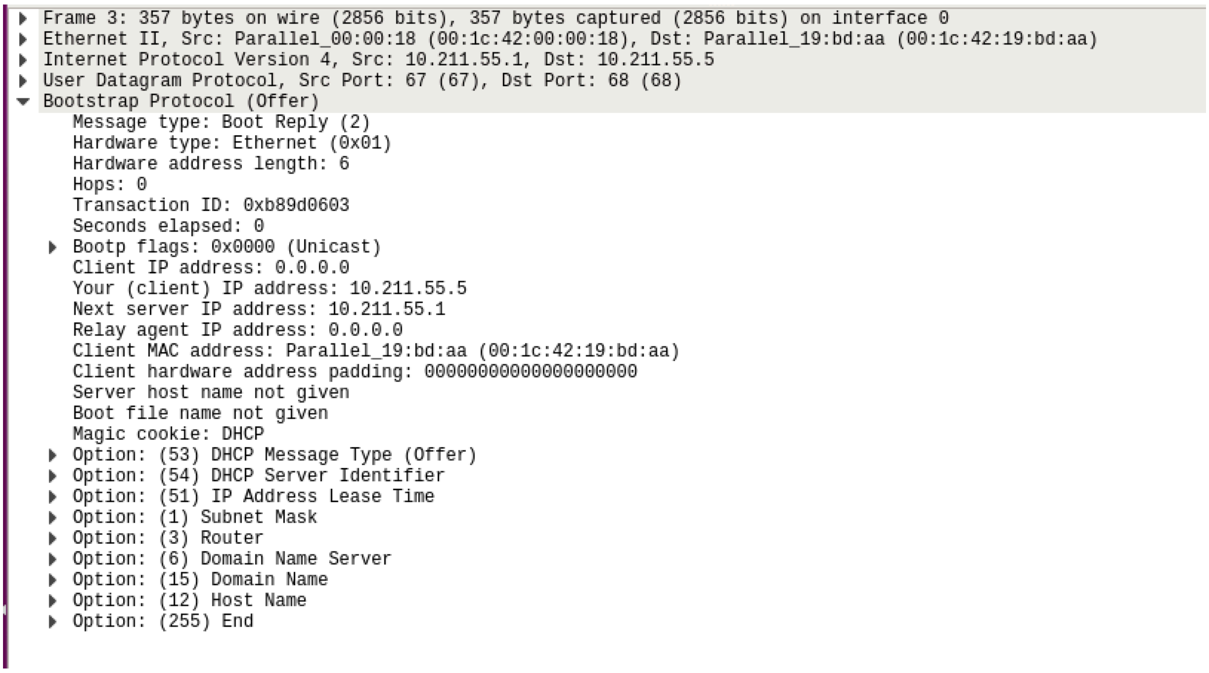
Field	Parameter	Explanation
Message type	Boot Request (1)	This is a request message.

Transaction ID	0xb89d0603	It’s used by the client to match responses with requests.
Hops	0	If the data packet transmission via router, each stand adds 1. If in the same network, then0
Client IP address	0.0.0.0	The client has no IP address after release. This filed in only when the client definitely knows its IP addresses.
Your IP address	0.0.0.0	This is the IP address the server wants to allocate to the client and it’s filled by the server.
Server IP address	0.0.0.0	This is filled with server’s IP address when it sends DHCPOFFER, DHCPACK and DHCPNACK packets.
Router IP address	0.0.0.0	This is filled with relay agent’s IP address.
Option=53	Length 1	DHCP Message Type, Discover (1)
Option=50	Length 4	Requested IP Address: 10.211.55.5
Option=12	Length 15	Host Name: ubuntu
Option=55	Length 13	Parameter Request List (e.g.: subnet mask, router, etc.)

2) Address

	Frame address	IP Address	Port Number
Source	Parallel_19:bd:aa (00:1c:42:19:bd:aa)	0.0.0.0	68
Destination	Broadcast (ff:ff:ff:ff:ff:ff)	255.255.255.255	67

- DHCP Offer Packet



```
▶ Frame 3: 357 bytes on wire (2856 bits), 357 bytes captured (2856 bits) on interface 0
▶ Ethernet II, Src: Parallel_00:00:18 (00:1c:42:00:00:18), Dst: Parallel_19:bd:aa (00:1c:42:19:bd:aa)
▶ Internet Protocol Version 4, Src: 10.211.55.1, Dst: 10.211.55.5
▶ 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: 0xb89d0603
    Seconds elapsed: 0
  ▶ Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 10.211.55.5
    Next server IP address: 10.211.55.1
    Relay agent IP address: 0.0.0.0
    Client MAC address: Parallel_19:bd:aa (00:1c:42:19:bd:aa)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    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
  ▶ Option: (1) Subnet Mask
  ▶ Option: (3) Router
  ▶ Option: (6) Domain Name Server
  ▶ Option: (15) Domain Name
  ▶ Option: (12) Host Name
  ▶ Option: (255) End
```

1) Critical parameters and explanation

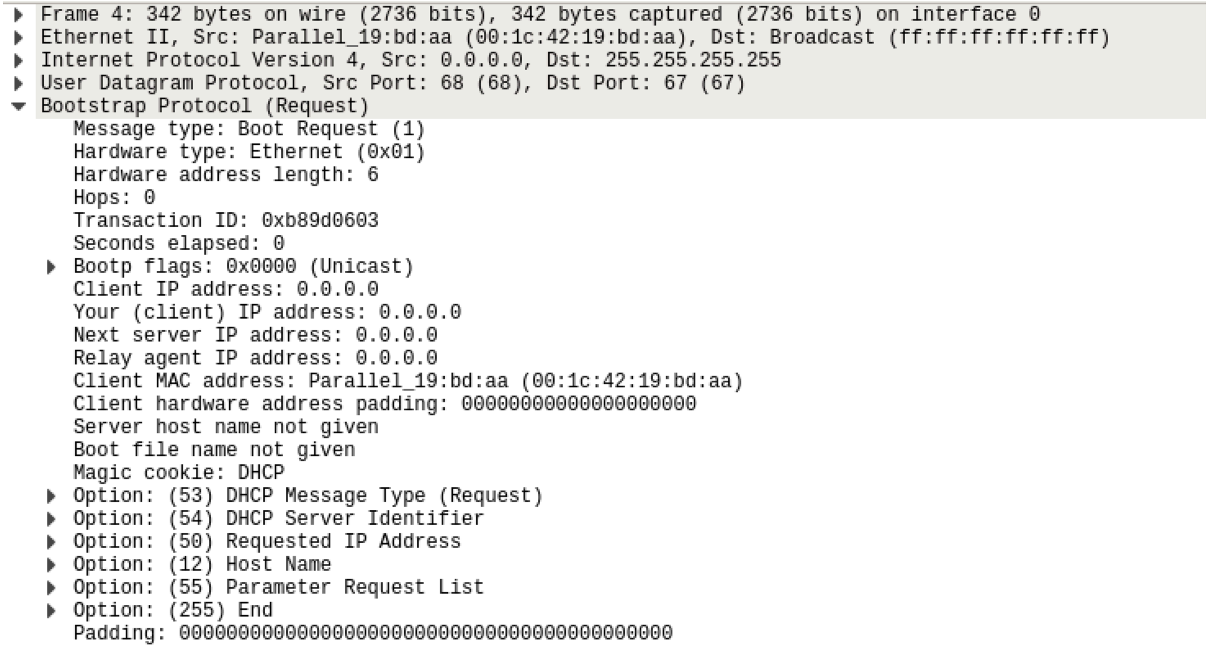
Filed	Parameter	Explanation
Message type	Boot Reply (2)	This is a request message.
Transaction ID	0xb89d0603	It's used by the client to match responses with requests.
Hops	0	If the data packet transmission via router, each stand adds 1. If in the same network, then0
Client IP address	0.0.0.0	The client has no IP address after release. This filed in only when the client definitely knows its IP addresses.
Your IP address	10.211.55.5	This is the IP address the server wants to allocate to the client and it's filled by the server.
Server IP address	10.211.55.1	This is filled with server's IP address when it sends DHCPOFFER,

		DHCPACK and DHCPNACK packets.
Router IP address	0.0.0.0	This is filled with relay agent's IP address.
Option=53	Length 1	DHCP Message Type, Discover (1)
Option=54	Length 4	IP Address Lease Time: (1800s) 30 minutes
Option=51	Length 15	Host Name: ubuntu
Option=1	Length 4	Subnet Mask: 255.255.255.0
Option=3	Length 4	Router: 10.211.55.1
Option=6	Length 4	Domain Name Server: 10.211.55.1
Option=15	Length 11	Domain Name: localdomain
Option=12	Length 26	Host Name: Ubuntu Linux 16.04 Desktop

2) Address

	Frame address	IP Address	Port Number
Source	Parallel_00:00:18 (00:1c:42:00:00:18)	10.211.55.1	67
Destination	Parallel_19:bd:aa (00:1c:42:19:bd:aa)	10.211.55.5	68

- DHCP Request Packet



```
▶ Frame 4: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
▶ Ethernet II, Src: Parallel_19:bd:aa (00:1c:42:19:bd:aa), 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 (Request)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xb89d0603
    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: Parallel_19:bd:aa (00:1c:42:19:bd:aa)
    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: (54) DHCP Server Identifier
  ▶ Option: (50) Requested IP Address
  ▶ Option: (12) Host Name
  ▶ Option: (55) Parameter Request List
  ▶ Option: (255) End
    Padding: 000000000000000000000000000000000000000000
```

1) Critical parameters and explanation

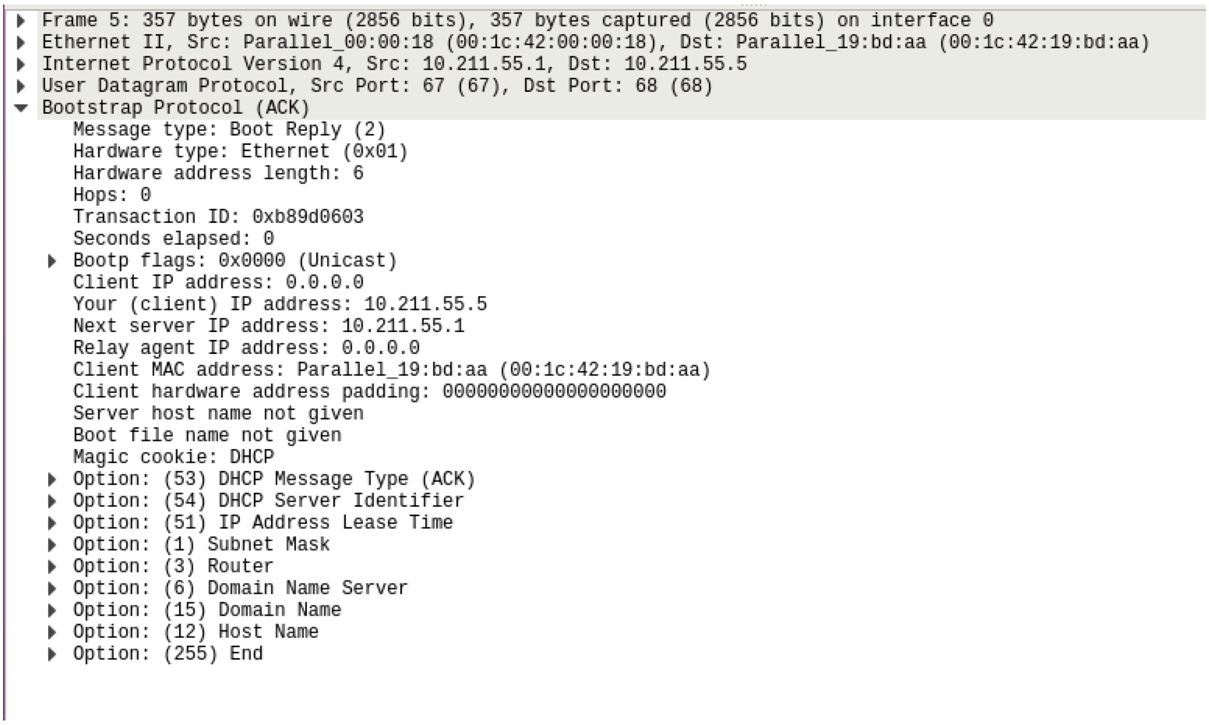
Filed	Parameter	Explanation
Message type	Boot Request (1)	This is a request message.

Transaction ID	0xb89d0603	It's used by the client to match responses with requests.
Hops	0	If the data packet transmission via router, each stand adds 1. If in the same network, then0
Client IP address	0.0.0.0	The client has no IP address after release. This filed in only when the client definitely knows its IP addresses.
Your IP address	0.0.0.0	This is the IP address the server wants to allocate to the client and it's filled by the server.
Server IP address	0.0.0.0	This is filled with server's IP address when it sends DHCPOFFER, DHCPACK and DHCPNACK packets.
Router IP address	0.0.0.0	This is filled with relay agent's IP address.
Option=53	Length 1	DHCP Message Type, Discover (1)
Option=50	Length 4	Requested IP Address: 10.211.55.5
Option=12	Length 15	Host Name: ubuntu
Option=55	Length 13	Parameter Request List (e.g.: subnet mask, router, etc.)

2) Address

	Frame address	IP Address	Port Number
Source	Parallel_19:bd:aa (00:1c:42:19:bb:aa)	0.0.0.0	68
Destination	Broadcast (ff:ff:ff:ff:ff:ff)	255.255.255.255	67

- DHCP ACK Packet



```
▶ Frame 5: 357 bytes on wire (2856 bits), 357 bytes captured (2856 bits) on interface 0
▶ Ethernet II, Src: Parallel_00:00:18 (00:1c:42:00:00:18), Dst: Parallel_19:bd:aa (00:1c:42:19:bd:aa)
▶ Internet Protocol Version 4, Src: 10.211.55.1, Dst: 10.211.55.5
▶ 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: 0xb89d0603
     Seconds elapsed: 0
   ▶ Bootp flags: 0x0000 (Unicast)
     Client IP address: 0.0.0.0
     Your (client) IP address: 10.211.55.5
     Next server IP address: 10.211.55.1
     Relay agent IP address: 0.0.0.0
     Client MAC address: Parallel_19:bd:aa (00:1c:42:19:bd:aa)
     Client hardware address padding: 00000000000000000000
     Server host name not given
     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
   ▶ Option: (1) Subnet Mask
   ▶ Option: (3) Router
   ▶ Option: (6) Domain Name Server
   ▶ Option: (15) Domain Name
   ▶ Option: (12) Host Name
   ▶ Option: (255) End
```

1) Critical parameters and explanation

Filed	Parameter	Explanation
Message type	Boot Reply (2)	This is a request message.
Transaction ID	0xb89d0603	It’s used by the client to match responses with requests.
Hops	0	If the data packet transmission via router, each stand adds 1. If in the same network, then0
Client IP address	0.0.0.0	The client has no IP address after release. This filed in only when the client definitely knows its IP addresses.
Your IP address	10.211.55.5	This is the IP address the server wants to allocate to the client and it’s filled by the server.
Server IP address	10.211.55.1	This is filled with server’s IP address when it sends DHCPOFFER, DHCPACK and DHCPNACK packets.
Router IP address	0.0.0.0	This is filled with relay agent’s IP address.

Option=53	Length 1	DHCP Message Type, Discover (1)
Option=54	Length 4	IP Address Lease Time: (1800s) 30 minutes
Option=51	Length 15	Host Name: ubuntu
Option=1	Length 4	Subnet Mask: 255.255.255.0
Option=3	Length 4	Router: 10.211.55.1
Option=6	Length 4	Domain Name Server: 10.211.55.1
Option=15	Length 11	Domain Name: localdomain
Option=12	Length 26	Host Name: Ubuntu Linux 16.04 Desktop

2) Address

	Frame address	IP Address	Port Number
Source	Parallel_00:00:18 (00:1c:42:00:00:18)	10.211.55.1	67
Destination	Parallel_19:bd:aa (00:1c:42:19:bd:aa)	10.211.55.5	68

- The each DHCP message, unicast or broadcast?
  1. Frame No.1 (discover) : broadcast
  2. Frame No.2 (offer) : unicast
  3. Frame No.3 (request) : broadcast
  4. Frame No.4 (ACK) : unicast

- Compare the value of fields of DHCP messages with the example in Lecture note

1) Frame No.1 (discover)

My Messages				Example in lecture notes			
1	1	6	0	1	1	6	0
0xb89d0603				12			
0		Flags		0		Flags	
0				0			
0				0			
0				0			
0				0			
00:1c:42:19:bd:aa				AA:EC:F9:23:44:19			
53	1		1	53	1		1

Except for the transaction ID and the mac address, all fields are the same.

2) Frame No.2 (Offer)

My Message	Example in lecture notes

2	1	6	0	2	1	6	0
0xb89d0603				12			
0		Flags		0		Flags	
0				0			
10.211.55.5				192.168.10.35			
10.211.55.1				192.168.10.98			
0				0			
00:1c:42:19:bd:aa				AA:EC:F9:23:44:19			
53	1	2		53	1	2	

Only the transaction ID, your IP address, the next server IP address and the mac address are not the same as the example in lecture notes.

3) Frame No.3 (Request)

My Message				Example in lecture notes			
1	1	6	0	1	1	6	0
12				12			
0		Flags		0		Flags	
0				0			
0				0			
0				0			
0				0			
00:1c:42:19:bd:aa				AA:EC:F9:23:44:19			
53	1	3		53	1	3	

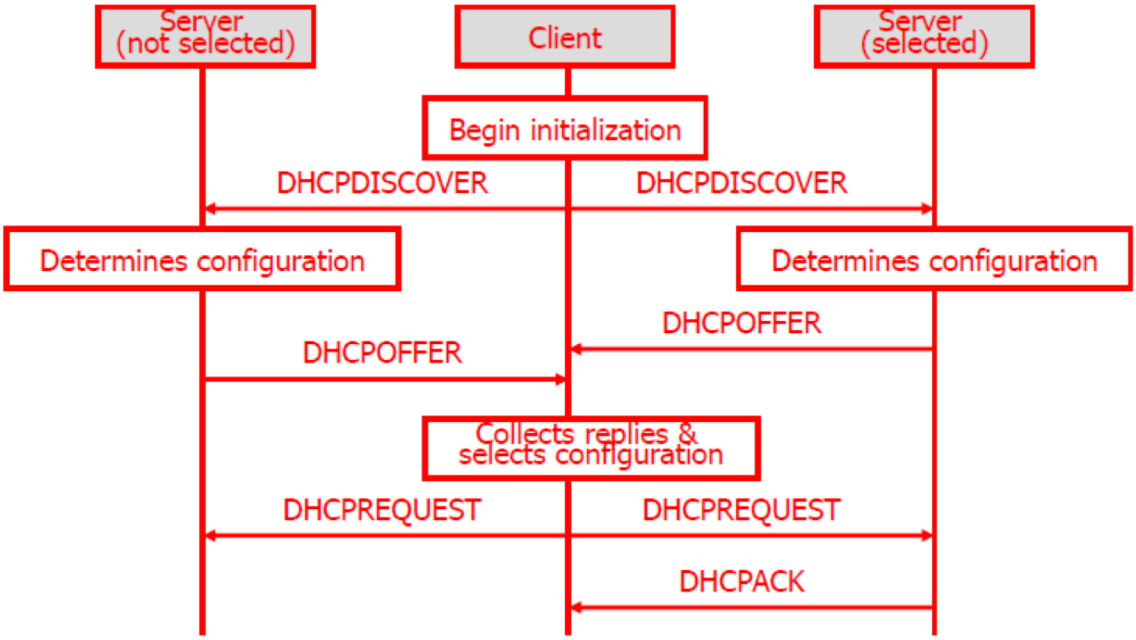
Except for the transaction ID and the mac address, all fields are the same.

4) Frame No.4 (ACK)

My Message				Example in lecture notes			
2	1	6	0	2	1	6	0
12				12			
0		Flags		0		Flags	
0				0			
10.211.55.5				192.168.10.35			
10.211.55.1				192.168.10.98			
0				0			
00:1c:42:19:bd:aa				AA:EC:F9:23:44:19			
53	1	5		53	1	5	

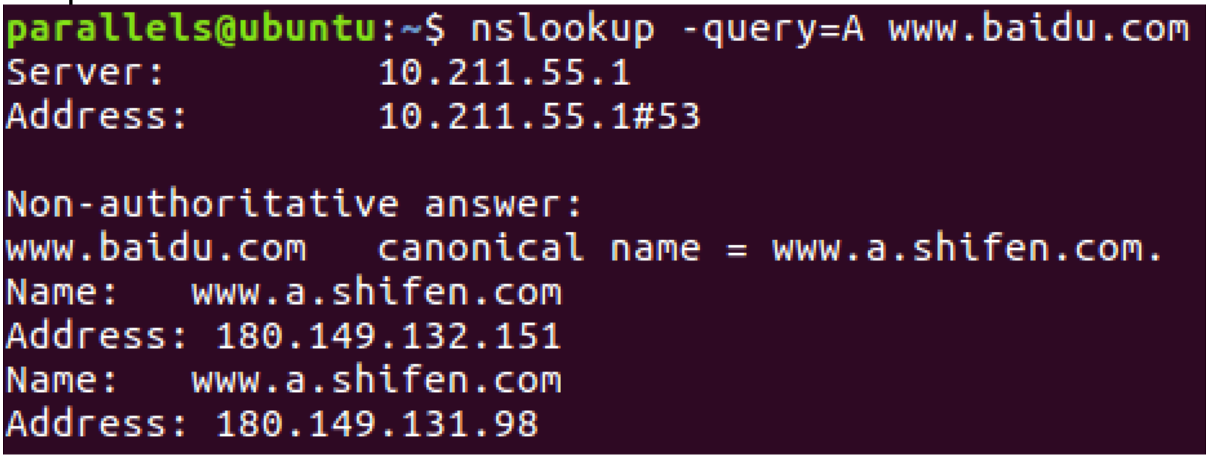
Only the transaction ID, your IP address, the next server IP address and the mac address are not the same as the example in lecture notes.

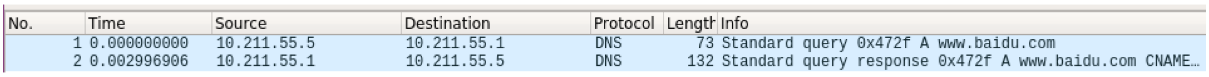
- Message Sequence Chart (MSC)



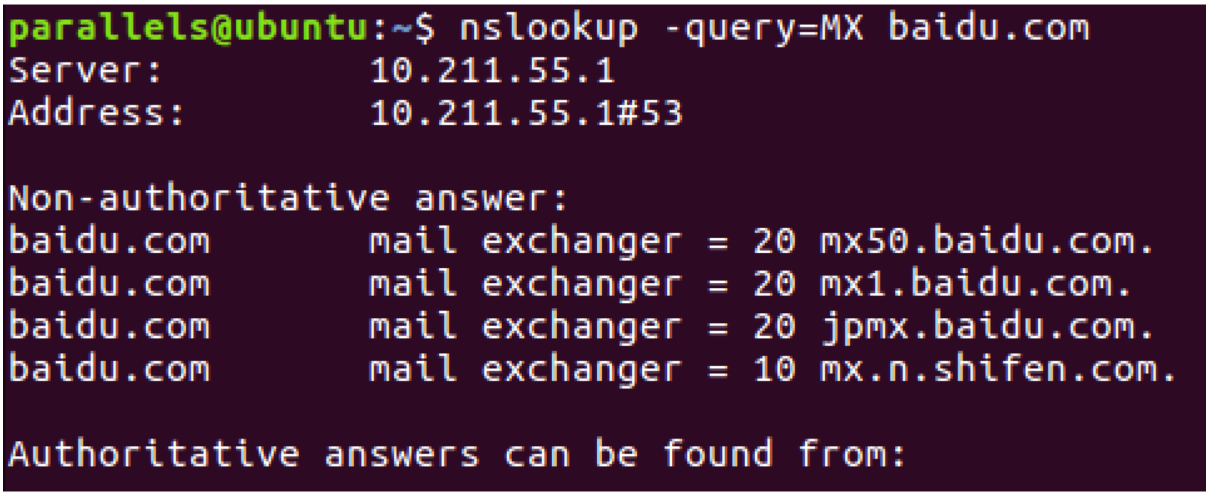
3. The result of DNS capture

3.1 Capture Packet

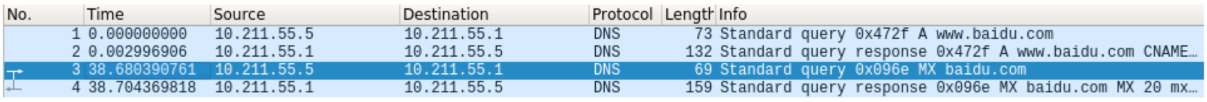

```
parallels@ubuntu:~$ nslookup -query=A www.baidu.com
Server:         10.211.55.1
Address:        10.211.55.1#53

Non-authoritative answer:
www.baidu.com   canonical name = www.a.shifen.com.
Name:   www.a.shifen.com
Address: 180.149.132.151
Name:   www.a.shifen.com
Address: 180.149.131.98
```



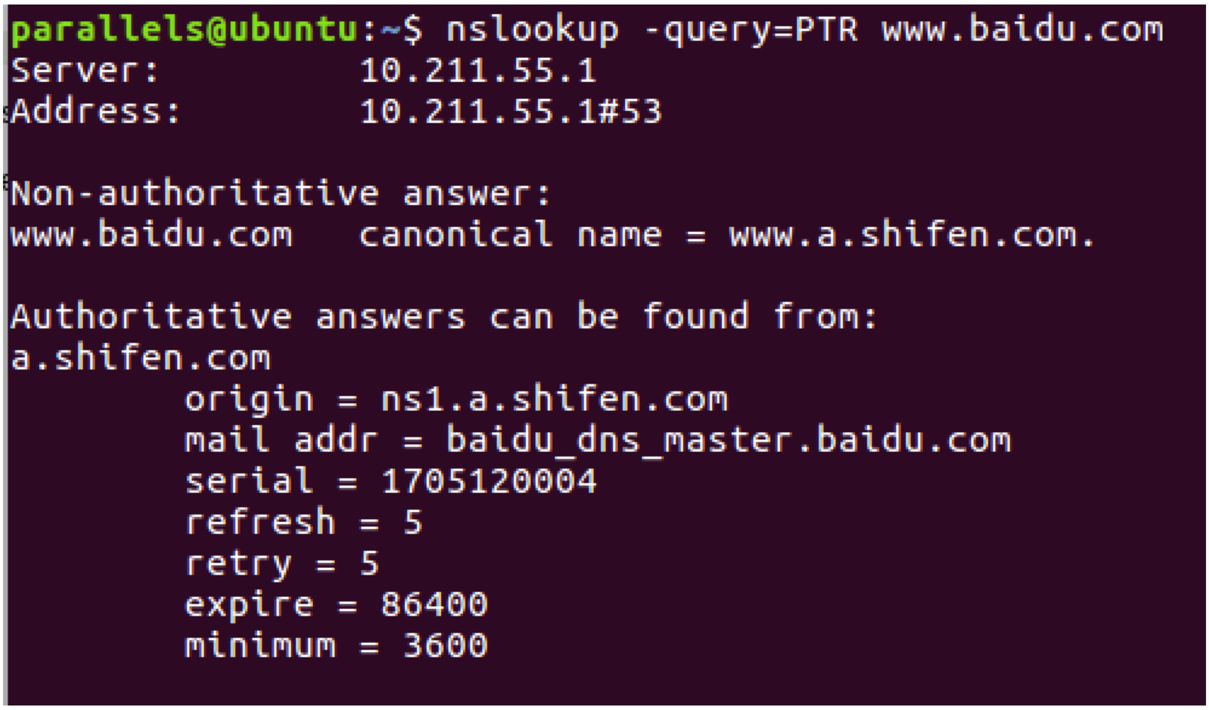
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.211.55.5	10.211.55.1	DNS	73	Standard query 0x472f A www.baidu.com
2	0.002996906	10.211.55.1	10.211.55.5	DNS	132	Standard query response 0x472f A www.baidu.com CNAME…



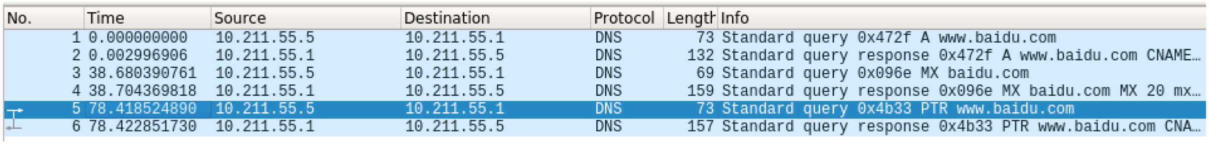
```
parallels@ubuntu:~$ nslookup -query=MX baidu.com
Server:         10.211.55.1
Address:        10.211.55.1#53

Non-authoritative answer:
baidu.com       mail exchanger = 20 mx50.baidu.com.
baidu.com       mail exchanger = 20 mx1.baidu.com.
baidu.com       mail exchanger = 20 jpmx.baidu.com.
baidu.com       mail exchanger = 10 mx.n.shifen.com.

Authoritative answers can be found from:
```



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.211.55.5	10.211.55.1	DNS	73	Standard query 0x472f A www.baidu.com
2	0.002996906	10.211.55.1	10.211.55.5	DNS	132	Standard query response 0x472f A www.baidu.com CNAME…
3	38.680390761	10.211.55.5	10.211.55.1	DNS	69	Standard query 0x096e MX baidu.com
4	38.704369818	10.211.55.1	10.211.55.5	DNS	159	Standard query response 0x096e MX baidu.com MX 20 mx…



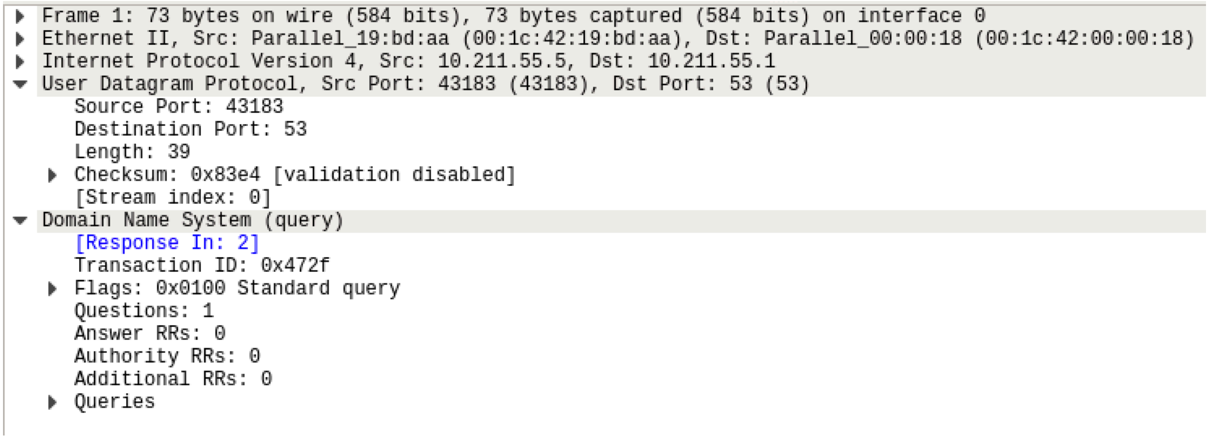
```
parallels@ubuntu:~$ nslookup -query=PTR www.baidu.com
Server:         10.211.55.1
Address:        10.211.55.1#53

Non-authoritative answer:
www.baidu.com   canonical name = www.a.shifen.com.

Authoritative answers can be found from:
a.shifen.com
        origin = ns1.a.shifen.com
        mail addr = baidu_dns_master.baidu.com
        serial = 1705120004
        refresh = 5
        retry = 5
        expire = 86400
        minimum = 3600
```



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.211.55.5	10.211.55.1	DNS	73	Standard query 0x472f A www.baidu.com
2	0.002996906	10.211.55.1	10.211.55.5	DNS	132	Standard query response 0x472f A www.baidu.com CNAME…
3	38.680390761	10.211.55.5	10.211.55.1	DNS	69	Standard query 0x096e MX baidu.com
4	38.704369818	10.211.55.1	10.211.55.5	DNS	159	Standard query response 0x096e MX baidu.com MX 20 mx…
5	78.418524890	10.211.55.5	10.211.55.1	DNS	73	Standard query 0x4b33 PTR www.baidu.com
6	78.422851730	10.211.55.1	10.211.55.5	DNS	157	Standard query response 0x4b33 PTR www.baidu.com CNA…

3.2 Packet analysis

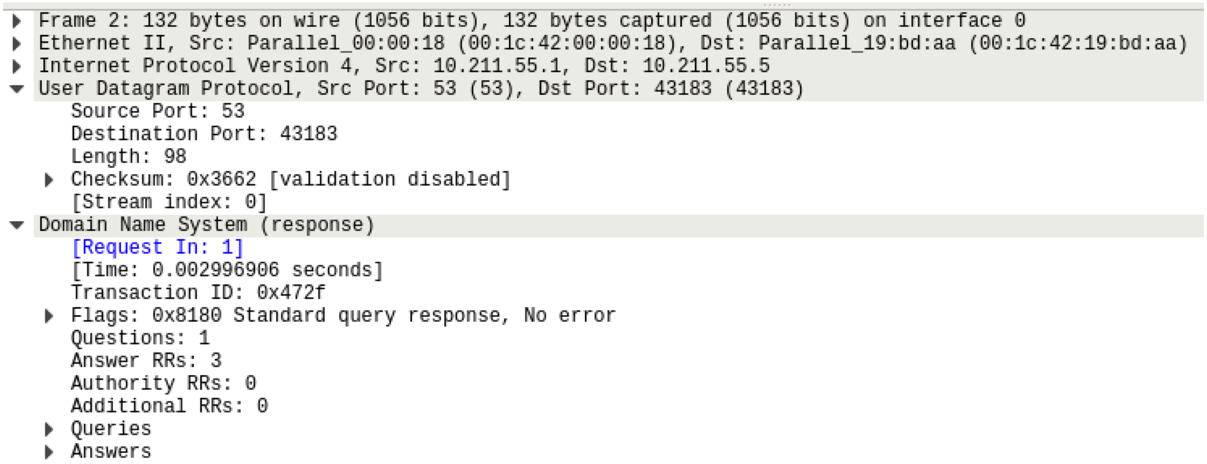
1) DNS Query Type=A



```
▸ Frame 1: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0
▸ Ethernet II, Src: Parallel_19:bd:aa (00:1c:42:19:bd:aa), Dst: Parallel_00:00:18 (00:1c:42:00:00:18)
▸ Internet Protocol Version 4, Src: 10.211.55.5, Dst: 10.211.55.1
▾ User Datagram Protocol, Src Port: 43183 (43183), Dst Port: 53 (53)
     Source Port: 43183
     Destination Port: 53
     Length: 39
   ▸ Checksum: 0x83e4 [validation disabled]
     [Stream index: 0]
▾ Domain Name System (query)
     [Response In: 2]
     Transaction ID: 0x472f
   ▸ Flags: 0x0100 Standard query
     Questions: 1
     Answer RRs: 0
     Authority RRs: 0
     Additional RRs: 0
   ▸ Queries
```

Critical Parameter		Value	Explanation
Transaction		0x472f	16-bit field used to correlate queries and responses.
Parameters 0x0100 Standard Query	Response	0… …. …. ….	1-bit field that identifies the message as a query (0) or response (1). Message is a query.
	Opcode	.000 0… …. ….	Standard query (name to address)
	Truncated	…. ..0. …. ….	Message is not truncated.
	Recursion desired	…. …1 …. ….	The resolver requests recursive service by the name server.
	Z	….. …. .0.. ….	Set to 0 for future use.
	Non-authenticated data	…. …. …0 ….	Unacceptable.
Flag		0x0100	This is a message that the host send to server, so it is a quire.
Question section		1	The number of available question is 1 (the question is at the end of the message).
Answer section Authority section Additional section		0 0 0	These three are in answer section. This is a query message, so the three are all 0.

Frame Address	Parallel_19:bd:aa (00:1c:42:19:bd:aa)	Source MAC Address.
	Parallel_00:00:18 (00:1c:42:00:00:18)	Destination MAC Address(Broadcast).
IP Address	10.211.55.5	Source IP Address.
	10.211.55.1	Destination IP Address.
Port Number	52656	Source port
	53	Destination port

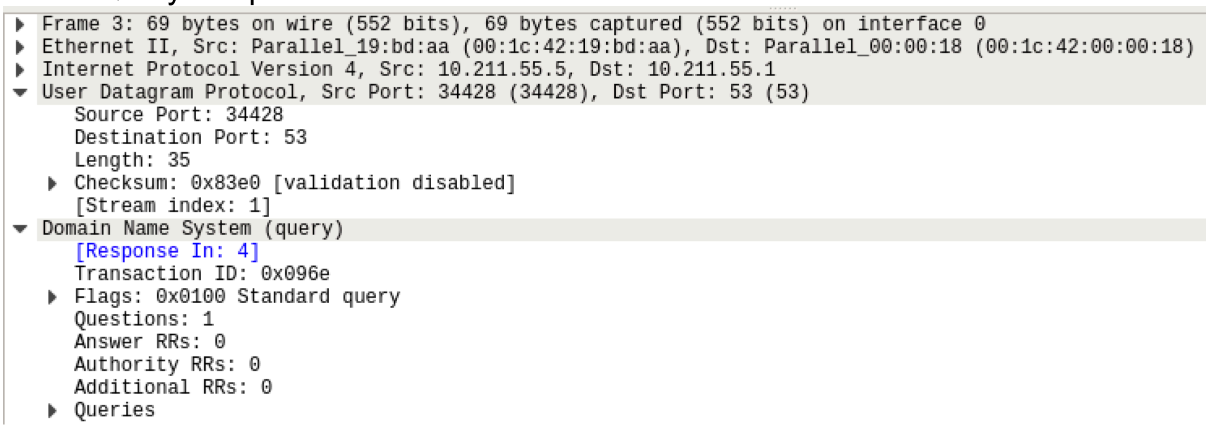


```
▶ Frame 2: 132 bytes on wire (1056 bits), 132 bytes captured (1056 bits) on interface 0
▶ Ethernet II, Src: Parallel_00:00:18 (00:1c:42:00:00:18), Dst: Parallel_19:bd:aa (00:1c:42:19:bd:aa)
▶ Internet Protocol Version 4, Src: 10.211.55.1, Dst: 10.211.55.5
▼ User Datagram Protocol, Src Port: 53 (53), Dst Port: 43183 (43183)
     Source Port: 53
     Destination Port: 43183
     Length: 98
   ▶ Checksum: 0x3662 [validation disabled]
     [Stream index: 0]
▼ Domain Name System (response)
     [Request In: 1]
     [Time: 0.002996906 seconds]
     Transaction ID: 0x472f
   ▶ Flags: 0x8180 Standard query response, No error
     Questions: 1
     Answer RRs: 3
     Authority RRs: 0
     Additional RRs: 0
   ▶ Queries
   ▶ Answers
```

Critical Parameter		Value	Explanation
Transaction		0x472f	16-bit field used to correlate queries and responses.
Parameters 0x0100 Standard Query	Response	1… …. …. ….	1-bit field that identifies the message as a query (0) or response (1). Message is a query.
	Opcode	.000 0… …. ….	Standard query (name to address)
	Truncated	…. ..0. …. ….	Message is not truncated.
	Recursion desired	…. …1 …. ….	The resolver requests recursive service by the name server.
	Recursion available	…. …. 1… ….	Server can do recursive queries
	Z	….. …. .0.. ….	Set to 0 for future use.
	Anwser authenticated	…. …. ..0. ….	Answer/authority portion was not

			authenticated by the server
	Non-authenticated Data	…. …. …0 ….	Unacceptable.
	Reply code:	…. …. …. 0000 =	No error (0)
Flag		0x8180	This is a message that the host send to server, so it is a quire.
Question section		1	The number of available question is 1 (the question is at the end of the message).
Answer section		3	There are 3 IP Addresses for baidu server.
Authority section		0	No Authority section.
Additional section		0	No Additional section.
Frame Address		Parallel_00:00:18 (00:1c:42:00:00:18)	Source MAC Address.
		Parallel_19:bd:aa (00:1c:42:19:bd:aa)	Destination MAC Address(Broadcast).
IP Address		10.211.55.1	Source IP Address.
		10.211.55.5	Destination IP Address.
Port Number		53	Source port
		52656	Destination port

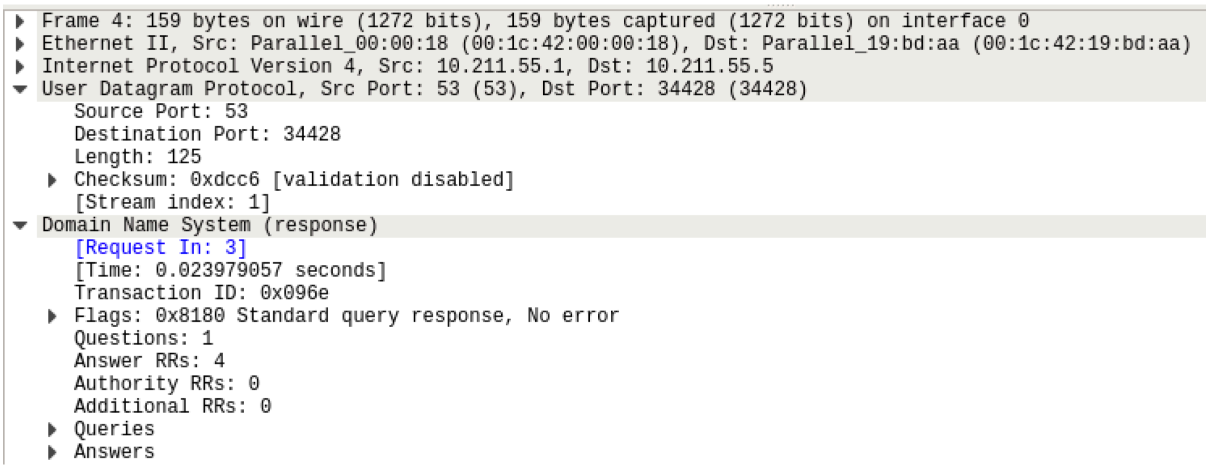
2) DNS Query Response TYPE=MX



```
▶ Frame 3: 69 bytes on wire (552 bits), 69 bytes captured (552 bits) on interface 0
▶ Ethernet II, Src: Parallel_19:bd:aa (00:1c:42:19:bd:aa), Dst: Parallel_00:00:18 (00:1c:42:00:00:18)
▶ Internet Protocol Version 4, Src: 10.211.55.5, Dst: 10.211.55.1
▼ User Datagram Protocol, Src Port: 34428 (34428), Dst Port: 53 (53)
     Source Port: 34428
     Destination Port: 53
     Length: 35
   ▶ Checksum: 0x83e0 [validation disabled]
     [Stream index: 1]
▼ Domain Name System (query)
     [Response In: 4]
     Transaction ID: 0x096e
   ▶ Flags: 0x0100 Standard query
     Questions: 1
     Answer RRs: 0
     Authority RRs: 0
     Additional RRs: 0
   ▶ Queries
```

Critical Parameter	Value	Explanation

Transaction		0x096e	16-bit field used to correlate queries and responses.
Parameters 0x0100 Standard Query	Response	0… …. …. ….	1-bit field that identifies the message as a query (0) or response (1). Message is a query.
	Opcode	.000 0… …. ….	Standard query (name to address)
	Truncated	…. ..0. …. ….	Message is not truncated.
	Recursion desired	…. …1 …. ….	The resolver requests recursive service by the name server.
	Z	….. …. .0.. ….	Set to 0 for future use.
	Non-authenticated data	…. …. …0 ….	Unacceptable.
Flag		0x0100	This is a message that the host send to server, so it is a quire.
Question section		1	The number of available question is 1 (the question is at the end of the message).
Answer section Authority section Additional section		0 0 0	These three are in answer section. This is a query message, so the three are all 0.
Frame Address		Parallel_19:bd:aa (00:1c:42:19:bd:aa)	Source MAC Address.
		Parallel_00:00:18 (00:1c:42:00:00:18)	Destination MAC Address(Broadcast).
IP Address		10.211.55.5	Source IP Address.
		10.211.55.1	Destination IP Address.
Port Number		34428	Source port
		53	Destination port

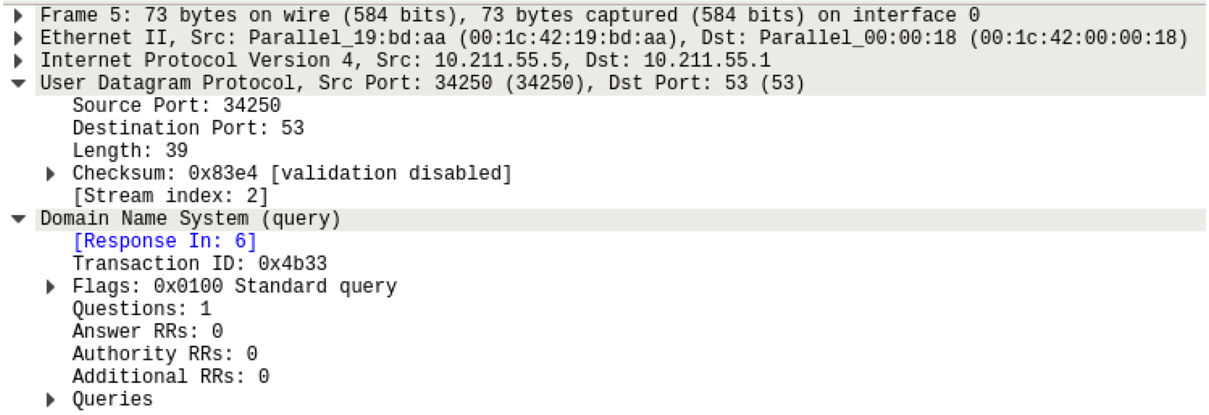


```
▶ Frame 4: 159 bytes on wire (1272 bits), 159 bytes captured (1272 bits) on interface 0
▶ Ethernet II, Src: Parallel_00:00:18 (00:1c:42:00:00:18), Dst: Parallel_19:bd:aa (00:1c:42:19:bd:aa)
▶ Internet Protocol Version 4, Src: 10.211.55.1, Dst: 10.211.55.5
▼ User Datagram Protocol, Src Port: 53 (53), Dst Port: 34428 (34428)
     Source Port: 53
     Destination Port: 34428
     Length: 125
   ▶ Checksum: 0xdcc6 [validation disabled]
     [Stream index: 1]
▼ Domain Name System (response)
     [Request In: 3]
     [Time: 0.023979057 seconds]
     Transaction ID: 0x096e
   ▶ Flags: 0x8180 Standard query response, No error
     Questions: 1
     Answer RRs: 4
     Authority RRs: 0
     Additional RRs: 0
   ▶ Queries
   ▶ Answers
```

Critical Parameter		Value	Explanation
Transaction		0x096e	16-bit field used to correlate queries and responses.
Parameters 0x0100 Standard Query	Response	1… …. …. ….	1-bit field that identifies the message as a query (0) or response (1). Message is a query.
	Opcode	.000 0… …. ….	Standard query (name to address)
	Truncated	…. ..0. …. ….	Message is not truncated.
	Recursion desired	…. …1 …. ….	The resolver requests recursive service by the name server.
	Recursion available	…. …. 1… ….	Server can do recursive queries
	Z	….. …. .0.. ….	Set to 0 for future use.
	Anwser authenticated	…. …. ..0. ….	Answer/authority portion was not authenticated by the server
	Non-authenticated Data	…. …. …0 ….	Unacceptable.
	Reply code:	…. …. …. 0000 =	No error (0)
Flag		0x8180	This is a message that the host send to server, so it is a quire.

Question section	1	The number of available question is 1 (the question is at the end of the message).
Answer section	4	There are 4 IP Addresses for baidu server.
Authority section	0	No Authority section.
Additional section	0	No Additional section.
Frame Address	Parallel_00:00:18 (00:1c:42:00:00:18)	Source MAC Address.
	Parallel_19:bd:aa (00:1c:42:19:bd:aa)	Destination MAC Address(Broadcast).
IP Address	10.211.55.1	Source IP Address.
	10.211.55.5	Destination IP Address.
Port Number	53	Source port
	34428	Destination port

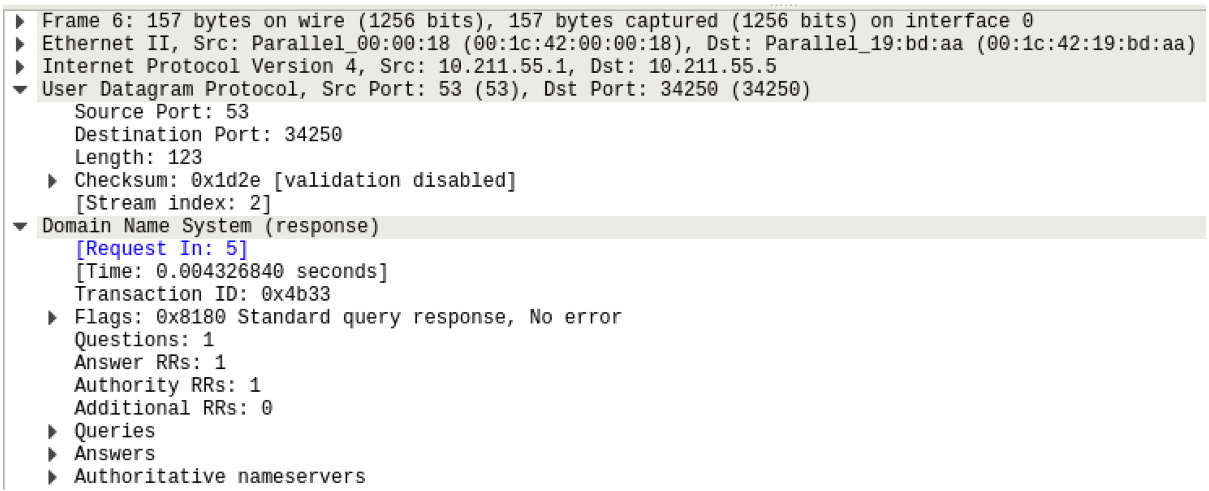
3) DNS QUERY TYPE=PTR



```
▸ Frame 5: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0
▸ Ethernet II, Src: Parallel_19:bd:aa (00:1c:42:19:bd:aa), Dst: Parallel_00:00:18 (00:1c:42:00:00:18)
▸ Internet Protocol Version 4, Src: 10.211.55.5, Dst: 10.211.55.1
▾ User Datagram Protocol, Src Port: 34250 (34250), Dst Port: 53 (53)
    Source Port: 34250
    Destination Port: 53
    Length: 39
  ▸ Checksum: 0x83e4 [validation disabled]
    [Stream index: 2]
▾ Domain Name System (query)
    [Response In: 6]
    Transaction ID: 0x4b33
  ▸ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▸ Queries
```

Critical Parameter		Value	Explanation
Transaction		0x4b33	16-bit field used to correlate queries and responses.
Parameters 0x0100 Standard Query	Response	0… …. …. ….	1-bit field that identifies the message as a query (0) or response (1). Message is a query.
	Opcode	.000 0… …. ….	Standard query (name to address)
	Truncated	…. ..0. …. ….	Message is not truncated.

	Recursion desired	…. …1 …. ….	The resolver requests recursive service by the name server.
	Z	….. …. .0.. ….	Set to 0 for future use.
	Non-authenticated data	…. …. …0 ….	Unacceptable.
Flag		0x0100	This is a message that the host send to server, so it is a quire.
Question section		1	The number of available question is 1 (the question is at the end of the message).
Answer section Authority section Additional section		0 0 0	These three are in answer section. This is a query message, so the three are all 0.
Frame Address		Parallel_19:bd:aa (00:1c:42:19:bd:aa)	Source MAC Address.
		Parallel_00:00:18 (00:1c:42:00:00:18)	Destination MAC Address(Broadcast).
IP Address		10.211.55.5	Source IP Address.
		10.211.55.1	Destination IP Address.
Port Number		34250	Source port
		53	Destination port



```
▶ Frame 6: 157 bytes on wire (1256 bits), 157 bytes captured (1256 bits) on interface 0
▶ Ethernet II, Src: Parallel_00:00:18 (00:1c:42:00:00:18), Dst: Parallel_19:bd:aa (00:1c:42:19:bd:aa)
▶ Internet Protocol Version 4, Src: 10.211.55.1, Dst: 10.211.55.5
▼ User Datagram Protocol, Src Port: 53 (53), Dst Port: 34250 (34250)
     Source Port: 53
     Destination Port: 34250
     Length: 123
   ▶ Checksum: 0x1d2e [validation disabled]
     [Stream index: 2]
▼ Domain Name System (response)
     [Request In: 5]
     [Time: 0.004326840 seconds]
     Transaction ID: 0x4b33
   ▶ Flags: 0x8180 Standard query response, No error
     Questions: 1
     Answer RRs: 1
     Authority RRs: 1
     Additional RRs: 0
   ▶ Queries
   ▶ Answers
   ▶ Authoritative nameservers
```

Critical Parameter	Value	Explanation

Transaction		0x4b33	16-bit field used to correlate queries and responses.
Parameters 0x0100 Standard Query	Response	1… …. …. ….	1-bit field that identifies the message as a query (0) or response (1). Message is a query.
	Opcode	.000 0… …. ….	Standard query (name to address)
	Truncated	…. ..0. …. ….	Message is not truncated.
	Recursion desired	…. …1 …. ….	The resolver requests recursive service by the name server.
	Recursion available	…. …. 1… ….	Server can do recursive queries
	Z	….. …. .0.. ….	Set to 0 for future use.
	Anwser authenticated	…. …. ..0. ….	Answer/authority portion was not authenticated by the server
	Non-authenticated Data	…. …. …0 ….	Unacceptable.
	Reply code:	.... 0000 =	No error (0)
Flag		0x8180	This is a message that the host send to server, so it is a quire.
Question section		1	The number of available question is 1 (the question is at the end of the message).
Answer section		0	There are 4 IP Addresses for baidu server.
Authority section		0	No Authority section.
Additional section		0	No Additional section.
Frame Address		Parallel_00:00:18 (00:1c:42:00:00:18)	Source MAC Address.

	Parallel_19:bd:aa (00:1c:42:19:bd:aa)	Destination MAC Address(Broadcast).
IP Address	10.211.55.1	Source IP Address.
	10.211.55.5	Destination IP Address.
Port Number	53	Source port
	34250	Destination port

- Compare the DNS message with the one in Lecture notes

1. DNS Query TYPE=A

	My Messages	Example in lecture notes
Header	Opcode=standard query	Opcode=standard query
Question	QNAME=www.baidu.com	QNAME=SRI-ARPA
	QCLASS=IN	QCLASS=IN
	QTYPE=A	QTYPE=A
Answer section	<empty>	<empty>
Authority section	<empty>	<empty>
Additional section	<empty>	<empty>

2. DNS Query Response TYPE=A

	My Messages	Example in lecture notes
Header	Opcode=standard query	Opcode=standard query
Question	QNAME=www.baidu.com	QNAME=SRI-ARPA
	QCLASS=IN	QCLASS=IN
	QTYPE=A	QTYPE=A
Answer section	www.baidu.com www.a.shifen.com (IN A 220.181.112.244)	SRI-NIC.ARPA 86400 IN A 26.0.0.73 86400 IN A 10.0.0.51
Authority section	<empty>	<empty>
Additional section	<empty>	<empty>

3. DNS Query TYPE=MX

	My Messages	Example in lecture notes
Header	Opcode=standard query	Opcode=standard query
Question	QNAME=www.baidu.com	QNAME=SRI-ARPA
	QCLASS=IN	QCLASS=IN

	QTYPE=MX	QTYPE=MX
Answer section	<empty>	<empty>
Authority section	<empty>	<empty>
Additional section	<empty>	<empty>

4. DNS Query Response TYPE=MX

	My Messages	Example in lecture notes
Header	Opcode=standard query	Opcode=standard query
Question	QNAME=www.baidu.com	QNAME=SRI-ARPA
	QCLASS=IN	QCLASS=IN
	QTYPE=MX	QTYPE=MX
Answer section	jpmx.baidu.com mx50.baidu.com mx1.baidu.com mx.n.shifen.com	SRI-NIC.ARPA 86400 IN A 26.0.0.73 86400 IN A 10.0.0.51
Authority section	<empty>	<empty>
Additional section	<empty>	<empty>

5. DNS Query TYPE=PTR

	My Messages	Example in lecture notes
Header	Opcode=standard query	Opcode=standard query
Question	QNAME=www.baidu.com	QNAME=SRI-ARPA
	QCLASS=IN	QCLASS=IN
	QTYPE=PTR	QTYPE=PTR
Answer section	<empty>	<empty>
Authority section	<empty>	<empty>
Additional section	<empty>	<empty>

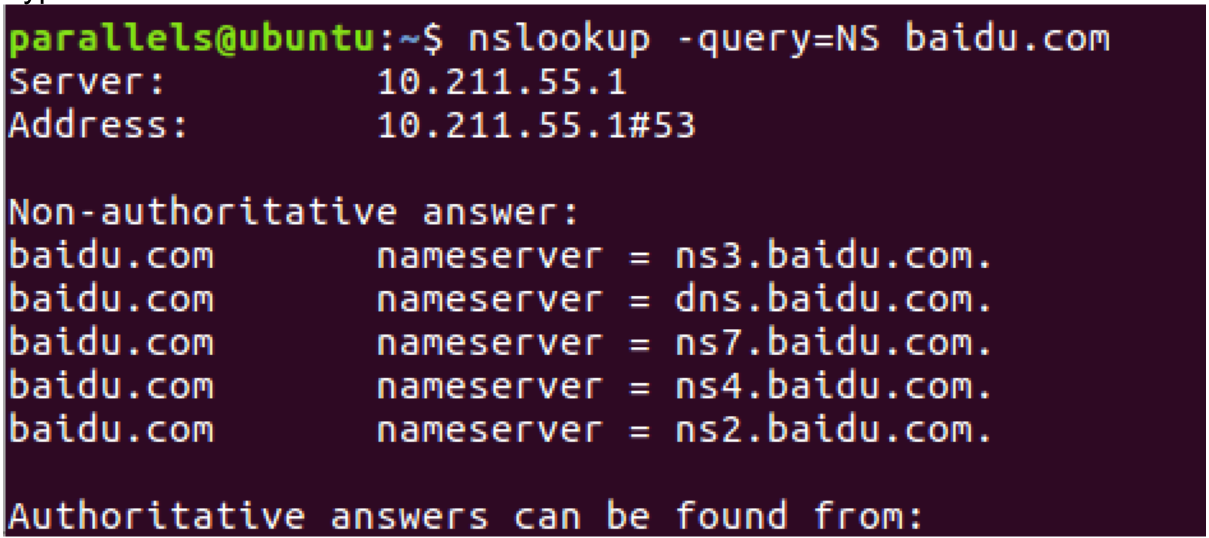
6. DNS Query Response TYPE=PTR

	My Messages	Example in lecture notes
Header	Opcode=standard query	Opcode=standard query
Question	QNAME=www.baidu.com	QNAME=SRI-ARPA
	QCLASS=IN	QCLASS=IN
	QTYPE=PTR	QTYPE=PTR
Answer section	www.a.shifen.com	SRI-NIC.ARPA

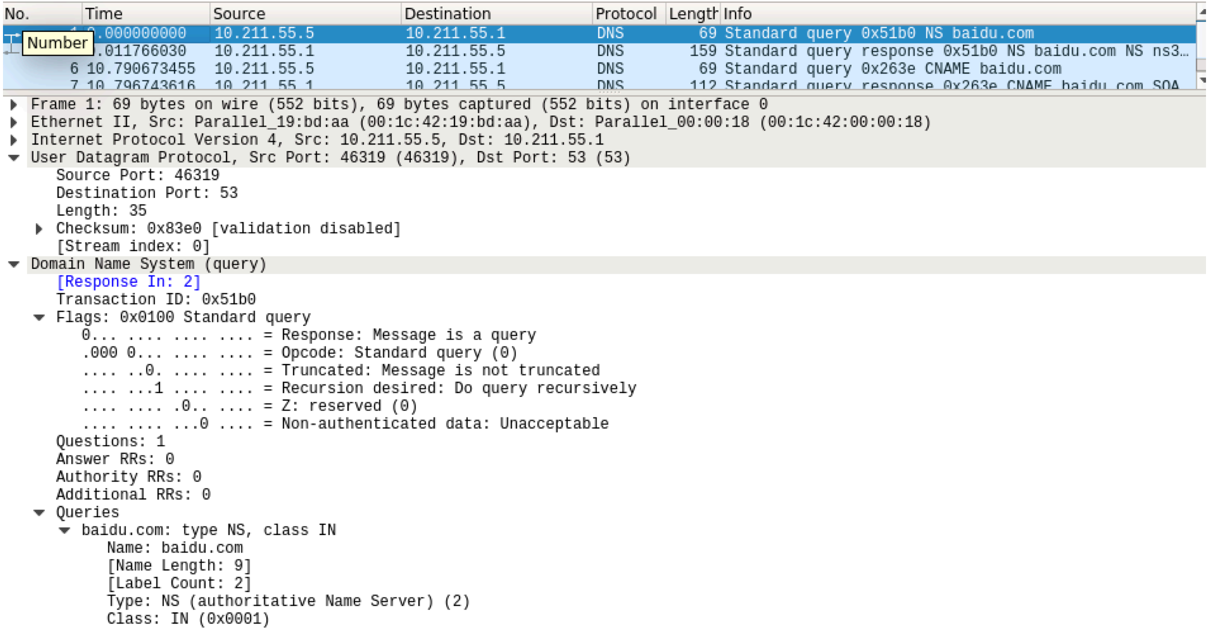
		86400 IN A 26.0.0.73 86400 IN A 10.0.0.51
Authority section	baidu_dns_master.baidu.com	mname
Additional section	<empty>	<empty>

- Use nslookup to resolve type ”NS” ， “CNAME” query.

1) Type=NS

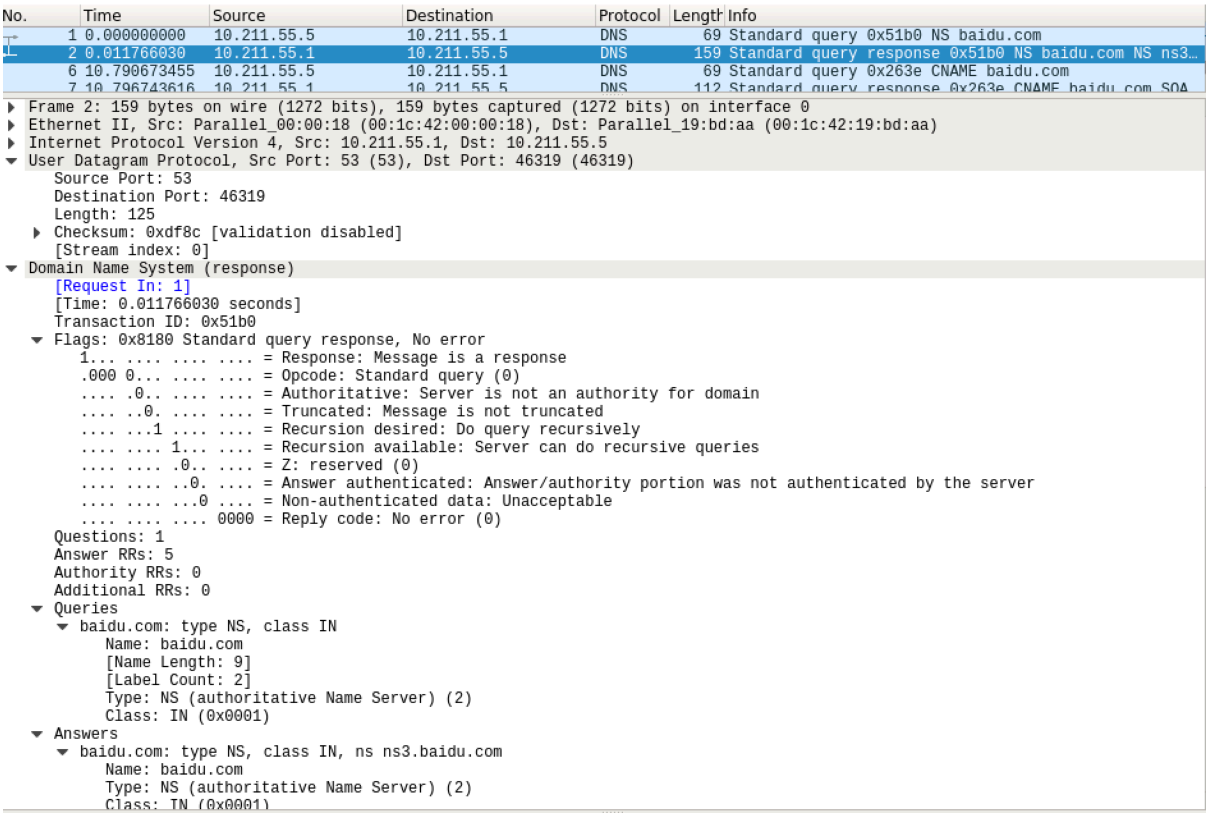


```
parallels@ubuntu:~$ nslookup -query=NS baidu.com
Server:         10.211.55.1
Address:        10.211.55.1#53

Non-authoritative answer:
baidu.com       nameserver = ns3.baidu.com.
baidu.com       nameserver = dns.baidu.com.
baidu.com       nameserver = ns7.baidu.com.
baidu.com       nameserver = ns4.baidu.com.
baidu.com       nameserver = ns2.baidu.com.

Authoritative answers can be found from:
```



```
No.   Time          Source        Destination   Protocol Length Info
    1 0.000000000   10.211.55.5   10.211.55.1   DNS        69 Standard query 0x51b0 NS baidu.com
     .011766030     10.211.55.1   10.211.55.5   DNS       159 Standard query response 0x51b0 NS baidu.com NS ns3…
    6 10.790673455  10.211.55.5   10.211.55.1   DNS        69 Standard query 0x263e CNAME baidu.com
    7 10.796743616  10.211.55.1   10.211.55.5   DNS       112 Standard query response 0x263e CNAME baidu.com SOA
```

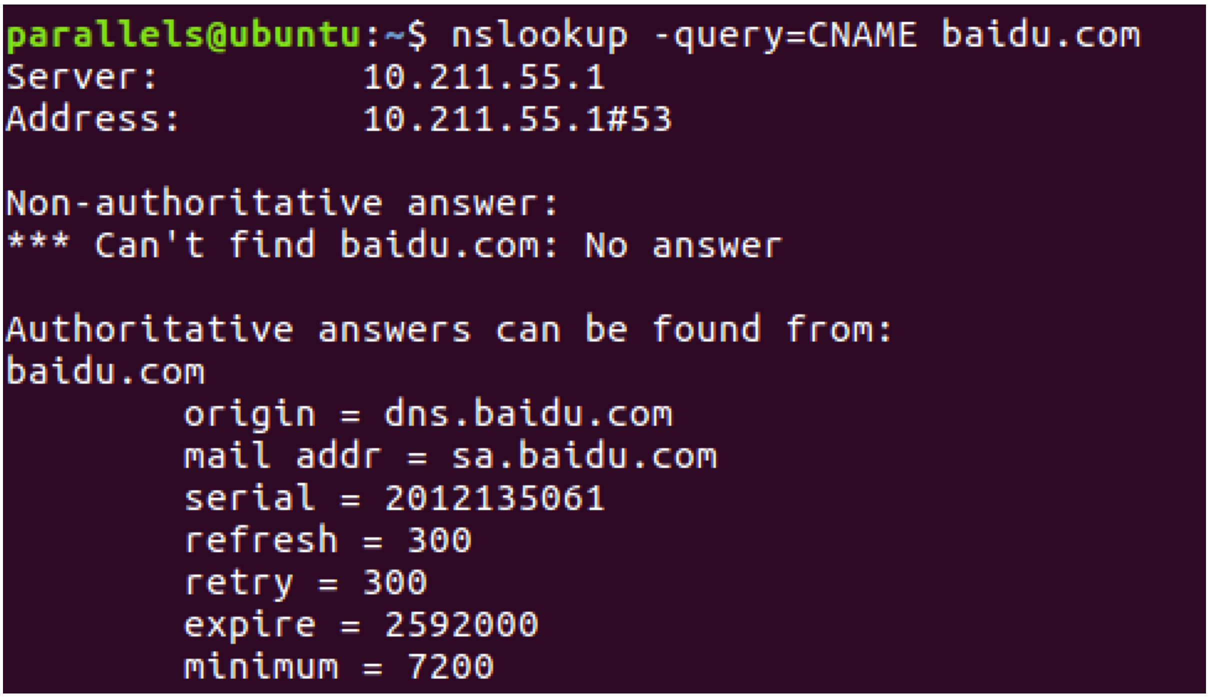
```
▸ Frame 1: 69 bytes on wire (552 bits), 69 bytes captured (552 bits) on interface 0
▸ Ethernet II, Src: Parallel_19:bd:aa (00:1c:42:19:bd:aa), Dst: Parallel_00:00:18 (00:1c:42:00:00:18)
▸ Internet Protocol Version 4, Src: 10.211.55.5, Dst: 10.211.55.1
▾ User Datagram Protocol, Src Port: 46319 (46319), Dst Port: 53 (53)
    Source Port: 46319
    Destination Port: 53
    Length: 35
  ▸ Checksum: 0x83e0 [validation disabled]
    [Stream index: 0]
▾ Domain Name System (query)
    [Response In: 2]
    Transaction ID: 0x51b0
  ▾ 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
    ▾ baidu.com: type NS, class IN
        Name: baidu.com
        [Name Length: 9]
        [Label Count: 2]
        Type: NS (authoritative Name Server) (2)
        Class: IN (0x0001)
```



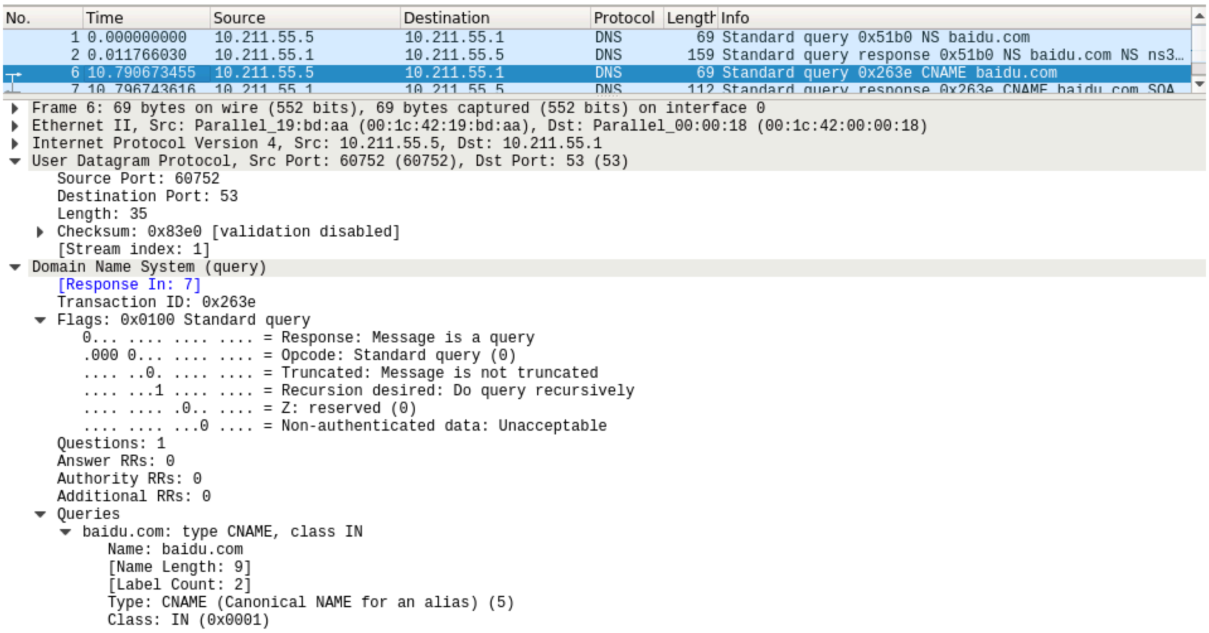
```
No.   Time          Source        Destination   Protocol Length Info
    1 0.000000000   10.211.55.5   10.211.55.1   DNS        69 Standard query 0x51b0 NS baidu.com
    2 0.011766030   10.211.55.1   10.211.55.5   DNS       159 Standard query response 0x51b0 NS baidu.com NS ns3…
    6 10.790673455  10.211.55.5   10.211.55.1   DNS        69 Standard query 0x263e CNAME baidu.com
    7 10.796743616  10.211.55.1   10.211.55.5   DNS       112 Standard query response 0x263e CNAME baidu.com SOA
```

```
▶ Frame 2: 159 bytes on wire (1272 bits), 159 bytes captured (1272 bits) on interface 0
▶ Ethernet II, Src: Parallel_00:00:18 (00:1c:42:00:00:18), Dst: Parallel_19:bd:aa (00:1c:42:19:bd:aa)
▶ Internet Protocol Version 4, Src: 10.211.55.1, Dst: 10.211.55.5
▼ User Datagram Protocol, Src Port: 53 (53), Dst Port: 46319 (46319)
    Source Port: 53
    Destination Port: 46319
    Length: 125
  ▶ Checksum: 0xdf8c [validation disabled]
    [Stream index: 0]
▼ Domain Name System (response)
    [Request In: 1]
    [Time: 0.011766030 seconds]
    Transaction ID: 0x51b0
  ▼ 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: 5
    Authority RRs: 0
    Additional RRs: 0
  ▼ Queries
    ▼ baidu.com: type NS, class IN
        Name: baidu.com
        [Name Length: 9]
        [Label Count: 2]
        Type: NS (authoritative Name Server) (2)
        Class: IN (0x0001)
  ▼ Answers
    ▼ baidu.com: type NS, class IN, ns ns3.baidu.com
        Name: baidu.com
        Type: NS (authoritative Name Server) (2)
        Class: IN (0x0001)
```

2) TYPE=CNAME

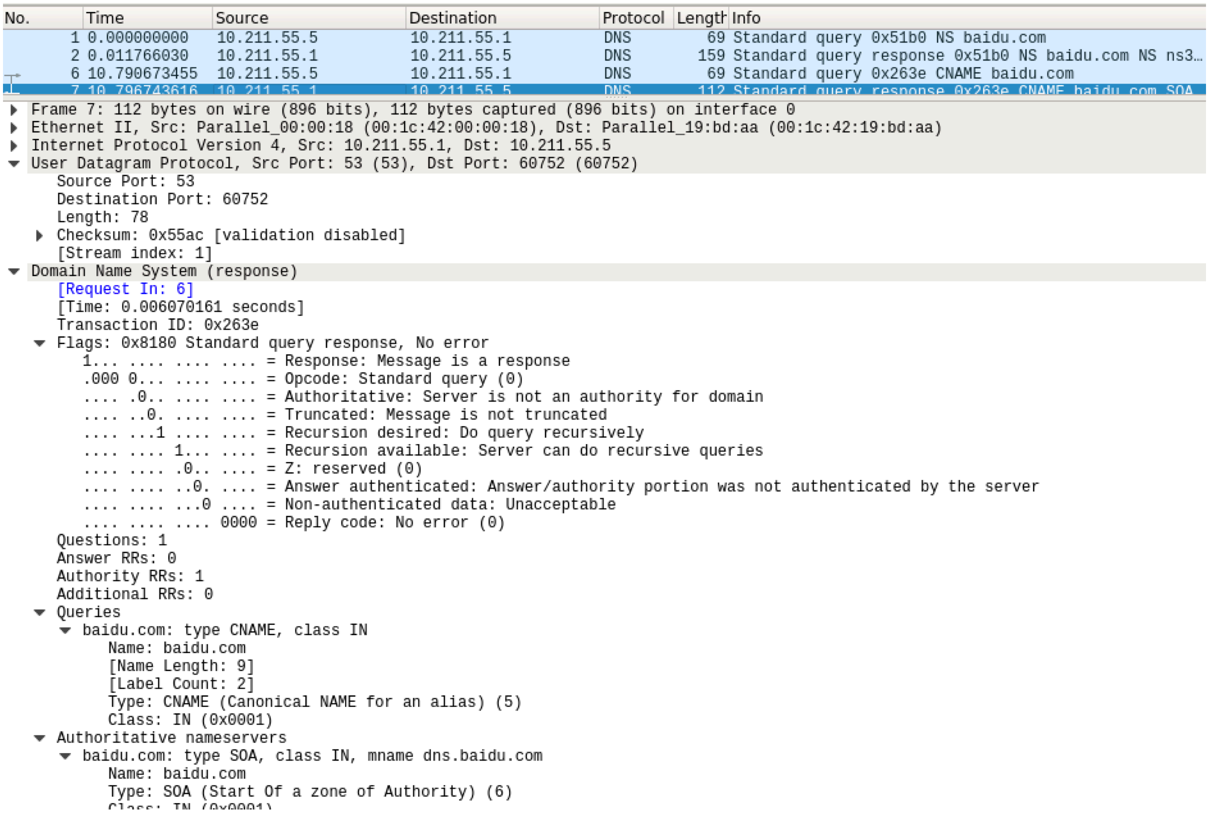


```
parallels@ubuntu:~$ nslookup -query=CNAME baidu.com
Server:         10.211.55.1
Address:        10.211.55.1#53

Non-authoritative answer:
*** Can't find baidu.com: No answer

Authoritative answers can be found from:
baidu.com
        origin = dns.baidu.com
        mail addr = sa.baidu.com
        serial = 2012135061
        refresh = 300
        retry = 300
        expire = 2592000
        minimum = 7200
```



```
No.   Time            Source          Destination     Protocol Length Info
    1 0.000000000     10.211.55.5     10.211.55.1     DNS       69 Standard query 0x51b0 NS baidu.com
    2 0.011766030     10.211.55.1     10.211.55.5     DNS      159 Standard query response 0x51b0 NS baidu.com NS ns3…
    6 10.790673455    10.211.55.5     10.211.55.1     DNS       69 Standard query 0x263e CNAME baidu.com
    7 10.796743616    10.211.55.1     10.211.55.5     DNS      112 Standard query response 0x263e CNAME baidu.com SOA
```

```
▸ Frame 6: 69 bytes on wire (552 bits), 69 bytes captured (552 bits) on interface 0
▸ Ethernet II, Src: Parallel_19:bd:aa (00:1c:42:19:bd:aa), Dst: Parallel_00:00:18 (00:1c:42:00:00:18)
▸ Internet Protocol Version 4, Src: 10.211.55.5, Dst: 10.211.55.1
▾ User Datagram Protocol, Src Port: 60752 (60752), Dst Port: 53 (53)
    Source Port: 60752
    Destination Port: 53
    Length: 35
  ▸ Checksum: 0x83e0 [validation disabled]
    [Stream index: 1]
▾ Domain Name System (query)
    [Response In: 7]
    Transaction ID: 0x263e
  ▾ 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
    ▾ baidu.com: type CNAME, class IN
        Name: baidu.com
        [Name Length: 9]
        [Label Count: 2]
        Type: CNAME (Canonical NAME for an alias) (5)
        Class: IN (0x0001)
```



```
No.   Time            Source          Destination     Protocol Length Info
    1 0.000000000     10.211.55.5     10.211.55.1     DNS       69 Standard query 0x51b0 NS baidu.com
    2 0.011766030     10.211.55.1     10.211.55.5     DNS      159 Standard query response 0x51b0 NS baidu.com NS ns3…
    6 10.790673455    10.211.55.5     10.211.55.1     DNS       69 Standard query 0x263e CNAME baidu.com
    7 10.796743616    10.211.55.1     10.211.55.5     DNS      112 Standard query response 0x263e CNAME baidu.com SOA
```

```
▸ Frame 7: 112 bytes on wire (896 bits), 112 bytes captured (896 bits) on interface 0
▸ Ethernet II, Src: Parallel_00:00:18 (00:1c:42:00:00:18), Dst: Parallel_19:bd:aa (00:1c:42:19:bd:aa)
▸ Internet Protocol Version 4, Src: 10.211.55.1, Dst: 10.211.55.5
▾ User Datagram Protocol, Src Port: 53 (53), Dst Port: 60752 (60752)
    Source Port: 53
    Destination Port: 60752
    Length: 78
  ▸ Checksum: 0x55ac [validation disabled]
    [Stream index: 1]
▾ Domain Name System (response)
    [Request In: 6]
    [Time: 0.006070161 seconds]
    Transaction ID: 0x263e
  ▾ 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
  ▾ Queries
    ▾ baidu.com: type CNAME, class IN
        Name: baidu.com
        [Name Length: 9]
        [Label Count: 2]
        Type: CNAME (Canonical NAME for an alias) (5)
        Class: IN (0x0001)
  ▾ Authoritative nameservers
    ▾ baidu.com: type SOA, class IN, mname dns.baidu.com
        Name: baidu.com
        Type: SOA (Start Of a zone of Authority) (6)
        Class: IN (0x0001)
```