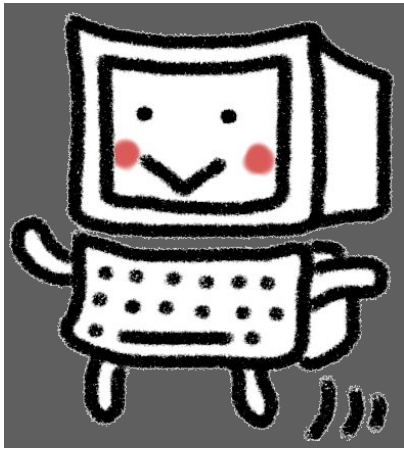


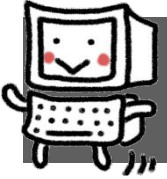
Introduction to Computer Network Project 1-3

Sniffing Software Installation &

Filtering Rules Exercise

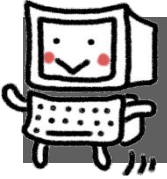
Date: 2017/10/12

Deadline: 2017/10/26 (Thu.) 23:59



Outline

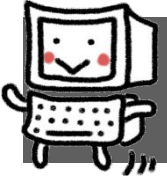
- 實驗目的
- 實驗環境
- 實驗流程
- 封包範例
- 如何找到正確封包
- 作業要求
- 本課程作業遲交扣分方式
- Q&A



實驗目的

- 熟悉如何使用封包擷取軟體 **Wireshark**
- 利用 **Filter** 從擷取的封包中過濾出特定封包來觀察

- **Wireshark**
  - 開放原始碼
    - 供免費使用且功能十分強大
  - 方便擷取網路上的封包
    - 可檢視各個封包的詳細資訊
  - 本次實驗練習的 Filter 技巧是最基本的操作
    - Wireshark 另有許多功能可分析網路狀態
  - 熟悉 Wireshark 的功能對往後課程與實驗皆很有很大幫助

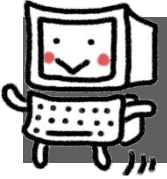


實驗環境

- 使用自己的電腦即可
  - 請確認該電腦可以正常連上網路
  - 亦可於之前作業所建立的環境完成本實驗
- Wireshark 支援多種作業系統
  - Windows
  - Linux
  - OS X
  - …
- 目前 Wireshark 的穩定版本為 2.4.1

實驗流程 (1/8)

- 安裝 Wireshark
  - Windows / macOS
    - 前往 Wireshark 官網 下載安裝程式
    - 執行安裝檔並一直按**下一步**即可
    - 中途要求安裝 WinPcap 請**一定要**安裝
      - WinPcap 是 Wireshark 擷取封包必需的 Library

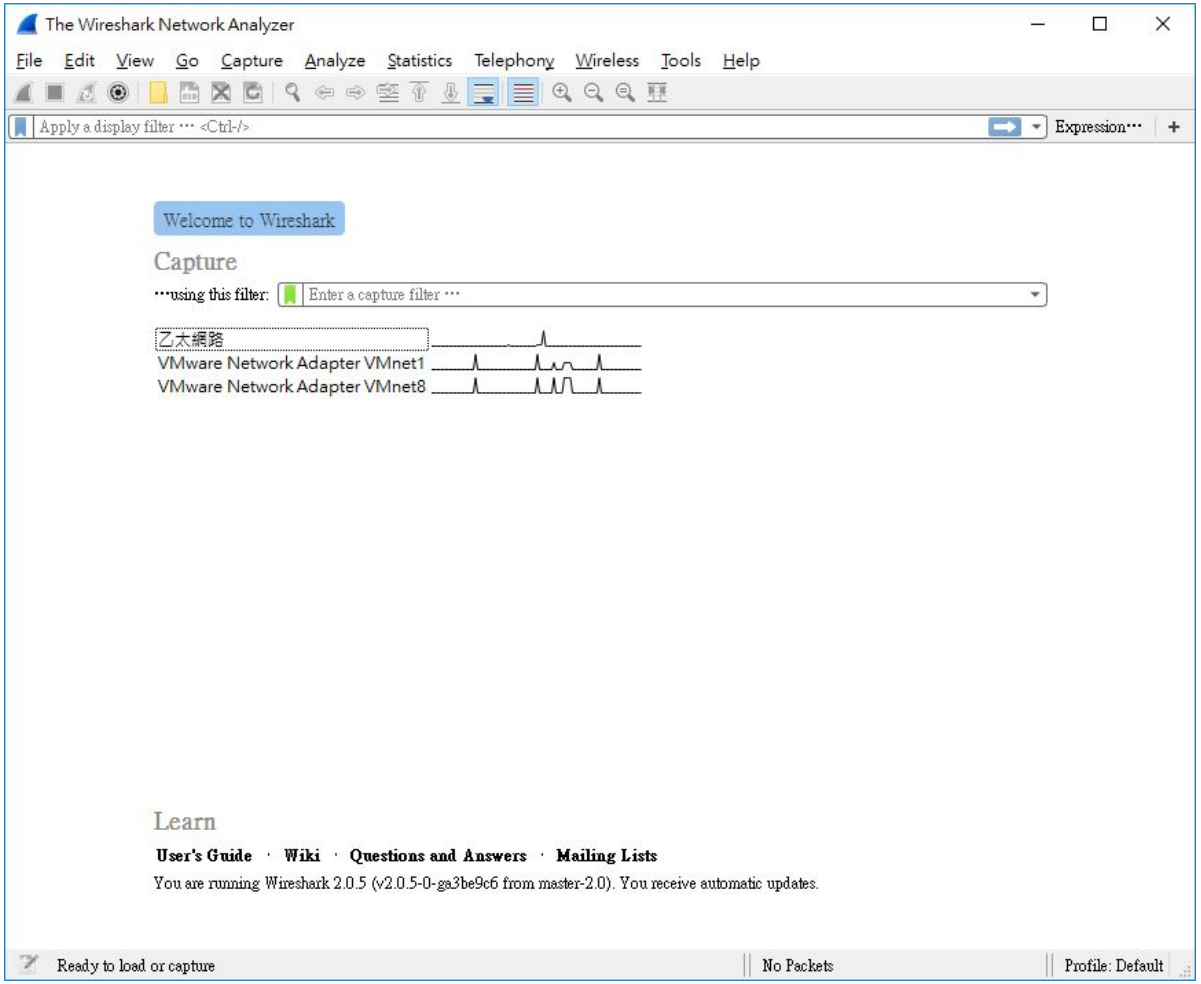


實驗流程 (2/8)

- 安裝 Wireshark
  - Linux (e.g. Ubuntu)
    - **在 Terminal 輸入以下指令**
    - sudo add-apt-repository ppa:wireshark-dev/stable
    - sudo apt-get update
    - sudo apt-get install wireshark
    - sudo dpkg-reconfigure wireshark-common **(選擇 YES)**
    - sudo usermod -a -G wireshark $USER
    - gnome-session-quit --logout --no-prompt **(即重新登入)**
    - wireshark **(即啟動 Wireshark)**

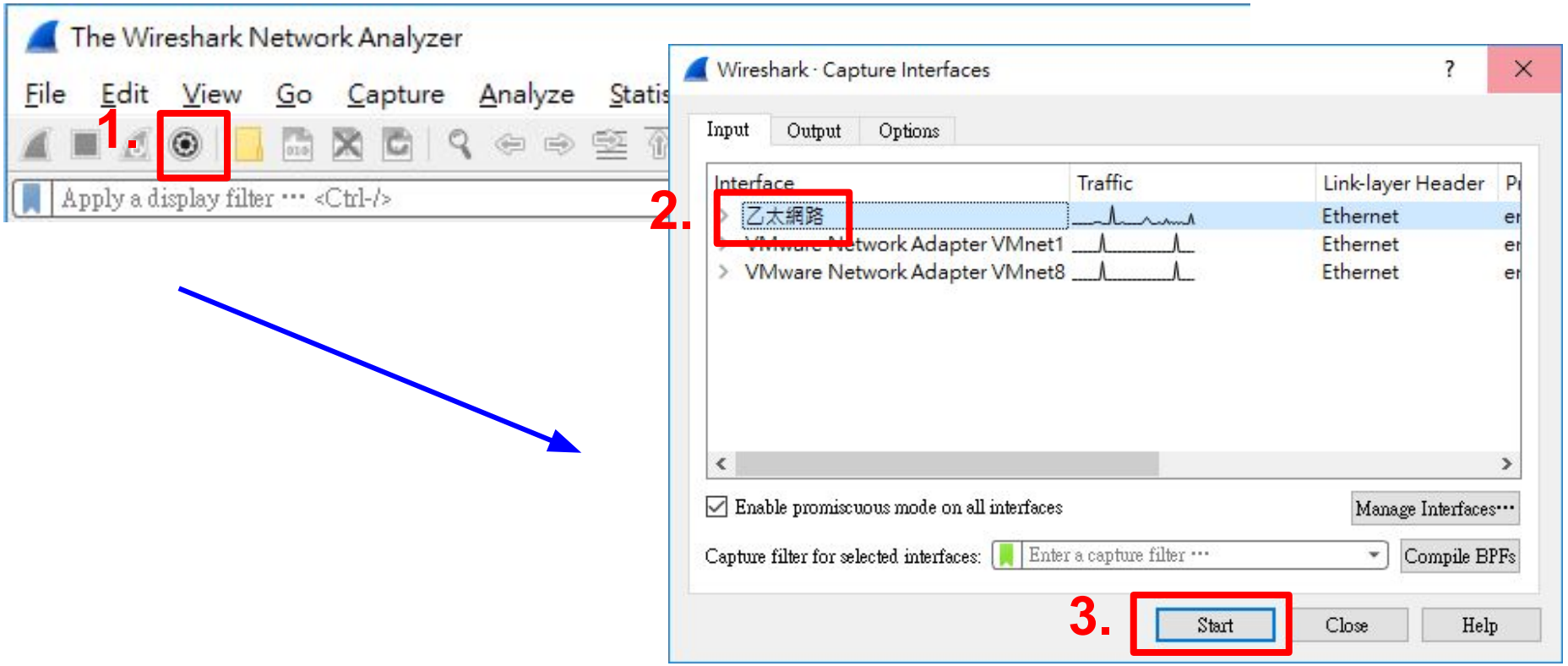
實驗流程 (3/8)

- Wireshark 起始畫面



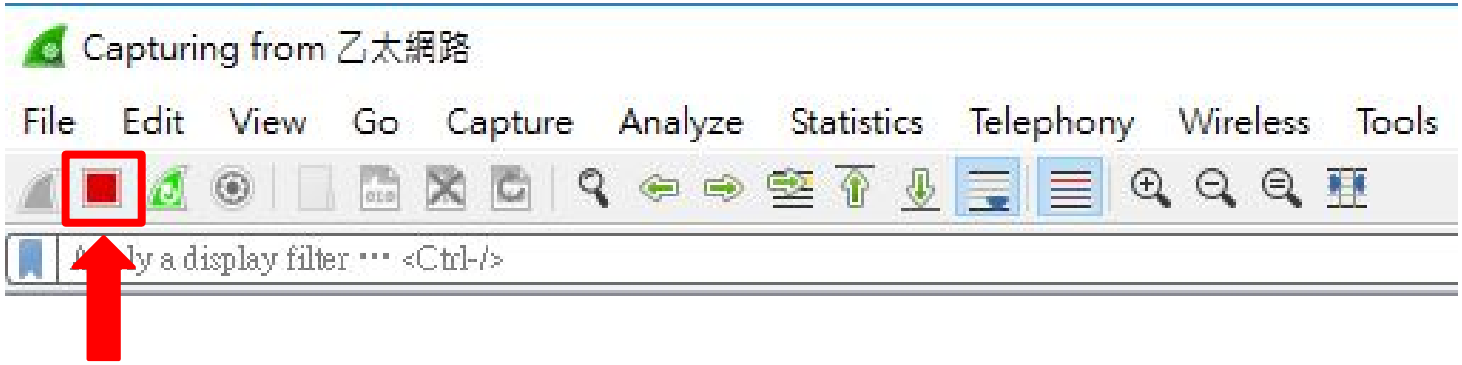
實驗流程 (4/8)

- 開始擷取封包
  1. 點選左上角 **Capture Options**
  2. 接著跳窗會列出此電腦所有的網卡
  3. 請選取擷取的目標網卡並按下 Start

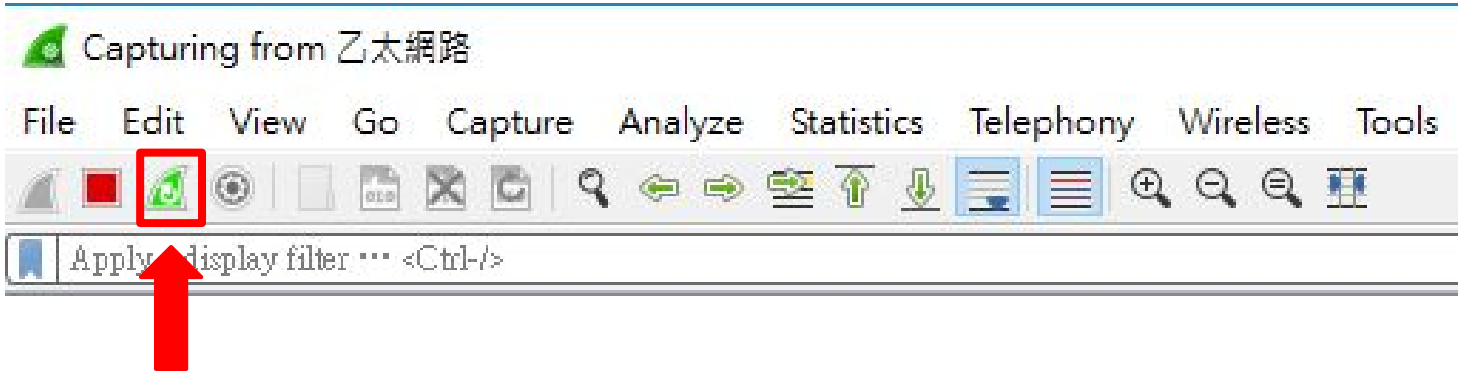


實驗流程 (5/8)

- 停止擷取封包
  - 按下左上角 **Stop the running capture**



- 重新開始擷取封包
  - 按下左上角 **Restart the running capture**



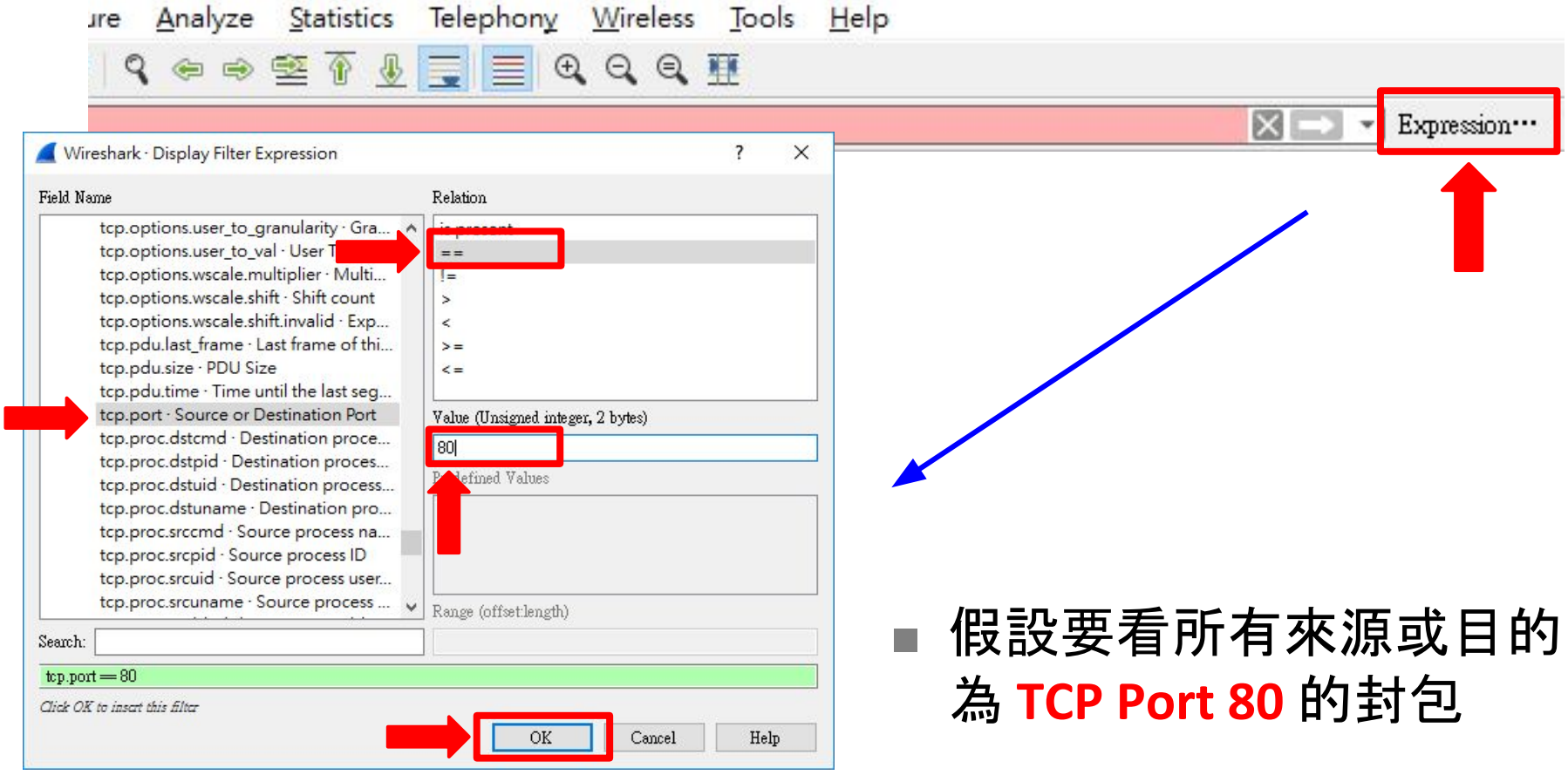
實驗流程 (6/8)

- 過濾封包
  - 在 **Filter 欄位**輸入條件後按 Enter

  - 條件錯誤就會呈現紅色

實驗流程 (7/8)

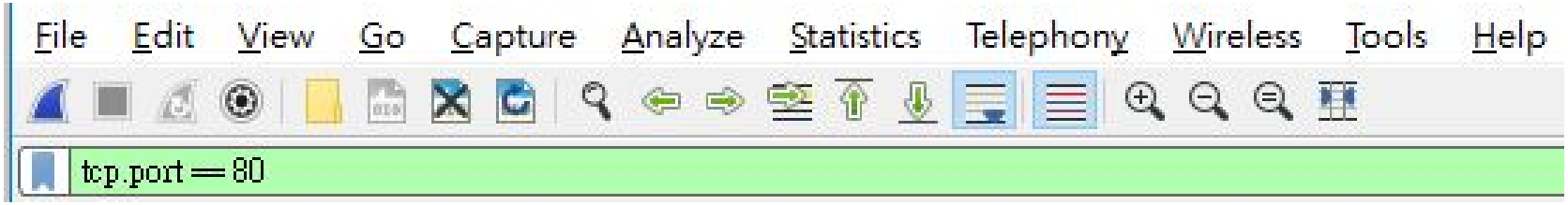
- Filter 條件選擇
  - 若還不熟悉 Wireshark 的 Filter 條件
  - 點選 Filter 欄位右側 **Expression** 會跳窗列出 Filter 條件選單



  - 假設要看所有來源或目的為 **TCP Port 80** 的封包

實驗流程 (8/8)

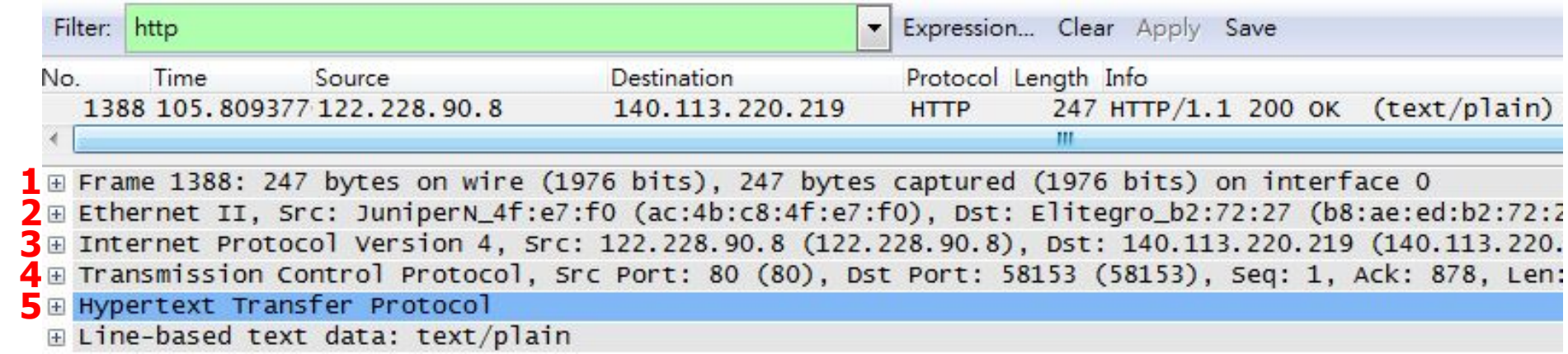
- 接著會自動產生過濾條件



  - 也可用類似 C 語言中 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 選項中測試學習
    - 或 google 使用說明文件

封包範例

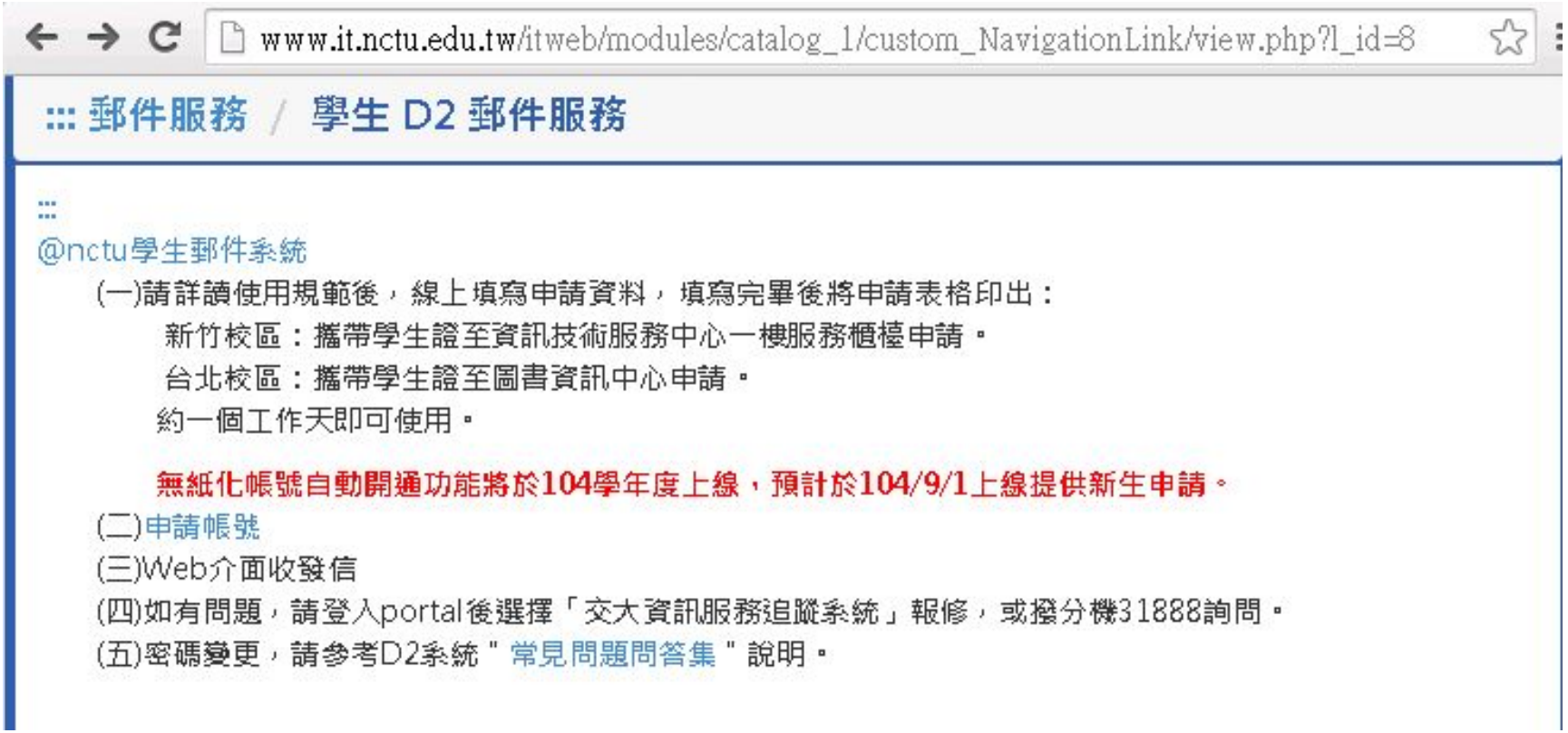
1. Frame information
2. Data link layer header (e.g. MAC address)
3. Network layer header (e.g. IP address)
4. Transport layer header (e.g. port number)
5. Application layer header (e.g. HTTP request)



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:

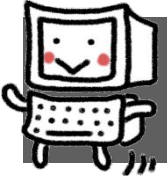
http://www.it.nctu.edu.tw/itweb/modules/catalog_1/custom_NavigationLink/view.php?l_id=8



如何找到正確封包 (2/2)

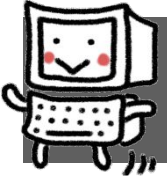
- 如何找到正確的 HTTP 封包?
  - 以交大 D2 信箱網頁為例:

http://www.it.nctu.edu.tw/itweb/modules/catalog_1/custom_NavigationLink/view.php?l_id=8



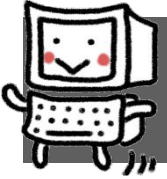
作業要求 (1/3)

- 利用瀏覽器連到以下網頁並分析 HTTP 封包
  - http://people.cs.nctu.edu.tw/~c0210024/ICN/Project1-3/
  - 請注意**不要**使用 **https**
- 需繳交報告一份
  - 實驗過程 (30%)
    - 文字敘述並附截圖
  - 心得 (10%)
    - 請**詳細**描述藉由實驗學習到的內容
  - 分析封包並回答問題 (60%)
    - 連到上述助教提供的網頁
    - 分析 HTTP Request 及 Response
    - 並回答下頁投影片中的問題



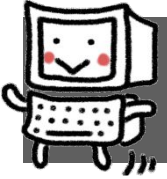
作業要求 (2/3)

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? What is the IP address of *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?



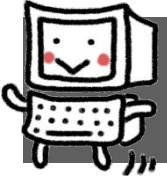
作業要求 (3/3)

- 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: 2017/10/26 (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
  - 在 Telegram Group 發問
    - https://t.me/nctuicn
  - 請來信 icnta@win.cs.nctu.edu.tw
  - 計網概助教關心您