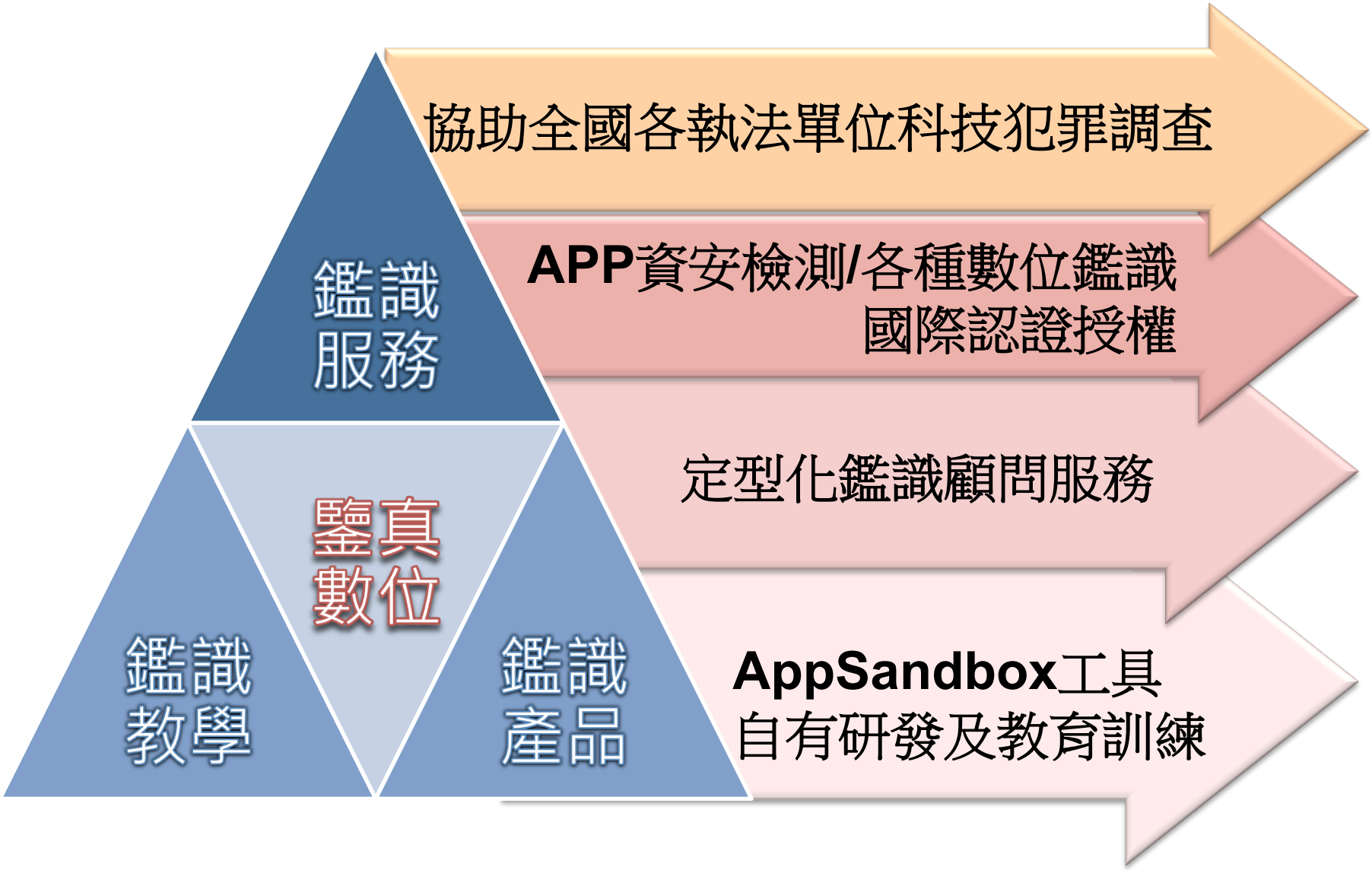
# APP 資通安全檢測服務說明

鑒真數位有限公司
service@iforensics.com.tw
2017/June

# 簡報議程

- 公司簡介
- APP普遍資安現況
- 檢測標準說明
- 鑒真數位檢測技術介紹
- 實驗室簡介

# 鑒真數位【公司簡介】


鑑識服務
鑑識教學
鑑識產品
鑒真數位
協助全國各執法單位科技犯罪調查
APP資安檢測/各種數位鑑識
國際認證授權
定型化鑑識顧問服務
AppSandbox工具
自有研發及教育訓練

# 智慧型手機APP普遍資安現況

# 行動裝置的特性及應考慮之資安問題(行動支付應用為例)


資料來源： ISACA 2015 Mobile Payment Security

# App 普遍基本資安問題說明 (一)

| 項目 | App資安問題描述 |
| --- | --- |
| 1. | App 權限宣告過多及逾越設計所需 |
| 2. | App 本身無沙箱防護機制 |
| 3. | App 憑證綁定/中間人攻擊防護漏洞檢測 |
| 4. | App 程式內發現敏感資料 |
| 5. | App 應用程式Log及Cache有敏感資料 |
| 6. | App 取用敏感資料無告知使用者及提供拒絕選項 |

# App 普遍基本資安問題說明 (二)

| 項目 | App資安問題描述 |
| --- | --- |
| 7. | App 敏感資料儲存不適當且無加密 |
| 8. | App 網路連線加密強度不足 |
| 9. | App 加密金鑰固定及演算法容易遭破解 |
| 10. | App 程式未適當混淆易遭破解 |
| 11. | App 輸入介面未做適當之字串檢查 |
| 12. | App 山寨防護檢測 |

# 行動裝置內建軟體應有的各階段資安稽核

| | | |
|---|---|---|
| 1 | 開發階段 | 程式的安全設計觀念 |
| 2 | 開發階段 | 安全的程式撰寫 |
| 3 | 開發階段 | 第三者程式檢視(避免惡意開發) |
| 4 | 發行前檢測階段 | 滲透測試 |
| 5 | 發行前檢測階段 | 安全的資料貯存(加密) |
| 6 | 發行前檢測階段 | 安全的資料傳輸(加密) |
| 7 | 發行前檢測階段 | 驗證完整憑證鏈及其憑證有效性、金鑰管理 |
| 8 | 發行前檢測階段 | 防止程式碼被逆向反組譯、除錯關閉、沙箱偵測 |
| 9 | 發行前檢測階段 | 敏感性資料保護及使用警示告知、最小權限取用 |
| 10 | 發行前檢測階段 | 使用者端安全認證 |
| 11 | 發行前檢測階段 | 應用程式惡意行為偵測、應用程式竄改偵測… |
| 12 | 發行階段: | 安全的發行、回饋及更新管道… |
| 13 | 發行後的管理階段: | 手機遺失、密碼忘記、舊版停用、舞弊偵測… |

# 檢測標準說明

# 鑒真數位App檢測服務

| | |
|---|---|
| 金融主管機關<br>要求事項 | • 11項（最小權限及存取控制等） |
| 經濟部工業<br>檢測基準 | • 17項（初、中、高級檢測） |
| OWASP | • 10項（Weak Server Side Controls等） |
| 鑒真數位<br>建議項目 | • 資安建議重點選項（5 - 10大項） |

以上均額外提供本公司特有沙箱
檢測報告約100-300頁電子檔

# 工業局：檢測基準安全等級示意

開發商參考之安全安求事項

| 檢測基準安全分級 / 行動應用程式分類 | 初級<br>檢測功能相關之安全性 | 中級<br>檢測連網及認證安全性 | 高級<br>檢測交易相關之安全性 |
|---|---|---|---|
| 第一類<br>純功能性 | ★ | ✓ | ✓ |
| 第二類<br>具認證功能與連網行為 | - | ★ | ✓ |
| 第三類<br>具交易功能<br>(認證功能與連網行為) | - | - | ★ |

★為必要通過之檢測等級　　✓為可自由選擇通過之檢測等級

# 行動應用基本資安檢測基準v2.0

| 五大面向 | 資訊安全技術要求事項 | 第一類 | 第二類 | 第三類 |
|---|---|---|---|---|
| 4.1.1 行動應用程式發布安全 | 行動應用程式發布 | | ✓ | ✓ |
| | 行動應用程式更新 | | 參考項目 | |
| | 行動應用程式安全性問題回報 | | ✓ | ✓ |
| 4.1.2 敏感性資料保護 | 敏感性資料蒐集 | | ✓ | ✓ |
| | 敏感性資料利用 | | 參考項目 | |
| | 敏感性資料儲存 | ✓ | ✓ | ✓ |
| | 敏感性資料傳輸 | | ✓ | ✓ |
| | 敏感性資料分享 | | ✓ | ✓ |
| | 敏感性資料刪除 | | 參考項目 | |
| 4.1.3 付費資源控管安全 | 付費資源使用 | | | ✓ |
| | 付費資源控管 | | | ✓ |
| 4.1.4 身分認證、授權、與連線管理安全 | 使用者身分認證與授權 | | ✓ | ✓ |
| | 連線管理機制 | | ✓ | ✓ |
| 4.1.5 行動應用程式碼安全 | 防範惡意程式碼與避免資訊安全漏洞 | ✓ | ✓ | ✓ |
| | 行動應用程式完整性 | | 參考項目 | |
| | 函式庫引用安全 | | ✓ | ✓ |
| | 使用者輸入驗證 | ✓ | ✓ | ✓ |

# 鑒真數位特有手機檢測技術介紹

# 使用鑑識級MSAB資料擷取暨分析設備(一)
# 可支援的各種主要行動裝置型號

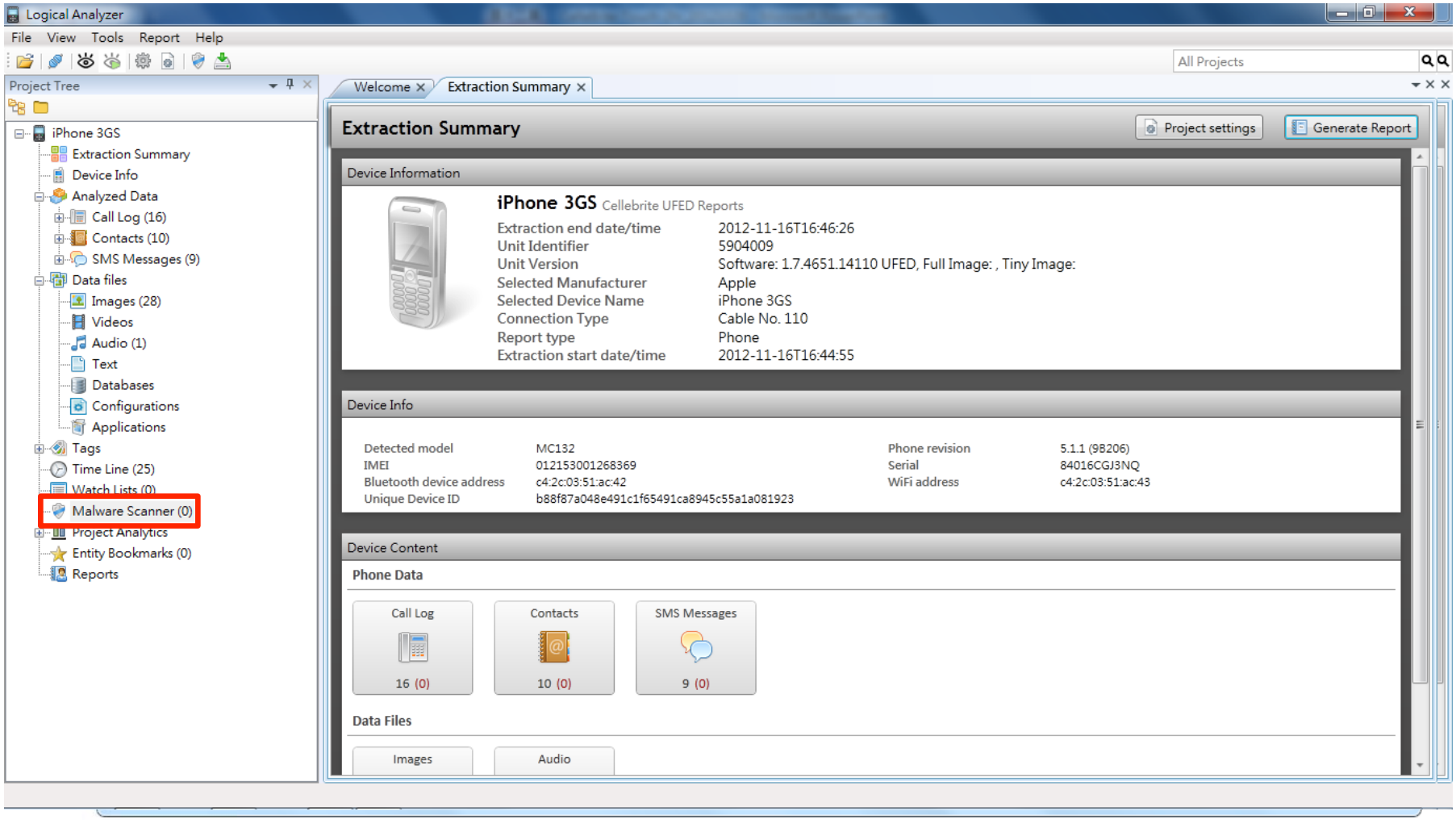
| Forensic Method | Total |
|---|---|
| XRY Logical | 8571 |
| XRY Physical Dumping | 4228 |
| XRY Physical Decoding | 3912 |
| XRY Security Code Only | 2600 |
| XRY Untested | 960 |
| Smartphone Apps | 1600 |
| **Total Device Profiles Supported** | **21871** |

# 使用鑑識級Cellebrite資料擷取暨分析設備(二)
# 強化各種資安漏洞檢測

使用鑑識級資料擷取暨分析設備



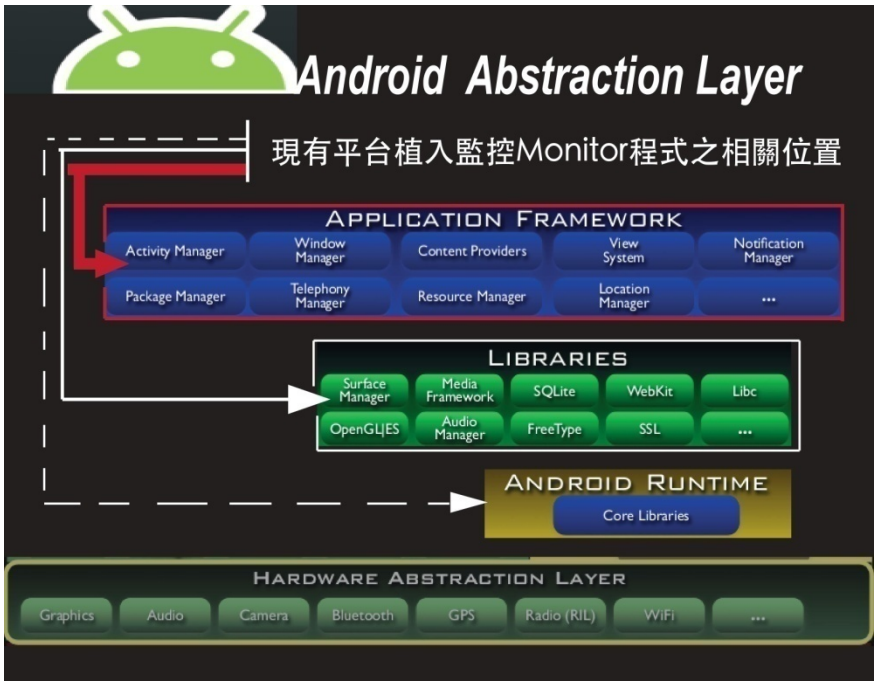
# 採用最新設備:可進行手機系統惡意程式掃描檢測

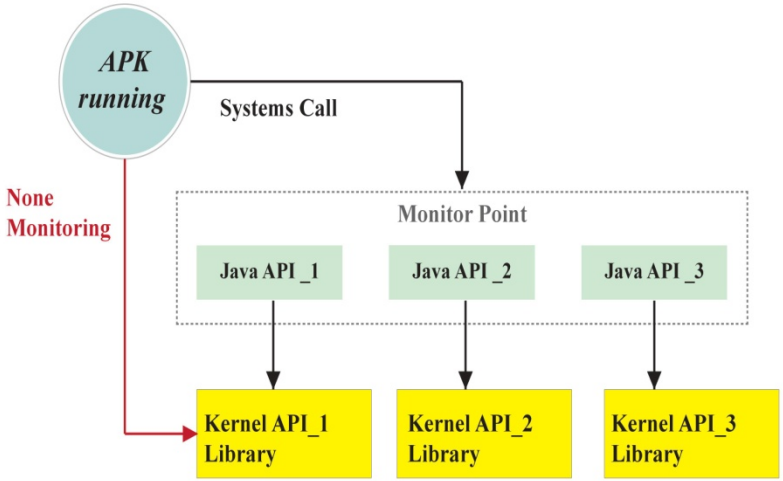


# Android APP檢測技術介紹

# 動態分析：使用多平台監控技術

■使用平台監控點移植技術示意圖及主要問題說明

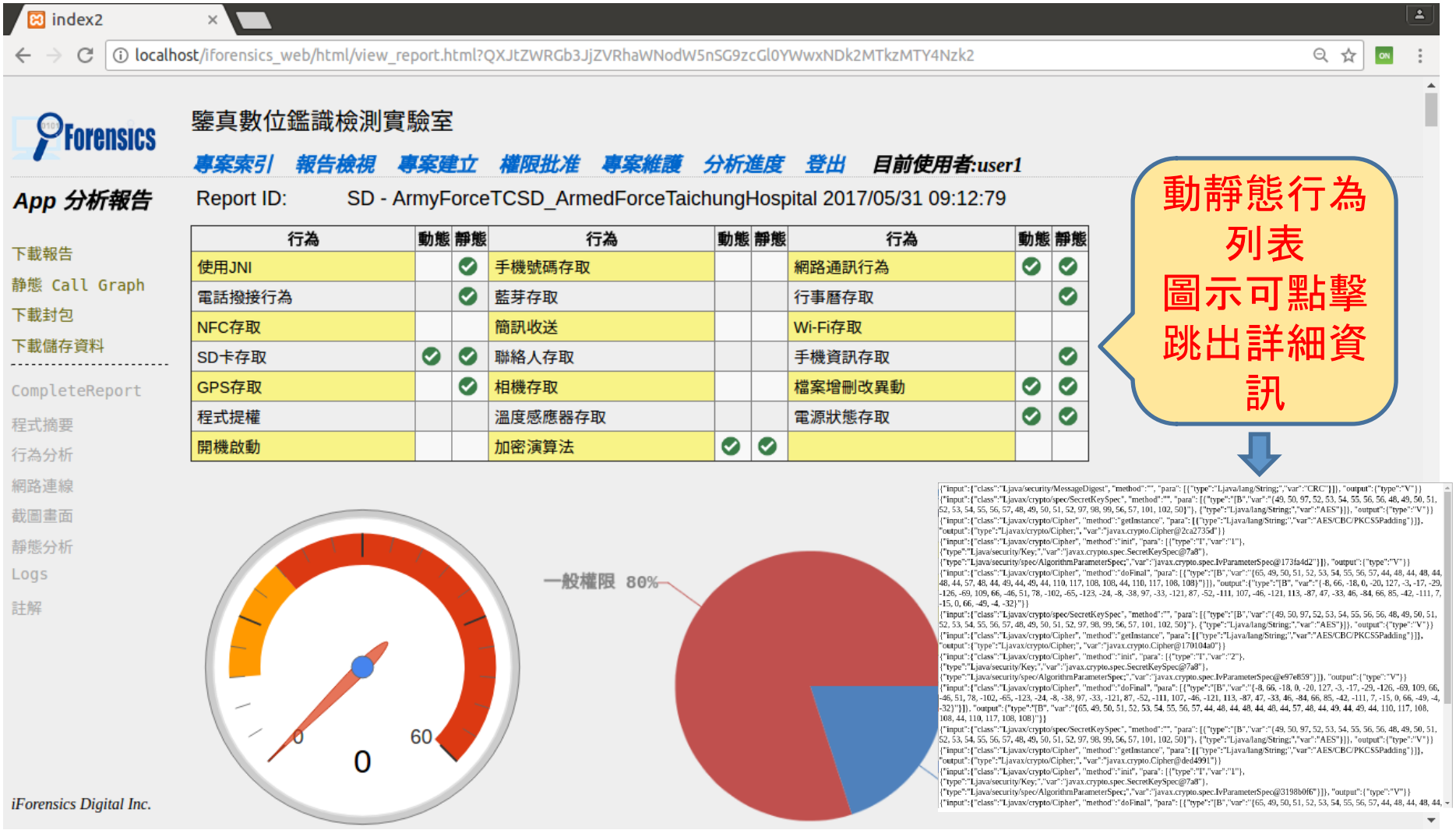



檢測重點:
1.File I/O
2.DB I/O
3.Function Call (傳的參數)
4.Networking

# 提供Android APP檢測沙箱 檢測結果報告

## ■檢測結果報告內容說明



# iOS APP檢測技術介紹

# 鑒真數位-iOS平台內建APP分析之重點

## APP 程式靜態分析

- iOS APP 為加密,必需先脫殼解密才能分析
- iOS 在Appstore 上的APP => xxx.ipa 檔 (可能也有其它檔案格式如 .APP, .PXL,.DEB)
- 可用工具組反組譯至 Object C程式碼
- 可搭配FileSystem Dump比較安裝APP前後的變化

## APP 程式動態行為分析

- iOS APP : 工具套件配置適當已處理之iOS平台硬體並進行 APP
- 使用系統經調校實機

## APP程式所產生的資料分析: DB, Plist, CFG...等

## APP Network 封包分析

- 側錄APP 的傳輸封包 (對於加密封包必需解密才能分析)

# iOS手機檢測工具套件可檢測各種資料型態

■工具套件能達成下列目標

- 可進行系統及APP檔案之擷取
- 可進行任何資料之Hex Code 檢視
- 可進行iOS平台之Plist 資料解析
- 可進行SQLite 資料庫資料解析
- 可進行iOS APP 加殼破密及程式反組譯

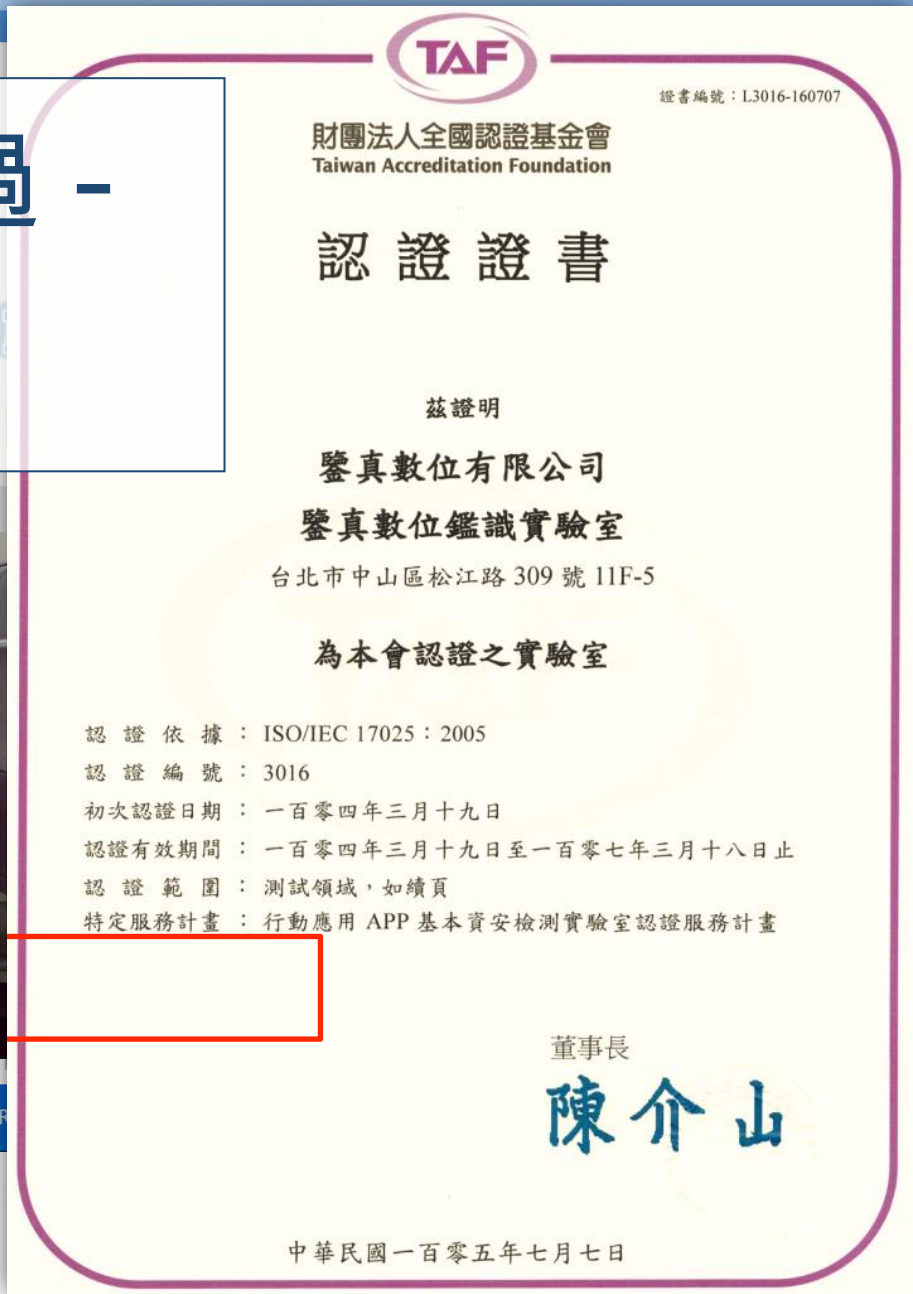
# 實驗室簡介

# 鑒真數位： 從駭客的角度思考手機系統及App資安問題

# 本公司實驗室認證、國際證照

## 2016年7月7日通過 -

## 行動應用App資安檢測

TAF

證書編號：L3016-160707

財團法人全國認證基金會
Taiwan Accreditation Foundation

認 證 證 書

茲證明

鑒真數位有限公司

鑒真數位鑑識實驗室

台北市中山區松江路 309 號 11F-5

為本會認證之實驗室

認 證 依 據 ： ISO/IEC 17025：2005
認 證 編 號 ： 3016
初次認證日期 ： 一百零四年三月十九日
認證有效期間 ： 一百零四年三月十九日至一百零七年三月十八日止
認 證 範 圍 ： 測試領域，如續頁
特定服務計畫 ： 行動應用 APP 基本資安檢測實驗室認證服務計畫

董事長

陳介山

中華民國一百零五年七月七日

# 工業局行動應用資安制度推動委員會
# 2017 檢測實驗室視察-各評委均予肯定


行動應用資安聯盟

視察重點說明:

1. APP 檢測流程檢視
2. 檢測標準暨技術應用
3. 實務通過狀況統計

STAR
Security, Trust & Assurance Registry

# 感謝聆聽、敬請賜教