

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





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: ✓

Folder:

ISO Image:

Edition:

Type: Ubuntu (64-bit) 64

Version:

Skip Unattended Installation

i No ISO image is selected, the guest OS will need to be installed manually.

Help Expert Mode Back **Next** Cancel





VirtualBox

Create Virtual Machine

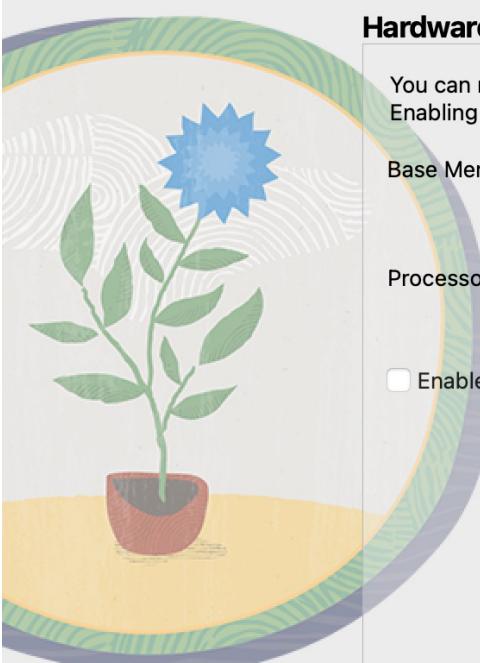
Hardware

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

Processors: 1 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

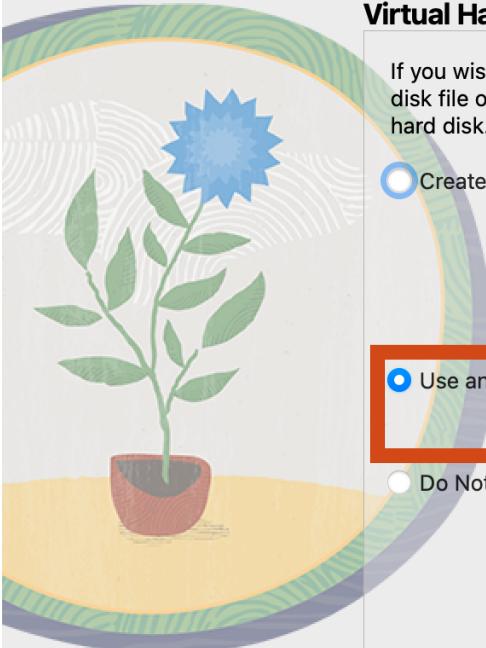
Pre-allocate Full Size

Use an Existing Virtual Hard Disk File

intro_to_cn.vdi (Normal, 20.00 GB)

Do Not Add a Virtual Hard Disk

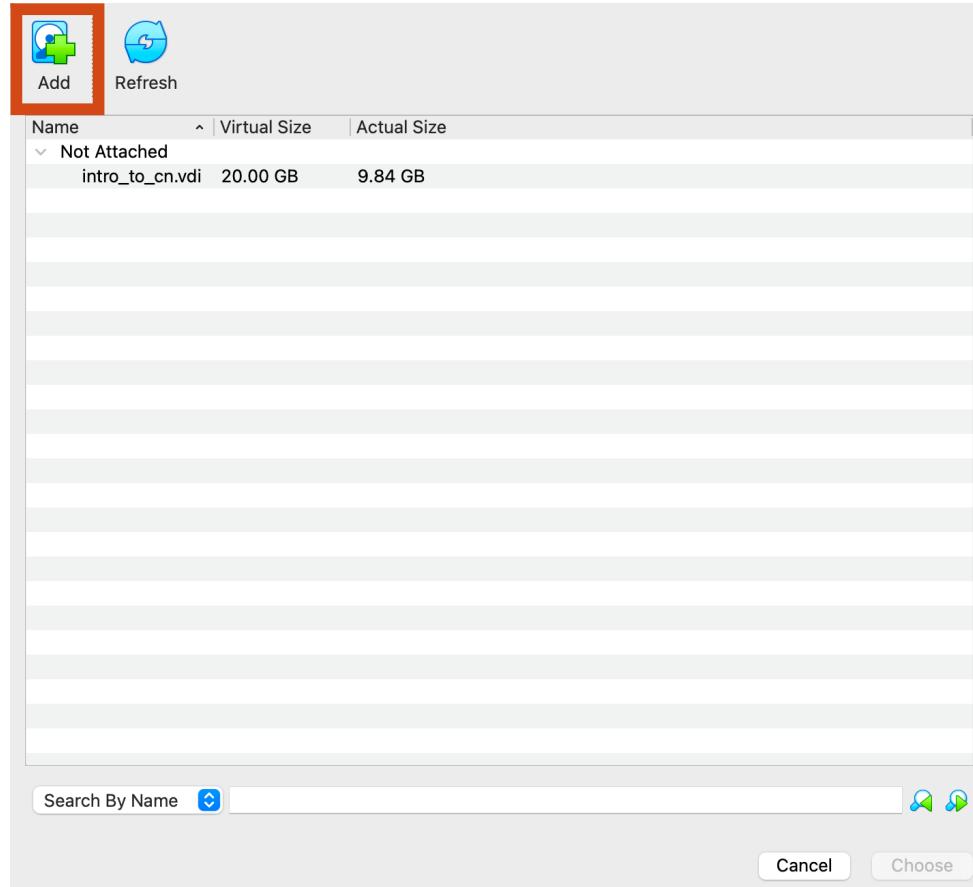
Help Back Next Cancel



The screenshot shows the 'Create Virtual Machine' wizard in VirtualBox. The current step is 'Virtual Hard disk'. It provides options to create a new disk, use an existing one, or skip it. A red box highlights the 'Use an Existing Virtual Hard Disk File' option, which is selected. The 'intro_to_cn.vdi' file is listed as an existing disk, showing its size as 20.00 GB and type as Normal. The background features a decorative illustration of a potted plant with a blue flower.



VirtualBox





Wireshark: Capture interface

The screenshot shows the Wireshark application window. The title bar reads "Wireshark" and "The Wireshark Network Analyzer". The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains icons for opening files, saving, zooming, and capturing. A search bar at the top right has the placeholder "Expression...". Below the toolbar is a status bar with "Apply a display filter ... <%>" and a plus sign icon. The main area is titled "Capture" with a sub-section "Welcome to Wireshark". It displays a list of available interfaces:

- Wi-Fi: en0
- Thunderbolt Bridge: bridge0
- p2p0
- awdl0
- utun0
- Thunderbolt 1: en1
- Loopback: lo0
- gif0
- stf0

At the bottom, there are links for "Learn" (User's Guide, Wiki, Questions and Answers, Mailing Lists) and a note: "You are running Wireshark 2.0.3 (v2.0.3-0-geed34f0 from master-2.0)." The status bar at the bottom also shows "Ready to load or capture", "No Packets", and "Profile: Default".



Wireshark: Capture interface

The screenshot shows the Wireshark application window. At the top, the menu bar includes 'Wireshark', 'File', 'Edit', 'View', 'Go', 'Capture' (which is currently selected and highlighted with a red box), 'Analyze', 'Statistics', 'Telephony', 'Wireless', 'Tools', and 'Help'. Below the menu is a toolbar with various icons. A dropdown menu is open under the 'Capture' menu, showing options like 'Options...', 'Start' (with a keyboard shortcut of ⌘E), 'Restart', 'Capture Filters...', and 'Refresh Interfaces'. The main pane is titled 'Capture' and contains a list of network interfaces: 'Wi-Fi: en0', 'Thunderbolt Bridge: bridge0', 'p2p0', 'awd10', 'utun0', 'Thunderbolt 1: en1', 'Loopback: lo0', 'gif0', and 'stf0'. Below this list is a section titled 'Learn' with links to 'User's Guide', 'Wiki', 'Questions and Answers', and 'Mailing Lists'. A status bar at the bottom indicates 'Ready to load or capture', 'No Packets', and 'Profile: Default'.



Wireshark: Capture interface

Wireshark · Capture Interfaces

Input **Output** **Options**

Interface	Traffic	Link-layer Header	Promiscuous	Snaplen (B)	Buffer (MB)	Monitor Mode	Captu
► Wi-Fi: en0	WWWWWWWW	Ethernet	enabled	default	2	disabled	
Thunderbolt Bridge: bridge0	_____	Ethernet	enabled	default	2	n/a	
p2p0	_____	Raw IP	enabled	default	2	n/a	
► awdl0	_____	Ethernet	enabled	default	2	n/a	
► utun0	_____	BSD loopback	enabled	default	2	n/a	
Thunderbolt 1: en1	_____	Ethernet	enabled	default	2	n/a	
► Loopback: lo0	_____	BSD loopback	enabled	default	2	n/a	
gif0	_____	BSD loopback	enabled	default	2	n/a	
stf0	_____	BSD loopback	enabled	default	2	n/a	

Enable promiscuous mode on all interfaces Manage Interfaces...

Capture filter for selected interfaces: Compile BPFs

Help Close Start



Wireshark: Data interface

Capturing from 乙太網路

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
384	40.535387	192.168.1.21	31.13.75.1	TCP	54	50164 → 443 [ACK] Seq=129 Ack=350 Win=1023 Len=0
385	40.541134	192.168.1.108	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
386	40.963391	192.168.1.21	52.193.110.50	TLSv1.2	110	Application Data
387	41.042220	52.193.110.50	192.168.1.21	TCP	60	443 → 49782 [ACK] Seq=225 Ack=329 Win=8 Len=0
388	41.554461	192.168.1.108	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
389	42.109946	ASUSTekC_b1:93:60	Spanning-tree-(for-... STP	STP	60	Conf. Root = 32768/0/70:8b:cd:b1:93:60 Cost = 0 Port
390	42.395657	142.251.43.10	192.168.1.21	UDP	160	443 → 62537 Len=118
391	42.397801	192.168.1.21	142.251.43.10	UDP	75	62537 → 443 Len=33
392	42.524576	8a:23:04:2d:45:7e	HonHaiPr_3f:e0:d3	ARP	42	Who has 192.168.99.99? Tell 192.168.1.21
393	42.530594	HonHaiPr_3f:e0:d3	8a:23:04:2d:45:7e	ARP	60	192.168.99.99 is at 60:6d:c7:3f:e0:d3
394	42.602579	192.168.1.21	142.251.43.10	UDP	75	62537 → 443 Len=33
395	42.607036	142.251.43.10	192.168.1.21	UDP	67	443 → 62537 Len=25

Identification: 0xa58d (42381)

Flags: 0x40, Don't fragment
...0 0000 0000 0000 = Fragment Offset: 0

Time to Live: 128

Protocol: UDP (17)

Header Checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]

Source Address: 192.168.1.21

Destination Address: 142.251.43.10

User Datagram Protocol, Src Port: 62537, Dst Port: 443

Data (33 bytes)
Data: 4ac652ca5d48a586da46b853593c78abaa4c0bb8dd1ff442e3f8920fd40bf44178

0000	70 8b cd b1 93 60 8a 23 04 2d 45 7e 08 00 45 00	p.....# --E~--E-
0010	00 3d a5 8d 40 00 80 11 00 00 c0 a8 01 15 8e fb	=...@....
0020	2b 0a f4 49 01 bb 00 29 7b fd 4a c6 52 ca 5d 48	+..I...) { -J-R-]H
0030	a5 86 da 46 b8 53 59 3c 78 ab aa 4c 0b b8 dd 1f	...F-SY< x..L....
0040	f4 42 e3 f8 92 0f d4 0b f4 41 78	.B..... Ax

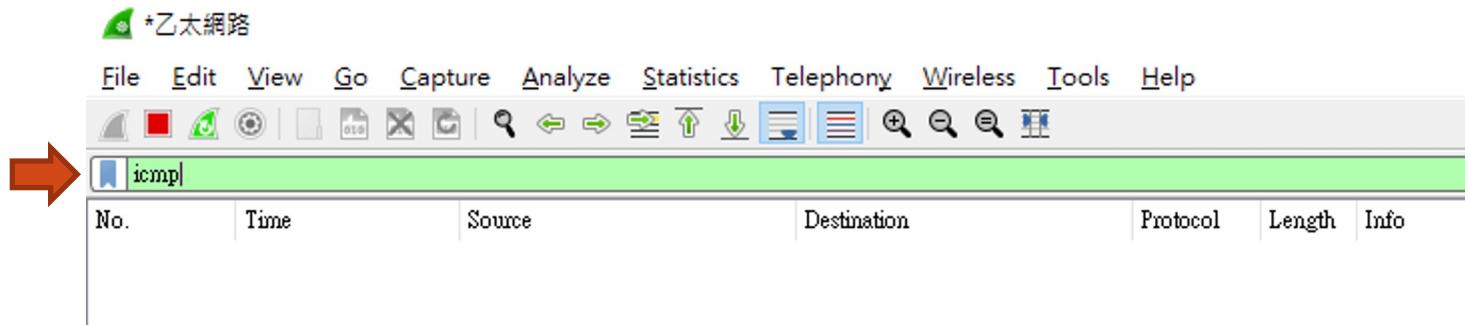
乙太網路: <live capture in progress>

Packets: 1136 · Displayed: 1136 (100.0%)

Profile: Default



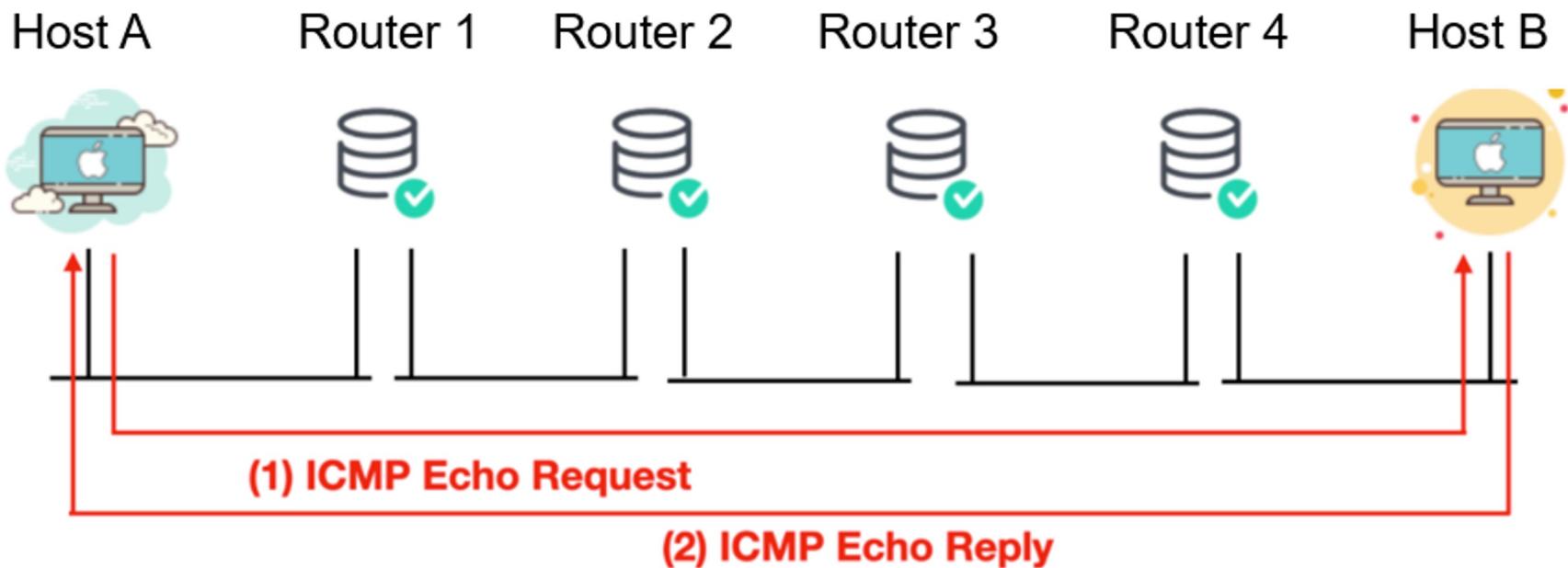
Wireshark: Check ping package





ICMP and ping

- ICMP : Internet Control Message Protocol





- 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

*乙太網路

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

No.	Time	Source	Destination	Protocol	Length	Info
2405	61.005831	192.168.1.21	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=9/2304, ttl=128 (req1)
2406	61.009555	8.8.8.8	192.168.1.21	ICMP	74	Echo (ping) reply id=0x0001, seq=9/2304, ttl=117 (rep1)
2419	62.014448	192.168.1.21	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=10/2560, ttl=128 (req2)
2420	62.018172	8.8.8.8	192.168.1.21	ICMP	74	Echo (ping) reply id=0x0001, seq=10/2560, ttl=117 (rep2)
2424	63.020141	192.168.1.21	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=11/2816, ttl=128 (req3)
2425	63.023949	8.8.8.8	192.168.1.21	ICMP	74	Echo (ping) reply id=0x0001, seq=11/2816, ttl=117 (rep3)
2430	64.030071	192.168.1.21	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=12/3072, ttl=128 (req4)
2431	64.038457	8.8.8.8	192.168.1.21	ICMP	74	Echo (ping) reply id=0x0001, seq=12/3072, ttl=117 (rep4)

```
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](#).

■ HTTP request message:

- ASCII (human-readable format)

request line (GET, POST,
HEAD commands)

```
GET /somefolder/index.html HTTP/1.1\r\n  
Host: www-net.cs.umass.edu\r\n  
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X  
10.15; rv:80.0) Gecko/20100101 Firefox/80.0 \r\n  
Accept: text/html,application/xhtml+xml\r\n  
Accept-Language: en-us,en;q=0.5\r\n  
Accept-Encoding: gzip,deflate\r\n  
Connection: keep-alive\r\n\r\n
```

header
lines

carriage return, line feed
at start of line indicates
end of header lines

carriage return (CR)
line-feed (LF) character

* Check out the online interactive exercises for more
examples: http://gaia.cs.umass.edu/kurose_ross/interactive/

HTTP response message:

status line

protocol status code status phrase

HTTP/1.1 200 OK

```
Date: Tue, 08 Sep 2020 00:53:20 GMT  
Server: Apache/2.4.6 (CentOS)  
OpenSSL/1.0.2k-fips PHP/7.4.9  
mod_perl/2.0.11 Perl/v5.16.3  
Last-Modified: Tue, 01 Mar 2016 18:57:50 GMT  
Accept-Ranges: bytes  
Content-Length: 2651  
Content-Type: text/html; charset=UTF-8  
\r\n  
data data data data data ...
```

header
lines

data, e.g., requested
HTML file



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:

▼ Internet Protocol Version 4, Src: 192.168.1.21, Dst: 8.8.8.8

▼ Internet Protocol Version 4, Src: 8.8.8.8, Dst: 192.168.1.21



Lab1

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

```
▶ Internet Protocol Version 4, Src: 1.200.64.103, Dst: 140.114.79.144
▶ Transmission Control Protocol, Src Port: 29247, Dst Port: 80, Seq: 1, Ack: 1, Len: 171
▶ Hypertext Transfer Protocol
▼ HTML Form URL Encoded: application/x-www-form-urlencoded
  ▶ Form item: "input" = "11001234"
```

```
[(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!