

# Introduction to Computer Network Project 1-3

## *Sniffing Software Installation & Filtering Rules Exercise*

Date: 2016/10/06

Deadline: 2016/10/20 (Thu.) 23:59



# Outline

- 實驗目的
- 實驗環境
- 實驗流程
- 封包範例
- 如何找到正確封包
- 作業要求
- 本課程作業遲交扣分方式
- Q&A



# 實驗目的

- 熟悉如何使用封包擷取軟體**Wireshark**
- 利用特定的**Filter**，從擷取到的封包中過濾出特定封包並加以觀察
- **Wireshark**
  - 開放原始碼，基於**GPL**授權
  - 免費使用，而且功能十分強大
  - 方便擷取網路上的封包，並檢視每一個封包的詳細資訊
  - 這次實驗練習的**Filter**技巧是最基本的操作，**Wireshark**還有許多功能可以分析及觀察網路流量
  - 熟悉**Wireshark**的功能對以後的實驗將會有幫助



# 實驗環境

- 使用自己的電腦即可
  - 請確定該電腦可以正常連上Internet
- Wireshark支援
  - Windows
  - Linux
  - OS X
  - ...等多種作業系統
- 目前Wireshark的穩定版本為2.0.5




# 實驗流程 (1/10)

## ● 下載Wireshark

■ <https://www.wireshark.org/download.html>

### Download Wireshark

The current stable release of Wireshark is 2.0.5. It supersedes all previous releases.

Stable Release (2.0.5)	^
<div> Windows Installer (64-bit) Windows Installer (32-bit) Windows PortableApps® (32-bit) OS X 10.6 and later Intel 64-bit .dmg OS X 10.6 and later Intel 32-bit .dmg Source Code</div>	
Old Stable Release (1.12.13)	^
Development Release (2.2.0rc1)	^
Documentation	^



## 實驗流程 (2/10)

- 安裝Wireshark

- Windows

- 執行安裝檔之後，一直按下一步即可
    - 中途會要求安裝WinPcap
      - WinPcap是Wireshark擷取封包會用到的Library

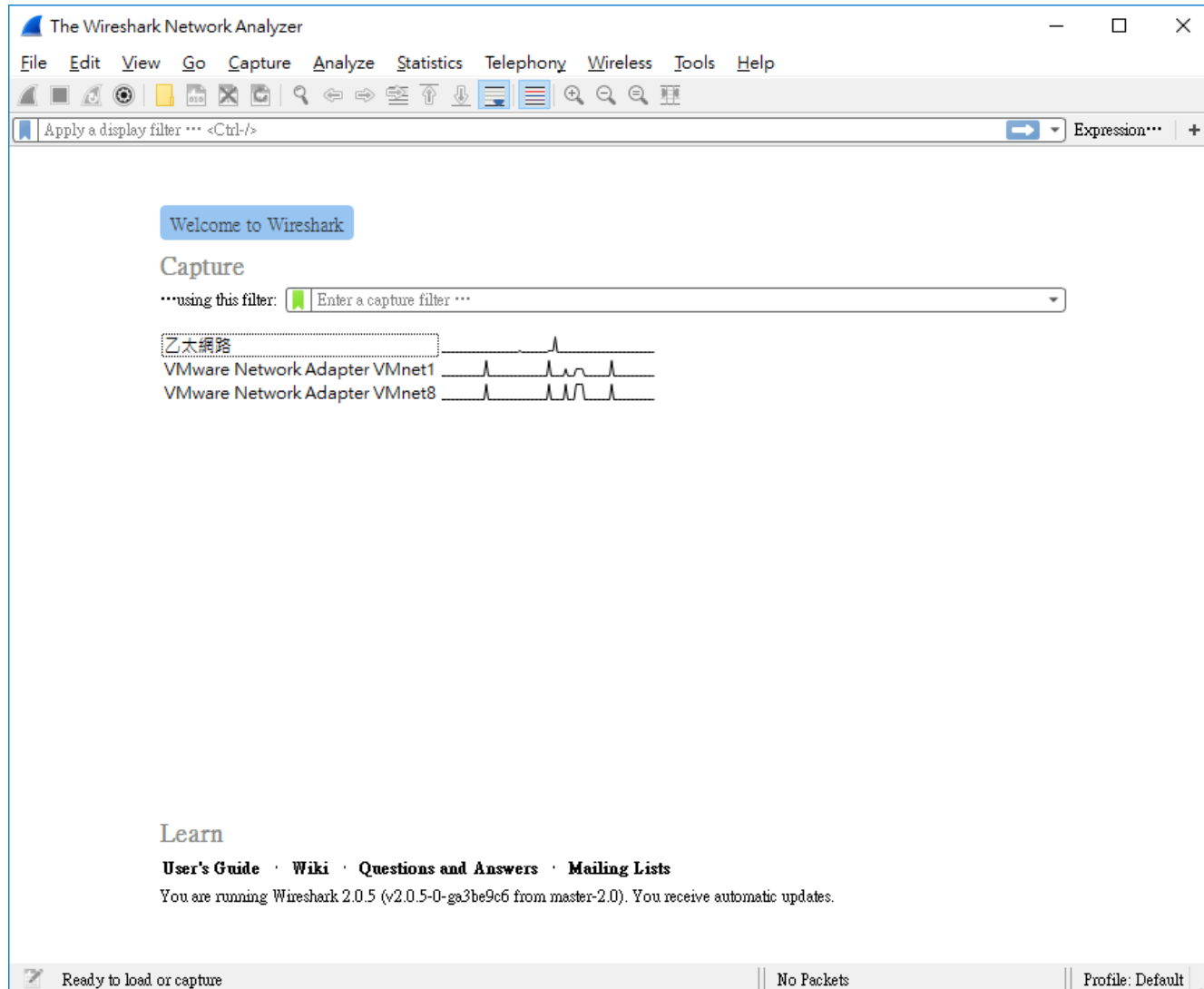
- Linux

- 在Ubuntu的terminal輸入: "sudo apt-get install wireshark"



# 實驗流程 (3/10)

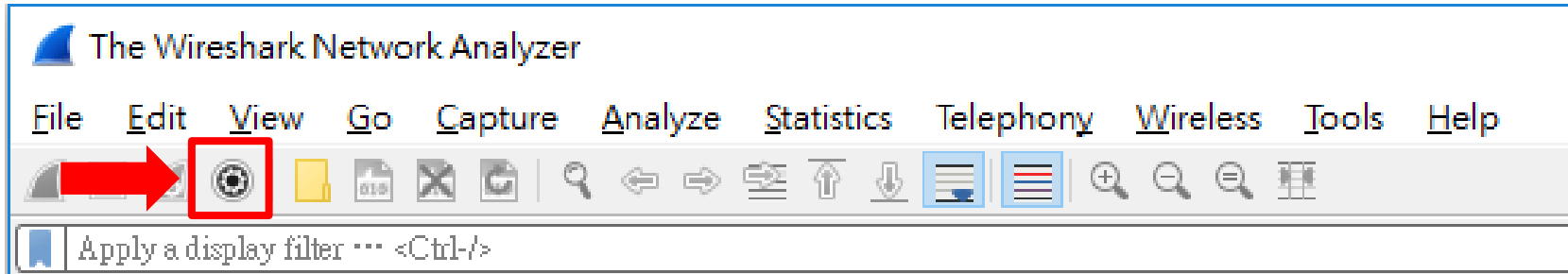
## ● 開啟Wireshark





## 實驗流程 (4/10)

- 開始擷取封包
  - 按一下左上角的Capture Options



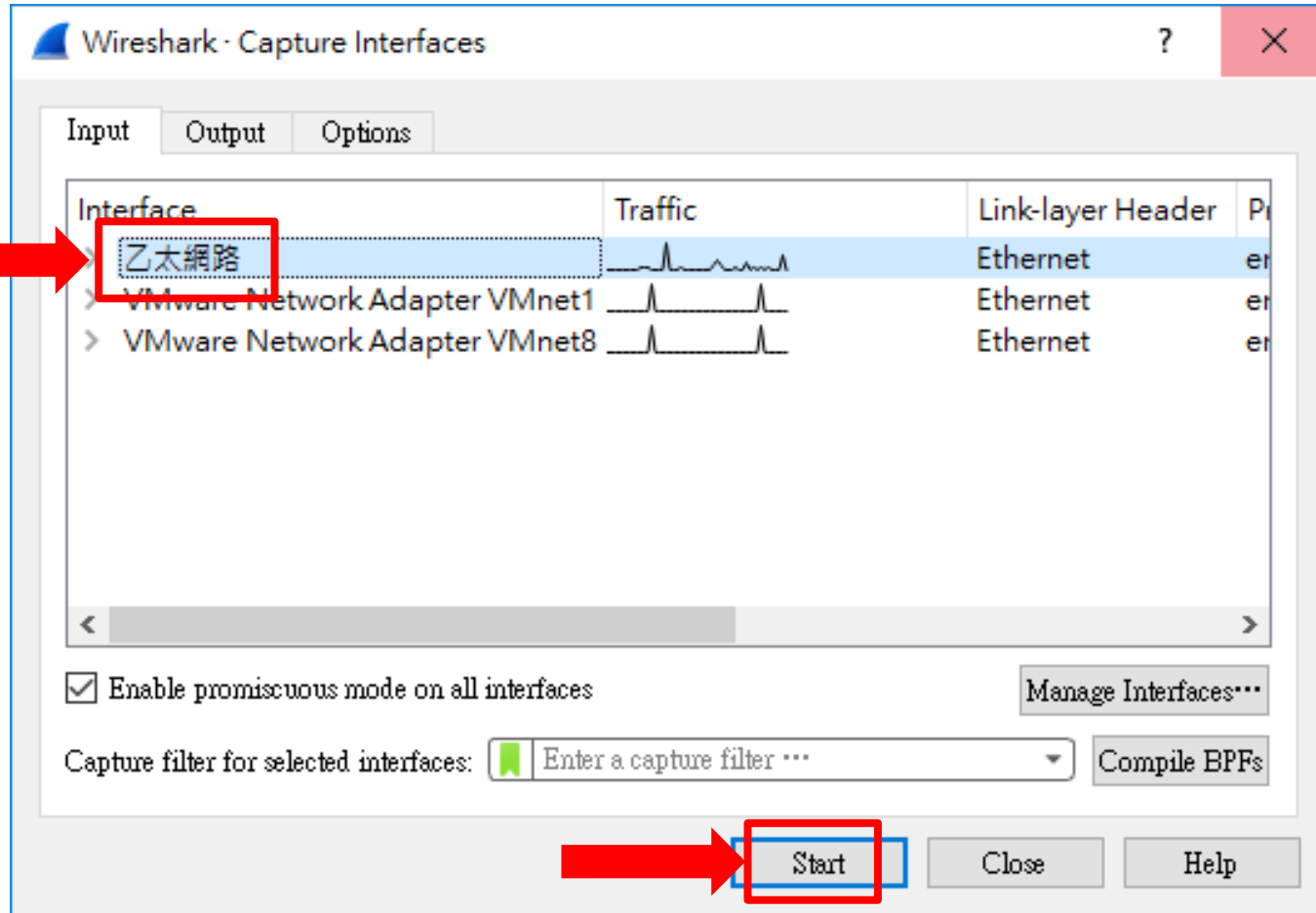
- (續下頁)





## 實驗流程 (5/10)

- 此時會列出電腦中所有的Interface，選擇要進行封包擷取的網路卡，按下Start

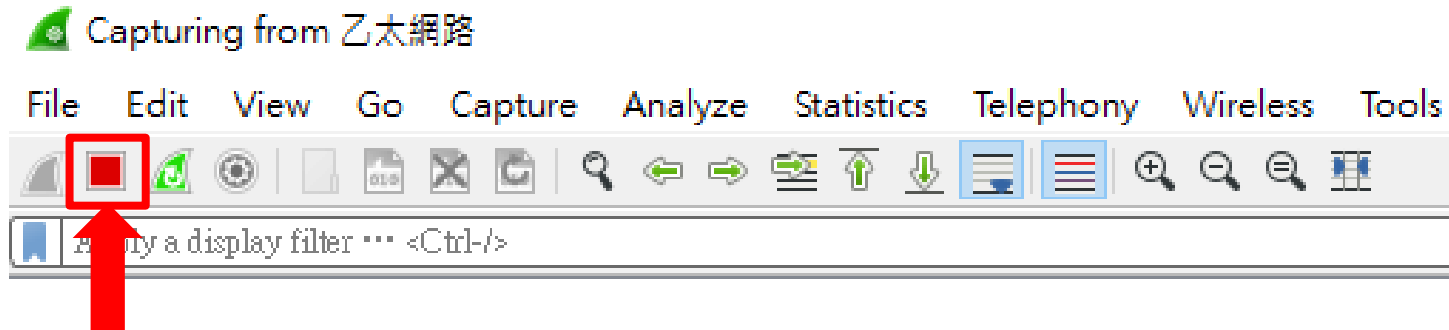




## 實驗流程 (6/10)

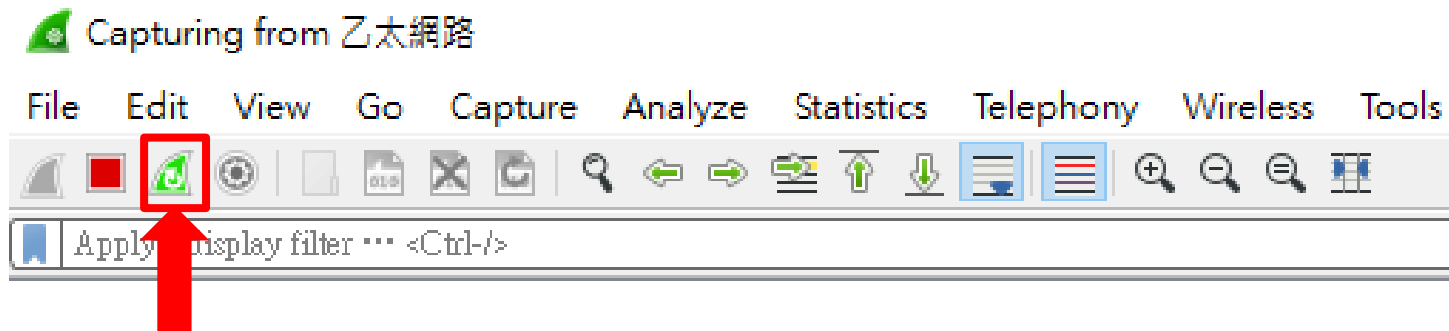
- 停止擷取封包

- 按一下左上角的 Stop the running capture



- 重新開始擷取封包

- 按一下左上角的 Restart the running capture



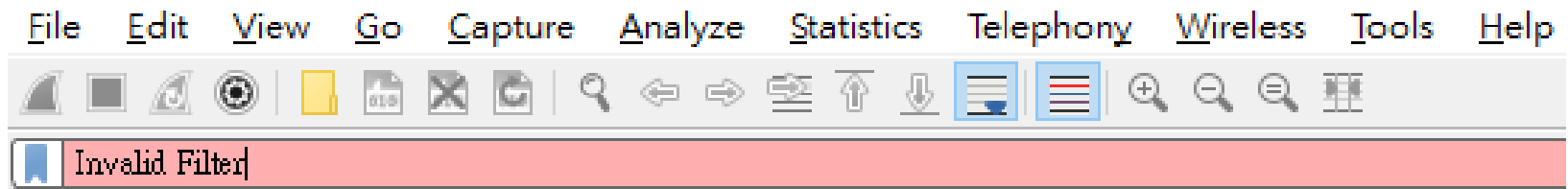


## 實驗流程 (7/10)

- 過濾封包 (Filter)
  - 在Filter欄位輸入條件後按Enter



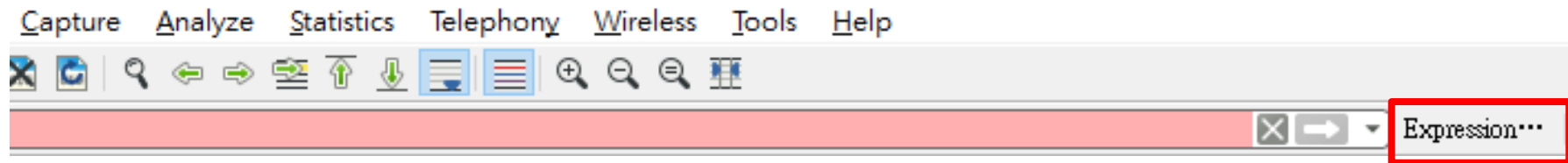
- 條件錯誤就會變成紅色





## 實驗流程 (8/10)

- 還不熟Wireshark，要怎麼知道正確的Filter條件呢？
- 點選Expression就可以看到Filter條件的選單

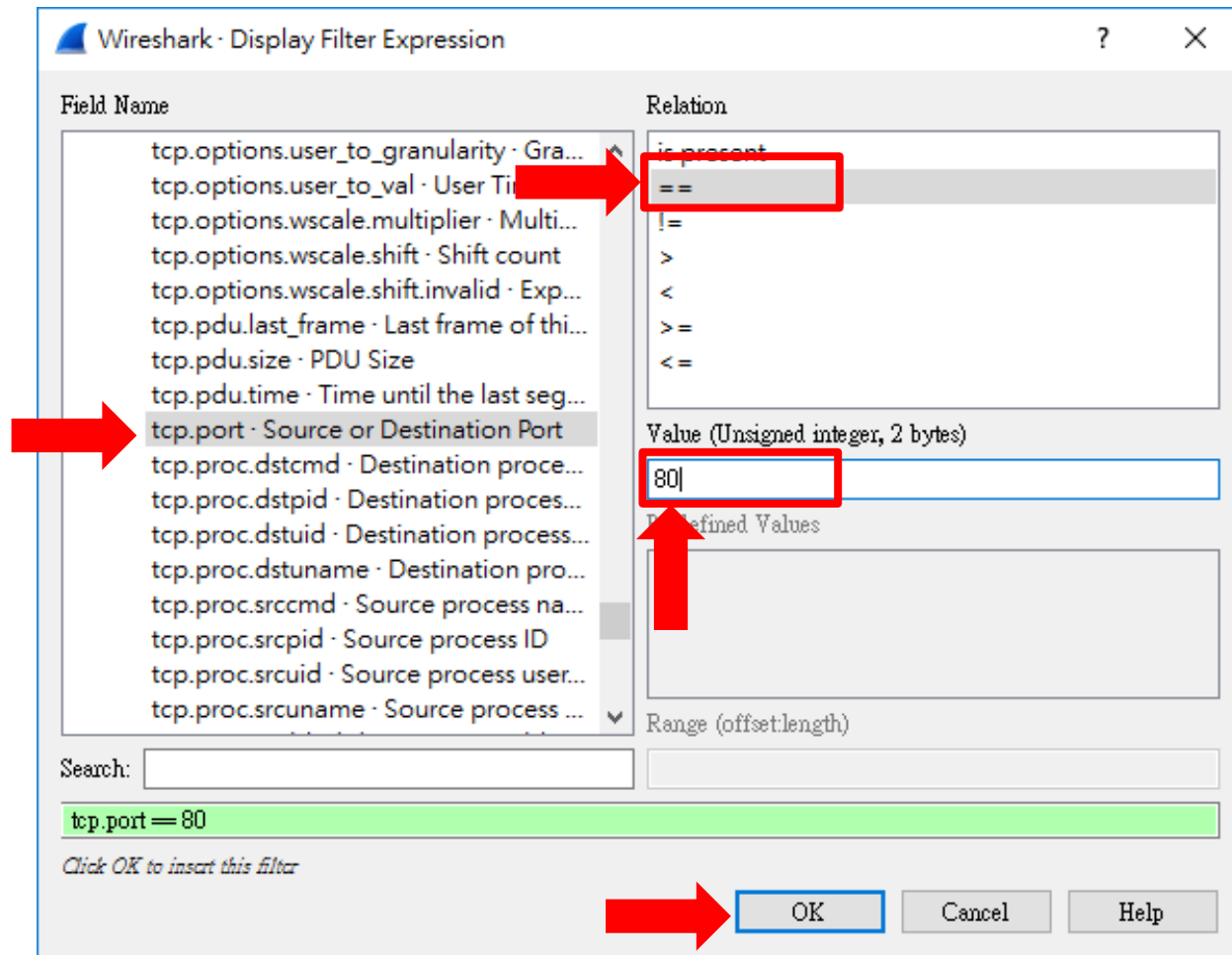


- (續下頁)



## 實驗流程 (9/10)

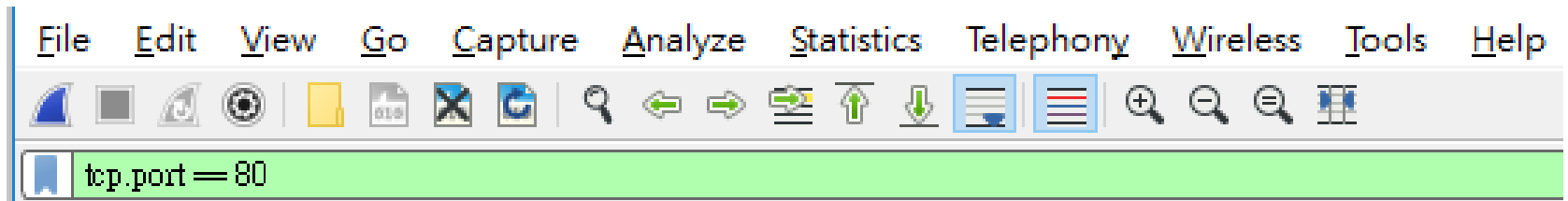
- 假設要看所有TCP port 80的封包





# 實驗流程 (10/10)

- 之後就會自動產生過濾條件



- 也可以用類似C語言and和or的寫法
  - `tcp.port==80 && ip.addr==10.0.0.100`
  - `tcp.port==80 || ip.addr==10.0.0.100`
- 更多Filter條件式請自行從Expression發掘或請洽google大神



# 封包範例

1. Frame information
2. Data link layer header (e.g. MAC address)
3. Network layer header (e.g. IP address)
4. Transport layer header (e.g. port number)
5. Application layer header (e.g. HTTP request)

Filter:	http	▼	Expression...	Clear	Apply	Save
No.	Time	Source	Destination	Protocol	Length	Info
1388	105.809377	122.228.90.8	140.113.220.219	HTTP	247	HTTP/1.1 200 OK (text/plain)
III						
+ Frame 1388: 247 bytes on wire (1976 bits), 247 bytes captured (1976 bits) on interface 0						
+ Ethernet II, Src: JuniperN_4f:e7:f0 (ac:4b:c8:4f:e7:f0), Dst: Elitegro_b2:72:27 (b8:ae:ed:b2:72:27)						
+ Internet Protocol Version 4, Src: 122.228.90.8 (122.228.90.8), Dst: 140.113.220.219 (140.113.220.219)						
+ Transmission Control Protocol, Src Port: 80 (80), Dst Port: 58153 (58153), Seq: 1, Ack: 878, Len: 247						
+ Hypertext Transfer Protocol						
+ Line-based text data: text/plain						

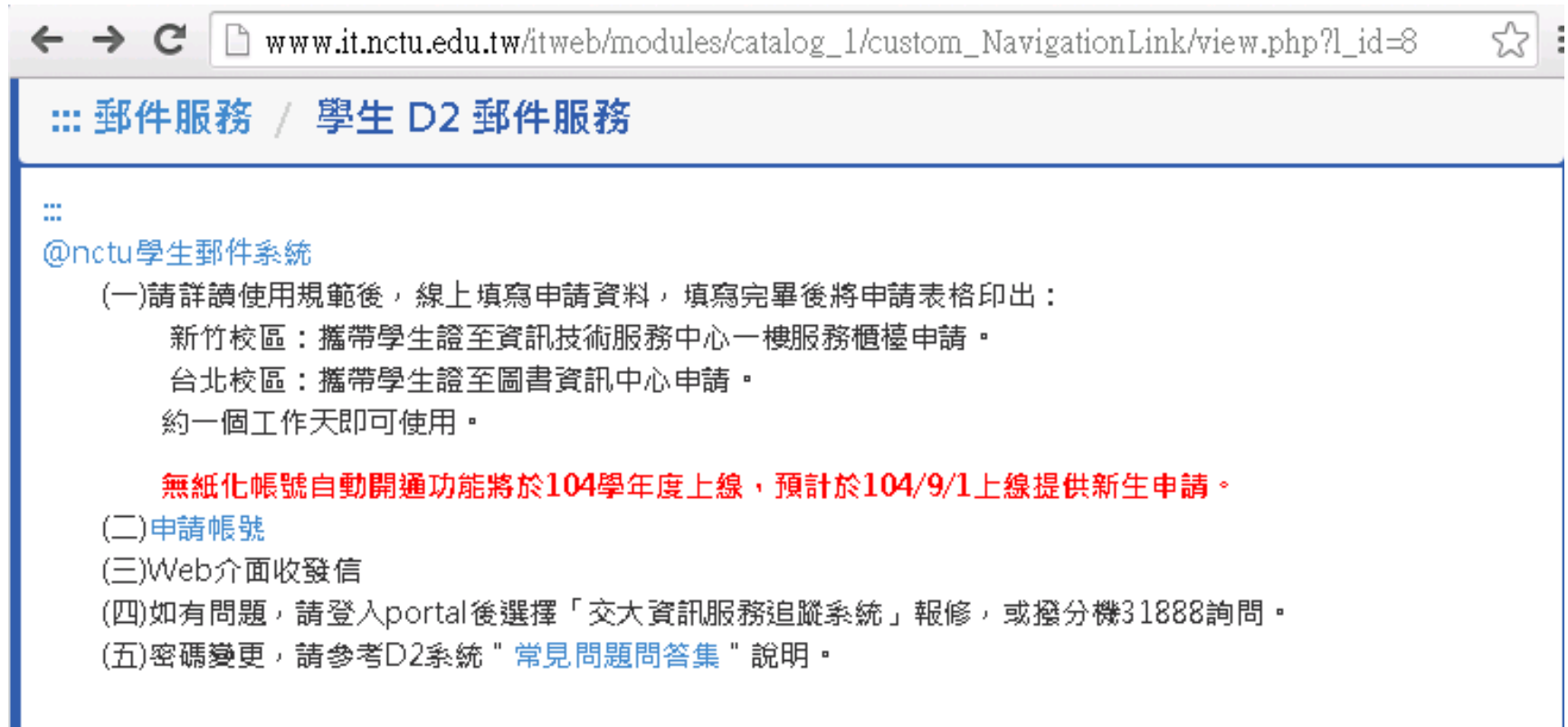


# 如何找到正確封包 (1/2)

## ● 如何找到正確的 HTTP 封包

### ■ 以交大 D2 信箱網頁為例：

[http://www.it.nctu.edu.tw/itweb/modules/catalog\\_1/custom\\_NavigationLink/view.php?l\\_id=8](http://www.it.nctu.edu.tw/itweb/modules/catalog_1/custom_NavigationLink/view.php?l_id=8)



The screenshot shows a web browser window with the address bar displaying the URL: [www.it.nctu.edu.tw/itweb/modules/catalog\\_1/custom\\_NavigationLink/view.php?l\\_id=8](http://www.it.nctu.edu.tw/itweb/modules/catalog_1/custom_NavigationLink/view.php?l_id=8). The page title is "郵件服務 / 學生 D2 郵件服務". The content area is titled "@nctu學生郵件系統" and contains the following text:

(一)請詳讀使用規範後，線上填寫申請資料，填寫完畢後將申請表格印出：  
新竹校區：攜帶學生證至資訊技術服務中心一樓服務櫃檯申請。  
台北校區：攜帶學生證至圖書資訊中心申請。  
約一個工作天即可使用。

**無紙化帳號自動開通功能將於104學年度上線，預計於104/9/1上線提供新生申請。**

(二)申請帳號  
(三)Web介面收發信  
(四)如有問題，請登入portal後選擇「交大資訊服務追蹤系統」報修，或撥分機31888詢問。  
(五)密碼變更，請參考D2系統 "常見問題問答集" 說明。



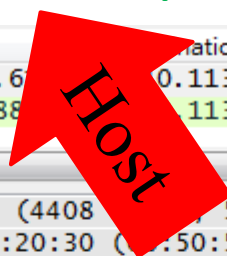


## 如何找到正確封包 (2/2)

- 如何找到正確的 HTTP 封包

- 以交大 D2 信箱網頁為例：

[http://www.it.nctu.edu.tw/itweb/modules/catalog\\_1/custom\\_NavigationLink/view.php?l\\_id=8](http://www.it.nctu.edu.tw/itweb/modules/catalog_1/custom_NavigationLink/view.php?l_id=8)



Time	Source	Destination	Protocol	Length	Info
63	2.87891400	140.113.221.61	140.113.40.88	HTTP	551 GET /itweb/modules/catalog_1/custom_NavigationLink/view.php?l_id=8
105	2.95814600	140.113.40.88	140.113.221.61	HTTP	273 HTTP/1.1 200 OK (text/html)

Frame 63: 551 bytes on wire (4408 bits) captured (4408 bits) on interface 0  
Ethernet II, Src: Vmware\_a5:20:30 (08:00:56:a5:20:30), Dst: JuniperN\_4f:e7:f0 (ac:4b:c8:4f:e7:f0)  
Internet Protocol Version 4, Src: 140.113.221.61 (140.113.221.61), Dst: 140.113.40.88 (140.113.40.88)  
Transmission Control Protocol, Src Port: 65165 (65165), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 497

### Hypertext Transfer Protocol

GET /itweb/modules/catalog\_1/custom\_NavigationLink/view.php?l\_id=8 HTTP/1.1\r\n

[Expert Info (Chat/Sequence): GET /itweb/modules/catalog\_1/custom\_NavigationLink/view.php?l\_id=8 HTTP/1.1\r\n]

Request Method: GET

Request URI: /itweb/modules/catalog\_1/custom\_NavigationLink/view.php?l\_id=8

Request Version: HTTP/1.1

Host: www.it.nctu.edu.tw\r\n

Connection: keep-alive\r\n

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,\*/\*;q=0.8\r\n

Upgrade-Insecure-Requests: 1\r\n

User-Agent: Mozilla/5.0 (Windows NT 6.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/45.0.2454.101 Safari/537.36\r\n

Accept-Encoding: gzip, deflate, sdch\r\n

Accept-Language: zh-TW,zh;q=0.8,en-US;q=0.6,en;q=0.4\r\n

Cookie: PHPSESSID=fpflk7oa9986q2ruga01tvnmb7\r\n

\r\n

[Full request URI: [http://www.it.nctu.edu.tw/itweb/modules/catalog\\_1/custom\\_NavigationLink/view.php?l\\_id=8](http://www.it.nctu.edu.tw/itweb/modules/catalog_1/custom_NavigationLink/view.php?l_id=8)]

[HTTP request 1/1]

[Response in frame: 105]





## 作業要求 (1/3)

- 利用瀏覽器連到以下網站，並分析HTTP封包  
<http://people.cs.nctu.edu.tw/~yangchh/ICN/Project1-3>
  - 注意**不要**使用**https**
- 需繳交報告一份
  - 實驗過程 (可截圖)
  - 心得 (或是過程中遇到的困難及解法)
  - 根據連線到助教所提供的網站的HTTP Request及Response，  
回答下頁投影片中的問題



## 作業要求 (2/3)

1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?
2. What languages (if any) does your browser indicate that it can accept to the server?
3. What is the IP address of your computer? Of the *people.cs.nctu.edu.tw*?
4. What is the status code returned from the server to your browser?
5. When was the web page that you are retrieving last modified at the server?
6. How many bytes of content are being returned to your browser?



## 作業要求 (3/3)

- 繳交方式
  - 上傳到e3，檔名格式為：**project1-3\_學號.pdf**
  - **檔名或格式錯誤者，不予計分**
  - Deadline: 2016/10/20 (Thu.) 23:59



## 本課程作業遲交扣分方式

- 遲交7日，Project 分數以原始分數九成計
- 遲交14日，Project 分數以原始分數七成計
- 超過14日，**不再接受繳交，Project 以零分計**



## Q&A

- 如果對Project有任何問題
  - 請來信 [icnta@win.cs.nctu.edu.tw](mailto:icnta@win.cs.nctu.edu.tw)
  - 計網概助教關心您