

# Lab8 – Capture DHCP&DNS Packets

BUPT/QMUL

5/3/2017

# Task(1)

- Understand and analyze the communication procedures and message formats of DHCP and DNS using **Wireshark**
- Submit a **lab report** (written in English).
- You need to .....
  1. Capture all packets of a **overall DHCP address acquisition procedure** including DHCPDISCOVER, DHCPOFFER, DHCPREQUEST and DHCPACK messages.
    - ◆ Analyze the captured packets in “field-level” and explain the meaning and value of each field.
    - ◆ Use screen shot to show the result (e.g., the change of IP address and MAC address and other important field).
    - ◆ Use **dhclient** to produce packets.

## Task(2)

2. Capture a pair of packets of **DNS procedure** including DNS QUERY and DNS Query RESPONSE.
  - ◆ Analyze the captured packets in “field-level” and explain the meaning and value of each field.
  - ◆ Use screen shot to show the result
  - ◆ Use **nslookup** to produce packets pairs of Type A, Type MX and Type PTR.

# Important Information

- Upload your report to FTP server

- ◆Server: **ftp://10.3.255.85**, port:21

- ◆User name: **gjxy2017** password: **student**

- Name your file as: **BUPTID-name-v[number].pdf**

- ◆e.g., 2011010276-ZHANGXiaoming-v1.pdf

- Deadline: before **17:00, 2017-05-14** (UTC+8)

**WARNING:** Please upload your report file into the **DHCP&DNS\_report** folder. This is a *write-only* folder. Please check your file repeatedly before uploading. You can increase the **version** number and upload another file if there were something unexpected. The maximum **version** number is 4 and all the redundancies will be ignored.

- Please contact [zhaoqin@bupt.edu.cn](mailto:zhaoqin@bupt.edu.cn) if the FTP server crashed.....

# What should be included in lab report? (1)

- Title and Topic of the Lab
- Your name, class and student ID (Both BUPT & QM)
- Explain the configuration of Wireshark
- Explain the result of capture [MAIN PART]
  - DHCP: DHCPDISCOVER, DHCPOFFER, DHCPREQUEST and DHCPACK
  - DNS: DNS Query and DNS Query Response (Type=A, Type=MX and Type=PTR)
  - Ignore the useless field that will not influence the process of DHCP and DNS, such as Type of Service, Checksum and so on.

# What should be included in lab report? (2)

- For DHCP capture
  - For each DHCP message, list the value of following critical parameters and explain their meanings
    - ✓ message type, transaction ID, hops, client IP address, your IP address, Server IP address, Router IP address, option t=1, 3, 6, 12, 15, 50, 51, 53, 54, 55, 58 and 59
    - ✓ List frame addresses, IP addresses and port numbers
  - For each DHCP message, is it sent by unicast or by broadcast?
  - Pay attention the fields of *hops*, *client IP address*, *your IP address*, *Server IP address*, *Router IP address*, if any field is different with the example in Lecture notes, list and explain.
  - Draw a **Message Sequence Chart (MSC)** to illustrate the procedure of address acquisition

*Note: The display filter of DHCP should be “bootp” but not “dhcp” (or **udp.port==67**)*

# What should be included in lab report? (3)

- For DNS capture
  - Three pairs of DNS messages for resolving different type of resource record have to be captured and analyzed  
Type=A      Type=MX      Type=PTR
  - For each DNS message, list the value of all fields and explain their meanings
    - ✓ List frame addresses, IP addresses and port numbers
  - Compare the DNS message format with the one in Lecture notes
  - Try to use nslookup to resolve different type of query.
  - Use “udp port 53” as capture filter
  - Use “dns” as display filter

# What should be included in lab report? (4)

- Pay all your attentions on answering the following questions in each step:
  - ✓What do you plan to do in this step?
  - ✓How do you operate (including your configuration and processing)?
  - ✓Explain what the expected result is (learn from the theoretical courses, including the MSC, option number, content and etc.)?
  - ✓Explain what the capturing result is (the details about the captured packets, including the port number, the option number, the order of packets [namely MSC] and etc.)?
  - ✓Are these two “results” consistent (matched)? Show the matching parts. Try to analyze and describe the non-matching parts. (This is the core content of the report)
- The inconsistent result DOES NOT always indicate that you are wrong.



# What is Wireshark?

- A network protocol analyzer (packet sniffer)
- Official website
  - <http://www.wireshark.org/>
- Renamed from Ethereal in 2006
- Able to capture packets transferred on the network and display packet fields and their meanings
- Used for network troubleshooting, analysis, software and communications protocol development, and education.
- Already Installed in your Ubuntu OS
  - Start Xmanager or Xquartz in your Physical Machine.
  - Input “sudo wireshark” in your Virtual Machine.

# Starting Wireshark

The image shows the 'Wireshark: Capture Options' dialog box. The 'Capture' tab is active. The 'Capture' table lists interfaces: eth0 (checked), nflog, nfqueue, and eth1. The 'Capture Filter' field is set to 'udp port 67'. The 'Start' button is highlighted. Red circles and arrows point to the settings icon, the 'eth0' row, the 'Capture Filter' field, and the 'Start' button. Red text annotations explain the actions: selecting the network card, filling the filter condition, and starting the capture.

**Wireshark: Capture Options**

**Capture**

Capture	Interface	Link-layer header	Prom. Mode	Snapplen [B]	Buffer [MiB]	Mon. Mode	Capture Filter
<input checked="" type="checkbox"/>	eth0 10.0.2.15 fe80::a00:27ff:fe49:67a3	Ethernet	enabled	default	2	n/a	udp port 67
<input type="checkbox"/>	nflog	Linux netfilter log messages	enabled	default	2	n/a	
<input type="checkbox"/>	nfqueue	Raw IPv4	enabled	default	2	n/a	
<input type="checkbox"/>	eth1 192.168.56.101 fe80::a00:27ff:fed3:fd00	Ethernet	enabled	default	2	n/a	

☐ Capture on all interfaces

☒ Use promiscuous mode on all interfaces

Capture Filter:

**Capture Files**

File:

☐ Use multiple files ☒ Use pcap-ng format

**Display Options**

☒ Update list of packets in real time

☒ Automatically scroll during live capture

**Start**

Choose one or more interfaces to capture on

☒ eth0

☐ nflog

☐ nfqueue

☐ eth1

☐ any

**Capture**

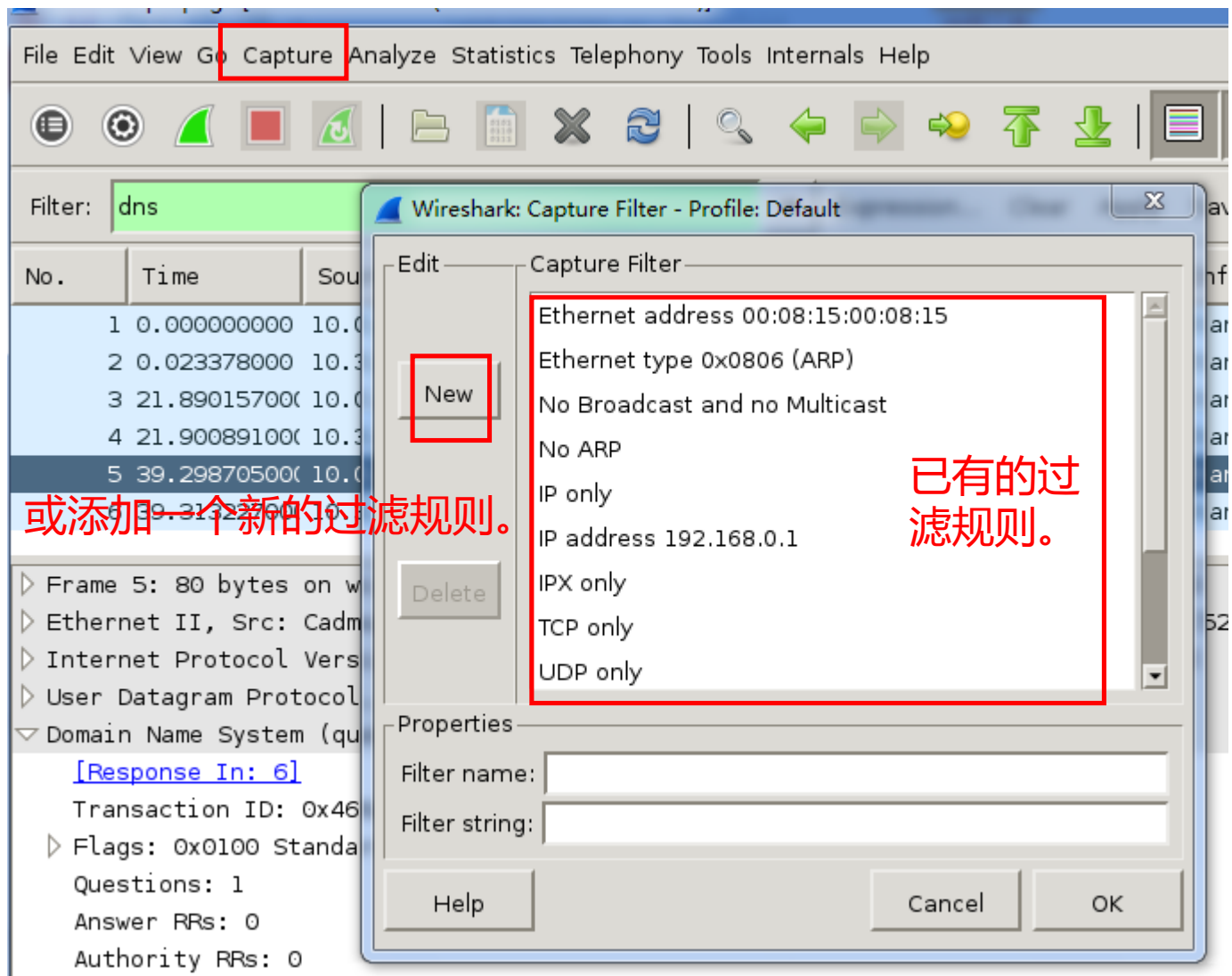
Start a capture

**Manage Interfaces**

**Compile selected BPFs**

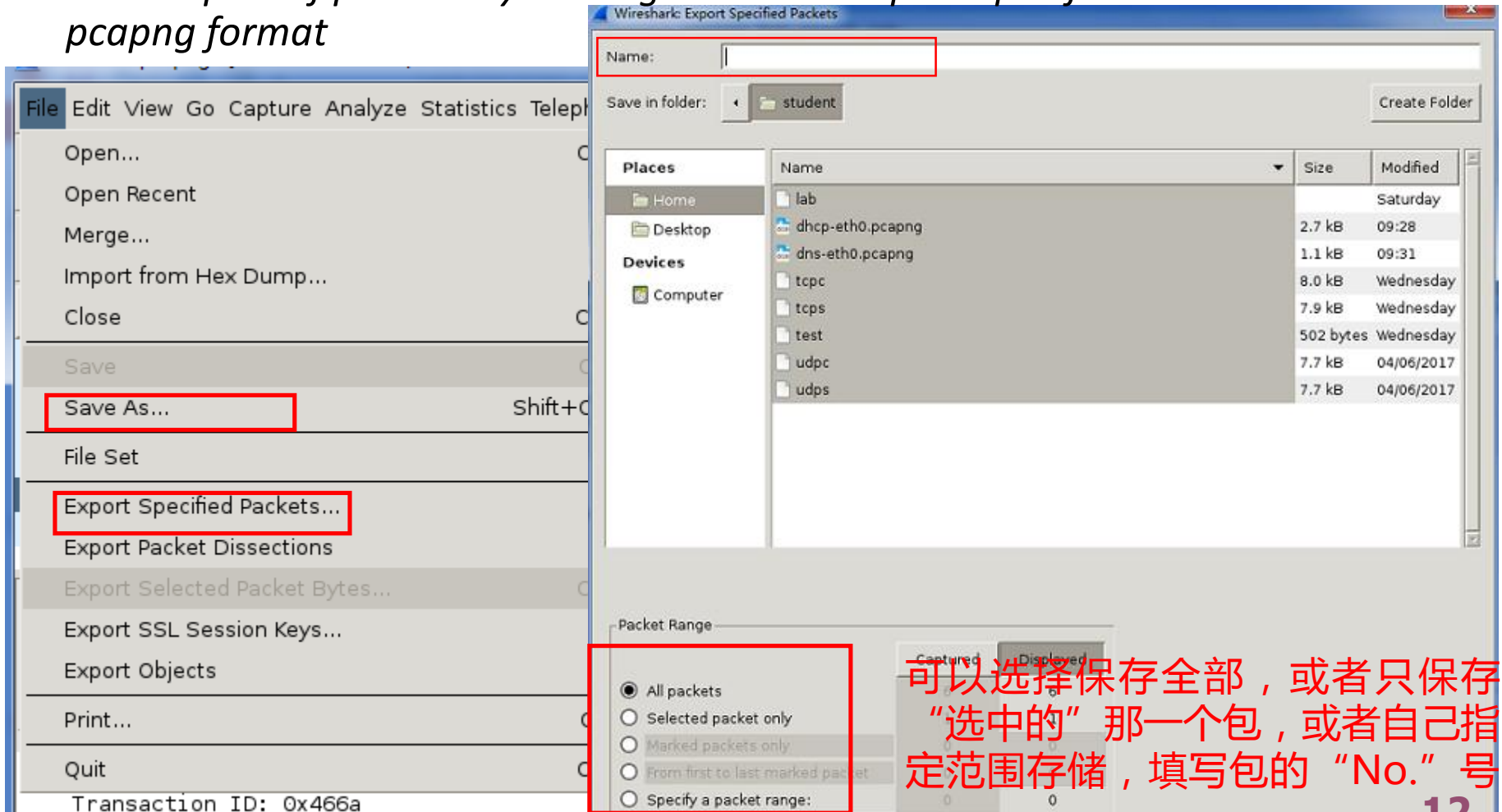
# Manage Capture Filter

- Also you can set capture filter in the main window, select *Capture* → *Capture Filters*



# Save your capturing

- Save all packets by clicking “File” → “save as ” as pcapng format
- Choose part of packets by clicking “File” → “Export Specified Packets” as pcapng format



可以选择保存全部，或者只保存“选中的”那一个包，或者自己指定范围存储，填写包的“No.”号。

# How to initiate the communications?

- DHCP

- Start wireshark, set capture options
  - ✓ in xShell or Terminal , `#sudo wireshark &`
- Initiate DHCP procedure
  - ✓ In xShell or Terminal , `#sudo dhclient -r eth0;sudo dhclient eth0`

- DNS

- Start Wireshark, set capture options
  - ✓ in xShell or Terminal, `#sudo wireshark &`
- use nslookup to query DNS server
  - ✓ in xShell or Terminal, `# nslookup -query=type [domain name or IP address]`

- *Note : if “error : XDG\_RUNTIME\_DIR not set in the environment ” when run “sudo wireshark &” , run “rm .Xauthority” to delete. Then disconnect virtual machine and reconnect again.*

# Example: Capture of DHCP messages

**Packet  
List pane**

No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000000	10.2.0.5	10.2.0.1	DHCP	342	DHCP Release - Transaction ID 0x18ae6d24
2	4.37138800	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x2a897b1e
3	5.43755000	10.2.0.1	255.255.255.255	DHCP	350	DHCP Offer - Transaction ID 0x2a897b1e
4	5.43811000	0.0.0.0	255.255.255.255	DHCP	352	DHCP Request - Transaction ID 0x2a897b1e
5	5.44119100	10.2.0.1	255.255.255.255	DHCP	350	DHCP ACK - Transaction ID 0x2a897b1e

⊕ Frame 2: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)  
⊕ Ethernet II, Src: WistronI\_3c:a7:0f (f0:de:f1:3c:a7:0f), Dst: Broadcast (ff:ff:ff:ff:ff:ff)  
⊕ Internet Protocol Version 4, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)  
⊕ User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)  
⊖ Bootstrap Protocol

**Packet Details  
pane**

Message type: Boot Request (1)  
Hardware type: Ethernet  
Hardware address length: 6  
Hops: 0  
Transaction ID: 0x2a897b1e  
Seconds elapsed: 0  
⊕ Bootp flags: 0x8000 (Broadcast)  
Client IP address: 0.0.0.0 (0.0.0.0)  
Your (client) IP address: 0.0.0.0 (0.0.0.0)  
Next server IP address: 0.0.0.0 (0.0.0.0)  
Relay agent IP address: 0.0.0.0 (0.0.0.0)  
Client MAC address: WistronI\_3c:a7:0f (f0:de:f1:3c:a7:0f)  
Client hardware address padding: 00000000000000000000  
Server host name not given  
Boot file name not given  
Magic cookie: DHCP  
⊕ Option: (53) DHCP Message Type  
⊕ Option: (61) Client identifier  
⊕ Option: (50) Requested IP Address  
⊕ Option: (12) Host Name  
⊕ Option: (60) vendor class identifier

00e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
00f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0100 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....

**Packet Bytes  
pane**

# Example: capture of DNS messages when resolve www.mit.edu

Thunderbolt Ethernet: en3

Display filter. 负责筛选哪些包被显示, 哪些不显示.

No.	Time	Source	Destination	Protocol	Length	Info
75	7.921675	10.109.242.45	10.3.9.4	DNS	94	Standard query 0x9ddd A tile-service.weather.microsoft.com
76	7.922145	10.109.242.45	10.3.9.4	DNS	94	Standard query 0xfdc3 AAAA tile-service.weather.microsoft.com
77	7.922204	10.3.9.4	10.109.242.45	DNS	199	Standard query response 0x9ddd A tile-service.weather.microsoft.com
78	7.922699	10.3.9.4	10.109.242.45	DNS	241	Standard query response 0xfdc3 AAAA tile-service.weather.microsoft.com
79	7.923521	10.109.242.45	10.3.9.4	DNS	88	Standard query 0xccf2 A cdn.content.prod.cms.msn.com
80	7.923812	10.109.242.45	10.3.9.4	DNS	88	Standard query 0x9c99 AAAA cdn.content.prod.cms.msn.com
81	7.923913	10.3.9.4	10.109.242.45	DNS	206	Standard query response 0xccf2 A cdn.content.prod.cms.msn.com CN
82	7.924292	10.3.9.4	10.109.242.45	DNS	233	Standard query response 0x9c99 AAAA cdn.content.prod.cms.msn.com
153	12.805698	10.109.242.45	10.3.9.4	DNS	90	Standard query 0xc0ee A nexusrules.officeapps.live.com
154	12.806345	10.3.9.4	10.109.242.45	DNS	155	Standard query response 0xc0ee A nexusrules.officeapps.live.com
184	16.913488	10.109.242.45	10.3.9.6	DNS	79	Standard query 0xa5bc A iphone-wu.apple.com
185	16.913558	10.109.242.45	10.3.9.6	DNS	79	Standard query 0x8e56 AAAA iphone-wu.apple.com
186	16.913968	10.3.9.6	10.109.242.45	DNS	153	Standard query response 0xa5bc A iphone-wu.apple.com CNAME wu.ap

- ▶ Frame 75: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface 0
- ▶ Ethernet II, Src: Apple\_9c:2b:aa (68:5b:35:9c:2b:aa), Dst: Hangzhou\_6a:09:78 (00:0f:e2:6a:09:78)
- ▶ Internet Protocol Version 4, Src: 10.109.242.45, Dst: 10.3.9.4
- ▶ User Datagram Protocol, Src Port: 57710 (57710), Dst Port: 53 (53)
- ▶ Domain Name System (query)

No. 不连续, 说明很多包被抓取, 但并没有显示