

Module – 02

電腦鑑識的調查程序



可以分為

事前準備 > 事中調查 > 事後報告 > 有必要時有專家、技術證人

此章探討程序的重要性，程序是整個鑑識過程的開始



LO # 01

了解鑑識調查的程序和他的重要性



為了讓標準一致，所以一切從程序開始，固定的格式、流程

Step 1 > 首先一定要有明確的目標，到底要鑑識什麼？

Step 2 > 適時的做條件假設，要靠觀察
e.g. 如果目標有裝Dropbox，可以假設在
C:\Users\Admin\AppData\Roaming\
C:\Program Files(x86)
C:\Program Files
以上資料夾中找到些什麼

Step 3 > 某些假設不能直接在目標上測試，所以要做實驗設計

Step 4 > 工具的選擇



Step 5 > 工具跑完後做結果審查和評估

Step 6 > 結論和意見陳述

根據事實做出結論

意見是根據事實在科學上所代表的意義

- 出庭做技術證人（有參與調查的過程）
詳細說明調查的過程並在最後做出結論
- 專家證人（沒有參與調查的过程）
給專業意見（必須要有履歷，被法院、法官認可）



LO # 02

了解調查前的階段



電腦鑑識實驗室的建置

Step 1 > 規劃與預算的考量

Step 2 > 實體與結構設計的考量

Step 3 > 工作區域的考量

Step 4 > 實體安全的考量

Step 5 > 人力資源的考量

Step 6 > 鑑識實驗室的執照

e.g. ASCLD/LAB、ISO/IEC 17025



建立調查團隊（較難）

單一任務的人員不能太多，用以保護調查的機密性，防止資訊洩露，但能量（實力）要夠

鑑識實驗室的軟、硬體需求（相對簡單，有錢就好）

- 硬體 > 最少要一台工作站
- 軟體 > 使用付費的軟體，一方面是符合法律規範，另一方面是破案速度快



軟、硬體的驗證

用某個工具分析證據，這個證據要能上法院，這個工具就要先通過**驗證**且必須**定時**驗證

目前驗證電腦鑑識工具最具代表性的是
Computer Forensics Tool Testing (CFTT) 為NIST制定電腦鑑識工具的標準

鑑識實驗室也要確保品質保證 (Quality Assurance,QA)



LO # 03

了解第一時間的反應



First Responder (FR) ，也可以稱為前端、現場人員

為第一個到案發現場的人員

FR可以分成三類

- 非鑑識人員
e.g. 目擊證人、警察...等
- 系統/網路管理員
最不希望的，有時候反而會造成反鑑識
- 鑑識人員



非鑑識人員的第一反應

比較不擔心，因為這類的人員比較不懂這方面的技術，有時候反而有好處

這類人員的主要目標為**保護現場**，讓現場保持一個**安全**的狀態

如果可以也可以記個筆記、拍個照

系統/網路管理員的第一反應

較擔心，因為這類的人員會想要**救系統**（IR流程），他們的努力就是鑑識人員的壓力

這類人員的主要目標為根據IR流程做**通報**且**不應該做任何動作**



鑑識人員的第一反應

前端人員做**收集**而非分析

Step 1 > 記錄、保護電子犯罪現場
拍照或素描

Step 2 > 收集危機事件的資訊
進行目擊證人的訪談（要**客觀**，不要被帶風向）

Step 3 > 扣押、搜索
要有搜索票



Step 4 > 辨識、收集電子證據

要看是開機還是關機，會攸關到資料型態

Step 5 > 打包電子證據

要預防實體破壞和電子干擾...等

Step 6 > 運輸電子證據



LO # 04

了解調查階段



Step 1 > 紀錄電子犯罪現場

Step 2 > 扣押、搜索

Step 3 > 證據的保存

Step 4 > 資料獲取

Step 5 > 資料分析

Step 6 > 案例分析

Step 7 > 報告

Step 8 > 作為專家證人（不一定會有這個）

Step 1~3 為FR，Step 4~8 為鑑識實驗室人員



Step 1 紀錄電子犯罪現場

此時**證物監管鏈**（後面會提到）就要開始紀錄且要遵守**規範**一切都要**符合程序**

拍照或素描

現在大多拍照、錄影，較少畫畫



Step 2 扣押、搜索

扣押、搜索的流程

1. 規劃扣押、搜索

- 1 尋求嫌疑人同意，簽自願同意搜索書（不同意則進入2）
- 2 取得證人簽名（不同意則進入3）
- 3 取得搜索令（不會開空白的搜索令）
- 4 收集危機事件資訊

在我國根據刑法搜索與扣押128、131條分成有令、無令搜索



2. 初步搜索現場

3. 保護和評估犯罪現場

4. 於犯罪現場取證

搜索令可分為

- 電子儲存設備
e.g. 軟、硬體、儲存設備、文件
- 服務提供者
e.g. 服務紀錄、帳單紀錄、客戶資訊

但實務上沒分那麼細



在**某些情況**，允許無搜索令的搜索

- 當證據即將銷毀時，如果有合理的理由相信所扣押的物品構成犯罪活動的證據，則無正當理由扣押該證據是合理的
- 在有權的人同意下，可以在沒有搜查令的情況下搜查

但如果不符合上述兩項，在等不到搜索令也沒有自願搜索同意書的情況下，搜到的證據上法院也無效



處理開機的電腦

- 應在執行任何動作前想清楚
- RAM會包含很多重要資訊，但他本身是易揮發的元件

情況1 > 如果電腦開機且可以看到螢幕畫面，就拍下當時的畫面和時間、紀錄清楚

情況2 > 如果電腦開機，但進入螢幕保護程式，慢慢地移動滑鼠，不要按任何按鈕，如果有畫面，就拍下當時的畫面和時間

情況3 > 移動滑鼠，沒有反應，直接拔電源線，可能還會在硬碟中保留一些暫存檔



處理關機的電腦

如果只是螢幕關閉，可以考慮打開，然後輕輕地移動滑鼠

但如果不是，就考慮打包、運送問題即可

處理有連網的電腦

將網路線拔除



不同OS的關機流程

正常情況下，使用工具將易揮發性的資料轉換成非揮發性的資料，再正常關機

如果沒辦法做到上述的流程，絕對不可以關機，直接拔插頭是唯一選擇

處理智慧型手機或其他手持式設備

讓他處於開機狀態，拍下當時的畫面和時間、紀錄清楚，並放入電磁波隔絕袋，防止電磁波干擾



Step 3 證據的保存

證據是犯罪現場收集來的，一年過後用在法院，經過時間、空間的改變，如何讓法官相信？

證物監管鏈 (Chain of Custody)

用來管理證據的收集、處理、存儲、測試和處置，並防止篡改或替換證據也就是
所有人、事、時、地、物的完整紀錄

證物監管鏈的要求

1. 格式、時間不能中斷
2. 完整且符合當地法規的程序要求



證據袋內容清單

1. 扣押日期和時間
2. 扣押證據的調查員
3. 編號
4. 扣押證據的地點
5. 證據袋中的詳細內容
6. 提交機構及其地址

Case # _____ Item # _____ Initials _____ Date _____ C495690

DO NOT TAMPER

FOLD LIP OVER OPENING TO SEAL

WARNING: TAMPER EVIDENT SECURITY PACKAGE ONCE SEALED.

EVIDENCE

Agency _____

Item No _____ Case No _____

Type of Offense _____

Victim _____

Suspect _____

Date of Collection _____ Time of Collection _____

Collected By _____

Description of Evidence _____

Location of Collection _____

CHAIN OF CUSTODY

Received From _____ By _____

Date _____ Time _____ AM/PM

Received From _____ By _____

Date _____ Time _____ AM/PM

Received From _____ By _____

Date _____ Time _____ AM/PM

1216-00000-EVIDENCE



證據袋要好好的保存

尤其是內容物，因為最後不管有罪無罪都要歸還

雖然看起來不怎麼樣，只是個小袋子，但有點貴、有專利

編號有固定格式

e.g. aaa/ddmmyy/nnnn/zz

- aaa > 調查人員的名稱縮寫
- ddmmyy > 扣押日期
- nnnn > 扣押證據的序號
- zz > 零件編號
e.g. a為電腦、b為螢幕、c為鍵盤...等等



所有的過程都要注意證物監管鏈不可中斷，要符合程序

Step 4 資料獲取

分析的第一步就是做鑑識備份，資料複製（Imaging），不太會用copy、backup這個詞，真的要用就使用Forensic copy

鑑識備份不是單純的檔案複製，而是整個磁碟、磁區複製（bit by bit 或是 bit to bit copy 或是 bit stream copy 或是 sector to sector）

要計算原始證物和鑑識備份的雜湊值，確保完整性

原始證據永遠不能被拿來做分析



R-Drive Image的實作

先把R-Drive Image安裝好（ 我使用6.3版，30天試用 ）

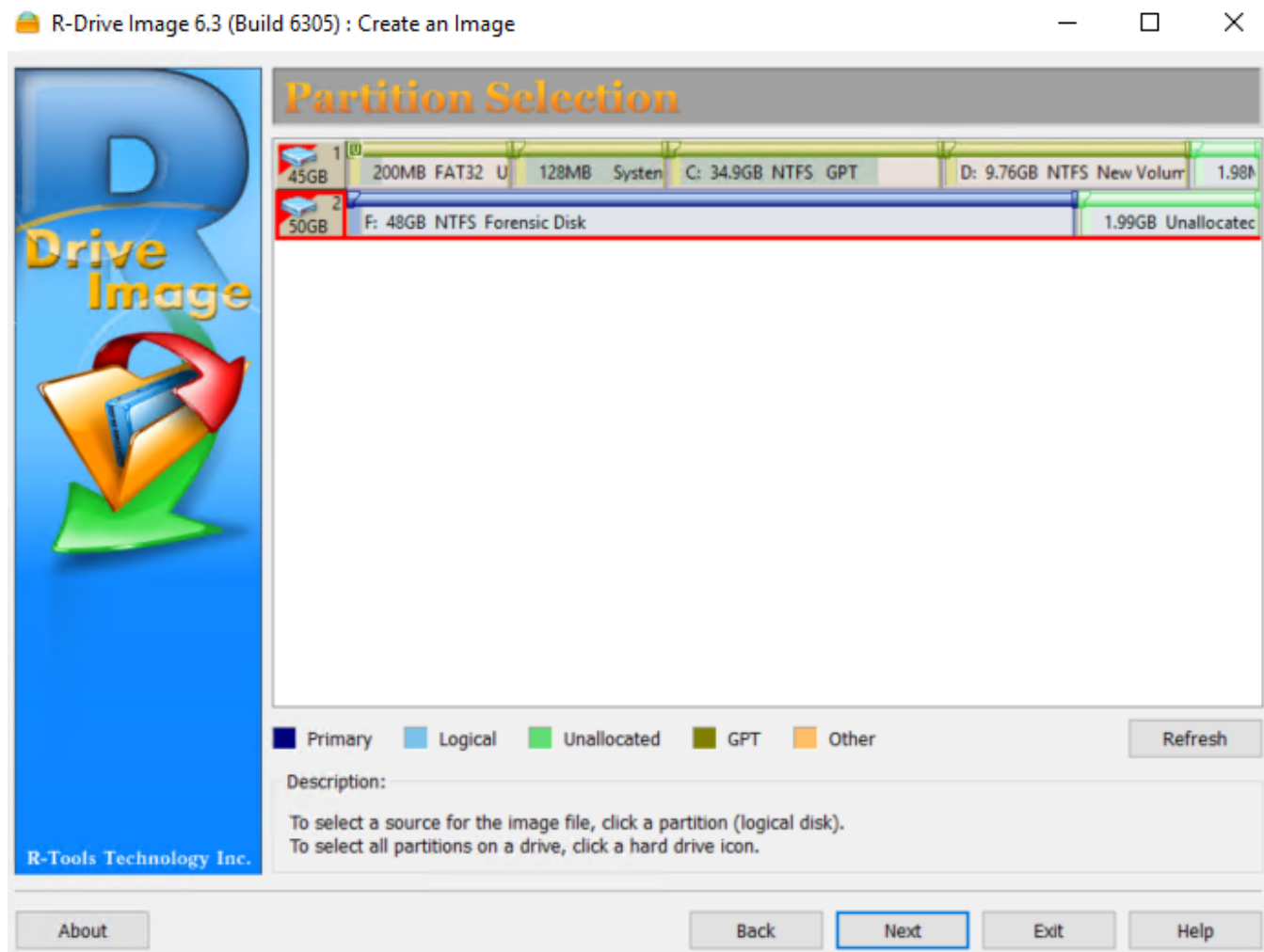
R-Drive Image會產出rdr副檔名，該副檔名為廠商的專屬格式，但R-Drive Image有過CFTT，所以可以在各個工具做轉換，但無法使用該廠商提供的特殊功能





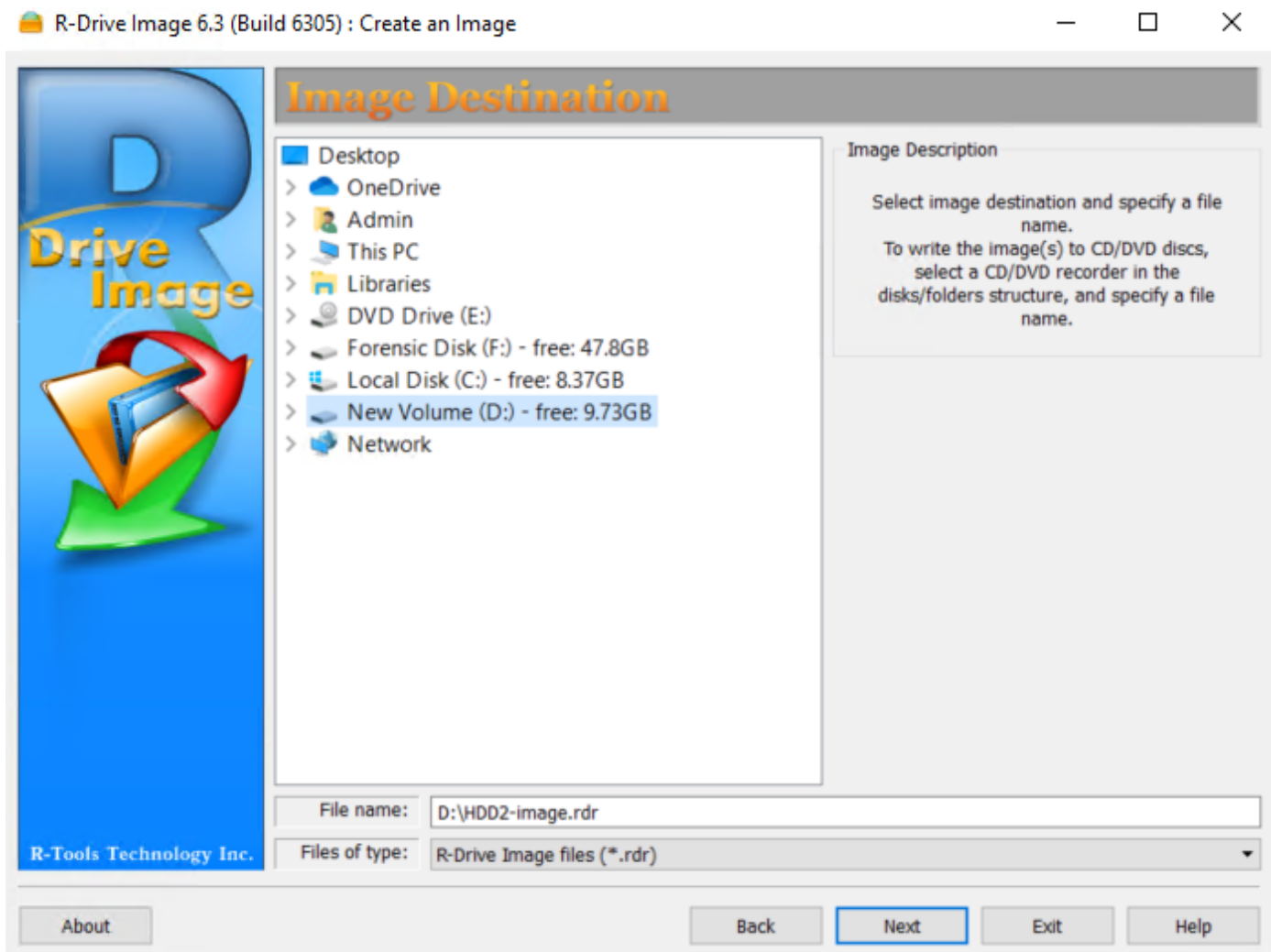
先製作一個映像檔





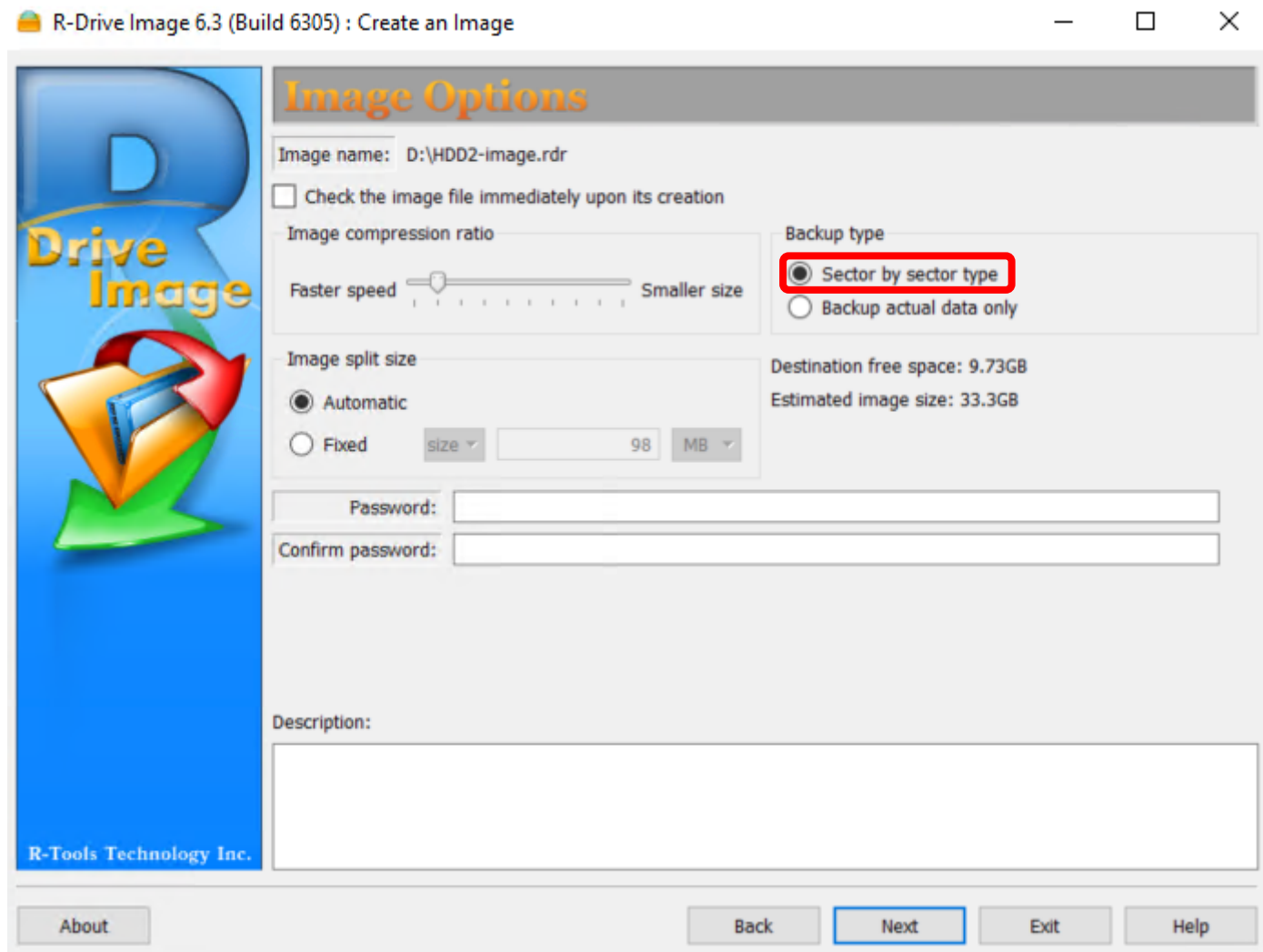
選擇要製作成映像檔的磁碟，切記要選擇到整個硬碟（注意紅框框）
因為我們要做的是Forensic copy






選擇要存放映像檔的位置，盡量不要放在要製作映像檔的那個硬碟中





注意備份種類要選擇Sector by sector，因為我們要做的是Forensic copy，其他都可以選擇預設值





Backup Options

Snapshot providers

- ☒ Windows Volume Snapshot Service
- ☒ R-TT Volume Snapshot Service

Process priority

Backup Process Priority: Normal

Use CPU Cores: Unlimited

☐ Notify system applications

Backup AUX applications

Before: ...

After: ...

Snapshot AUX applications

Before: ...

After: ...

☐ Ignore disk read errors (bad sectors)

皆為預設值即可





確定沒問題，就可以開始製作了
製作完成後，即可按關閉，拿這個映像檔去做分析



Step 5 資料分析

識別和分類相關的資料順序

Step 6 案例分析

一旦分析了與案件有關的證據，偵查人員就可以利用它來重建犯罪並找出缺失的環節，分成以下三類

- 時間分析（Temporal analysis），事件軌跡的順序性（時間有順序，前後關聯性）
- 關係分析（Relational analysis），分析出其中的關聯（與目標之間的關係）
- 功能分析（Functional analysis），環境跟其他的條件、變數



從社交網路收集證據

可能留下足跡，幫助建立攻擊的時間序、地理位置，但較難判讀真假，只能做為輔助證據



LO # 05

了解事後調查階段



Step 7 報告

遵守格式，符合當地法規、時間、**程序**的**規範**

鑑識調查報告範本需要包含下列內容（統整性的架構）

- 執行摘要
- 調查目標
- 危機事件的詳情
- 調查過程
- 證據資訊
- 評估和分析過程
- 相關調查結果
- 支持的文件
- 其他支持的細節



報告要符合時間的要求在規定內的時間寫完，證據沒有候補，除非是有新發現的事證，報告（必須要符合法律規範，要搭配證物監管鏈給一個完整的紀錄）要交給法律代表送上法庭

報告的原則以完整、清楚、高品質為優先，盡可能寫白話

Step 8 作為專家證人

分為技術、專家證人

必須要非常客觀、專業、有道德性且尊重法庭、程序，有就有，沒有就沒有，沒有應該這兩個字

