Some tips

bananaapple

Who am I?

- ID : bananaapple
- 學校科系 : 交通大學資工系
- 年級 : 大四
- 目前為 Bamboofox 中的一員
- 學習資安約一年

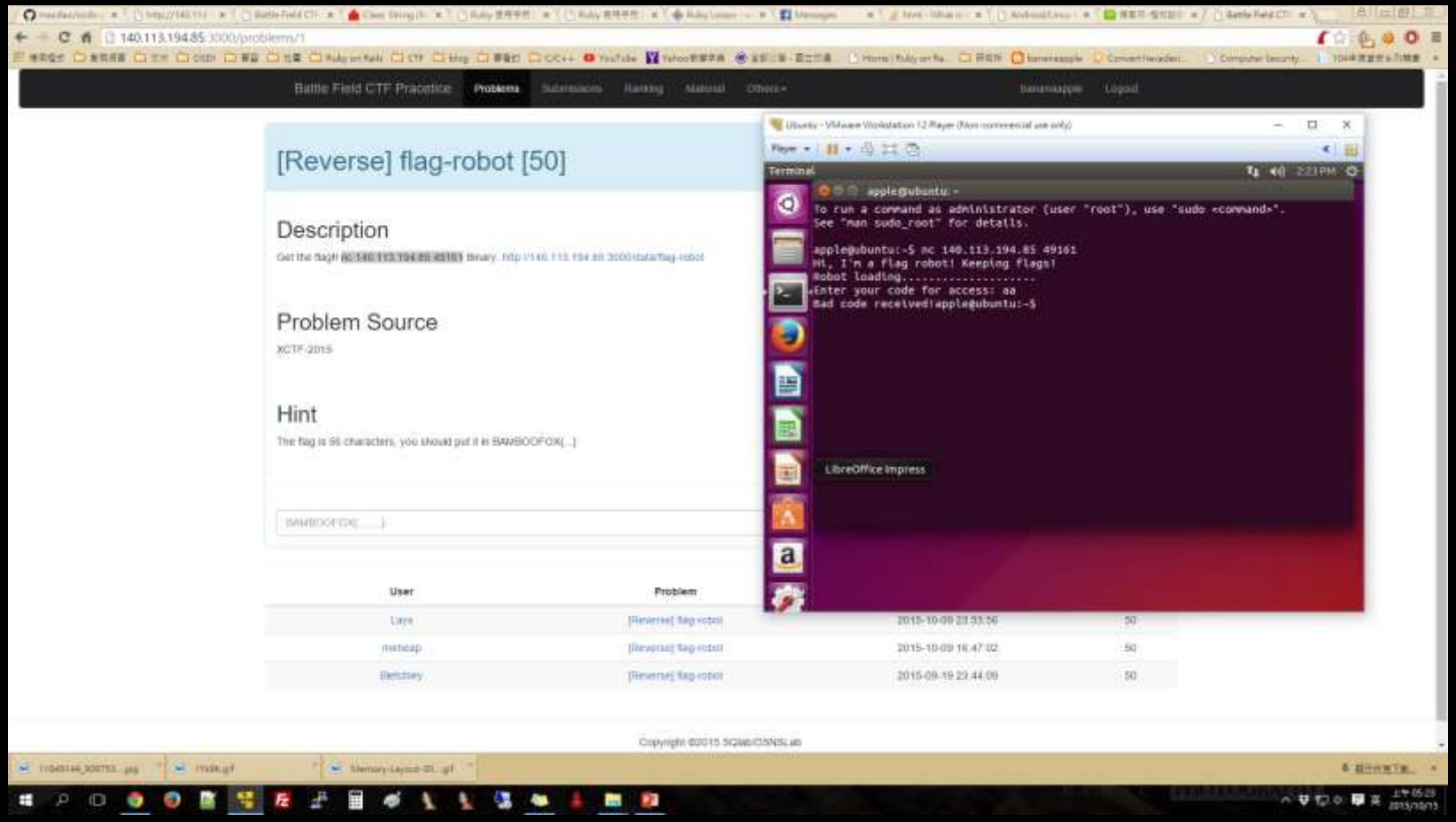
Outline

- 作業系統選擇
- Virtual Box VMware Player
- 電腦架構
- RAM
- OS
- i386 and amd64
- Vim
- Tmux
- Fast tips

作業系統選擇

- 沒有最好的作業系統
- 選擇自己最熟悉、用起來最順手的
- 個人偏愛使用 Windows 搭配虛擬機 Linux
- Windows 小算盤 (程式設計師模式)
- Putty 或 Cygwin
- 虛擬機請務必安裝 Guest Addition
- 才可以方便地使用共用剪貼簿和複製貼上

作業系統選擇


Battle Field CTF Practice
Problems
Submissions
Ranking
Material
Others
[Reverse] flag-robot [50]
Description
Problem Source
Hint
Terminal
apple@ubuntu: ~
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
apple@ubuntu:~$ nc 140.113.194.85 49161
Hi, I'm a flag robot! Keeping flags!
Robot loading.....
Enter your code for access: aa
Bad code received!apple@ubuntu:~$
LibreOffice Impress
User
Problem

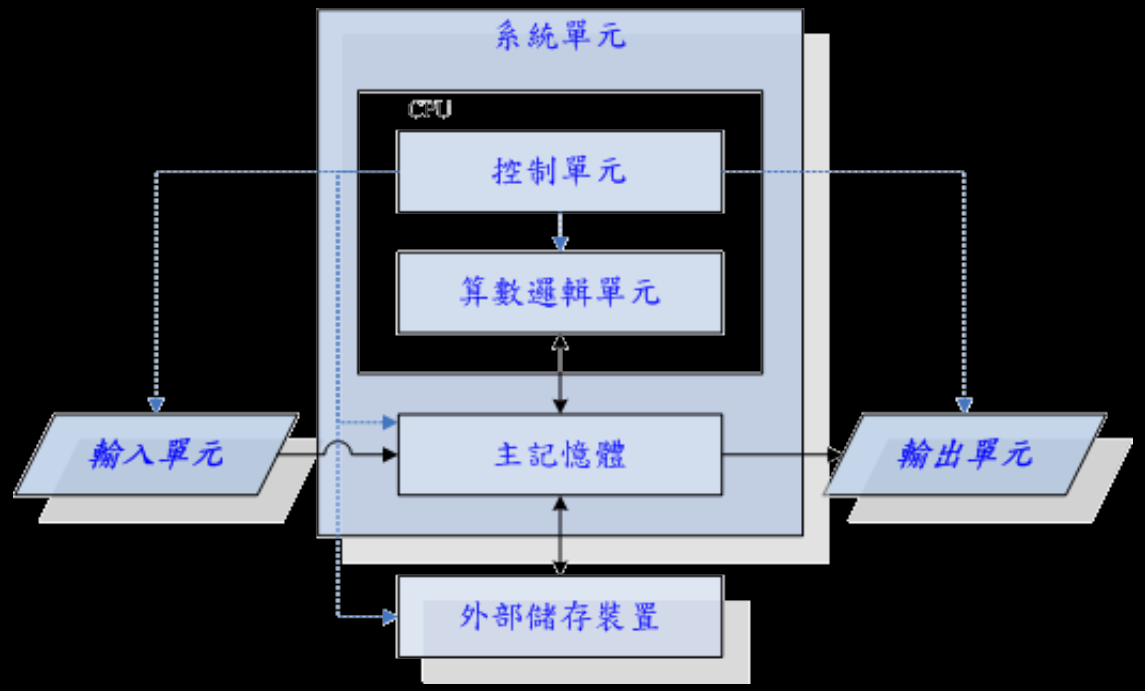
Virtual Box VMware Player

- Vmware Player
- 支援Windows、Linux
- 有方便的自動安裝(設定好帳號和密碼後幫你灌系統，目前有Ubuntu Kali還沒有)
- 使用 Ctrl+Alt 來切換
- 個人推薦使用 Vmware

- Virtual Box
- 支援Windows、Linux、OS X
- Virtual Box 5.0出來後
- 把原本 Vmware 有的 drag and paste.....都做出來了
- 基本上和現在的Vmware沒什麼差異
- 使用Ctrl來切換

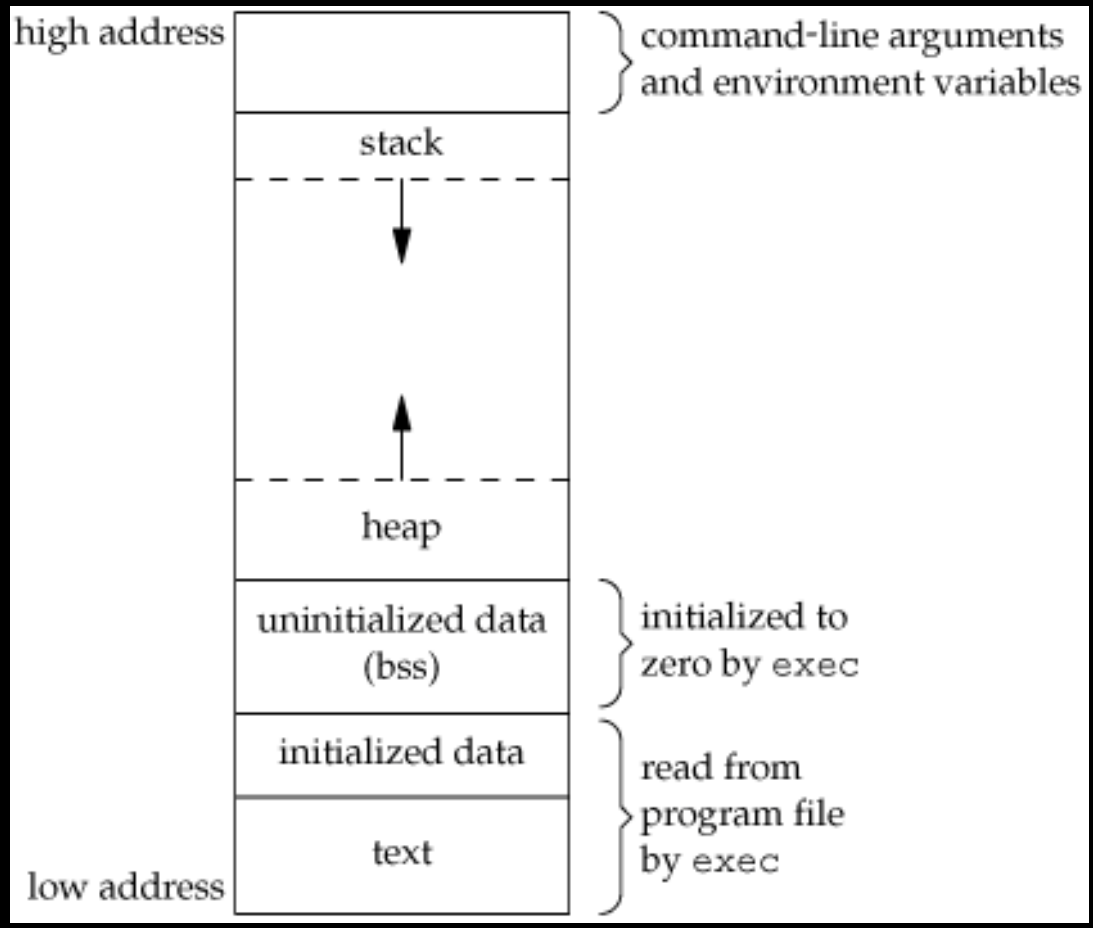
電腦架構

- 先來講講電腦架構吧
- 輸入單元：滑鼠、鍵盤……任何能讓你傳送訊息的元件
- 輸出單元：螢幕、音響、印表機……
- 主記憶體就是我們常說的RAM
- CPU就是整個電腦的核心
- 所有的運算都在CPU進行
- 外部儲存裝置：硬碟、隨身碟



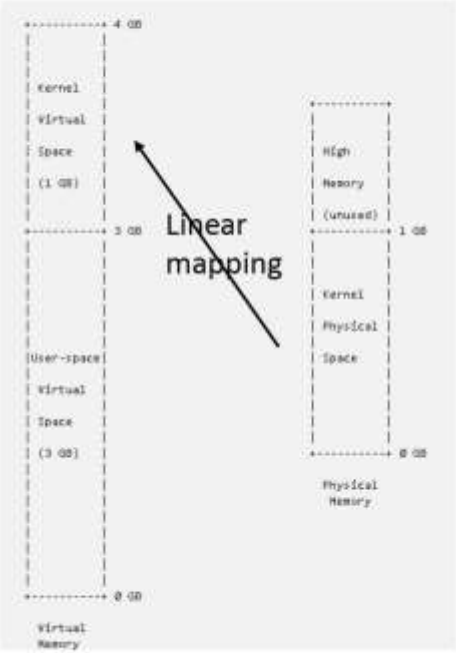
RAM

- 現在我們能看到的 memory address 都稱作 Virtual Address
- 可以達到 memory 隔離
- 避免存取到其他process的 memory
- 使用 Paging 來實作
- 在硬體實作上使用 MMU (Memory Management Unit) 將 Virtual Address 轉換為 Physical Address



RAM

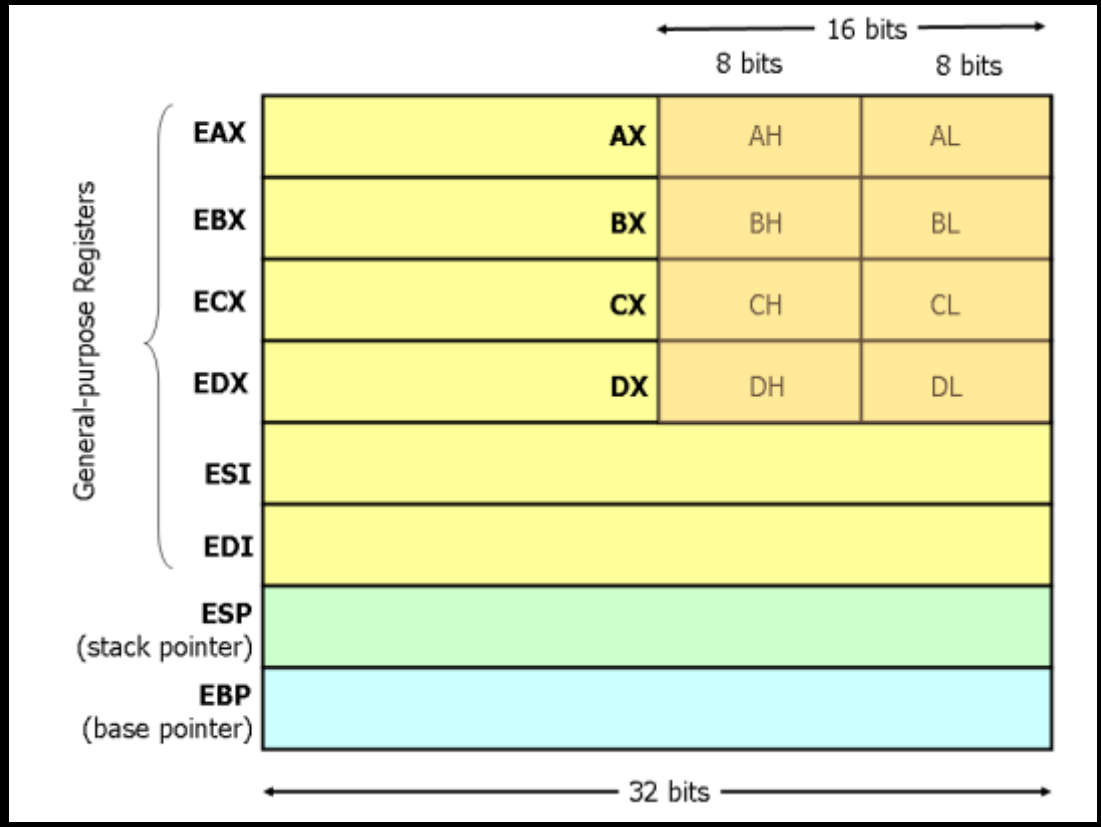
Kernel Address Mapping



- The kernel uses linear mapping from the 1st GB of the physical memory to the 4th GB of the virtual memory
- Physical memory beyond the 1st GB (high memory) can be accessed by kernel only via kernel page mapping (i.e., kernel page table)

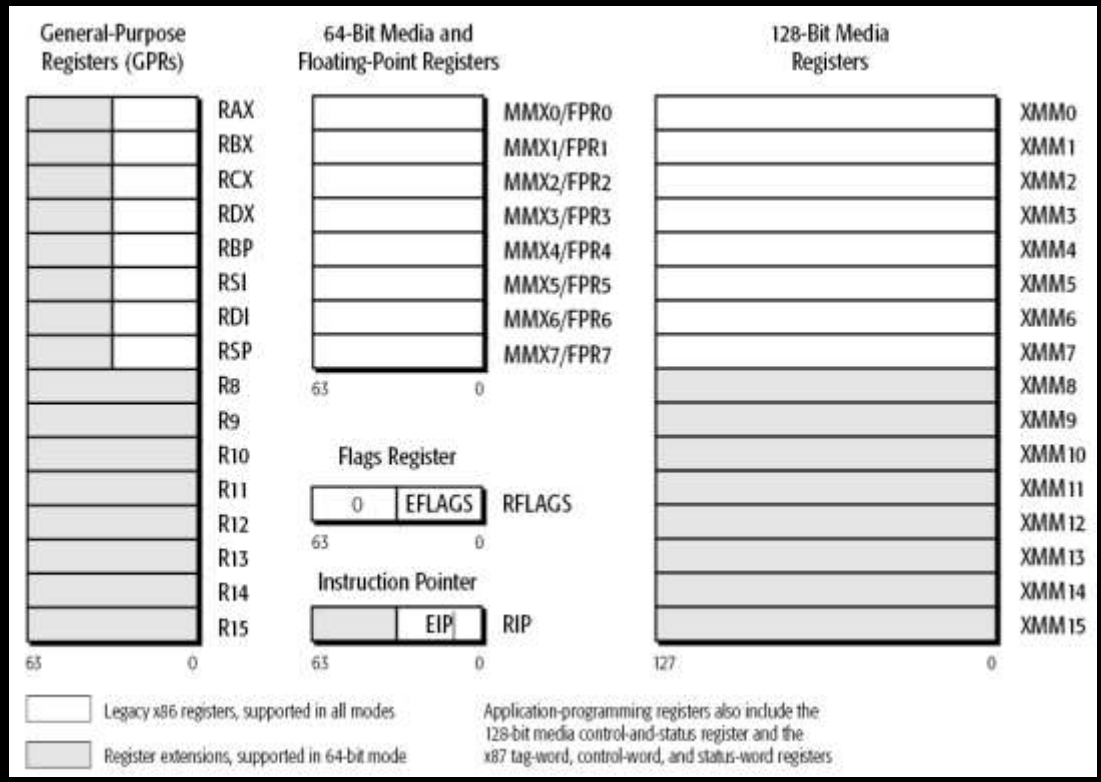
i386 and amd64

- 通常我們會把 CPU 和指令集架構一起講
- CPU 分為 32 bits 和 64 bits
- 這裡的 32 bits 和 64 bits 指的是 CPU registers 的大小
- i386 是一個統稱代表所有 32 bits 架構的 CPU
- IA-32的機器有i386、i486、i586、i686……也可以稱為 x86



i386 and amd64

- amd64、x86-64、x64指的都是64 bits的指令集架構
- amd64 是因為 amd 率先使用了 64 bits 的技術
- 同樣的所有的 registers 都是 64 bits
- 現在大多數電腦作業系統都使用 64 bits



i386 and amd64

Q&A time

- 要是在 32 bits 的 CPU 上插超過 4GB的 RAM 會怎麼樣?

沒有功用因為 x86 的 CPU 只能定址到 2^32 的 memory

- Program Files 和 Program Files (x86) 資料夾有什麼差?

因為 x64 的 CPU 也可以執行 32 bits 的程式，所以會把 x86 的程式安裝在這個資料夾裡

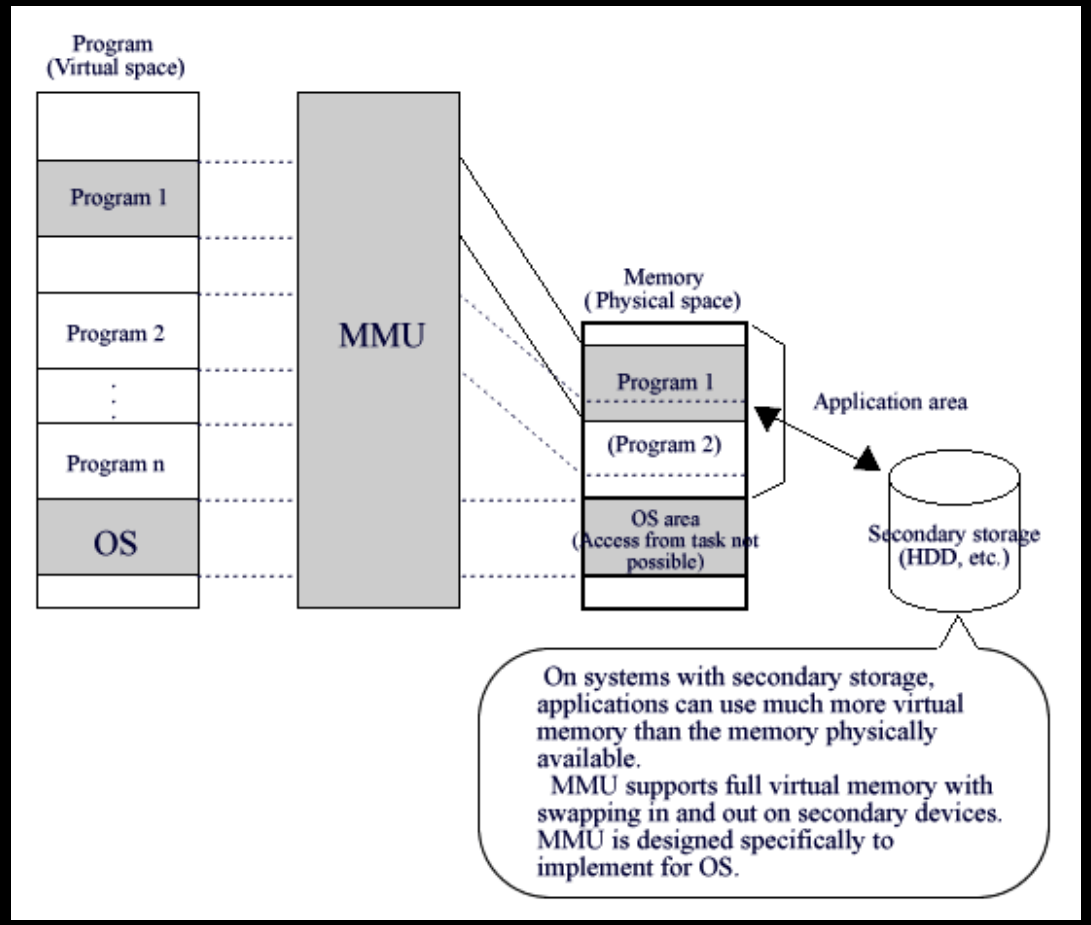
OS

- 一支長駐在記憶體中的程式
- 扮演硬體與軟體間的橋梁
- 有效率地規劃並使用硬體資源
- 提供 API 給 program 來存取硬體資源
- Linux System call

http://docs.cs.up.ac.za/programming/asm/derick_tut/syscalls.html

- 分成兩種 Mode (Kernel Mode and User Mode)

OS


Program
(Virtual space)
Program 1
Program 2
Program n
OS
MMU
Memory
(Physical space)
Program 1
(Program 2)
OS area
(Access from task not possible)
Application area
Secondary storage
(HDD, etc.)
On systems with secondary storage, applications can use much more virtual memory than the memory physically available.
MMU supports full virtual memory with swapping in and out on secondary devices.
MMU is designed specifically to implement for OS.

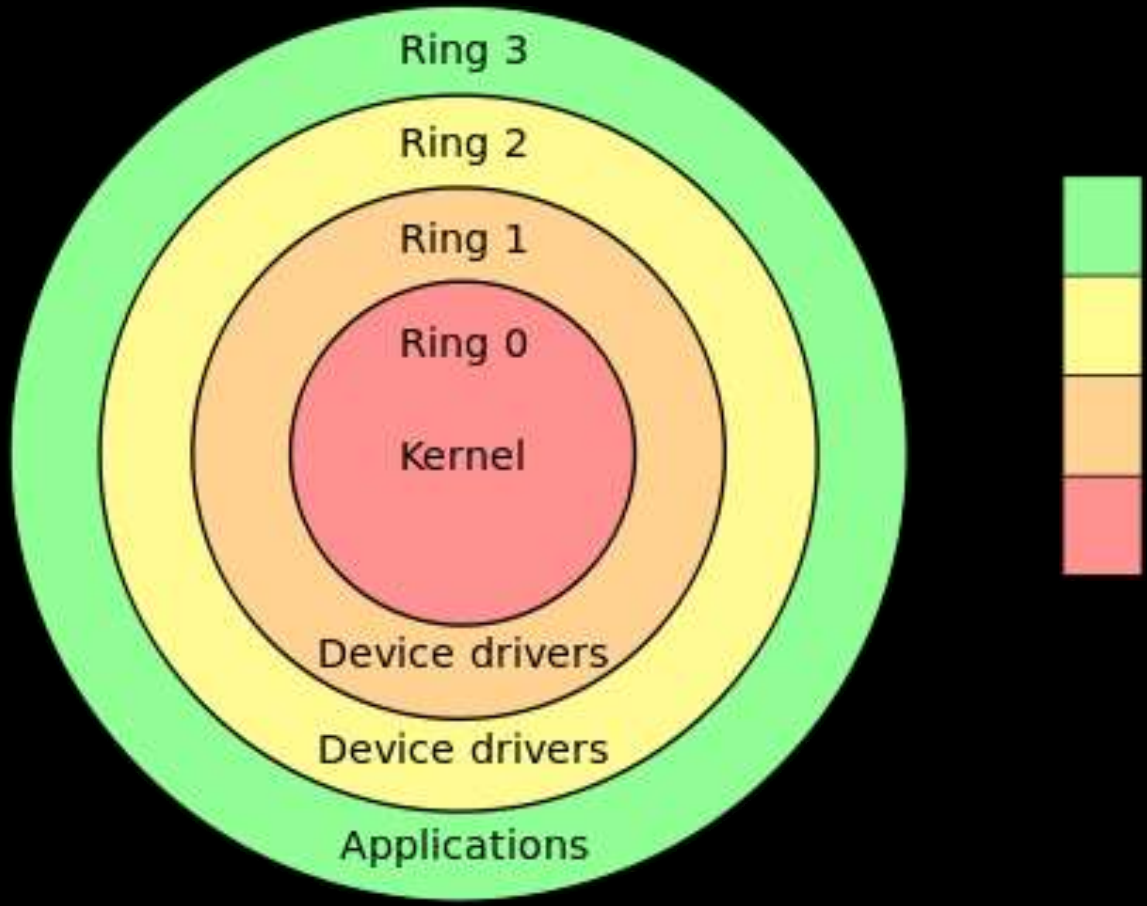
OS

- 實際上只有使用 Ring 0 (User Mode) 和 Ring 3 (Kernel Mode)
- Kernel Mode

所有指令都可以執行

- User Mode

只能執行一些有限的指令，可以透過 Interrupt 來切換到 Kernel Mode



Vim

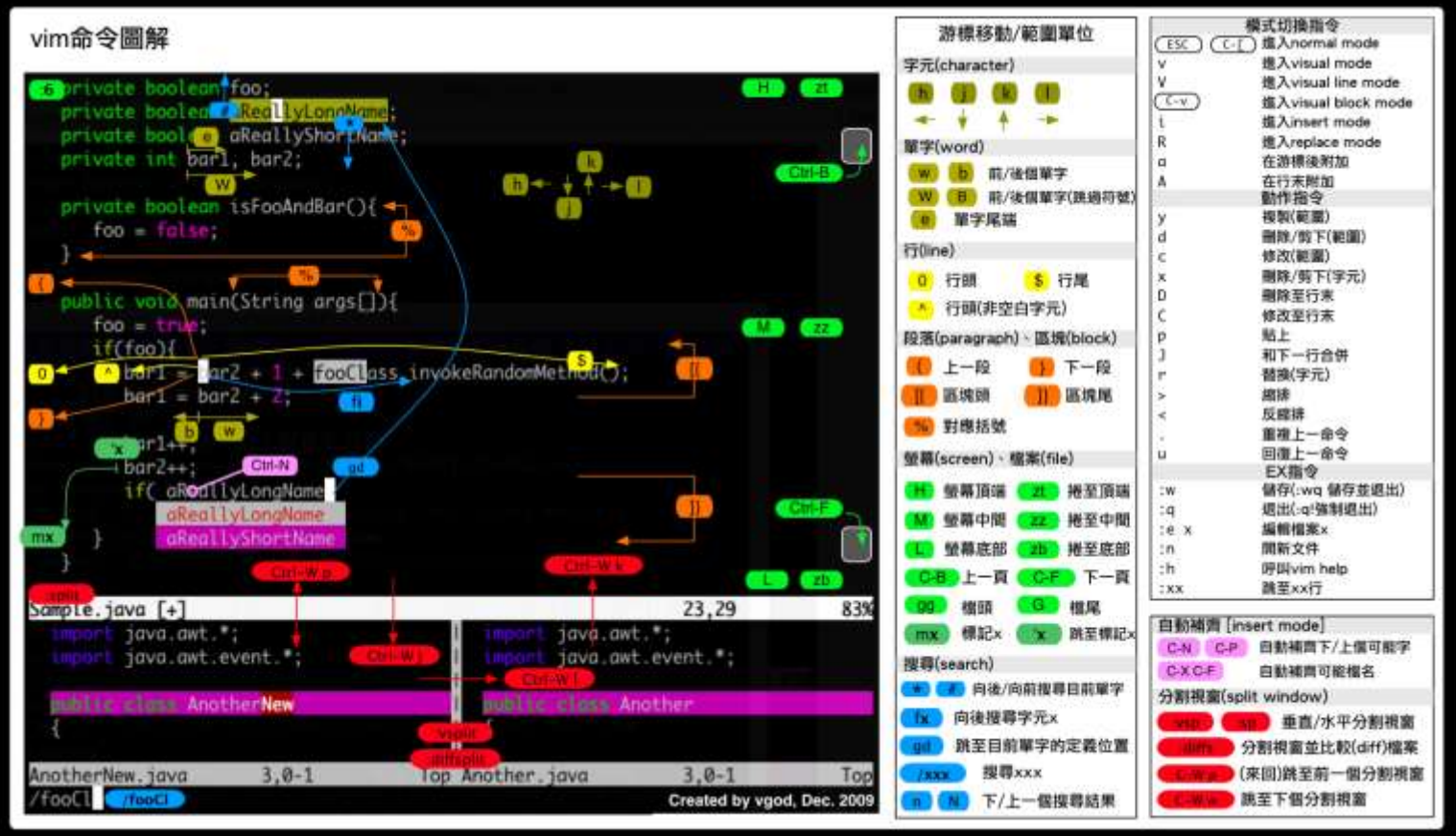
- Command-line based text editor
- open terminal type vimtutor
- 教學部分請各位自行參考
- Vbird

http://linux.vbird.org/linux_basic/0310vi.php

- Study Area

http://www.study-area.org/tips/vim/

Vim


vim命令圖解
游標移動/範圍單位
字元(character)
單字(word)
行(line)
段落(paragraph)、區塊(block)
螢幕(screen)、檔案(file)
搜尋(search)
模式切換指令
動作指令
EX指令
自動補齊 [insert mode]
分割視窗(split window)
Created by vgod, Dec. 2009

Vim

- Vundle

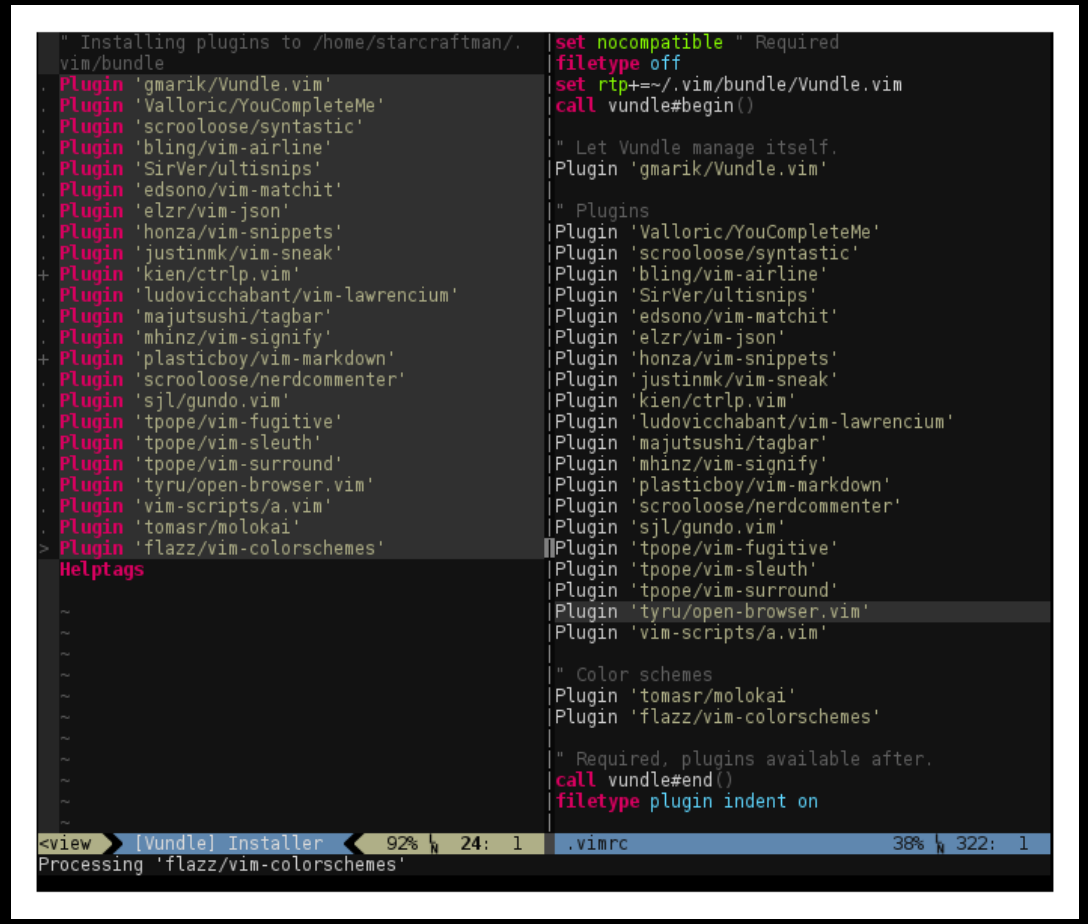
https://github.com/VundleVim/Vundle.vim

- Powerline

https://github.com/powerline/powerline

- NERD-tree

https://github.com/scrooloose/nerdtree

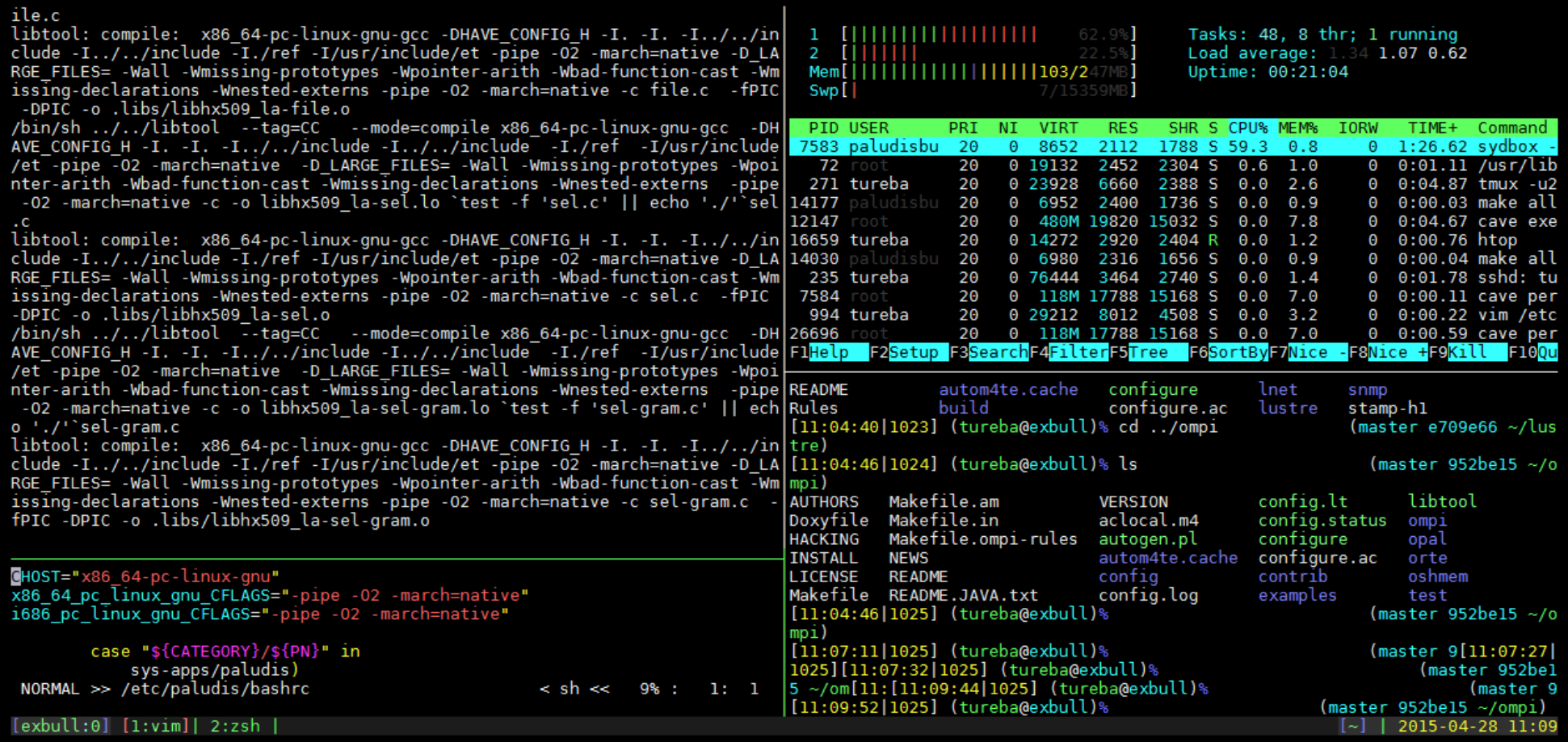


Screen and Tmux

- 不想開太多 Terminal?
- 想回到上次的工作階段?
- Keep online
- 既然 Tmux 比較新我們就學 Tmux 吧!!!
- Debian GNU / Linux

apt-get install tmux

Screen and Tmux



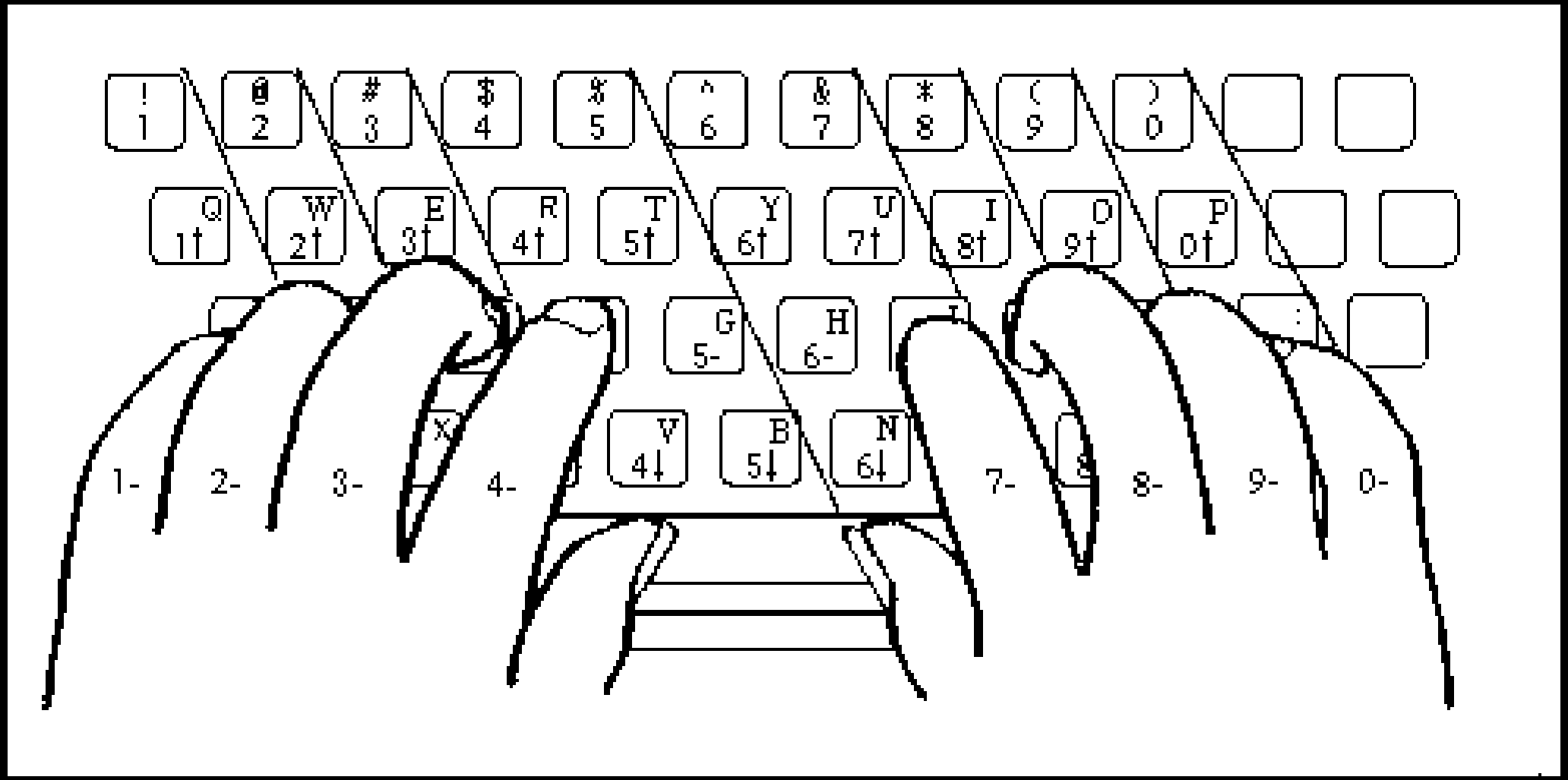
Screen and Tmux

- Ctrl+b 組合鍵 : Ctrl 按住不放再按b
- Ctrl+b c : 建立新的視窗
- Ctrl+b & : 刪除目前的視窗
- Ctrl+b n : 切換到下一個視窗
- Ctrl+b p : 切換到上一個視窗
- Ctrl+b d : detach 目前的 session
- Ctrl+b attach : 回到上次 detach 的 session
- Ctrl+b % : 左右分割兩個視窗

Fast tips

- 能不要碰滑鼠盡量不要碰
- Bash 快捷鍵像是 Ctrl+a可以跳到行首
- 熟悉 vim 裡面的 Mode 切換和快捷鍵使用
- 熟悉 nc、wget、cat、echo……指令
- 有現成的工具就用現成的，不要重複去寫需要的功能
- 請盡量保持手型像是下一張投影片 這樣
- 左手食指放在 f 右手食指放在 j 上

Fast tips



Reference

- VMWare Player vs. VirtualBox

http://teddy-chen-tw.blogspot.tw/2010/07/vmware-player-vs-virtualbox.html

- Vbird鳥哥私房菜

http://linux.vbird.org/linux_basic/0105computers.php

- Memory layout of c program

http://www.geeksforgeeks.org/memory-layout-of-c-program/

- 程式設計師的自我修養

http://www.books.com.tw/products/0010456858

Reference

- Wiki os

https://en.wikipedia.org/wiki/Operating_system

- Wiki x86

https://zh.wikipedia.org/wiki/X86

- Wiki x86-64

https://zh.wikipedia.org/wiki/X86-64

- Screen and Tmux

https://nasa.cs.nctu.edu.tw/sa/2015/slides/IRC_tmux_screen.pdf