Report of Lab 7 – Using Wireshark to Capture DHCP&DNS Messages

Name: Jinyi Guo (郭进一) Class: 2011215116 Student ID: 2011213244

Configuration of Wireshark

1. Start wireshark and select available network connection

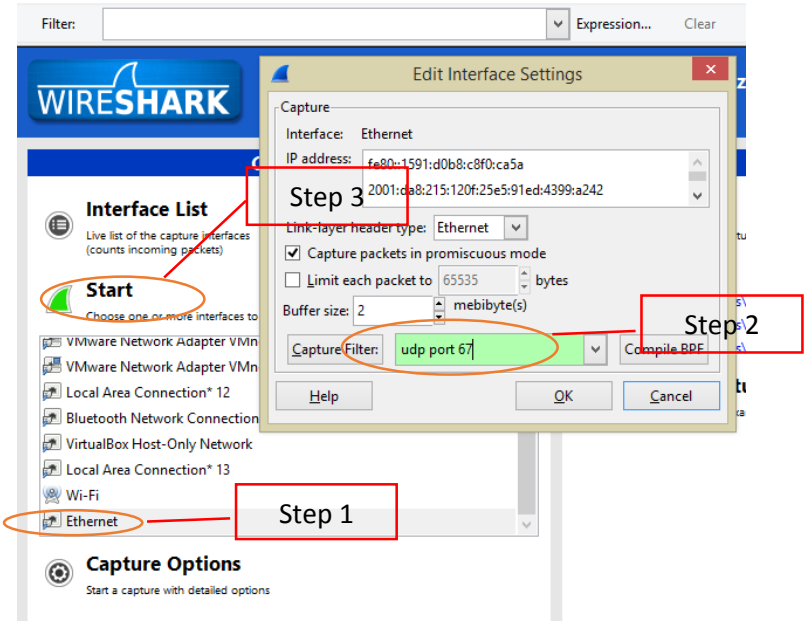

Figure 1 Wireshark Configuration

2. Set the value of Capture Filter
3. Start capturing

Procedure and Result of Capture

DHCP Capture

Steps:

1. Before capturing, set the Capture Filter to “udp port 67”, then click “OK”.

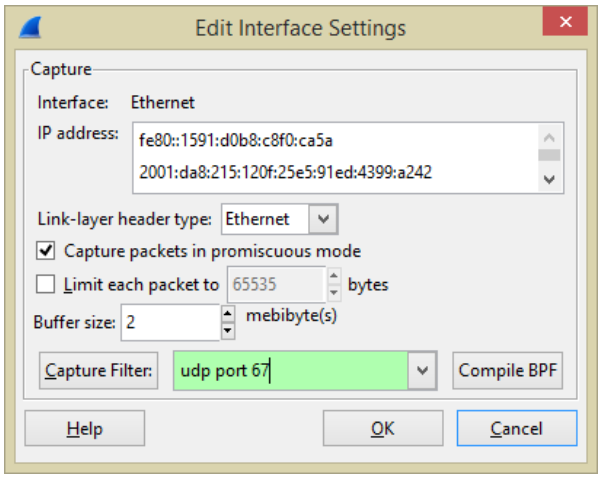

Figure 2 DHCP Capture

2. Start capturing, the interface should look like the figure below.

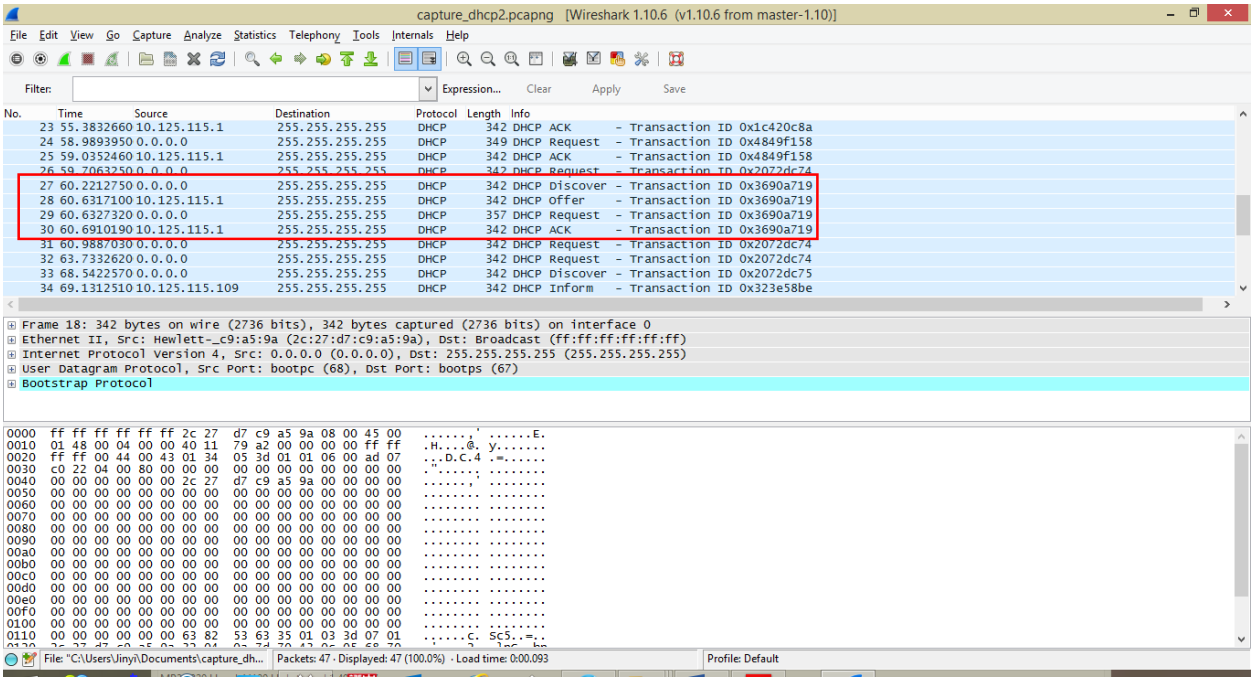

Figure 3 DHCP Capture Interface

Result Analysis:

In figure 3, a set of DHCP packets that include a whole process of address acquisition is highlighted, we will focus on analyzing these four packets.

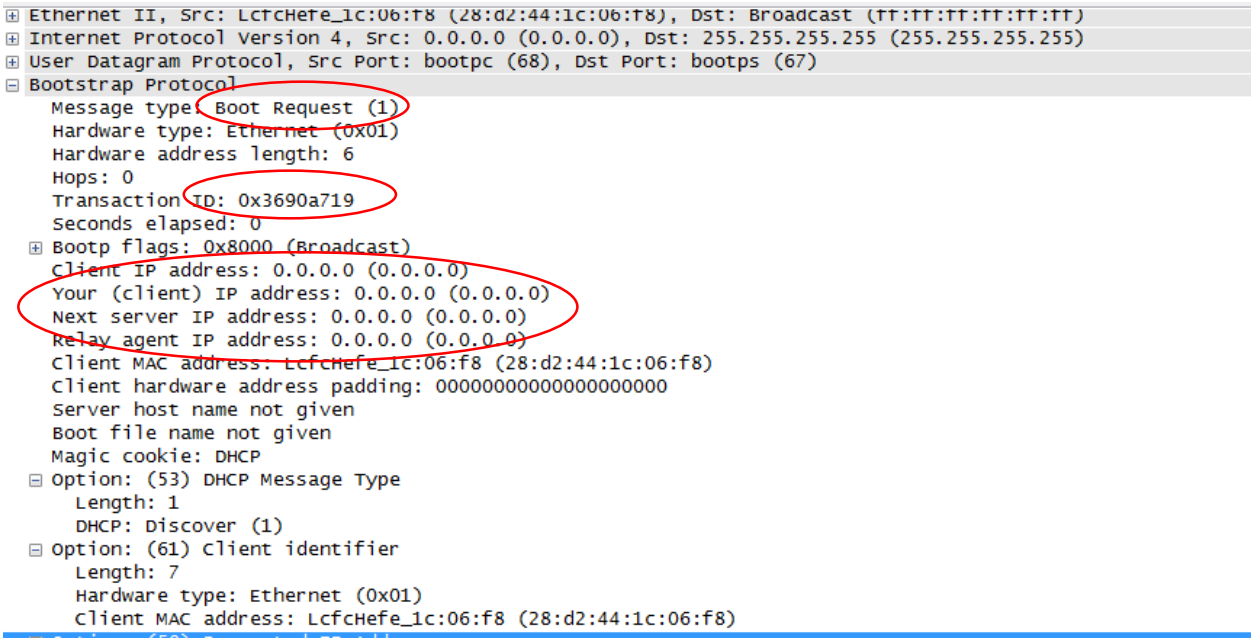

Figure 4 Details of DHCP Message (Discover)

For the **Discover message**, we list all the values of its critical parameters and corresponding meanings here.

- **Message type:** Boot Request (1). This means the message was sent by a client (indicated by the "1" in the parentheses) requesting the location of a DHCP server with IP address information.
- **Transaction ID:** 0x3690a719. This integer is generated randomly for client to match response with requests.
- **Client IP address:** 0.0.0.0. The address remains blank since its unknown. It is only filled in if client is in BOUND, RENEW or REBIND state.
- **Your IP address**: 0.0.0.0, which is same as client IP address.
- **Next server IP address:** 0.0.0.0. This option is used by a DHCP server to indicate to a DHCP client the IP address of a secondary server from where it can retrieve other parts of its configuration.
- **Relay agent:** 0.0.0.0. It relays DHCP messages between DHCP clients and DHCP servers on different IP networks.
- **Option** t=53: Discover (DHCP Message Type), t=50: 10.125.115.132 (Requested IP Address), t=12: Lenovo-PC (Host name), t=55: Parameter Request List (Detailed list omitted here).

We list the parameters of the rest messages in the following chart.

	Offer	Request	ACK
Message Type	Boot Relay (2)	Boot Request (1)	Boot Reply (2)
Transaction ID	0x3690a719	0x3690a719	0x3690a719
Client IP	0.0.0.0	0.0.0.0	0.0.0.0
Your IP	10.125.115.132	0.0.0.0	10.125.115.132
Next server IP	0.0.0.0	0.0.0.0	0.0.0.0
Relay agent	10.125.115.1	0.0.0.0	10.125.115.1

Option	t=53: Offer, t=54: 10.125.118.35 (DHCP Server Identifier), t=51: 1 hour (IP Address Lease Time), t=1: 255.255.255.0 (Subnet Mask), t=15: bupt.edu.cn (Domain Name), t=3: 10.125.115.1 (Router), t=6: 10.3.9.4/10.3.9.5/10.2.9.6/10.3.9.7 (Domain Name Servers).	t=53: Request, t=50: 10.125.115.132 (Requested IP Address), t=54: 10.125.118.35, t=12: Lenovo-PC, t=55: (omitted).	t=53: ACK, t=54: 10.125.118.35, t=51: 1 hour, t=1: 255.255.255.0, t=15: bupt.edu.cn, t=3: 10.125.115.1, t=6: 10.3.9.4/10.3.9.5/ 10.2.9.6/10.3.9.7

The frame addresses, IP addresses and port numbers of the four messages are listed below:

	Discover	Offer	Request	ACK
Frame Address (Source)	28:d2:44:1c:06:f8	00:0f:e2:6a3c:fd	28:d2:44:1c:06:f8	00:0f:e2:6a3c:fd
Frame Address (Destination)	ff:ff:ff:ff:ff:ff	ff:ff:ff:ff:ff:ff	ff:ff:ff:ff:ff:ff	ff:ff:ff:ff:ff:ff
IP Address (Source)	0.0.0.0	10.125.115.1	0.0.0.0	10.125.115.1
IP Address (Destination)	255.255.255.255	255.255.255.255	255.255.255.255	255.255.255.255
Port Number (Source)	bootpc (68)	Bootps (67)	bootpc (68)	Bootps (67)
Port Number (Destination)	Bootps (67)	Bootpc (68)	Bootps (67)	Bootpc (68)

Comparison with Lecture Notes

For Discover package, the source mac address (frame address) and transaction ID are different for they depend on the network you use.

For Offer package, the source mac address, source IP, transaction ID and your IP address are all different, the nextserver IP address of our captured package is 0.0.0.0, indicating that there is no secondary server available, while the package in lecture notes has one.

For Request package the situation is same as Discover package.

The difference of ACK package is same as Offer package.

Additionally, for the frame header of each package, the field type is different. In lecture note the value is 0x8035 (Ethernet), while in our example the value is 0x0800.

Procedure of Address Acquisition

We use a MSC chart to show this process. Actually in the example above, there is only one offer package received, which means the right part of the chart does not exist in our example.

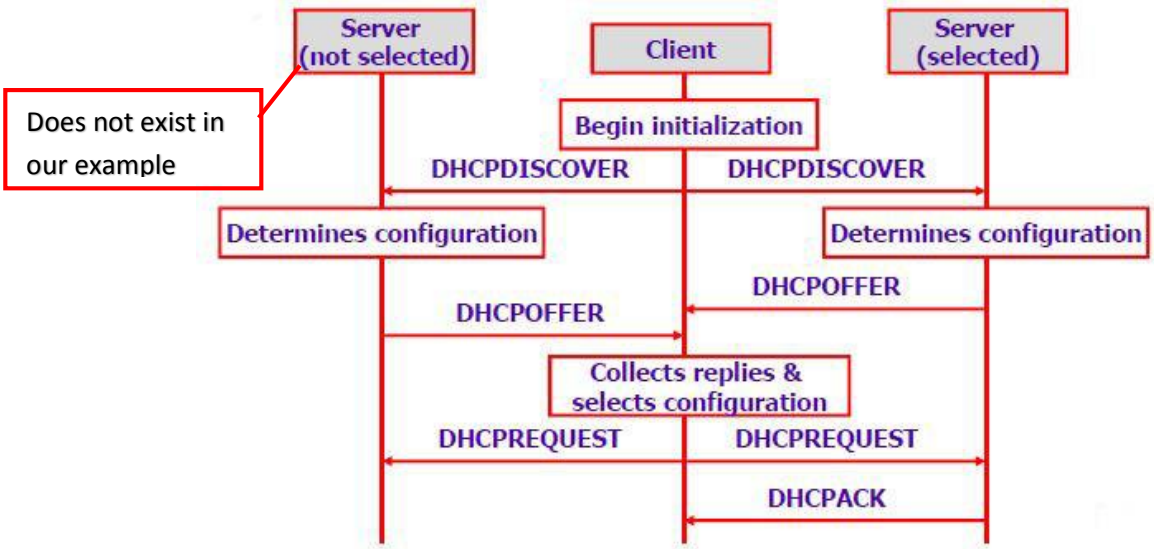

Figure 5 MSC Chart of Address Acquisition

DNS Capture

Steps

The procedure of capturing DNS packets is similar to DHCP capture, except you should set the value of Capture Filter to “udp port 53”.

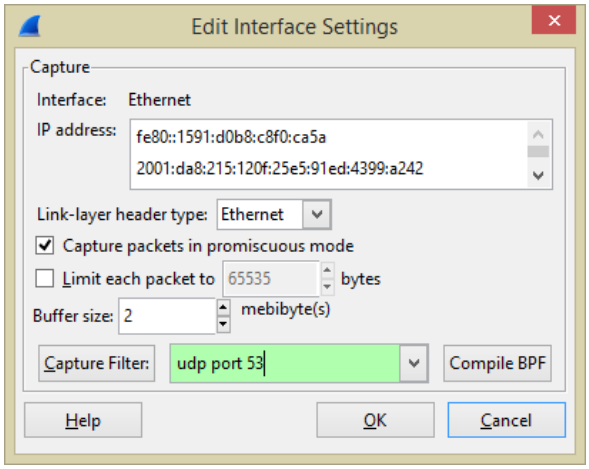

Figure 6 DNS Capture

Result Analysis

We select a pair of DNS query/response package to analyze.

10 8.45595500	10.125.115.132	10.3.9.4	DNS	71	Standard query 0xc2bc A sina.com.cn
11 8.45595500	10.125.115.132	10.3.9.4	DNS	73	Standard query 0x342a A m.sina.com.cn
12 8.45598300	10.125.115.132	10.3.9.4	DNS	76	Standard query 0xf063 A tech.sina.com.cn
13 8.45619800	10.125.115.132	10.3.9.4	DNS	71	Standard query 0x7733 AAAA sina.com.cn
14 8.45619800	10.125.115.132	10.3.9.4	DNS	73	Standard query 0xf43f AAAA m.sina.com.cn
15 8.45623800	10.125.115.132	10.3.9.4	DNS	76	Standard query 0xfd97 AAAA tech.sina.com.cn
16 8.45787800	10.3.9.4	10.125.115.132	DNS	223	Standard query response 0xc2bc A 202.108.33
17 8.45792900	10.3.9.4	10.125.115.132	DNS	272	Standard query response 0x342a CNAME jupite
18 8.45795800	10.3.9.4	10.125.115.132	DNS	275	Standard query response 0xf063 CNAME jupiter

Figure 7 Captured DNS package

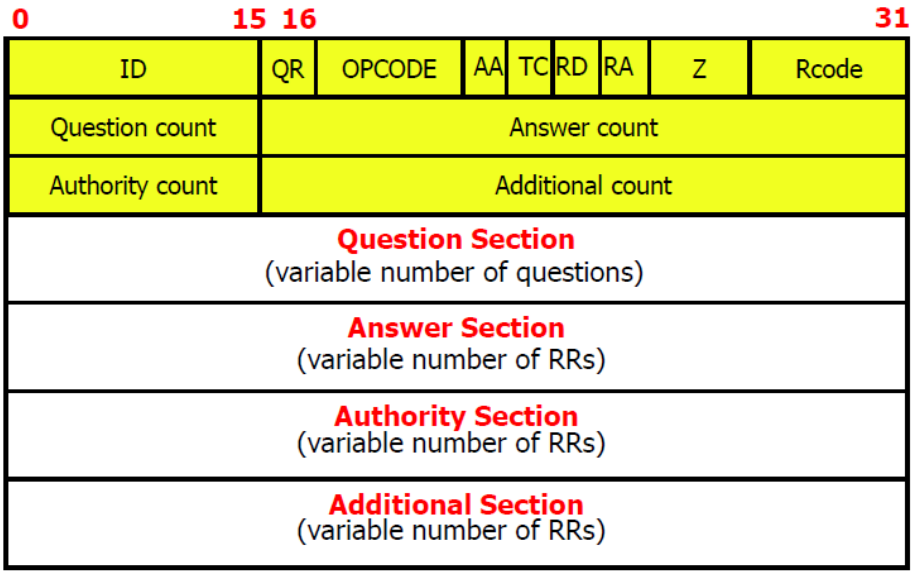

Figure 8 DNS Message Format

For the query and response message, we list the value and corresponding meaning of each part below.

Query

- **ID:** 0x342a, which is used to correlate the message with its response.
- **QR:** 0, indicating that it is a query message.
- **OPCODE:** 0000, which means that it is a standard query (name to address).
- **AA:** Not set here. “AA” is short for Authoritative Answer, when the value is set to I, identifies this response is made by an authoritative name server, therefore not useful for hosts.
- **TC:** 0. 0 means the message is not truncated. Otherwise, set to 1.
- **RD:** 1. Recursion desired, here it is set to 1 to request recursive service by the name server.
- **RA:** Not set here. Recursion Available is set to 1 by name server to indicate recursive query support is available. It is not used by hosts.
- **Z:** 0. Reserved for future use.
- **Rcode:** not used here. It is a 4-bit field that is set by the name server to identify the status of the query.
- **Question count:** 1. Number of entries in the question section.
- **Answer count:** 0. Number of resource records in the answer section.
- **Authority count:** 0. Number of name server resource records in the authority section.
- **Additional count:** 0. Number of resource records in the additional records section.
- **Question Section:**

- **Query domain name:** m.sina.com.cn
- **Query type:** A (Maps the name of a system to its address).
- **Query class:** IN (Internet System)

Response

- **ID:** 0x342a, which is used to correlate the message with its query.
- **QR:** 1. Message is a response.
- **OPCODE:** 0000 (Standard query).
- **AA:** 0. Server is not an authority for domain.
- **TC:** 0. Message is not truncated.
- **RD:** 1. Do query recursively.
- **RA: 1.** Server can do recursive queries.
- **Z:** 0. Reserved.
  - 0. Answer authenticated: Answer/authority portion was not authenticated by the server.
  - 0. Non-authenticated data: Unacceptable.
- **Question count:** 1. Number of entries in the question section.
- **Answer count:** 3. Number of resource records in the answer section.
- **Authority count:** 4. Number of name server resource records in the authority section.
- **Additional count:** 4. Number of resource records in the additional records section.
- **Question Section:** m.sina.com.cn: type A, class IN.
- **Answer Section:**
  - m.sina.com.cn: type CNAME, class IN, cname jupiter.sina.com.cn
    - Domain name: m.sina.com.cn.
    - Type: CNAME (Maps an alias name to the true, canonical name).
    - Class: IN.
    - TTL: 28 seconds.
    - Resource data length: 10.
  - jupiter.sina.com.cn: type CNAME, class IN, cname cernetnews.sina.com.cn
    - Domain name: jupiter.sina.com.cn.
    - Type: CNAME (Canonical name for all alias).
    - Class: IN.
    - TTL: 59 minutes, 59 seconds.
    - Resource data length: 13.
  - cernetnews.sina.com.cn: type A, class IN, addr 121.194.0.239
    - Domain name: cernetnews.sina.com.cn.
    - Type: A (Host Address).
    - Class: IN.
    - TTL: 9 seconds.
    - Resource data length: 4.
    - Addr: 121.194.0.239.
- **Authority Section:**
  - sina.com.cn: type NS, class IN, ns ns3.sina.com.cn
    - Domain name: sina.com.cn.

        - Type: NS (Maps a domain name to the name of a computer that is authoritative for the domain).
        - Class: IN.
        - TTL: 16 hours, 3 minutes, 48 seconds.
        - Resource data length: 6.
        - Name server: ns3.sina.com.cn
    - sina.com.cn: type NS, class IN, ns ns4.sina.com.cn
    - sina.com.cn: type NS, class IN, ns ns1.sina.com.cn
    - sina.com.cn: type NS, class IN, ns ns2.sina.com.cn
- **Additional Section:**
    - ns1.sina.com.cn: type A, class IN, addr 202.106.184.166
        - Domain name: ns1.sina.com.cn.
        - Type: A (Host address).
        - Class: IN.
        - TTL: 17 hours, 21 minutes, 49 seconds.
        - Resource data length: 4.
        - Addr: 202.106.184.166.
    - ns2.sina.com.cn: type A, class IN, addr 61.172.201.254
    - ns3.sina.com.cn: type A, class IN, addr 123.125.29.99
    - ns4.sina.com.cn: type A, class IN, addr 121.14.1.22

Comparison to Lecture Notes

The captured DNS message is of similar format with the one in lecture notes, except the fact that there are some parts of the format not filled in the query package.