Lab1 - WireShark

Introduction to Computer Networks

2023/03/09

Download & Install VirtualBox

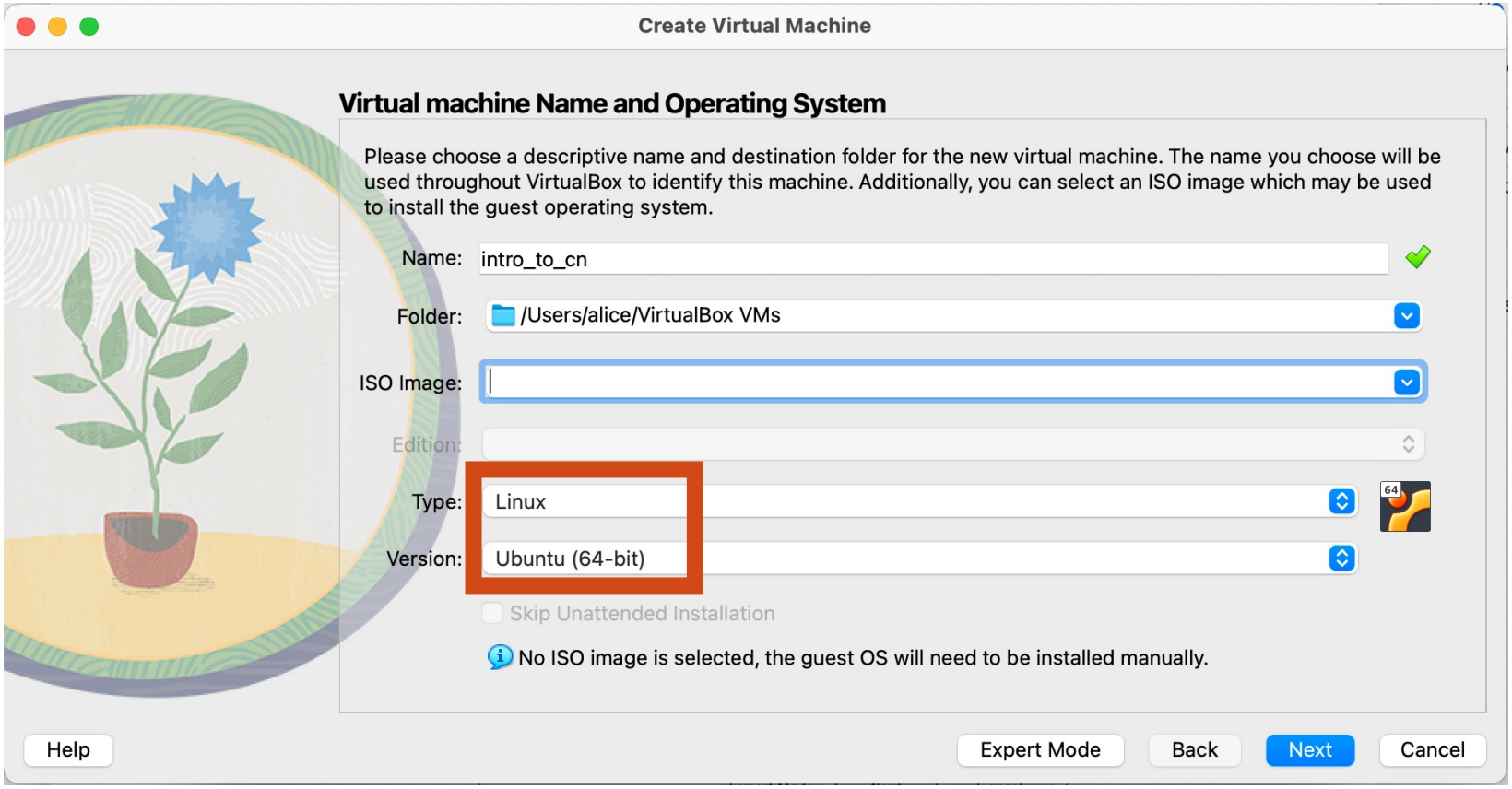
- VirtualBox
- Allows users to extend their existing computer to run multiple operating systems.
  - Download
  - Virtual disk file

- Inside the Virtual Disk, you will already have:
  - Ubuntu OS
  - VS Code
  - Wireshark

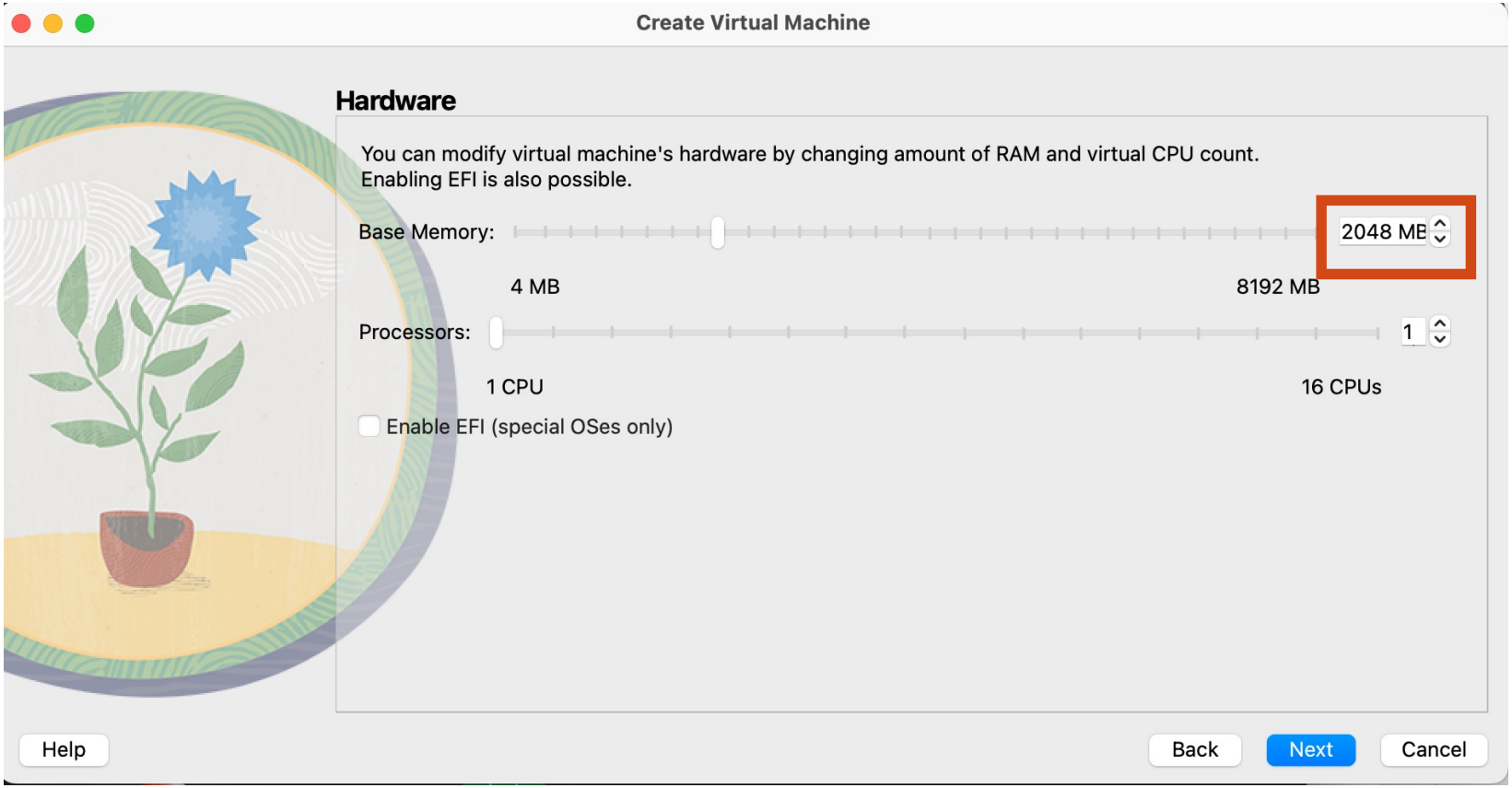
VirtualBox


Oracle VM VirtualBox Manager
BETA
Tools
Preferences
Import
Export
New
Add
Dev Preview
Welcome to VirtualBox!
The left part of application window contains global tools and lists all virtual machines and virtual machine groups on your computer. You can import, add and create new VMs using corresponding toolbar buttons. You can popup a tools of currently selected element using corresponding element button.
You can press the ⌘? key to get instant help, or visit www.virtualbox.org for more information and latest news.

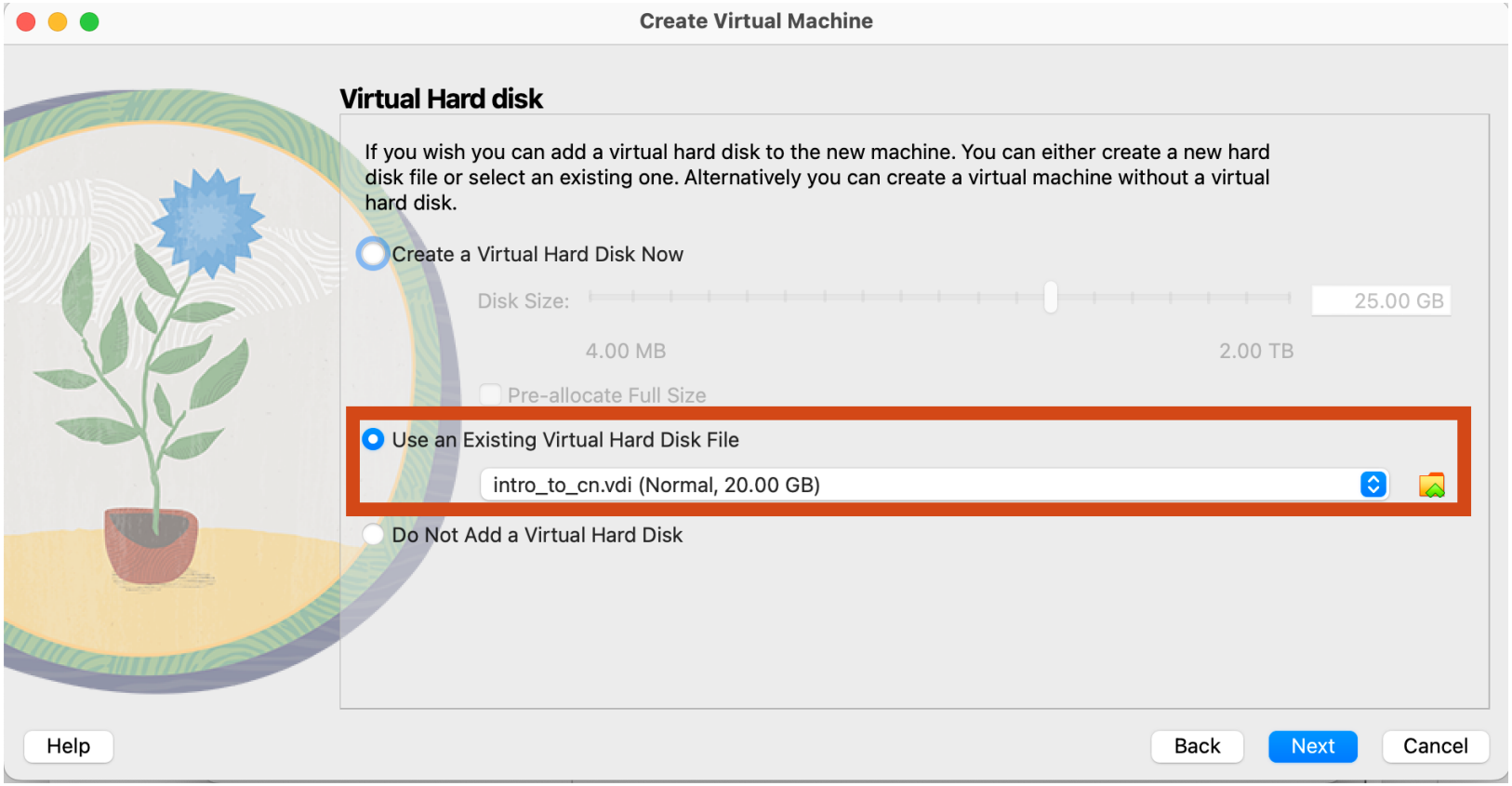
VirtualBox


Create Virtual Machine
Virtual machine Name and Operating System
Please choose a descriptive name and destination folder for the new virtual machine. The name you choose will be used throughout VirtualBox to identify this machine. Additionally, you can select an ISO image which may be used to install the guest operating system.
Name: intro_to_cn
Folder: /Users/alice/VirtualBox VMs
ISO Image:
Edition:
Type: Linux
Version: Ubuntu (64-bit)
Skip Unattended Installation
No ISO image is selected, the guest OS will need to be installed manually.
Help
Expert Mode
Back
Next
Cancel

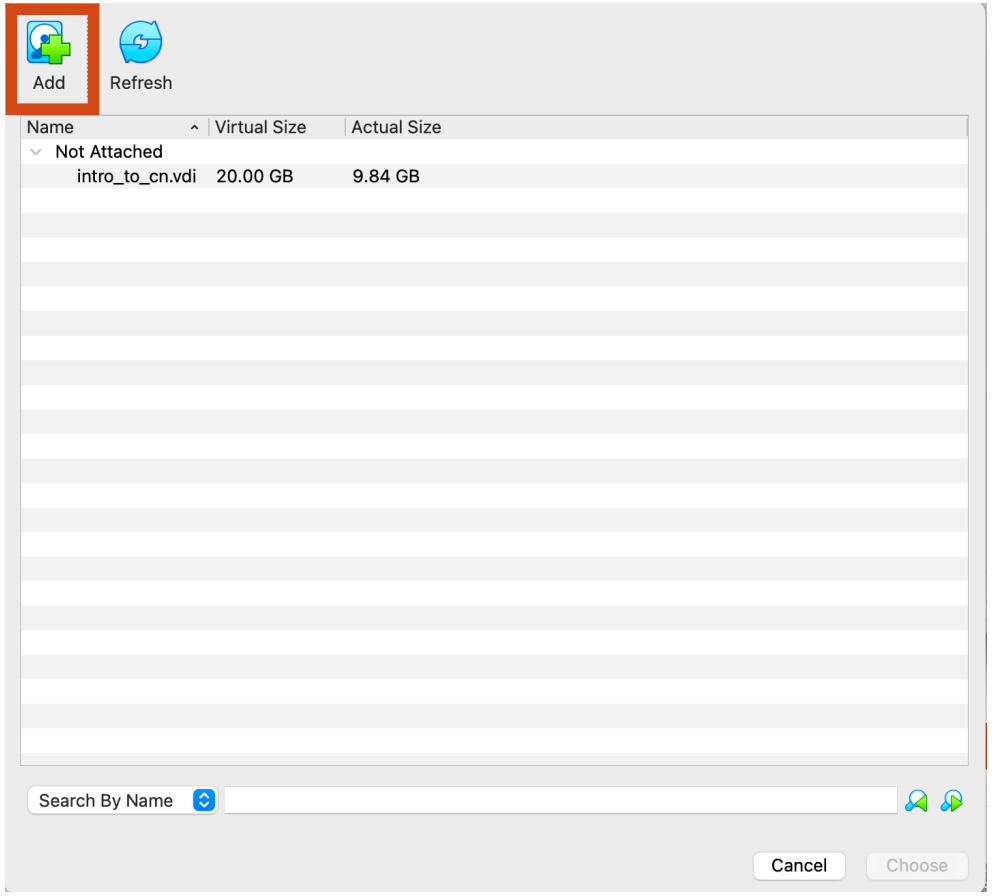
VirtualBox


Create Virtual Machine
Hardware
You can modify virtual machine's hardware by changing amount of RAM and virtual CPU count.
Enabling EFI is also possible.
Base Memory:
2048 MB
4 MB
8192 MB
Processors:
1
1 CPU
16 CPUs
Enable EFI (special OSes only)
Help
Back
Next
Cancel

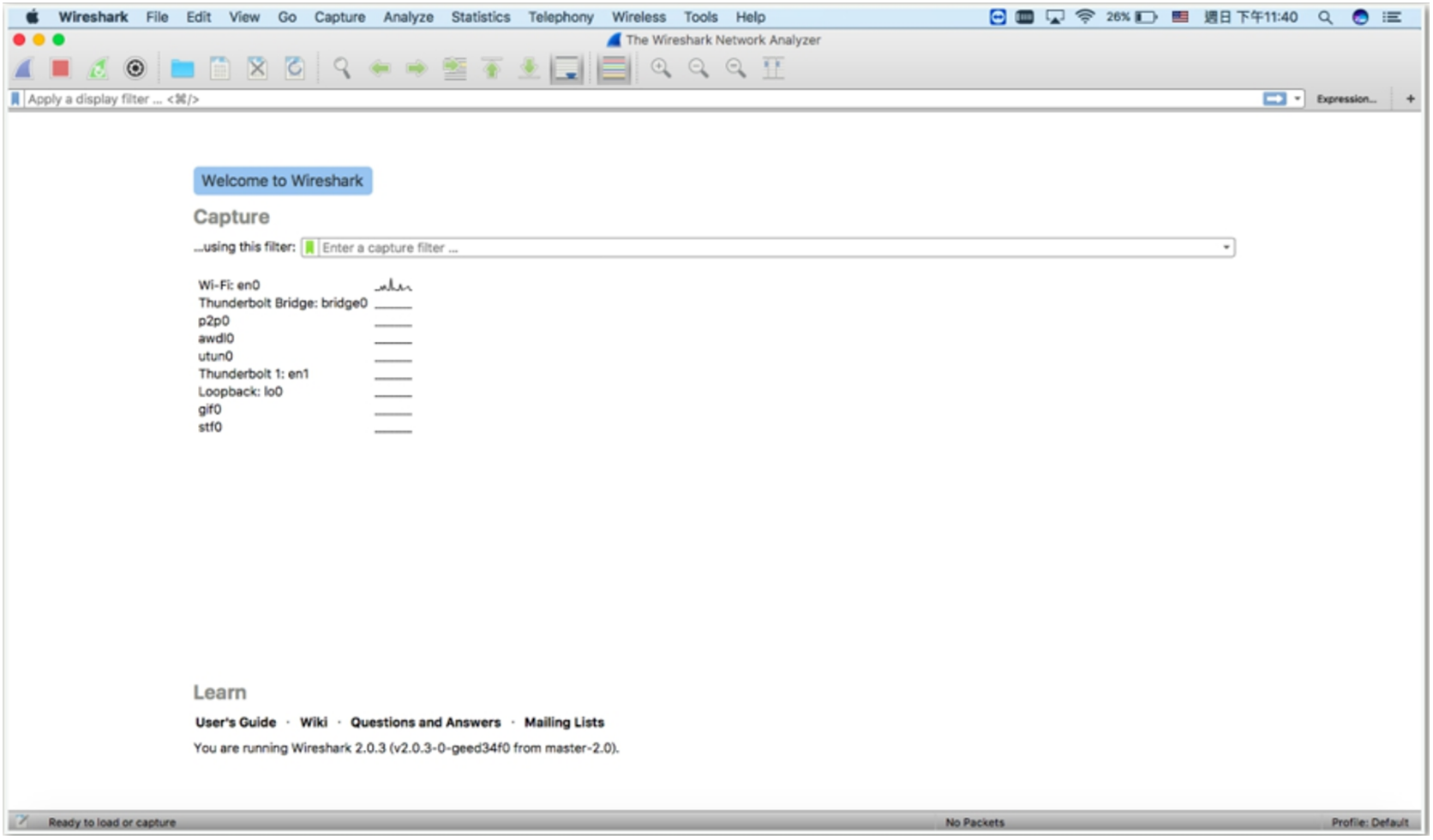
VirtualBox


Create Virtual Machine
Virtual Hard disk
If you wish you can add a virtual hard disk to the new machine. You can either create a new hard disk file or select an existing one. Alternatively you can create a virtual machine without a virtual hard disk.
Create a Virtual Hard Disk Now
Disk Size:
25.00 GB
4.00 MB
2.00 TB
Pre-allocate Full Size
Use an Existing Virtual Hard Disk File
intro_to_cn.vdi (Normal, 20.00 GB)
Do Not Add a Virtual Hard Disk
Help
Back
Next
Cancel

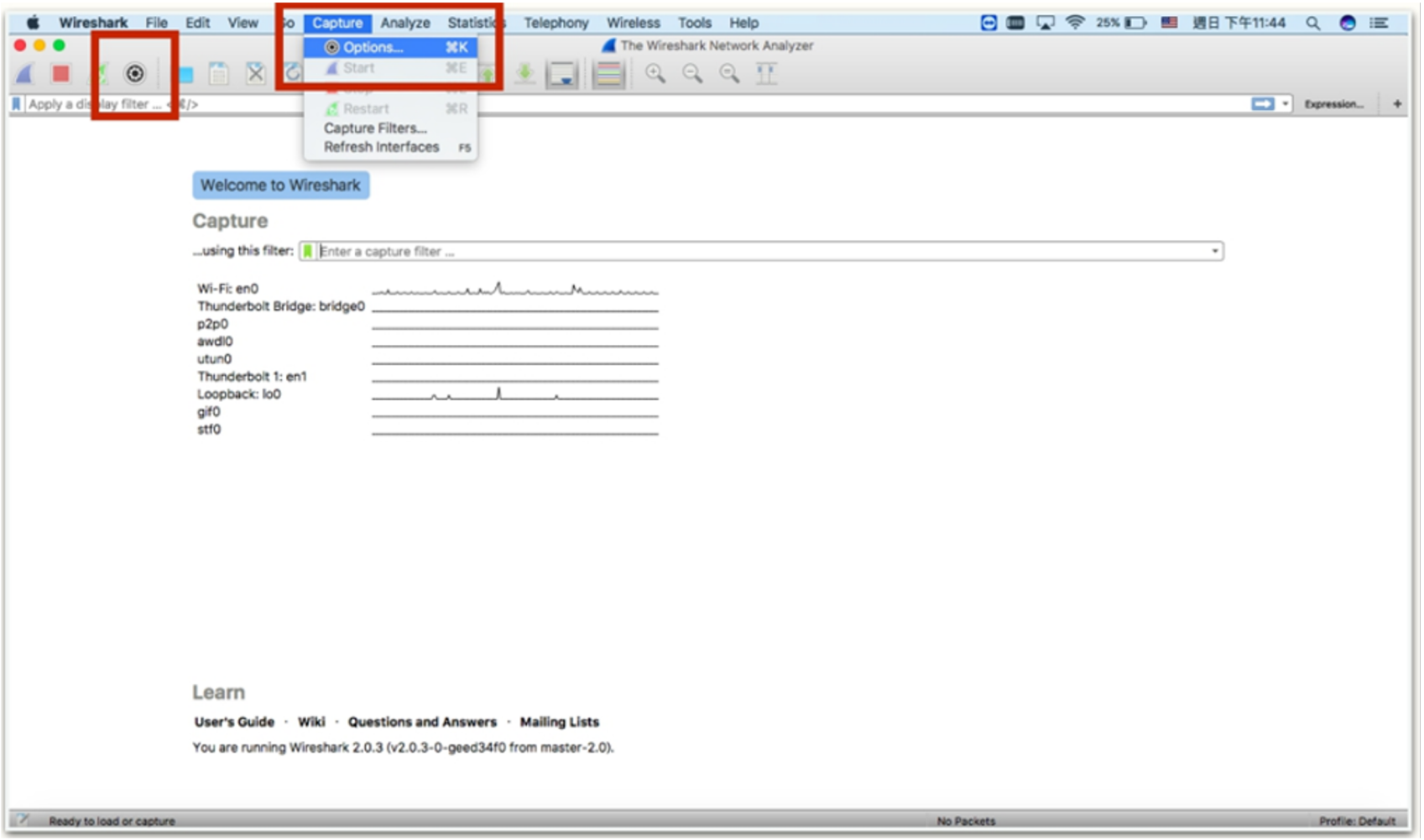
VirtualBox


Add
Refresh
Name
Virtual Size
Actual Size
Not Attached
intro_to_cn.vdi
20.00 GB
9.84 GB
Search By Name
Cancel
Choose

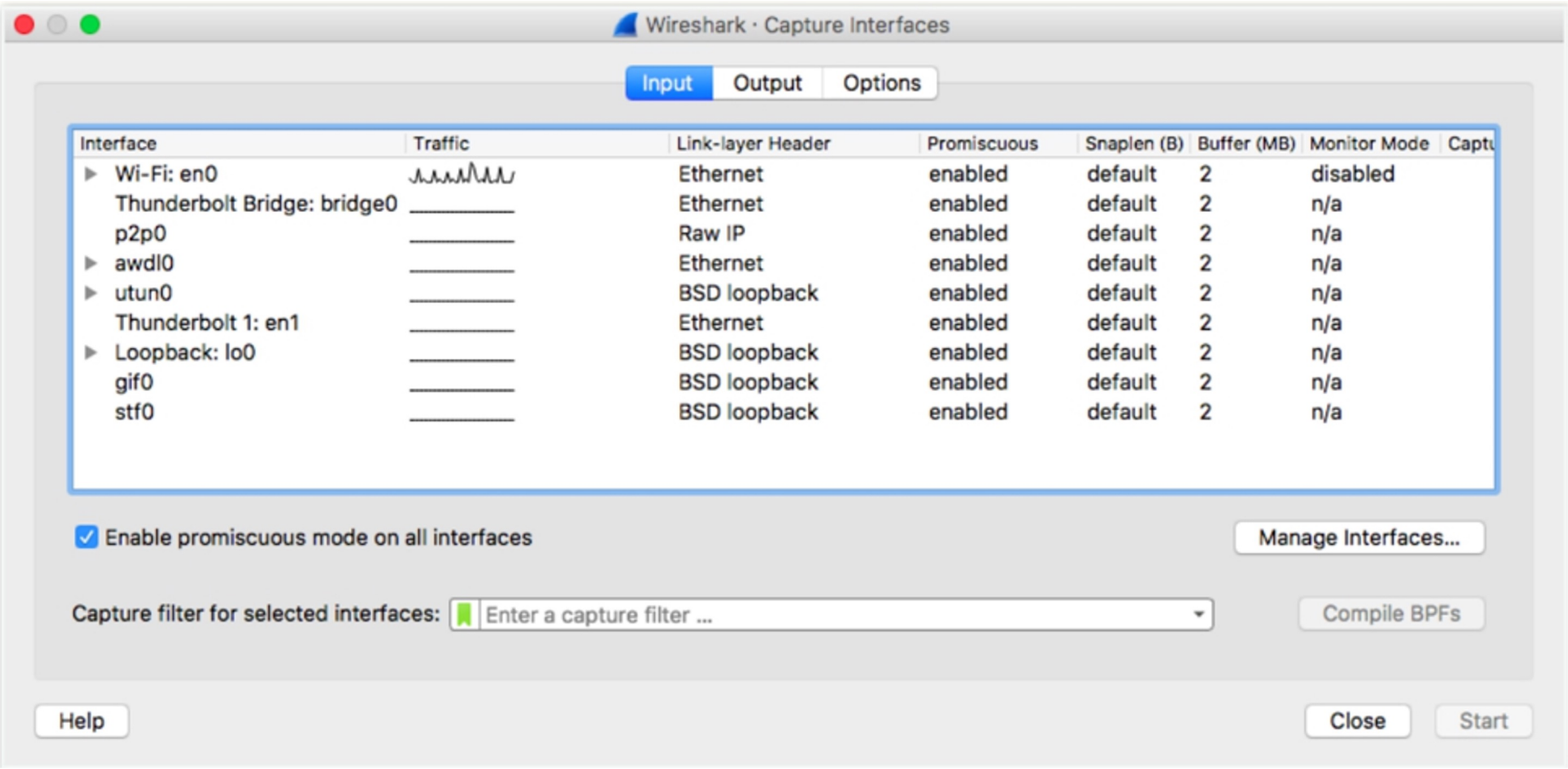
Wireshark: Capture interface



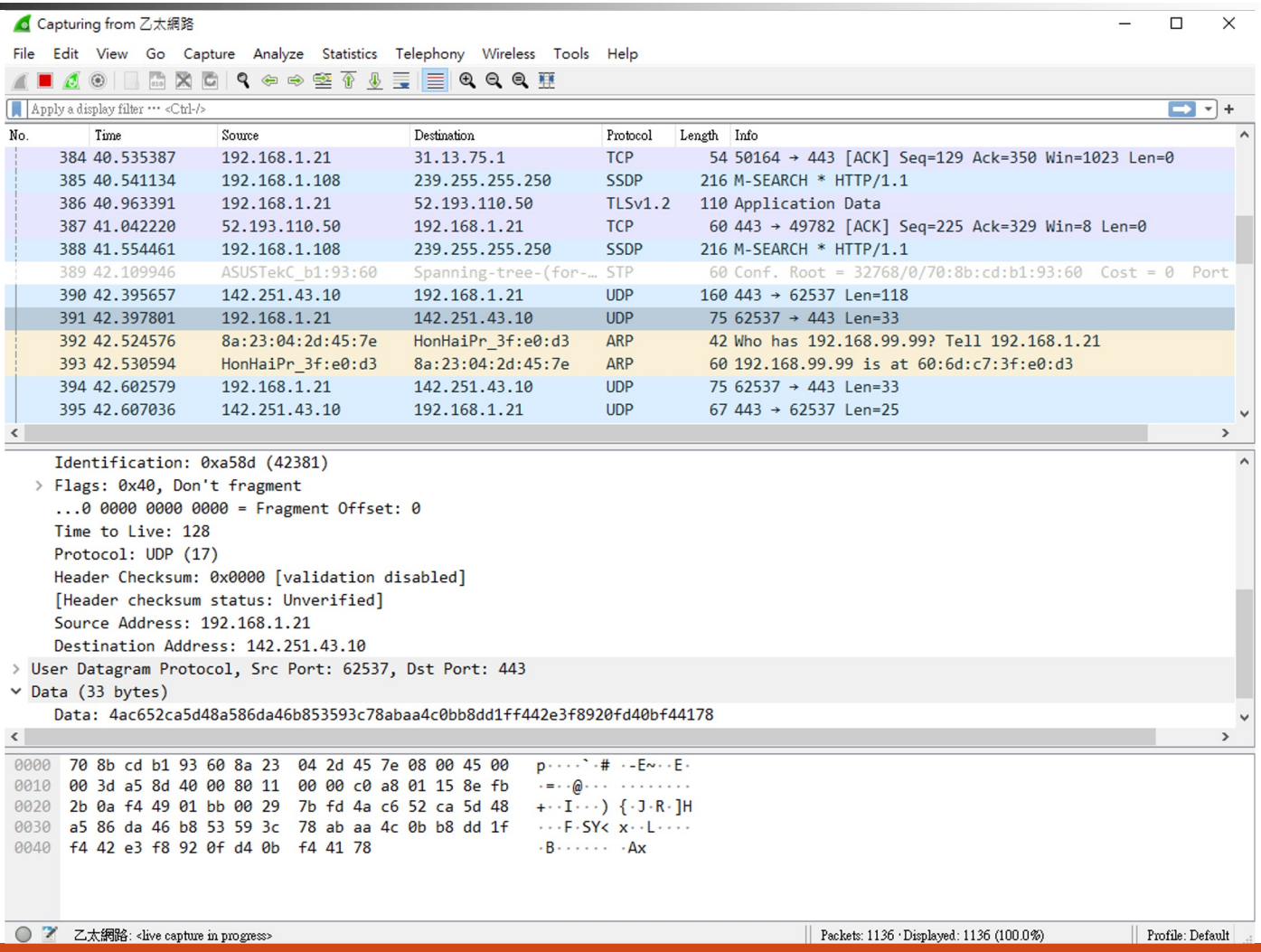
Wireshark: Capture interface



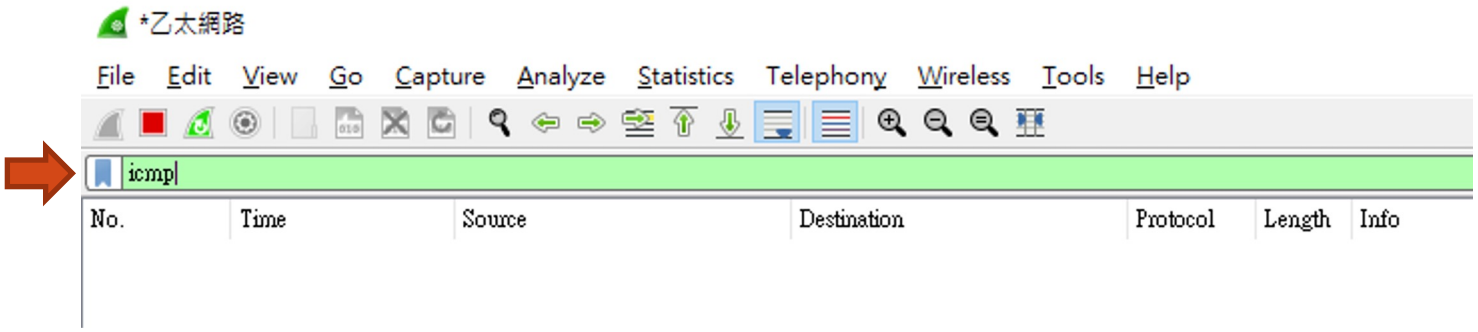
Wireshark: Capture interface



Wireshark: Data interface

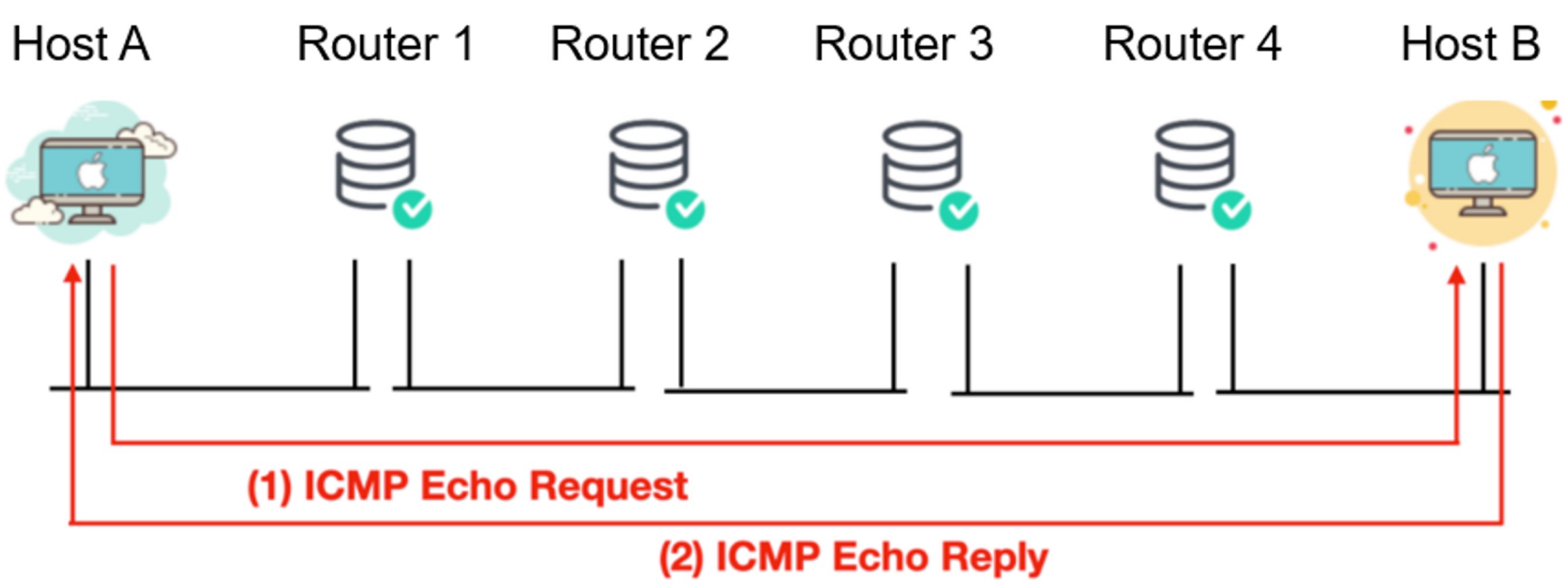


Wireshark: Check ping package



ICMP and ping

- ICMP : Internet Control Message Protocol



DNS

- DNS : Domain Name System
  - Hostname to IP address translation
- Google Public DNS
  - Google provides a free DNS
  - IPv4 address :
    - 8.8.8.8 (google-public-dns-a.google.com)
    - 8.8.4.4 (google-public-dns-b.google.com)

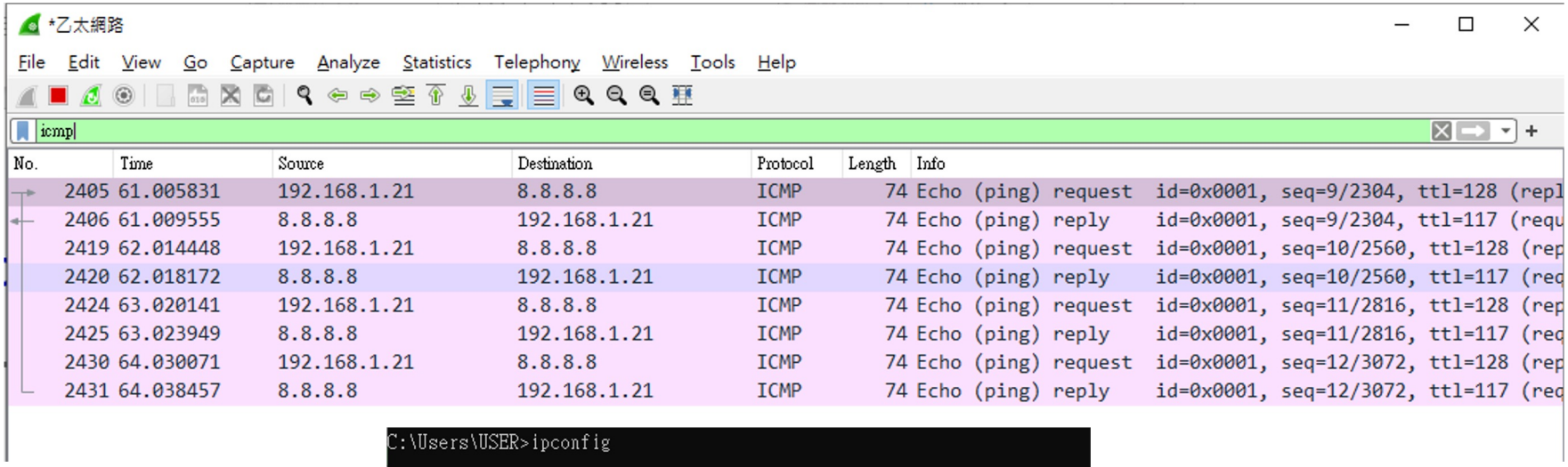
Check ping package

```
C:\Users\USER>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=4ms TTL=117
Reply from 8.8.8.8: bytes=32 time=3ms TTL=117
Reply from 8.8.8.8: bytes=32 time=3ms TTL=117
Reply from 8.8.8.8: bytes=32 time=3ms TTL=117

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 4ms, Average = 3ms
```

Check ping package




```
C:\Users\USER>ipconfig

Windows IP Configuration


Ethernet adapter 乙太網路:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::81ef:fb41:fb3b:8e22%9
   IPv4 Address. . . . . . . . . . . : 192.168.1.21
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . : 192.168.1.1

Ethernet adapter VirtualBox Host-Only Network:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::c149:ba75:f83e:7f06%11
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
```

WireShark filter

Use filter to find the packets we need.

- Ex 1: request method

```
http.request.method == "POST"
```

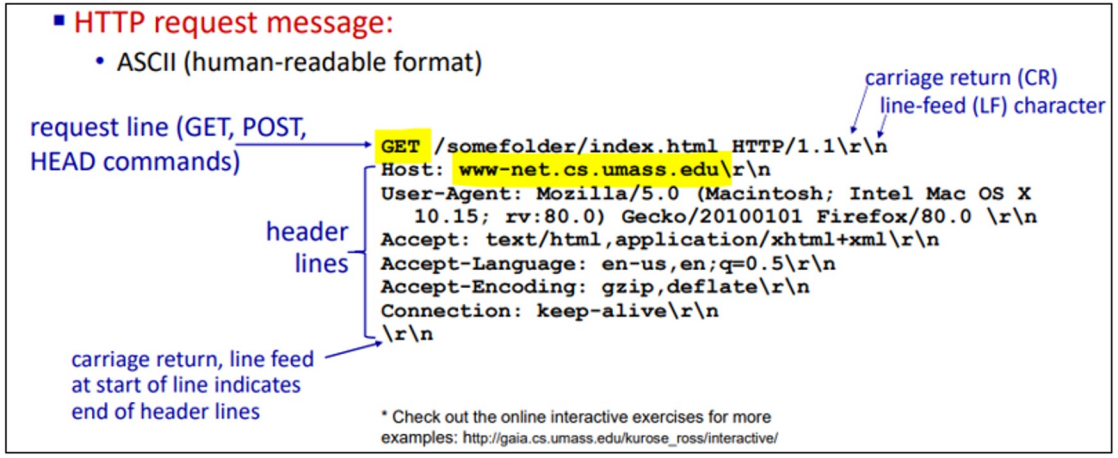
- Ex 2: src/dst

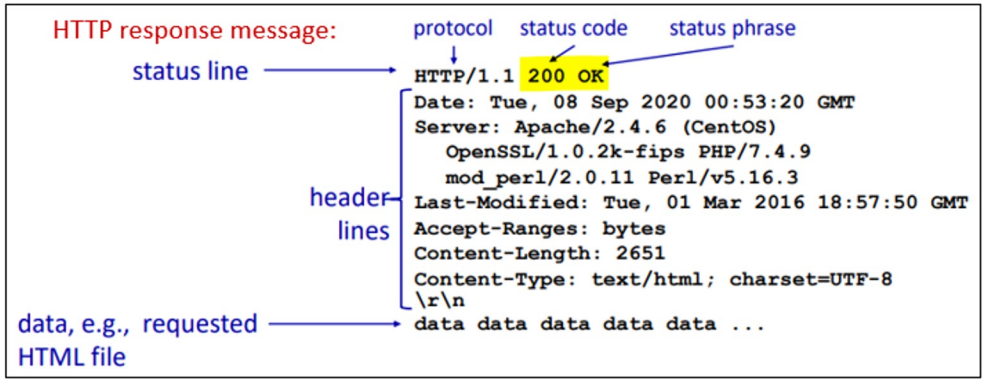
```
ip.src == 140.114.69.135
ip.dst == www.nthu.edu.tw
```

- Ex 3: status

```
http.response.code == 200
```

- For more example, check manual.





Curl

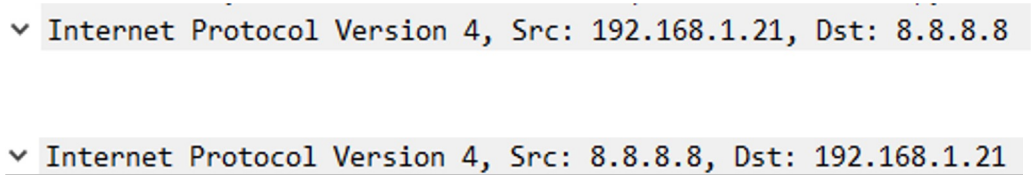
- Curl is a command-line utility that allows users to create network requests.

```
[(base) alice@Alices-MacBook-Air ~ % curl -X POST --data "input=11001234"]
  http://140.114.79.144/index.php
Your student ID is: 11001234
```

- **-X** : Use the specified http method to issue an http request
- **--data** : Carry HTTP POST data
- **“input=[insert your student ID]”** : e.g “input=11001234”
- **http://140.114.79.144/index.php** : URL that get request
- Your student ID is: 11001234 : response

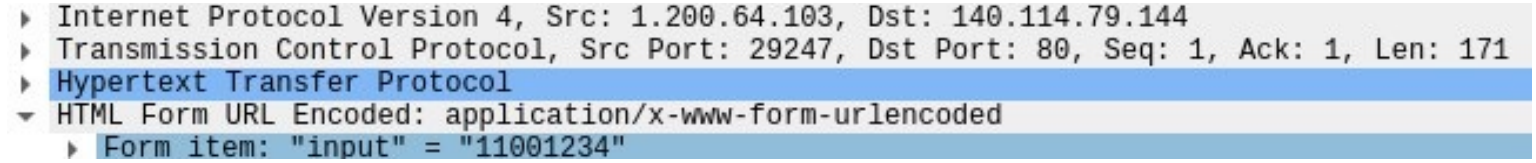
Lab1

- 1. Check your ping package (70%)
  - Screenshot the following:



Lab1

- 2. Check your POST package (30%)
  - Screenshot the following:




```
(base) alice@Alices-MacBook-Air ~ % curl -X POST --data "input=11001234"
 http://140.114.79.144/index.php
Your student ID is: 11001234
```

Lab1

3. Put all of the screenshots in one PDF file.
- Name the file **Lab1_studentID.pdf**
  - (e.g Lab1_11001234.pdf)
- Upload to eeclass!