App 資安檢測服務說明

鑒真數位有限公司

service@iforensics.com.tw

2016 V3

簡報大綱

- 關於鑒真數位
- App資安現況及檢測重要性
- App檢測項目說明
- App資安檢測技術能力說明
- 問題與討論

關於鑒真數位

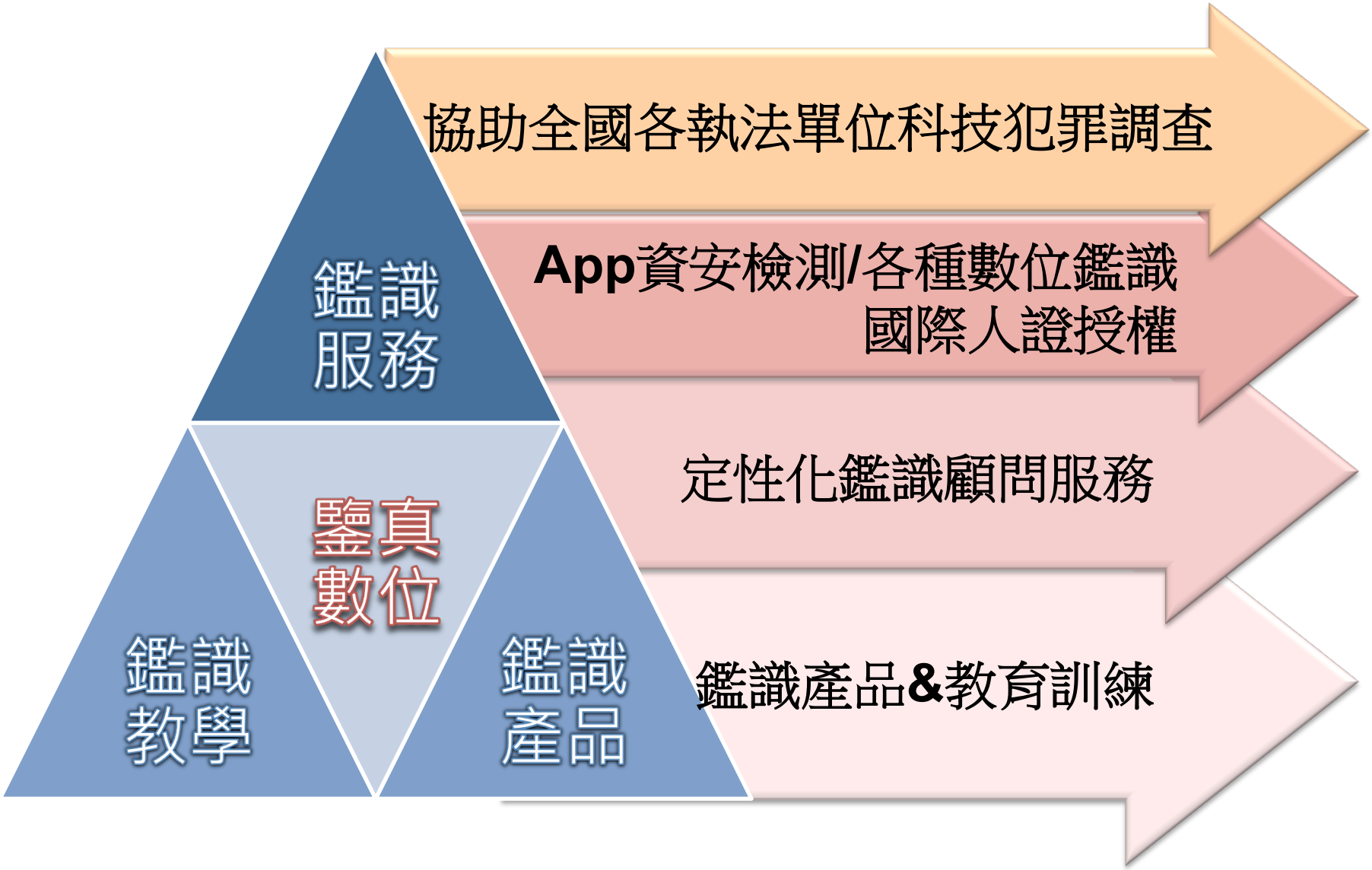
鑒真數位公司介紹

鑒真數位有限公司自民國97年成立以來，即以數位鑑識產業為公司主要營運業務，以全球華人為服務對象的專業「數位證據鑑識」公司。

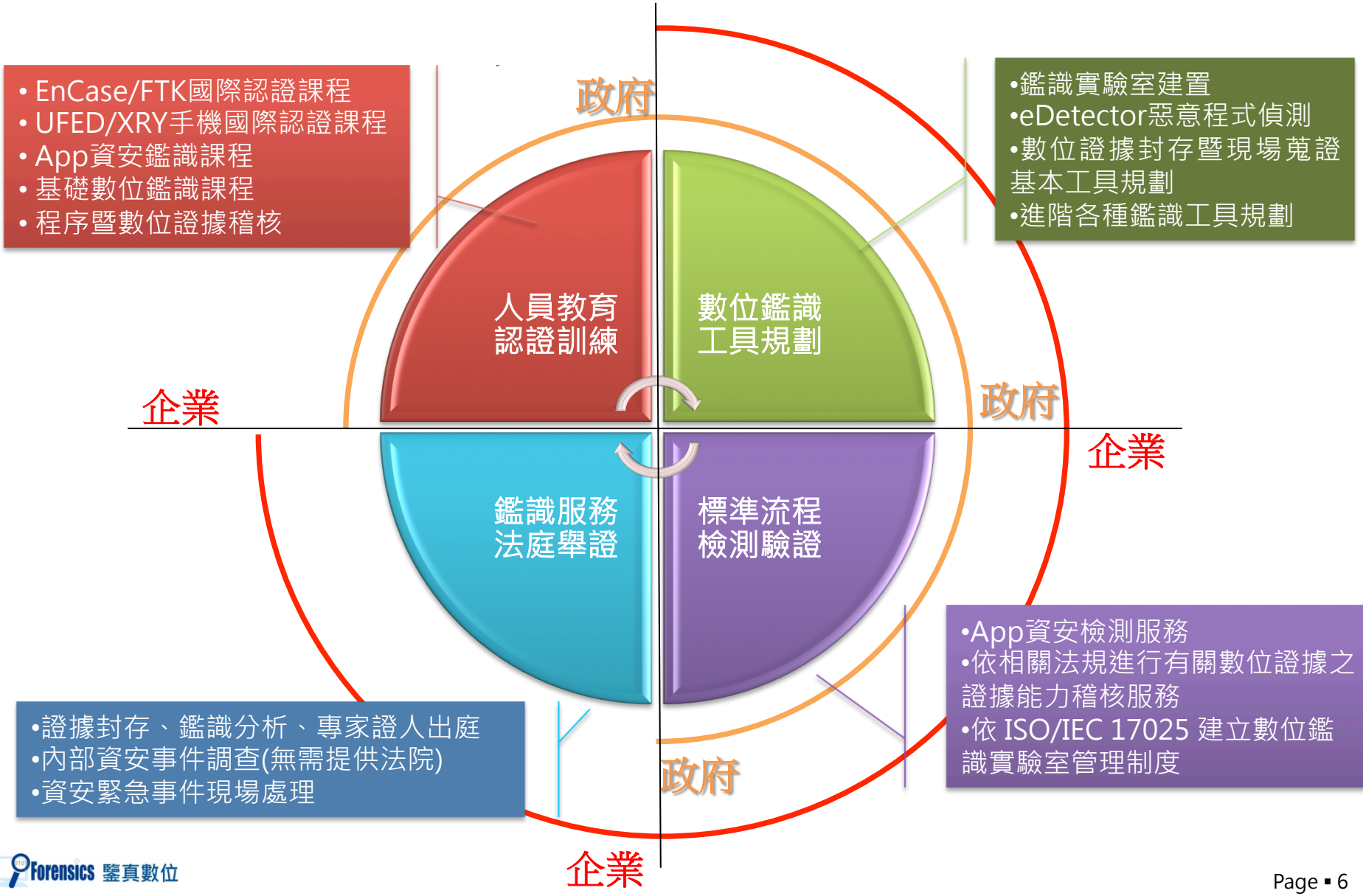
開發專業的數位鑑識及資安檢測軟體，並提供鑑識產品、服務及教育訓練，以進一步協助營利企業、政府、非營利組織和個人在遭遇到智財侵權、駭客入侵、商業洩密、犯罪相關及任何民訴或刑事法律訴訟時所需要在數位證據上的任何技術支援及諮詢服務。

除本身具有專業商用之數位鑑識實驗室外，也協助全國各執法單位或民間公司建立數位鑑識實驗室。

鑒真數位【經營模式】


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
國際人證授權
定性化鑑識顧問服務
鑑識產品&教育訓練

公司主要在數位鑑識服務之四大主軸



鑒真數位專業能力

證照名稱	類別	培訓能力	說明
CCPA Cellebrite Certified Physical Analyst		是，團隊即為講師群	手機鑑識國際認證 （發行國家以色列）
MSAB Micro Systemation		是，團隊即為講師群	手機鑑識國際認證 （發行國家瑞典）
CCE Certified Computer Examiner		是，團隊即為組織成員	科技犯罪調查國際認證 （發行國家美國）
EnCE Encase Certified Computer Examiner		是，團隊即為講師群	數位鑑識調查國際認證 （發行國家美國）
ACE AccessData Computer Examiner		是，團隊即為講師群	數位鑑識調查國際認證 （發行國家美國）

鑒真數位之手機 / 資安鑑識證照【全國民間最多】

編號	名　　稱	取得(核准)日期/字號	國名/機構名稱
1	AccessData BootCamp, Android Analysis	2016.07.27	美國 / AccessData
2	MSAB XRY Advanced Phone Acquisition	2015.11.27	瑞典/XRY
3	MSAB XRY Intermediate forensics Examiner	2014.12.03	瑞典/XRY
4	AmpedFive Image and Video Enhancement Examiner	2014.01.17	義大利/AmpedFive
5	CelleBrite Certificated Instructor	2013.10.01	以色列/CelleBrite
6	FTK BootCamp Certificated Instructor	2013.01.05	美國/AccessData
7	ACE (AccessData Certifid Examiner)	2012.01.08	美國 / AccessData
8	EnCase Certified Examiner	2009.03.31 2011.09.20 2014.06.16	美國 / Guidance Software
9	EnCase Certified Instructor	2011.12.20	美國 / Guidance Software
10	CCE (Certified Computer Examiner	2008.08.04 -982 2013,2013 renew	美國 / ISFCE
11	CEH (Certified Ethical Hacker)	2004.09.17	美國 / EC-Council
12	CEI (Certified EC-Council Instructor)	2005.07.04 2010.06.21 renew	美國 / EC-Council
13	CHFI (Computer Hacking Forensic Investigator)	2005.06.16	美國 / EC-Council
14	CIFI(Certified Information Forensics Investigator)	2008.04.12	美國 /IISFA
15	CISSP	2005.12 / 84397 2006.05 / 90840	美國 / $(ISC)^2$
16	CISA	2009.06.16 / 0975051	美國 / ISACA
17	BS 7799/ISO 27001:2005 Lead Auditor	BSI / TRAIN / ISO27001 / LA011507	英國 / BSI
18	Certified HEX Analysis and CelleBrite Physical Analyzer	2010.04.16	美國 / H-11
19	Certified CelleBrite UFED Mobile Device Examiner	001336	美國 / H-11
20	MCP(Microsoft Certified Professional)	2004	美國 / Microsoft
21	MCSA(Microsoft Certified Systems Administrator)	2004	美國 / Microsoft

2016年7月7日通過 -

行動應用App資安檢測

於我們 ▾ App認證 ▾ 實驗室認證 ▾ 公告專區 ▾

首頁 / 實驗室認證 / 實驗室認證通過名錄

☰ 實驗室認證通過名錄

本名錄係登載由「行動應用App基本資安制度推動委員會」（以下簡稱本委員會）依據工業局公
委員會所認可之「行動應用App基本資安檢測實驗室」。

為確保測試報告之公信力，本委員會建議您，請於委託測試時，要求檢測實驗室出具合格證書。
資安檢測實驗室權利義務規章」(詳附件)。

實驗室認證編號	機構名稱	實驗室名稱	TAF認可日期	聯
3016	鑒真數位有限公司	鑒真數位鑑識實驗室	2016/07/07	
[redacted]	[redacted]	資安科技暨鑑識分析中心	2016/07/07	

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

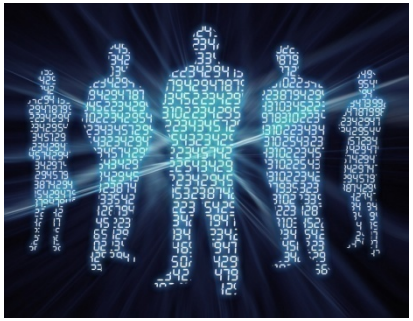
全國【規模最大】商用數位鑑識實驗室

最專業App 鑑識服務:

- 國際手機鑑識大廠

  Cellebrite / XRY 唯一授權台灣教育訓練代理
- 自有檢測沙箱研發
- 定期教授各種App鑑識專業課程

App資安現況及檢測重要性



政府將嚴格要求各金融機關App通過安全檢測

金融業認同 全力補App破網

分享 | G+ 分享 | 留言 | 列印 | 存新聞 | A- A+

2016-04-07 03:01 經濟日報 記者韓化宇／台北報導 讚 分享 19 傳送 G+1 0

金管會清查銀行App是否存有資安漏洞，並要求提高資安防護等級，對此作法，銀行業者皆大表認同。

到底目前的銀行App，是否真的存有資安漏洞？受訪的銀行業者直言，「資安漏洞」是一個相對性的詞彙，假設銀行的App連小學生都駭的進來，那確實可以稱為「漏洞」；但若是被全球最頂尖的駭客組織侵入，是否也能視為「漏洞」？

金融業高層表示，台灣向來是全球駭客入侵最嚴重的地區之一，雖然加強資安管理，要投入更多成本，但「若不先蓋好堤防，一旦洪水淹進來，後果不堪設想」。

業者坦言，駭客防不慎防，資安廠商FireEye報告指出，去年下半年有六成台灣企業成為網路攻擊的目標，且至少遭受18個組織攻擊。銀行App上架前都有請資安公司做檢測，但

http://goo.gl/Jq4aGn

鑒真把關 - 從駭客的角度思考App資安問題

銀行資安風暴2

駭客就在你身邊 銀行app資安危機

app也不安全

一銀事件凸顯金融資安的重要。資安認證業者鑒真數位發現，台灣前二十大國銀app，竟有十一支被查出嚴重資安缺陷。金融資安危機，已經出現在你我身邊。

文・盧沛樺　攝影・陳德信

在網路空間裡，……壞人等於是在我們睡覺的時候已經站在床邊，但大多數人卻依然從容，甚至是對這種威脅一無所知。

～國際刑警組織顧問、《未來的犯罪》作者馬克・古德曼（Marc Goodman）

一銀ATM到底如何被植入惡意程式，迄今檢調仍在調查中。但離我們更切身的的資安危機，已經迫近。

根據《天下雜誌》獨家取得鑒真數位app資安檢定調查，過半在Google Play上架的國銀app，有明顯的資安漏洞，在公用無線上網WiFi環境下，駭客就有機會能竊取用戶的帳號密碼。

鑒真數位是老字號的資安鑑識業者，也是國內少數通過財團法人全國認證基金會（TAF）公告，能做「行動應用app基本資安檢測實驗室」的公司，其客戶包括法務部、調查局。

鑒真數位抽測國內資本額前二十大銀行，在Google Play上架的行動網銀app，共二十支，其中包括六家公股行庫、十四家民間銀行。檢測項目包括四項：憑證綁定、虛擬環境偵測及反制、程式碼混淆、除錯訊息是否含

天下雜誌

本公司報告說明請參考：

鑒真數位Facebook

https://www.facebook.com/iforensics.com.tw/

App檢測項目說明

鑒真數位App檢測服務

金融主管機關 要求事項	• 11項（最小權限及存取控制等）
經濟部工業 檢測基準	• 17項（初、中、高級檢測）
OWASP	• 10項（Weak Server Side Controls等）
鑒真數位 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 檢測功能相關之安全性	中級 檢測連網及認證安全性	高級 檢測交易相關之安全性
第一類 純功能性	★	✓	✓
第二類 具認證功能與連網行為	-	★	✓
第三類 具交易功能 (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	✓	✓	✓

金管會 - 行動裝置應用程式注意事項（將改版）

1	檢視系統所需最小權限，並進行存取控制
2	敏感資料應採取加密或亂碼化等相關機制保護
3	黑箱測試或滲透測試
4	裝置疑似遭破解時，應提示使用者注意風險
5	應提示使用者安裝防毒軟體＝》改測是否App本身遭植入惡意程式
6	應建立可信任憑證清單並驗證完整憑證鏈及其憑證有效性
7	應確認使用者身分，並採用嚴密的技術防護措施
8	應確認行動裝置及應用程式之正確性，並進行端點對端點全程加密防護
9	應確認使用者指定之安全儲存媒介編號，並於SE內增設存取控管
10	技術進行付款交易資料傳輸前，應經由使用者人工確認
11	提供應用程式之名稱、版本與下載位置

App程式山寨植入木馬問題 - 額外檢測項目

App應用程式於執行時應檢視簽章，避免程式被植入惡意程式後於山寨市集發行

檢測發現此部份大多無防制，詐騙盛行！

資安人 INFO SECURITY
作對事、用對方法、找對夥伴

首頁 | 焦點新聞 | 資安知識庫 | 研討會 | 產業快訊 | 個資法專區 | 資安急診室 | 資安

首頁 > 產業快訊

分享

八成Google Play前 50 大熱門免費 App有山寨版 ！

隨著行動裝置使用者數量不斷成長，山寨App數量也以驚人的速度竄升。根據針對Google Play 商店前 50 大熱門免費 App 調查顯示，高達80% 應用程式皆有對應假冒版本，其中以小工具、影片及財經類別App擁有假冒版本的比例竟達100%！趨勢科技建議，為避免行動裝置威脅，使用者請務必從信任的來源下載程式，並安裝有信的行動防護程式如趨勢科技『安全達人』免費App，以保障自身的行動裝置安全。

趨勢科技研究發現，截至2014年四月，在890,482 個山寨App樣本中，有 59,185 是越權廣告程式，另有 394,263 個為惡意程式；而在所有山寨App 中，有 50% 以

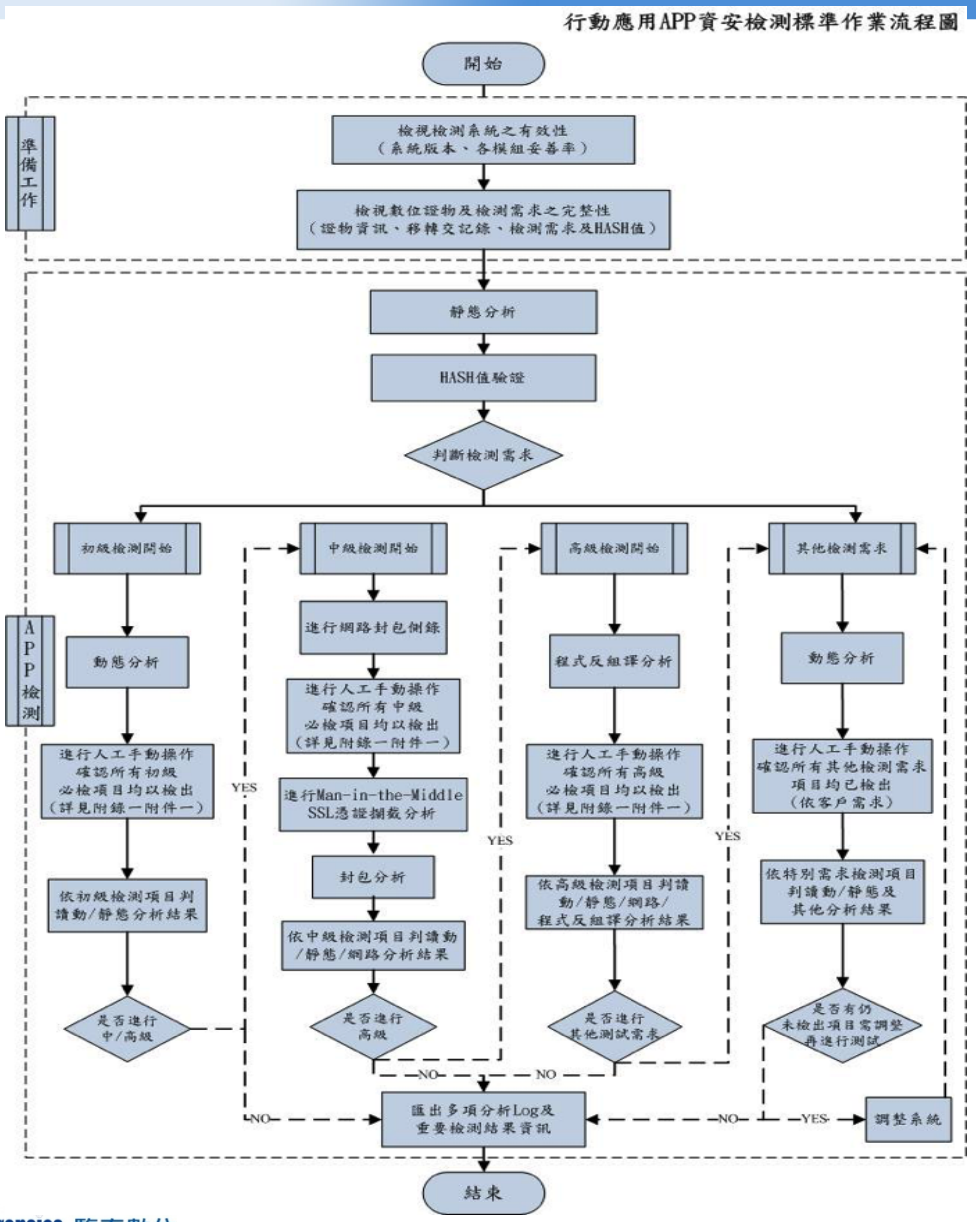
次，該遊戲的突然下架引發網友大量討論，吸引網路犯罪者推出「Flappy Bird」木馬化版本；其中一個木馬化版本會要求使用者允許開發者發送簡訊，導致使用者電信通訊費用帳單因而突然飆高。

金融類App

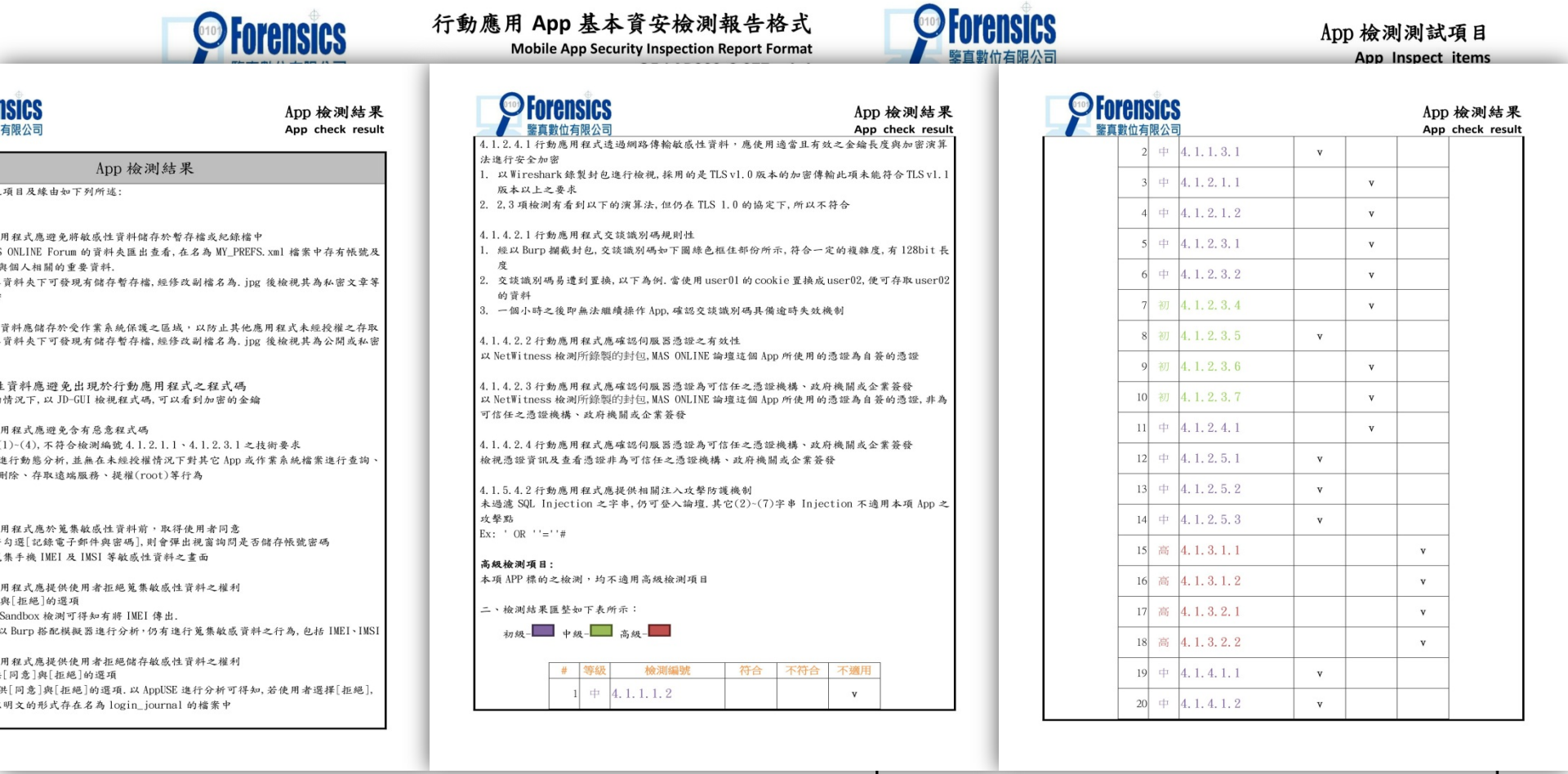
遭木馬化的銀行App常見的被攻擊手法為將知名金融機構的 Google Play 應用程式移除，並換上木馬化版本，竊取受害者的金融相關資訊以協助歹徒發動網路釣魚攻擊，造成使用者重大損失。

http://goo.gl/QcAx6V

ISO 17025 App 檢測標準流程（整合OWASP 項目)



鑑識級檢測報告，可被法院及各檢警單位採用



行動應用 App 基本資安檢測報告格式
Mobile App Security Inspection Report Format

App 檢測測試項目
App Inspect items

App 檢測結果
App check result

App 檢測結果

項目及緣由如下列所述:

用程式應避免將敏感性資料儲存於暫存檔或紀錄檔中
S ONLINE Forum 的資料夾匯出查看，在名為 MY_PREFS.xml 檔案中存有帳號及
與個人相關的重要資料.
資料夾下可發現有儲存暫存檔，經修改副檔名為. jpg 後檢視其為私密文章等

資料應儲存於受作業系統保護之區域，以防止其他應用程式未經授權之存取
資料夾下可發現有儲存暫存檔，經修改副檔名為. jpg 後檢視其為公開或私密

生資料應避免出現於行動應用程式之程式碼
情況下，以 JD-GUI 檢視程式碼，可以看到加密的金鑰

用程式應避免含有惡意程式碼
(1)-(4)，不符合檢測編號 4.1.2.1.1、4.1.2.3.1 之技術要求
進行動態分析，並無在未經授權情況下對其它 App 或作業系統檔案進行查詢、
刪除、存取遠端服務、提權(root)等行為

用程式應於蒐集敏感性資料前，取得使用者同意
句選[記錄電子郵件與密碼]，則會彈出視窗詢問是否儲存帳號密碼
集手機 IMEI 及 IMSI 等敏感性資料之畫面

用程式應提供使用者拒絕蒐集敏感性資料之權利
與[拒絕]的選項
Sandbox 檢測可得知有將 IMEI 傳出.
以 Burp 搭配模擬器進行分析，仍有進行蒐集敏感資料之行為，包括 IMEI、IMSI

用程式應提供使用者拒絕儲存敏感性資料之權利
[同意]與[拒絕]的選項
供[同意]與[拒絕]的選項. 以 AppUSE 進行分析可得知，若使用者選擇[拒絕]，
明文的形式存在名為 login_journal 的檔案中

App 檢測結果
App check result

4.1.2.4.1 行動應用程式透過網路傳輸敏感性資料，應使用適當且有效之金鑰長度與加密演算法進行安全加密
1. 以 Wireshark 錄製封包進行檢視，採用的是 TLS v1.0 版本的加密傳輸此項未能符合 TLS v1.1 版本以上之要求
2. 2,3 項檢測有看到以下的演算法，但仍在 TLS 1.0 的協定下，所以不符合

4.1.4.2.1 行動應用程式交談識別碼規則性
1. 經以 Burp 攔截封包，交談識別碼如下圖綠色框住部份所示，符合一定的複雜度，有 128bit 長度
2. 交談識別碼易遭到置換，以下為例. 當使用 user01 的 cookie 置換成 user02，便可存取 user02 的資料
3. 一個小時之後即無法繼續操作 App，確認交談識別碼具備逾時失效機制

4.1.4.2.2 行動應用程式應確認伺服器憑證之有效性
以 NetWitness 檢測所錄製的封包，MAS ONLINE 論壇這個 App 所使用的憑證為自簽的憑證

4.1.4.2.3 行動應用程式應確認伺服器憑證為可信任之憑證機構、政府機關或企業簽發
以 NetWitness 檢測所錄製的封包，MAS ONLINE 論壇這個 App 所使用的憑證為自簽的憑證，非為可信任之憑證機構、政府機關或企業簽發

4.1.4.2.4 行動應用程式應確認伺服器憑證為可信任之憑證機構、政府機關或企業簽發
檢視憑證資訊及查看憑證非為可信任之憑證機構、政府機關或企業簽發

4.1.5.4.2 行動應用程式應提供相關注入攻擊防護機制
未過濾 SQL Injection 之字串，仍可登入論壇. 其它(2)-(7)字串 Injection 不適用本項 App 之攻擊點
Ex: ' OR ''='' #

高級檢測項目：
本項 APP 標的之檢測，均不適用高級檢測項目

二、檢測結果匯整如下表所示：

初級- 中級- 高級-

#	等級	檢測編號	符合	不符合	不適用
1	中	4.1.1.1.2			v

App 檢測結果
App check result

2	中	4.1.1.3.1	v			
3	中	4.1.2.1.1		v		
4	中	4.1.2.1.2		v		
5	中	4.1.2.3.1		v		
6	中	4.1.2.3.2		v		
7	初	4.1.2.3.4		v		
8	初	4.1.2.3.5	v			
9	初	4.1.2.3.6		v		
10	初	4.1.2.3.7		v		
11	中	4.1.2.4.1		v		
12	中	4.1.2.5.1	v			
13	中	4.1.2.5.2	v			
14	中	4.1.2.5.3	v			
15	高	4.1.3.1.1			v	
16	高	4.1.3.1.2			v	
17	高	4.1.3.2.1			v	
18	高	4.1.3.2.2			v	
19	中	4.1.4.1.1	v			
20	中	4.1.4.1.2	v			

檢測結果：部分初級、中級檢測未通過

檢測起始日期：2016 年 3 月 17 日

檢測完成日期：2016 年 3 月 23 日

聲明事項：本報告內容為機密之資料，非經授權請勿閱讀！

App 送檢之服務流程

1 App案件委託

- 檢測項目說明
- 委鑑需求表
- 報價簽回

2 確認檢測程序及項目及預訂期程

- 委任授權書
- 保密協議書
- 訪談及需求確認

3 App 證物封存

- App 封存
- 製作 App 映像檔

4 檢測分析

- 1.初、中、高級檢測
- 2.金管會要求項目
- 3.Owasp及公司資安重點檢測

5 檢測結果

- 檢測報告

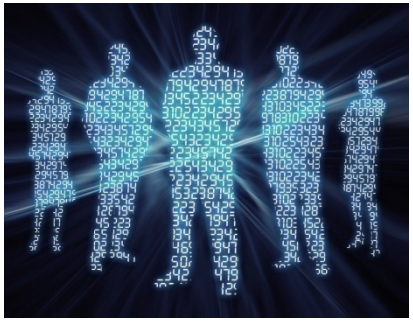
6 專家諮詢/複檢

- App 改善諮詢建議

7 結案

- 出具合格證明／滿意度調查

App資安檢測技術能力說明



本公司研討會發表相關數位鑑識最新技術

2009／2014駭客年會

介紹手機資料救援技術、大陸山寨機破密鑑識案例分享、實體毀損手機晶片取出救援等

2013 ／ 14 Cellebrite行動裝置鑑識研討會

UFED 4 PC 、UFED touch等行動裝置鑑識工具

2015 SecureTech App反組譯技術發表

智慧型手機App反組譯暨封包防駭資安分析

2015 HoneyNet App鑑識

基礎鑑識及鑑識案例分享演講、資安專題演講

駭客年會 - 資安場次教育訓練

台灣駭客年會 HITCON X Training

2014/08/18 09:00 ~ 2014/08/18 17:00 (iCal/Outlook, Google 日曆)

恆逸上課教室 / 台北市復興北路99號14樓

主辦單位 台灣駭客年會 HITCON

聯絡主辦單位

- **課程五：**

EnCase Enterprise 駭客入侵暨商業侵權實務調查

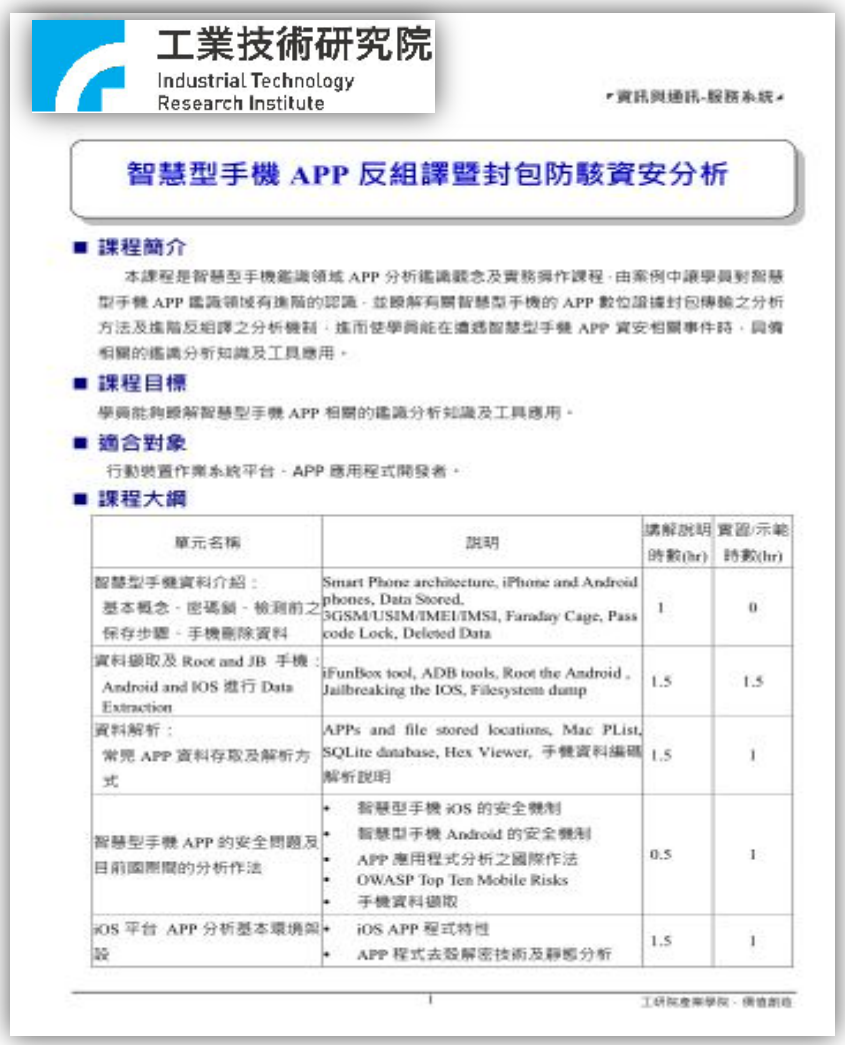
- **課程六：**

如何整合並自製**APT**惡意程式調查工具

App鑑識相關課程持續授課

鑒真數位2016年教育訓練時程表						
月份	日期	天數	課程名稱	類別	課程編號	課程費用/每人
1月	15	1	數位鑑識現場處理	數位鑑識基礎	GE01	$12,000
1月	18	1	AmpedFive影像強化鑑識	影像鑑識	VD01	$12,000
1月	19.20	2	資安緊急應變惡意程式鑑識教育訓練	資安鑑識	NM02	$24,000
1月	28.29	2	智慧型手機鑑識教育訓練	智慧型手機鑑識	SP01	$26,000
2月	19	1	智慧型手機破密	智慧型手機鑑識	SP02	$12,000
2月	25.26	2	網路鑑識及惡意程式分析(含記憶體分析及Sandbox分析)	資安鑑識	NM01	$24,000
3月	02.03.04	3	AccessData原廠授權認證課程 FTK BootCamp (含ACE認證考試)	國際數位鑑識認證	AF01	$70,000
3月	07.08	2	數位(電腦)鑑識實務案例調查教育訓練	數位鑑識基礎	IF02	$26,000
3月	14.15	2	智慧型手機APP反組譯暨傳輸封包鑑識分析	智慧型手機鑑識	PW01	$24,000
3月	21.22.23.24	4	Guidance原廠授權認證課程EnCase Computer Forensic I (CF1)	國際數位鑑識認證	GE01	$75,000
3月	28.29.30.31	4	Guidance原廠授權認證課程EnCase Computer Forensic II (CF2)	國際數位鑑識認證	GE02	$75,000
4月	06.07.08	3	專業手機暨硬碟資料救援教育訓練課程	資料救援	ID01	$38,000
4月	13.14.15	3	AccessData Android Forensic認證	國際數位鑑識認證	AF02	$75,000
4月	22	1	數位(電腦)鑑識現場處理教育訓練	現場蒐證	IF01	$12,000
4月	27.28.29	3	AccessData原廠授權認證課程 FTK BootCamp (含ACE認證考試)	國際數位鑑識認證	AF01	$70,000
5月	03.04.05.06	4	Guidance原廠授權認證課程EnCase Computer Forensic I (CF1)	國際數位鑑識認證	GE01	$75,000
5月	03.04.05.06	4	Guidance原廠授權認證課程EnCase Computer Forensic II (CF2)	國際數位鑑識認證	GE02	$75,000
5月	12.13	2	原廠認證 XRY Certification Smart Phone Training	國際手機鑑識認證	XPA02	$72,000
5月	18.19.20	3	原廠認證Cellebrite Certified Physical Analyst (CCPA)	國際手機鑑識認證	CCPA01	$75,000
5月	25.26.27	3	智慧型手機破密暨手機APP分析教育訓練	智慧型手機鑑識	PW02	$38,000
5月	30.31	2	網路鑑識及惡意程式分析(含記憶體分析及Sandbox分析)	資安鑑識	NM01	$24,000
6月	06.07.08	3	AccessData原廠授權認證課程 Android Forensic	國際數位鑑識認證	AF03	$75,000
6月	13.14.15	3	Guidance原廠授權認證課程EnCase Computer Forensic I (CF1)	國際數位鑑識認證	GE03	$60,000
6月	16	1	AccessData ACE 認證考試 Preparation 課程	國際數位鑑識認證	AF02	$15,000
6月	17	1	數位(電腦)鑑識現場處理教育訓練	現場蒐證	IF01	$12,000
6月	20.21.22.23	4	Guidance原廠授權認證課程EnCase Computer Forensic I (CF1)	國際數位鑑識認證	GE01	$75,000
6月	27.28.29	3	原廠認證XRY Smart Phone Training	國際手機鑑識認證	XPA01	$75,000
7月	14.15	2	數位(電腦)鑑識基礎教育訓練	數位鑑識基礎	IF02	$24,000
7月	20.21.22	3	專業手機暨硬碟資料救援教育訓練課程	資料救援	ID01	$38,000
7月	26.27.28.29	4	Guidance原廠授權認證課程EnCase Computer Forensic II (CF2)	國際數位鑑識認證	GE02	$75,000
8月	03.04	2	智慧型手機鑑識教育訓練	智慧型手機鑑識	SP01	$26,000
8月	10.11.12	3	AccessData原廠授權認證課程 FTK BootCamp (含ACE認證考試)	國際數位鑑識認證	AF01	$70,000
8月	23.24.25.26	4	Guidance原廠授權認證課程EnCase Computer Forensic I (CF1)	國際數位鑑識認證	GE01	$75,000
9月	5.6	2	網路鑑識及惡意程式分析(含記憶體分析及Sandbox分析)	資安鑑識	NM01	$24,000
9月	21.22.23	3	原廠認證Cellebrite Certified Physical Analyst (CCPA)	國際手機鑑識認證	CCPA01	$75,000
9月	30	1	智慧型手機破密	智慧型手機鑑識	SP02	$12,000
10月	12.13.14	3	AccessData原廠授權認證課程 Android Forensics	國際數位鑑識認證	AF02	$75,000
10月	25.26.27.28	4	Guidance原廠授權認證課程EnCase Computer Forensic I (CF1)	國際數位鑑識認證	GE01	$75,000
11月	15.16.17.18	4	Guidance原廠授權認證課程EnCase Computer Forensic II (CF2)	國際數位鑑識認證	GE02	$75,000
11月	23.24.25	3	AccessData原廠授權認證課程 FTK BootCamp (含ACE認證考試)	國際數位鑑識認證	AF01	$70,000
12月	05.06.07	3	EnCase EnCE 認證考試 Preparation 課程	國際數位鑑識認證	GE03	$60,000
12月	12	1	AccessData ACE 認證考試 Preparation 課程	國際數位鑑識認證	AF02	$15,000
12月	14.15.16	3	專業手機暨硬碟資料救援教育訓練課程	資料救援	ID01	$38,000

鑒真數位2016年預計開立之教育訓練					
	天數	課程名稱	類別	課程編號	課程費用/每人
依報名人數不定期開班	4	X-ways鑑識軟體教育訓練課程	國際數位鑑識認證	XWAY01	$80,000
	5	CCE進階數位鑑識課程	國際數位鑑識認證	CCE01	$150,000
	5	AmpedFive原廠影像鑑識課程	國際影像鑑識認證	$95,000	$95,000



工業技術研究院
Industrial Technology Research Institute

資訊與通訊-服務系統

智慧型手機 APP 反組譯暨封包防駭資安分析

■ 課程簡介

本課程是智慧型手機鑑識領域 APP 分析鑑識觀念及實務操作課程，由案例中讓學員對智慧型手機 APP 鑑識領域有進階的認識，並瞭解有關智慧型手機的 APP 數位證據封包傳輸之分析方法及進階反組譯之分析機制，進而使學員能在遭遇智慧型手機 APP 資安相關事件時，具備相關的鑑識分析知識及工具應用。

■ 課程目標

學員能夠瞭解智慧型手機 APP 相關的鑑識分析知識及工具應用。

■ 適合對象

行動裝置作業系統平台、APP 應用程式開發者。

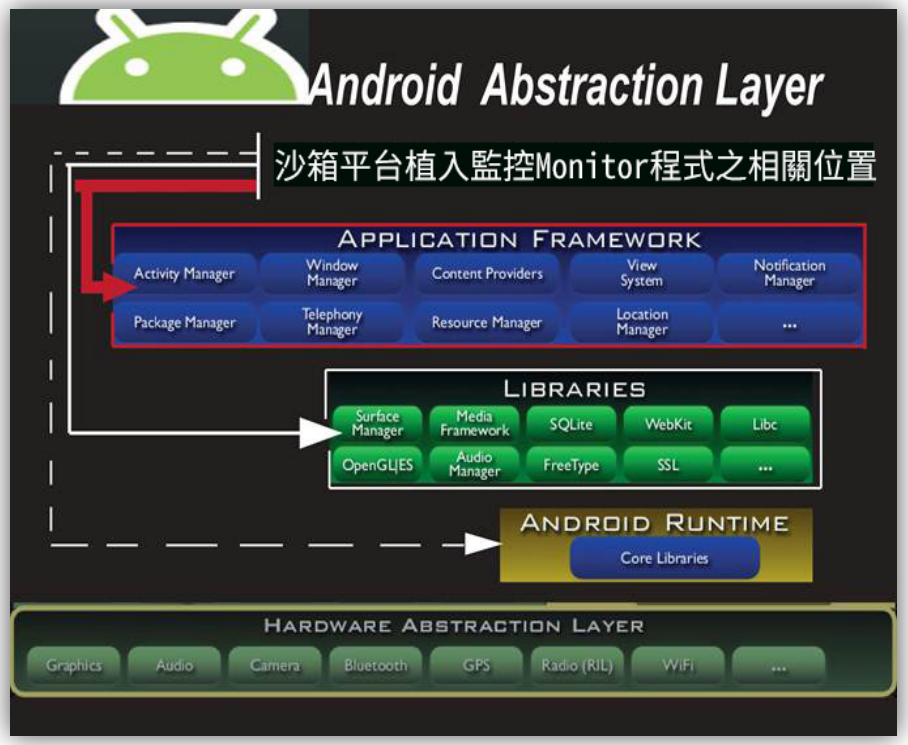
■ 課程大綱

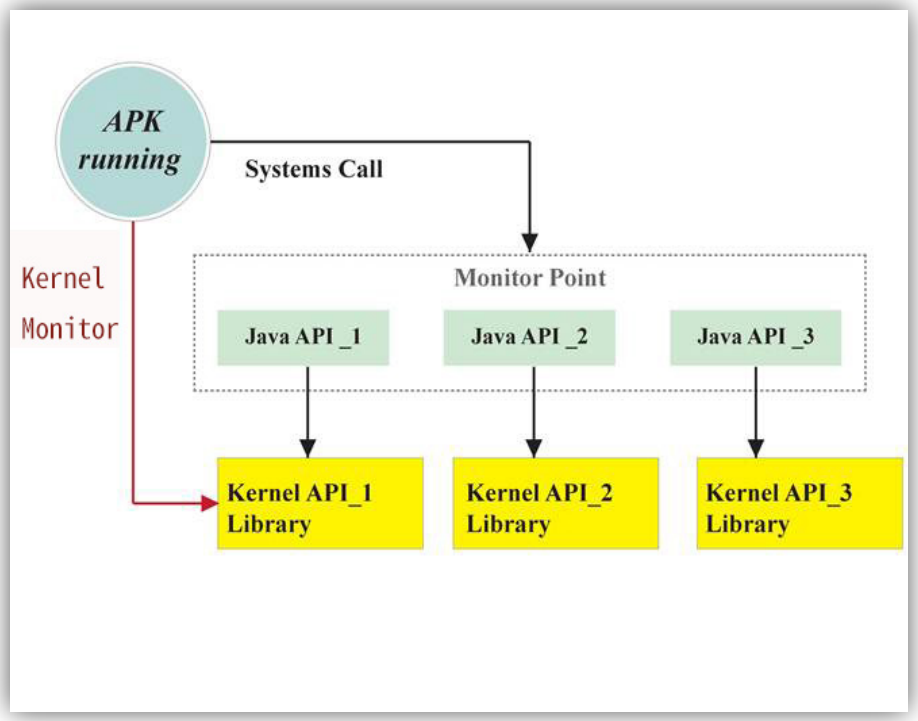
單元名稱	說明	講解說明時數(hr)	實習/示範時數(hr)
智慧型手機資料介紹：基本概念、密碼鎖、檢測前之保存步驟、手機刪除資料	Smart Phone architecture, iPhone and Android phones, Data Stored, 3GSM/USIM/IMEI/IMSI, Faraday Cage, Pass code Lock, Deleted Data	1	0
資料擷取及 Root and JB 手機：Android and IOS 進行 Data Extraction	iFunBox tool, ADB tools, Root the Android, Jailbreaking the IOS, Filesystem dump	1.5	1.5
資料解析：常見 APP 資料存取及解析方式	APPs and file stored locations, Mac PList, SQLite database, Hex Viewer, 手機資料編碼解析說明	1.5	1
智慧型手機 APP 的安全問題及目前國際間的分析作法	• 智慧型手機 iOS 的安全機制 • 智慧型手機 Android 的安全機制 • APP 應用程式分析之國際作法 • OWASP Top Ten Mobile Risks • 手機資料擷取	0.5	1
iOS 平台 APP 分析基本環境架設	• iOS APP 程式特性 • APP 程式去殼解密技術及靜態分析	1.5	1

1

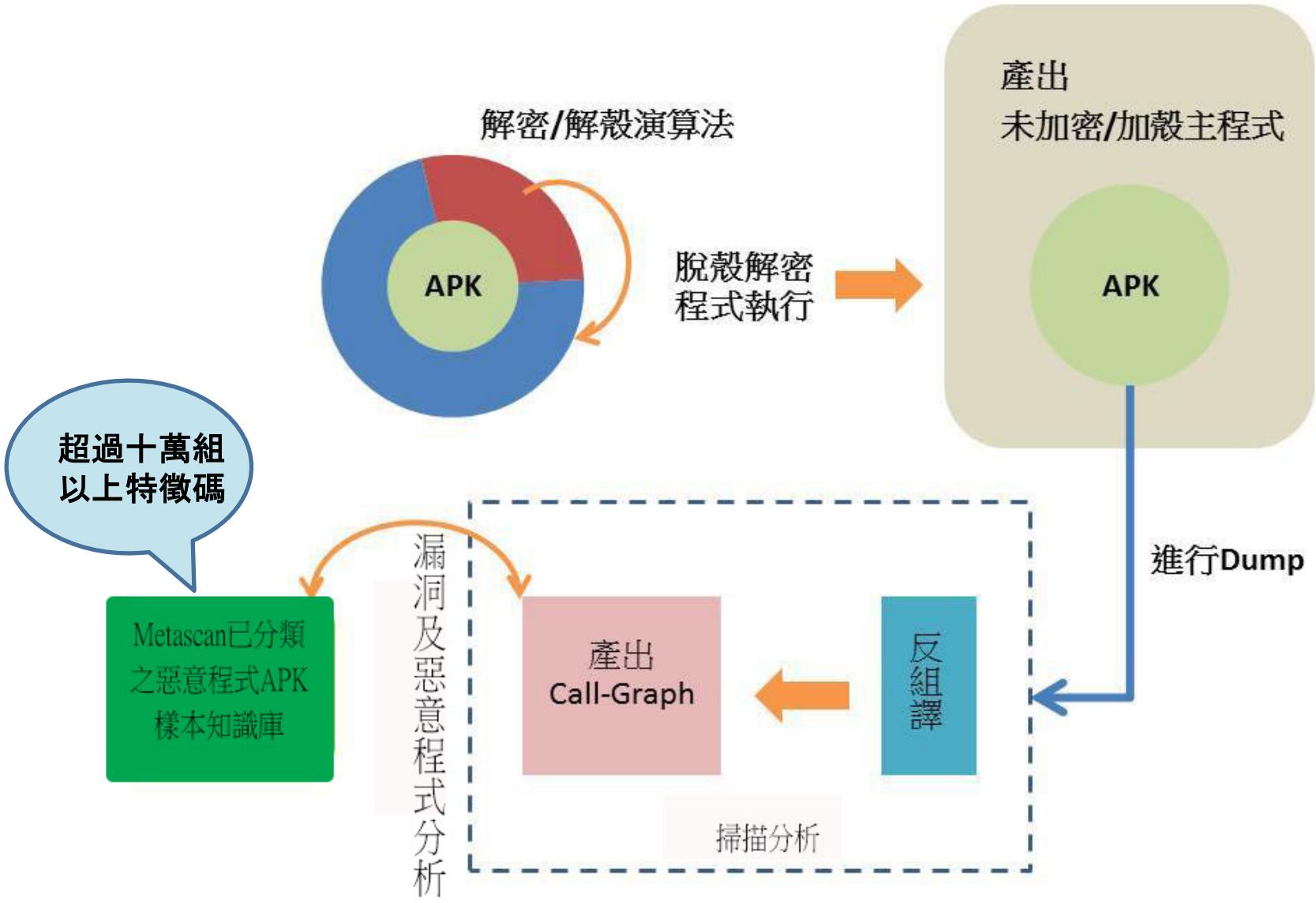
工研院產業學院 - 價值創造

iForensics自有研發 Sandbox 檢測技術





特有APP加殼程式分析技術說明



公司參考客戶


達文西個資暨高科技法律事務所
Personal Data and High-Tech Law Firm


理律法律事務所
LEE AND LI
ATTORNEYS-AT-LAW


萬國法律事務所
Formosa Transnational
Attorneys at Law


MEDIATEK


tsmc


FAREASTONE
遠傳


htc
quietly brilliant


中華電信


國立臺灣大學
National Taiwan University


中華民國國防部
Ministry of National Defense R.O.C.


NARLabs 國家實驗研究院
國家高速網路與計算中心
National Center for High-performance Computing


中央警察大學
誠
CENTRAL POLICE UNIVERSITY


HFU
華梵大學


NCCST
國家資通安全科技中心
National Center for Cyber Security Technology


國家通訊傳播委員會
NATIONAL COMMUNICATIONS COMMISSION


刑事警察局
CRIMINAL INVESTIGATION BUREAU


法務部
廉政署
AGENCY AGAINST CORRUPTION

目前已提供資安初檢之金融單位

永豐銀行 Bank SinoPac

中國信託銀行 CTBC BANK

臺灣銀行 BANK OF TAIWAN

國泰世華銀行 Cathay United Bank

台新銀行

日盛金控 日盛銀行

台北富邦銀行

玉山銀行 E.SUN BANK

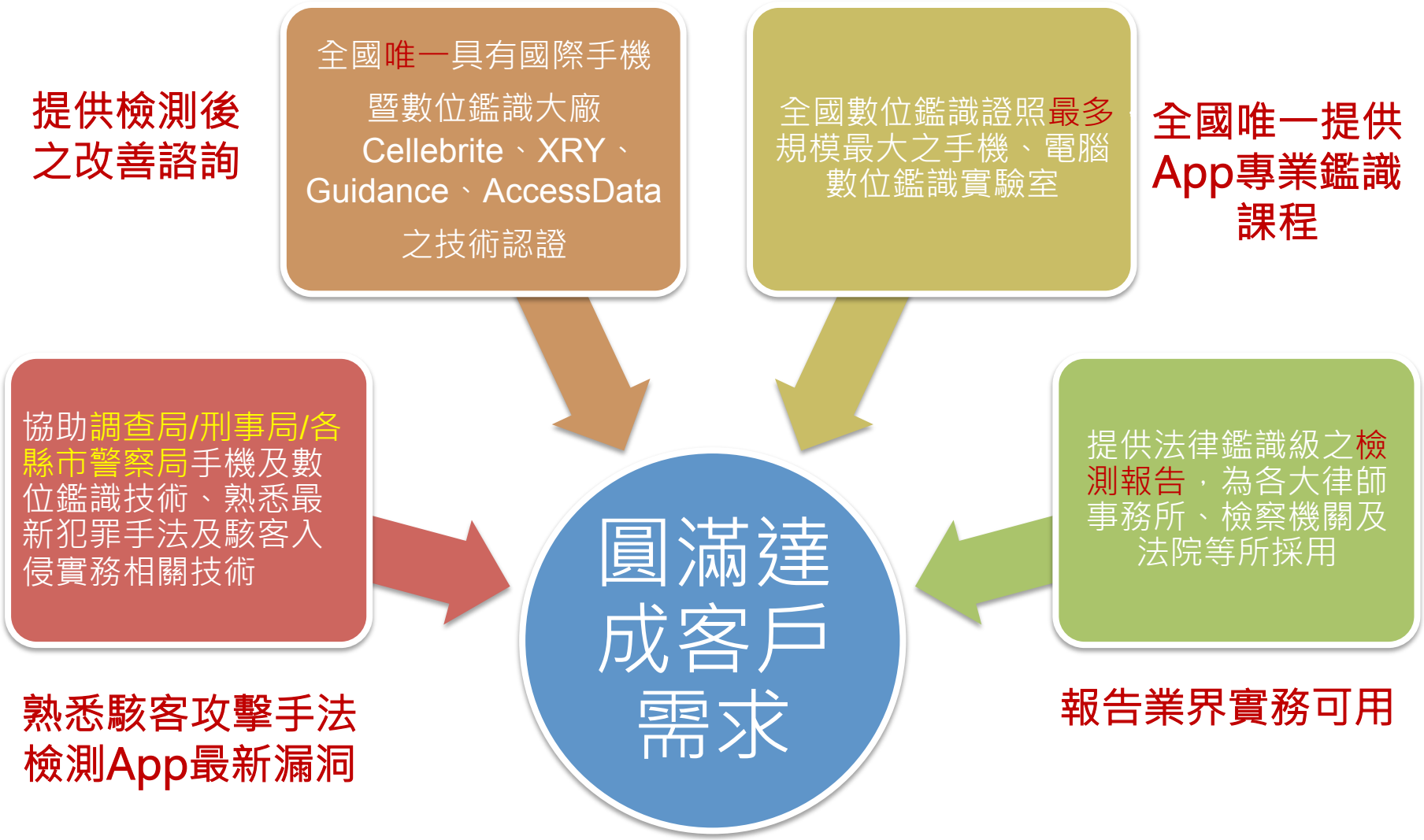
兆豐國際商業銀行 Mega International Commercial Bank

第一銀行 First Bank

5大項App 資安漏洞檢測 - 現場提供10名免費

項目	App資安問題描述
1.	App 權限內容安全分析檢測
2.	App 沙箱防護機制分析檢測
3.	App 憑證攻擊防護漏洞檢測
4.	App 程式反組譯分析機制防護漏洞檢測
5.	App 應用程式Debug安全漏洞檢測

為何選擇鑒真數位公司


提供檢測後之改善諮詢
全國唯一具有國際手機暨數位鑑識大廠Cellebrite、XRY、Guidance、AccessData之技術認證
全國數位鑑識證照最多規模最大之手機、電腦數位鑑識實驗室
全國唯一提供App專業鑑識課程
協助調查局/刑事局/各縣市警察局手機及數位鑑識技術、熟悉最新犯罪手法及駭客入侵實務相關技術
圓滿達成客戶需求
提供法律鑑識級之檢測報告，為各大律師事務所、檢察機關及法院等所採用
熟悉駭客攻擊手法檢測App最新漏洞
報告業界實務可用

感謝聆聽、敬請賜教