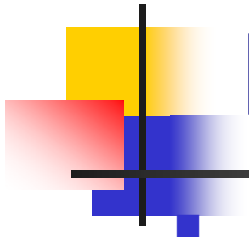
Lab7– Using Wireshark to capture DHCP&DNS messages

BUPT/QMUL

2014-04-10

北京郵電大學
BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

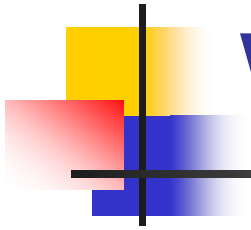
Electronic Engineering



Lab7

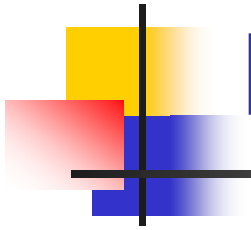
- Using Wireshark (Etheral) to learn about the communication procedure and message formats of DHCP and DNS
- An Analysis report (in English) is required to submit
- Report naming format:

  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.



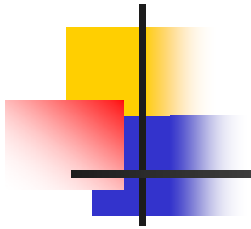
Download Wireshark

- 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：

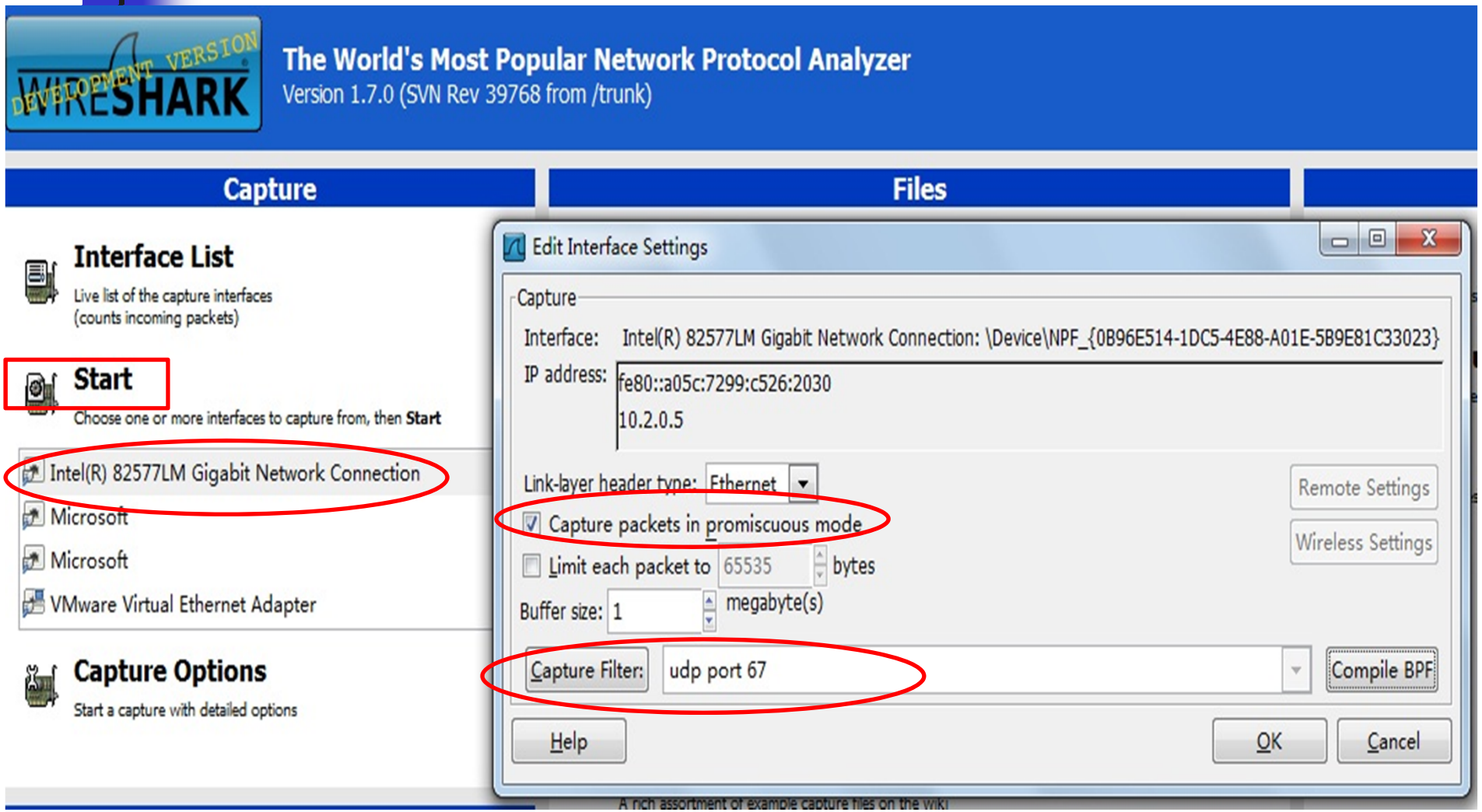
    # ./wireshark

    就会运行wireshark，打开图形界面的窗口。

Starting wireshark in windows

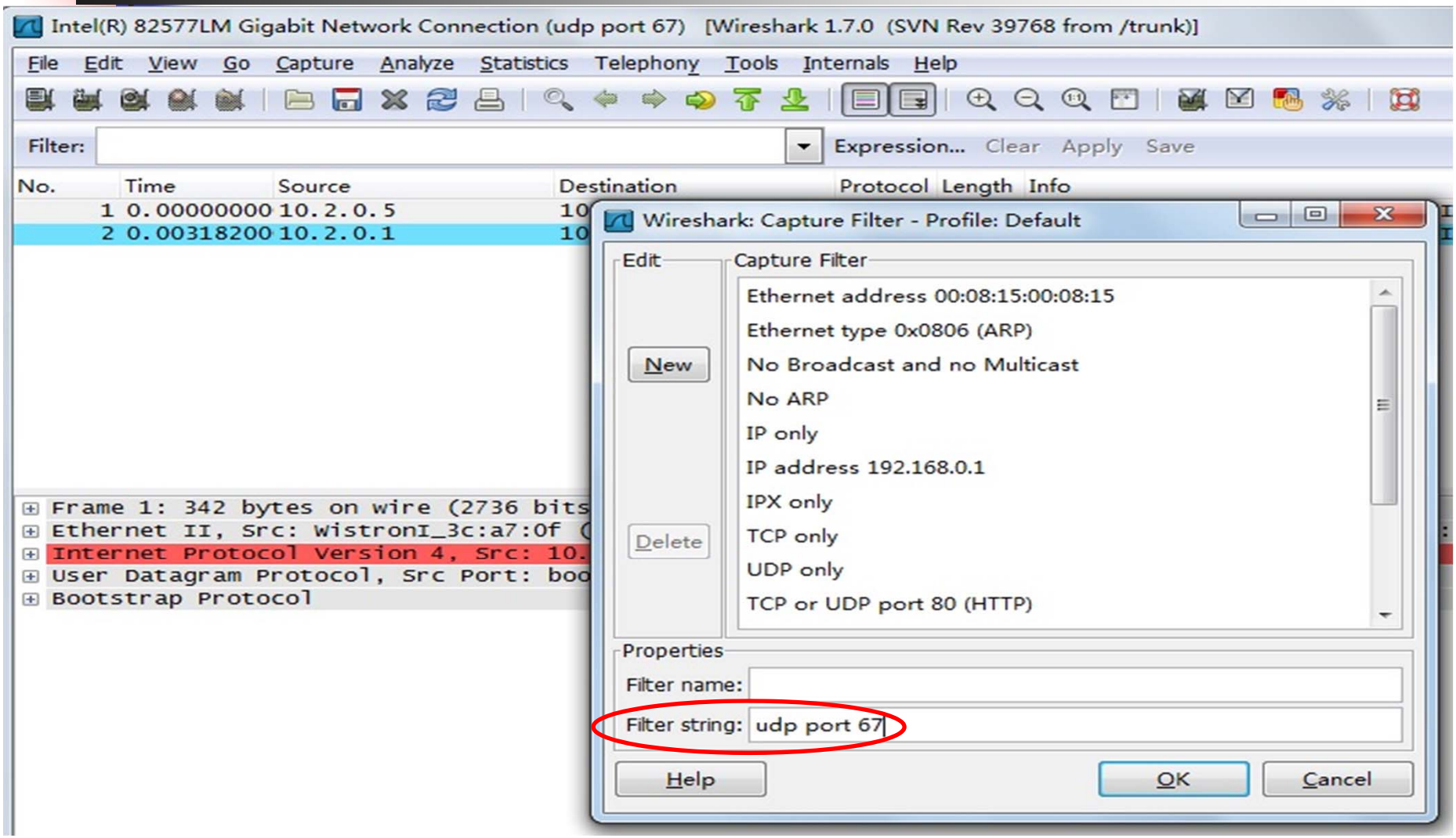
以管理员身份运行

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



Making Capture Filter in Main Window

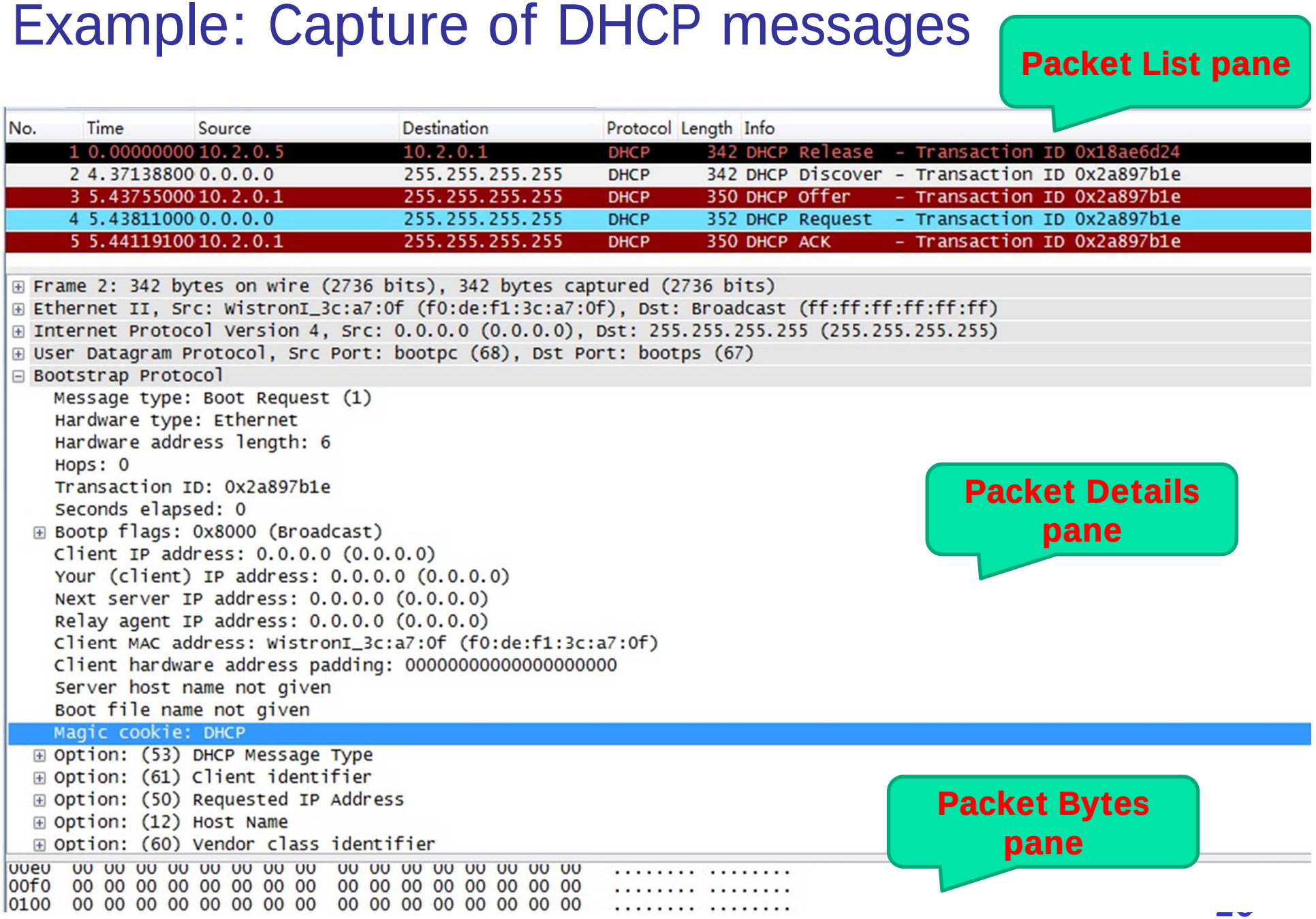
In then menu, select Capture→Capture Filters, then input Capture Filter expression



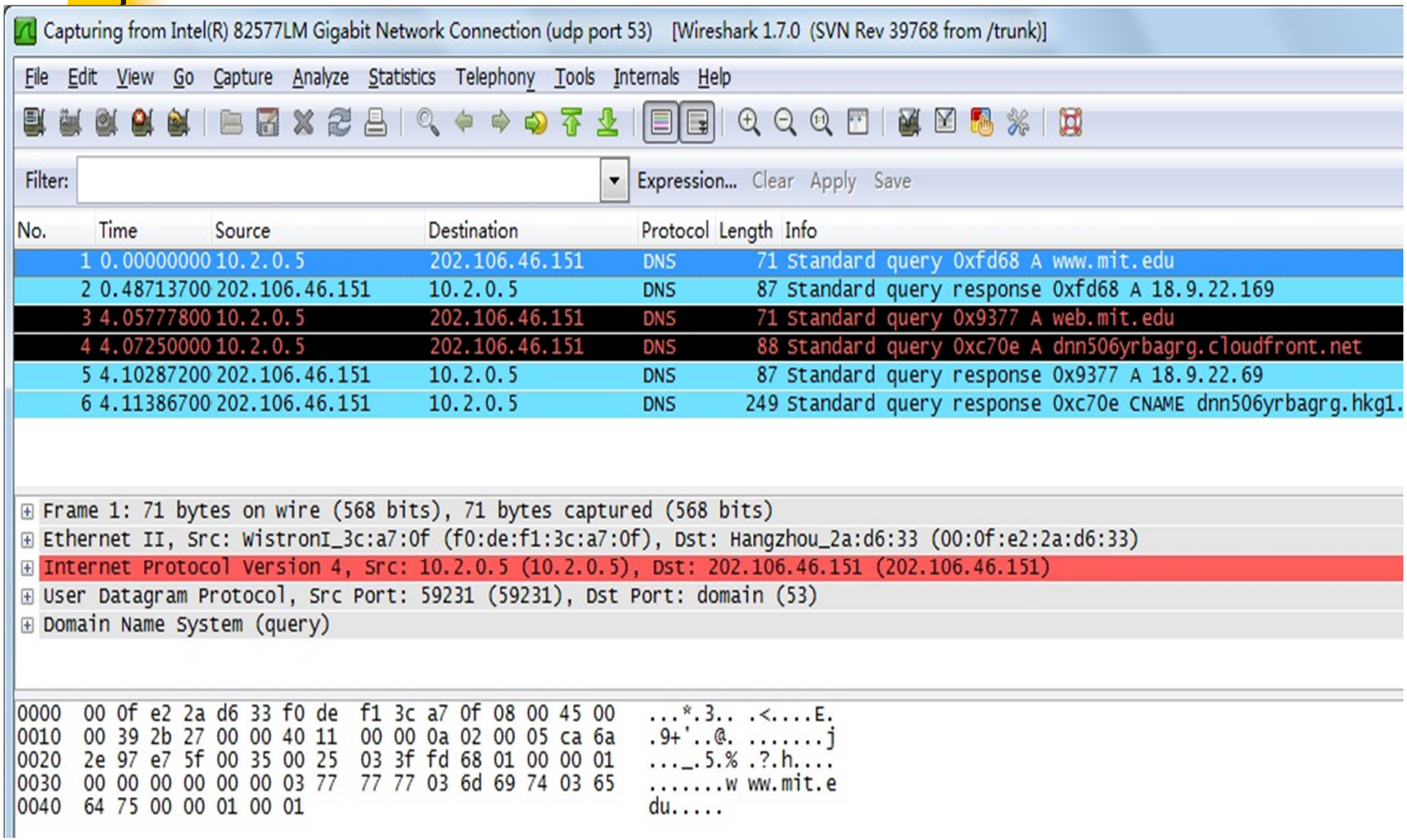
How to initiate the communications?

- 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

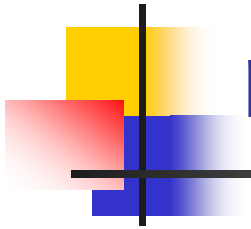
Example: Capture of DHCP messages



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



What shall be included in lab report? (1)

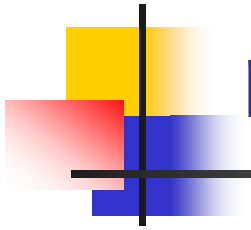


- Title and Topic of the Lab
- Your name, class and student ID
- Explain the configuration of wireshark
- Explain the procedure of capture

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