【手機鑑識技術及實務分享】

鑒真數位有限公司

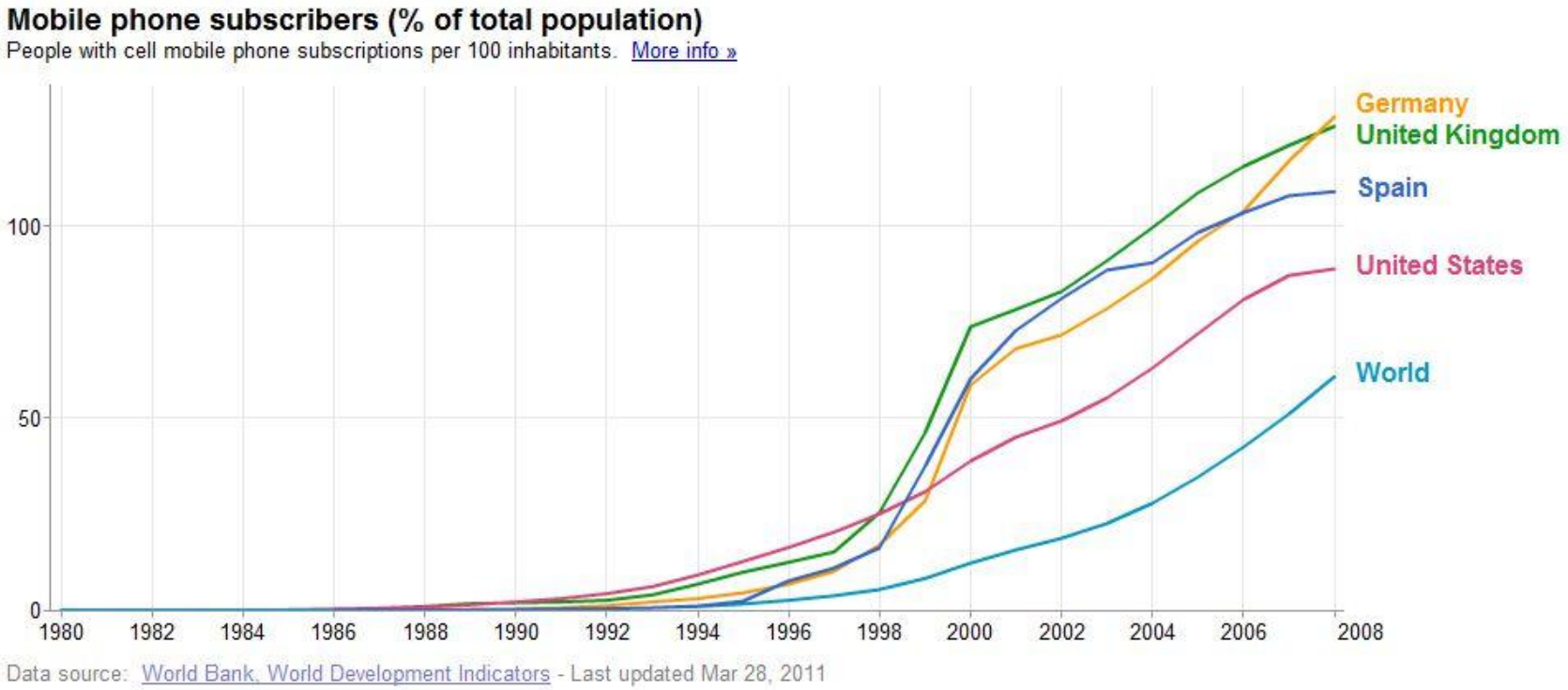
黃敬博 (po@iforensics.com.tw)

時間:2011/07/23

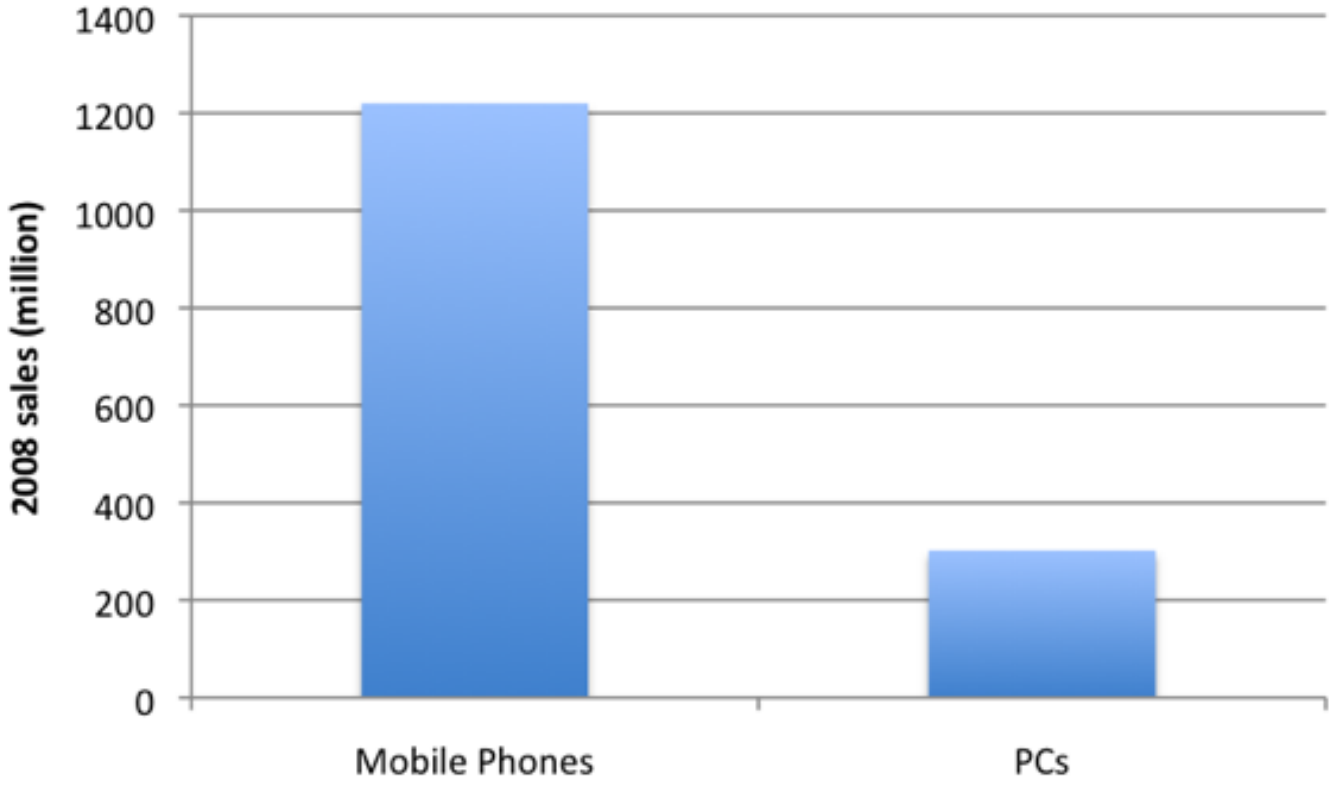
Agenda

- Trend of Mobile Forensics
- Smart Phone Forensics Focus
- Commercial Solutions
- Q & A

Mobile Phone Subscribers



Computers versus Mobiles



Mobiles are supplanting traditional computing – it is now predicted by the end of 2011, that sales of “smart-phones” alone will have passed that of computing devices

Spot the difference?

Mobile Devices Forensics Scope

Sim Card

Phone / Smartphone

Memory Stick / SD Card

Watch Phone

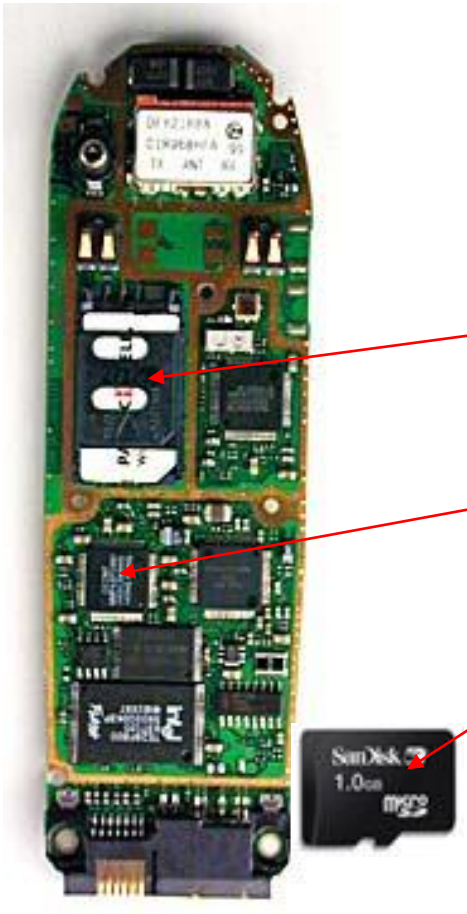
GPS

Mobile Modem

Media Device

Tablet

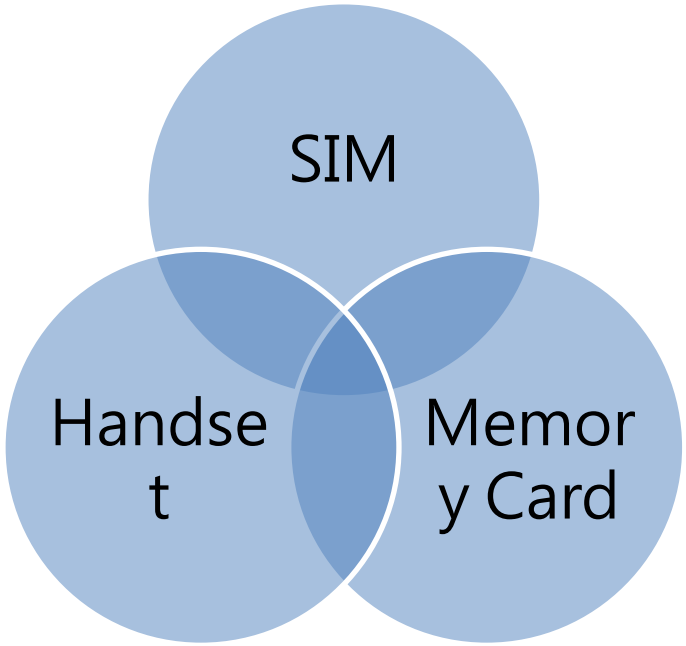
Mobile Forensics Key Factors



SIM

Handset

Memory Card



SIM-ID Cloner Device

Memory Card Reader

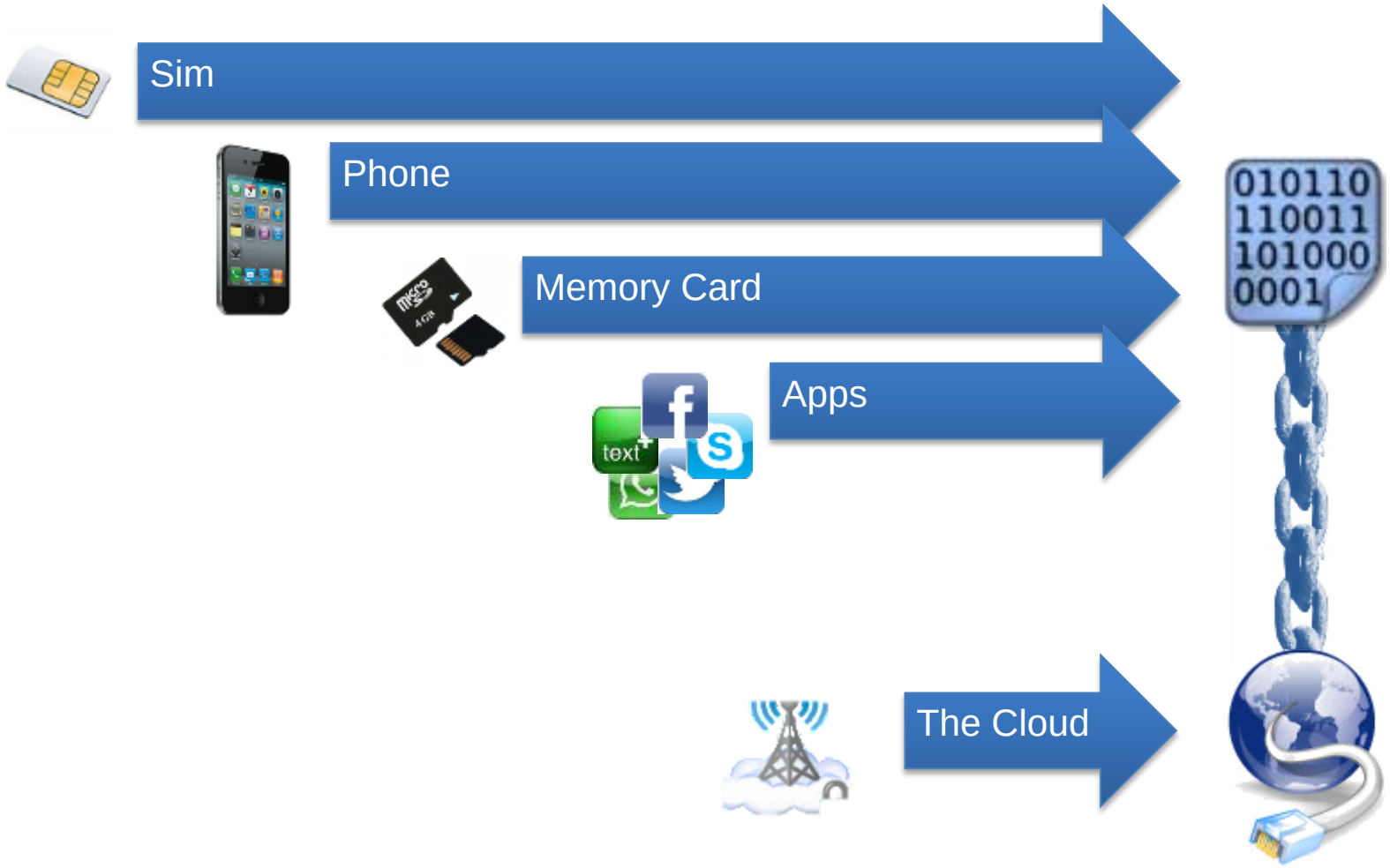
The Best Easy Forensics Tools:

1. FTK Image Light
2. Forensics Card Reader
3. SIM Card Reader

What evidence can we expect in a mobile today?

- Contacts
- Calls (dialled, missed, received)
- Text Messages (SMS) & Multimedia (MMS)
- Times / Dates
- Pictures, Audio and Video Images
- Tasks / Notes / Calendars
- Application Files
- Bluetooth Pairing
- Maps, GPS Locations
- E-mail, browser History
- Smartphone ‘App’ Data – Facebook, Skype, Gmail etc…

Evolution of data storage and Forensics focus



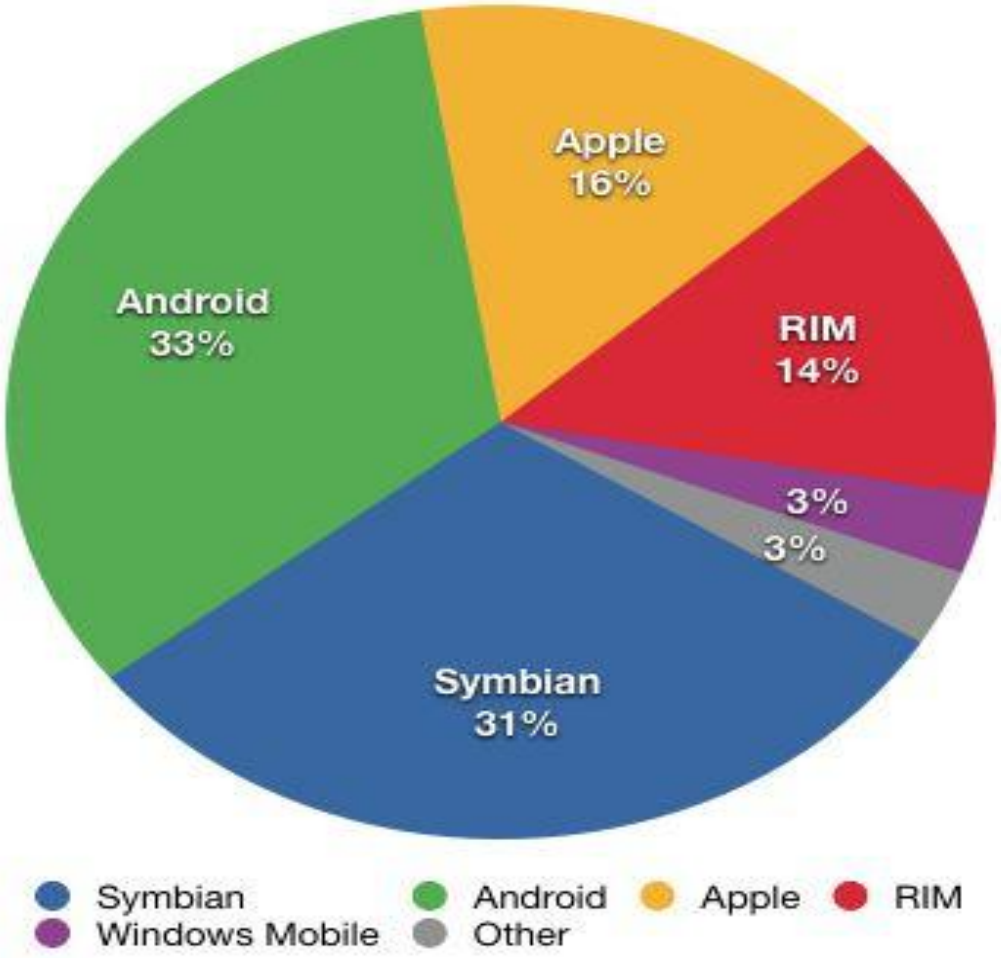
Mobile Device Market Trend – December 2010

Top 30 Mobile Devices* CHART B

millennial media's mobilemix THE MOBILE DEVICE INDEX

Rank	Phones	November	Type	OS
1	Apple iPhone	12.45%	Smartphone	iOS
2	BlackBerry Curve	6.55%	Smartphone	BlackBerry OS
3	Apple iPod Touch	6.47%	Connected Device	iOS
4	HTC Nexus One (Passion)	4.14%	Smartphone	Android
5	Motorola Droid	2.84%	Smartphone	Android
6	Samsung Freeform (SCH-R350)	2.47%	Feature Phone	BREW
7	HTC G2 Touch Hero	2.15%	Smartphone	Android
8	Apple iPad	2.04%	Connected Device	iOS
9	Samsung Vibrant Galaxy S		Smartphone	Android
10	BlackBerry Bold 2	1.72%	Smartphone	BlackBerry OS
11	HTC Evo	1.68%	Smartphone	Android
12	Motorola Droid 2	1.61%	Smartphone	Android
13	HTC Aria	1.31%	Smartphone	Android
14	HTC Droid Incredible	1.30%	Smartphone	Android
15	Samsung Messager II	1.21%	Feature Phone	BREW
16	Sanyo Incognito (SCP-6760)	1.13%	Feature Phone	Java
17	Motorola Droid X	1.06%	Smartphone	Android
18	Motorola Cliq (MB200)	1.06%	Smartphone	Android
19	HTC MyTouch 2 (Espresso)	0.98%	Smartphone	Android
20	HTC MyTouch Magic	0.97%	Smartphone	Android

Smartphone Market Share



Complicated Forensics focus in APPs

3rd party Apps... What doesn't it do?

- Accounts
  - E-mail, ICQ Free, AOL Instant Messenger
- Bookmarks
  - Web browser, Google Maps
- Dynamic Keyboard Cache
- History
  - Web browser, Google Maps, YouTube, Google Earth
- IP-telephony
  - Skype, Viber
- Messaging
  - Skype, Viber, WhatsApp, Yahoo Messenger, AOL Instant Messenger
- Navigation Data
  - TomTom
- Social Engineering
  - Facebook
  - Twitter

Android (Google APP World)

Search

Gmail

Calendar

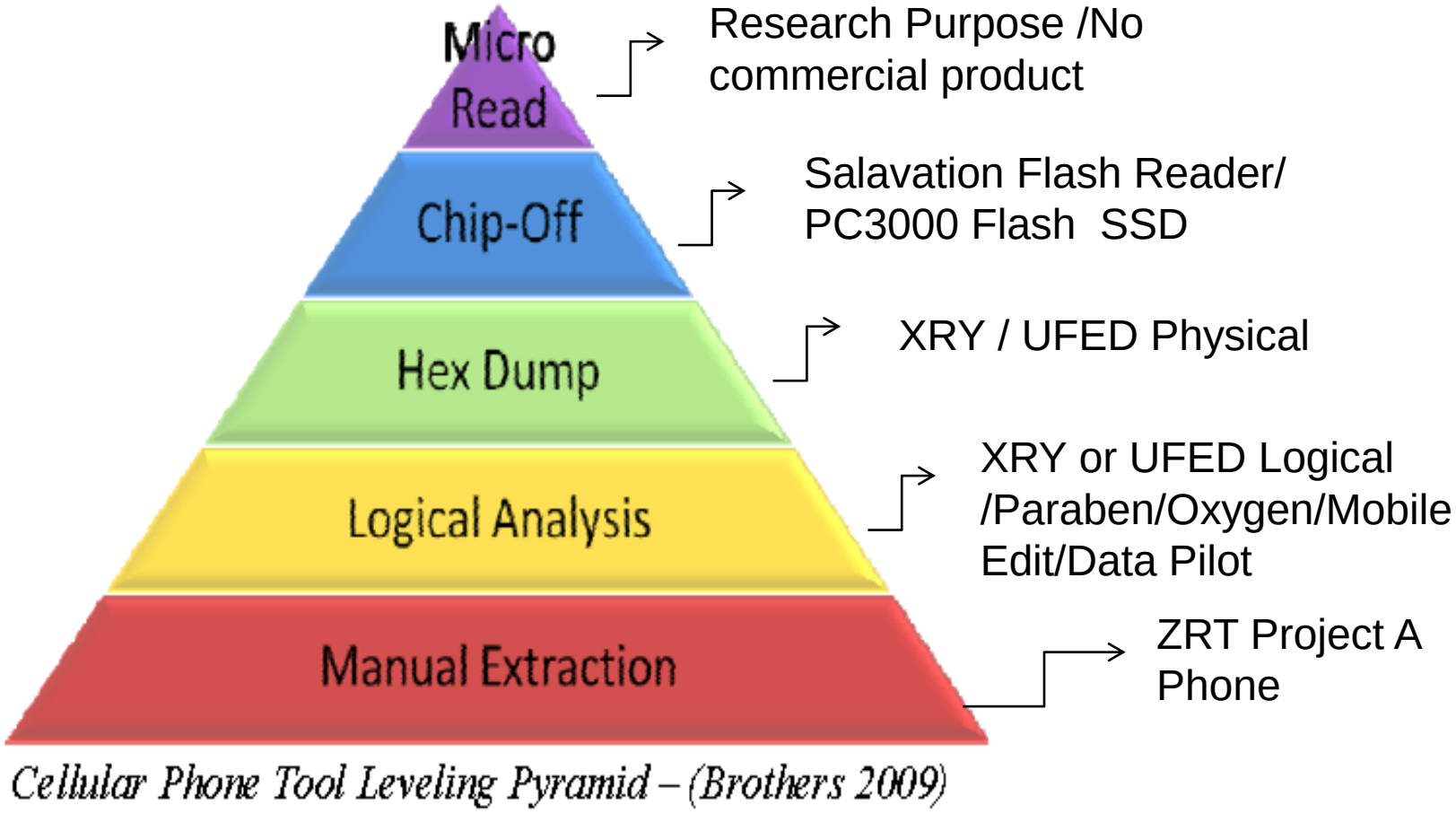
Contact

YouTube

Talk

Maps

Mobile Forensics Approach



Cellular Phone Tool Leveling Pyramid – (Brothers 2009)

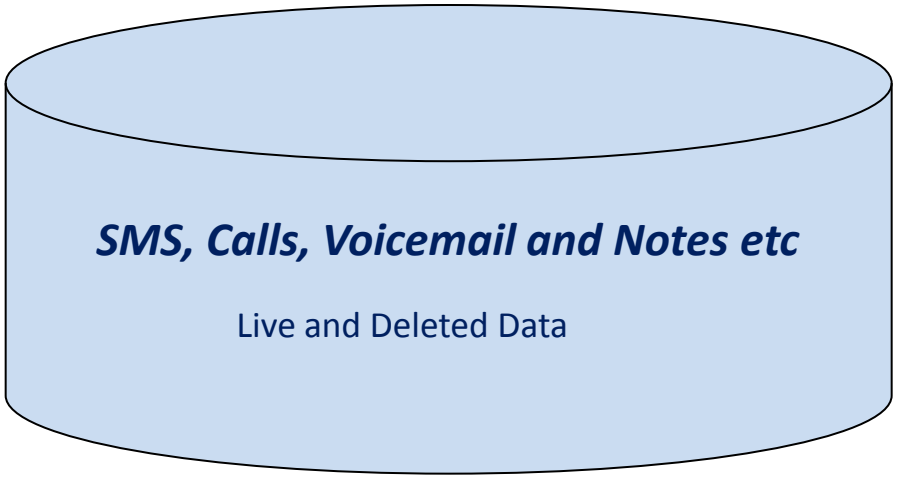
ZRT System

What Can a Logical Extraction Retrieve?

LIVE	Live SIM data can be retrieved	Live handset data can be retrieved
DELETED	Only deleted SMS can be retrieved (using card reader)	Deleted handset data cannot be retrieved

Backup Software iTunes Extraction (Logical) …

Deleted data in SQLite Db remains – Why?



- ***On the iDevice the Logical extraction retrieves the SQLite database***
  - ***Same thing as a Physical dump of the data***
- ***iOS Live and Deleted data such as***
  - ***SMS, Calls, Voicemail and Notes are never erased, only the pointers are re-arranged***

Physical Extraction

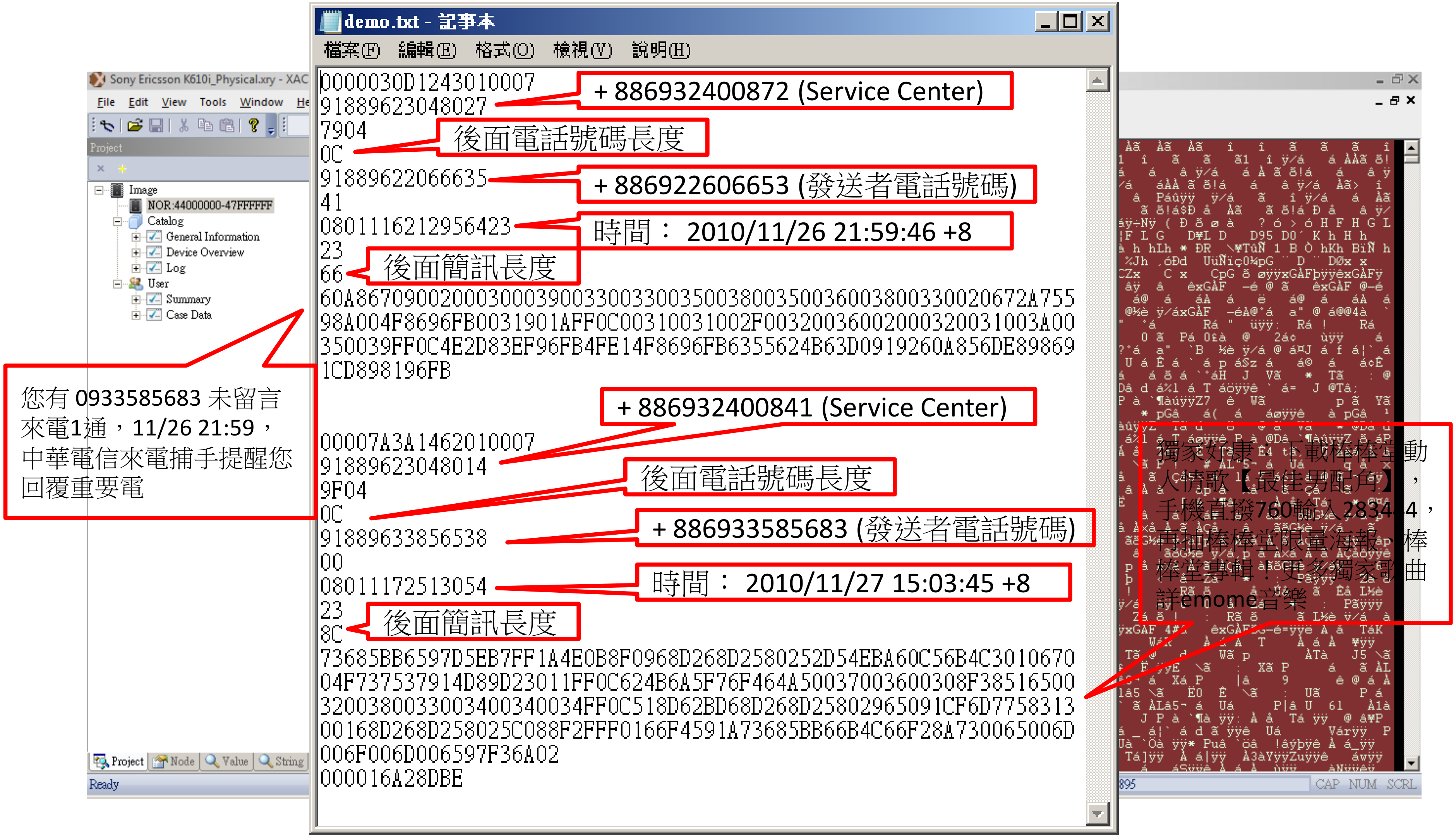
- Benefits
  - Full device image
  - Carve live & deleted data with Good Tools
    (The best tool “XACT” free to be downlowded)
  - Export live data using 3rd party tools

- Issues with a Physical Extraction
  - Not possible on passcoded devices
  - Jailbroken is a key
  - Newer iDevices together with iOS 4 or later are very hard to decode due to hardware encryption

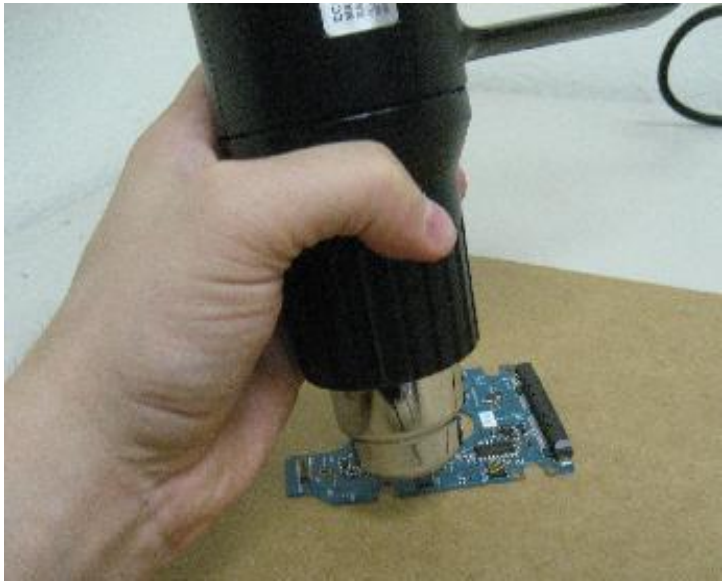
Flashboxes Engineering Mode

- No official support, Risky
- Not friendly User Interface, Easy to destroy
- Many different Boxes for different phones

Sony Ericsson K610i



Chip-off – Advanced Data Analysis



Commercial Forensics Products

XRY PHYSICAL

MOBILedit FORENSIC

Logicube

paraben corporation

Guidance SOFTWARE

Remote wipe ?!

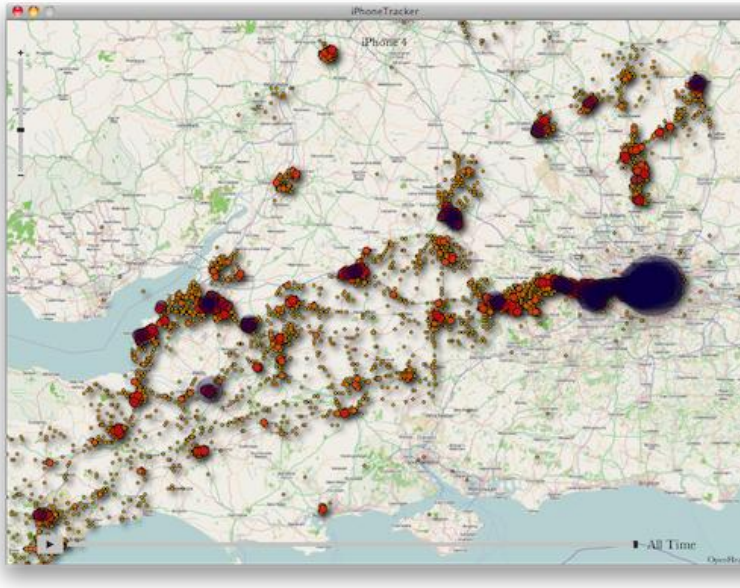
- Farady Box
- Phone Jammer

iOS JB steps(all versions)

- 精靈找工具Jailbreak-me.info
- Download http://www.felixbruns.de/iPod/firmware/
  - Firmware must be the same as your iphone version
- 用工具打開韌體 IPSW
  - 工具會修改 IPSW
  - 工具會提示準備進入 “DFU Mode” (進入BIOS)
    - 手機關機，USB連線插入
    - Home + Lock 按住不放 7 秒
    - 白蘋果出現，繼續按
    - 白蘋果消失，繼續按住 Lock 3 秒，放開 Lock
    - 到這裡都不放開 Home，繼續按住 10 秒
    - 螢幕不會顯示畫面，但會亮起來，電腦會抓到DFU裝置
  - 工具Next 會完成JB

iPhone JB Digging

- Dig all app “accounts” name in iPhone
- Dig last input Keyboard text
- Google Maps History log
- Application/Snapshot/ have the last screen shut
- Consolidated.db
  - Have all records of your tracks
  - Use XRY map to Google Earth



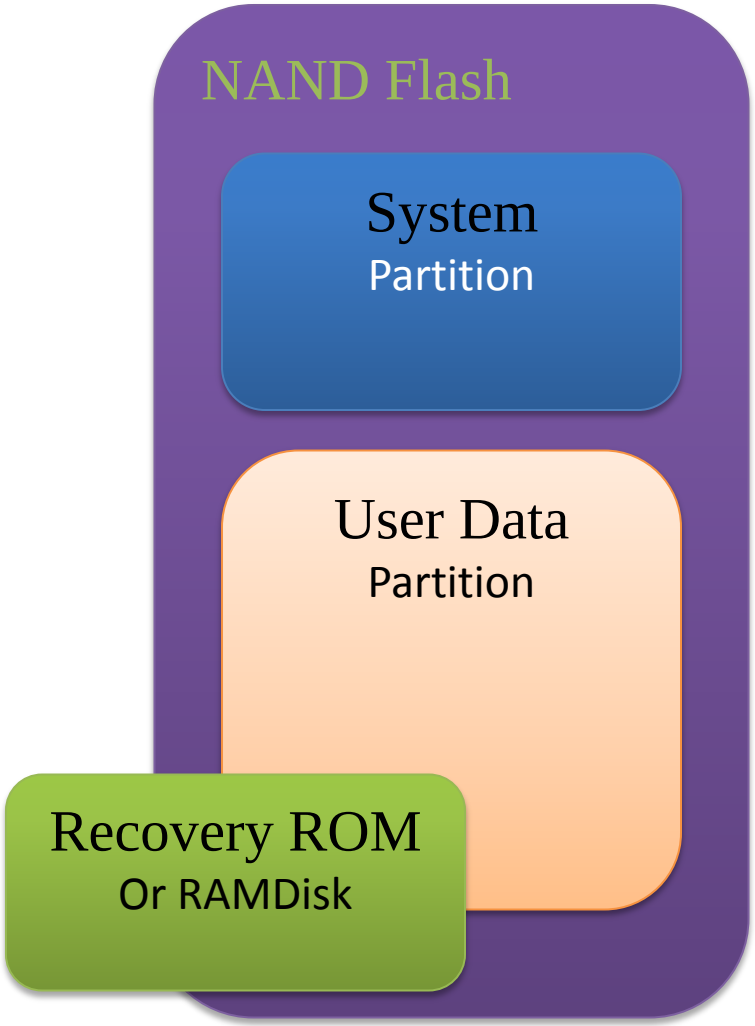
Android Phone Case Study:

Android Free JB tool

- Connect the Phone to PC
  - Download and install ‘SuperOneClick’
  - Install Phone Driver，depends on each phone
  - Phone Turn on USB Debug Mode
- Use “Shell Root” to JB Android phone

Full NAND Backup

- Best Method, Forensically Sound
- Idea is similar to LiveCD Boot then dd image
- For all Android and iOS with most iBoot (Except iPad2)



Smart Phone Extraction Methods

	iTunes Backup	Logical Backup	Physical Jailbreak	Physical Ramdisk
要錢？	Free	$$$	$$$	Free
對象	電腦硬碟	裝置	裝置	裝置
PassCode密碼	需GPU破加密	沒密碼就沒轍	無影響	無影響
證物完整性	Write-block	Write-block	會寫入資料	Write-block
使用者資料*	V	V	V	V
App 程式資料	不完整	不完整	V	V
系統資料	少數 過去GPS座標/網路SSID**		完整 程式關閉畫面	
已刪除資料	X	X	V (用DD挖出)	V (用DD挖出)
資料整理	iBackupbot PhoneView	UFED/XRY 最有組織性	要自己動手挖	要自己動手挖
所需時間 16GB或32GB	10~20min 可能很久沒同步	UFED 4~8Hr XRY 10~20min	UFED 6-10Hr XRY 30~50min	DD 50~100min

* 系統的電子郵件從 iOS 4 開始硬體AES加密，尚未有方法解密
刪除的資料如簡訊、聯絡人若SQLite尚未覆蓋可能解出
** iOS 4.3.2 開始僅紀錄有限時間內的GPS座標

如何 decode dd 出來的 DMG?

- 正常大小
  - System 510mb, 750mb, 1000mb 左右
  - Data 14.2G or 30.2G 左右
- Mac OS X 可以直接掛載
  - Mac 上的檔案救援軟體都可使用
  - 檔案系統叫做 HFS+ 的 iOS 特別版
- iFunbox 工具（只能看到未刪除）
- FTK 3.x 版（解出目錄和檔案+Unallocate）
- XRY Physical decoding , or use XACT 分析
- 用EnCase V7 版smpart phone mobule解析

Suggest of Solutions

- Best and Easy approach ($$$ cost!)
  - XRY Office Complete (3 phones in a time!)
    - Very fast and have the most detailed report
  - UFED + Physical Pro (Easy to use)
  - EnCase (New smart phone module)
- No budget:
  - XACT (Free downloaded from XRY)
  - iFunbox /SuperOneClick
  - SQLite/Plist Editor
  - FlashBox…

Forensics 鑒眞數位

Q&A

Thanks for your attention ,

courtesy for MSAB marketing information

More demo videos can be downloaded from:

http://www.iforensics.com.tw/

po@iforensics.com.tw