Forensic

whoami

- 蔡聿善 / Chumy
  - CSIE @ NCKU
  - 網管 兼 CTF Web/Misc/Rev @ B33F 50uP
  - 資安組實習生 @ TTC
  - 出題 Web & Rev @ AIS3
  - 設定與管理 Infra & 出題 Rev @ TSCCTF
  - https://blog.chummydns.com/

競賽經驗

- 第 47 屆國際技能競賽國手選拔賽 - 資訊與網路技術備取國手
- balsn CTF 2021 - rank 9
- HITCON CTF 2022 - rank.2(台灣區排名) / rank.37
- Balsn CTF 2023 - 臺灣第二名
- 2023 CGGC - 決賽第五名
- 2023 資安技能金盾獎 - 第六名 展露頭角獎
- 2023 T貓盃 - 第一名
- AIS3 EOF CTF 2024 - 決賽第四名
- 第 54 屆全國技能競賽 南區分區賽 - 網路安全 第一名

甚麼是 Forensic

- 一種偏向藍隊的技術
- 主要講述如何回復電腦上的一些操作上的痕跡，比如駭客的攻擊紀錄等等。

Forensic 要學習的能力

- 封包分析
- 記憶體分析
- 硬碟分析
- 檔案分析
- Log 分析
- 各種奇奇怪怪的技術（要學的技術範圍應該比 Web 廣）
- 通常比較吃經驗

封包分析

封包分析工具

- 錄封包工具
  - Wireshark
  - tcpdump
  - ssldump
- 封包分析工具
  - Wireshark
  - Python 的 pyshark
  - Python 的 Scapy
- 封包竄改工具
  - Python 的 Scapy

Tcpdump

- Linux CLI base 的封包攝取工具
- 可以設定 filter 並將攝取到的封包印到 output 或者存到 pcap 檔內（通常用來方便拿去用 wireshark 分析）

Tcpdump

抓包：

`tcpdump -i <網卡>`

抓 ethernet frame：

`tcpdump -ei <網卡>`

印出 raw data：

`tcpdump -Ai <網卡>`

Tcpdump

匯出 pcap：

```
tcpdump -i <網卡> -w <file>
```

過濾：

```
tcpdump -i <網卡> <filter rule>
```

https://hackmd.io/@Jimmy01240397/rJxI49dxEA

Wireshark

- GUI base 的封包攝取工具
- 功能強大的封包分析工具也有很多插件可以裝

Wireshark-LAB

[震撼彈] AIS3 官網疑遭駭！

壓縮檔破解

明文攻擊

當你手上剛好有壓縮檔中其中一個或多個檔案的明文時就能夠將該壓縮檔破解

https://github.com/keyunluo/pkcrack

```
zip plain.data.zip plain.data
```

```
./pkcrack -C Secret.zip -c plain.data -P plain.data.zip -p plain.data
```

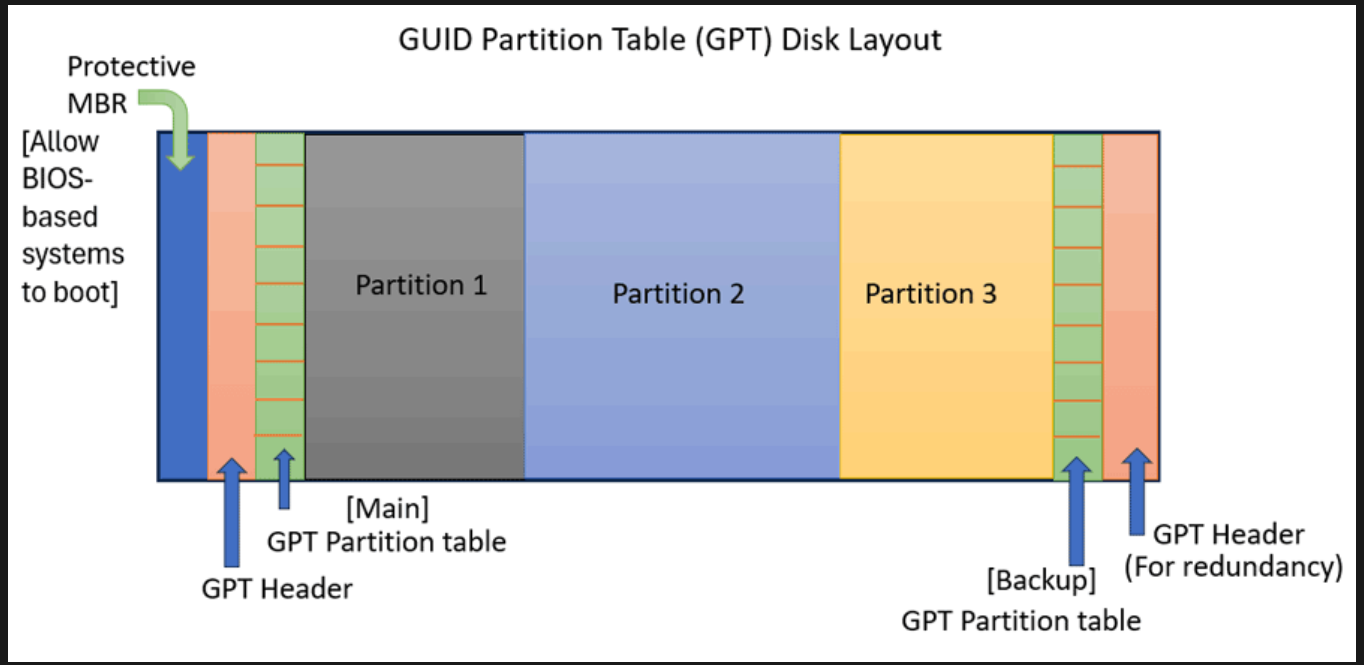
```
./zipdecrypt key0 key1 key2 ../../Secret.zip secret.zip
```

明文攻擊-LAB

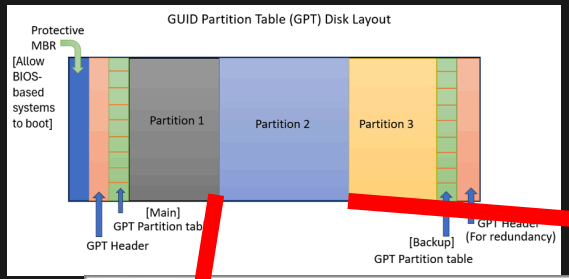
The truth of Plain

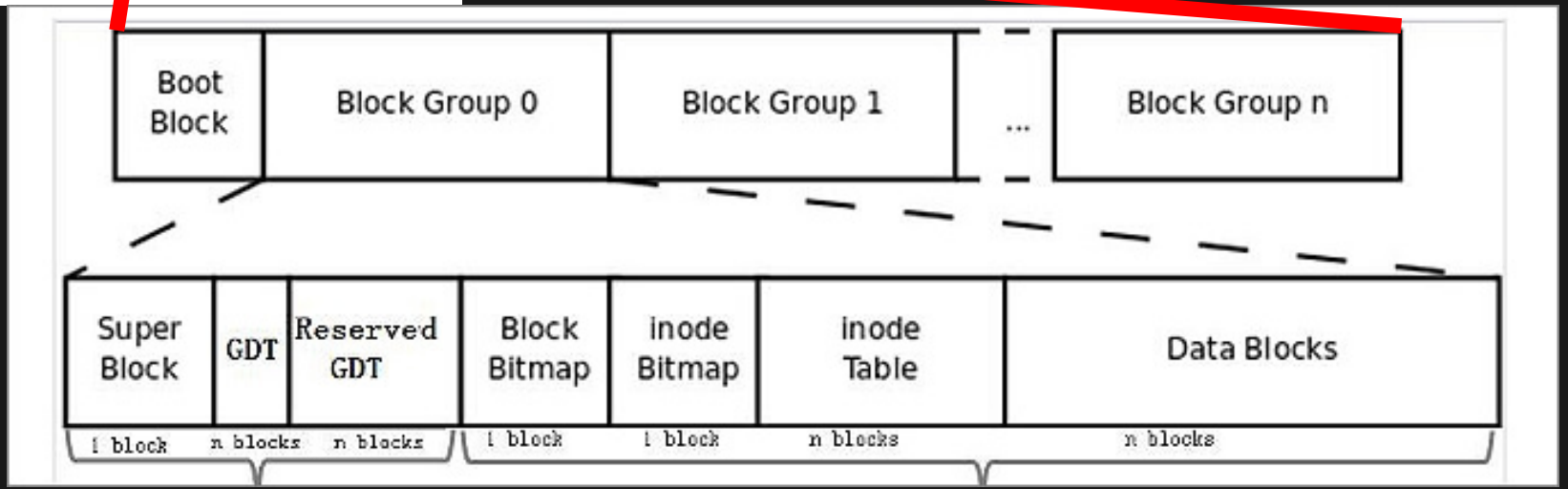
資料鑑識

Disk Layout

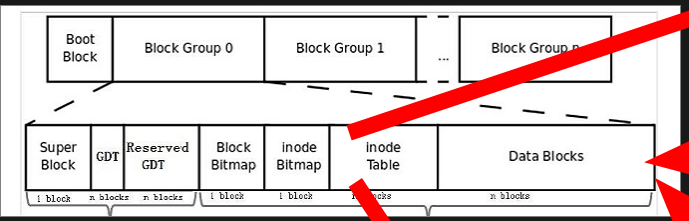

GUID Partition Table (GPT) Disk Layout
Protective MBR
[Allow BIOS-based systems to boot]
Partition 1
Partition 2
Partition 3
[Main] GPT Partition table
GPT Header
[Backup] GPT Partition table
GPT Header (For redundancy)

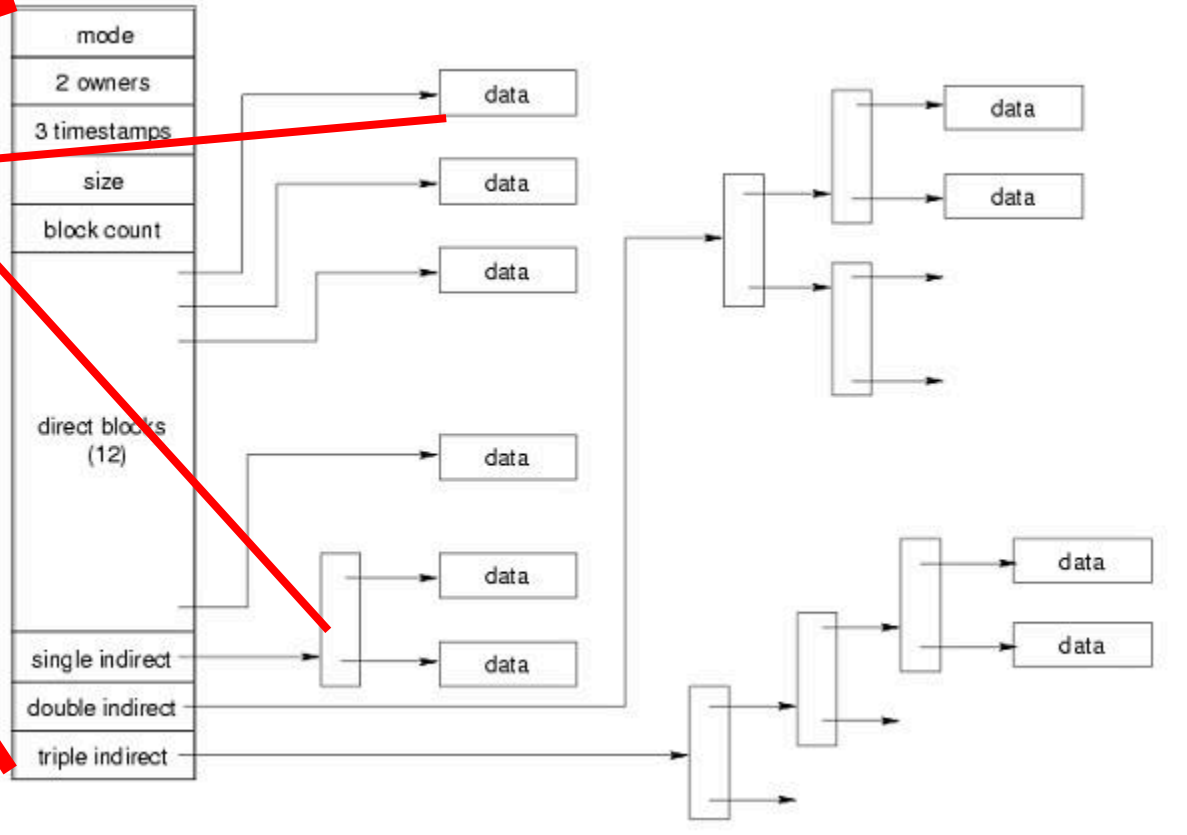
Disk Layout


GUID Partition Table (GPT) Disk Layout
Protective MBR
[Allow BIOS-based systems to boot]
Partition 1
Partition 2
Partition 3
[Main]
GPT Partition tab
GPT Header
[Backup]
GPT Partition table
(For redundancy)


Boot Block
Block Group 0
Block Group 1
...
Block Group n
Super Block
GDT
Reserved GDT
Block Bitmap
inode Bitmap
inode Table
Data Blocks
1 block
n blocks
n blocks
1 block
1 block
n blocks
n blocks

Disk Layout


Boot Block
Block Group 0
Block Group 1
...
Block Group n
Super Block
GDT
Reserved GDT
Block Bitmap
inode Bitmap
inode Table
Data Blocks
1 block
n blocks
n blocks
1 block
1 block
n blocks


mode
2 owners
3 timestamps
size
block count
direct blocks (12)
single indirect
double indirect
triple indirect
data
data
data
data
data
data
data
data
data
data
data

Disk Layout

找文件流程：

```
t1dotlessj -> ../share/lcdf-typetools/./t1dotlessj/t1dotlessj
t1lint -> ../share/lcdf-typetools/./t1lint/t1lint
t1rawafm -> ../share/lcdf-typetools/./t1rawafm/t1rawafm
t1reencode -> ../share/lcdf-typetools/./t1reencode/t1reencode
t1testpage -> ../share/lcdf-typetools/./t1testpage/t1testpage
```

1. 找 root inode 也就是 inode 2
2. 如果是目錄，到 Data 裡找下一層的名稱，裡面會有紀錄對應的 inode index
3. 如果是 symbolic link，到 Data 裡找 link 到的名稱，回上層按照新名稱找 inode index
4. 如果是檔案，到 Data 直接讀檔
5. 重複執行以上步驟直到找到目標

fdisk or gdisk

用來調整分割表的工具

`fdisk <disk>`

用命令 p 可以看硬碟的布局

```
Command (m for help): p

Disk /dev/sda: 30 GiB, 32212254720 bytes, 62914560 sectors
Disk model: QEMU HARDDISK
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x2163ce12

Device     Boot    Start      End  Sectors  Size Id Type
/dev/sda1           2048 60819455 60817408   29G 83 Linux
/dev/sda2       60819456 62914559  2095104 1023M  5 Extended
/dev/sda5       60819458 62914559  2095102 1023M 82 Linux swap / Solaris
```

fdisk or gdisk

用命令 n 可以新增 partition

用命令 d 可以刪除 partition

在這邊誤刪沒有太大的關系，因為他只會動分割表，不會真的動 partition 或 filesystem

只要你能知道 offset 就能重新 new 回來，但千萬不要清掉 filesystem 的 header

testdisk

強大的硬碟修復工具

```
sudo apt install testdisk
```

```
sudo testdisk
```

testdisk

找回 partition offset

選擇創建新的日誌檔案或者追加到現有的日誌檔案。

選擇你需要恢復的磁碟。TestDisk 會列出所有可用的存儲裝置。

選擇分區表類型（通常 TestDisk 能自動檢測，例如 EFI GPT 或 MBR）。

選擇 [Analyze] 選項進行分區結構分析。

進行深度掃描（如果快速掃描未能找到分區）：

選擇 [Quick Search] 進行快速掃描。

如果快速掃描未找到丟失的分區，可以選擇 [Deeper Search] 進行更深入的掃描。

Lab

Fix disk partition

如何掛整顆硬碟：

```
losetup --partscan --find --show /mnt/discforensic.raw
```

掛 partition：

```
mount /dev/loop<index>p<partition num> <目錄>
```

解掛：

```
umount <目錄>

losetup --detach /dev/loop<index>
```

Sleuth kit

一套 CLI base 的硬碟鑑識工具集，包含：fls、fcat、icat、mmls

看硬碟布局：

```
mmls <disk>
```

list file on disk:

```
fls -o <partition offset> <disk> <inode index>
```

list file on partition:

```
fls <partition> <inode index>
```

Sleuth kit

cat file on disk:

```
fcat -o <partition offset> <file path> <disk>
```

cat file on partition:

```
fcat <file path> <partition>
```

cat inode data on disk:

```
icat -o <partition offset> <disk> <inode index>
```

cat inode data on partition:

```
icat <partition> <inode index>
```