

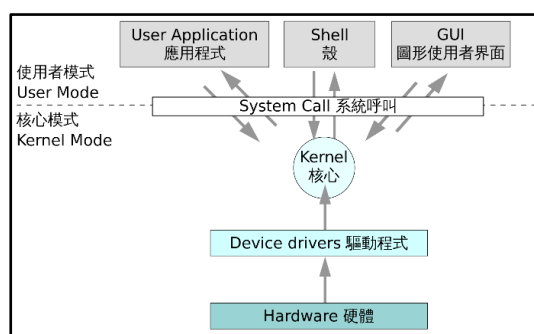
Linux 心得

一開始學習 linux 時，因為不熟指令，所以就花蠻多時間在搜尋指令的用法，但熟悉指令後，我覺得 CLI(Command-Line Interface)好像比 GUI(Graphical User Interface)更來的方便及快速。

Linux 是一種自由和開放源碼的類 UNIX 作業系統。也因為 Linux 有開放源碼的工具，所以可以根據自己的需求去訂製與配置，對於「駭客」來說這功能非常讚。

學習 Linux 過程中，看到很多 Linux 優點。Linux 優點整理如下：

- 免費
- 穩定性高
- 跨平台硬體支援
- 安全性可靠
- 網路功能完善
- 豐富的軟體支援
- 多使用者、多工

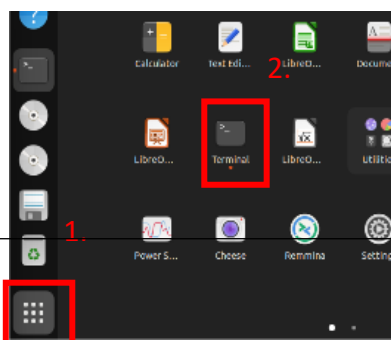


➡ 作業系統架構
(Linux 也是作業系統)

Linux 指令實作

使用虛擬機：VMware Workstation Player

使用 Linux 發行版：Ubuntu 22.04 64 位元



Linux 執行指令需要開啟終端機

方法 1：開啟終端機可以按 CTRL-ALT-T

方法 2：直接點擊圖標應用程式(Application) → 終端機(Terminal)

Linux 基本指令：

路徑操控

ls (list) 這個指令用來查看目錄中內

```
ehac@ehac-virtual-machine:~$ ls
Desktop Documents Downloads Music Pictures Public snap Templates Videos
```

參數(補充)

- ls -a //列出所有檔案 (包含隱藏檔)
- ls -l //列出檔案資訊 (大小、權限等)
- ls -R //列出所有子目錄內的檔案

cd (change directory) 這個指令用來切換目錄

```
ehac@ehac-virtual-machine:~$ ls
Desktop Documents Downloads Music Pictures Public snap Templates Videos
ehac@ehac-virtual-machine:~$ cd Documents
ehac@ehac-virtual-machine:~/Documents$ ls
```

pwd (present working directory) 這個指令可以回傳當前目錄位

```
ehac@ehac-virtual-machine:~$ pwd
/home/ehac
```

- Linux 相對 Windows，Linux 目錄位置較不明顯

檔案操控

mkdir (make directory) 新增目錄

- 新增後再輸入 ls 就會看到剛新增的目錄(newfolder)新增成功

```
ehac@ehac-virtual-machine:~$ ls
Desktop Documents Downloads Music Pictures Public snap Templates Videos
ehac@ehac-virtual-machine:~$ mkdir newfolder
ehac@ehac-virtual-machine:~$ ls
Desktop Downloads newfolder Public Templates
Documents Music Pictures snap Videos
ehac@ehac-virtual-machine:~$
```

rmdir 刪除空目錄

```
ehac@ehac-virtual-machine:~$ rmdir newfolder
ehac@ehac-virtual-machine:~$ ls
Desktop Documents Downloads Music Pictures Public snap Templates Videos
```

modch (change mode) 修改檔案權限

```
ehac@ehac-virtual-machine:~/folder$ ls -l
total 8
-rw-rw-r-- 1 ehac ehac 20  26 11:57 text1
-rw-rw-r-- 1 ehac ehac  6  26 13:48 text2
ehac@ehac-virtual-machine:~/folder$ chmod 777 text1
ehac@ehac-virtual-machine:~/folder$ ls -l
total 8
-rwxrwxrwx 1 ehac ehac 20  26 11:57 text1
-rw-rw-r-- 1 ehac ehac  6  26 13:48 text2
```

權限分成三種類型

r: 可讀 w: 可寫 x: 可執行

第一組為『擁有人的權限』

第二組為『同群組的權限』

第三組為『其他非本群組的權限』

文字檔案操控

cat (concatenate)

```
ehac@ehac-virtual-machine:~/folder$ cat text1
hello
ehac@ehac-virtual-machine:~/folder$ cat >> text1
hello world

ehac@ehac-virtual-machine:~/folder$ cat text1
hello
hello world
```

帳號操控

whoami 這個指令可以查看目前登入的使用者身分

```
ehac@ehac-virtual-machine:~$ whoami
ehac
```

其他

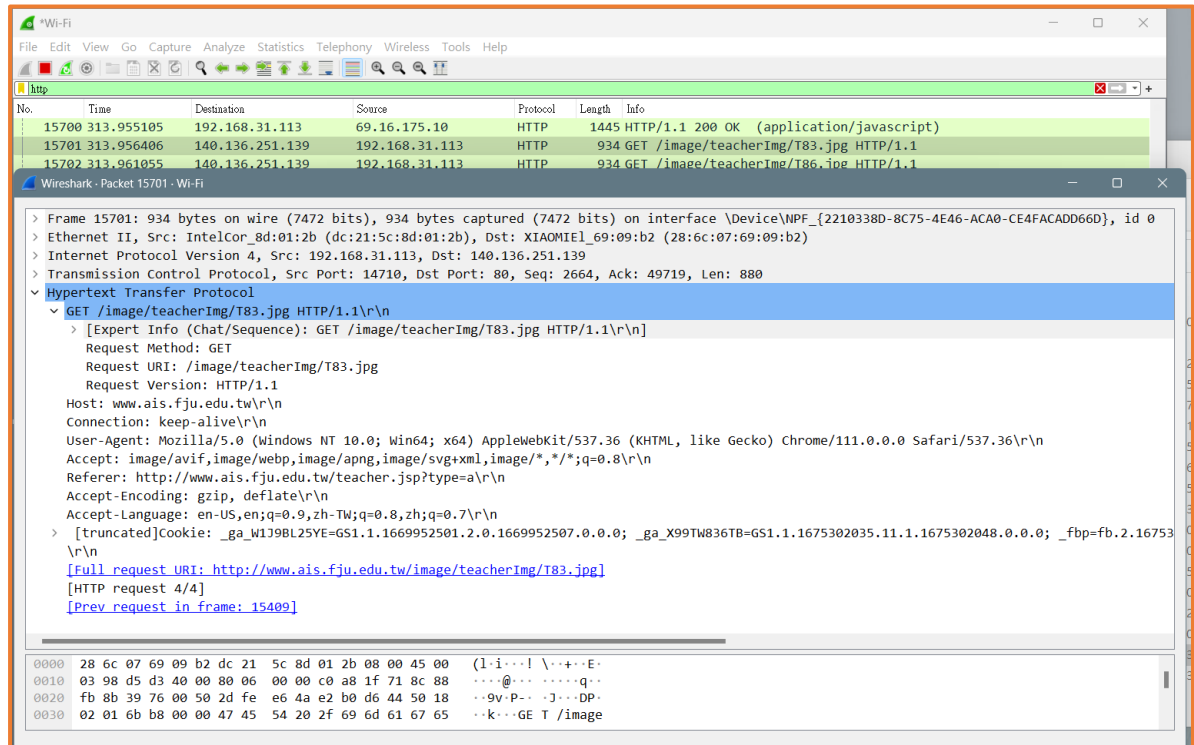
nslookup DNS 查詢

```
ehac@ehac-virtual-machine:~$ nslookup
> www.youtube.com
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
www.youtube.com canonical name = youtube-ui.l.google.com.
Name:   youtube-ui.l.google.com
Address: 172.217.160.78
Name:   youtube-ui.l.google.com
Address: 142.251.42.238
Name:   youtube-ui.l.google.com
Address: 172.217.163.46
Name:   youtube-ui.l.google.com
Address: 142.251.43.14
Name:   youtube-ui.l.google.com
Address: 2404:6800:4012::200e
Name:   youtube-ui.l.google.com
Address: 2404:6800:4012:2::200e
Name:   youtube-ui.l.google.com
Address: 2404:6800:4012:4::200e
Name:   youtube-ui.l.google.com
Address: 2404:6800:4012:3::200e
```

Wireshark

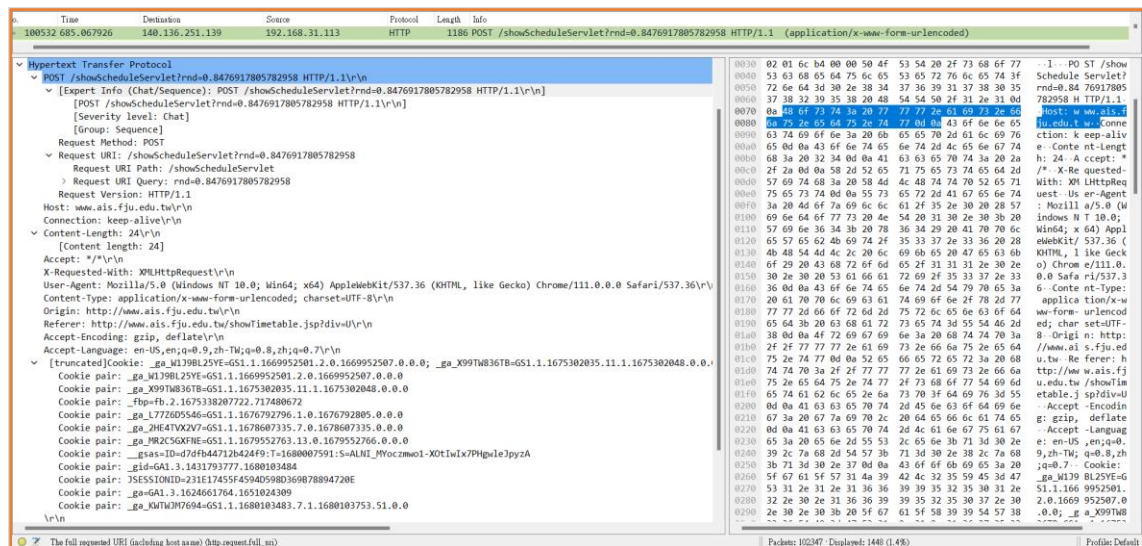
Get



網址：<http://www.ais.fju.edu.tw/image/teacherImg/T83.jpg>

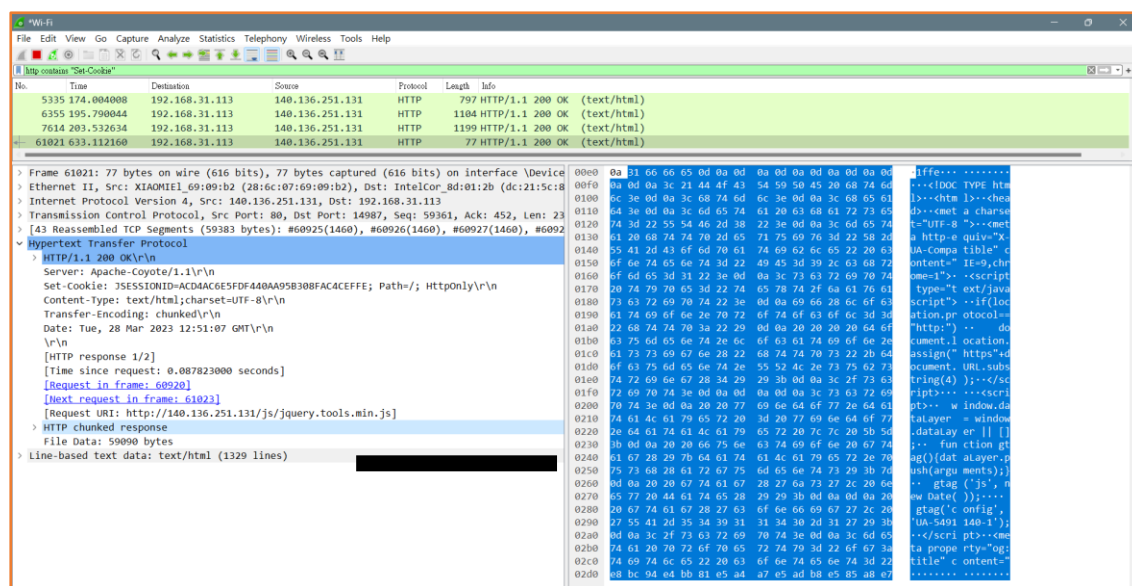
- 雙方瀏覽器運行的 HTTP 版本皆為 1.1
- 140.136.251.139 為對方 IP
- 可以觀察到我在 fju ais 的網站點擊一個 jpg 檔

Post



- Post 與 Get 差異：post 提交的資料放置在是 HTTP 包的包體中，但 get 請求的資料會附在 URL 之後

Set cookie



- HTTP 200 OK 為成功狀態碼且請求成功\
- Http Only 要求瀏覽器不要通過 HTTP（和 HTTPS）以外的管道使用 cookie
這意味著無法通過客戶端手稿語言（尤其是 JavaScript）存取 cookie，因此無法通過跨站點指令碼攻擊輕易竊取
(此段文字取自 <https://zh.wikipedia.org/zh-tw/Cookie>)

wireshark 心得

一開始使用 wireshark 擷取封包時完全不知道這些封包內容可以幹嘛，學習過程中查詢許多資料，發現其實封包裡藏很多資訊。

這次是擷取 http 協定的封包，是沒有經過加密的(明文)，所以如果使用未加密網站傳輸資料時，就等同於自己暴露自己的資料，是非常危險的。

在外如果需要網路也不要亂連接，一旦連接上了，有如自己脫光衣服裸奔，甚麼都被看光光。在資訊發達的年代，資訊安全是人人都必須瞭解的事。