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 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

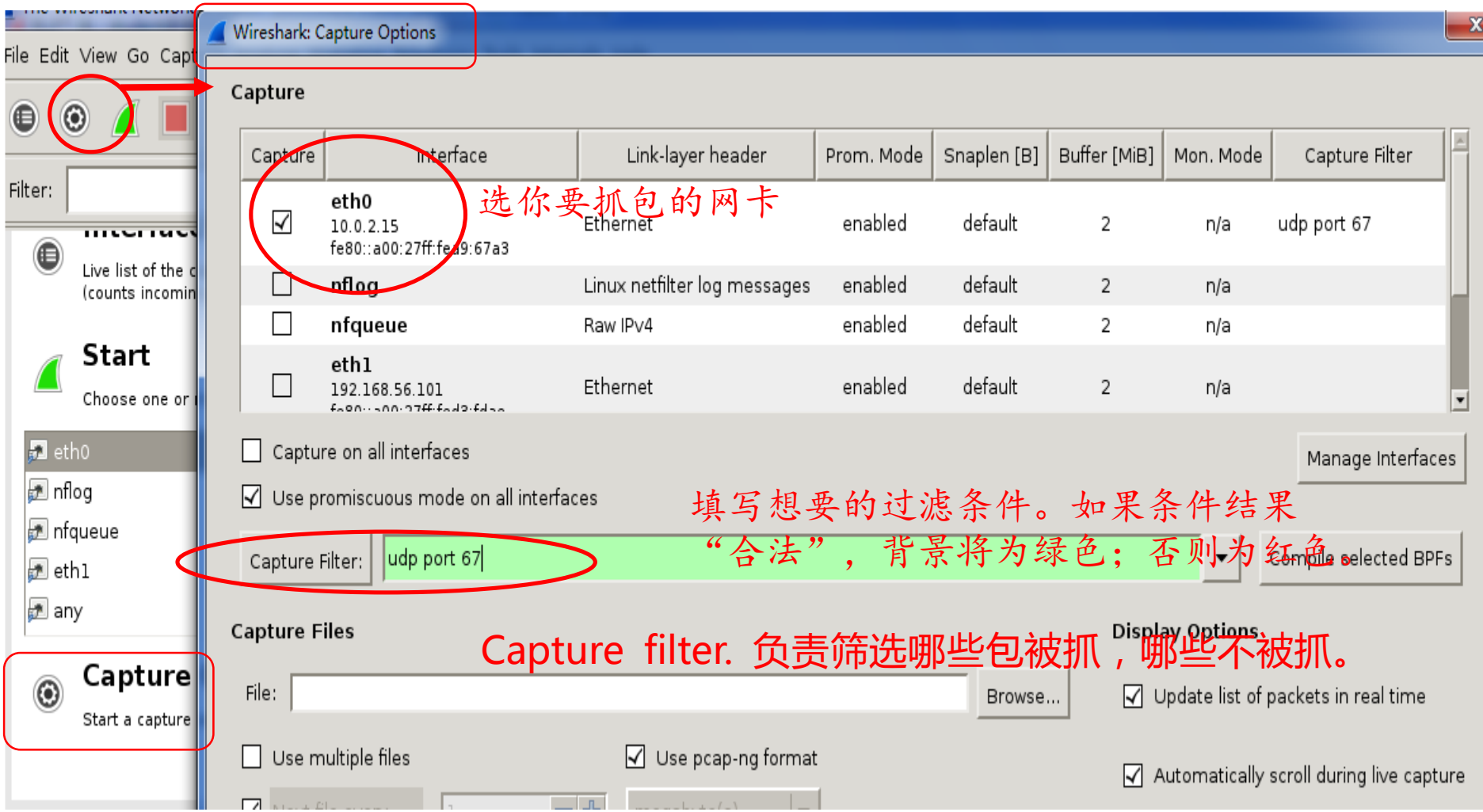
What should be included in lab report? (4)

- 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)
- <u>The inconsistent result DOES NOT always indicate that you are wrong.</u>

What is Wireshark?

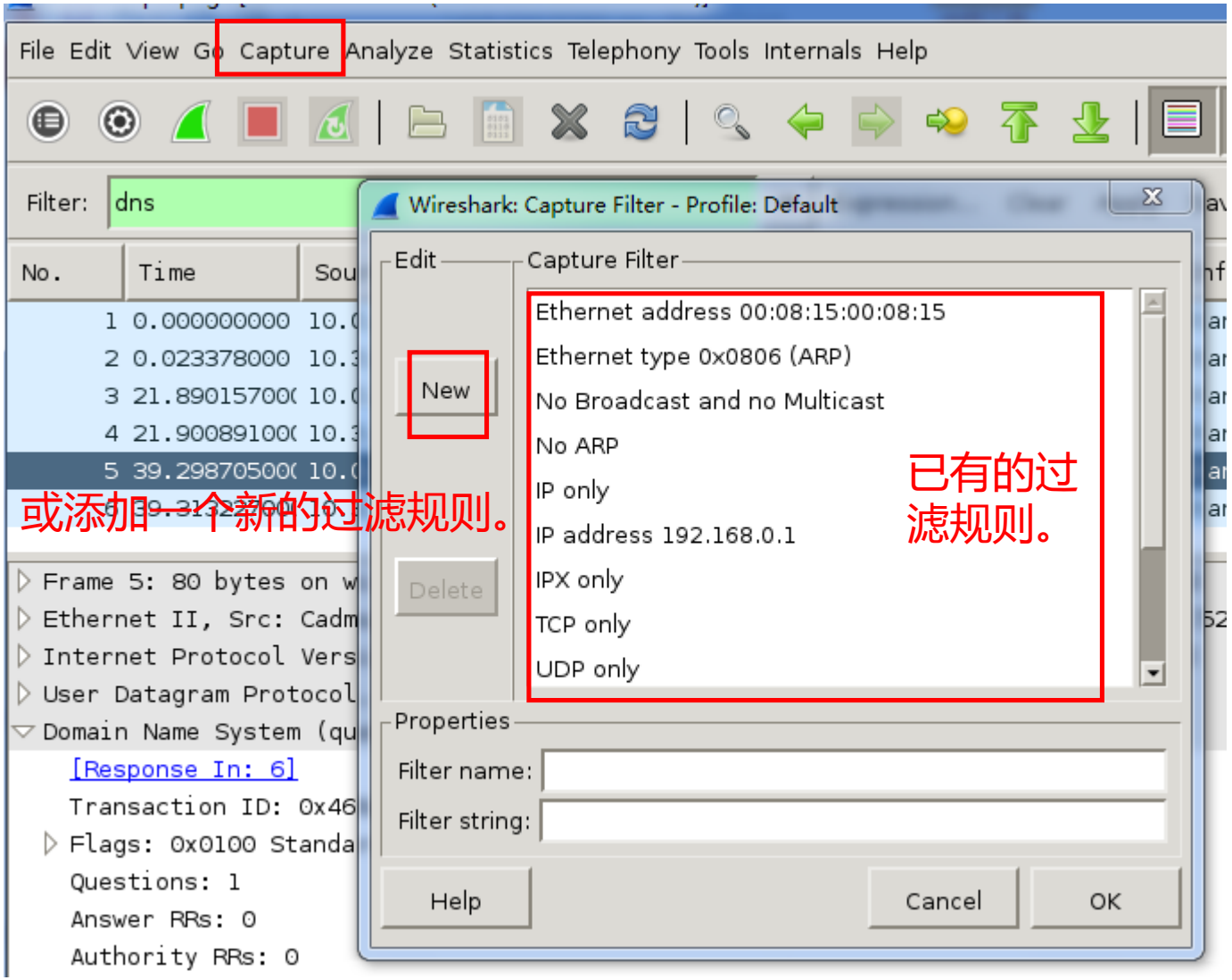
- A network protocol analyzer (packet sniffer)
- Official website
  - http://www.wireshark.org/
- Renamed from Ethereal in 2006
- Able to capture packets transferred on the network and display packet fields and their meanings
- Used for network troubleshooting, analysis, software and communications protocol 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



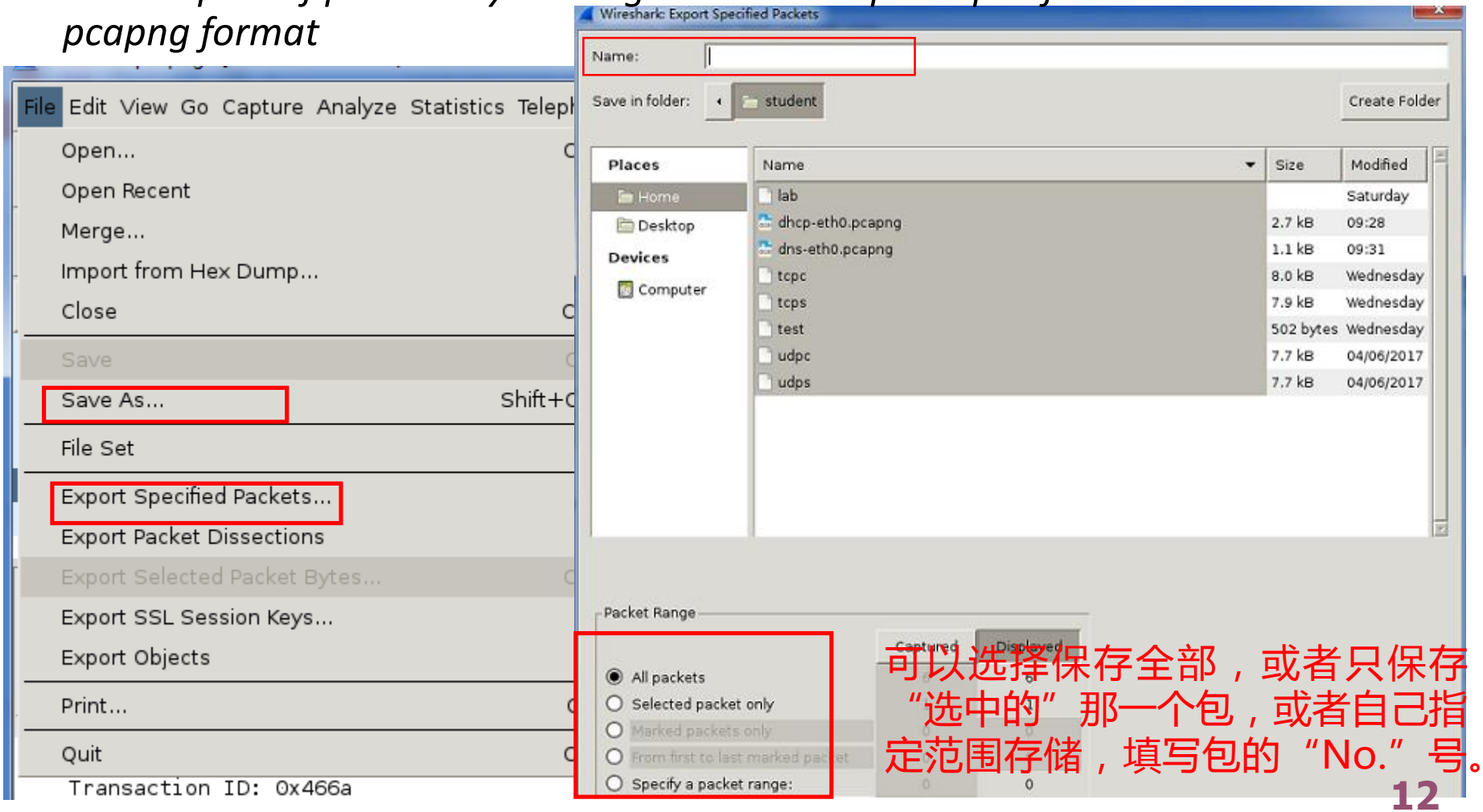
Manage Capture Filter

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



Save your capturing

- *Save all packets by clicking "Flie" → "save as " as pcapng format*
- *Choose part of packets by clicking "File" → "Export Specified Packets" as pcapng format*

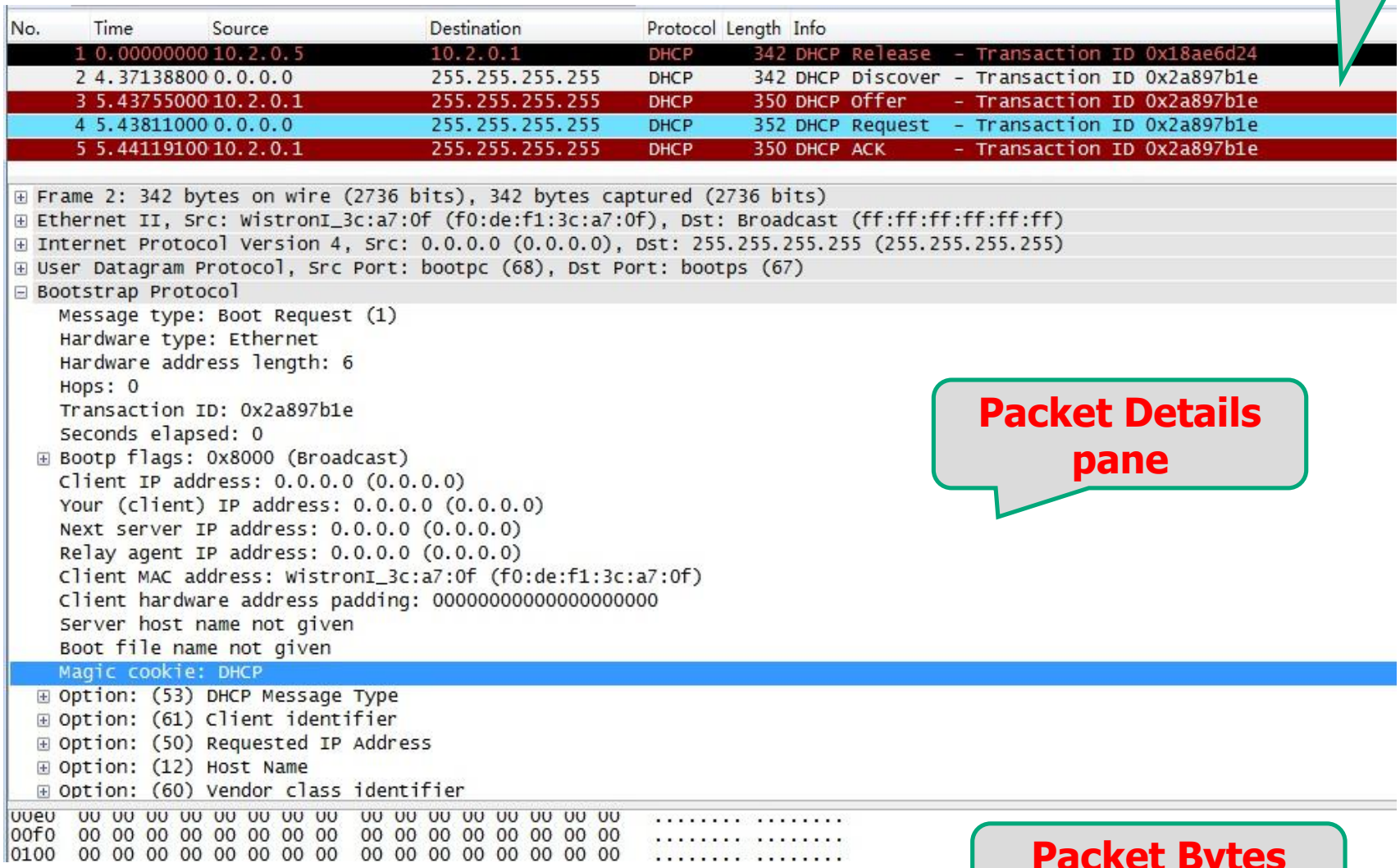


How to initiate the communications?

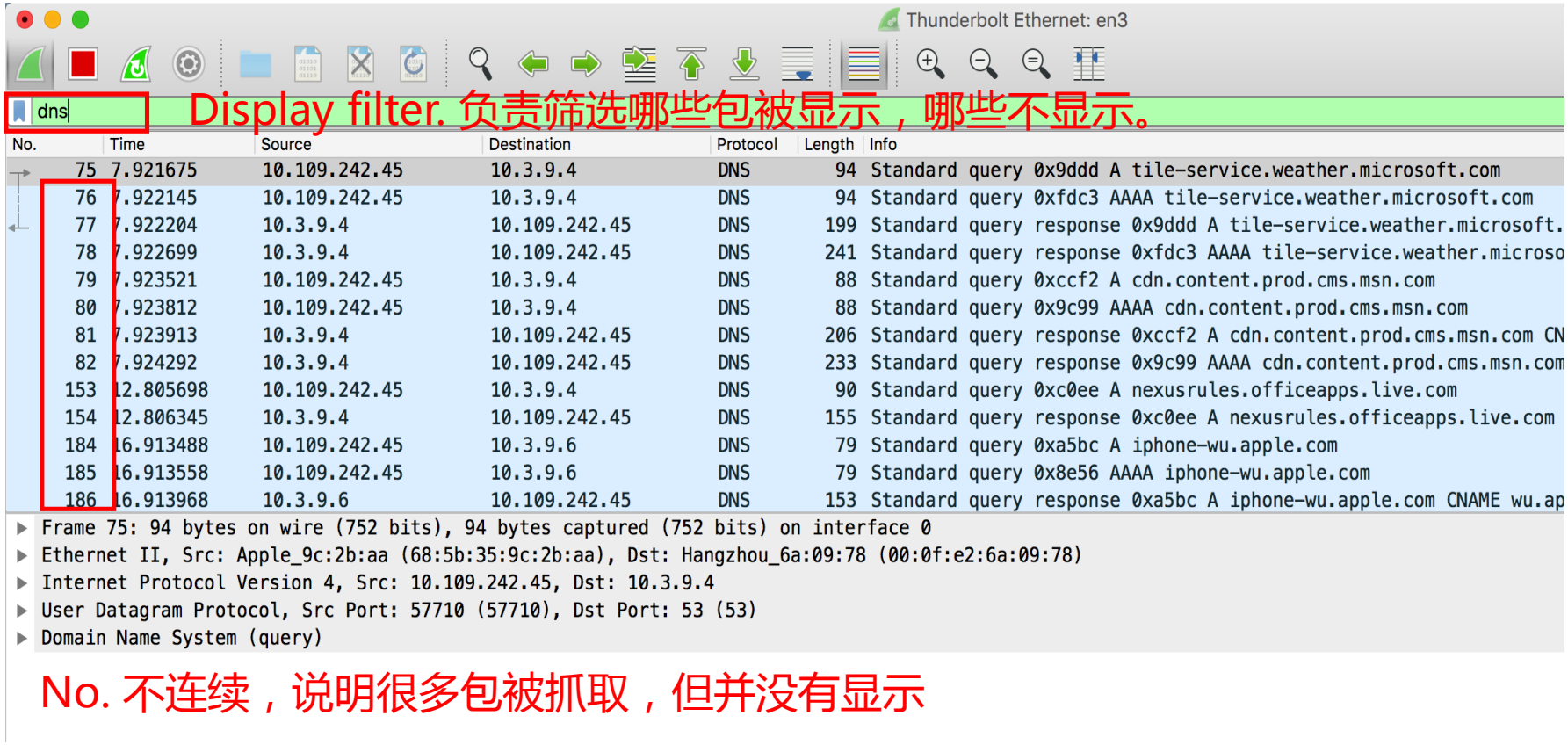
- DHCP
  - Start wireshark, set capture options
    - ✓in xShell or Terminal，#sudo wireshark &
  - Initiate DHCP procedure
    - ✓In xShell or Terminal，#sudo dhclient -r eth0;sudo dhclient eth0
- DNS
  - Start Wireshark, set capture options
    - ✓in xShell or Terminal, #sudo wireshark &
  - use nslookup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



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



No. 不连续，说明很多包被抓取，但并没有显示