電腦與手機鑑識 - 根基於數位證據 (ISO/IEC DIS 27037:2011)

楊中皇
中華民國資訊安全學會常務理事
國立高雄師範大學資訊教育研究所教授
http://security.nknu.edu.tw/

2012年第1季資訊安全管理系統標準化系列討論會(2012年1月11日)

大綱

1. 數位鑑識
2. 電腦鑑識
3. 手機鑑識

研究動機

- 與電腦及網路相關的犯罪與訴訟案件增多
  - 2005年UBS Warburg銀行因性別歧視(gender discrimination)被罰US$29.3M
  - 2010年個人資料保護法(個資法)
- 電腦與手機等數位設備存放隱私資料
- 商業鑑識軟體價格昂貴且多為英文界面
- 開放原始碼鑑識工具不易使用
- 國科會研究計畫
  - 數位鑑識分析平台之技術研發與建置(2009/08 – 2012/07)
  - 雲端運算數位鑑識系統之技術研發與建置(2011/10 – 2012/07)
  - 15位以上畢業碩士, 30篇以上國內外研討會論文

鑑識(Forensics)

- 狄仁傑(630 - 700)，唐朝宰相(大理寺丞)
- 宋慈(1186 – 1249)，法醫學之父
- CSI犯罪現場 (Crime Scene Investigation)
- 刑事鑑識專家李昌鈺(Henry Lee)博士，
  http://www.drhenrylee.com/

資訊安全研究領域(國科會分類)

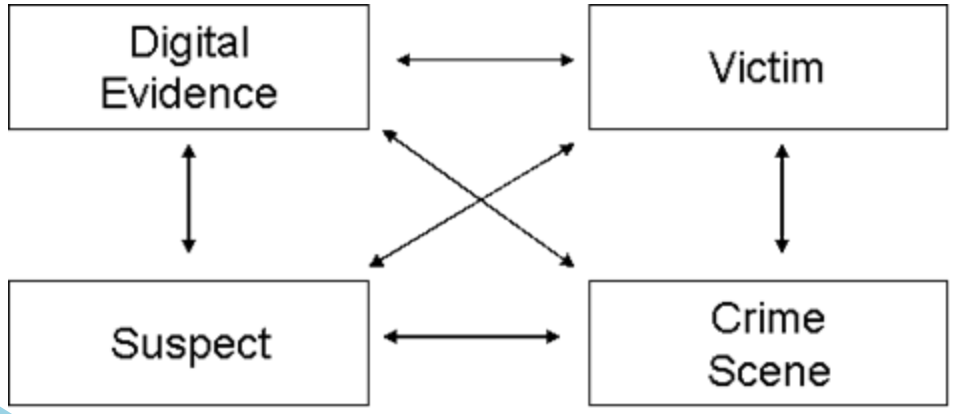
- E08180001-對稱金鑰密碼學 (如私密金鑰密碼系統、串流密碼系統、隨機數列、雜湊函數等)
- E08180002-公開金鑰密碼學 (如公開金鑰密碼系統、橢圓曲線密碼系統、多變量密碼系統、雙線性函數密碼系統、電子簽章等)
- E08180003-密碼分析 (如密碼系統分析、雜湊函數分析等)
- E08180004-密碼演算法
- E08180005-編碼理論 (如代數編碼理論、消息理論、改錯碼等)
- E08180006-量子密碼學 (如量子資訊、量子金鑰分配、量子密碼協定等)
- E08180007-密碼協定 (如身分認證、資料鑑定、智慧卡安全、生物測定、金鑰分配、公開金鑰基礎建設、多方安全計算、模糊傳輸、機密共享等)
- E08180008-密碼系統應用 (如廣播加密、屬性加密、密文可搜尋式加密、電子錢幣、電子投票、電子拍賣、電子付款、電子商務、電子政府、電子病歷、雲端計算安全、隱私保護、位址服務隱私保護等)
- E08180009-系統安全 (如存取控制、資訊流控制、作業系統安全、弱點分析與滲透測試、信賴計算、資料庫安全、安全軟體工程、實體安全、側通道分析等)
- E08180010-網路安全 (如入侵偵測與防禦、惡意程式碼偵測、無線網路安全、行動網路安全、感測網路安全、網頁安全、電子信件安全)
- E08180011-數位版權保護及管理 (如軟體保護、資料隱藏、浮水印、公平交換等)
- E08180012-資訊安全管理 (如資訊安全政策、風險分析、資訊安全標準,守則,準則、內部控制監視與稽核等)
- **E08180013-數位犯罪鑑識 (如數位證據取得,保存、數位鑑識流程、鑑識軟體與硬體等)**

數位證據 (Digital Evidence)

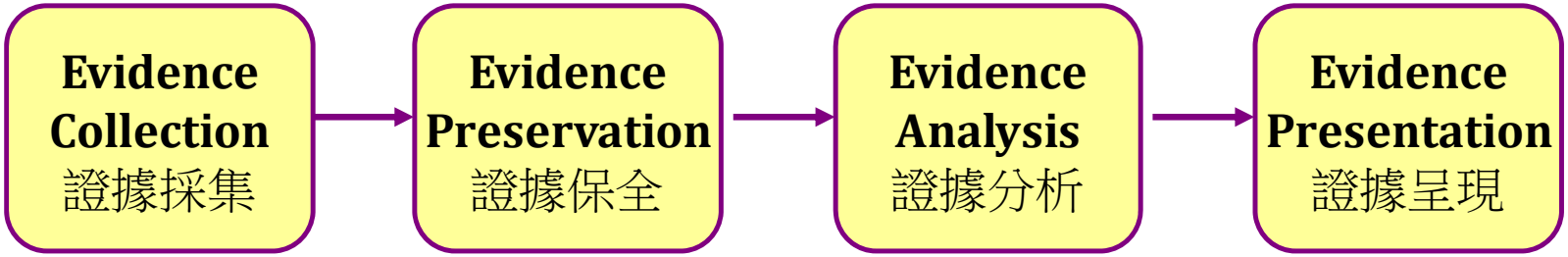
- probative information stored or transmitted in digital form that a party to a court case may use at trial (Casey 2004)
- ISO/IEC DIS 27037: Guidelines for identification, collection and/or acquisition and preservation of digital evidence
- 證據來源
  - 桌上型電腦與筆記型電腦
  - 手機、個人數位助理(PDA)
  - 可攜式媒體: CD/DVD, USB disk, tape
  - 伺服器: email, instant messaging, database, VoIP
  - Third parties: Google Docs, blog, facebook

數位鑑識 (Digital Forensics)

- 以科學的方式採集、保存、分析及呈現數位證據
- 可幫助回答電腦與網路案件相關的時間(when)、內容(what)、相關人員(who)、地點(where)、目的(why)、如何發生(how)
- 記憶體鑑識、電腦鑑識、網路鑑識、手機鑑識
- Four-Way Linkage Theory [Henry Lee's crime scene handbook, 2001]



數位鑑識流程



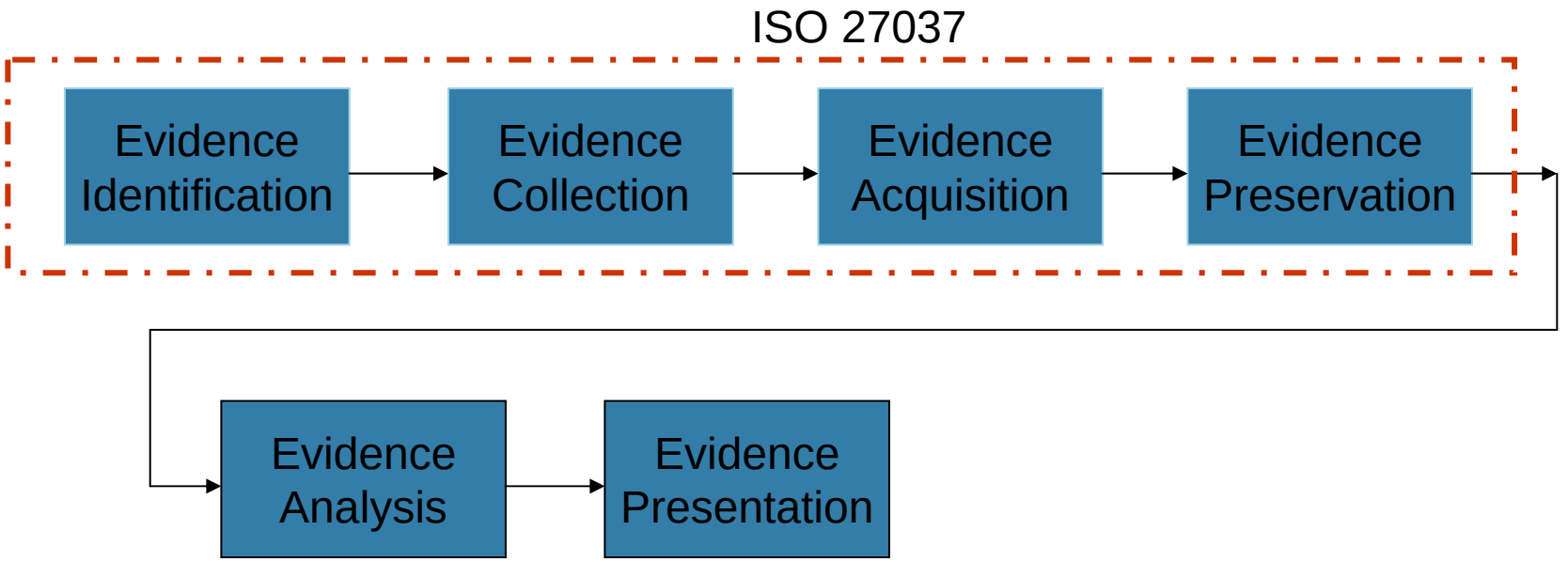
- 證據採集（Evidence Collection/Acquisition）：
  - 電腦與手機的記憶體(RAM)、磁碟機、快閃式記憶體(flash)及其他傳輸媒體與數位媒體。
- 證據保全（Evidence Preservation）：
  - 將證據以可靠與可驗證的方式保存，使用密碼學的單向雜湊函數(one-way hash function)。
- 證據分析（Evidence Analysis）：
  - 例如Skype/MSN/QQ即時通訊內容、電子郵件、手機的簡訊與通聯記錄，GPS定位資料、相機照片隱藏的時間與地點資料、微軟公司Office文件內藏的作者姓名與修改日期等。
- 證據呈現（Evidence Presentation）：
  - 提出鑑識分析後的數位證據，也包含說明文件。

數位鑑識相關法律與規範

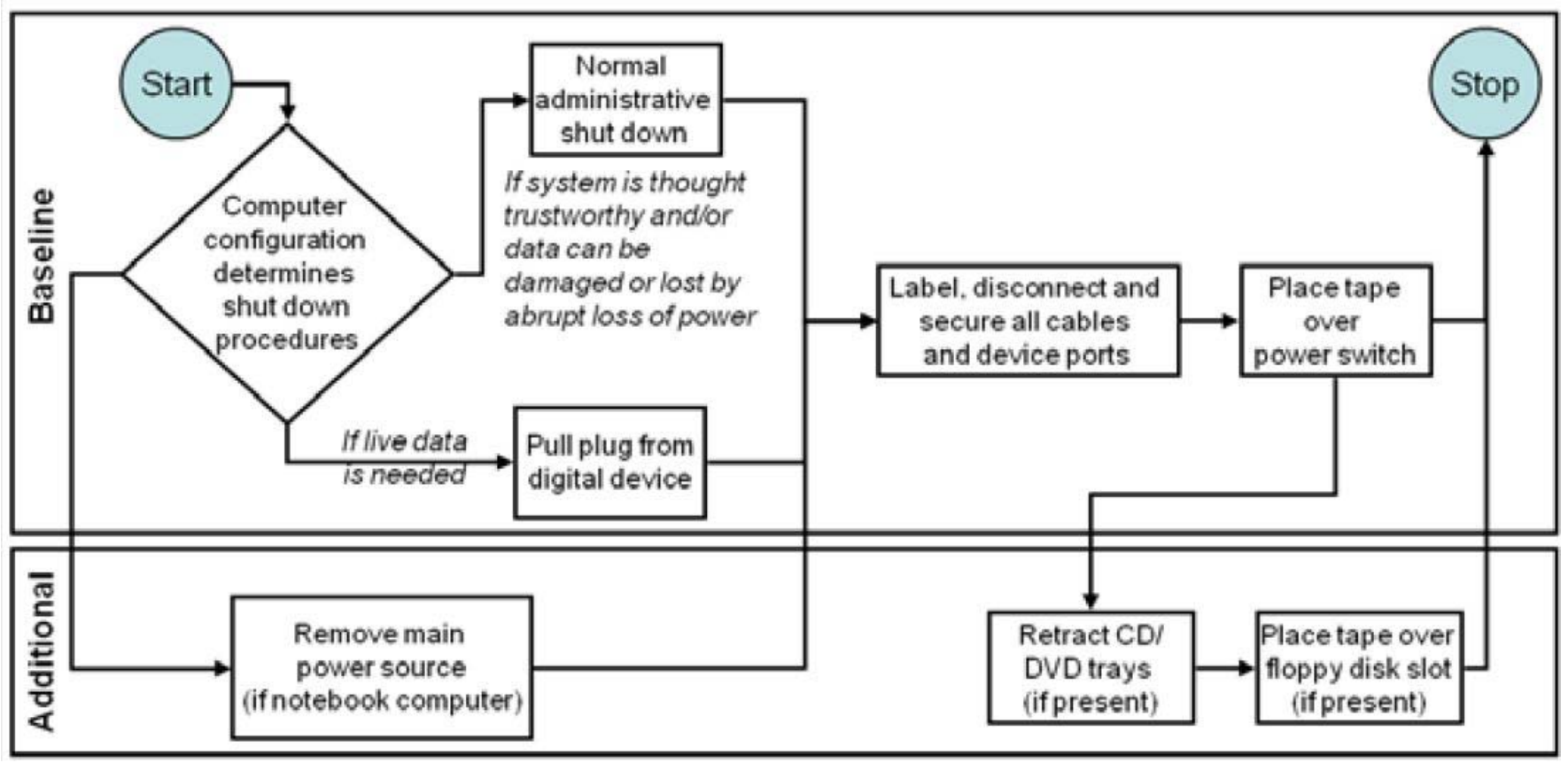
- Canada's Uniform Electronic Evidence Act (1998)
- USA's Uniform Rules of Evidence (1999)
- California Electronic Discovery Act (2009)
- China: (2009)
  - 電子物證數據搜索檢驗技術規範
  - 電子物證文件一致性檢驗技術規範
  - 電子物證軟體一致性檢驗技術規範
  - 電子物證軟體功能檢驗技術規範
- ISO/IEC 27037, Guidelines for identification, collection, acquisition and preservation of digital evidence (Draft International Standard).

ISO/IEC 27037

ISO/IEC 27037 (DIS): Guidelines for identification, collection, acquisition and preservation of digital evidence

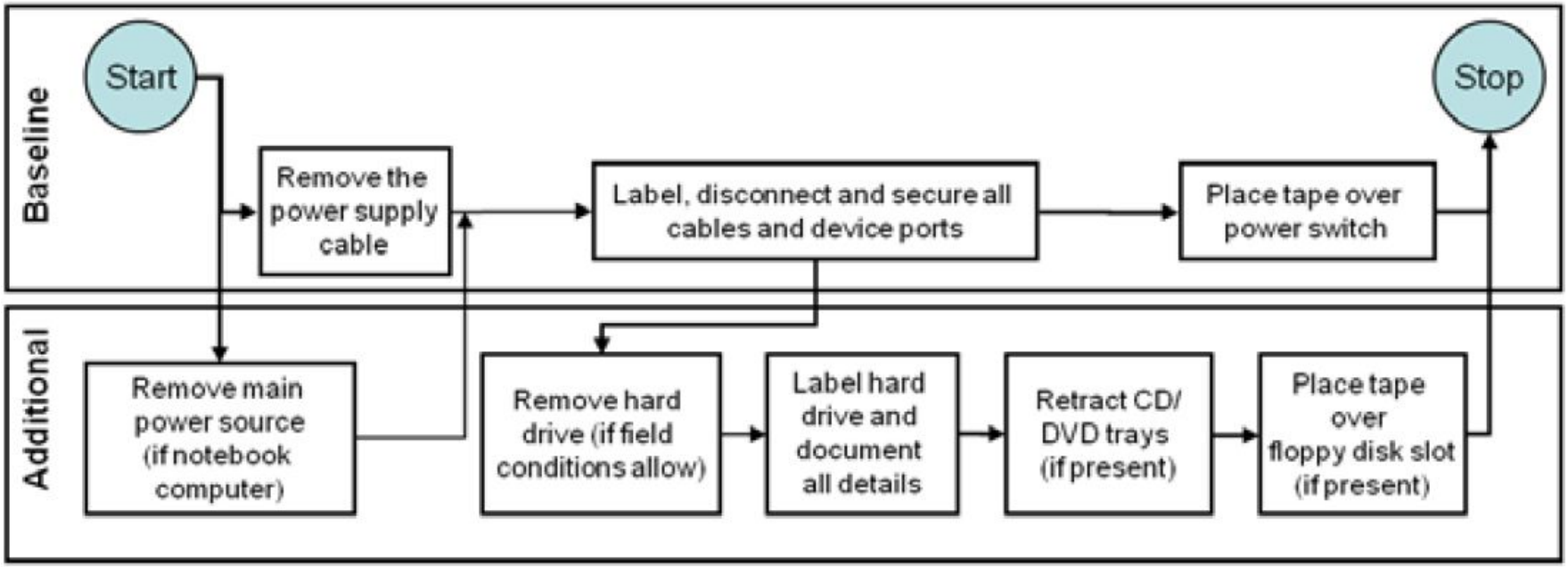


Evidence collection of powered-on device



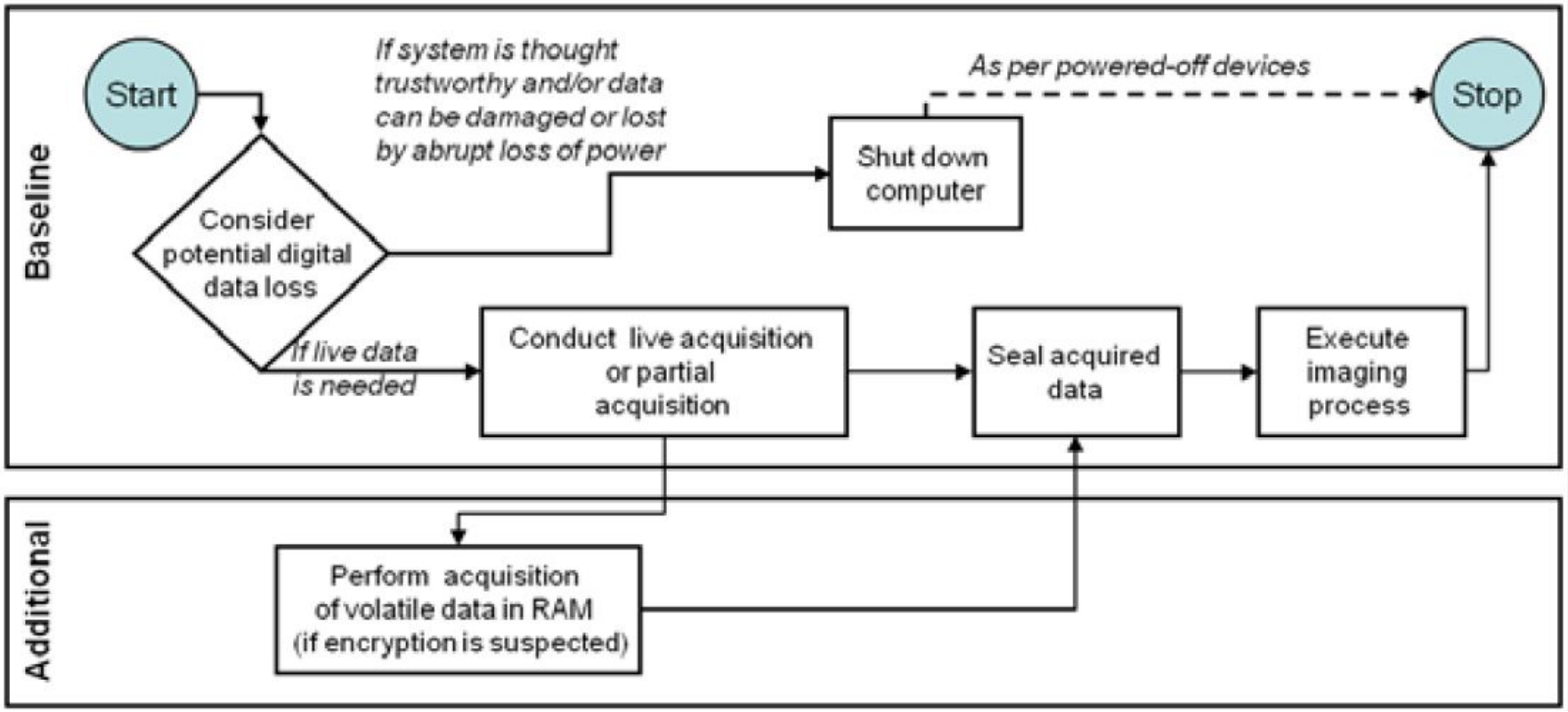
資料來源：ISO/IEC 27037

Evidence collection of powered-off device



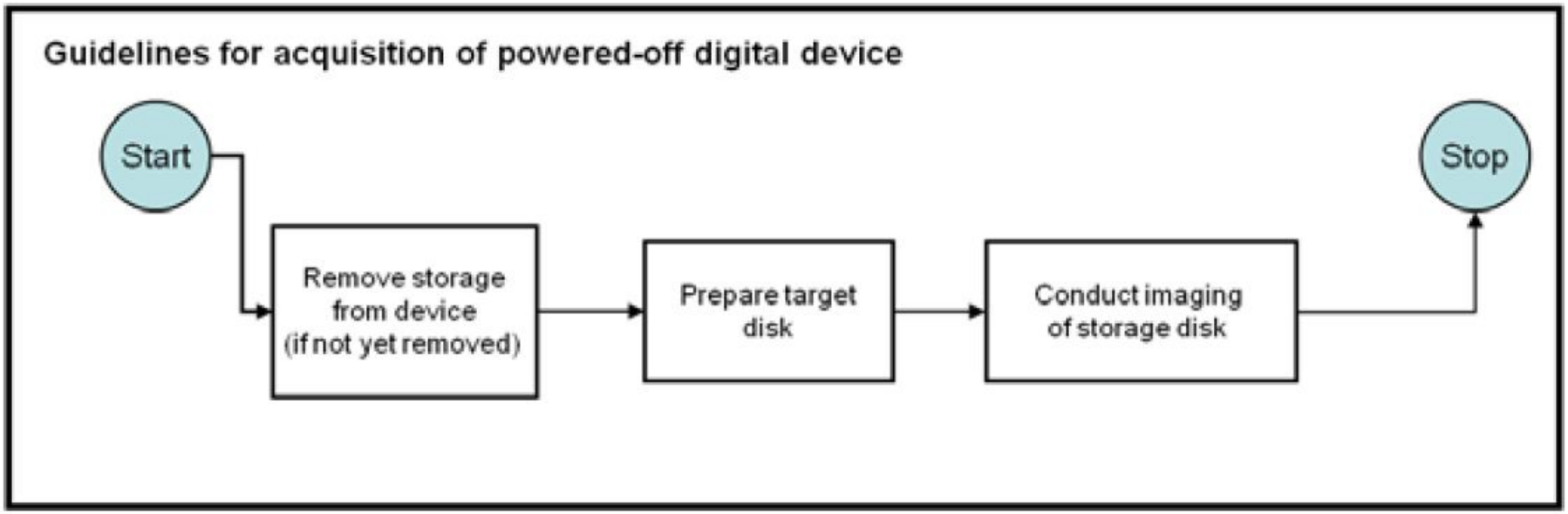
資料來源：ISO/IEC 27037

Evidence acquisition of powered-on device



資料來源：ISO/IEC 27037

Evidence acquisition of powered-off device



資料來源：ISO/IEC 27037

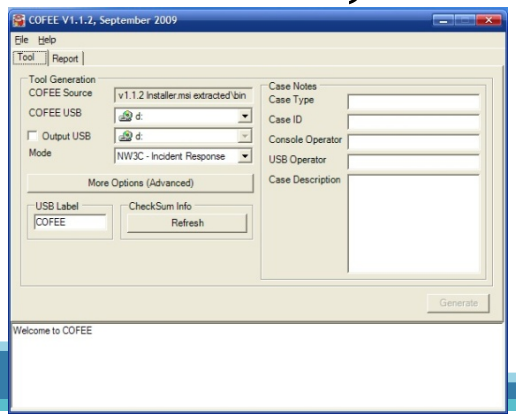
電腦關機後，自RAM復原密鑰

- http://citp.princeton.edu/research/memory/

- information in RAMs will persist from several seconds to a minute
- attacks against several disk encryption systems: BitLocker, FileVault, dm-crypt, and TrueCrypt

COFEE

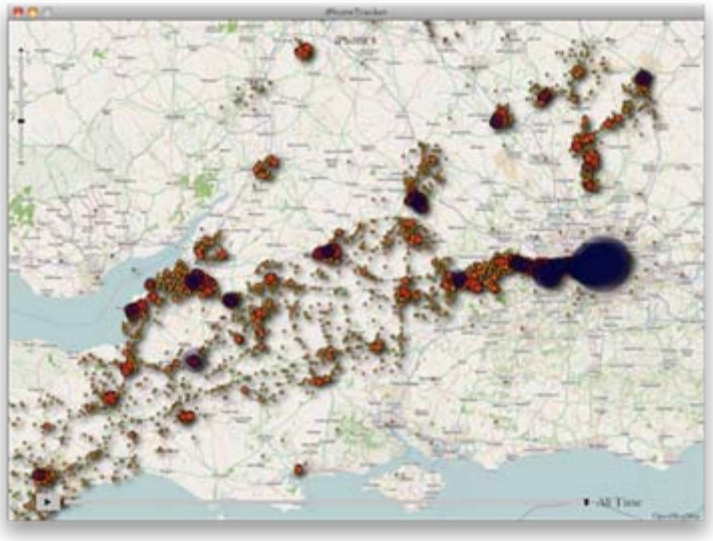
- Computer Online Forensic Evidence Extractor (COFEE),http://www.microsoft.com/industry/government/solutions/cofee/
- 微軟公司免費提供給國際刑警組織成員
- To collect volatile live evidence, such as active system processes and network data
- Installed on a USB flash drive or other external disk drive, over 150 software commands



- Windows Sysinternals, http://technet.microsoft.com/zh-tw/sysinternals/

iPhone/Android記錄隱私資料

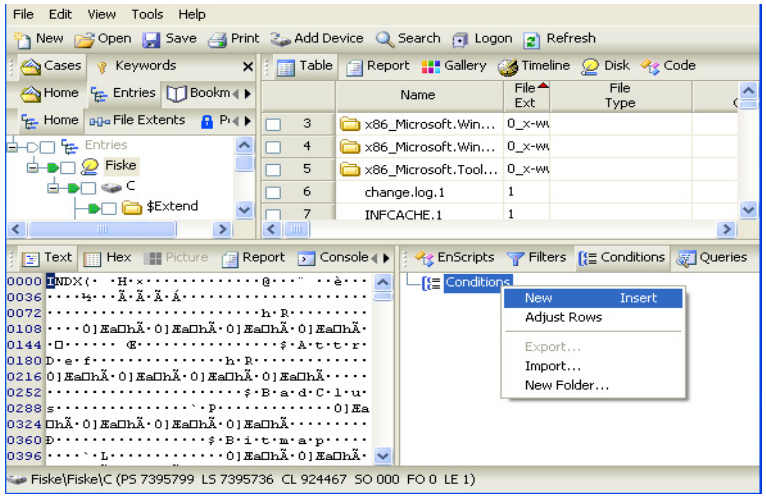
- iPhone Tracker
- Android Location Cache
- Carrier IQ



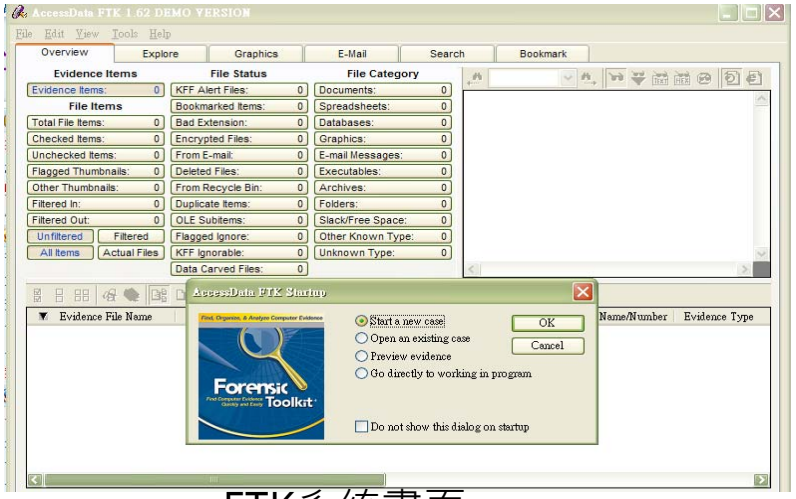
電腦鑑識
(Computer Forensics)

商業電腦鑑識系統

- **EnCase**是由Guidance software公司推出,因其功能完整、圖形化之介面,且該公司提供鑑識之訓練課程,目前為美國最多執法機構所採用的軟體。
  - http://www.guidancesoftware.com/
- **Forensic Tool Kit (FTK)**為Access Data公司之電腦鑑識軟體,直覺式的操作介面很適合開始接觸電腦鑑識的人員所使用 。
  - http://www.accessdata.com/



EnCase系統畫面



FTK系統畫面

鑑識模式

- 可分為live-analysis及dead-analysis (Carrier, 2003)
- Dead-analysis
  - 傳統進行電腦鑑識時關閉目標主機,進行證據(記憶體、硬碟)的收集與分析
- Live-analysis受到重視,目的為收集揮發性資訊
  - 關閉目標主機的同時,可能會造成揮發性資訊的流失。
  - 揮發性資訊：執行中的程序(process)、網路連線狀態、登入的使用者、開啟的檔案、記憶體使用狀況、即時通訊記錄、GPS資料等等。

Live CD/DVD/USB

- A live CD/DVD/USB separates the operating system from the computer. Whereas an operating system is usually permanently installed on the computer's hard disk, a live CD is typically designed to boot and run entirely from a read-only medium (such as a CD-ROM).
- Examples of Live CD/DVD
  - Knoppix – Remastering
    - http://www.knoppix.net/
  - Fedora – Kadischi
    - http://fedoraproject.org/wiki/Kadischi
  - Gentoo – Catalyst
    - http://www.gentoo.org/proj/en/releng/catalyst/

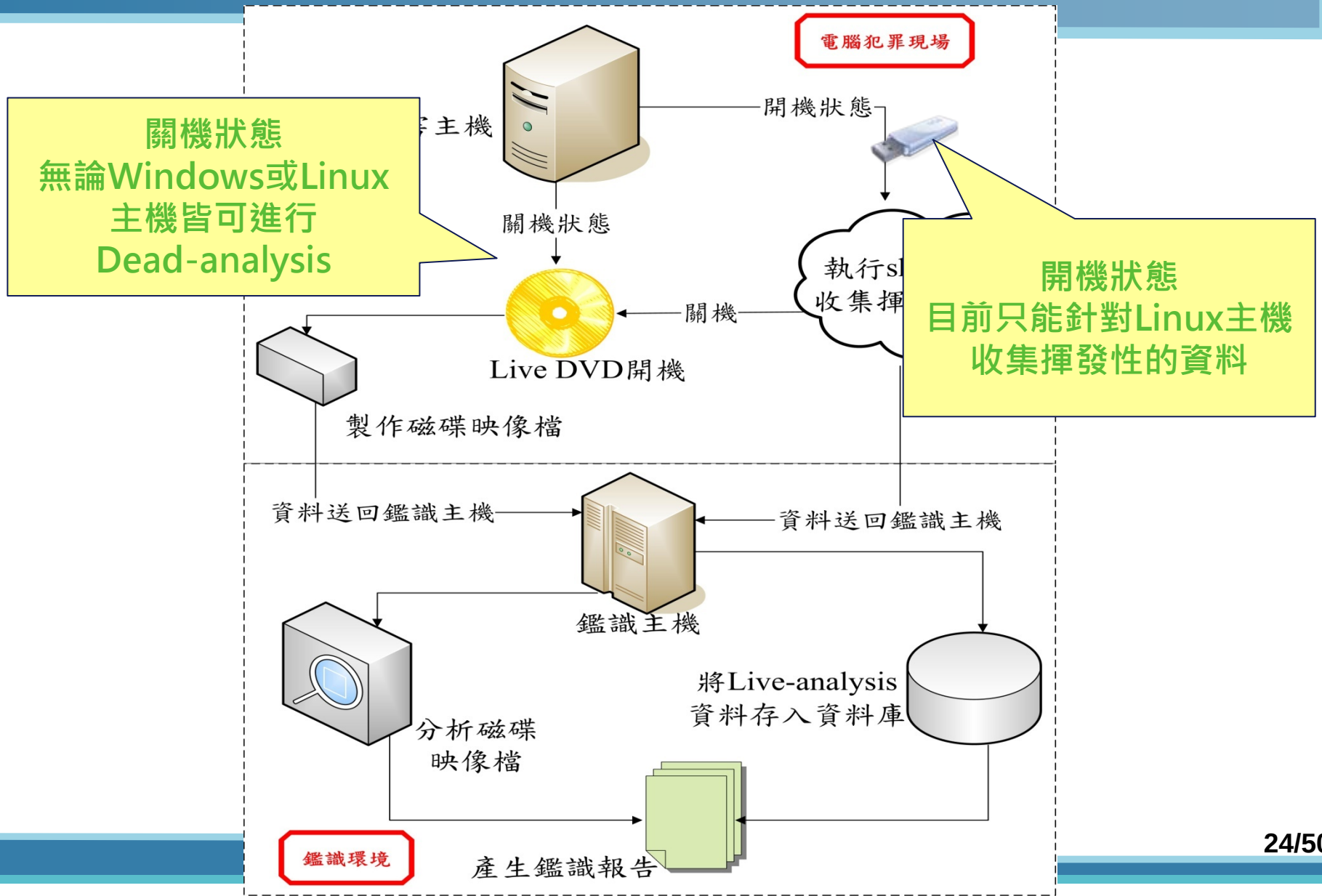
Forensic Live CD: Helix

http://www.e-fense.com/helix/

Forensic Live CD: caine

http://www.caine-live.net/

電腦鑑識系統之設計與實現



電腦鑑識系統之開發環境

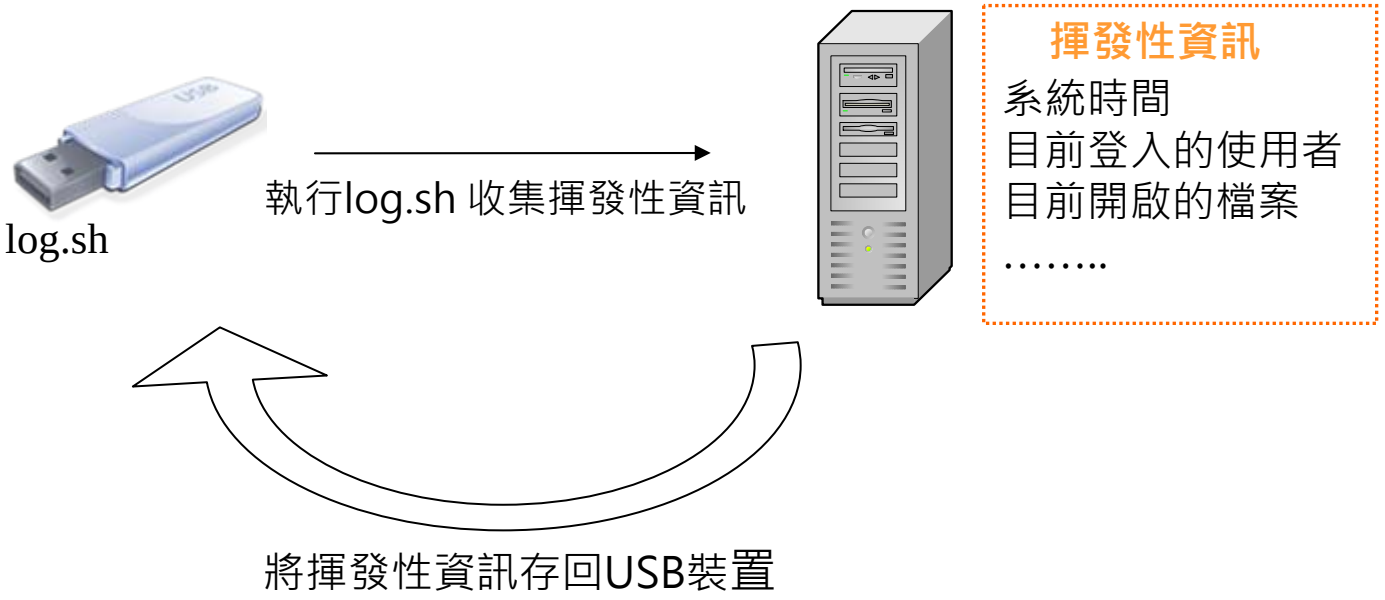
開發平台	xUbuntu 8.04
主要開發語言	Shell Script Python 2.5.2
Autopsy-SHA-256	Perl Digest::SHA - Perl extension for SHA-1/224/256/384/512
圖形化	Python 2.5.2 Xdialog 2.3.1
Live DVD	Tux2live 1.0.2

揮發性資訊收集指令

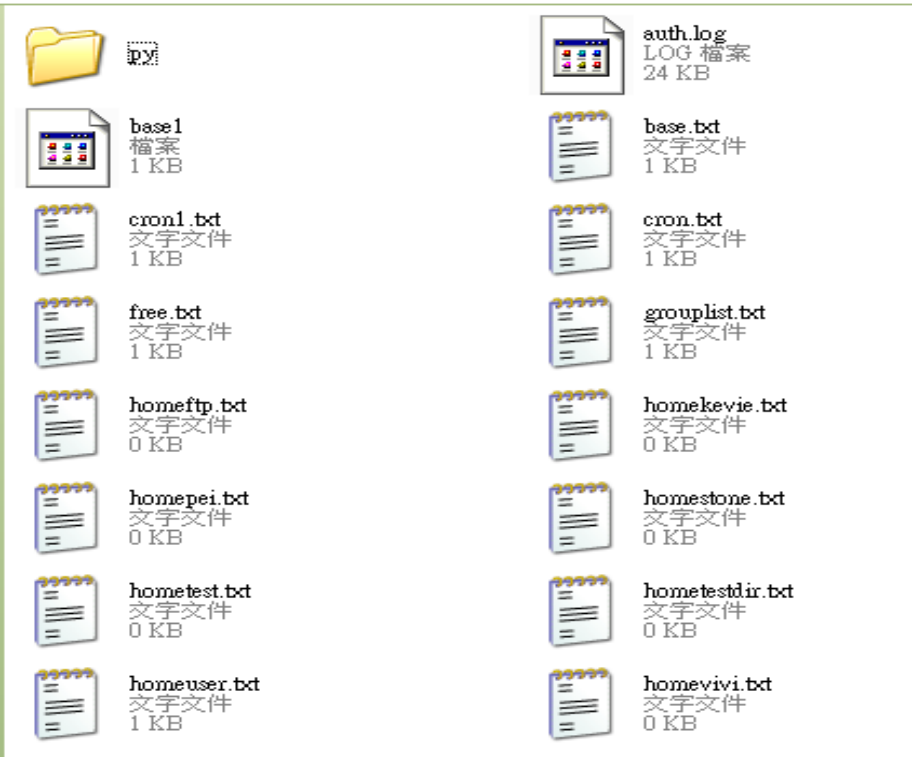
資料類別	Unix/Linux 指令
系統時間	date
目前登入的使用者	who
目前開啟的網路連線與埠號	netstat
目前正在執行的程序	ps
目前開啟的檔案	lsof
執行過的指令	history
…	…

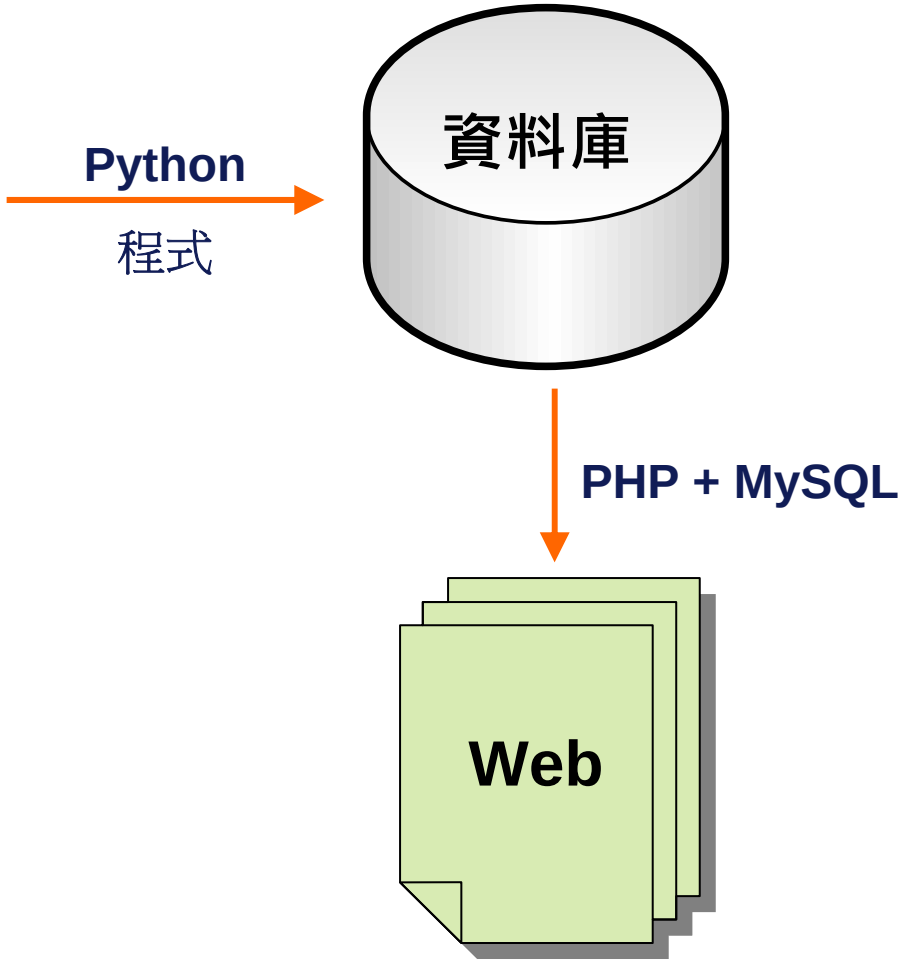
Live-analysis系統開發

- 自行撰寫Shell Script（log.sh）程式收集揮發性的資訊，並將所採集的數位證據存入資料庫中，再以Web的方式程呈現,以方便鑑識人員閱覽及分析，降低使用的障礙 。



建立揮發性資訊之檔案


py
base1
檔案
1 KB
cron1.txt
文字文件
1 KB
free.txt
文字文件
1 KB
homeftp.txt
文字文件
0 KB
homepei.txt
文字文件
0 KB
hometest.txt
文字文件
0 KB
homeuser.txt
文字文件
1 KB
auth.log
LOG 檔案
24 KB
base.txt
文字文件
1 KB
cron.txt
文字文件
1 KB
grouplist.txt
文字文件
1 KB
homekevie.txt
文字文件
0 KB
homestone.txt
文字文件
0 KB
hometestdir.txt
文字文件
0 KB
homevivi.txt
文字文件
0 KB


Python
程式
資料庫
PHP + MySQL
Web

系統登入失敗鑑識資訊

Digital Forensic

取自於auth.log

Home | User Data | Network Setting | System Data | Log Data

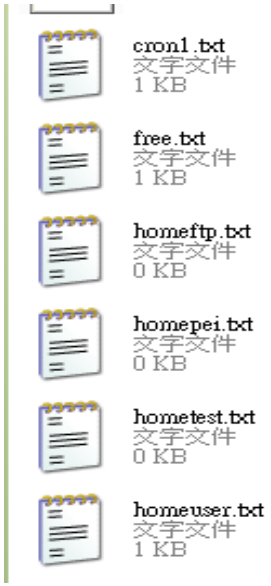
連線方式	使用者名稱	惡意來源IP
sshd[7484]	t1na	66.64.128.234
sshd[7486]	alexis	66.64.128.234
sshd[7488]	t1na	66.64.128.234
sshd[7490]	a	66.64.128.234
sshd[7492]	art	66.64.128.234

User Data
- 登入系統失敗記錄
- 惡意IP來源列表
- 目前登入的使用者
- 所有使用者列表
- 所有群組列表

Network Setting
- TCP埠與UDP埠狀態

System Data
- 硬碟分割狀態
- 目前開啟的檔案
- 目前開啟的裝置
- 目前系統執行的程序

揮發性資訊之 SHA-256值



hash值	檔案名稱
2a10a2f221e277694fcff173700d89fad49e0762e81a105f1774d89bc933f7ab	auth.log
a70717990e4cb1dfc5a0ade672cbefc8dbb4e698780d9faf6b8a75e17cd6dc23	base1
a70717990e4cb1dfc5a0ade672cbefc8dbb4e698780d9faf6b8a75e17cd6dc23	base.txt
5b856d7fdff8f6b762e57ed8f8022a46b53b236f9a6b2083b828d9f65c57d5df	cron1.txt
d14307849698f0c02f7d8a1b0bd9042f32781cd2b80c179b5ca7ab3c77168786	cron.txt

Dead-analysis 系統開發

- 本系統整合鑑識流程中會使用的鑑識工具於Live DVD/USB中。
- 工具選單包含鑑識工具與安全工具兩大類，又依鑑識的功能分為三項
  - 映像檔製作工具
  - 分析、還原工具
  - 呈現報告
- 本研究電腦鑑識系統Live DVD下載網址 http://security.nknu.edu.tw/download/

功能選單分類列表

功能項目	說明
映像檔製作	用來製作磁碟映像檔的工具
鑑識分析	針對映像檔還原、分析的工具
鑑識報告	用來產生最後的鑑識報表
資訊收集	對目標電腦系統收集相關資訊的工具
網路探測	用來探測目標電腦的開啟的埠號及服務等的工具
弱點評估	用來探測目標電腦弱點的工具
滲透測試	可針對目標的弱點進行滲透測試的工具
入侵及誘捕	可用來架設誘捕系統的工具
無線網路安全	用來擷取無線網路封包並進行分析的工具
加解密工具	可用於加解密的相關工具
安全程式碼檢測	用來檢測程式碼弱點的工具
其他	密碼破解、病毒檢測等等

Live DVD電腦鑑識工具畫面

本系統鑑識工具清單

映像檔製作工具	1. Guymager 2. AIR
鑑識工具	1. Autopsy (整合性鑑識工具) 2. SFDUMPER (檔案還原) 3. Scalpel (檔案還原) 4. Foremost (檔案還原) 5. Fundl (檔案還原) 6. Ddrescue (資料救援) 7. Gddrescue (資料救援) 8. Magicrescue(檔案還原)

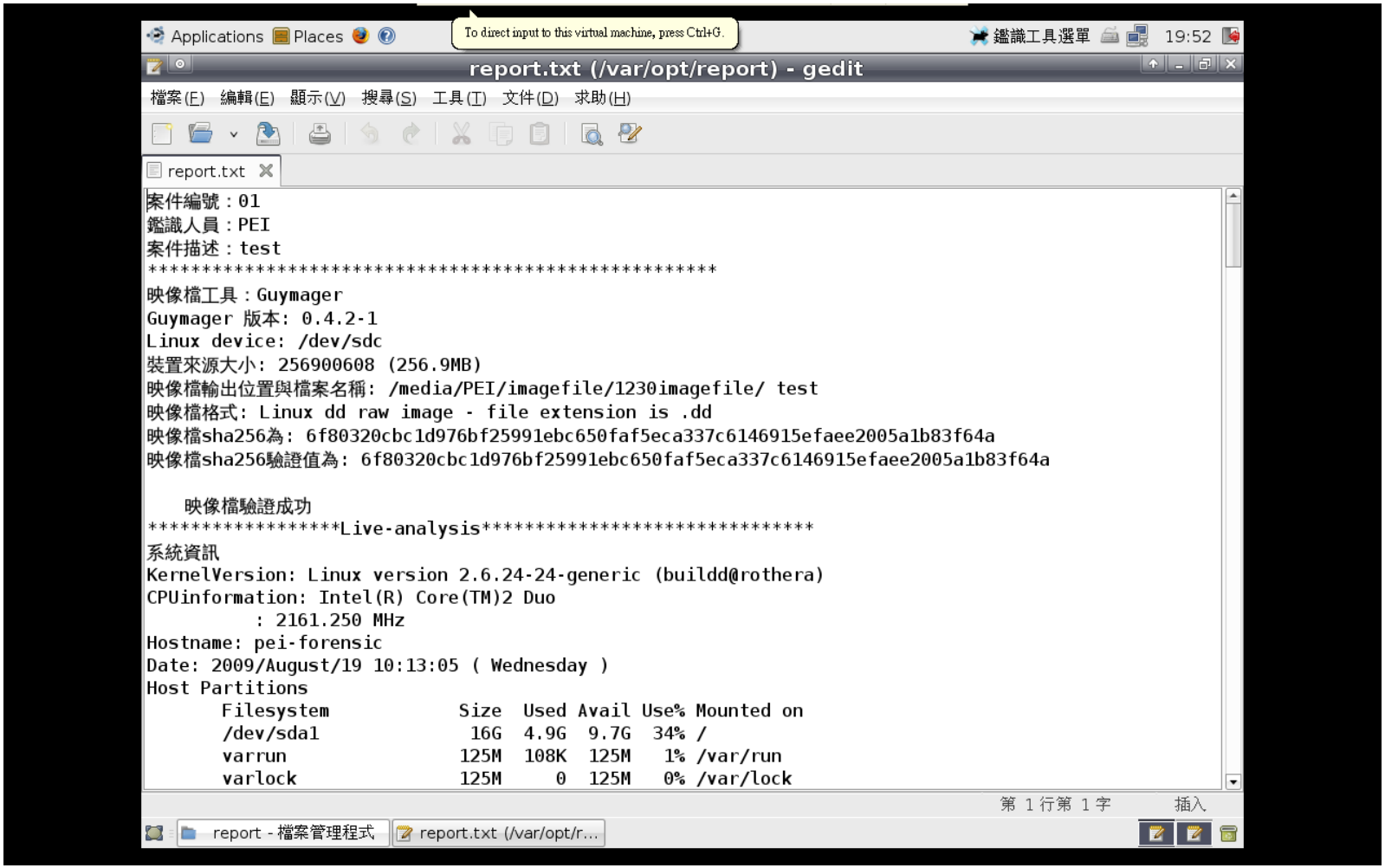
中文化-Autopsy


應用程式 位置 系統
4月1日(三) 21:30 pei
Autopsy Forensic Browser - Mozilla Firefox
檔案(F) 編輯(E) 檢視(V) 歷史(S) 書籤(B) 工具(T) 說明(H)
http://localhost:9999/autopsy
Google
最常瀏覽的網站 Getting Started Latest Headlines 新手上路 即時新聞 Yahoo!奇摩服務 今日新聞
歡迎使用 Ubuntu 8.04 LTS!
Autopsy Forensic Browser
WARNING: Your browser currently has Java Script enabled.
You do not need Java Script to use Autopsy and it is recommended that it be turned off for security reasons.
Autopsy Forensic Browser 2.20
http://www.sleuthkit.org/autopsy/
開啟案件
新增案件
問題解答
完成
[Synaptic 套件管理程...
[鳥哥的 Linux 私房菜 ...
Autopsy Forensic Bro...
root@pei: /usr/local/a...

中文化-Autopsy


test2:host1:vol1 - Mozilla Firefox
http://localhost:9999/autopsy?mod=1&submod=2&case=test2&host=host1&ir
**檔案分析 關鍵字搜尋 檔案格式 映像檔詳細資訊 資料單元 協助 關閉
目錄搜尋
請輸入你要檢視的目錄名稱.
C:/
檢視
檔案名稱搜尋
請輸入你搜尋的檔案名稱以Perl的規則表示.
搜尋
檢視所有刪除的檔案
延展目錄
目前目錄: C:/
@加入註解
@產生檔案的MD5清單
刪除 類型 dir / in 名稱 寫入時間 存取時間 建檔時間 檔案大小 UID GID META
r / r 90316~1.BAC 2009-03-16 2009-03-16 2009-03-16 262984192 0 0 22
計算SHA-256 (須要一些時間)
"/media/PEI/imagefile/1230imagefile/test.dd"
SHA-256值: e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
測試磁區
複製映像檔至證據存放的目錄(此動作須要一些時間)
新增映像檔的ID img1
Disk image (type dos) added with ID vol1
映像檔(99 to 501247 - fat32 - C:)加入ID vol2
確 定
新增映像檔

鑑識報告


Applications Places
To direct input to this virtual machine, press Ctrl+G.
鑑識工具選單
19:52
report.txt (/var/opt/report) - gedit
檔案(F) 編輯(E) 顯示(V) 搜尋(S) 工具(T) 文件(D) 求助(H)
report.txt
案件編號：01
鑑識人員：PEI
案件描述：test
****
映像檔工具：Guymager
Guymager 版本: 0.4.2-1
Linux device: /dev/sdc
裝置來源大小: 256900608 (256.9MB)
映像檔輸出位置與檔案名稱: /media/PEI/imagefile/1230imagefile/ test
映像檔格式: Linux dd raw image - file extension is .dd
映像檔sha256為: 6f80320cbc1d976bf25991ebc650faf5eca337c6146915efaee2005a1b83f64a
映像檔sha256驗證值為: 6f80320cbc1d976bf25991ebc650faf5eca337c6146915efaee2005a1b83f64a
映像檔驗證成功
**********Live-analysis**********
系統資訊
KernelVersion: Linux version 2.6.24-24-generic (buildd@rothera)
CPUinformation: Intel(R) Core(TM)2 Duo
: 2161.250 MHz
Hostname: pei-forensic
Date: 2009/August/19 10:13:05 (Wednesday)
Host Partitions
Filesystem Size Used Avail Use% Mounted on
/dev/sda1 16G 4.9G 9.7G 34% /
varrun 125M 108K 125M 1% /var/run
varlock 125M 0 125M 0% /var/lock
第 1 行第 1 字
插入
report - 檔案管理程式
report.txt (/var/opt/r...

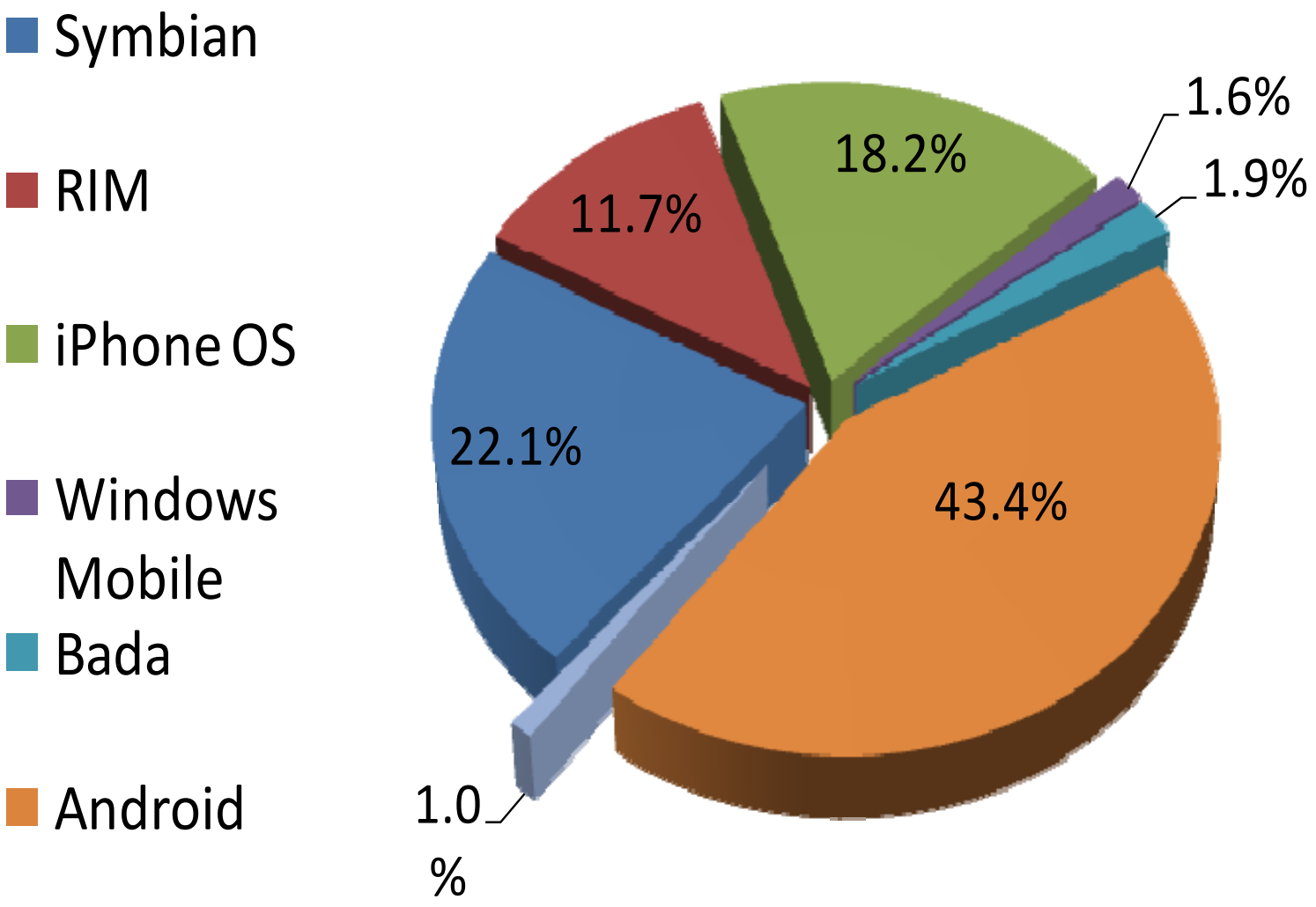
手機鑑識
(Mobile Phone Forensics)

手機(Android, Symbian)鑑識

- 智慧型手機鑑識數位證據來源:

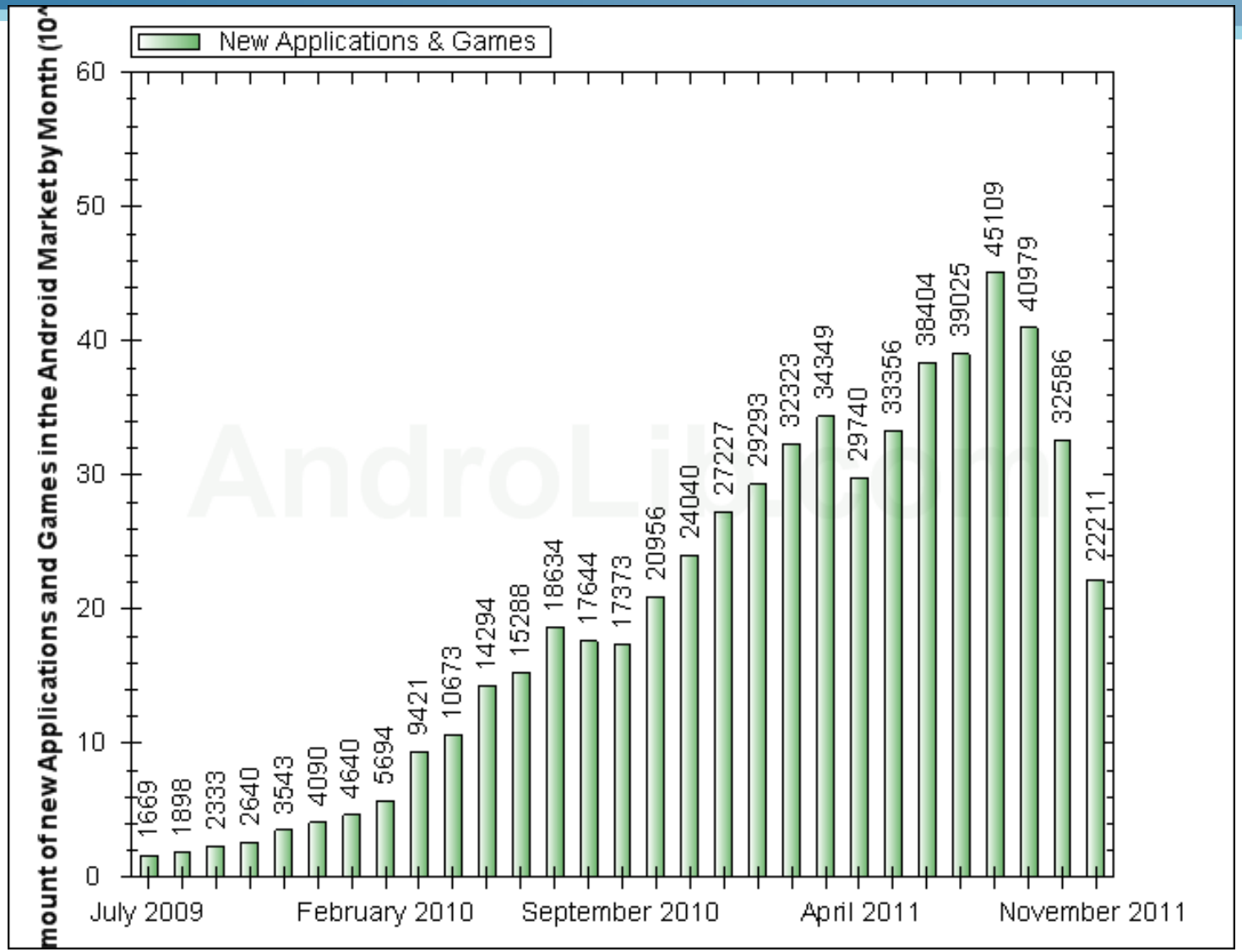

- 手機有多種作業系統、硬體介面、驅動程式
- 我們針對Android手機開發鑑識軟體

手機作業系統



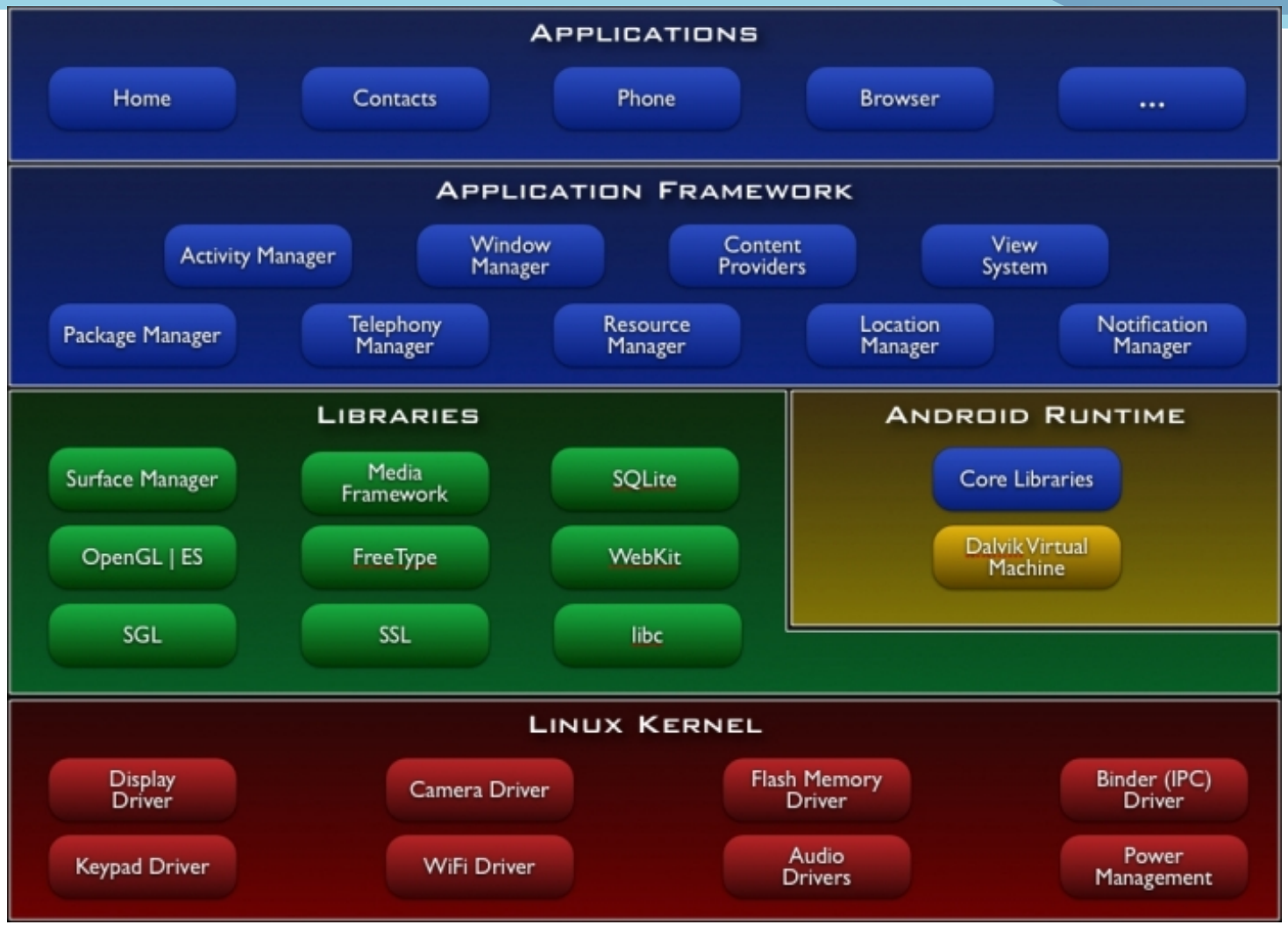
Source: Gartner, Inc. (August 2011)

Android每月新軟體



Source: AndroidLib

Android Architecture



Source: http://developer.android.com/guide/basics/what-is-android.html

手機鑑識方式

記憶卡執行鑑識 (雛形系統改良中)

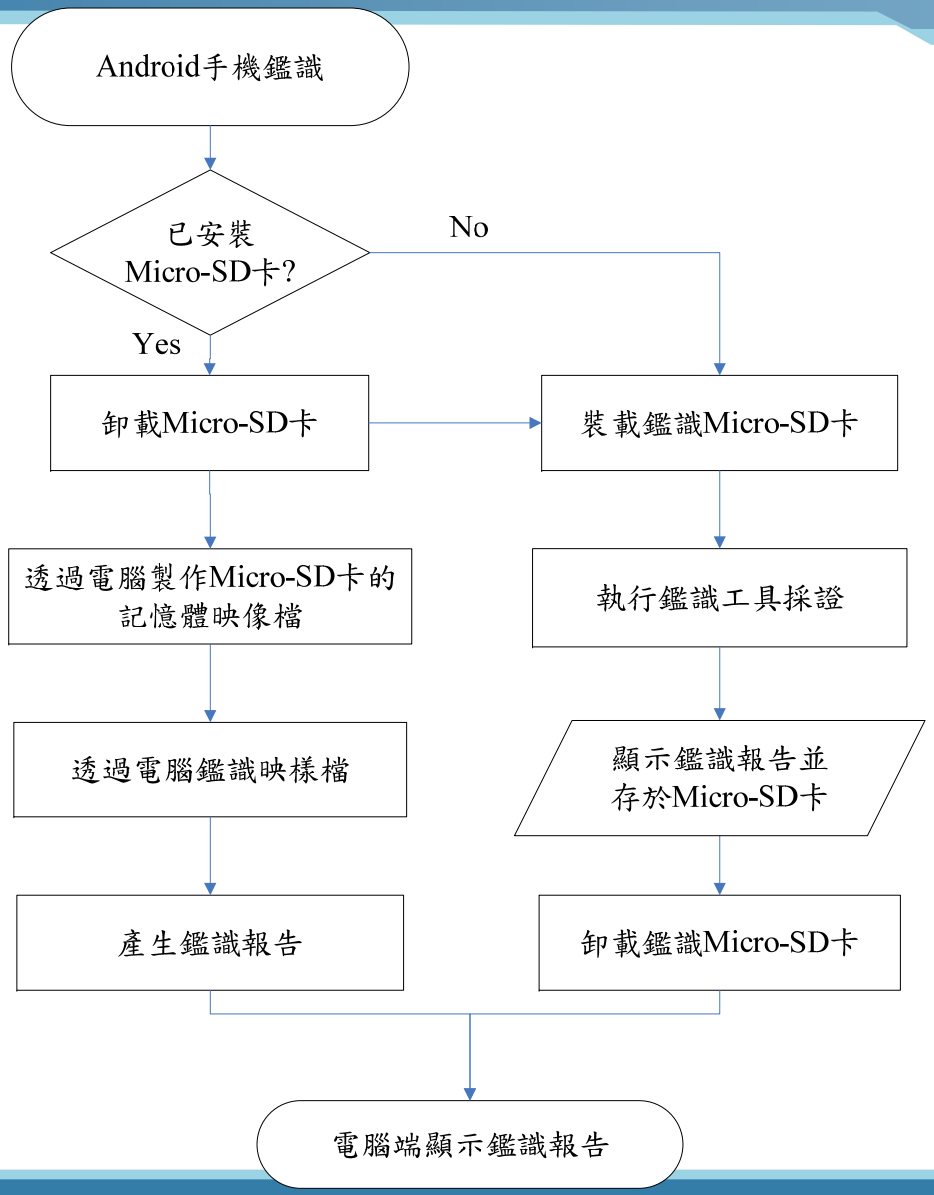
電腦端控制鑑識　(系統開發中)

雲端控制鑑識　(系統開發中)

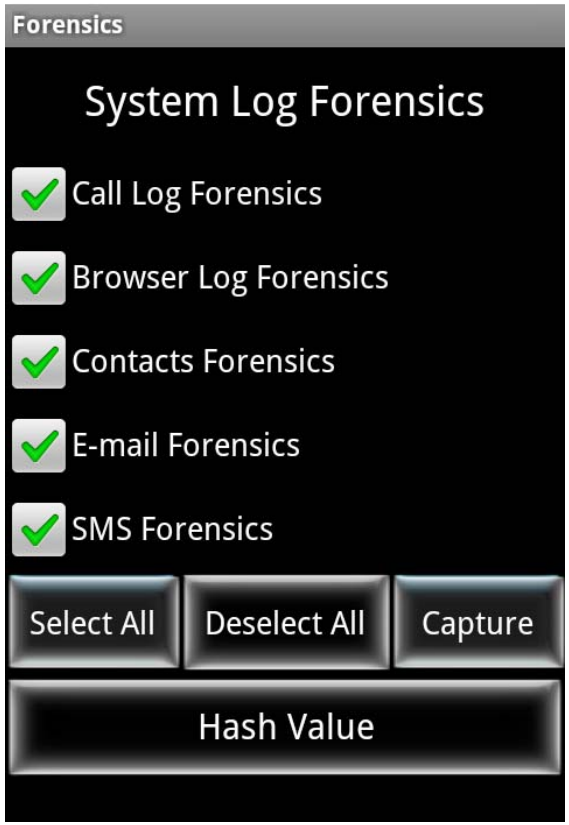
Android手機鑑識系統

- Java程式語言
- JDK + eclipse + Android SDK 免費的開發環境
- 初期參考開放原始碼Android Forensics
- 透過Android API及Linux指令建置鑑識系統
- 收集手機的數位證據
  - 電話通聯記錄、簡訊、通訊錄
  - 瀏覽網頁記錄、搜尋記錄
  - Email
  - Wi-Fi資料

Android手機鑑識流程



系統實作



http://security.nknu.edu.tw/download/ForenDroid1.0.apk

鑑識報告


Forensics
Forensics Reporting
Hash Value :
case123.txt:
MD5:484b038bc6cfcd7d14fc1763f64721c2
SHA-256:13cd4c128990aa6ab197c116f6bc704482
347050bc0b089b64a6f89c9b5deecd
Phonestate.txt:
MD5:7fd95fb7ee6950de27f46b82db9ae26c
SHA-256:521618c803bd40af6309fb981b7d7ed85
30ab4d8cb48d7951349e95b0f1aea94
Phonestate-Runningprocess.txt:
MD5:255adaa36efc34cf141a9afc6bb33933
SHA-256:c4f009009ccb86d018ba5fa05b9eca299d
9cdf403a0babbbb78137f2e58d42ea
Phonestate-Memorystates.txt:
MD5:f49f66b2c30f6a71025067d9bd5763a3
SHA-256:e557bc6f7b1b568e046d7457579256964
72ab9576dc5e915543bbadaf11f0ef7
SIM.txt:
MD5:e1fbb1c624664a2e4213f9e4b88350e7
SHA-256:93fa0acac69678d032fd064c479de16412
784e2ba5c3f879c606ab106d70a5c2


Forensics
Forensics Reporting
Forensics File Report
Phone Status Report
SIM Card Status Report
Running process Report
Memory states Report
System Log Report

總結

- 鑑識人員在資安事件發生後,須從數位裝置上收集證據
- 鑑識工具也可協助瞭解數位裝備中的個人隱私資料
- 本研究開發中文化開機鑑識DVD與Android手機鑑識軟體，持續進行手機(反)鑑識軟體與雲端鑑識軟體
- 雛型軟體參見http://security.nknu.edu.tw/download/
- ISO/IEC (early draft)
  - 27041: Assurance for digital evidence investigation methods
  - 27042: Analysis and interpretation of digital evidence
  - 27043: Digital evidence investigation principles and processes

References

1. E. Casey (ed.), *Handbook of Digital Forensics and Investigation*, Academic Press, 2010.
2. J.M. Aquilina, E. Casey, and C.H. Malin, *Malware Forensics: Investigating and Analyzing Malicious Code*, Syngress, 2008.
3. T.V. Lillard, C.P. Garrison, C.A. Schiller, and J.J. Steele, *Digital Forensics for Network, Internet, and Cloud Computing: A Forensic Evidence Guide for Moving Targets and Data*, Syngress, 2010.
4. S. Garfinkel, "Digital Forensics Research: The Next 10 Years,"10th Digital Forensics Research Conference, August 2010, http://www.dfrws.org/2010/proceedings/2010-308.pdf

敬請批評指教