出手偷摸
摸透iOS app 原來那麼簡單！

Hacks in Taiwan Conference 台灣駭客年會
HITCON X Playground

何宜霖 L1oHo

#whoamI

- 何宜霖 L1oHo
  L1o.ho.sec@gmail.com
- 曾經
  擔任 某資安公司 工讀生
- 現今
  華梵大學
  數位鑑識實驗室 努畢生

#whoamI

- **專長**
  iOS安全檢測
  數位鑑識處理
  駭客攻擊手法

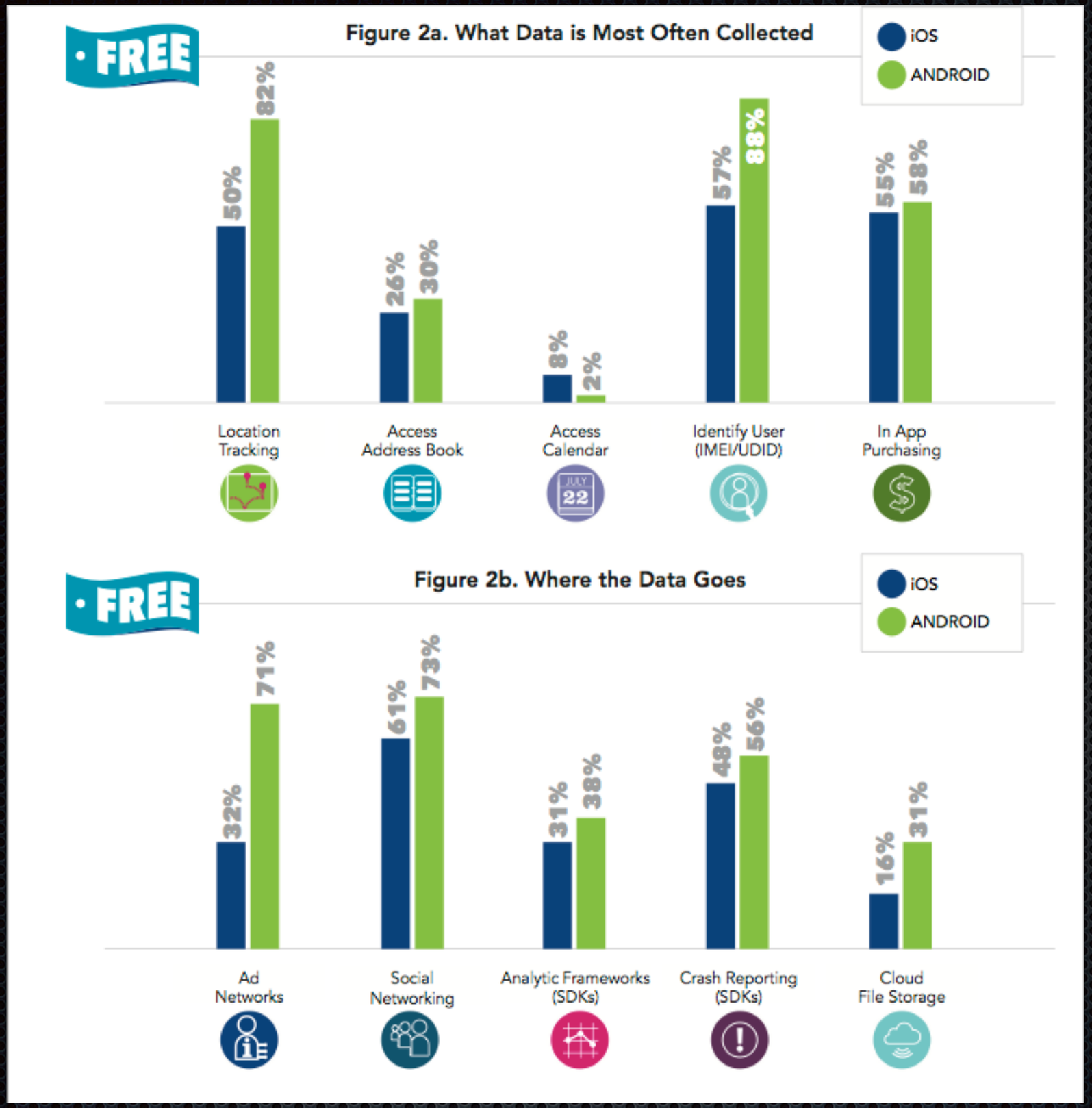
- **協助檢測**
  金融單位App
  通訊軟體App
  遊戲App

- **相關證照**
  Certificated Ethical Hacker
  Computer Hacking Forensic Investigator
  ISO 27001 / ISO 20000 / BS 10012

2005

2013

以往都是從新聞事件開始...



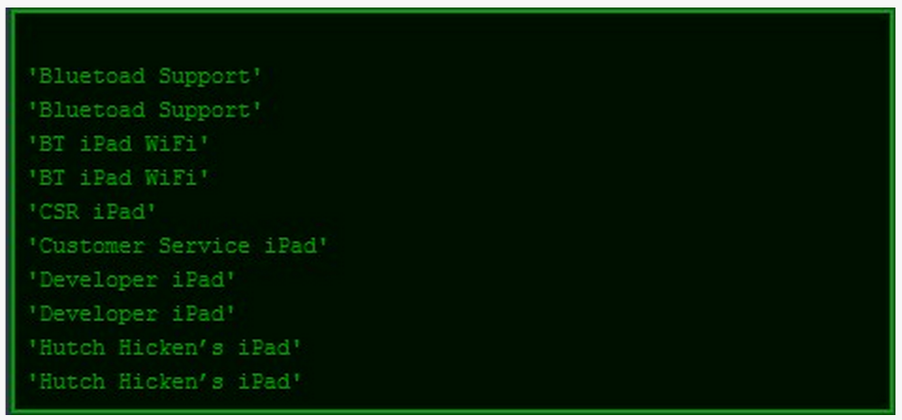
App超愛 You的隱私

https://www.appthority.com/app-reputation-report/report/AppReputationReportSummer14.pdf

蘋果百萬筆UDID資料外洩元凶是iOS App開發商

Intrepidus Group資料鑑識專家發現多筆資料內含有Blue Toad一詞或相關詞，於是決定通知該公司。BlueToad雖然藉藉無名，但該公司的技術卻可能接觸到上百萬名使用者資料。它為6000多家出版商提供數位出版和應用建置服務，每月處理的網頁瀏覽率高達1億頁。

文/ 林妍溱 | 2012-09-11 發表



資料鑑識專家發現到洩露源頭指向iOS App開發商Blue Toad。

上周駭客宣稱自FBI筆電取得上千萬筆蘋果裝置的UDID資料之後，經資料鑑識專家追查，發現iOS的數位出版開發商Blue Toad嫌疑重大，Blue Toad執行長Paul DeHart並已向媒體坦承，資料確實是該公司所洩露。

上周自稱是AntiSec成員的駭客宣稱自FBI取得高達1200筆蘋果用戶裝置辨識號

不良開發商
導致Your隱私被看透

http://www.ithome.com.tw/node/76120

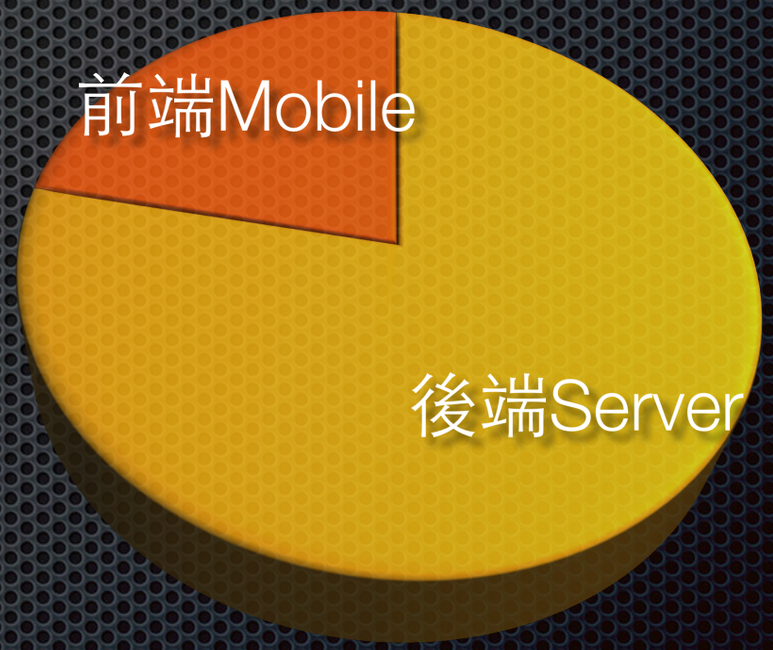
你知道有幾個人在看你嘛？

今天來聊

iOS app全身檢查的方法

app現況疾病檢查方法

- 只針對後端安全去檢測
  - 檢測方法，跟以往一樣
  - 檢測的工具，可以沿用
- 前端mobile檢測技術，資訊太少
  - 前端檢測工具並不多



OWASP

世界衛生組織

為了降低app罹癌提供最高指導準則

OWASP Top Ten Mobile Risks

OWASP Top Ten Mobile Risks 最新版本 2014 RC 1

常見的故事

M1

Weak Server Side Controls

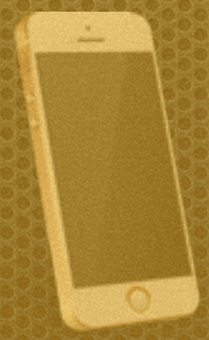
伺服器端安全控制脆弱

IPC

網路傳輸

後端伺服器

App傳輸資料
儲存



實體偷取

常見的故事

M2

Insecure Data Storage

不安全的資料儲存於用戶端

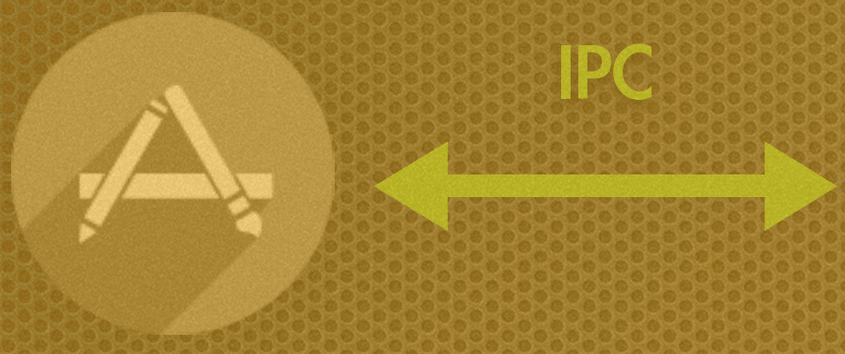
M6

Broken Cryptography

加密方法不嚴謹或失效 。

使用者輸入

IPC



後端伺服器

App傳輸資料
儲存

實體偷取

常見的故事

M3

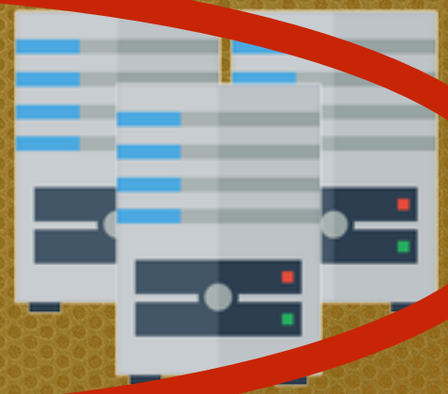
Insufficient Transport Layer Protection

傳輸層保護不足

使用者輸入

IPC

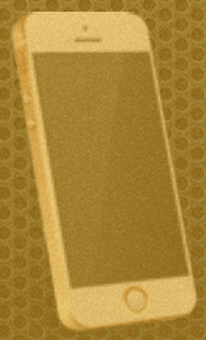
網路傳輸



後端伺服器

App傳輸資料儲存

實體偷取



常見的故事

M4

Unintended Data Leakage

非故意/意外造成資料外洩。

M8

Security Decisions Via Untrusted Inputs

對於不受信任輸入來源的檢測處置。

M10

Lack of Binary Protections

封裝檔案保護不足。

常見的故事

M5

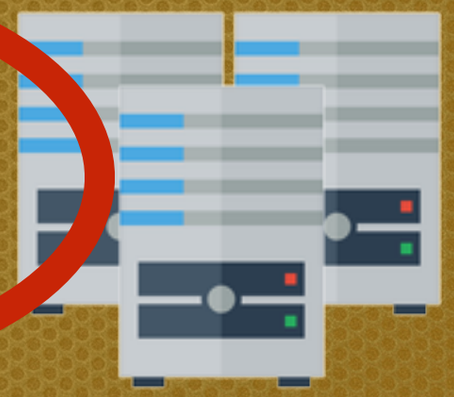
Poor Authorization and Authentication

身分鑑別與授權機制不嚴謹。

使用者輸入

IPC

網路傳輸



後端伺服器

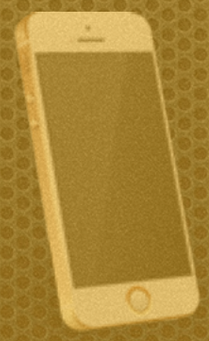
M9

Improper Session Handling

連線階段處理不適當。

App傳輸資料
儲存

實體偷取



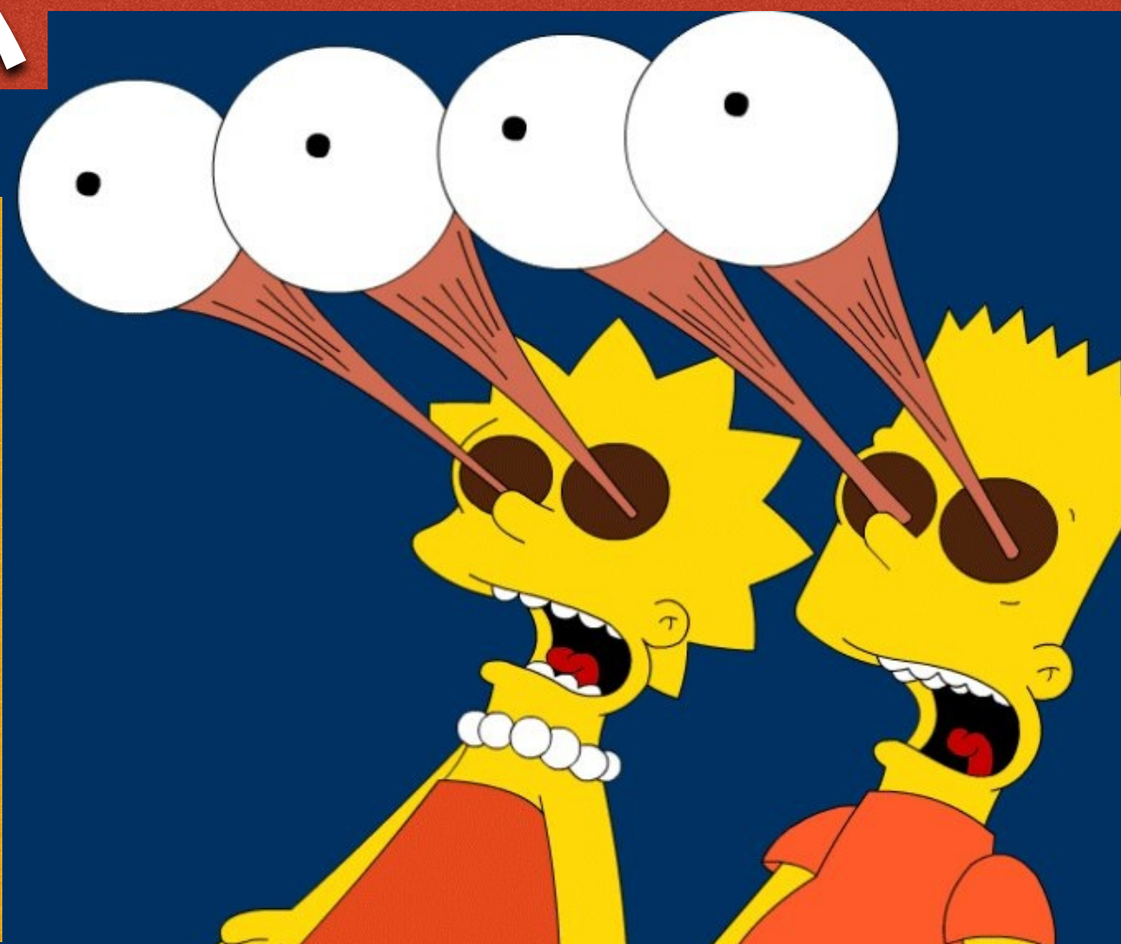
自己用App自己摸

「讓你親自動手摸，摸的的開心，摸的自然。」

靜態

操法

動態



檢測準備

iDevice JailBroken

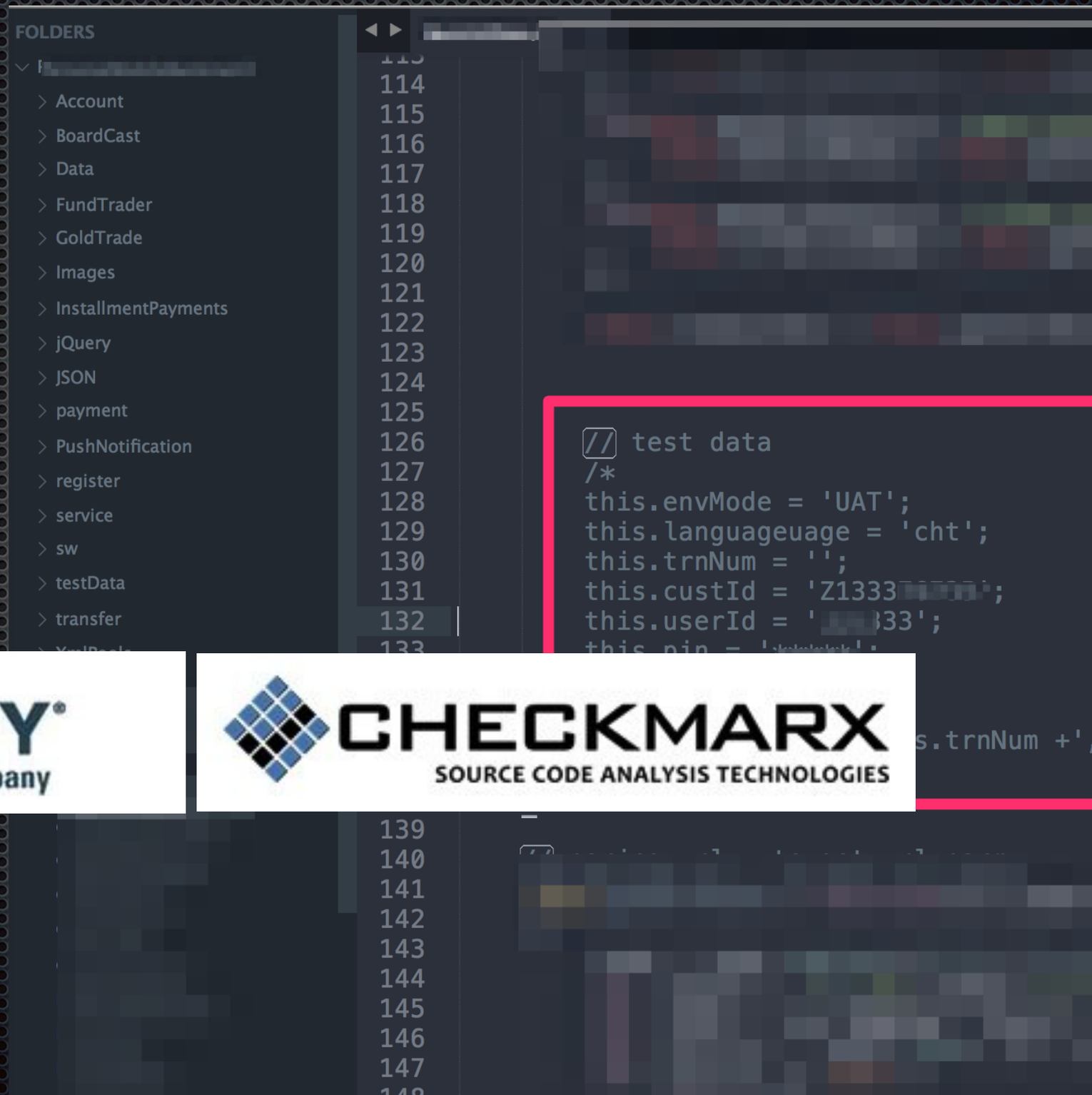
Sniffer Packet

靜態

摸法

靜態檢測

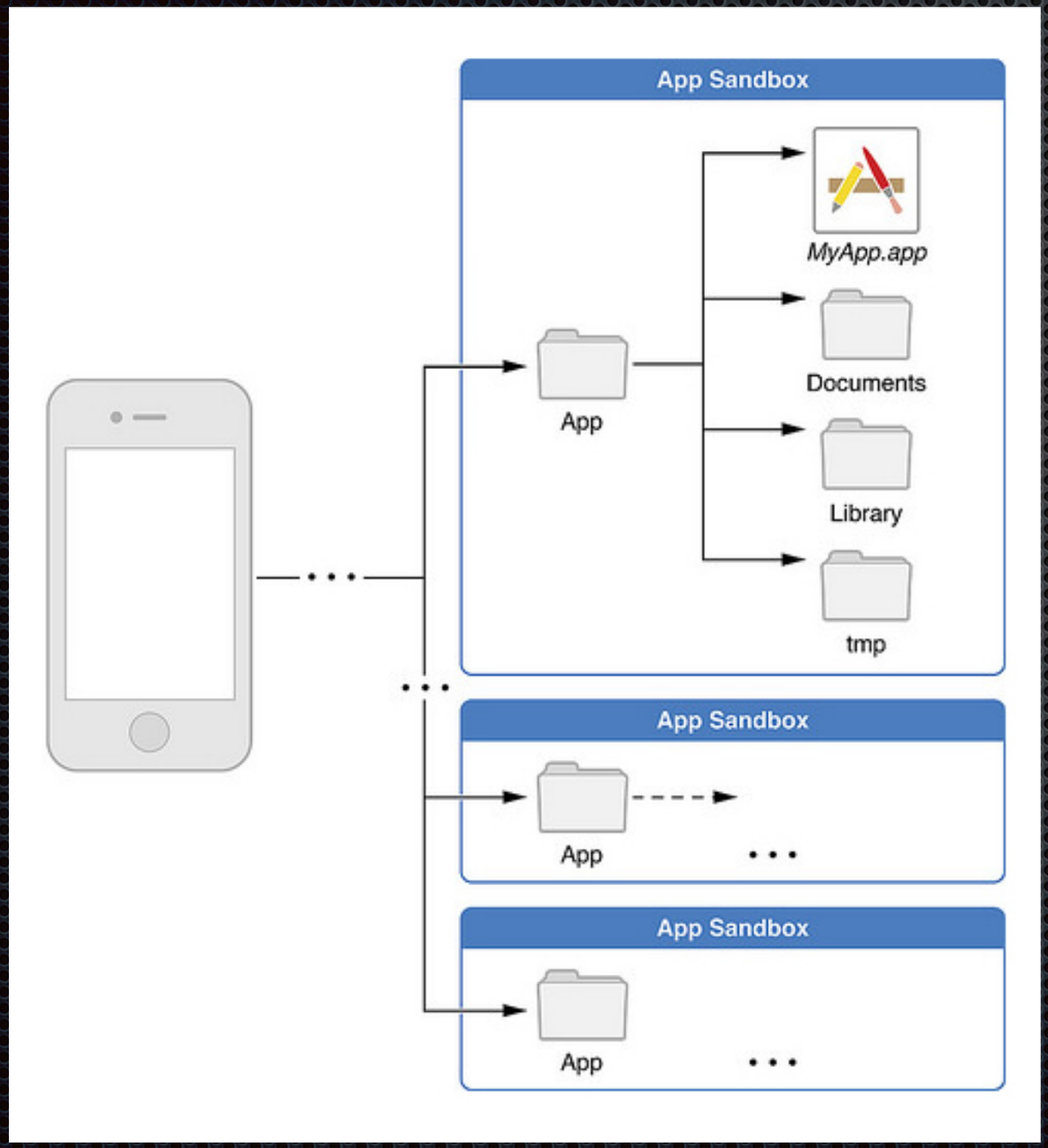
- 檢查Binary
  - ipa為壓縮檔案
- Strings找垃圾
- Code Review 最佳



FORTIFY An HP Company

CHECKMARX SOURCE CODE ANALYSIS TECHNOLOGIES

靜態檢測



- 儲存於app內資料
  - Plist or SQLite or binary
  - Document
  - Library
    - Preferences
    - Caches
      - Background Screenshot
  - KeyChain

靜態檢測工具

- iFile / iTools / iFunbox
- Hex Viewer
- Plist Viewer
- SQLite Viewer
- Clutch + IDA

Demo

iFunBox

新資料夾 重新整理 Go Up Level 從Mac複製 複製到Mac 安裝應用程式 Leo 的 iPh... Current Device 切換視角

iFoxbox

SQLite Database Browser

Database Structure | Browse Data | Execute SQL

Name	Object	Type	Schema

SQLite Browser

Leo — ssh — 80×24

```
root@192.168.2.2's password:
Leo-de-iPhone:~ root#
Leo-de-iPhone:~ root#
Leo-de-iPhone:~ root#
Leo-de-iPhone:~ root#
Leo-de-iPhone:~ root#
Leo-de-iPhone:~ root#
```

SSH

tw.gov.npa.110APP.plist

tw.gov.npa.110APP.plist 〉 No Selection

Key	Type	Value
▶ Root	Dictionary	(43 items)

Plist Viewer

Freeway1968HD

Save Copy Cut Paste Undo Redo Hex Text search Go To Offset Find (Text search)

```
00000  CA FE BA BE 00 00 00 02 00 00 00 0C 00 00 00 09 00 00 40 00 00 05 F3  ..................@....
00017  D0 00 00 00 0E 00 00 00 0C 00 00 00 0B 00 06 40 00 00 05 F3 D0 00 00  ..............@.......
0002E  00 0E 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........................
00045  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........................
0005C  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........................
00073  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........................
0008A  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........................
000A1  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........................
000B8  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........................
000CF  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........................
000E6  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........................
000FD  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........................
00114  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........................
0012B  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........................
00142  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........................
00159  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........................
00170  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........................
00187  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........................
0019E  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........................
001B5  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........................
001CC  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........................
001F3  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........................
```

Type	Value
8 bit signed	
8 bit unsi...	
16 bit signed	
16 bit uns	

Hex Viewer

Hex Little Endian Insert ASCII Offset: 0 Selection: 0

gidb

gidb Features

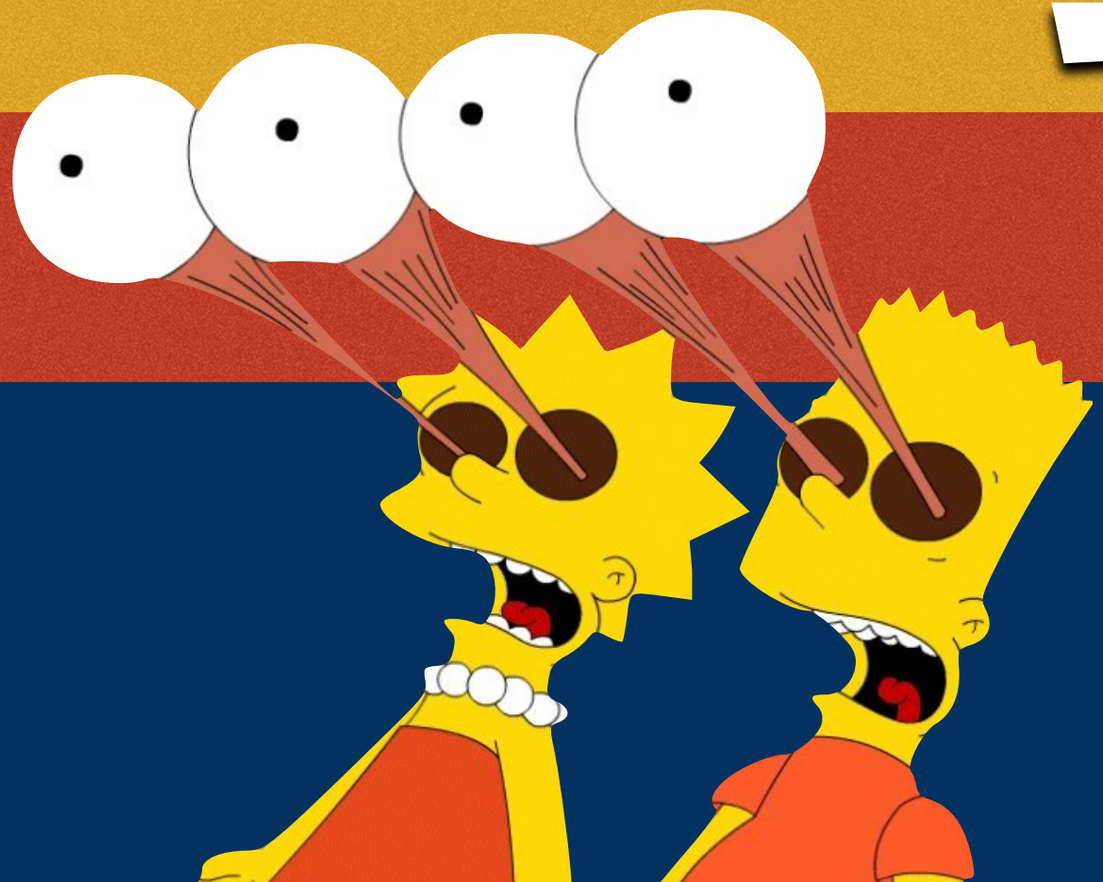
- Simplified pentesting setup
  - Setup port forwarding
  - Certificate management
- iOS log viewer
- Screen shot utility
  - Simplifies testing for the creation of backgrounding screenshots
- App-related functions
  - App binary
    - Download
    - List imported libraries
    - Check for encryption, ASLR, stack canaries
    - Decrypt and download an app binary (requires dumpdecrypted)
  - Launch an app
  - View app details such as name, bundleid, and `Info.plist` file.
- Inter-Process Communication
  - URL Handlers
    - List URL handlers
    - Invoke and fuzz URL handlers
  - Pasteboard monitor
- Analyze local file storage
  - Search for, download, and view plist files
  - Search for, download, and view sqlite databases
  - Search for, download, and view local caches (`Cache.db`)
  - File system browser
- Install utilities on iDevices
  - Install iOS SSL killswitch
  - alpha: Compile and install dumpdecrypted
- Alpha:
  - Cycript console
  - Snoop-It integration

https://github.com/dmayer/idb

Demo

動態

摸法



動態檢測

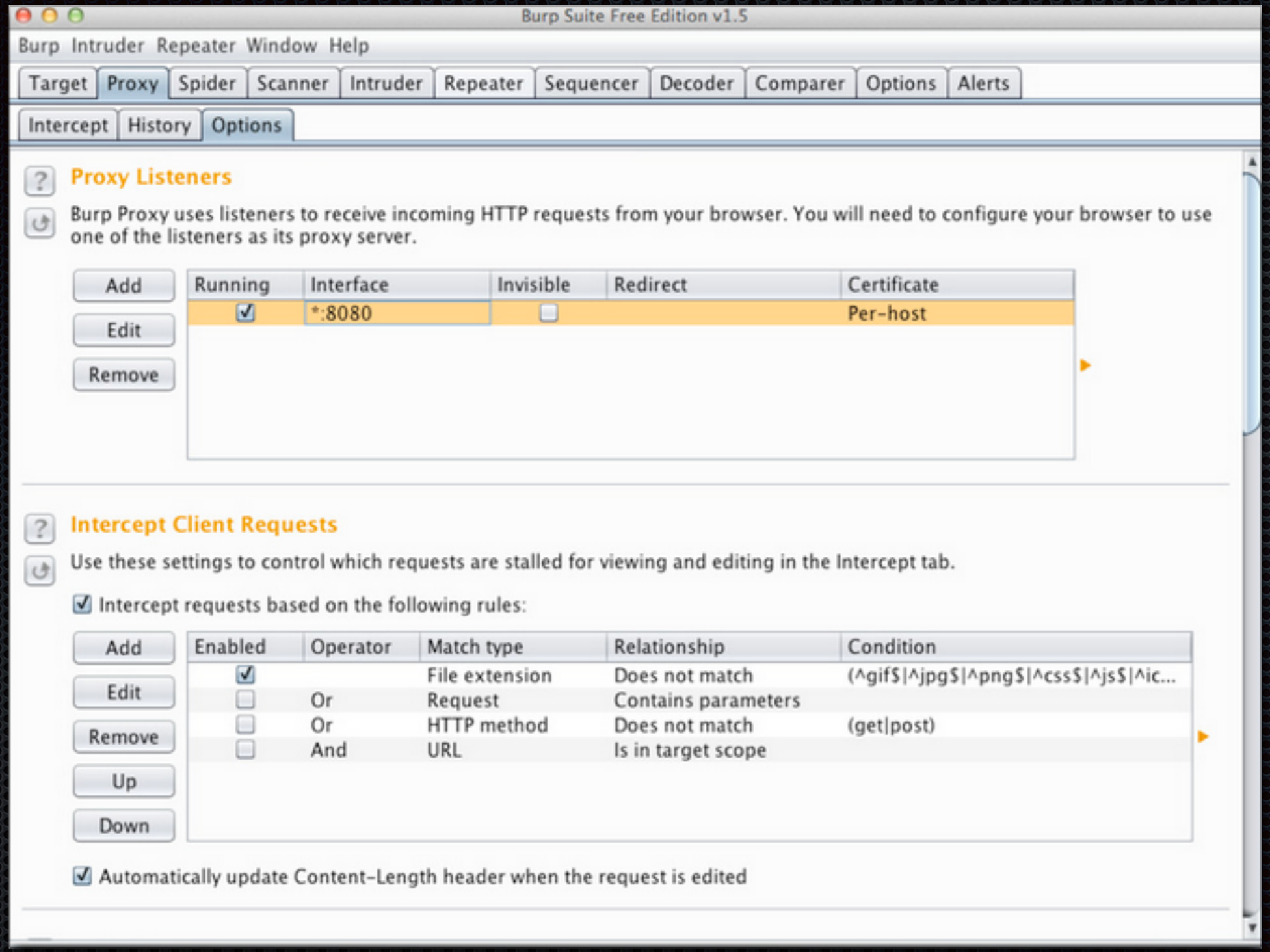
- API調用
- 網路傳輸封包
- 檔案系統讀寫
- Keychain調用
- 調用方法

以往
動態檢測需要以下工具來協助

class-dump-z
Cycript
gdb
.....

對囉！

還有App的封包還沒看！



建立一個Proxy Server

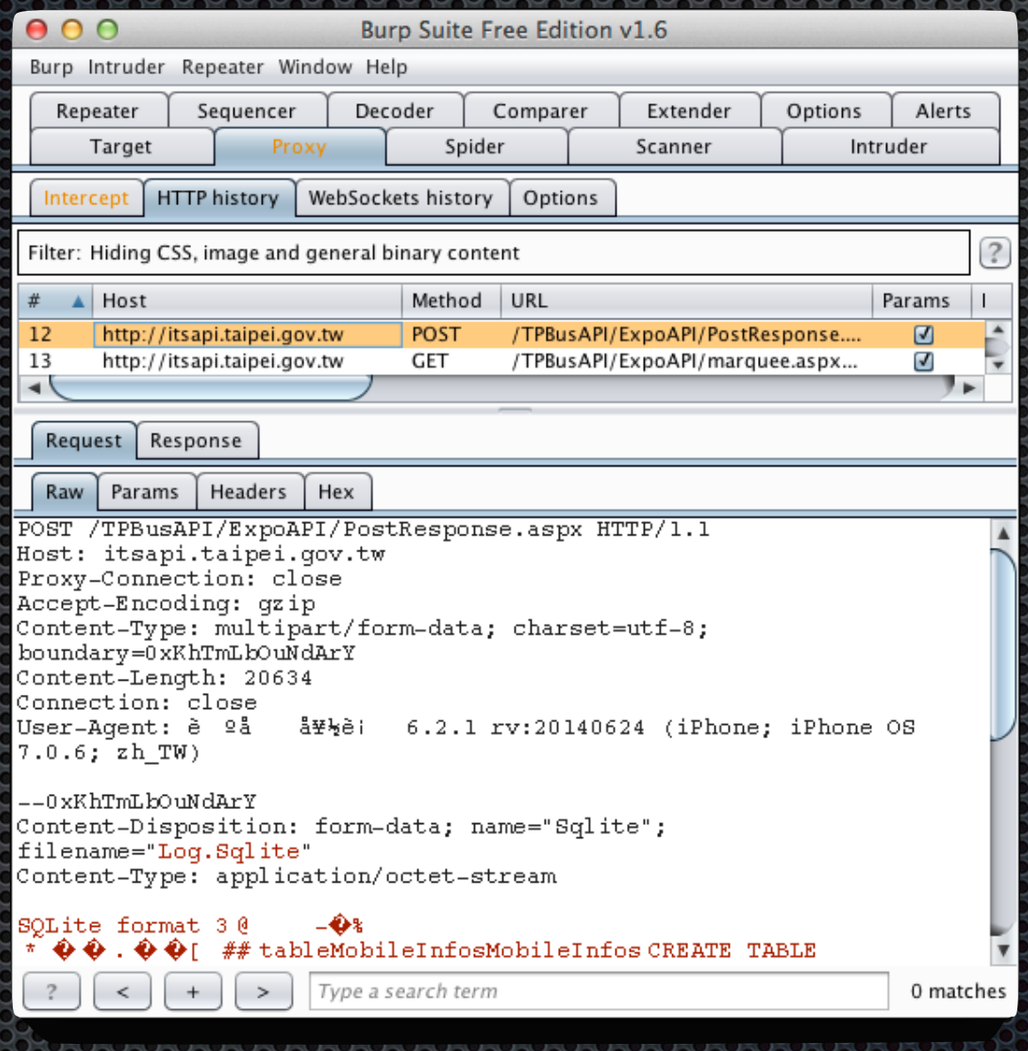
設定iOS ProxyIP

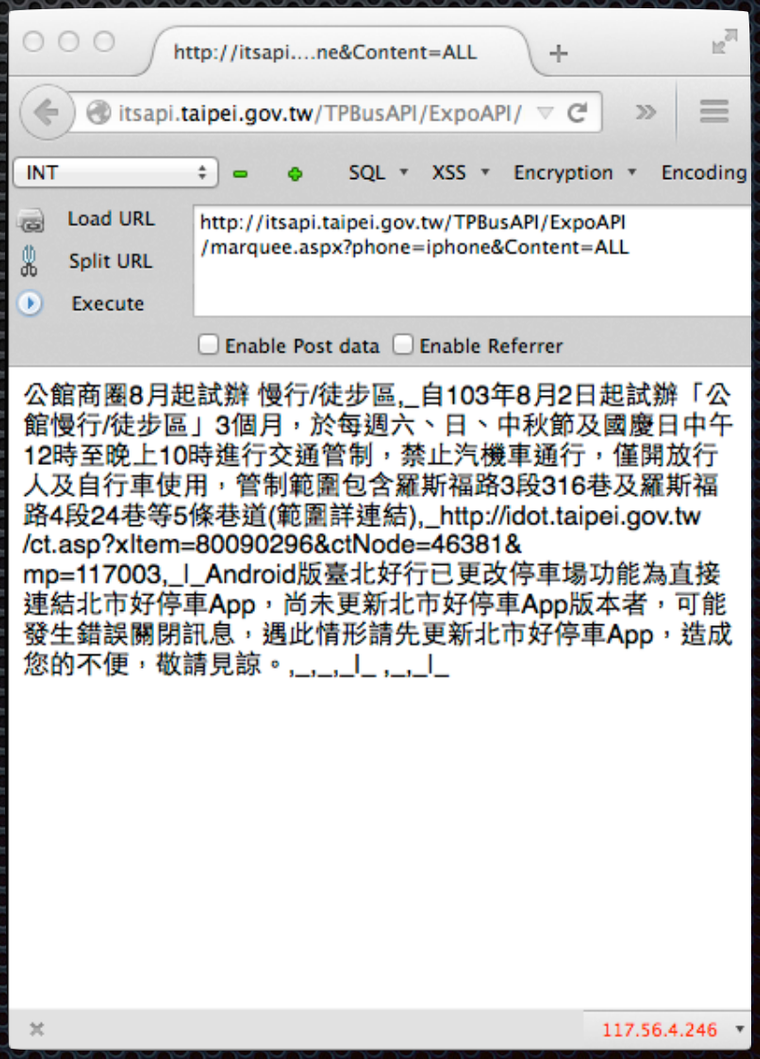

PortSwigger CA
Not Trusted
Install
Received Jan 9, 2013
Contains Certificate
More Details


PortSwigger CA
Trusted
Received Jan 9, 2013
Contains Certificate
More Details

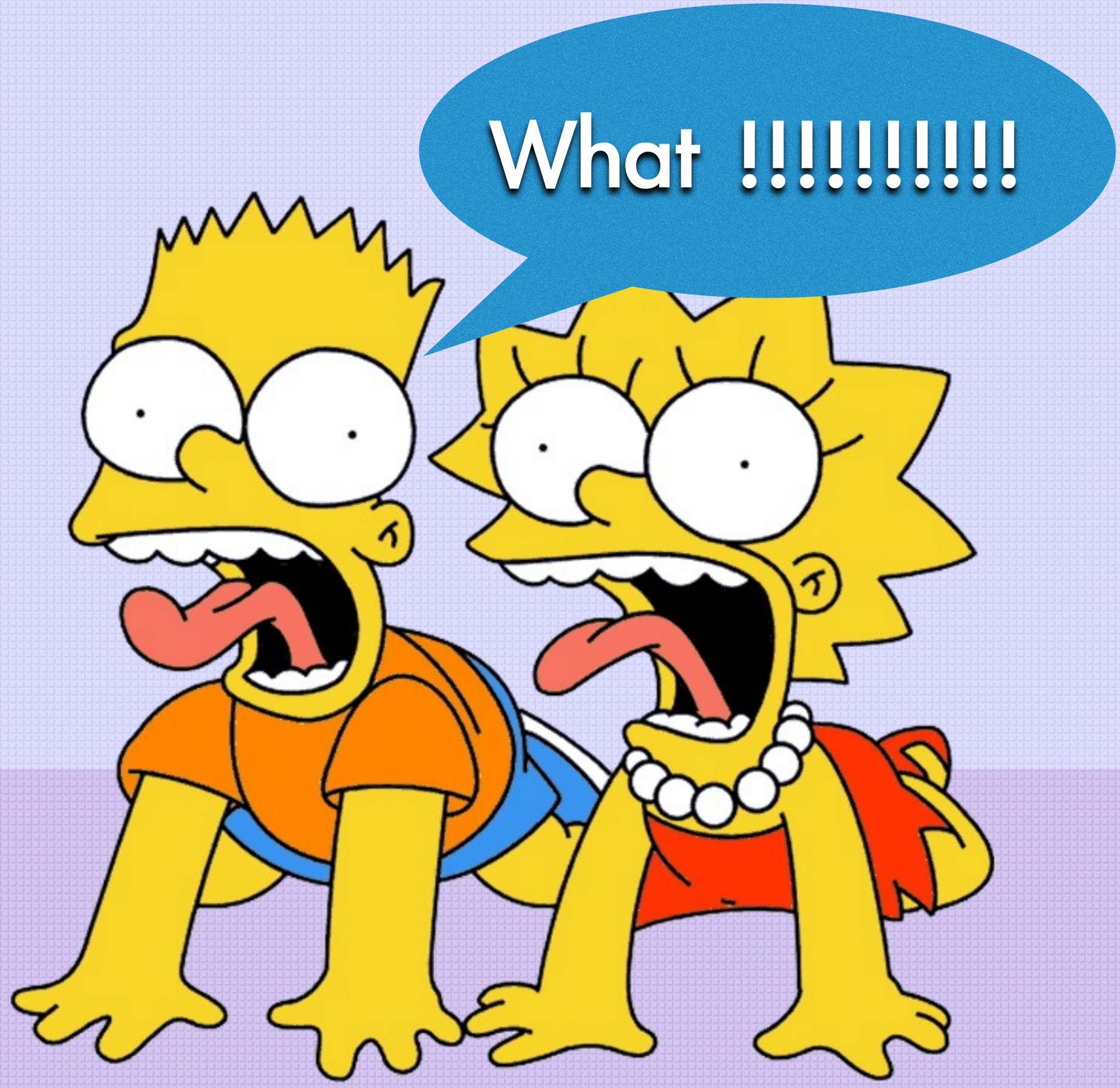
將憑證安裝至手機中

分析封包的環境





Device ⟷ Proxy ⟷ Server


What !!!!!!!!!!

Snoop-it

Monitoring

- File system access (print data protection classes)
- Keychain access
- HTTP(S) connections (`NSURLConnection`)
- Access to sensitive API (address book, photos etc.)
- Debug outputs (`NSLog`)
- Tracing App internals (`objc_msgSend`)

Analysis/Manipulation

- Fake hardware identifier (UDID, Wireless MAC, etc.)
- Fake location/GPS data
- Explore and force display of available `ViewController`
- List custom URL schemes
- List available Objective-C classes, objects and methods
- Invoke arbitrary methods at runtime
- Bypass basic jailbreak detection mechanisms

Other

- Simple installation and configuration
- Easy to use graphical user interface
- Plenty of filter and search options
- Detailed description of the XML-RPC web service interface

安裝步驟

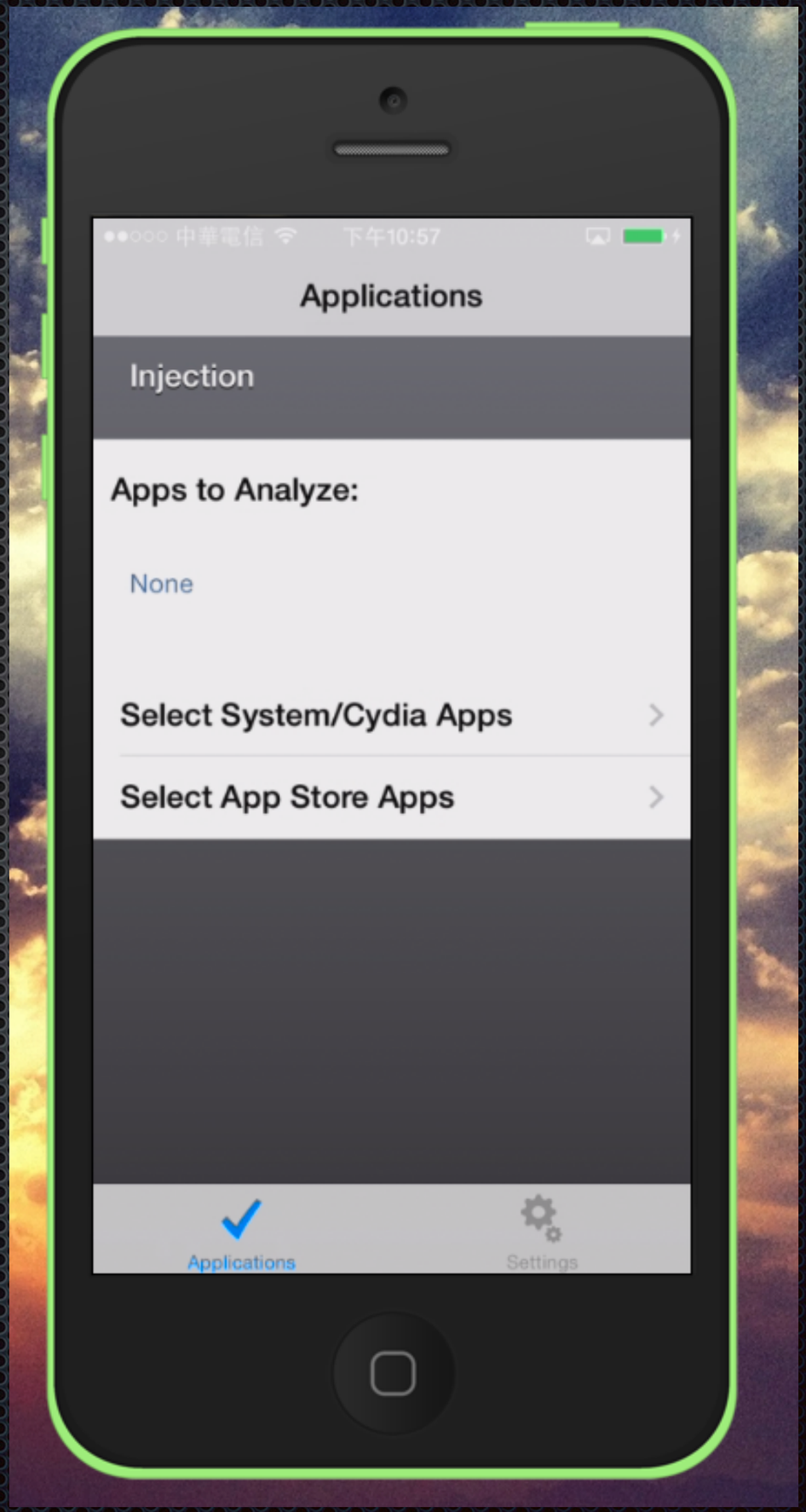
1.新增軟體源
http:/repo.nesolabs.de/

2.搜尋snoop-it
進行安裝

使用說明

1.選擇需要分析的app

2.開啟瀏覽器進行分析



Demo

App永遠都是你
最佳的解密工具

還是想知道key是什麼！

Introspy

The Problem

In 2013, assessing the security of iOS applications still involves a lot of manual, time-consuming tasks - especially when performing a black-box assessment. Without access to source code, a comprehensive review of these application currently requires in-depth knowledge of various APIs and the ability to use relatively complex, generic tools such as Cycript, or Mobile Substrate - or just jump straight into the debugger.

To simplify this process, we are releasing Introspy - an open-source security profiler for iOS. Introspy is designed to help penetration testers understand what an application does at runtime.

How Introspy works

The tool comprises two separate components: Introspy-iOS and Introspy-Analyzer.

Introspy-iOS is a tracer that can be installed on a jailbroken iOS device. It will hook security-sensitive APIs called by a given application, including functions related to cryptography, IPCs, data storage / protection, networking, and user privacy. The call details are all recorded and persisted in a SQLite database on the device

This database can then be fed to Introspy-Analyzer, which generates an HTML report displaying all recorded calls, plus a list of potential vulnerabilities affecting the application.

Tracer

Once installed, Introspy-iOS will store in a SQLite database all calls made by iOS applications to security-sensitive APIs.

https://github.com/iSECPartners/Introspy-iOS

Live Demo

gidb	gidb ifunbox	Burp Suite OWASP ZAP	Snoop-it Introspy
Binary 檢查	儲存資料檢查	傳輸過程	進階測試

是否有完善保護	是否有敏感資訊	是否有將敏感資料加密	Cache DebugLog KeyChain BackGround Screenshot 是否有敏感資料	伺服器是否有驗證機制	傳送敏感資料是否加密	Runtime 攻擊	是否能夠取得加密Key 高權限

App安全
取決於App的需求性

研究生禮貌運動！
-Be kind to Postgraduated

1. 看到研究生請不要露出「你怎麼還沒畢業?」的表情
   - Don't show the "why do you still here?" look!
2. 切勿詢問研究生何時畢業、論文進度、現在幾年級、何時初審、口試?
   - Don't ask the questions about time!!
3. 部分研究生不太喜歡討論與指導教授的相處狀況，請察言觀色.
   - Don't talk about their Boss!!!
4. 遇見研究生進行紓壓休閒娛樂時，請不要提醒他/她論文還沒寫!
   - Don't tell them "Your thesis haven't done yet!"

Q&A