## 安裝與使用FTK Imager

|  |  |  |
| --- | --- | --- |
| 題目描述 | 安裝與使用FTK Imager進行資料擷取 | |
| 目的 | 熟悉FTK Imager數位鑑識工具的使用 | |
| 對象 | 學員 | |
| 先備知識 | Windows 標準軟體安裝 | |
| 範圍 | 第二單元(數位鑑識類型與流程) | |
| 時數 | 20分鐘 | |
| 實作流程 | 講師說明 | 5分鐘 |
| 學員實作練習 | 10分鐘 |
| 講師總結 | 5分鐘 |

### 2.2.1實作內容

* 此實作練習包含底下實作內容:

### 實作內容1:下載與安裝FTK Imager工具

### 實作內容2:硬碟擷取(會花很長時間) 建議學員回家練習

### 實作內容3:記憶體擷取

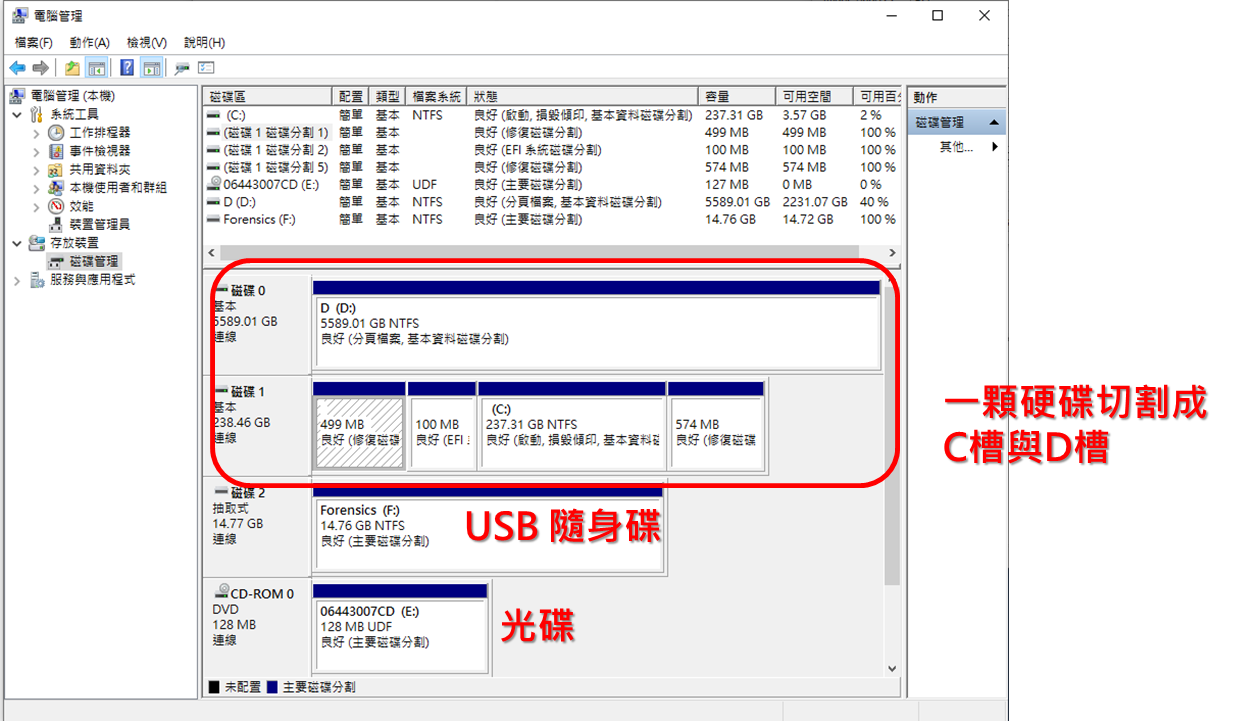
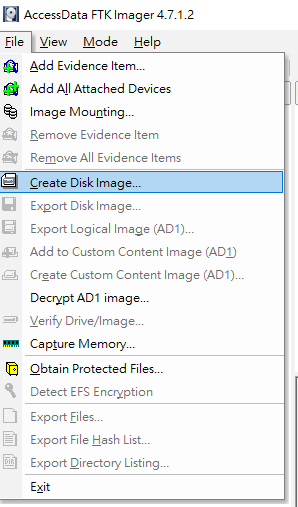
### 實作內容4:USB隨身碟擷取

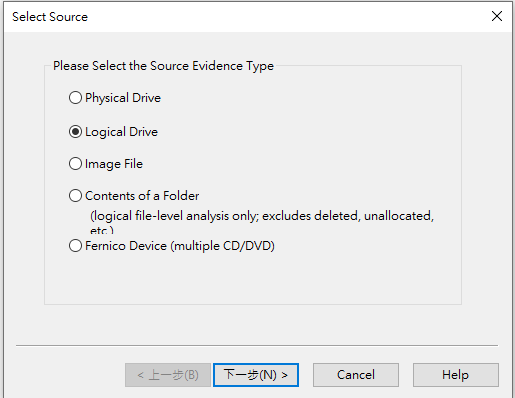
### 實作內容1: 下載與安裝FTK Imager工具

### 步驟1:前往官網下載FTK Imager

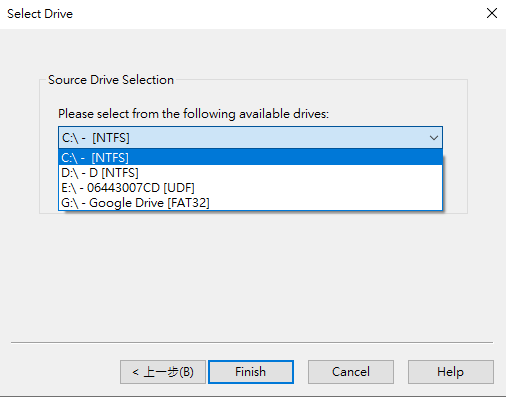
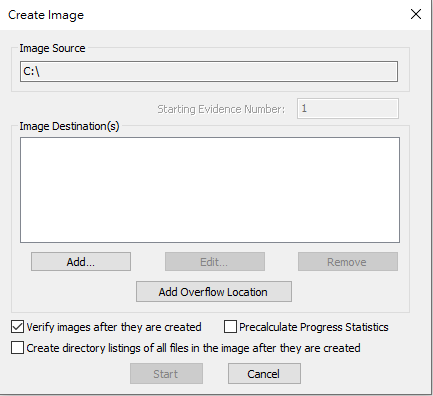
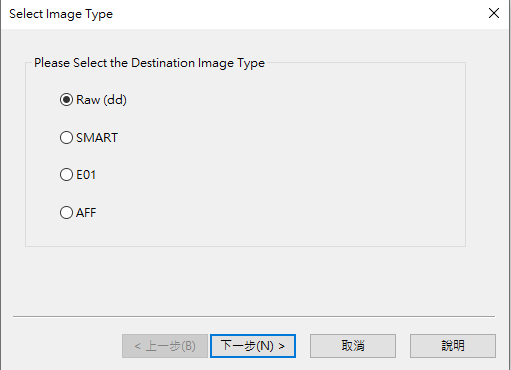
### <https://www.exterro.com/ftk-imager>

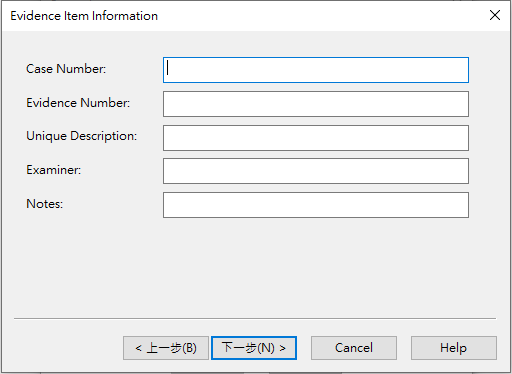
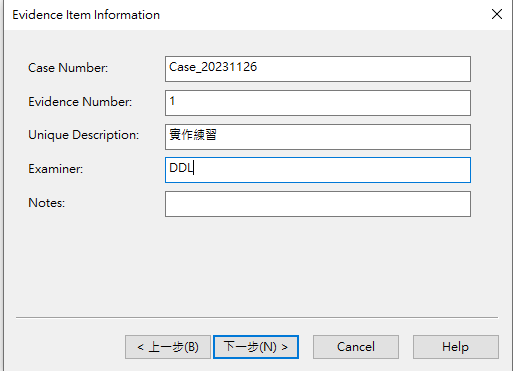
### 步驟2:按標準安裝方式安裝FTK Imager

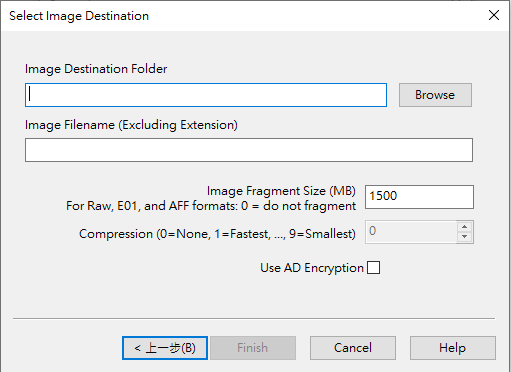
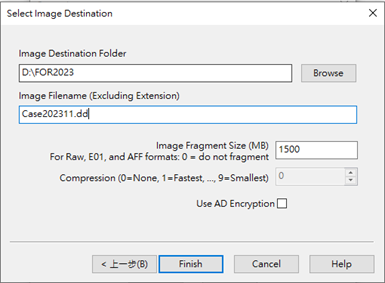
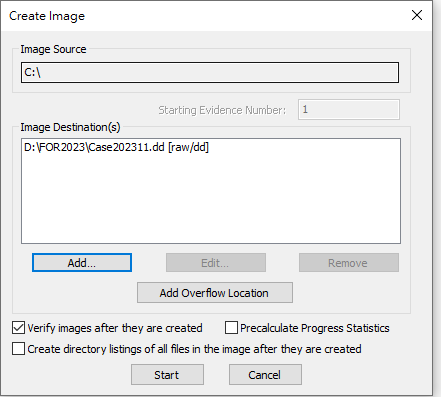
* 實作內容2: 硬碟擷取(會花很長時間)
  + 實作內容將C槽的系統(200+GB)製作成鑑識分析image
  + 步驟2-1:開啟FTK Imager，點選File | Create Disk Image
  + 步驟2-2: 選擇Logical Drive

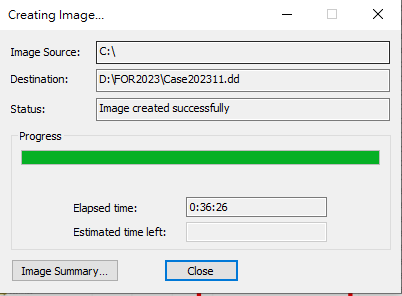
physical drives 是整顆硬碟(physical hard drives),

logical drives 可以選定分割區(partitions)

* + 步驟2-3: 選擇C:\
  + 步驟2-4: 點選ADD 設定擷取後檔案存放位置
  + 步驟2-5:選擇擷取檔案儲存類型 
* Raw (dd): 這是現代分析工具最常用的image格式。這些原始檔案格式的圖像不包含表頭(headers)、元資料(metadata)或魔法值(magic values)。原始格式通常包含對有意跳過的任何記憶體範圍或擷取工具無法讀取的記憶體範圍進行填充(padding)，這有助於保持空間完整性(spatial integrity:資料之間的相對偏移)。
* SMART: 此檔案格式是專為 Linux 檔案系統設計。這種格式將磁碟映像保持為純位元流(bitstreams)，並具有可選的壓縮功能(optional compression)。 該檔案由一個標準的 13-byte表頭與後面的一系列sections組成。每個sections都包含其type string、到下一部分的 64 位元偏移量、其 64 位元大小、填充(padding)與 CRC，以及實際資料或註釋。
* E01: 這是Guidance Software公司EnCase所開發的專有格式。此格式會壓縮image(磁碟映像)。這種格式的image以頁首與頁尾中的大小寫資訊開頭，其中包含整個位元流的 MD5 雜湊值。此格式資訊包含取得日期與時間、檢查者姓名、特別說明及可選密碼(optional password)。
* AFF: Advance Forensic Format (AFF) 是Simson Garfinkel 與 Basis Technology 開發的格式，其最新實作為 AFF4。
* 步驟2-6:填寫資本資料



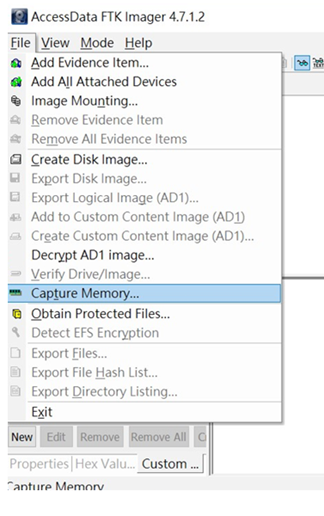
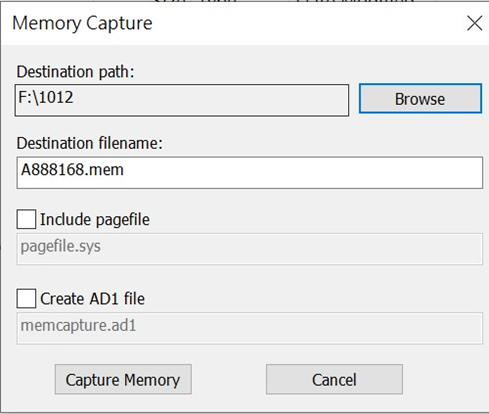
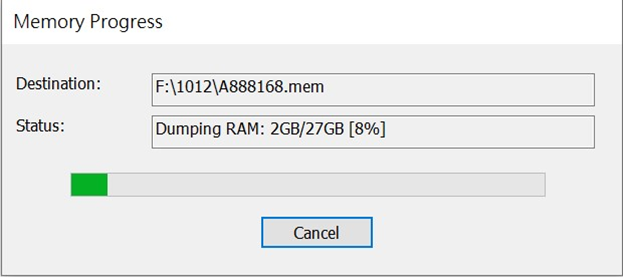
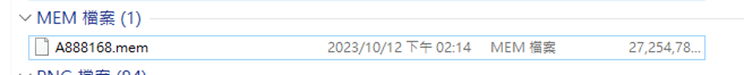
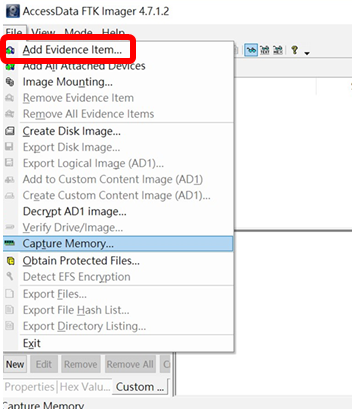
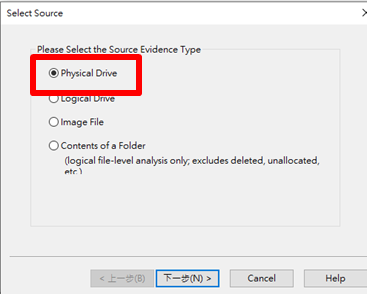
* + 步驟2-7:新增Image目的地(將保存Image檔案的位置)、Image檔案名稱及片段大小。
  + 步驟2-8:設定完成即可點選start開始擷取

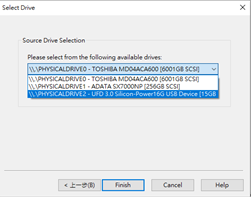
共花了36分鐘26秒

在D:\FOR2023目錄有Case202311.dd.001.txt及Case202311.dd.001~

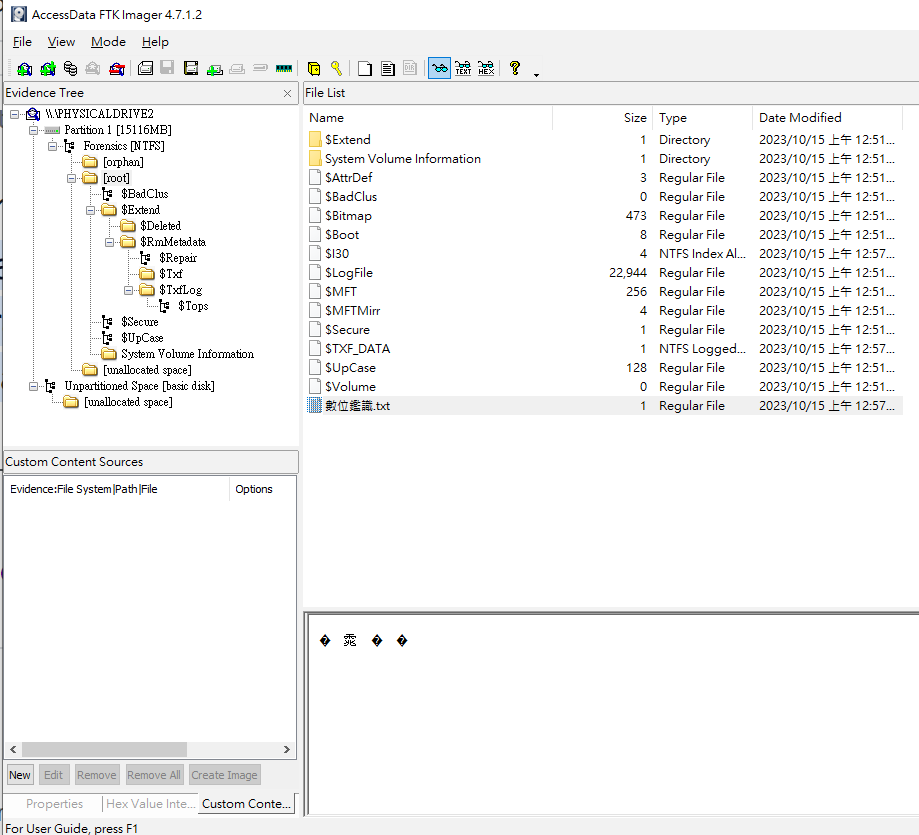
Case202311.dd.163共164個檔案

Case202311.dd.001.txt是描述此次擷取的相關資料:

* 實作內容3:記憶體擷取:
  + 步驟3-1: 點選File | Capture Memory
  + 步驟3-2: 設定存放位置與檔名
    - pagefile：由於RAM的限制， pagefile.sys在 Windows 作業系統中被當作記憶體使用(虛擬記憶體)。它位於“C”partition 下。因此，考慮到RAM記憶體，該檔案可以包含相當多的有價值的資料。因此，建議在採集中捕獲並收集該文件。打勾即可產生pagefile.sys。
    - AD1 檔案： AD1 是 FTK影像檔。鑑識人員可以選擇建立 AD1 檔案以供以後使用。
  + 步驟3-3: 記憶體擷取中
  + 步驟3-4: 擷取完成後，目標資料夾將包含擷取的記憶體，檔案副檔名為“.mem”
* 實作內容4:USB隨身碟擷取
  + 步驟4-1:使用小容量(16GB)的USB 隨身碟並格式化成NTFS格式
  + 步驟4-2:放一個txt文件如下
  + 步驟4-3:開啟FTK Imager並執行底下步驟
    - 步驟4-3-1:點選File | Add Evidence Item…
    - 步驟4-3-2: 選擇Physical Drive
    - 步驟4-3-3: 選擇USB隨身碟



* + - 步驟4-3-4: 完成

 除了檔案外還有一堆NTFS檔案系統的資訊