國立臺灣大學

Assignment 1

Packet Analysis

Prof. Ai-Chun Pang
TA / Yu-Yu Chen, Shao-Cheng Fan, Kuang-Hui Huang

Environment Setup

Environment

- We provide a VirtualBox VM that can run Wireshark in this environment and later assignments.
- Here is information about our environment:
  - Ubuntu 20.04 x64
  - OpenCV 4.2.0 (will be required in later assignments)

VirtualBox Setup

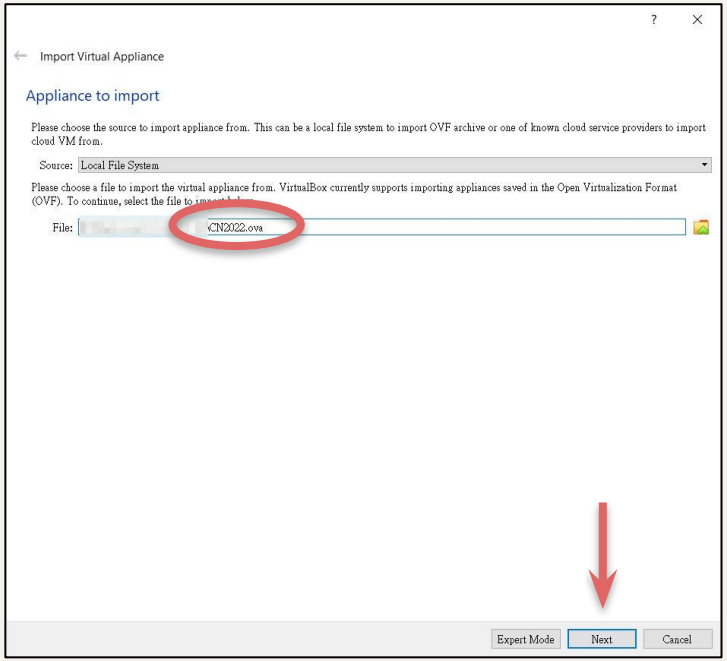
- Download the VM from
  - Our Google Drive
  - The password of our VM is **cn2022**.
- Install Virtualbox (natively installed on the computers of Lab R204).

VirtualBox Setup

- Click “**Import**” to import the “**CN2022.ova**”

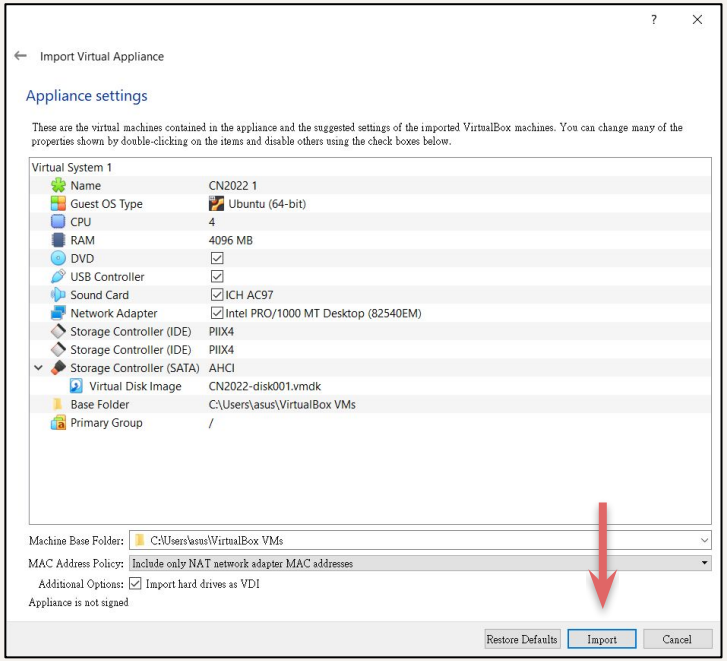
VirtualBox Setup

- Choose “**CN2022.ova**” file and click “**Next**”



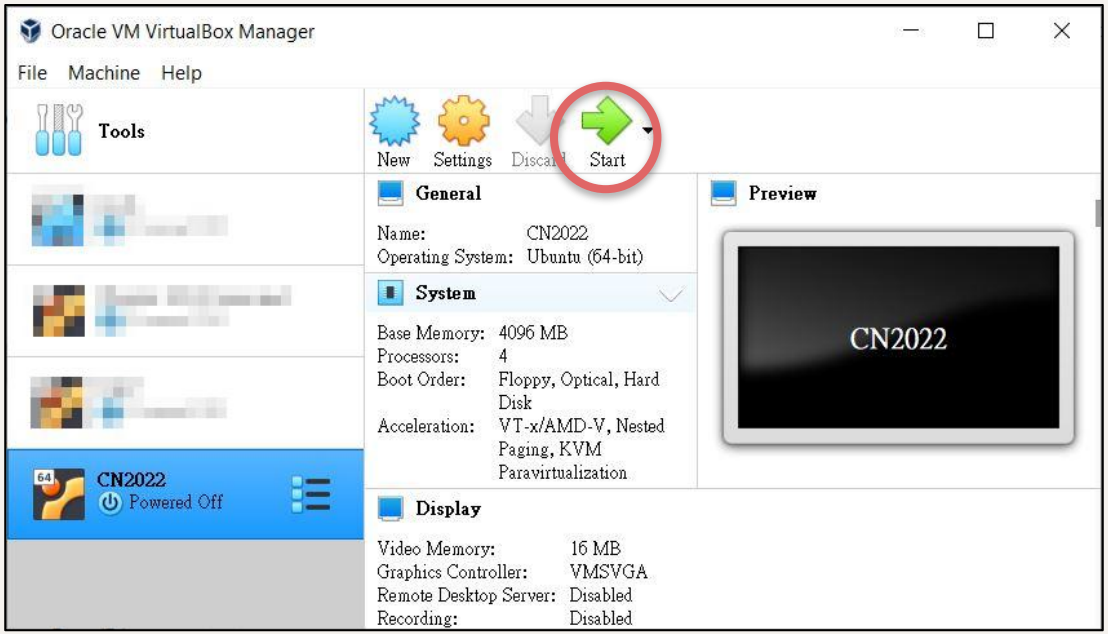
VirtualBox Setup

- Click “**Import**” to import the “**CN2022.ova**”



VirtualBox Setup

- Choose “**CN2022**” and then start the machine.



Wireshark

Wireshark Installation

- Wireshark is a widely-used network protocol analyzer.
- You can
  - install Wireshark (3.6.8) on your computer, or
  - use the VM we prepared with Wireshark installed (recommended).

Wireshark Installation

- Superuser permission is necessary to install and execute Wireshark.
- To install Wireshark on your own, use the following command:

```
$ sudo apt update
```

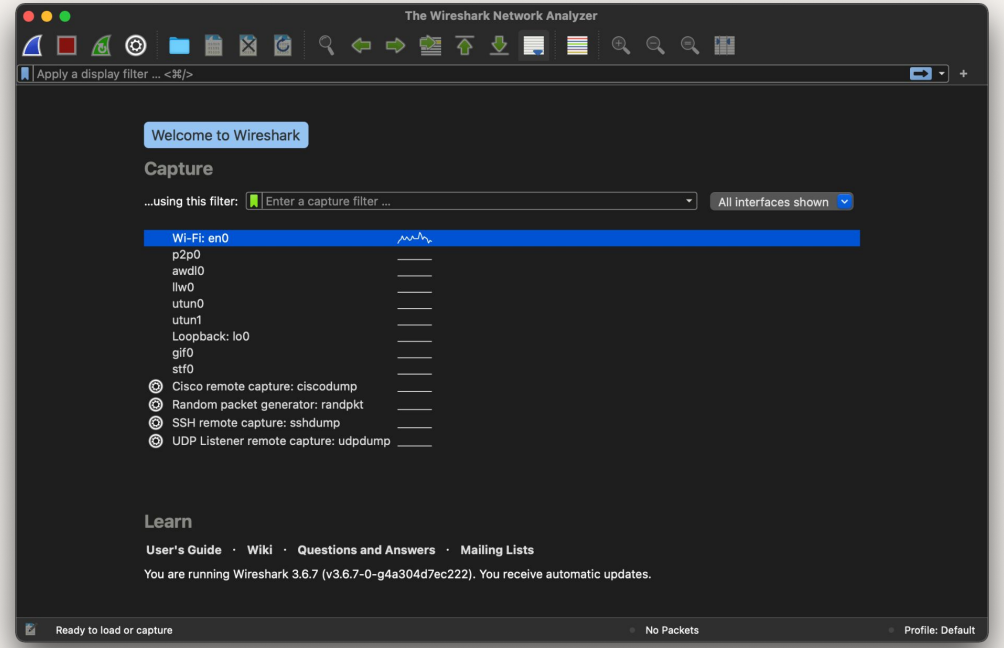
```
$ sudo apt install wireshark
```

- To launch the Wireshark, run the following command:

```
$ sudo wireshark
```

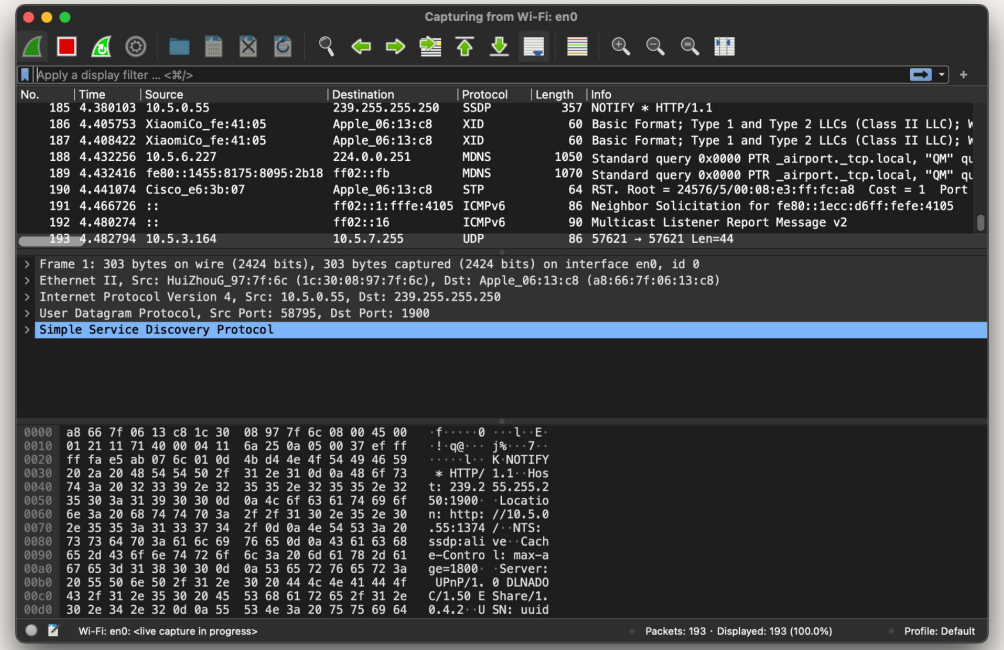
Wireshark Instruction

- Double click the network interface card.



Wireshark Instruction

- Then, you can see all the packets sent from and to this machine (that is, virtual machine if you use our VirtualBox).

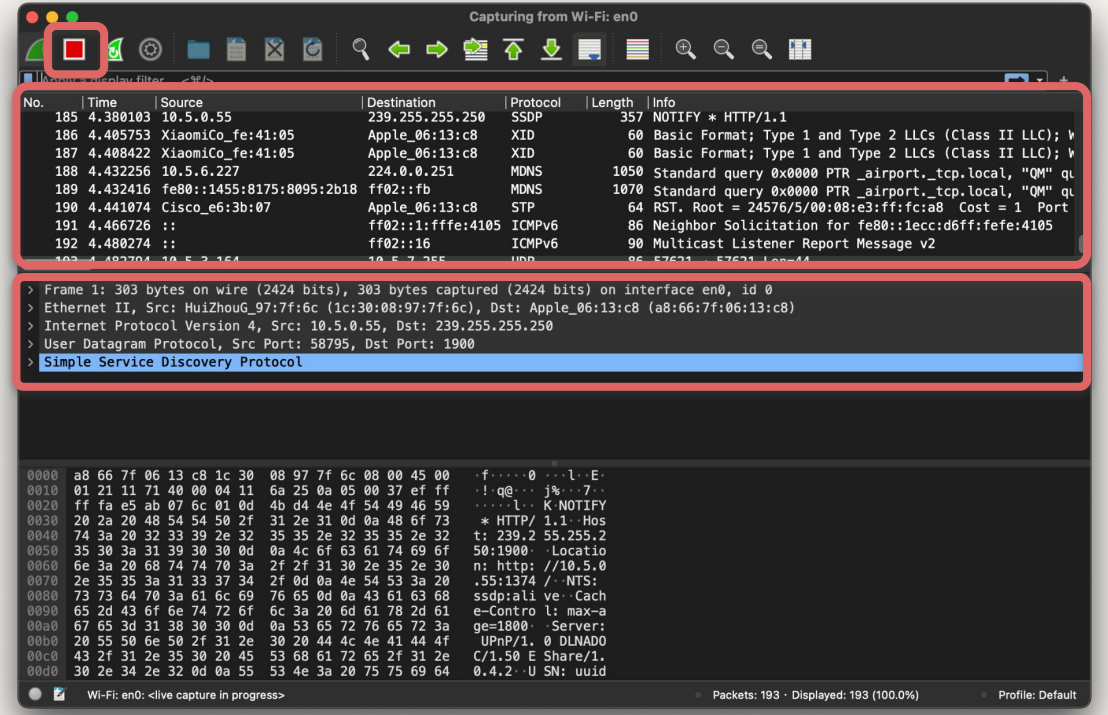


Wireshark Instruction

Stop Capture

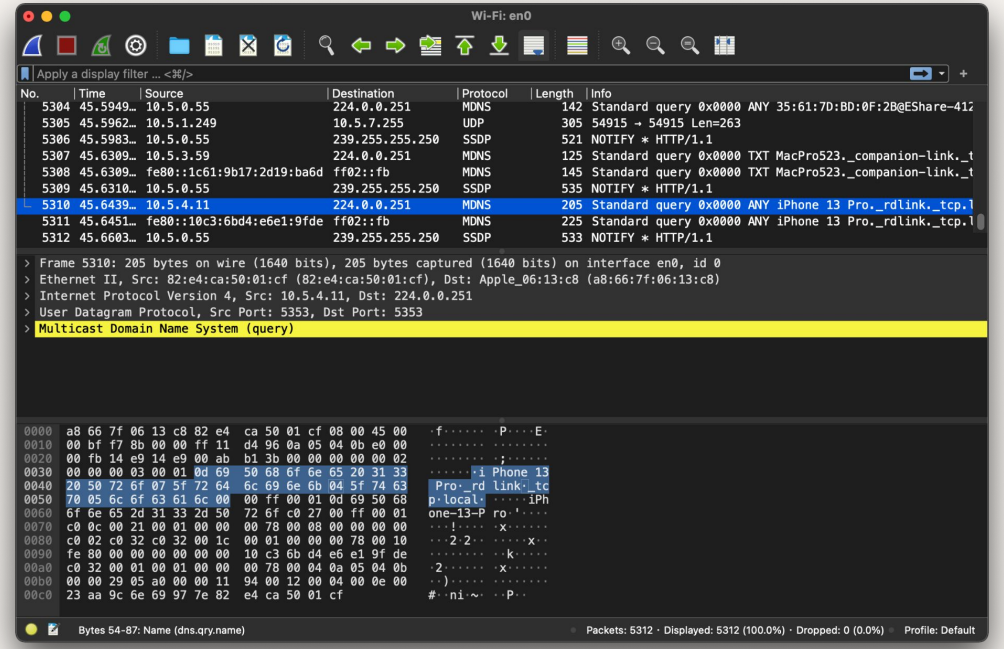
Packet List

Packet Detail



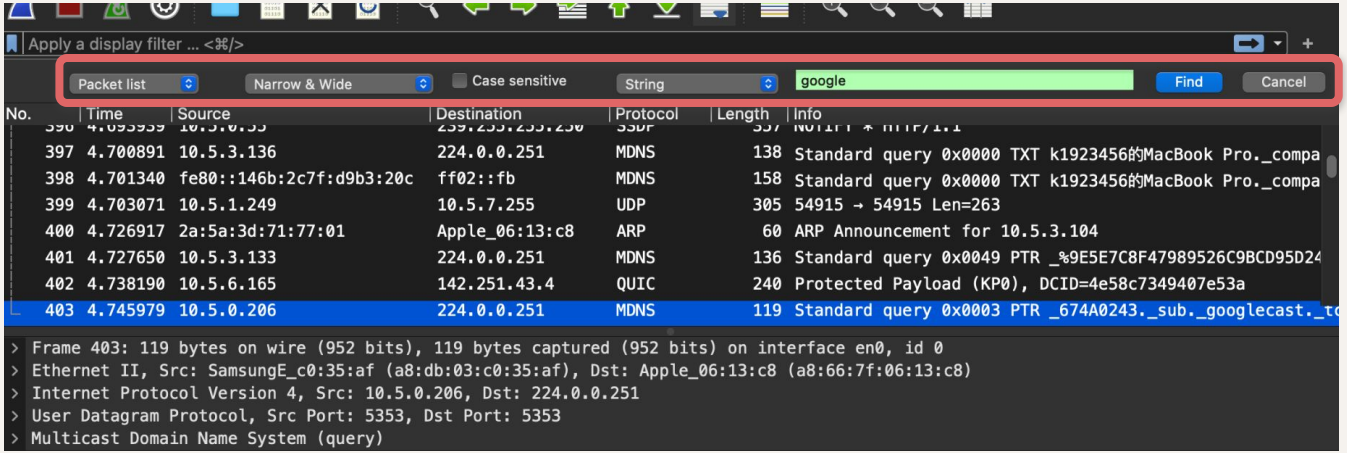
Wireshark Instruction

- Packet information is in the middle, and the raw binary data is at the bottom.



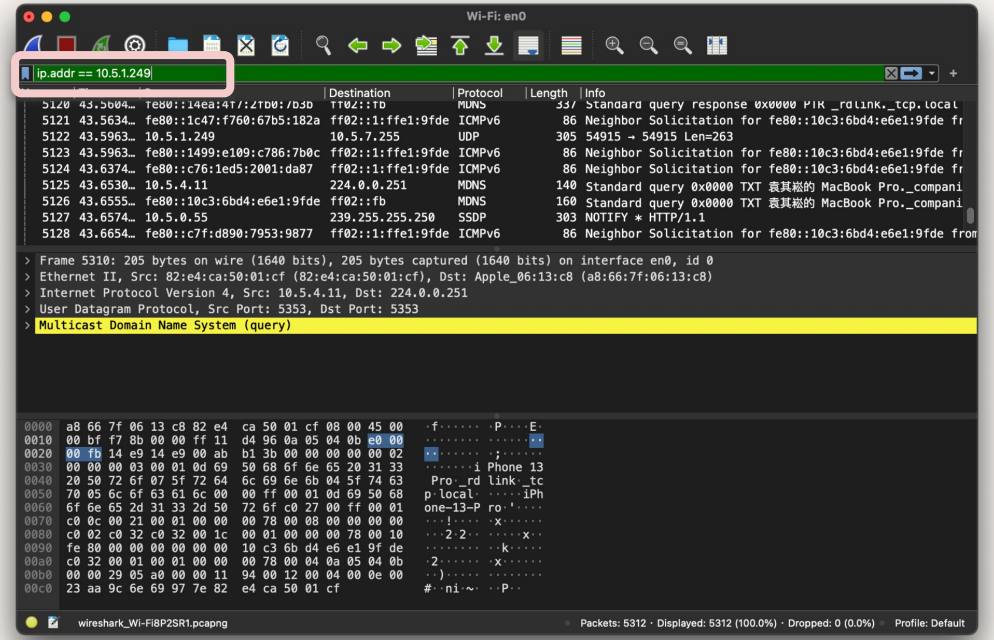
Wireshark Instruction

- Press “Ctrl + F” or “Command + F,” and then you can see some patterns on the packets.



Wireshark Instruction

- If you want to display only some packets of given statements, enter some expressions on “Apply a display filter ….”



Wireshark Instruction

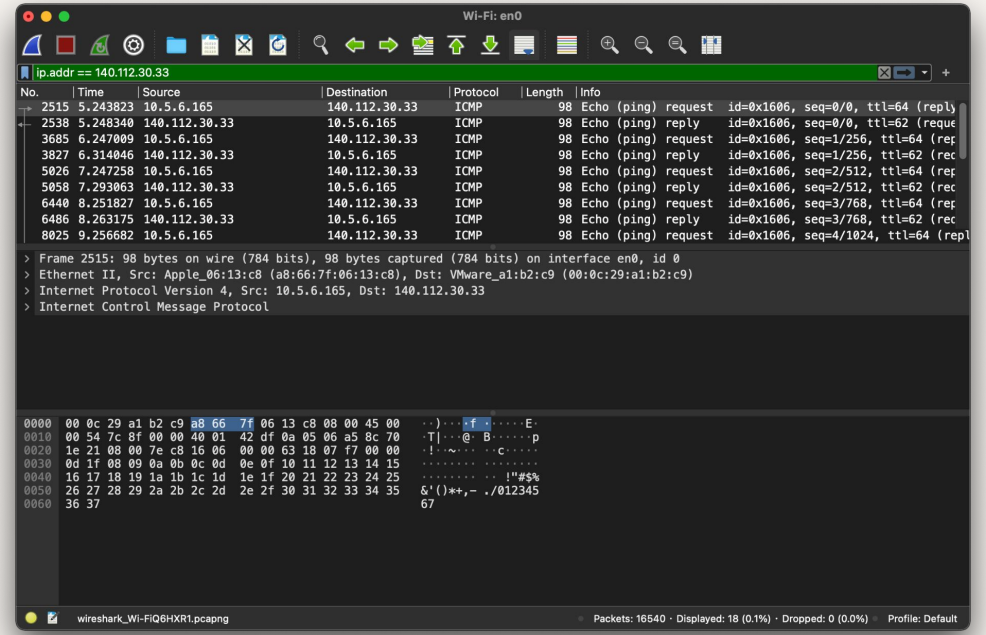
- Here are some common fields.

field	description
ip.addr	IP of all hosts
ip.src	IP of all source hosts
ip.dst	IP of all destination hosts
ip.proto	Protocol of all packets
tcp.port	Port of TCP packets
udp.port	Port of UDP packets

operator	description
&&	AND
||	OR
!	NOT

Wireshark Instruction

- For example, if you enter “ip.addr == 140.112.30.33”, it will retain all packets sent from or to 140.112.30.33.



Assignment 1 Announcement

Assignment 1 – Specification (1/5)

- Analysis of UDP (User Datagram Protocol) packets.
  - Please find out a UDP packet on Wireshark.
    - Take a screenshot of the UDP packet containing the source and destination port.
  - Write down which website/server it is and what kind of service this website/server provides.
  - Write down which port this service uses for this application.

Assignment 1 – Specification (2/5)

- Analysis of TCP (Transmission Control Protocol) packets.
  - Connect to NTU CSIE workstation (or another server) through SSH, and observe the packets in the SSH connection.

    $ ssh <studentID>@linux<1~15>.csie.ntu.edu.tw

    If you use another server, write down what server and its IP address you connect to.

  - Please find out a TCP packet on Wireshark.
    - Take a screenshot of the TCP packet containing the source and destination port.
  - Write down which port this SSH server uses.
- Determine whether your machine uses public or private IP in the TCP packet you find out, and explain how you know that.

Assignment 1 – Specification (3/5)

- Compare the headers of transport layer between TCP and UDP.
  - List at least 2 same fields between these 2 protocols.
  - List at least 3 different fields between these 2 protocols.

Assignment 1 – Specification (4/5)

- Find out a plaintext password in the packet.
  - Take a screenshot of one packet with your password in plaintext. (You can put a black bar or do pixelate on your password)
  - Write down which website it is.
  - Why is it not safe to send passwords in plaintext?

Assignment 1 – Specification (5/5)

- If you have other observations, please write them down in your report.

Grading Policy

- This assignment accounts for 10% of the total score.
- Report
  - Analysis of UDP packets (20%)
  - Analysis of TCP packets (25%)
  - Comparing between UDP and TCP packets (25%)
  - Find out a plaintext password (25%)
  - Other observations (5%)

Plagiarism

- You will get **zero points** on this homework if you copy others' code or reports.
- Please follow the honor code below:
  - https://communitystandards.stanford.edu/policies-guidance/honor-code

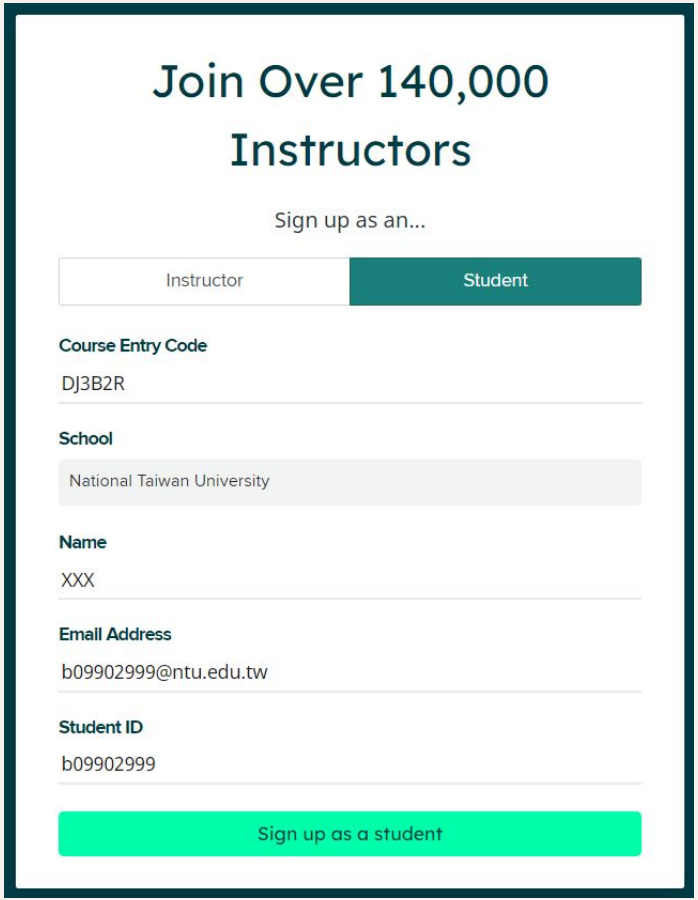
Submission

- Requirements
  - Your report can be a **pdf** or **clear image** file, or you will get zero point.
  - PDF file name: **<studentID>_hw1.pdf**
    - e.g. B09902999_hw1.pdf
  - Please submit your report to **Gradescope**.
- Deadline
  - Due Date : 23:59:59, October 4th, 2022
  - Penalty for late submission is **20 points per day**.

Gradescope

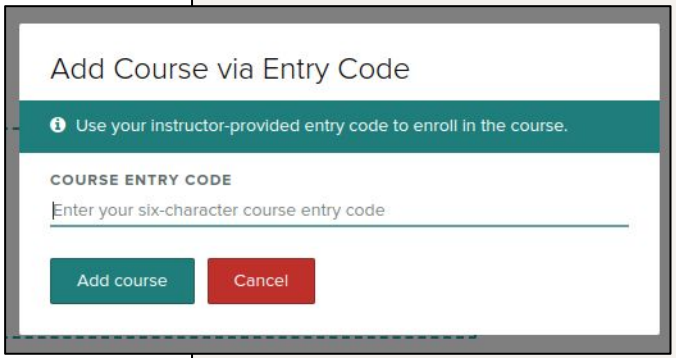
Add a Course in Gradescope

- **If you are an auditor, please don’t add this course to Gradescope.**
- Sign up as a student.
- Enter entry code **DJ3B2R**.
- Enter your school name, Chinese name, school email, and student ID.
- You’ll receive an email to set up your password.



Add a Course in Gradescope

- If you have signed up for Gradescope before, enter the entry code.



You can ask questions on NTU COOL Discussion Forum or mail to TA with the tag **[HW1]** in the title. •ω•)ค

TA Email: ntu.cnta@gmail.com