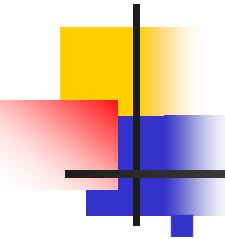


Lab7– Using Wireshark to capture DHCP&DNS messages

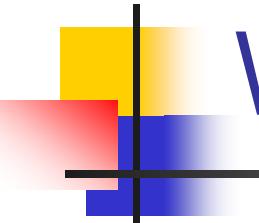
BUPT/QMUL

2014-04-10



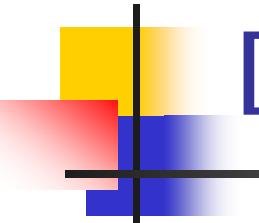
Lab7

- Using Wireshark (Ethereal) to learn about the communication procedure and message formats of DHCP and DNS
 - An Analysis report (in English) is required to submit
 - Report naming format:
DHCP-report_studentnumber_name.pdf or .doc
 - Deadline: upload to **ftp.mayan.cn**,
 - User name: **ma** password: **bupt**
 - before the **0:00, April 28**



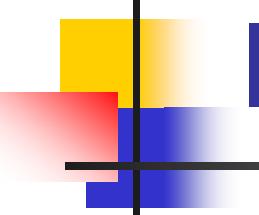
What is wireshark?

- A network protocol analyzer (packet sniffer)
- 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.



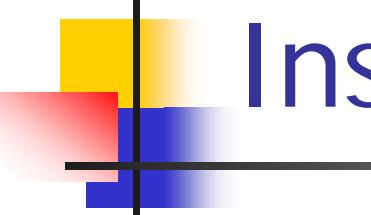
Download Wireshark

- Official website
 - <http://www.wireshark.org/>
- Download page
 - <http://www.wireshark.org/download.html>
- Available newest versions
 - For windows:
 - wireshark-win32-1.10.6.exe
 - wireshark-win64-1.10.6.exe
 - For Linux:
 - wireshark-1.10.6.tar.bz2



Install Wireshark (1)

- Windows
 - As easy as any other windows software
- Ubuntu
 - # aptitude install wireshark
 - 目前统一安装的版本没有图形界面，因此不能使用 wireshark



Install Wireshark (2)

■ Linux

- (1) 在终端窗口中，在安装文件（wireshark-1.10.6.tar.bz2）所在目录，执行命令：

```
# tar jxvf wireshark-1.10.6.tar.bz2
```

- (2) 此时会生成一个目录，名字是wireshark-1.10.6。进入这个目录，依次执行以下命令：

```
# ./configure
```

```
# make
```

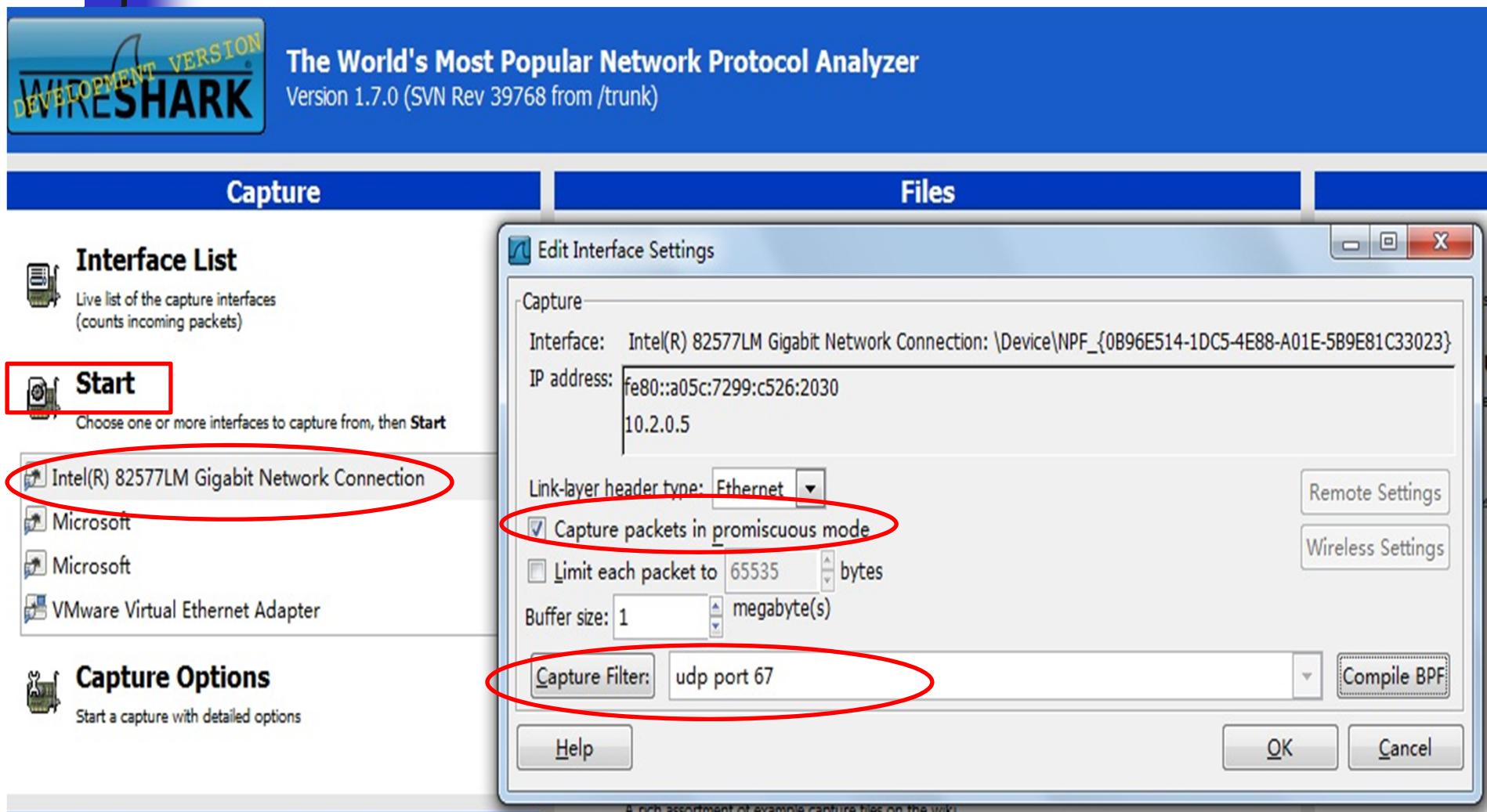
- (3) 此时会生成可执行的文件wireshark，执行命令：

```
# ./wireshark
```

就会运行wireshark，打开图形界面的窗口。

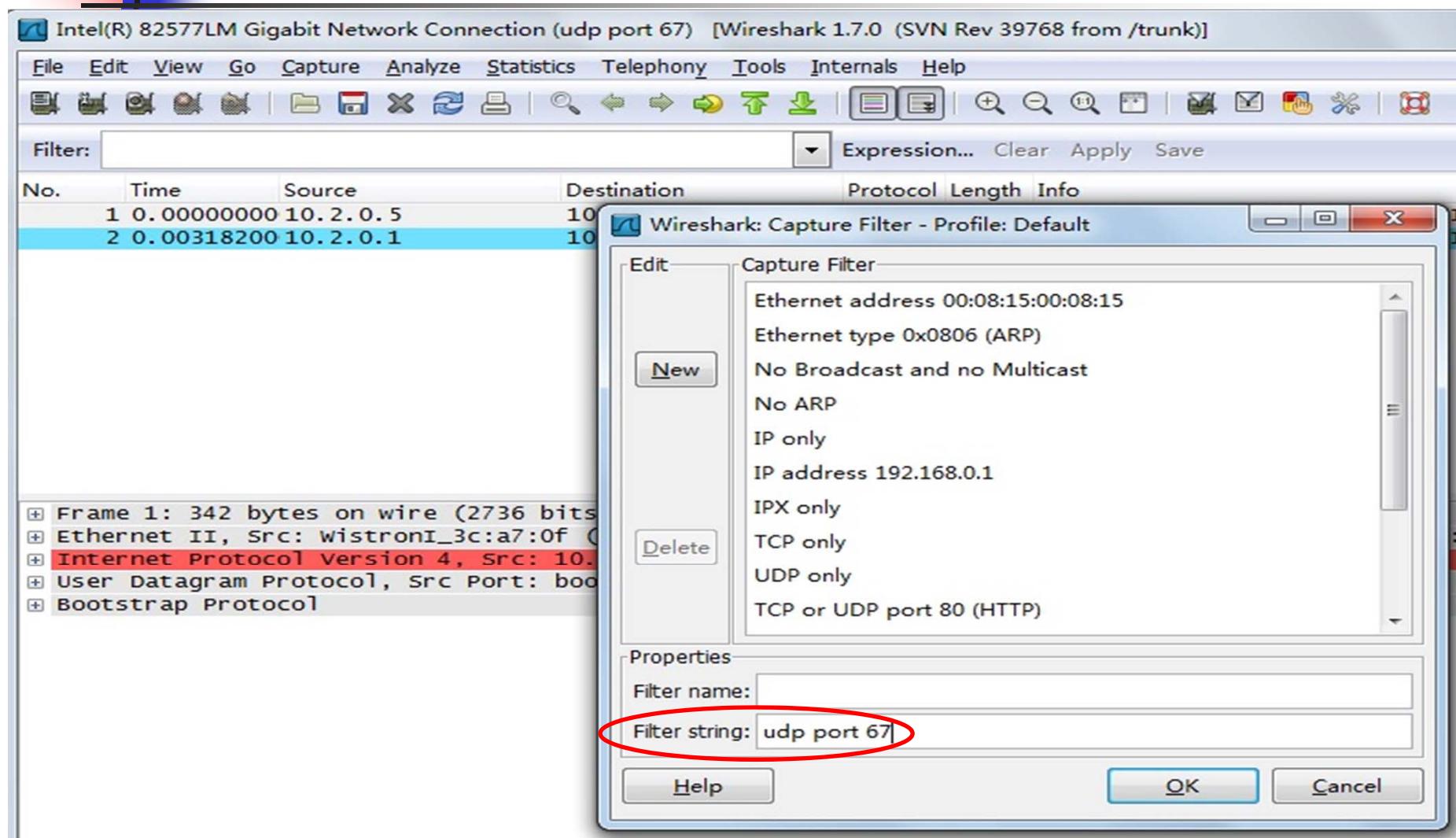
Starting wireshark in windows 以管理员身份运行

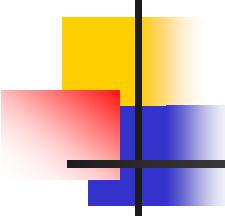
Select *Interface*, double click, then input *Capture Filter expression*, then press *Start*



Making Capture Filter in Main Window

*In then menu, select **Capture**→**Capture Filters**, then input **Capture Filter** expression*





How to initiate the communications?

- DHCP
 - In Windows: 先启动wireshark，之后在命令窗口里，先执行ipconfig /release，再执行ipconfig /renew
 - In Linux: 先启动wireshark，之后在终端窗口里，执行killall dhclient3，再执行dhclient -d eth0
- DNS
 - Start Wireshark
 - You can type in: telnet bbs.newsmth.net
 - Or you can access a website in your browser

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
```

```
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: 000000000000000000000000
Server host name not given
Boot file name not given
```

- + Option: (53) DHCP Message Type
- + Option: (61) Client identifier
- + Option: (50) Requested IP Address
- + Option: (12) Host Name
- + Option: (60) Vendor class identifier

Packet Details pane

Packet Bytes pane

Example: capture of DNS messages by inputting www.mit.edu in the browser

The screenshot shows a Wireshark capture window with the following details:

Capturing from Intel(R) 82577LM Gigabit Network Connection (udp port 53) [Wireshark 1.7.0 (SVN Rev 39768 from /trunk)]

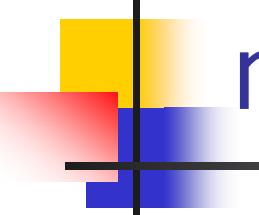
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.2.0.5	202.106.46.151	DNS	71	Standard query 0xfd68 A www.mit.edu
2	0.48713700	202.106.46.151	10.2.0.5	DNS	87	Standard query response 0xfd68 A 18.9.22.169
3	4.05777800	10.2.0.5	202.106.46.151	DNS	71	Standard query 0x9377 A web.mit.edu
4	4.07250000	10.2.0.5	202.106.46.151	DNS	88	Standard query 0xc70e A dnn506yrbagrg.cloudfront.net
5	4.10287200	202.106.46.151	10.2.0.5	DNS	87	Standard query response 0x9377 A 18.9.22.69
6	4.11386700	202.106.46.151	10.2.0.5	DNS	249	Standard query response 0xc70e CNAME dnn506yrbagrg.hkg1.

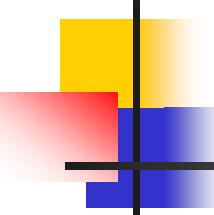
Frame 1: 71 bytes on wire (568 bits), 71 bytes captured (568 bits)
Ethernet II, Src: WistronI_3c:a7:0f (f0:de:f1:3c:a7:0f), Dst: Hangzhou_2a:d6:33 (00:0f:e2:2a:d6:33)
Internet Protocol version 4, Src: 10.2.0.5 (10.2.0.5), Dst: 202.106.46.151 (202.106.46.151)
User Datagram Protocol, Src Port: 59231 (59231), Dst Port: domain (53)
Domain Name System (query)

0000	00 0f e2 2a d6 33 f0 de	f1 3c a7 0f 08 00 45 00	...*.3.. .<....E.
0010	00 39 2b 27 00 00 40 11	00 00 0a 02 00 05 ca 6a	.9+...'@.j
0020	2e 97 e7 5f 00 35 00 25	03 3f fd 68 01 00 00 015%.?h....
0030	00 00 00 00 00 00 03 77	77 77 03 6d 69 74 03 65w ww.mit.e
0040	64 75 00 00 01 00 01		du.....



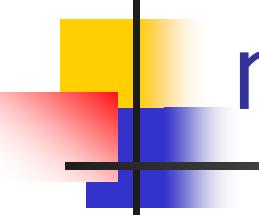
What shall be included in lab report? (1)

- Title and Topic of the Lab
- Your name, class and student ID
- Explain the configuration of wireshark
- Explain the procedure of capture



What shall 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, client IP address, your IP address, Next server IP address, Relay agent, option t=1, 3, 6, 12, 15, 50, 51, 53, 54, 55, 58 and 59
 - List frame addresses, IP addresses and port numbers
 - Compare the value of fields of each DHCP message with the example in Lecture notes
 - Draw a Message Sequence Chart (MSC) to illustrate the procedure of address acquisition



What shall be included in lab report? (3)

- For DNS capture
 - 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