ComputerForensics

電腦鑑識分析

only for TACERT資安課程使用

警政署資訊室

叢培侃 (peikan@gmail.com)

大綱

- 電腦鑑識與數位證據
- 電腦鑑識種類與技術
- 電腦鑑識案例探討
- 電腦鑑識未來挑戰

電腦鑑識概念

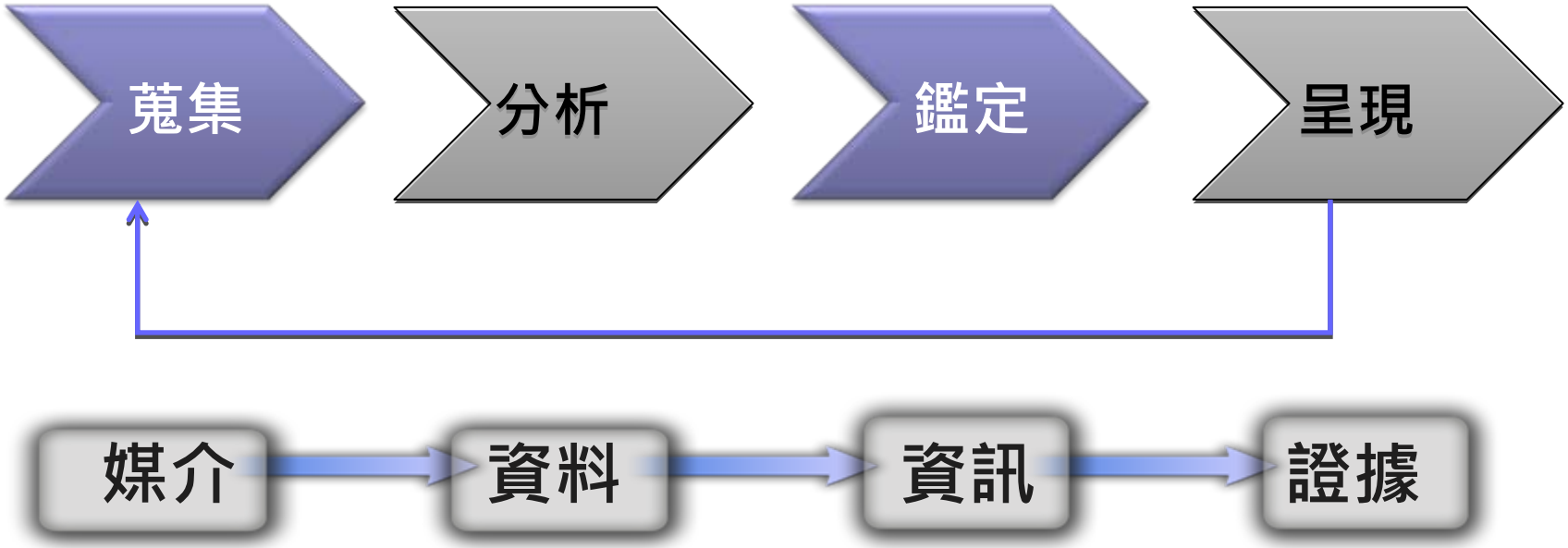
- 電腦鑑識為一種運用科學的技術與方法，對數位證物實施蒐集、分析、鑑定與保存等作為。換言之，電腦鑑識是當事件正發生或發生後，對電腦(資訊)系統或設備找尋與案件有關的數位證據之系統化活動或作為，而經此系統化之作為所呈現的證據，可做為法庭所接受之證據。
- 數位證據具有易被修改、損毀、偽造與刪除的特性，因此，在現場處理證物時，必須在不改變原始證據(最小更動)的原則下，將證物加以紀錄、保存、送往鑑驗等，且務必保持證物鏈之完整。
- 鑑識人員應依照鑑識規範與SOP步驟實施蒐集、保存、鑑定、分析等用以呈現相關證物與該電腦設備或人是否存在不可否認性。

數位證據

Edmond Locard

- 數位證據是一種以二進位(數位)的方式儲存、傳輸的各種可能資訊，包含:圖片、音樂、簡訊、檔案、封包、影像等。 (SWGDE, July 1998).
- 在20世紀初鑑識學家Edmond Locard’s致力於鑑識科學和犯罪現場重建之研究，提出路卡交換原理(Locard ‘s exchange principle):任何人、物只要進入了犯罪現場，必會帶走現場某些東西；必然也會留下某些東西，亦即所謂微物跡証之相互移轉，以數位證據的角度來看你瀏覽一個網站你的電腦必會留下該網站資訊(如:history 、cookies)，而該網站也會留下你的瀏覽紀錄(如web server log、UserAssist等) 。

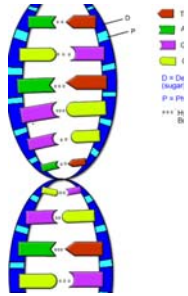
數位鑑識流程



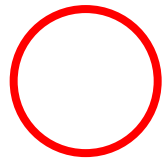
Evidence Viability=Data Preservation+ Data Integrity+ Documentation

常見之電腦犯罪類型

- 以電腦為犯罪工具
  - 非法販賣—販賣違禁品(毒品、槍枝等)
  - 煽惑犯罪—網路三七仔、六合彩明牌
  - 網路詐騙—拍賣詐欺、網路男蟲
  - 非法言論—千面人恐嚇、妨害名譽
  - 非法傳輸—P2P

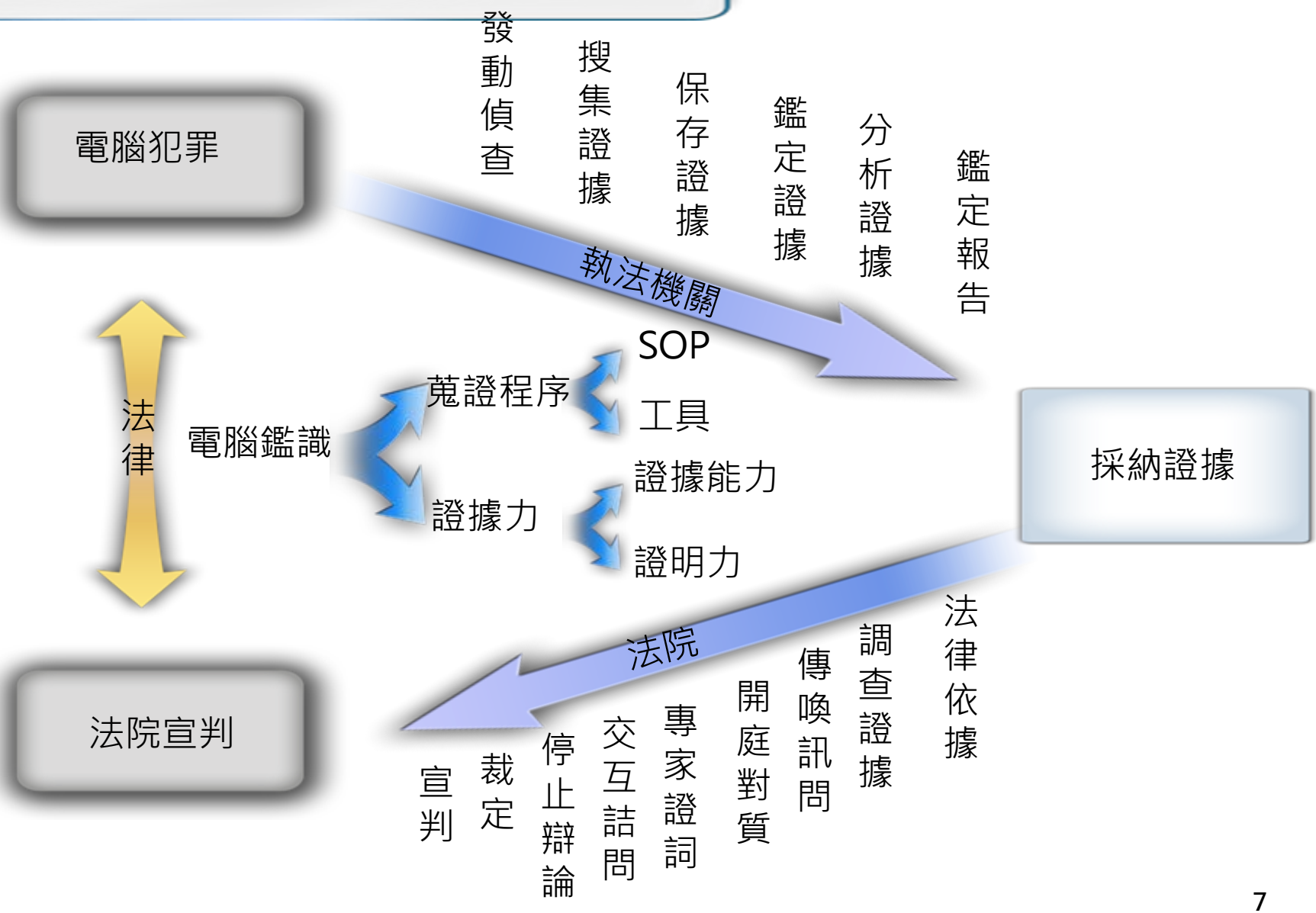


- 以電腦為犯罪場所
  - 侵害著作權—盜版光碟
  - 妨害風化—色情網站
  - 網路賭博—賭博網站

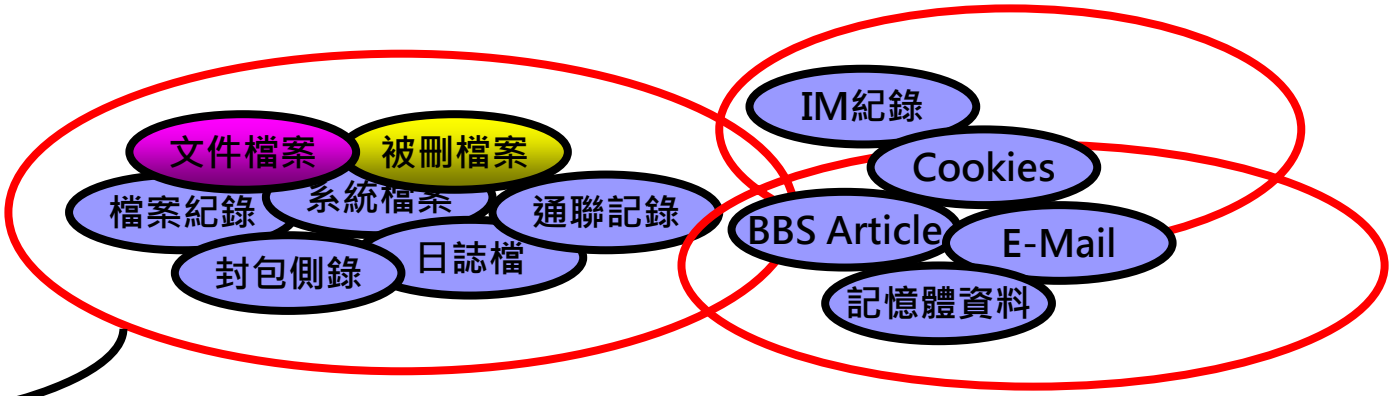


- 以電腦為犯罪標的
  - 入侵主機—竊取資料庫、破壞系統
  - 電腦病毒—破壞電腦、植入後門
  - 盜用帳號—小額付款、遊戲裝備、網路銀行轉帳、下單

電腦犯罪與數位鑑識


電腦犯罪
發動偵查
搜集證據
保存證據
鑑定證據
分析證據
鑑定報告
執法機關
SOP
工具
證據能力
證明力
採納證據
法律依據
調查證據
傳喚訊問
開庭對質
專家證詞
交互詰問
停止辯論
裁定
宣判
法院
法院宣判
法律
電腦鑑識
蒐證程序
證據力

All Data can be Evidence ?



1

可不可以作為證據?

證據能力

1. 是否是經合法之調查程序 ?
2. 是否出於強暴、脅迫、利誘、詐欺、疲勞訊問、違法羈押？
3. 傳聞證據無證據能力。
4. 是否與犯罪事實有關聯性？

2

能夠證明為真實的程度如何？

證明力

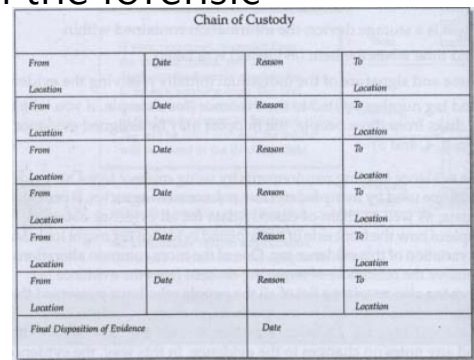
1. 蒐證的證據能提供證明犯罪事實的程度？
2. 足以證明哪些行為？ 證據充分嗎？
3. 影響因子：
   ① 蒐證的方法是否正確？
   ② 蒐證時使用的工具是否經過測試？
   ③ 證據的保存是否完備？有跡可循？

法律小百科：刑事訴訟法第一百五十五條第二項〔無證據能力、未經合法調查之證據，不得作為判斷之依據〕。

數位證物處理

- During adverse civil or criminal proceedings, your collection, handling, and storage of electronic media, paper documents, equipment, and any other physical evidence can be challenged by an adversary.

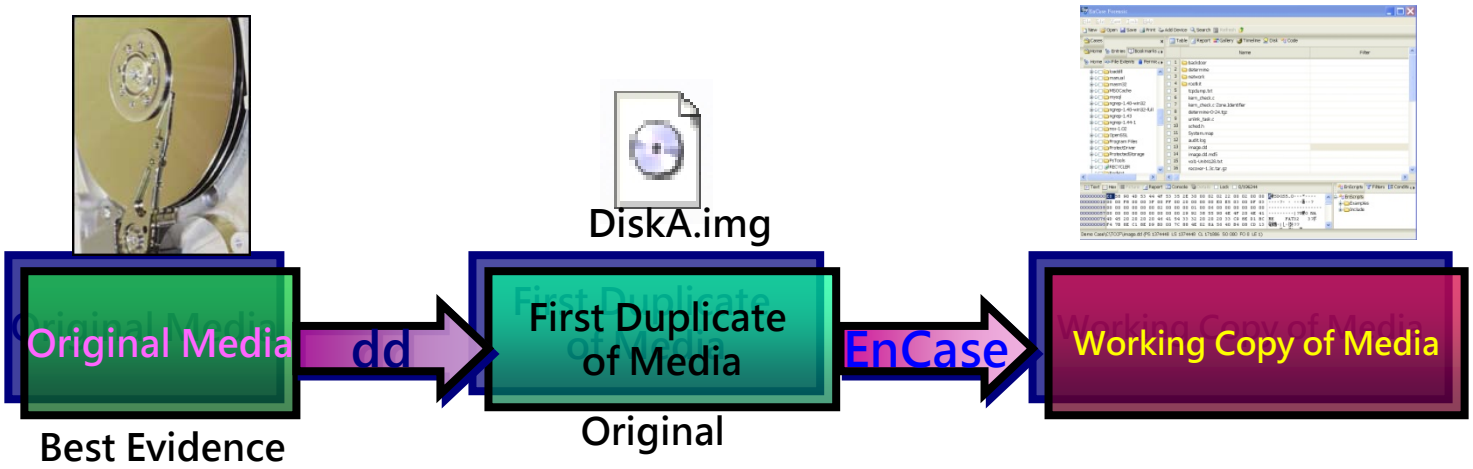
- Authentication
  - Basically means that whomever collected the evidence should testify during direct examination that the information is what the proponent claims.
- Chain of Custody
  - Chain of custody requires that you can trace the location of the evidence from the moment it was collected to the moment it was presented in a judicial proceeding.
- Evidence Validation
  - The data you collected is identical to the data that you present in court.
  - Ensuring MD5 hashes of the original media match those of the forensic duplication.


Chain of Custody

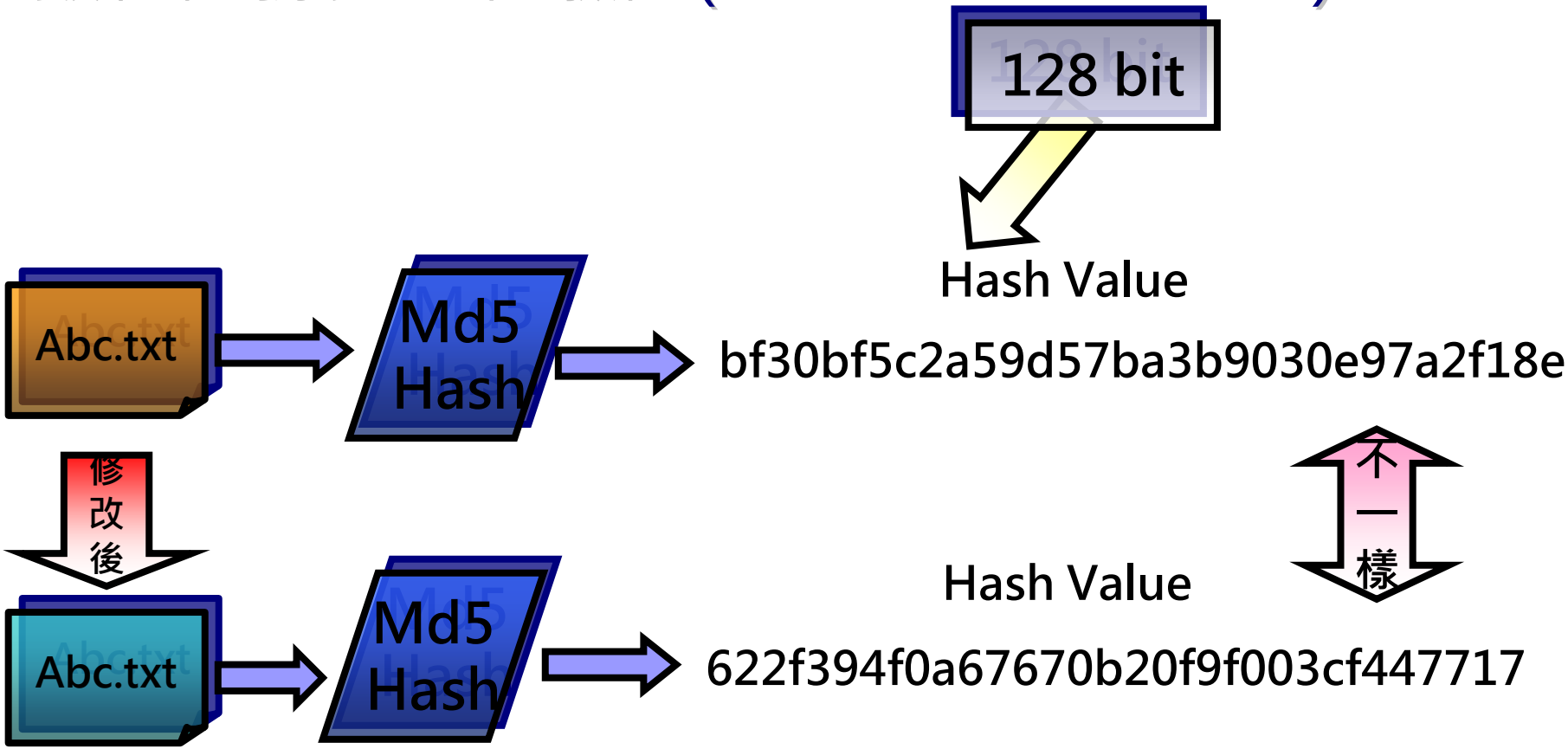
From Location	Date	Reason	To Location
From Location	Date	Reason	To Location
From Location	Date	Reason	To Location
From Location	Date	Reason	To Location
From Location	Date	Reason	To Location
From Location	Date	Reason	To Location
Final Disposition of Evidence		Date	

最佳證據法則

- 以美國的最佳證據法則(FER 1002)而言，其定義何謂原始證據(或稱最佳證據)，在法院審理時要求檢方必須提出原始證據，另外副本的證據能力(FER 1003)則規範副本的來源必須是要從原始證據獲得，而經由原始證據產生的副本其法律效力與原始證據相同。因此，鑑識人員得以使用副本進行解析，但必須能夠證明副本是由原始證據產生，如何能證明副本和原始證據是一致的呢？

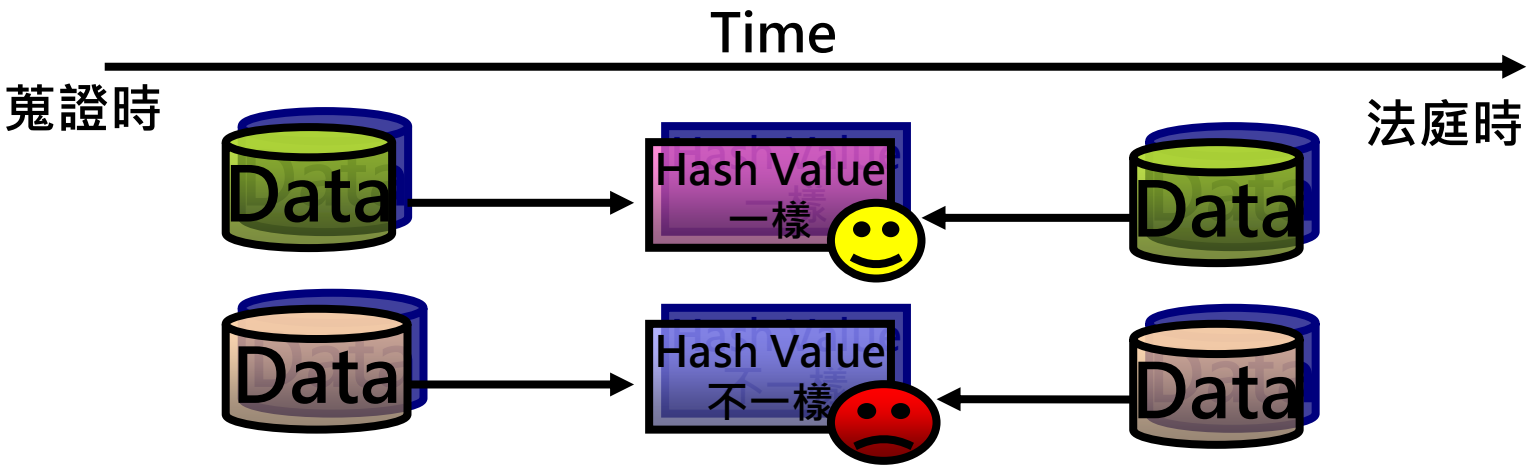


數位證據完整性驗證(Evidence Validation)



數位證據完整性驗證(Evidence Validation)

- 數位證據蒐證時必須對所蒐集到的資料做完整性驗證並記錄Hash值於相關表單中。
- 在法院時如對交付之證據有疑議時，可以對原始資料做一次完整性驗證，如果Hash值與蒐證時所記錄的數值一樣的話表示數位證據從蒐證到法院的期間並未受到任何修改。



電腦鑑識實驗室

- 電腦鑑識案件種類：
  - 刑案現場搜索與扣押
  - 硬碟資料復原與解析
  - 惡意程式分析與鑑識
  - 手機資料存取與解讀
  - 網路封包監察與解析
  - 駭客入侵偵查與追蹤

刑案現場搜索與扣押





- 搜索前
  - 調查人員事前必須擬定搜索計畫，做好萬全的準備。
  - 準備相關扣押設備，如:扣押物清單、證物標籤、證物袋(箱)、麥克筆與攝影機等。
  - 準備電腦鑑識開機光碟、工具箱、網路線、電源延長線、網路集線器、隨身碟等。
- 搜索中
  - 電腦狀態為關機？或開機？如在關機狀態不可開啟電腦電源；如在開機狀態必須詢問現場專家意見，是否需要進行Live Forensic，勿逕行關閉電源。
  - 手持式裝置狀態為關機？或開機？如在關機狀態不可開啟電源如在開機狀態不可關閉電源，並注意是否需補充電池電量。
  - 標示、照相及攝影現場所有設備與處裡之人員。
  - 仔細尋找任何可攜式裝置(如：PDA、手機)、儲存媒體(MS、MMC、SD記憶卡、磁碟片、隨身碟)等。

Ps.有關LiveForensic可參閱2007.10資安人雜誌—漫談電腦鑑識流程與技術

刑案現場搜索與扣押(count.)

- 留意電腦四周各種文件，並注意其所記載之資訊(如:帳號、密碼等)
- 搜齊特殊設備所需之周邊元件，以免多次搜索。
- 標示證物之原始狀態，何處取得？誰取得？為何取得等資訊。
- 標示設備之連接線順序、插孔位置、型號等
- 所有證物必須予以拍照、並黏貼證物標籤。
- 記錄所有搜索過程與動作。

搜索後

- 迅速將所蒐證物運送至安全存放地點，等待進一步鑑定。
- 維持證物保管鏈之完整性，所有經手人皆需詳細記載與簽名。



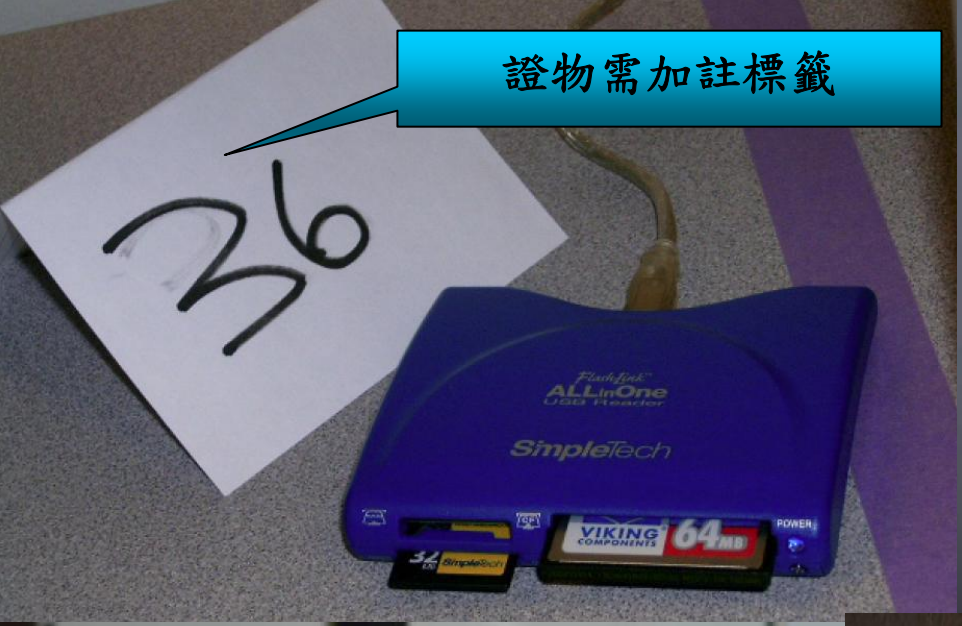


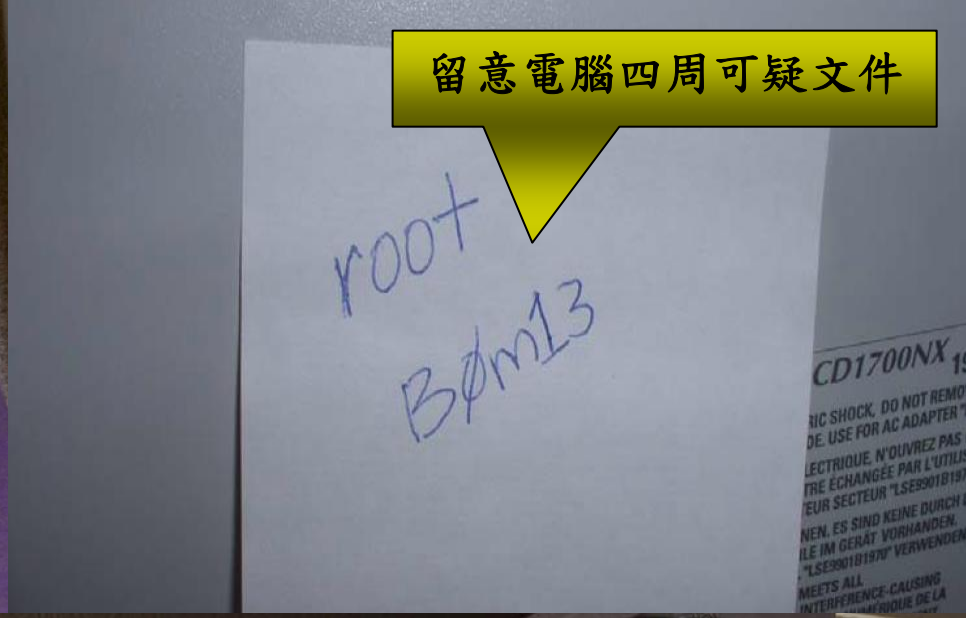
現場應予全部拍照

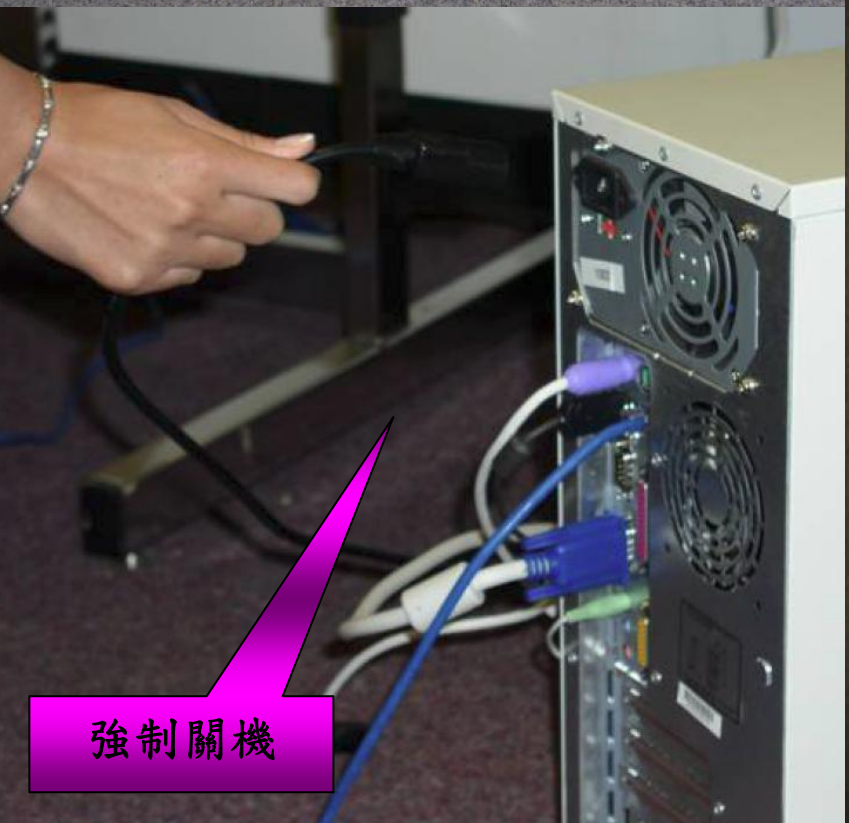

NEC
SNICKERS
現場電腦狀態應予拍照

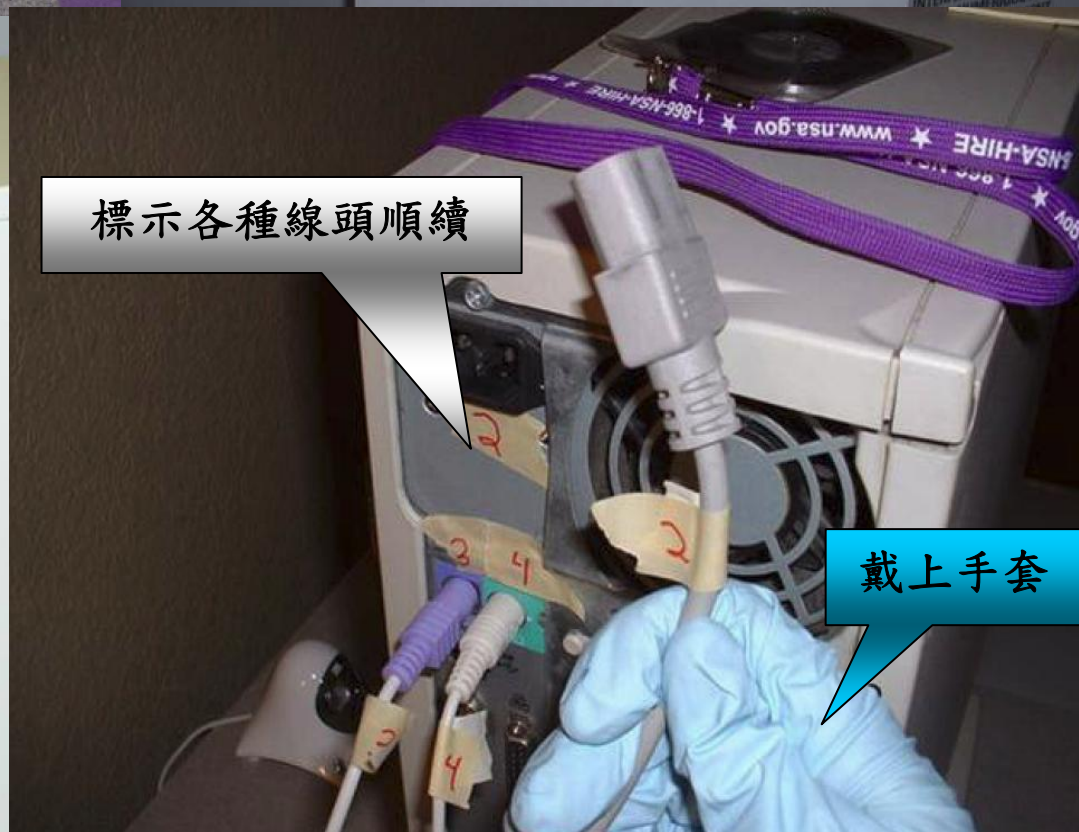

留意所有可能放置空間


現場應予全部拍照


證物需加註標籤
36
SimpleTech
VIKING
64MB


留意電腦四周可疑文件
root
Bøm13

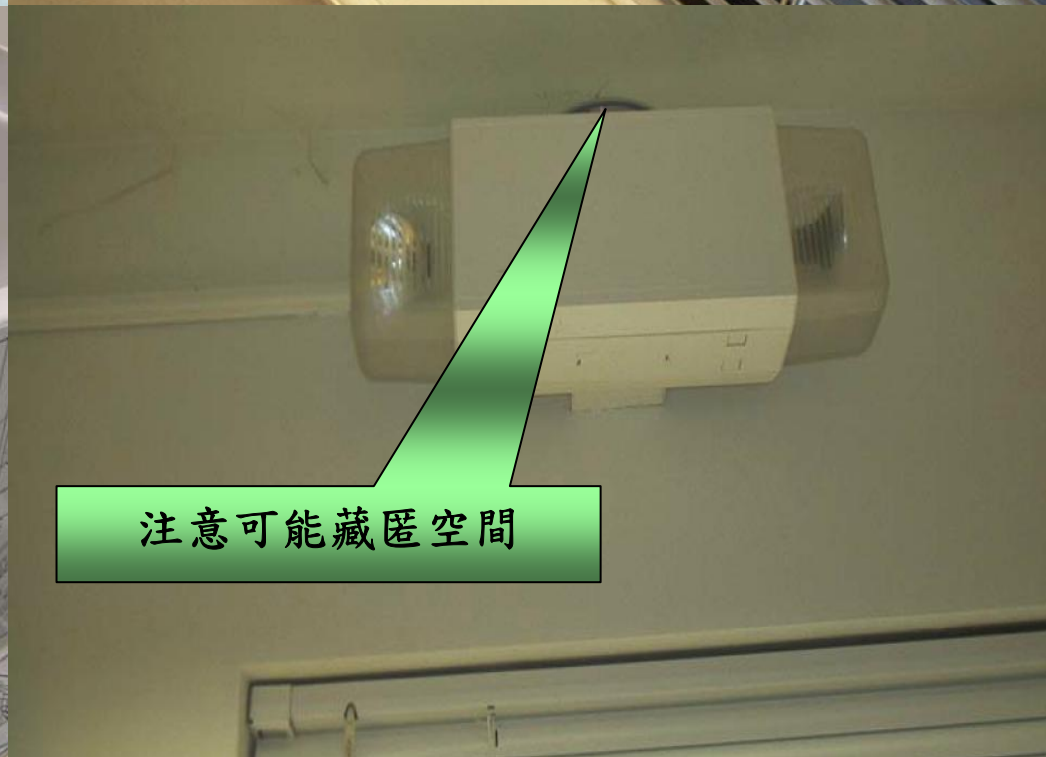

強制關機

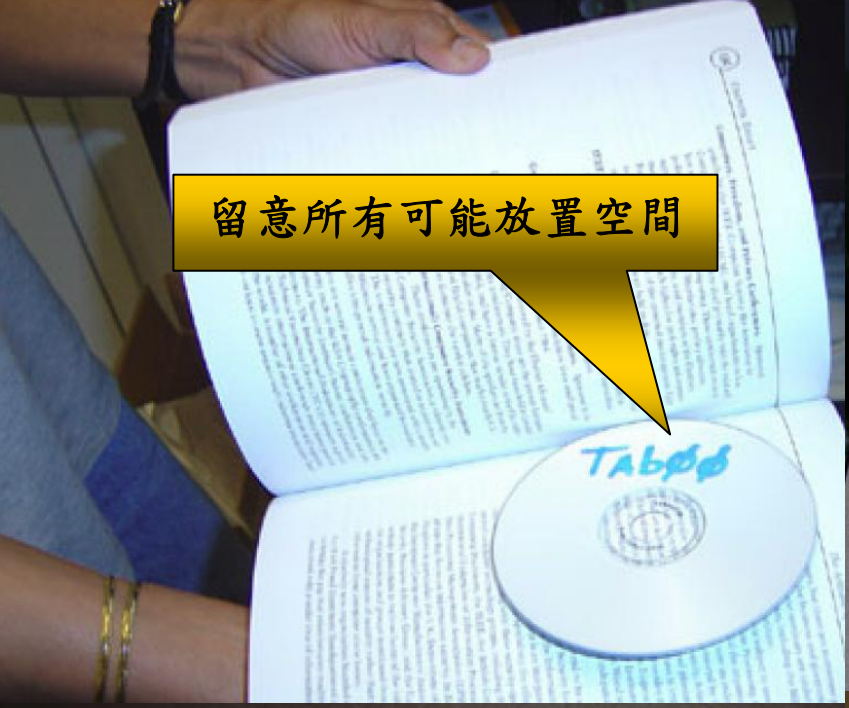

標示各種線頭順續
戴上手套

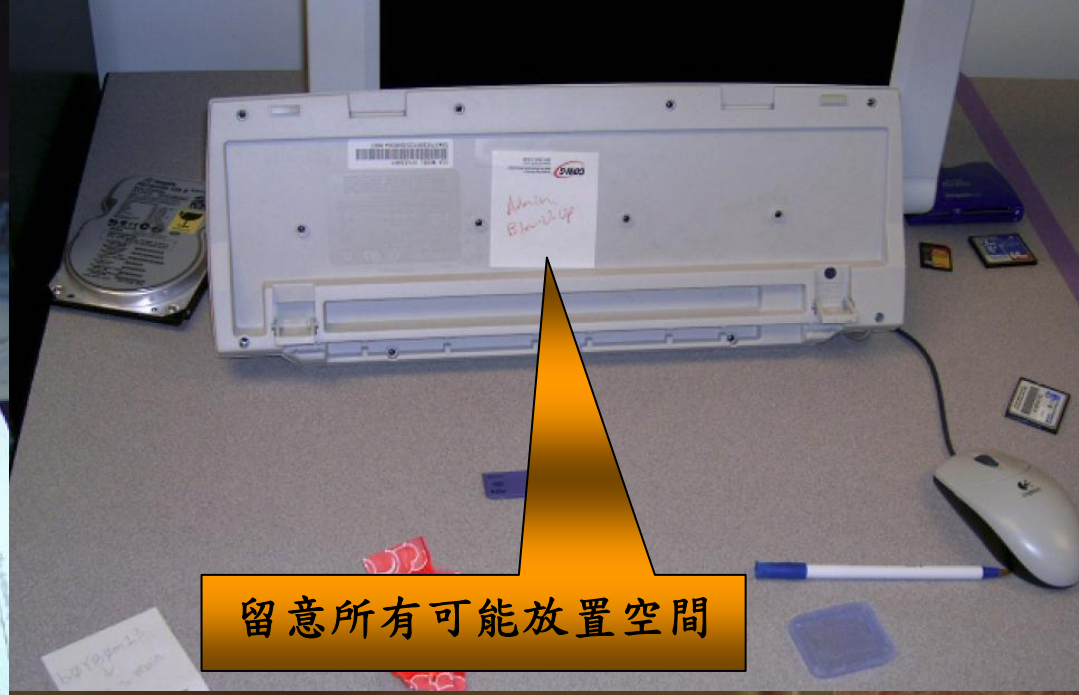

Verbatim
DataLife
DC 2120
留意所有可能放置空間


仔細尋找各種儲存媒體


YELLOW
129.244.241.248
留意電腦四周可疑文件

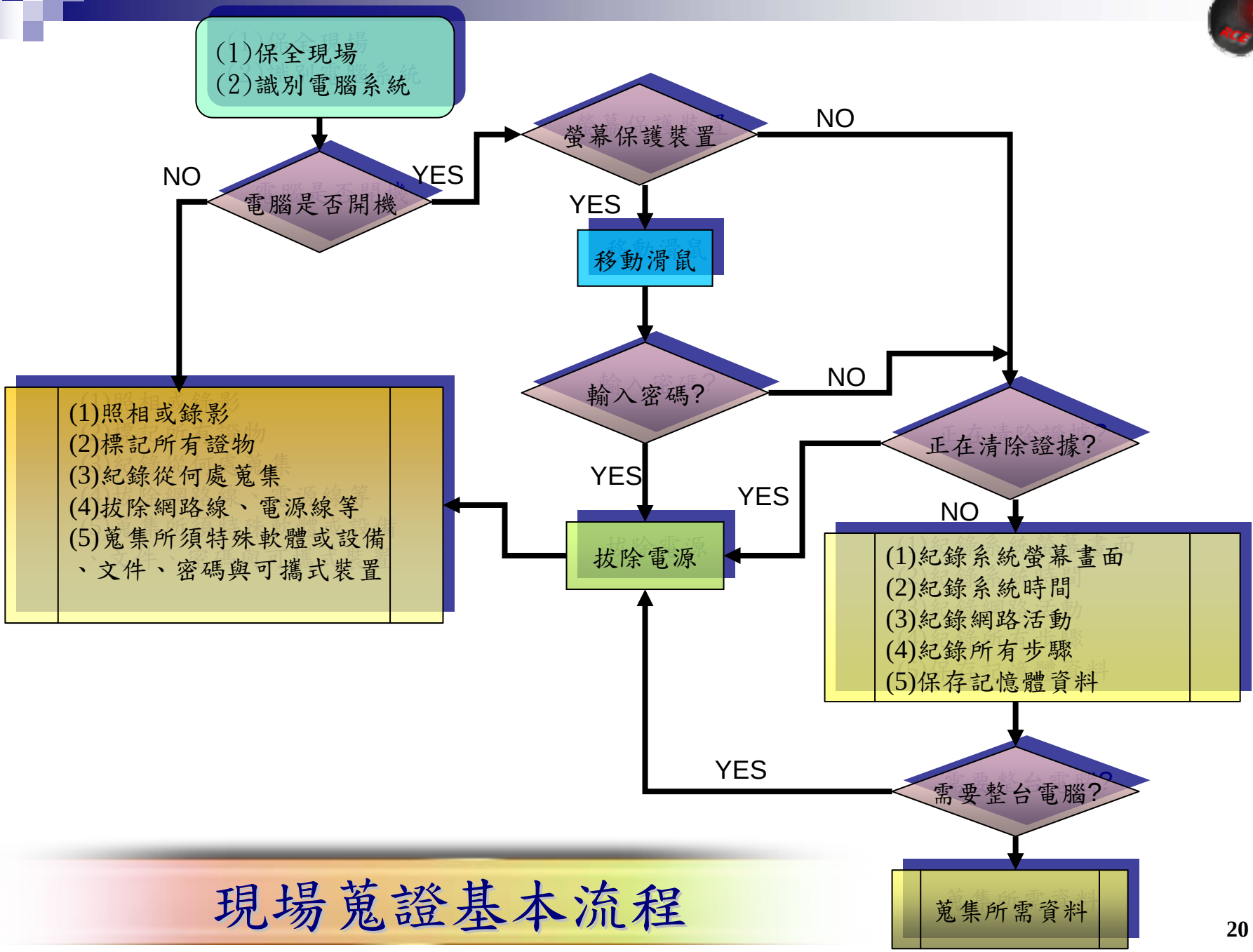

注意可能藏匿空間


留意所有可能放置空間


留意所有可能放置空間


留意所有可能放置空間


仔細尋找各種儲存媒體

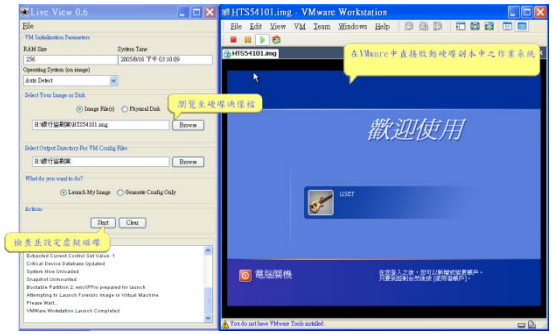

(1)保全現場
(2)識別電腦系統
螢幕保護裝置
NO
YES
電腦是否開機
NO
YES
移動滑鼠
輸入密碼?
NO
正在清除證據?
YES
YES
NO
(1)照相或錄影
(2)標記所有證物
(3)紀錄從何處蒐集
(4)拔除網路線、電源線等
(5)蒐集所須特殊軟體或設備、文件、密碼與可攜式裝置
拔除電源
(1)紀錄系統螢幕畫面
(2)紀錄系統時間
(3)紀錄網路活動
(4)紀錄所有步驟
(5)保存記憶體資料
YES
需要整台電腦?
蒐集所需資料

現場蒐證基本流程

硬碟資料復原與解析

- 製作硬碟副本
  - 為維護電腦系統的持續運作，硬碟無法帶離現場，或需要鑑定硬碟資料，且不可修改或破壞原始硬碟資料時。
  - dd、dcfldd、encase、ftk imager、 Forensic Talon

- 硬碟鑑識分析
  - 將映像檔載入鑑識軟體分析->EnCase、FTK
  - 將映像檔掛載成一個或多個虛擬磁碟機->Mount Image Pro
  - 利用VMware軟體掛載成虛擬磁碟並啟動作業系統->LiveView
- 常遇到的挑戰
  - Encrypted File System
  - Steganographic(資訊影藏)
  - Partition table、FAT、MFT損毀
  - RAID 故障或設定錯誤



Ps.有關Forensic Analysis可參閱補充資料，「漫談電腦鑑識流程與技術」一文

惡意程式分析與鑑識

- 實體硬碟分析→LiveView啟動後檢查是否感染惡意程式
  - 自動化行為分析->NPASCAN
  - 檢查系統可疑物件->Autoruns、ProcessExplorer、IceSword
  - 系統網路連線狀況檢查->Ethereal 、Wireshark
- 惡意程式樣本分析→分析惡意程式行為與目的
  - 沙箱測試法->Norman Sandbox、Winalysis
  - 惡意程式行為剖繪-> API Hooking Technique
  - 惡意程式逆向工程->OllyDbg
- 常遇到的挑戰
  - 惡意程式加猛殼
  - 反虛擬機器技術
  - 系統存在Rootkit程式

手機資料存取與解讀

- 非智慧型手機
  - 非開放式作業系統，手機有甚麼功能就用甚麼功能
  - 使用者不可以自行安裝應用程式
- 智慧型手機

  - 開放式作業系統
    - Palm OS ->Treo
    - BlackBerry OS-> BlackBerry
    - Pocket PC / Windows Mobile (Microsoft)
    - Embedded Linux ->OpenMoko Neo 1973
    - Symbian / EPOC ->Nokia 、Sony Ericsson 、Motorola
    - iOS ->IPOD、IPHONE、IPAD

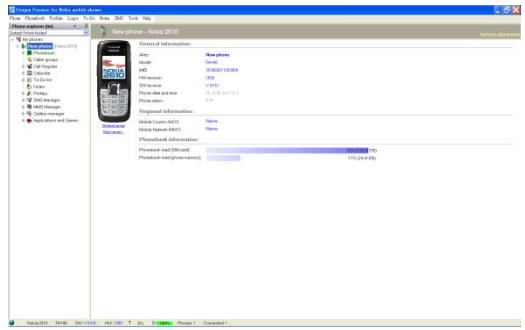
  - 使用者可以自行安裝應用程式

手機資料存取與解讀(cont’ d)

- 手機內會有甚麼資料？
  - 手機電話簿中之聯絡人
  - 已接、未接來電
  - 手機模式(標準、靜音、會議等)
  - 行事曆
  - 影像
  - 簡訊
  - 聲音
  - 其他資訊(IMEI、系統程式)
- SIM卡內會有甚麼資料？
  - SIM卡連絡人
  - 簡訊
  - 其他資訊(IMSI)

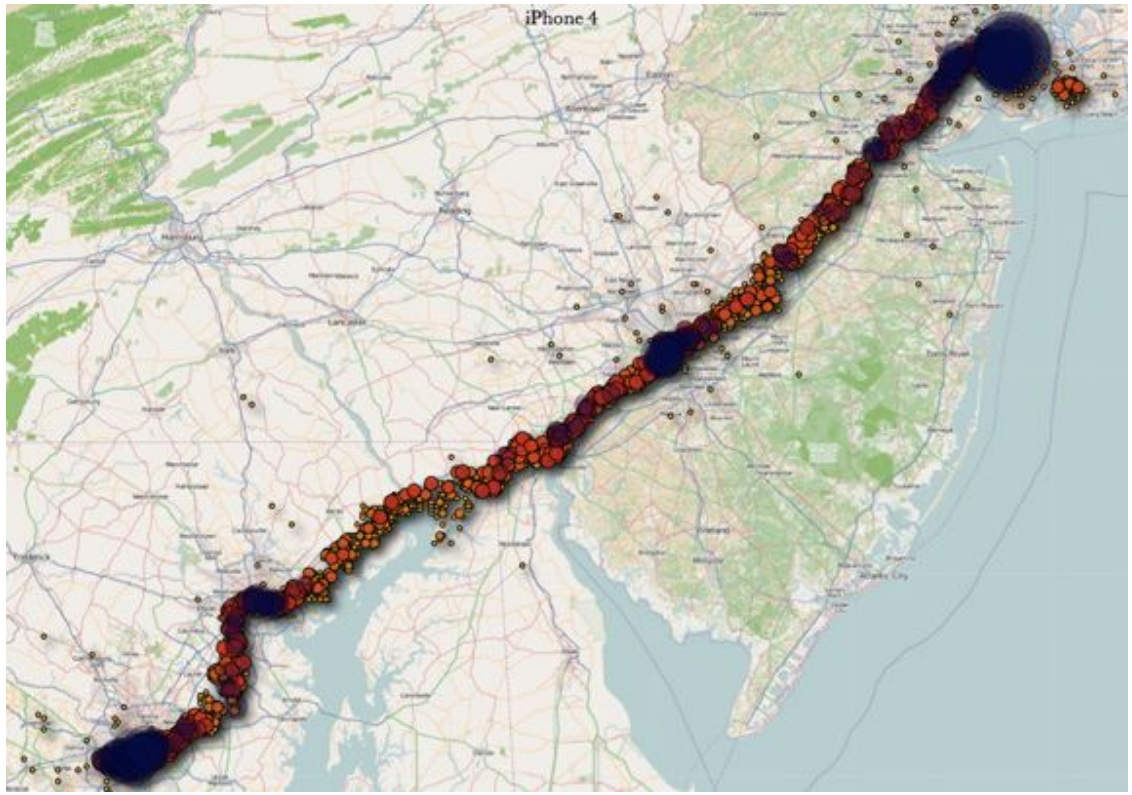
手機資料存取與解讀(cont’d)

- 手機資料蒐集
  - 選擇一種的連接方式(Cable 、Bluetooth、IrDA)
  - 針對裝置選擇鑑識軟體
    - 非智慧型手機
      - Oxygen Forensic for Nokia phones
      - MOBILedit!
    - 智慧型手機
      - Windows CE、Palm系列
        - Paraben For PDA(Data Acquisition)
      - Symbian系列
        - Oxygen Forensic for Symbian OS
      - iOS-ramdisk (Elcomsoft)
      - Andriod- Dalvik VM
  - 可攜式行動裝置鑑識設備
    - CellDEK (Software implement)
    - CellDEK TEK (Hardware implement)
    - CellBrite



IPhone Tracker

- Library/Caches/locationd/consolidated.db
- SELECT * FROM CellLocation;", @"SELECT * FROM WifiLocation;



駭客入侵偵查與追蹤

- 入侵網站或個人電腦
  - 盜取個人資料(網銀、線上遊戲、Yahoo 、無名帳密等)
  - 受委託網路徵信
  - 首頁置換炫耀
  - 網頁掛馬
  - 作為跳板主機
- 入侵方式
  - 針對網站
    - XSS
    - SQL Injection
    - Cookie Spoofing
    - File Inclusion
  - 針對個人
    - 綑綁木馬、下載者程式、USB Worm四處散播
    - 目標式攻擊(利用Office、Acrobat PDF、WinRAR、Realplayer等弱點)

電腦鑑識光碟介紹與使用

常用電腦鑑識軟體

- Non-Commercial based Solution
  - Unix-Based
    - Live Collecton
      - Trusted System Command (ps、lsof、netstat.,etc.)
      - chkrootkit、rkhunter
    - Forensic Duplication
      - dcfl-dd
    - Network Collection
      - Tcpdump
      - Ethereal、Ettercap
      - tcpxtract、foremost
  - Windows-Based
    - Live Collection
      - Forensic Acquisition Utilities (dd、md5sum.,etc.)
      - netcat
      - Sysinternals (PsXXX)
      - PTFinder
      - Windows Forensic Toolchest (WFT)
    - Forensic Duplication
      - DD
      - Network Evidence Duplicator(NED)
      - Ftk Imager
    - Network Collection
      - Ethereal 、ettercap
      - windump
- Commercial based Solution
  - EnCase
  - SafeBack
  - Access Data FTK
  - X-Ways Forensics
  - Paraben P2

Incident Response & Computer Forensics Live CD
http://www.e-fense.com/helix/

Forensic and Incident Response Environment
http://fire.dmzs.com/?section=main

The Sleuth Kit & Autopsy Browser
http://www.sleuthkit.org/

Forensic Toolkit
http://www.accessdata.com/

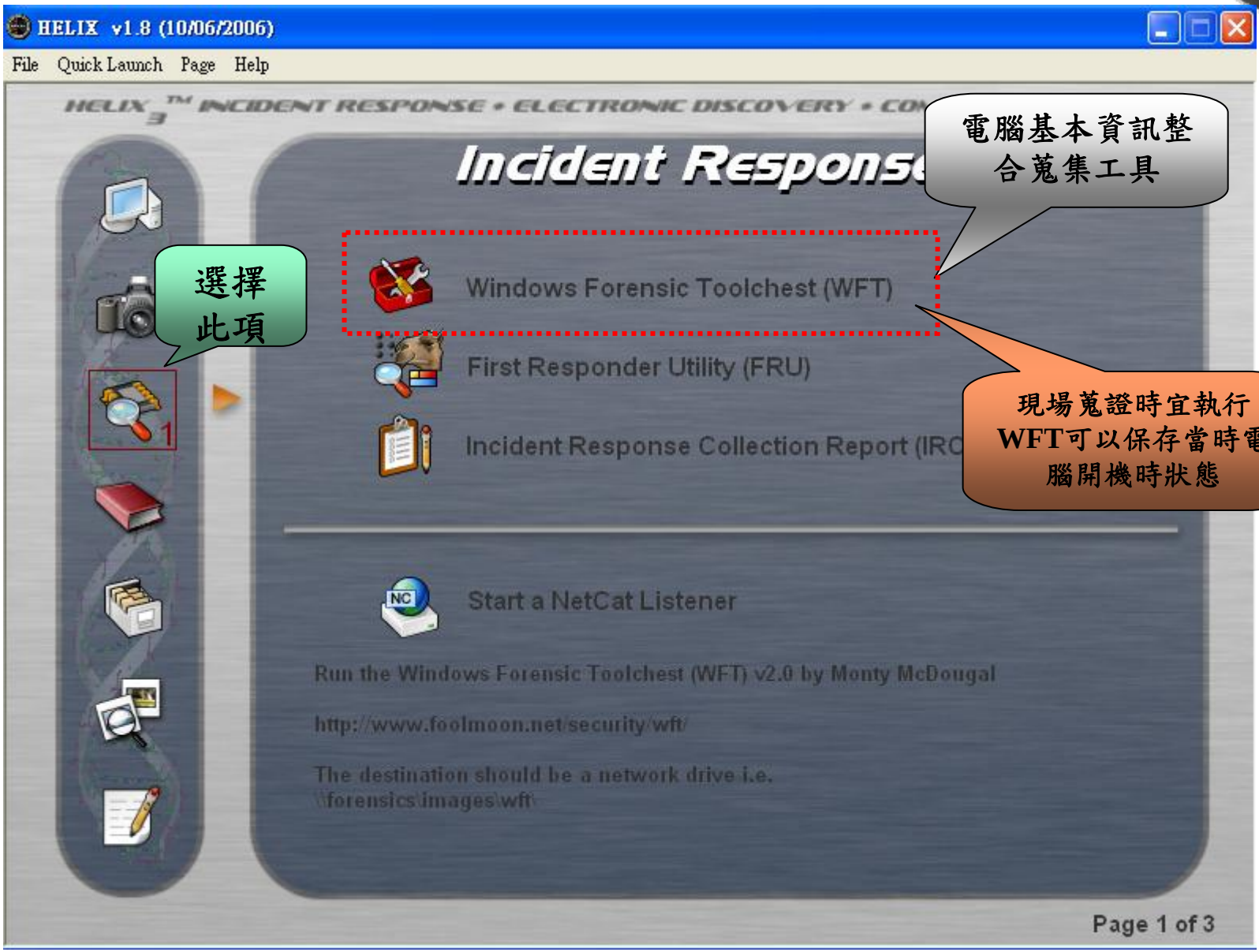
EnCase
http://www.guidancesoftware.com/

http://www.paraben-forensics.com

X-Ways forensics
http://www.x-ways.net/

鑑識光碟介紹

- Helix是一片多功能的開機光碟(LiveCD)，集成網路上各式各樣好用的免費Windows與Unix鑑識工具，他可以在網路下載燒錄成CD後使用，目前版本為2008R1版:
  - 2008 R1
    - http://distrowatch.com/?newsid=05102
  - 2007
    - http://ftp.ntua.gr/pub/linux/helix/Helix_V1.9-07-13a-2007.iso
- Chntpw是一種可以離線修改windows開機密碼的小工具，如果win2k~Win7等作業系統有設定開機密碼的時候可以用他來重設密碼，他可以在網路下載燒錄成CD後開機使用:
  - http://pogostick.net/~pnh/ntpasswd/cd100627.zip


HELIX v1.8 (10/06/2006)
File Quick Launch Page Help
INCIDENT RESPONSE • ELECTRONIC DISCOVERY
Incident Response
電腦基本資訊整合蒐集工具
選擇此項
Windows Forensic Toolchest (WFT)
First Responder Utility (FRU)
Incident Response Collection Report (IRC
現場蒐證時宜執行WFT可以保存當時電腦開機時狀態
Start a NetCat Listener
Run the Windows Forensic Toolchest (WFT) v2.0 by Monty McDougal
http://www.foolmoon.net/security/wft/
The destination should be a network drive i.e.
\\forensics\images\wft
Page 1 of 3


HELIX v1.8 (10/06/2006)
File
Quick Launch
Page
Help
System
Acquire
Incident Response
Documentation
Browse
Image Scanner
Volatile Tools
Misc Tools
Password Tools
選擇密碼工具
Outlook密碼獲取工具
MSN密碼獲取工具
E-Mail密碼獲取工具
IE歷史紀錄獲取工具
Cookie紀錄獲取工具
PST Password Viewer
Messenger Password
Protected Storage Viewer
IE History Viewer
IE Cookie Viewer
Mail Password Viewer
Network Password
Asterisk Logger
Mozilla Cookie Viewer
Registry Viewer
Mail密碼獲取工具
網路密碼查看器
星號密碼查看器
Mozilla Cookie查看器
登錄檔查看器
Page 3 of 3

電腦鑑識實例探討

File Carving

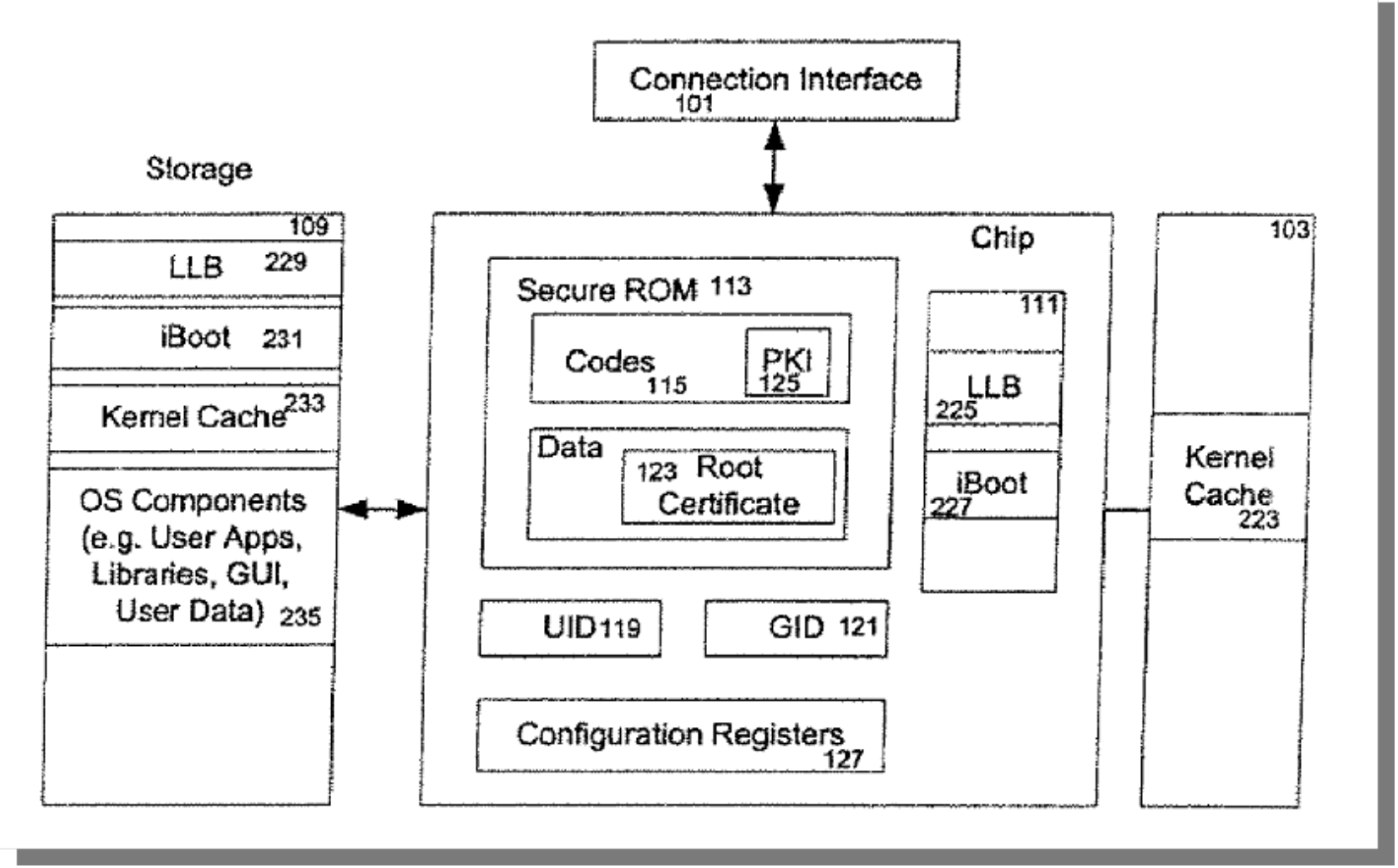
- File Carving, or sometimes simply Carving, is the practice of searching an input for files or other kinds of objects based on content, rather than on metadata. File carving is a powerful tool for recovering files and fragments of files when directory entries are corrupt or missing, as may be the case with old files that have been deleted or when performing an analysis on damaged media.
- Memory carving is a useful tool for analyzing physical and virtual memory dumps when the memory structures are unknown or have been overwritten.

File Carving Tool- Foremost or scalpel

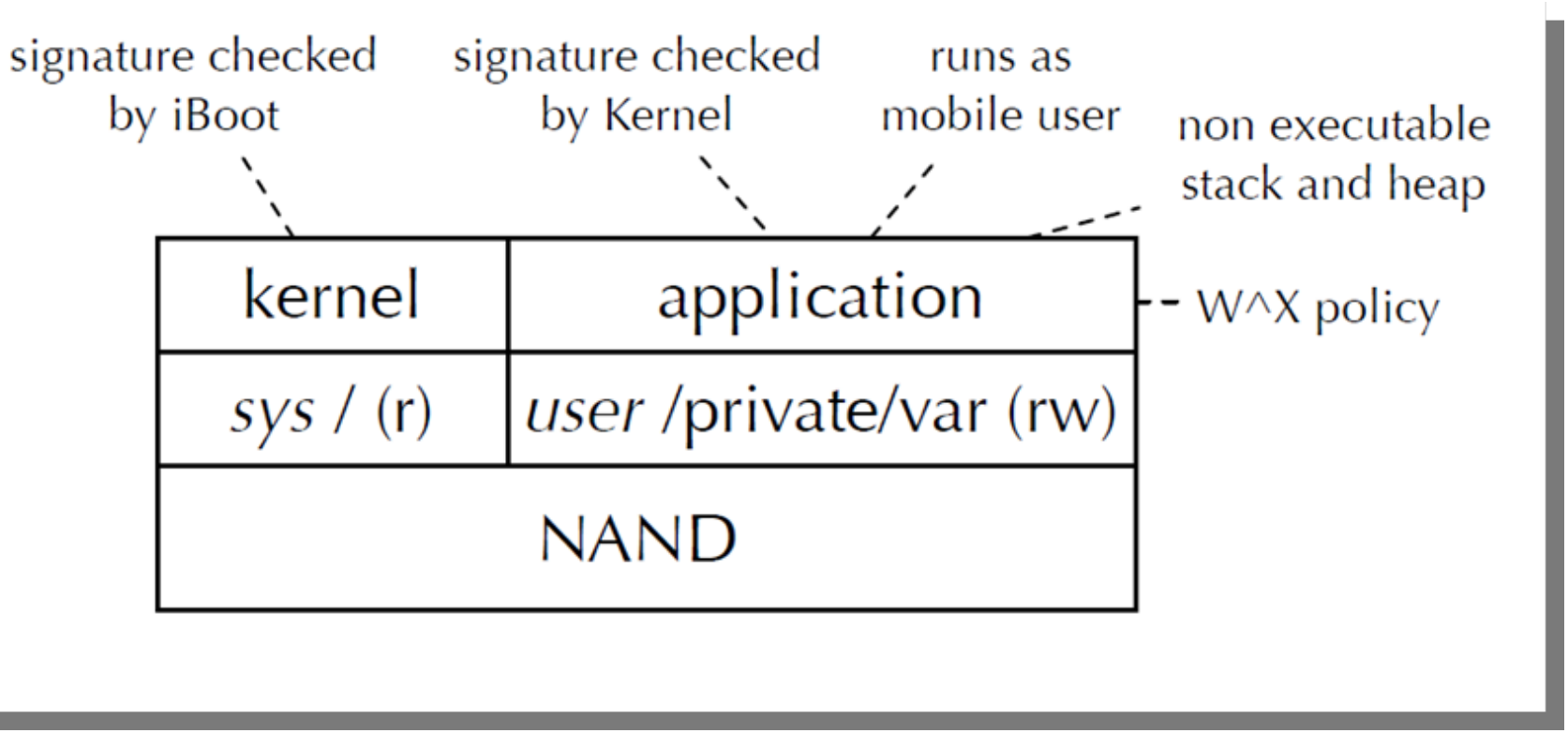
- Foremost is a console program to recover files based on their headers, footers, and internal data structures. This process is commonly referred to as data carving.
- Foremost can work on image files, such as those generated by dd, Safeback, Encase, etc, or directly on a drive.
- The headers and footers can be specified by a configuration file or you can use command line switches to specify built-in file types.
- These built-in types look at the data structures of a given file format allowing for a more reliable and faster recovery.

IPhone forensics via physical acquisition

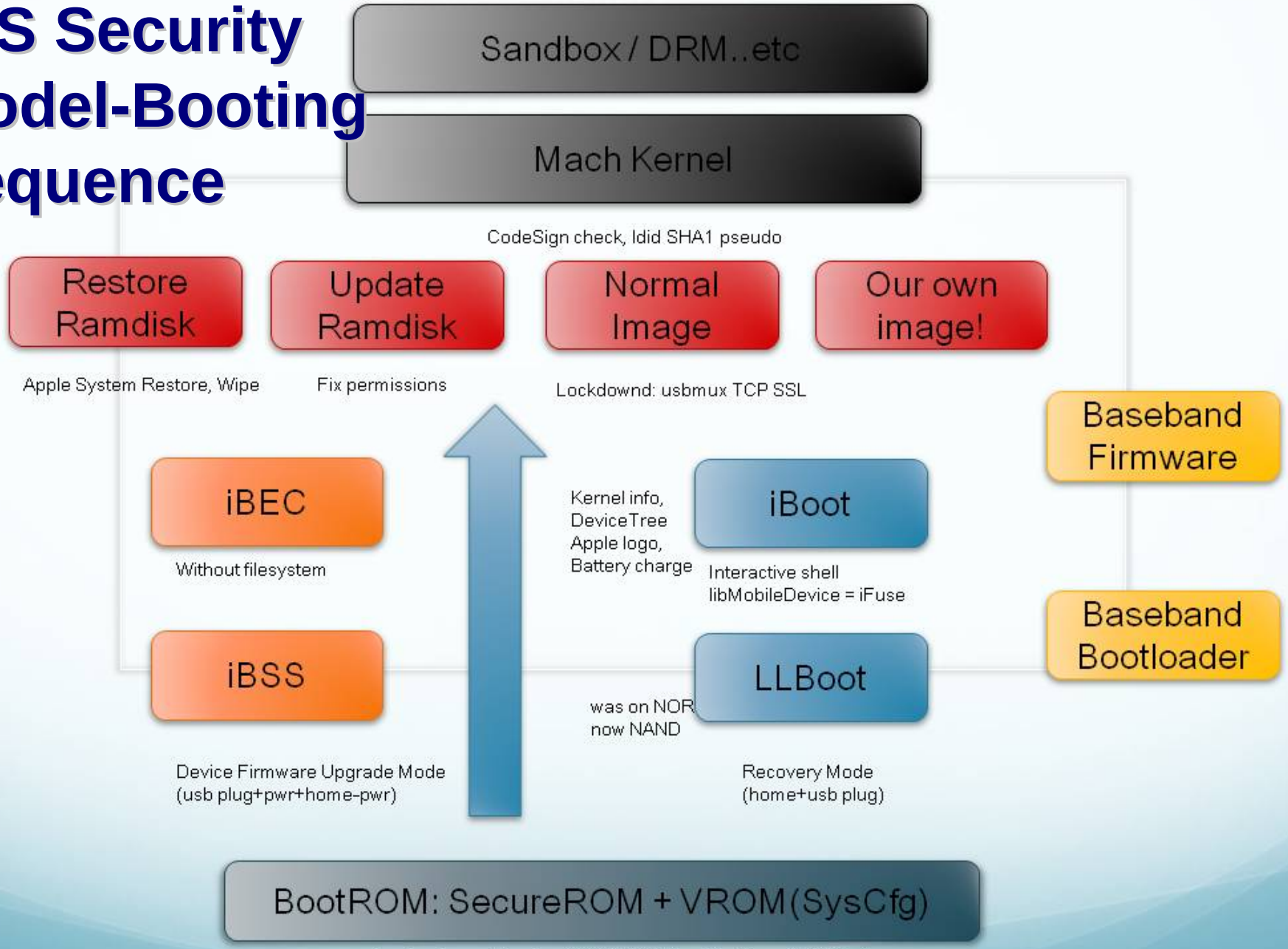
iOS Security Model(1/2)



iOS Security Model-Sandbox(Seatbelt)



iOS Security Model-Booting Sequence



Tethered vs. Untethered


DFU Mode
ReCovery Mode
iPhoneIndiaBlog.com

IPhone Forensics

- logical forensics
  - Itunes backup (IPhoneBackupExtractor)
    - %APPDATA%/Apple Computer/MobileSync/Backup/<udid>
    - Encrypted (AES-256 CBC)
    - Filenames : SHA1 hashes
- Physical forensics
  - Forensics Ram disk(custom)
    - Use exploit to disable signature checks
    - Blackra1n iBoot exploit (firmware ! 3.1.2)
    - Pwnage 2 BootROM exploit on older devices (iPhone ! 3G)
    - Limera1n/greenpoison BootROM exploit on newer devices (iPhone 4)
    - Load our own ramdisk with extraction tool (iOS 4 data protection)

Booting SSH ramdisk (IPhone 3G)

- Getting into fake FDU mode and boot
  - itunnel_mux.exe --ibec iBEC.n82ap.RELEASE.dfu --ramdisk 038-0029-002.dmg.ssh --devicetree DeviceTree.n82ap.img3 --kernelcache kernelcache.release.n82
- Setting SSH tunnel via USB
  - itunnel_mux.exe --lport 22 (alpine)
- Mount Partitions
  - mount /
  - mount_hfs /dev/disk0s1 /mnt1
    - fsck_hfs /dev/disk0s1
  - mount_hfs /dev/disk0s2 /mnt2
- Setting environment variable
  - export PATH=$PATH:/mnt1/bin:/mnt1/sbin:/mnt2/stash/bin:
  - export DYLD_LIBRARY_PATH=/mnt1/usr/lib

電腦鑑識的挑戰

- 儲存容量倍數成長，鑑識人員工作吃重。
- 資訊隱藏技術成熟，工具更是隨手可得。
- 犯罪證據備援於國外機房或利用VPN連線，造成偵查與蒐證的困難。
- 資料復原觀念普及，犯罪者多使用安全的檔案清除工具。
- 檔案系統加密技術之使用，硬碟分區之解密增加鑑識難度。
- 智慧型手機的價位趨於大眾接受，桌上型電腦的應用快速轉移至手機上，手機鑑識將成為主流。

Q/A

If you have any questions, please contact me at

pk@npa.gov.tw
peikan@gmail.com