Capture DHCP&DNS Packets and Analysis

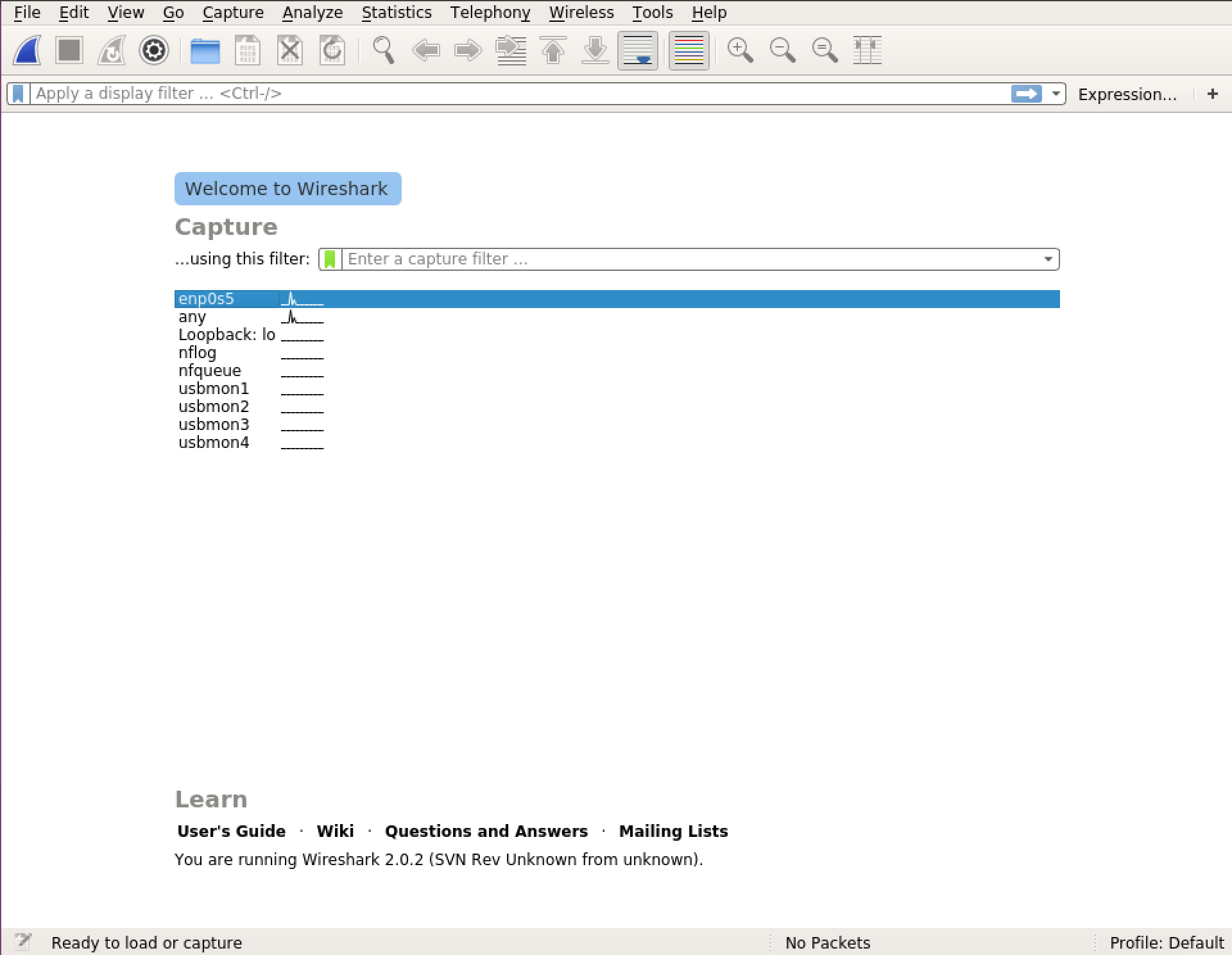
Name: Ou Yihang

Class: 2014215104

BUPT Student ID: 2014212948

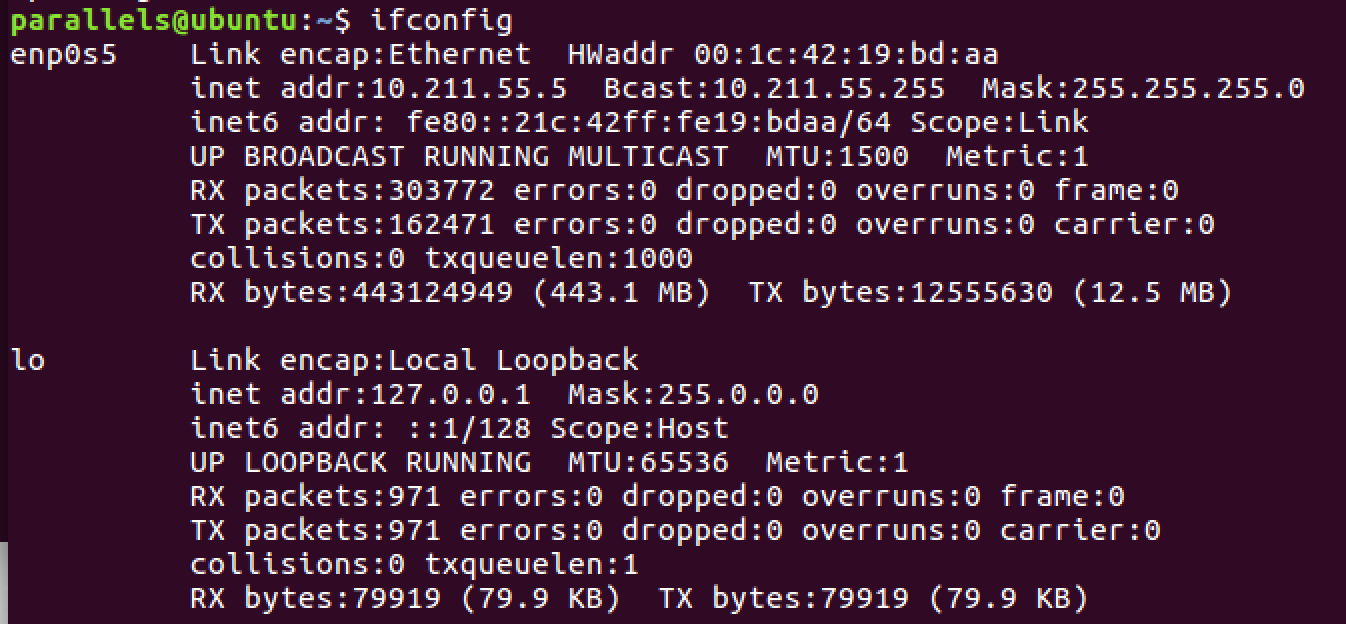
QM Student ID: 140919433

1. The configuration of Wireshark
2. Using the command “scp –X student@192.168.56.101” to connect the physical machine and virtual machine.
3. Using the command “sudo wireshark” then input the password to start the wireshark, then this will be show in the screen.



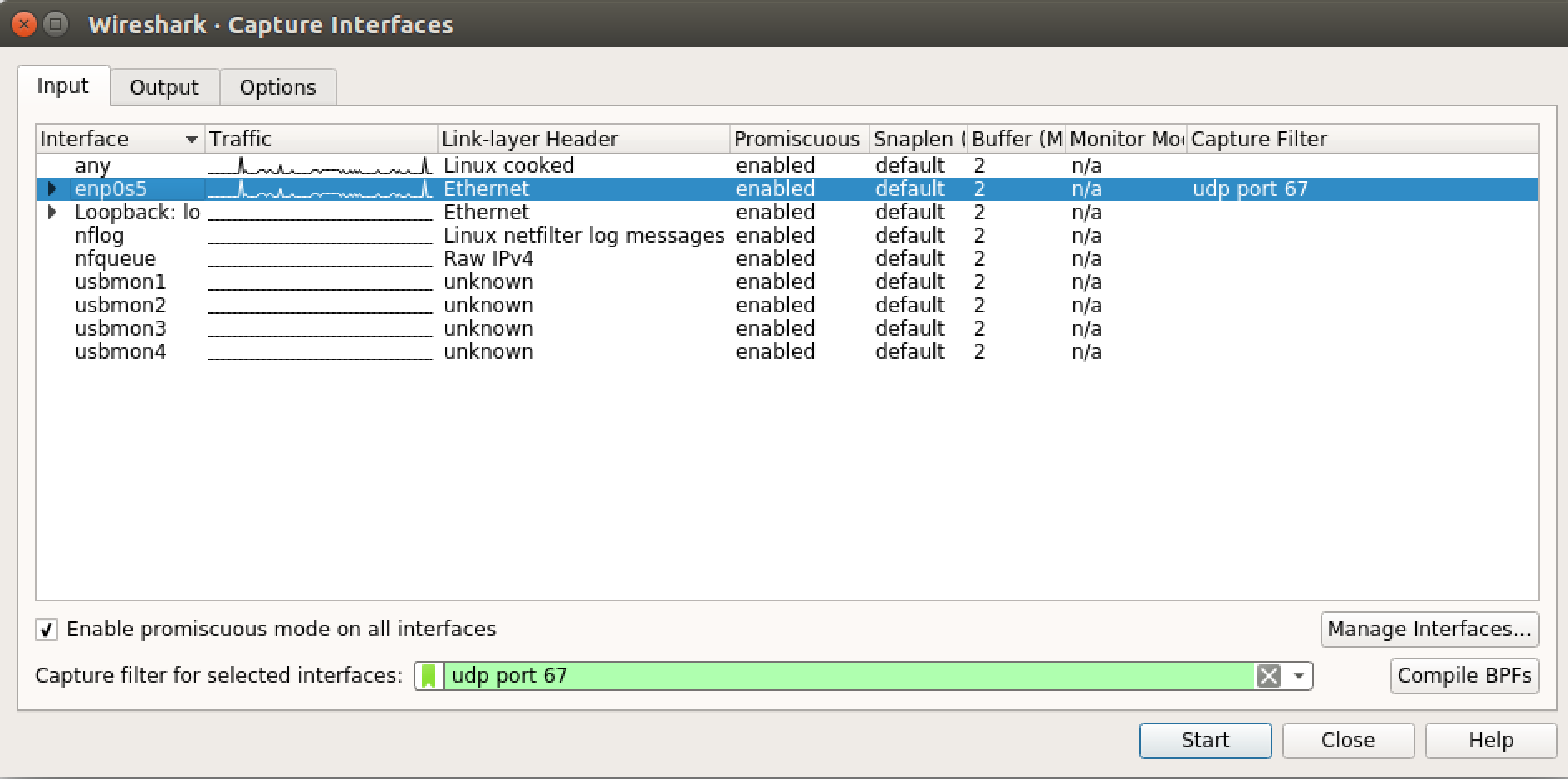
from this picture, there are 2 network is available.

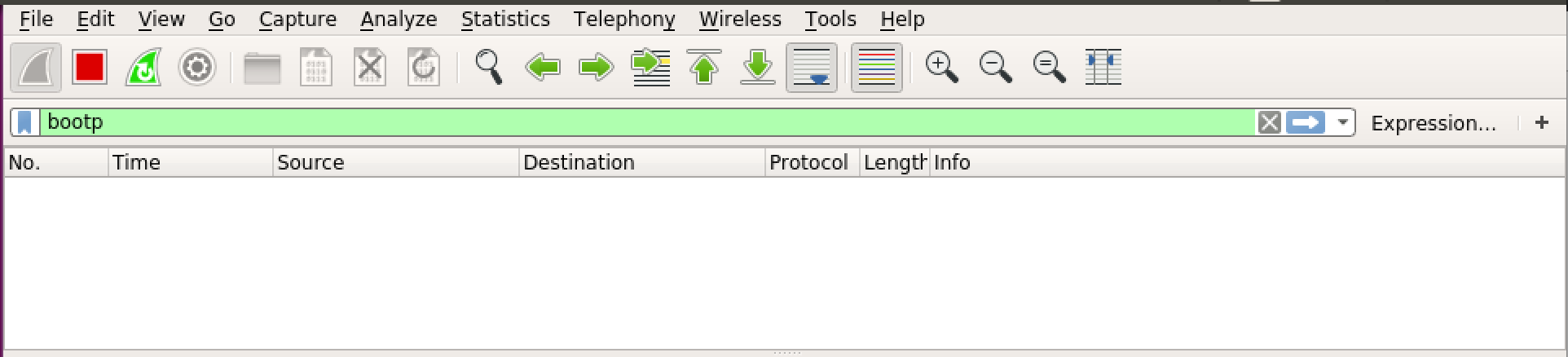
Using the “ifconfig” to check the network status, then you could know the network “enp0s5” could use for capture packet.



1. Capture DHCP packet

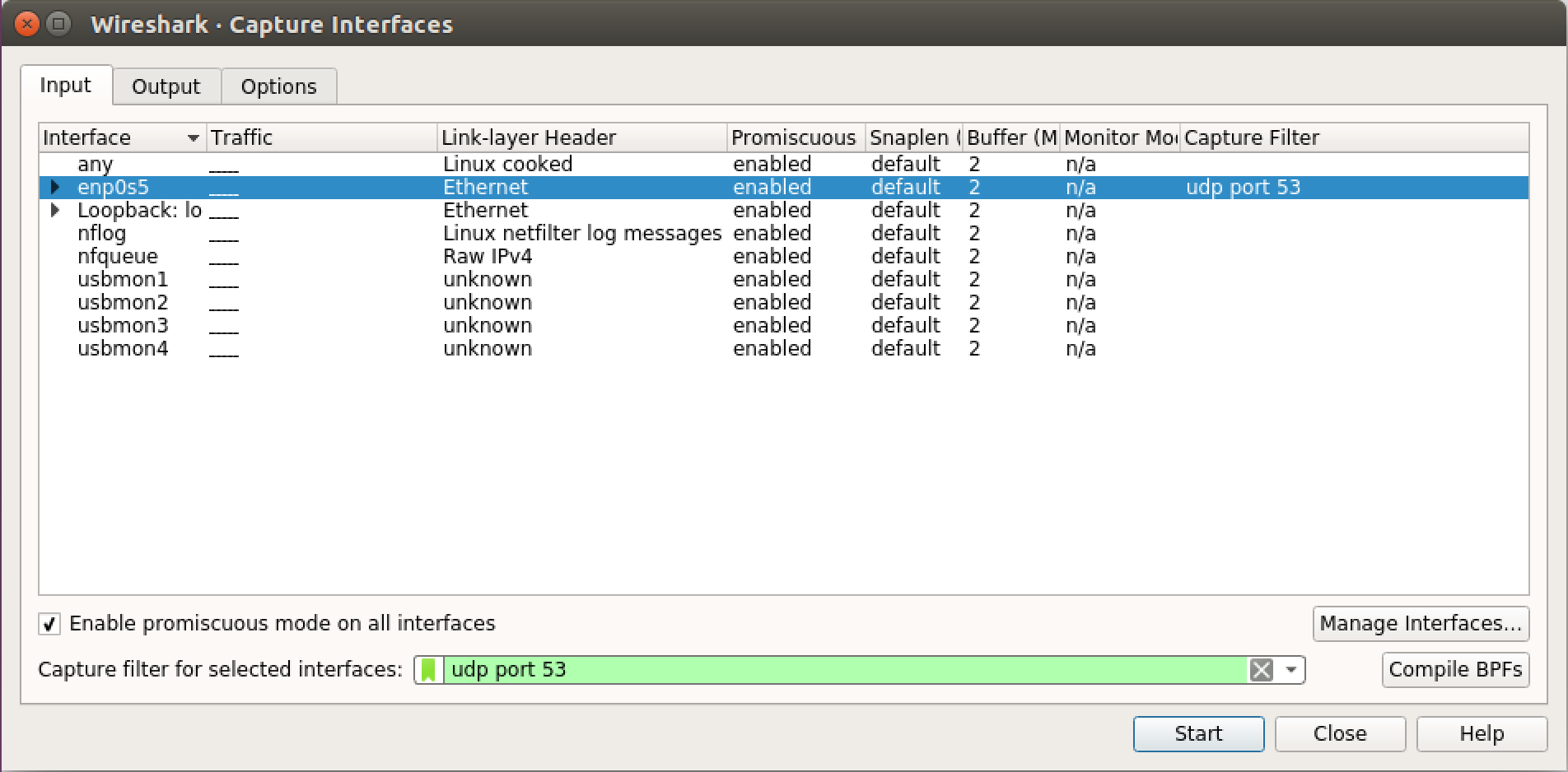
To capture DHCP packet, use “udp port 67” as capture filter, click “click”, use” bootp” to display filter.

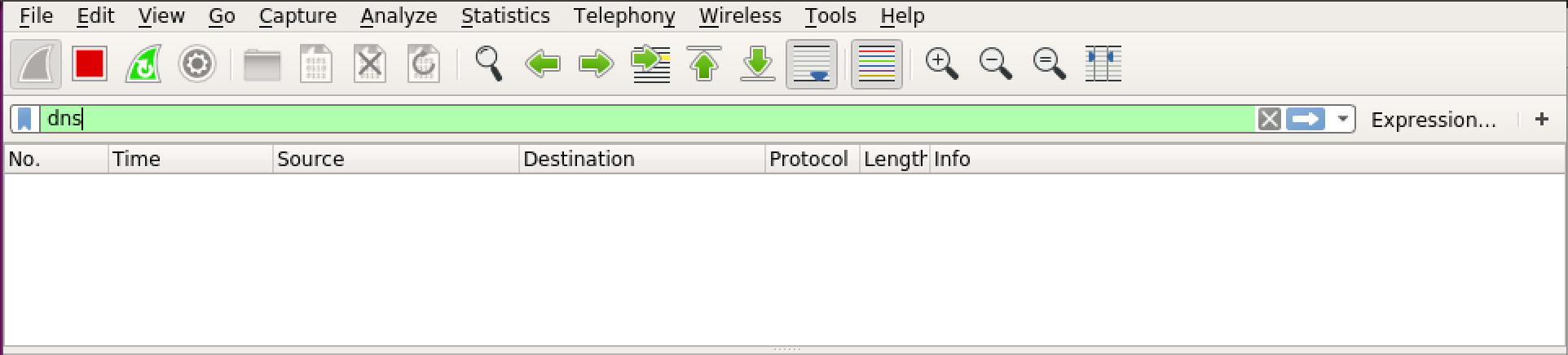




1. Capture DNS packet

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

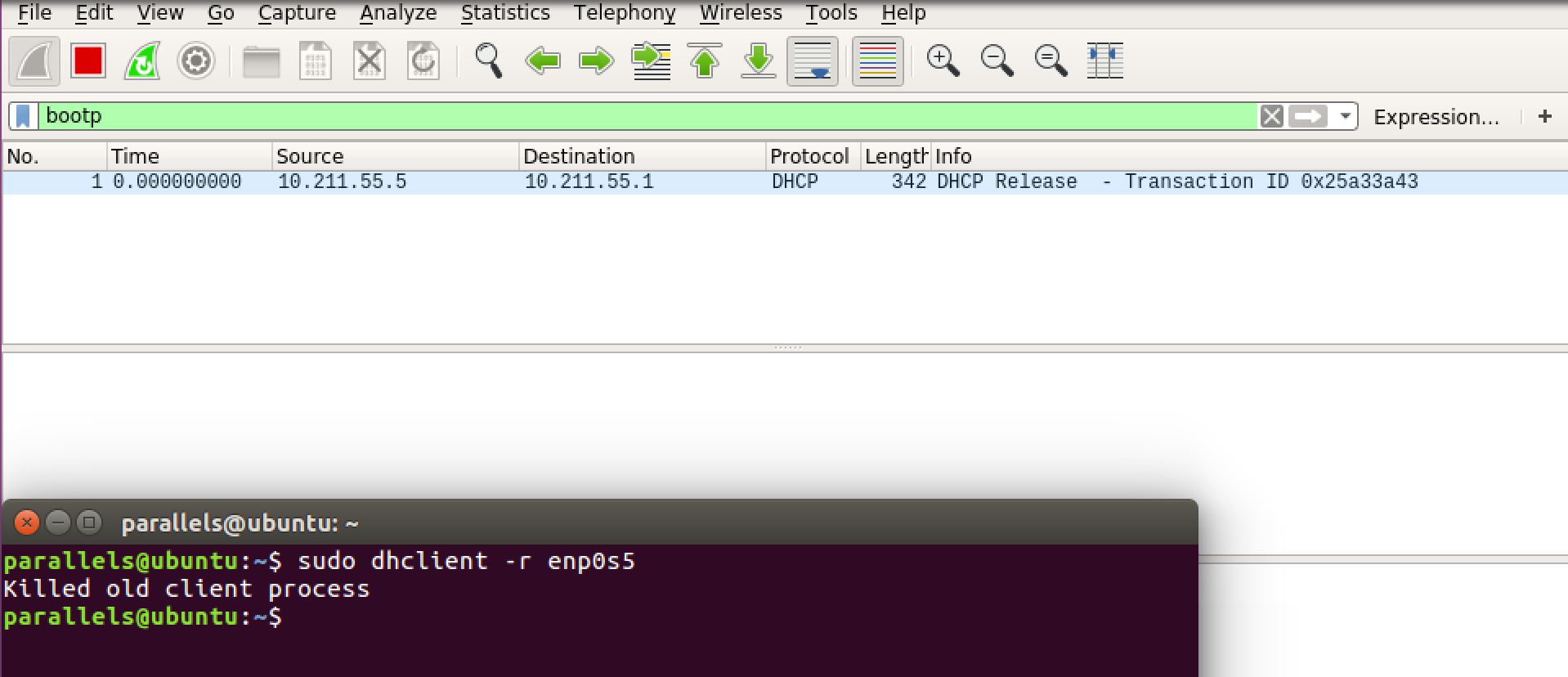




1. The result of DHCP capture and packet analysis
2. Capture packet

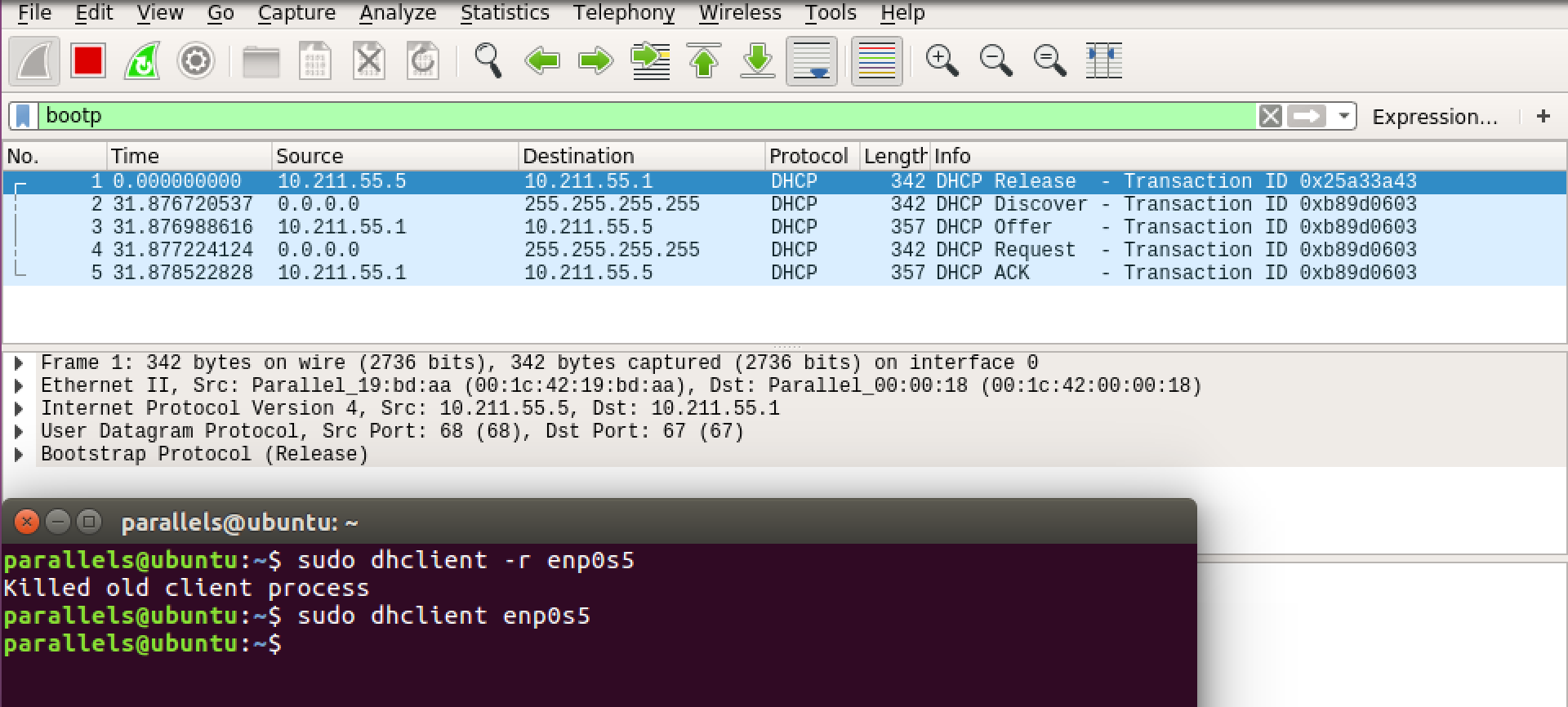
After configure the wireshark, we start the DHCP packet capture.

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



from this picture, we get the DHCP Release packet.

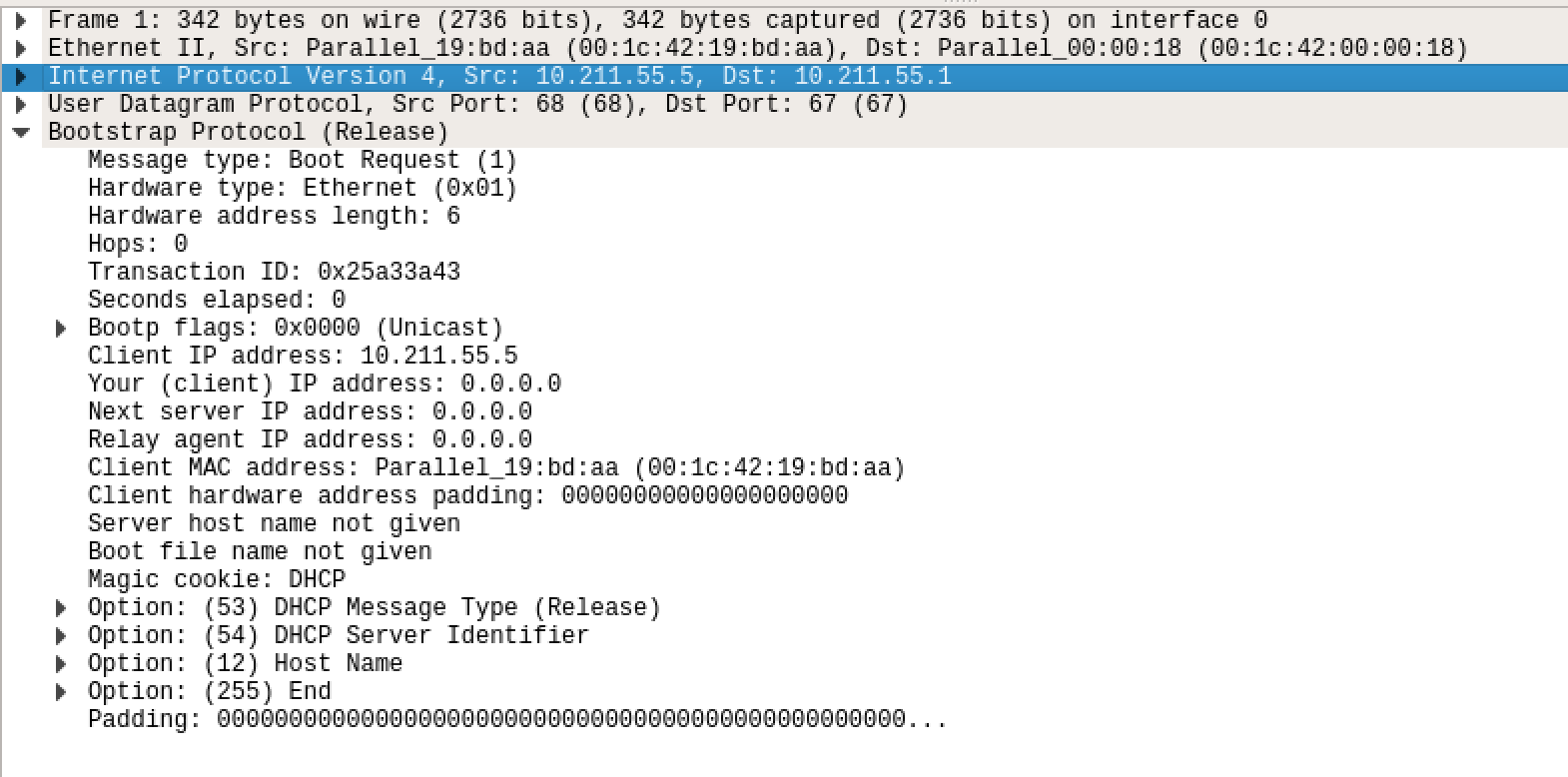
Use the “sudo dhclient enp0s5”to initial the DHCP connection.



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

1. Packet analysis

* DHCP release Packet



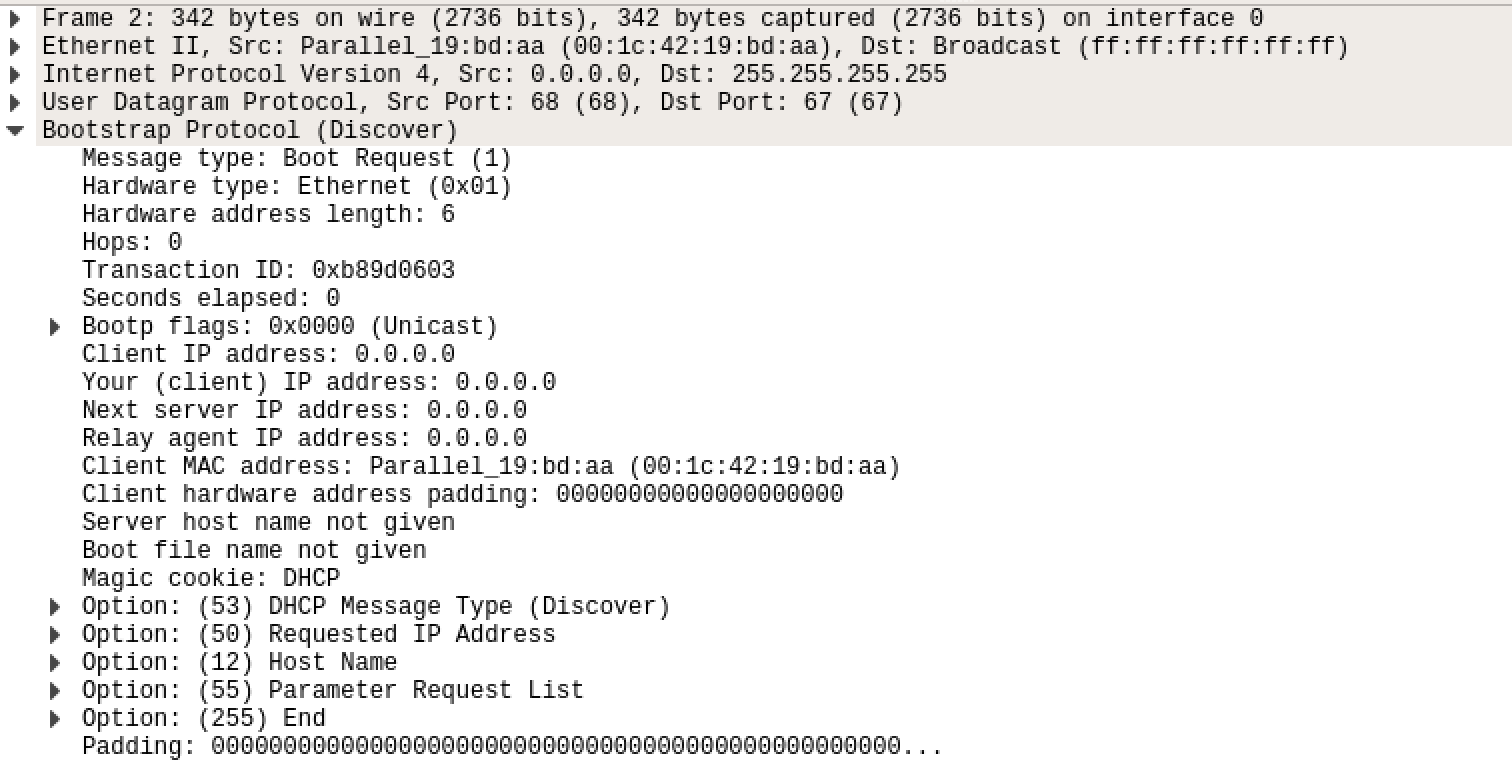
1. Critical parameters and explanation

|  |  |  |
| --- | --- | --- |
| 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 |

1. 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



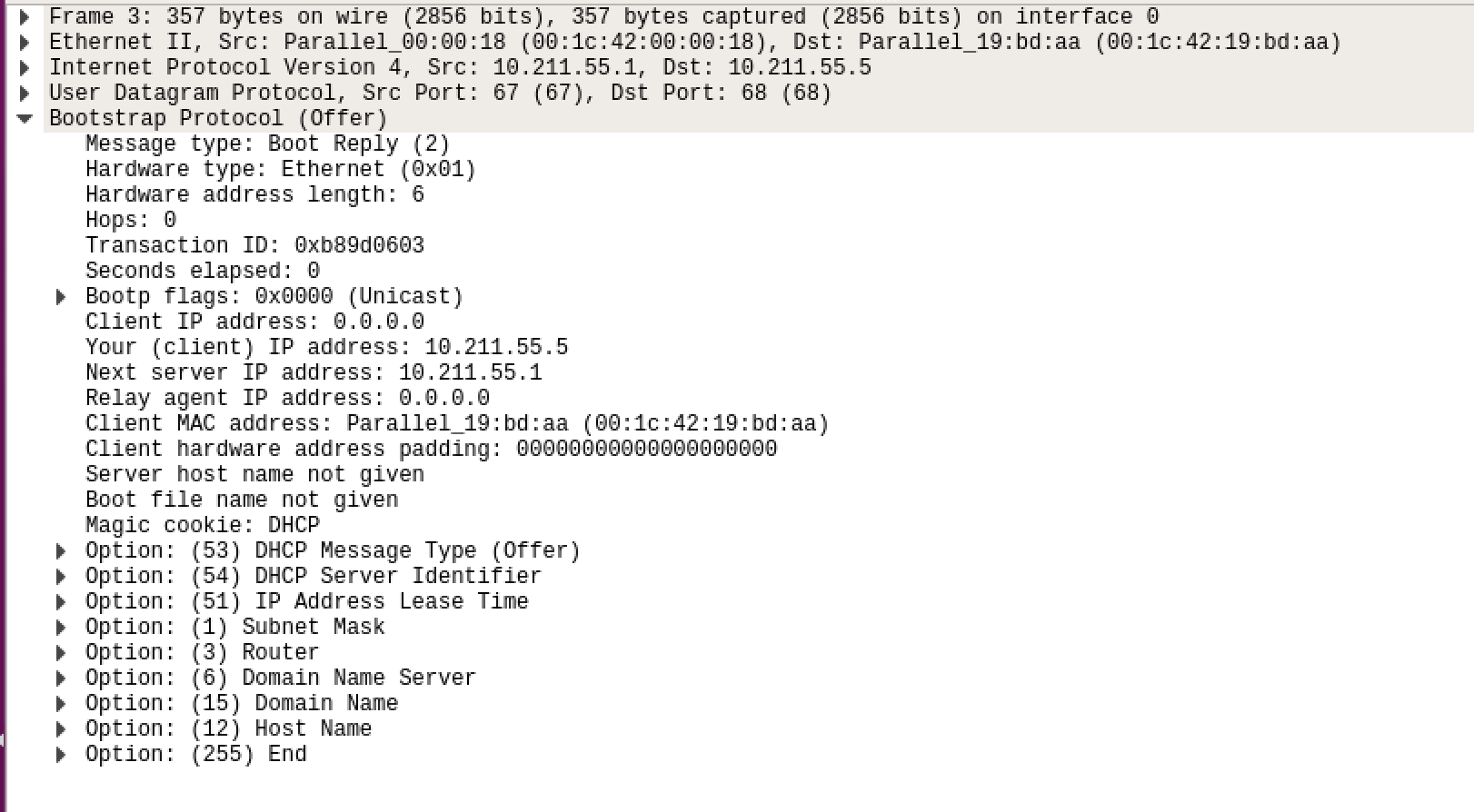
1. Critical parameters and explanation

|  |  |  |
| --- | --- | --- |
| 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.) |

1. 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



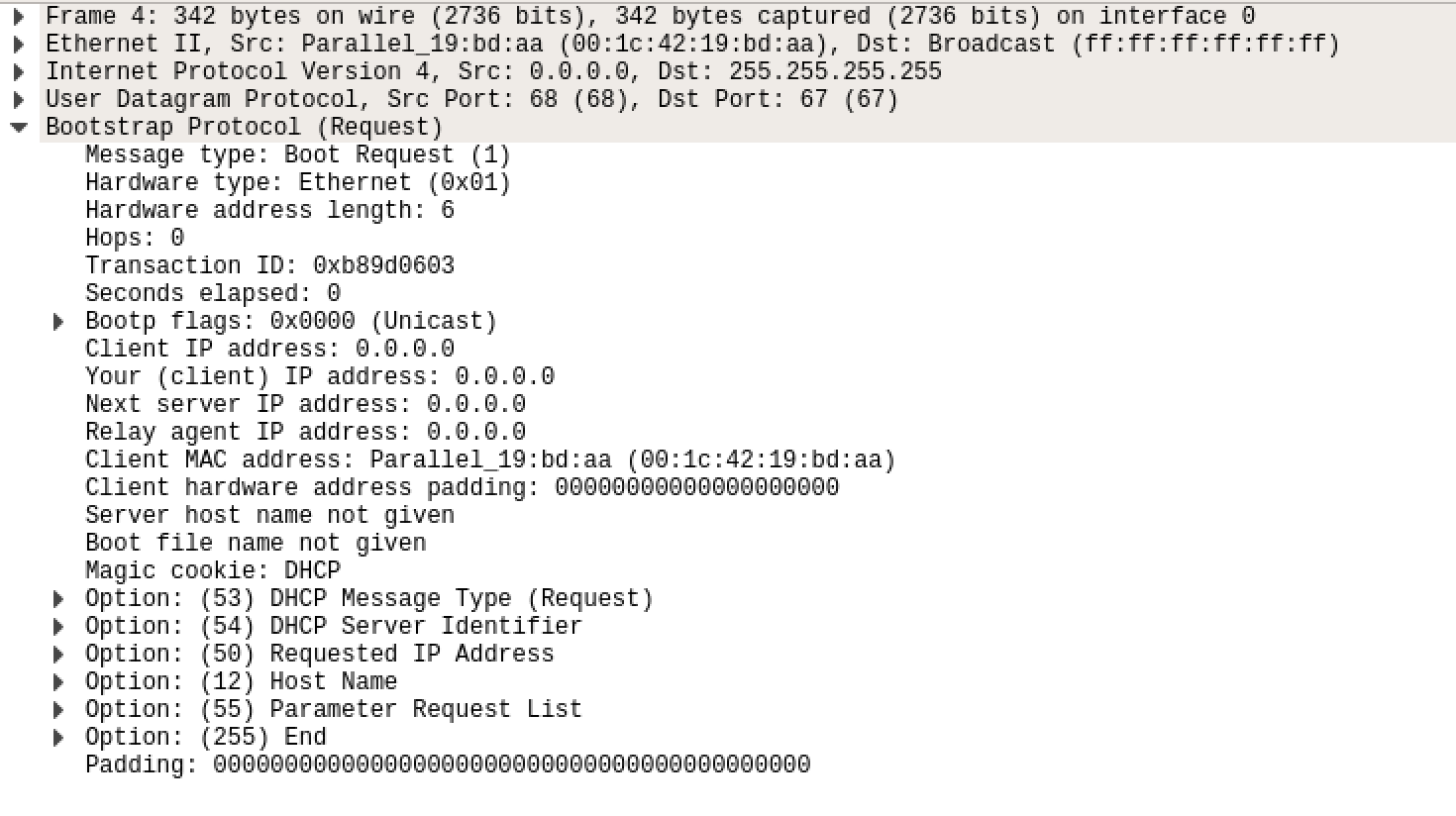
1. Critical parameters and explanation

|  |  |  |
| --- | --- | --- |
| 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 |

1. 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



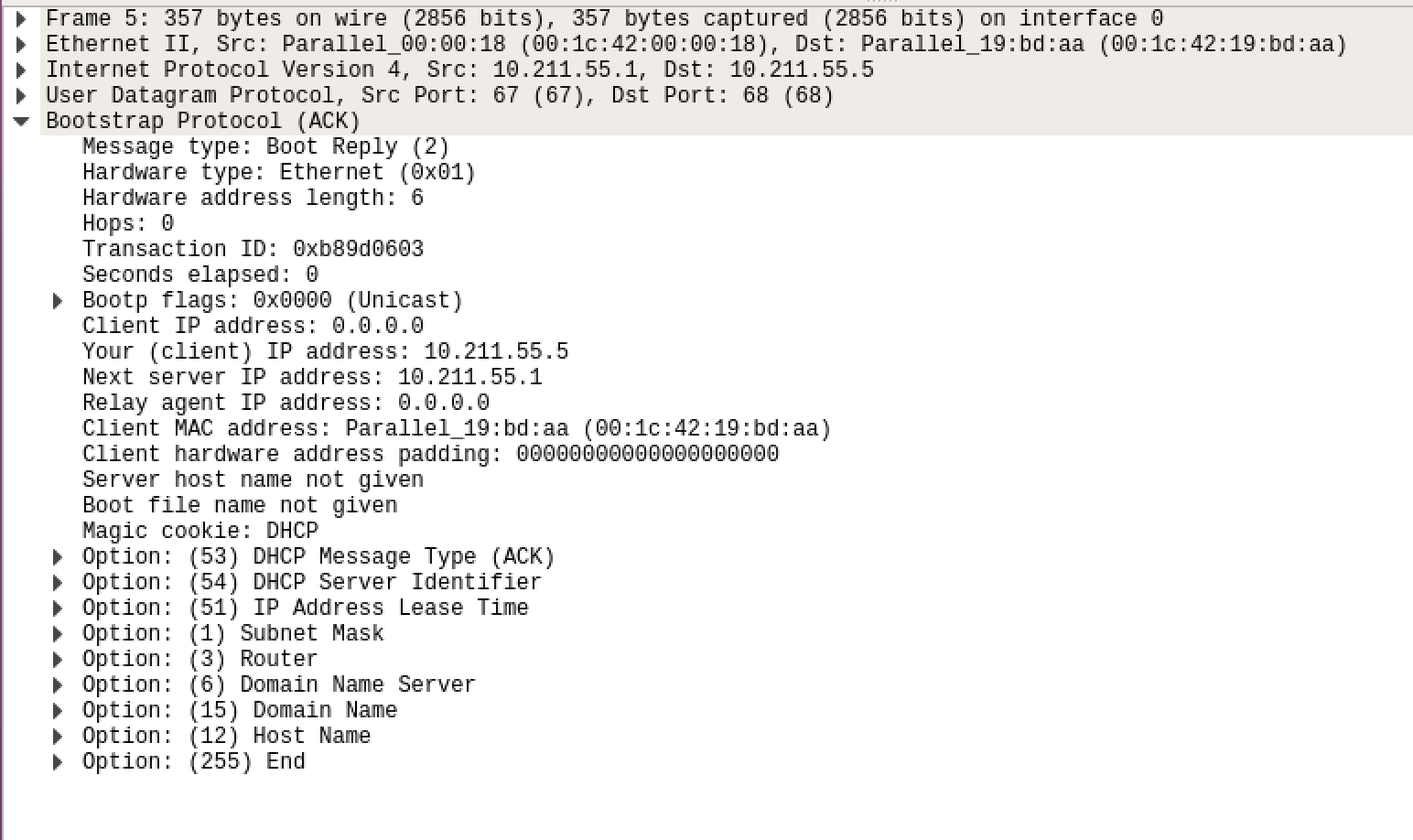
1. Critical parameters and explanation

|  |  |  |
| --- | --- | --- |
| 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.) |

1. 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



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 |

1. 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.

1. 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.

1. 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 | |

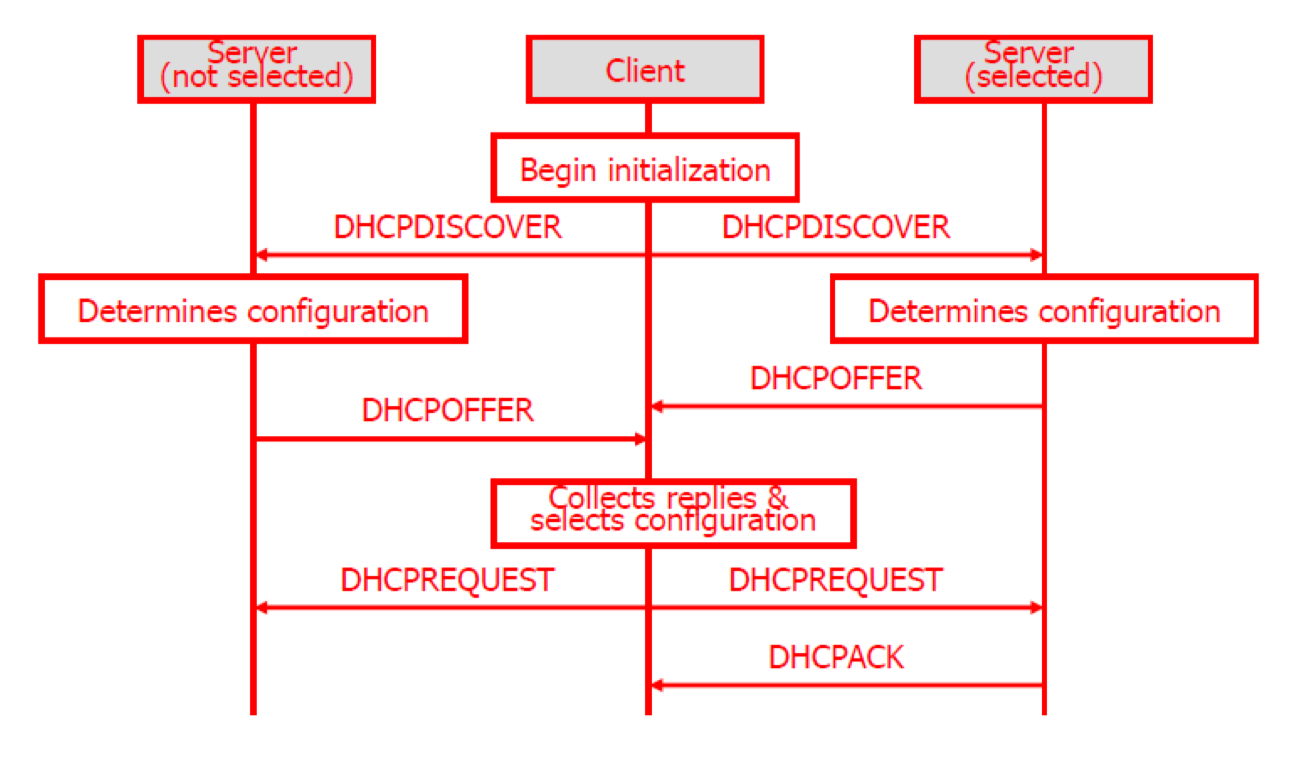
Except for the transaction ID and the mac address, all fields are the same.

1. Frame No.4 (ACK)

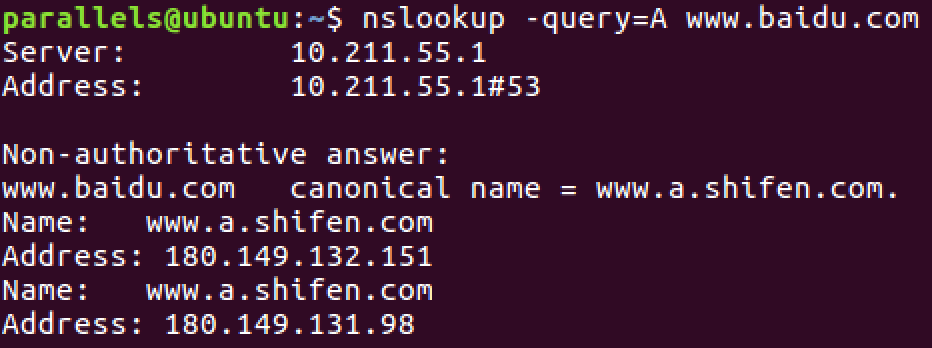
|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| My Message | | | | | | Example in lecture notes | | | | | |
| 2 | 1 | | 6 | | 0 | 2 | 1 | | 6 | | 0 |
| 12 | | | | | | 12 | | | | | |
| 0 | | | Flags | | | 0 | | | Flags | | |
| 0 | | | | | | 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 | |

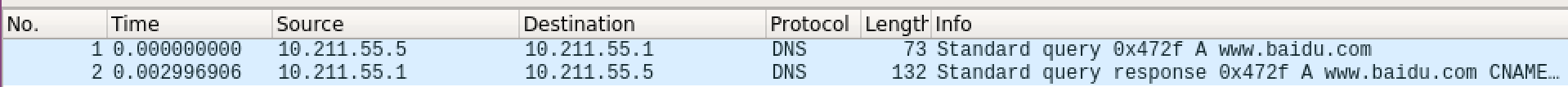
Only the transaction ID, your IP address, the next server IP address and the mac address are not the same as the example in lecture notes.

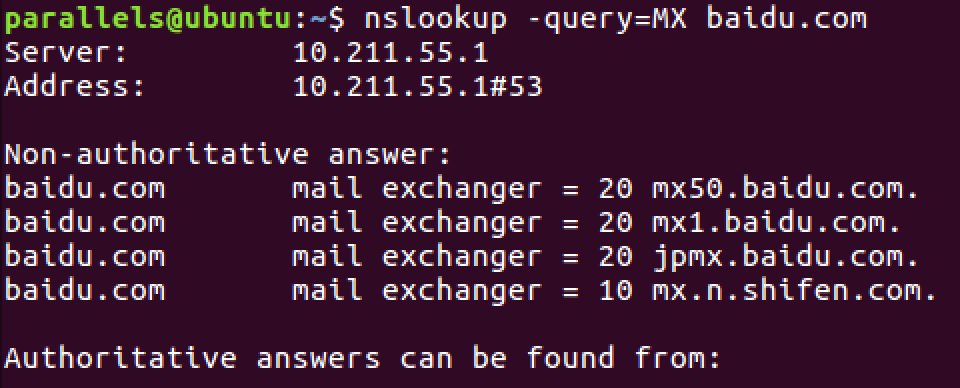
* Message Sequence Chart (MSC)

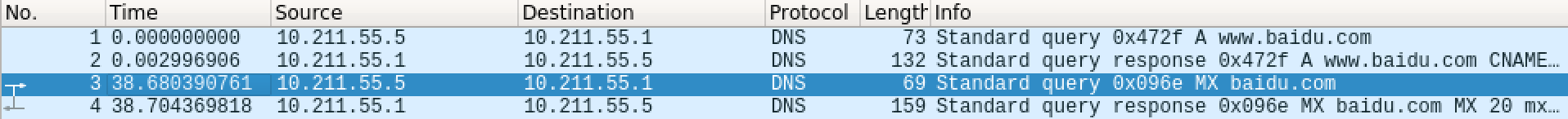


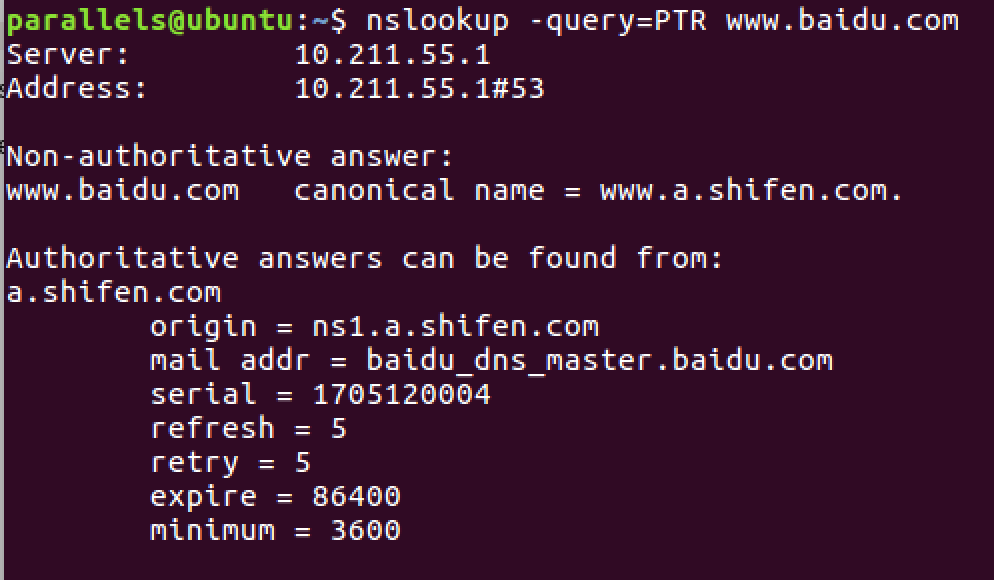
1. The result of DNS capture
2. Capture Packet

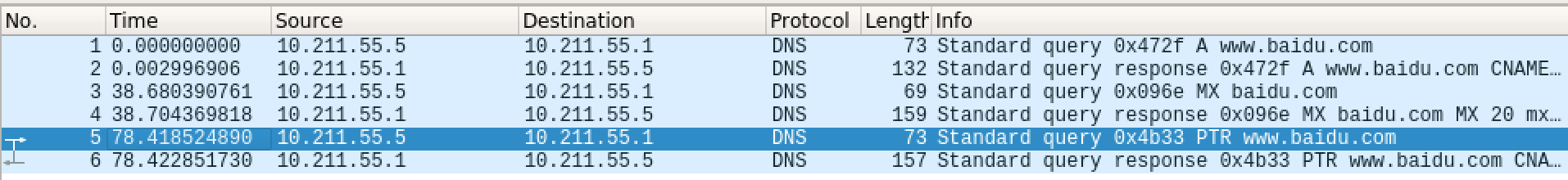




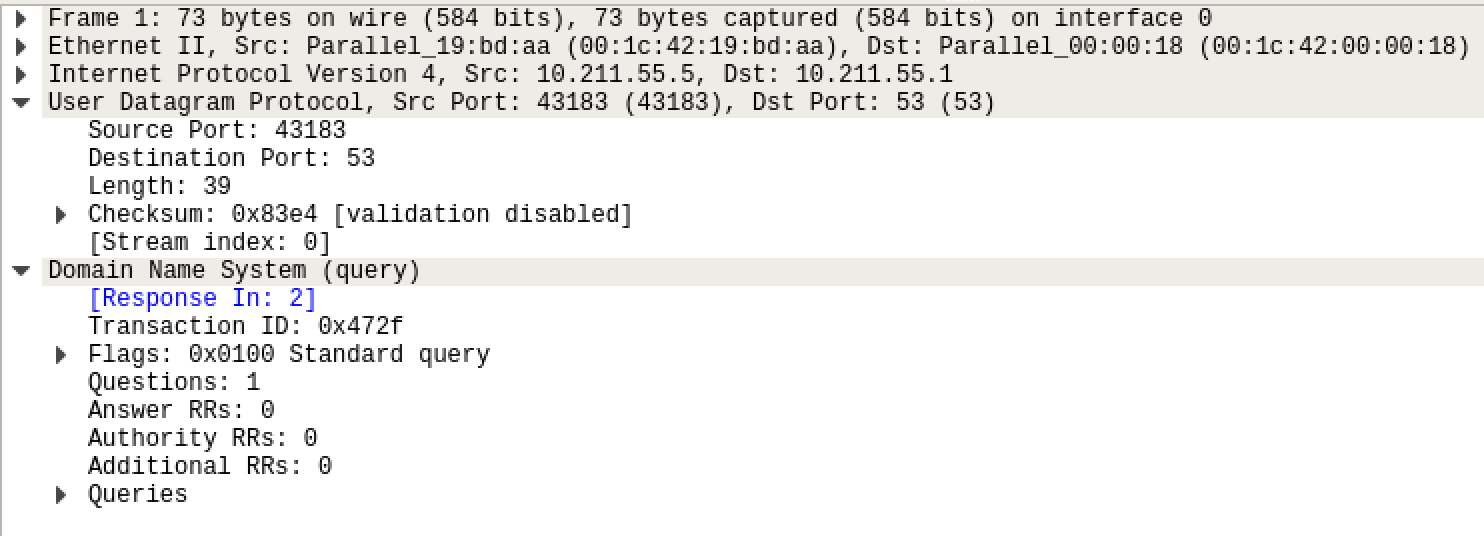




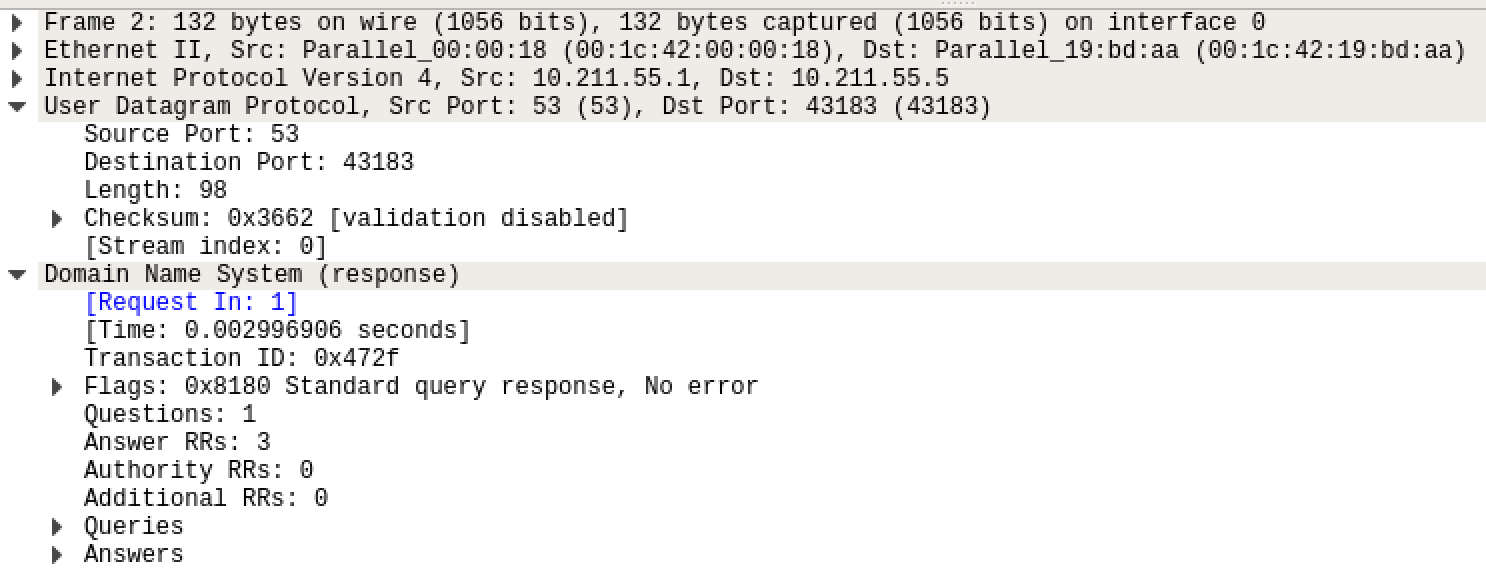




1. Packet analysis
2. DNS Query Type=A

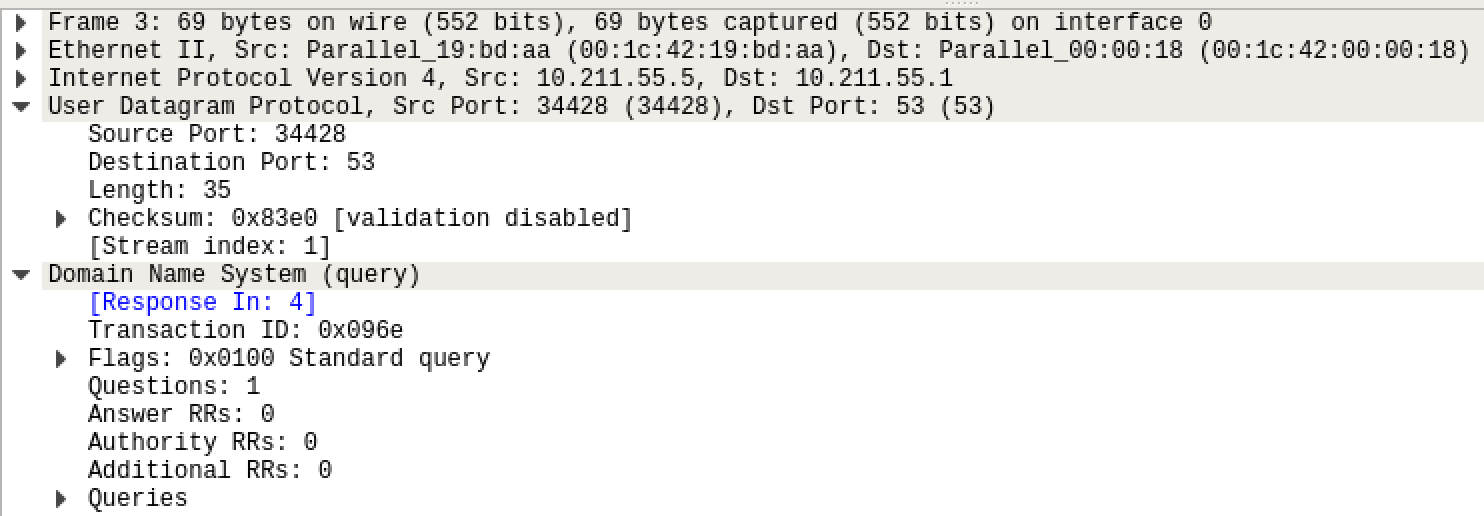


|  |  |  |  |
| --- | --- | --- | --- |
| Critical Parameter | | Value | Explanation |
| Transaction | | 0x472f | 16-bit field used to correlate queries and responses. |
| Parameters  0x0100  Standard  Query | Response | 0… …. …. …. | 1-bit field that identifies the message as a query (0) or response (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 |

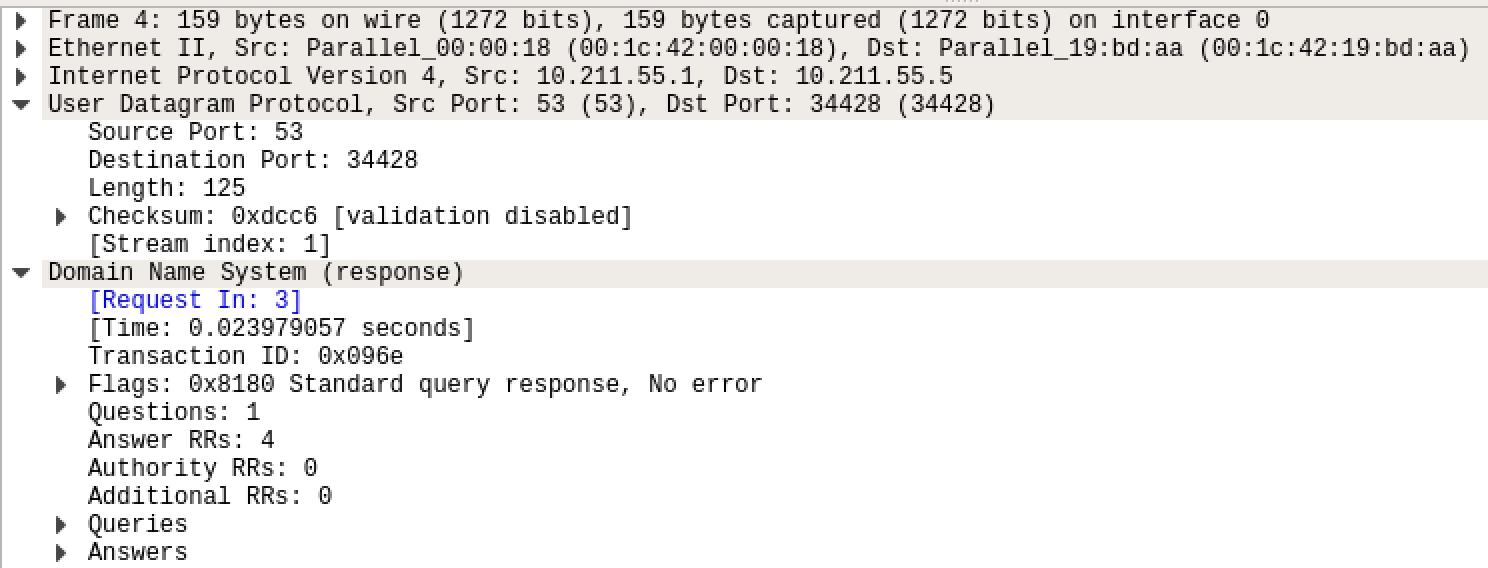


|  |  |  |  |
| --- | --- | --- | --- |
| Critical Parameter | | Value | Explanation |
| Transaction | | 0x472f | 16-bit field used to correlate queries and responses. |
| Parameters  0x0100  Standard  Query | Response | 1… …. …. …. | 1-bit field that identifies the message as a query (0) or response (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 |

1. DNS Query Response TYPE=MX

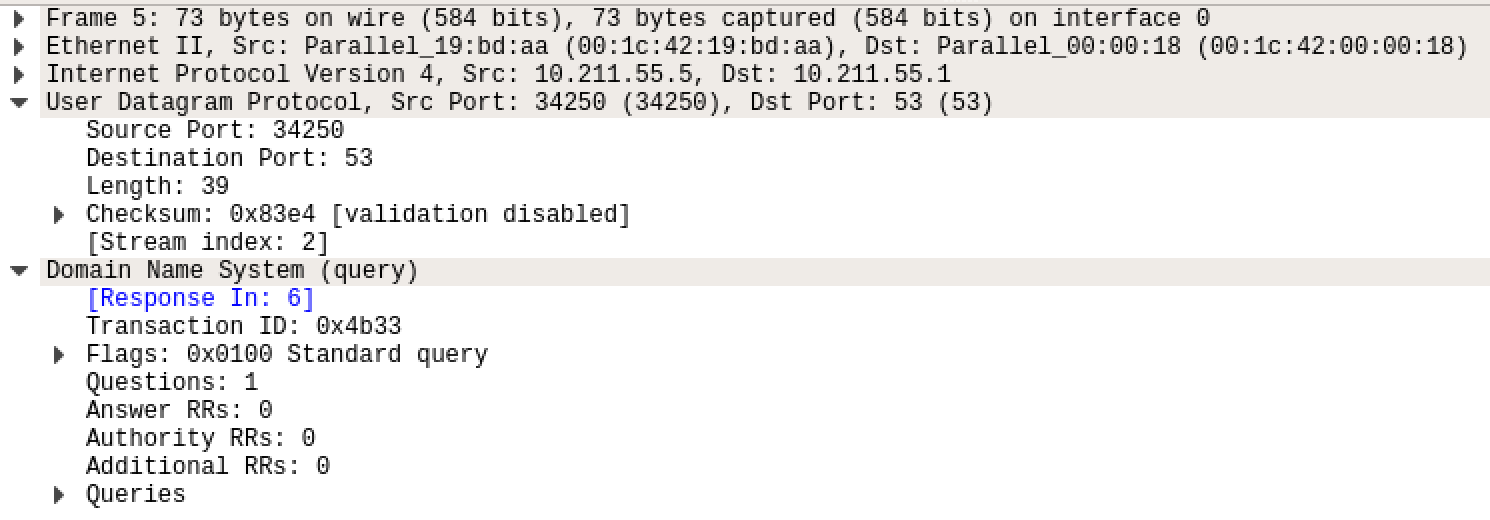


|  |  |  |  |
| --- | --- | --- | --- |
| Critical Parameter | | Value | Explanation |
| Transaction | | 0x096e | 16-bit field used to correlate queries and responses. |
| Parameters  0x0100  Standard  Query | Response | 0… …. …. …. | 1-bit field that identifies the message as a query (0) or response (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 |

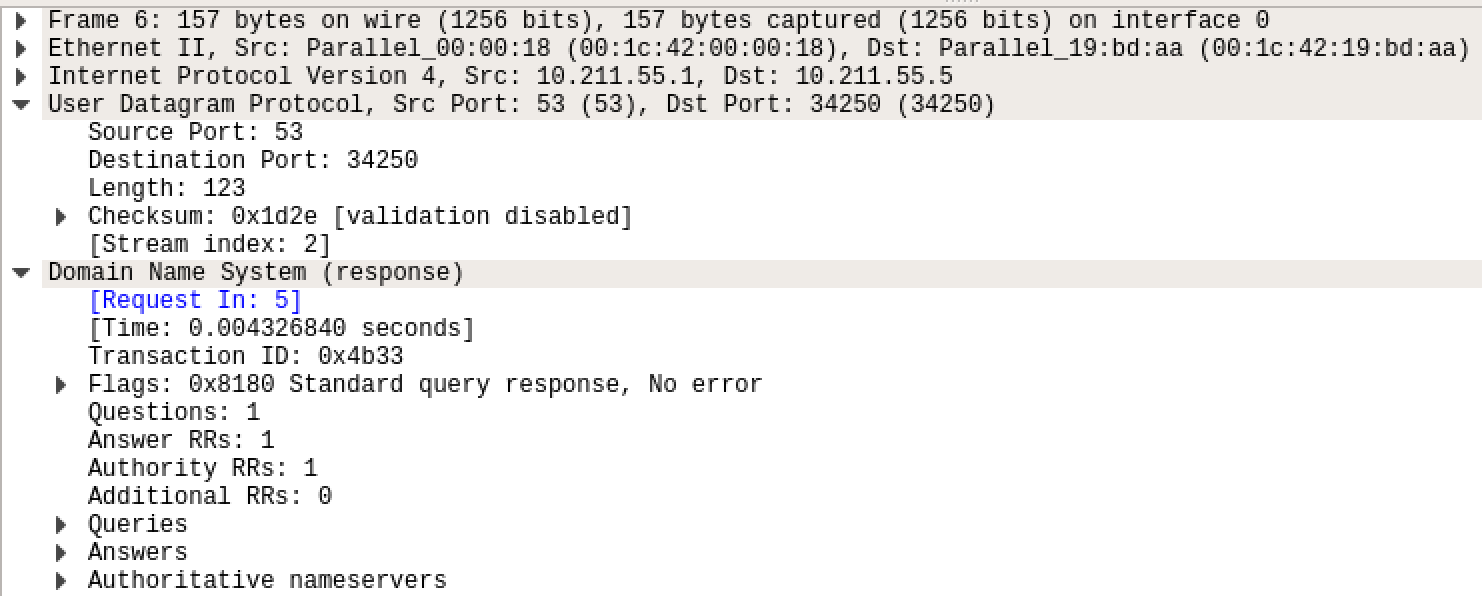


|  |  |  |  |
| --- | --- | --- | --- |
| Critical Parameter | | Value | Explanation |
| Transaction | | 0x096e | 16-bit field used to correlate queries and responses. |
| Parameters  0x0100  Standard  Query | Response | 1… …. …. …. | 1-bit field that identifies the message as a query (0) or response (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 |

1. DNS QUERY TYPE=PTR



|  |  |  |  |
| --- | --- | --- | --- |
| 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 |



|  |  |  |  |
| --- | --- | --- | --- |
| 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> |

1. 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> |

1. 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> |

1. 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> |

1. DNS Query TYPE=PTR

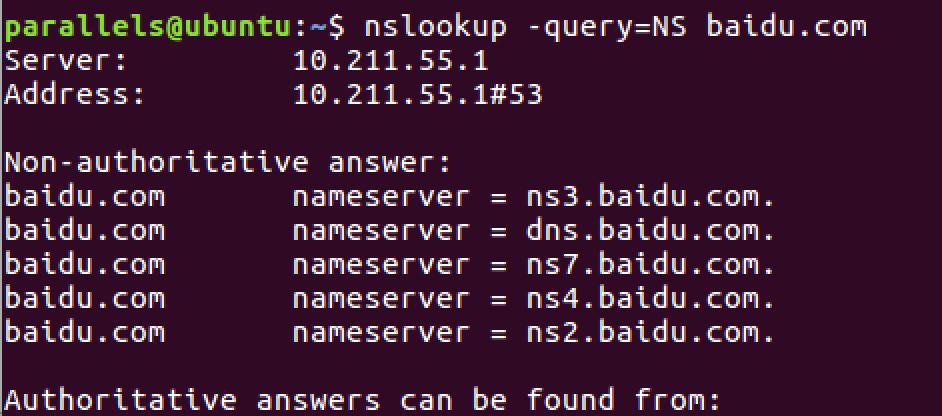
|  |  |  |
| --- | --- | --- |
|  | My Messages | Example in lecture notes |
| Header | Opcode=standard query | Opcode=standard query |
| Question | QNAME=www.baidu.com | QNAME=SRI-ARPA |
| QCLASS=IN | QCLASS=IN |
| QTYPE=PTR | QTYPE=PTR |
| Answer section | <empty> | <empty> |
| Authority section |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

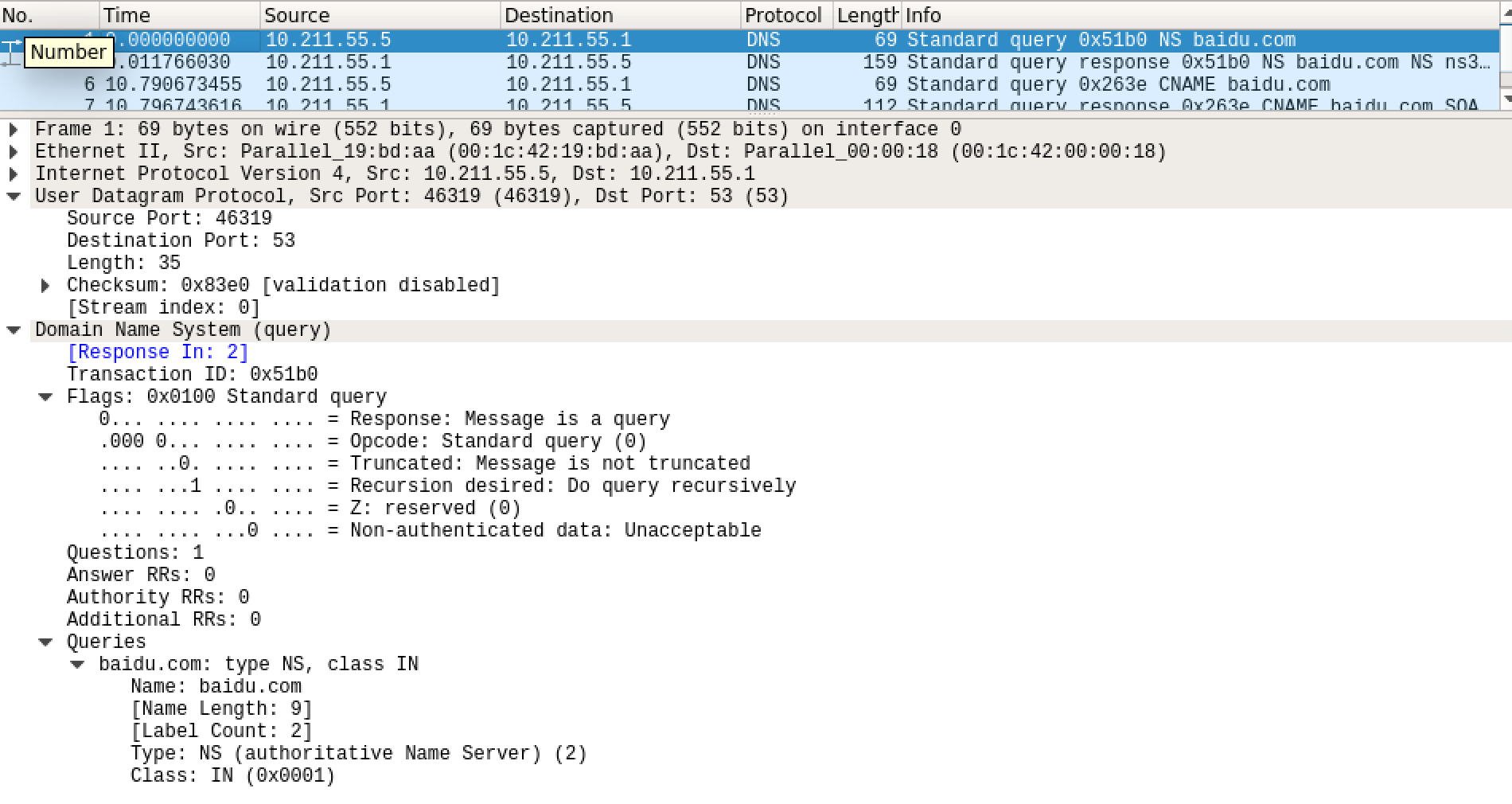
1. DNS Query Response TYPE=PTR

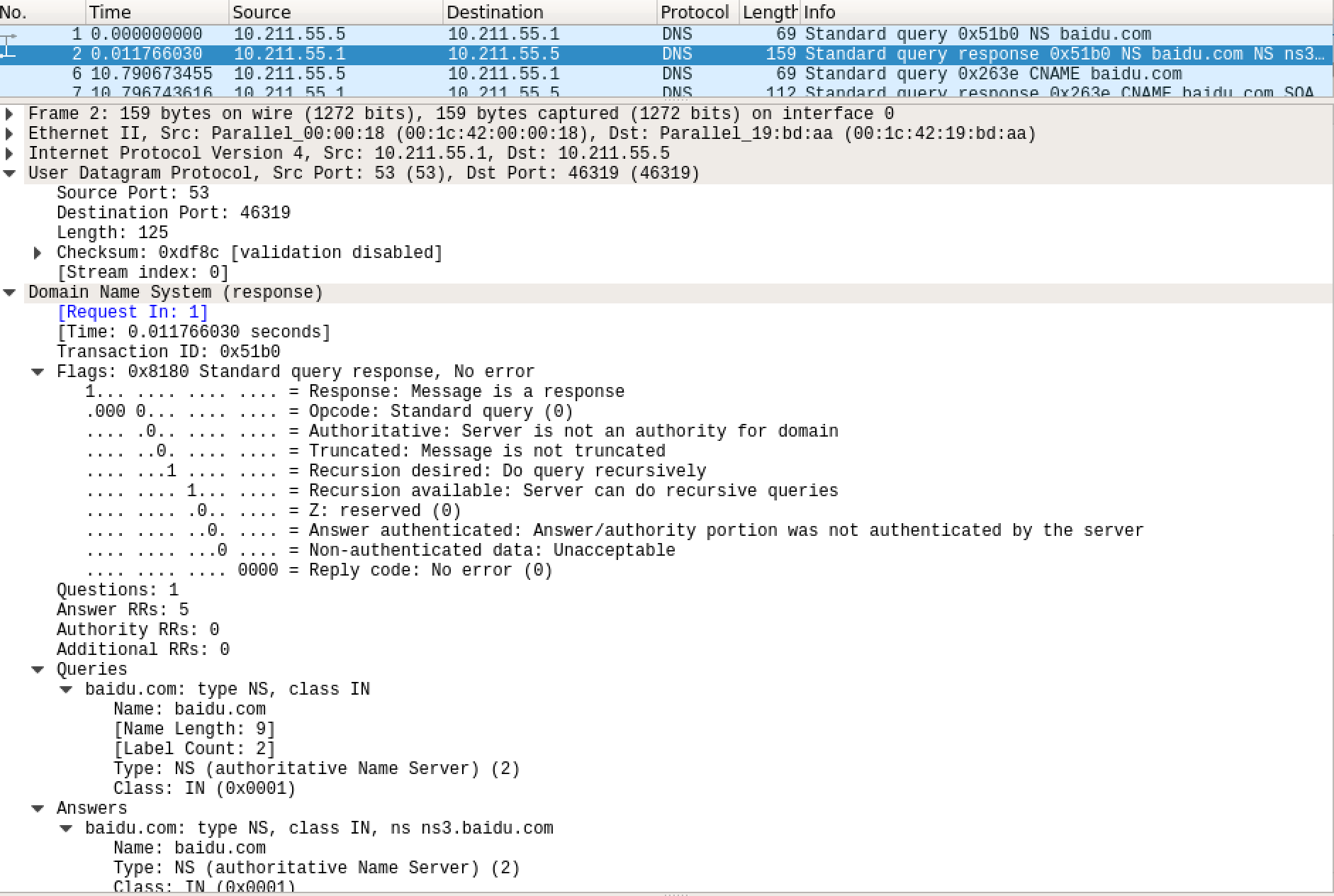
|  |  |  |
| --- | --- | --- |
|  | My Messages | Example in lecture notes |
| Header | Opcode=standard query | Opcode=standard query |
| Question | QNAME=www.baidu.com | QNAME=SRI-ARPA |
| QCLASS=IN | QCLASS=IN |
| QTYPE=PTR | QTYPE=PTR |
| Answer section | www.a.shifen.com | SRI-NIC.ARPA  86400 IN 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







1. TYPE=CNAME

