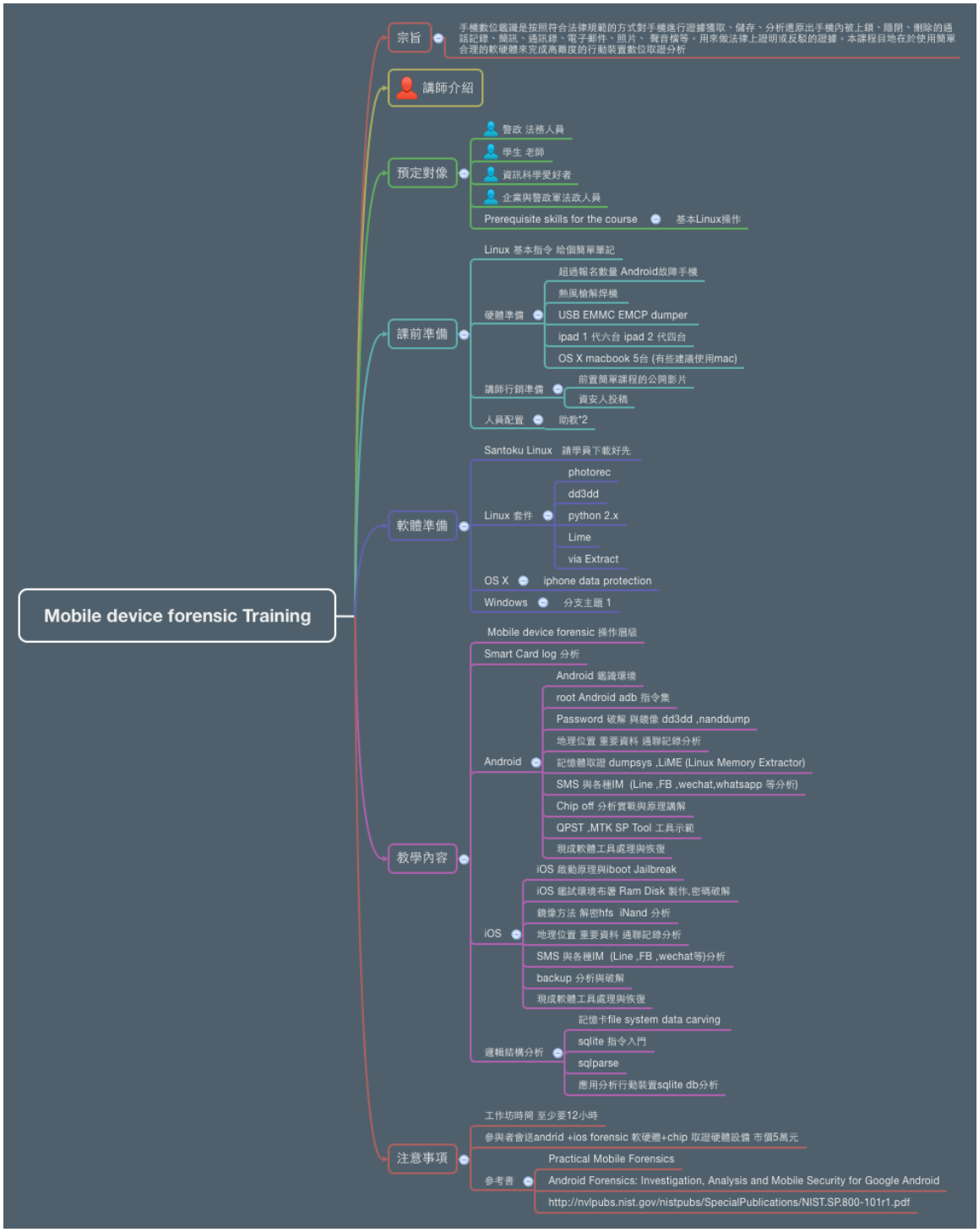
Mobile device forensic Training


Mobile device forensic Training
宗旨
手機數位鑑識是按照符合法律規範的方式對手機進行證據獲取、儲存、分析遺原出手機內被上鎖、隱閉、刪除的通話記錄、簡訊、通訊錄、電子郵件、照片、 聲音檔等。用來做法律上證明或反駁的證據。本課程目地在於使用簡單合理的軟硬體來完成高難度的行動裝置數位取證分析
講師介紹
預定對像
警政 法務人員
學生 老師
資訊科學愛好者
企業與警政軍法政人員
Prerequisite skills for the course
基本Linux操作
課前準備
Linux 基本指令 給個簡單筆記
硬體準備
超過報名數量 Android故障手機
熱風槍解焊機
USB EMMC EMCP dumper
ipad 1 代六台 ipad 2 代四台
OS X macbook 5台 (有些建議使用mac)
講師行銷準備
前置簡單課程的公開影片
資安人投稿
人員配置
助教*2
軟體準備
Santoku Linux 請學員下載好先
Linux 套件
photorec
dd3dd
python 2.x
Lime
via Extract
OS X
iphone data protection
Windows
分支主題 1
教學內容
Mobile device forensic 操作層級
Smart Card log 分析
Android
Android 鑑識環境
root Android adb 指令集
Password 破解 與鏡像 dd3dd ,nanddump
地理位置 重要資料 通聯記錄分析
記憶體取證 dumpsys ,LiME (Linux Memory Extractor)
SMS 與各種IM (Line ,FB ,wechat,whatsapp 等分析)
Chip off 分析實戰與原理講解
QPST ,MTK SP Tool 工具示範
現成軟體工具處理與恢復
iOS
iOS 啟動原理與iboot Jailbreak
iOS 鑑試環境布署 Ram Disk 製作,密碼破解
鏡像方法 解密hfs iNand 分析
地理位置 重要資料 通聯記錄分析
SMS 與各種IM (Line ,FB ,wechat等)分析
backup 分析與破解
現成軟體工具處理與恢復
邏輯結構分析
記憶卡file system data carving
sqlite 指令入門
sqlparse
應用分析行動裝置sqlite db分析
注意事項
工作坊時間 至少要12小時
參與者會送andrid +ios forensic 軟硬體+chip 取證硬體設備 市價5萬元
參考書
Practical Mobile Forensics
Android Forensics: Investigation, Analysis and Mobile Security for Google Android
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf

1. 宗旨

1.1. 手機數位鑑識是按照符合法律規範的方式對手機進行證據獲取、儲存、分析還原出手機內被上鎖、隱閉、刪除的通話記錄、簡訊、通訊錄、電子郵件、照片、
聲音檔等。用來做法律上證明或反駁的證據。本課程目地在於使用簡單合理的軟硬體來完成高難度的行動裝置數位取證分析

2. 講師介紹

3. 預定對像

3.1. 警政 法務人員

3.2. 學生 老師

3.3. 資訊科學愛好者

3.4. 企業與警政軍法政人員

3.5. Prerequisite skills for the course

3.5.1. 基本Linux操作

4. 課前準備

4.1. Linux 基本指令 給個簡單筆記

4.2. 硬體準備

4.2.1. 超過報名數量 Android故障手機

4.2.2. 熱風槍解焊機

4.2.3. USB EMMC EMCP dumper

4.2.4. ipad 1 代六台 ipad 2 代四台

4.2.5. OS X macbook 5台 (有些建議使用mac)

4.3. 講師行銷準備

4.3.1. 前置簡單課程的公開影片

4.3.2. 資安人投稿

4.4. 人員配置

4.4.1. 助教*2

5. 軟體準備

5.1. Santoku Linux 請學員下載好先

5.2. Linux 套件

5.2.1. photorec

5.2.2. dd3dd

5.2.3. python 2.x

5.2.4. Lime

5.2.5. via Extract

5.3. OS X

5.3.1. iphone data protection

5.4. Windows

5.4.1. 分支主題 1

6. 教學內容

6.1. Mobile device forensic 操作層級

6.2. Smart Card log 分析

6.3. Android

6.3.1. Android 鑑識環境

6.3.2. root Android adb 指令集

6.3.3. Password 破解 與鏡像 dd3dd ,nanddump

6.3.4. 地理位置 重要資料 通聯記錄分析

6.3.5. 記憶體取證 dumpsys ,LiME (Linux Memory Extractor)

6.3.6. SMS 與各種IM (Line ,FB ,wechat,whatsapp 等分析)

6.3.7. Chip off 分析實戰與原理講解

6.3.8. QPST ,MTK SP Tool 工具示範

6.3.9. 現成軟體工具處理與恢復

6.4. iOS

6.4.1. iOS 啟動原理與iboot Jailbreak

6.4.2. iOS 鑑試環境布署 Ram Disk 製作,密碼破解

6.4.3. 鏡像方法 解密hfs iNand 分析

6.4.4. 地理位置 重要資料 通聯記錄分析

6.4.5. SMS 與各種IM (Line ,FB ,wechat等)分析

6.4.6. backup 分析與破解

6.4.7. 現成軟體工具處理與恢復

6.5. 邏輯結構分析

6.5.1. 記憶卡file system data carving

6.5.2. sqlite 指令入門

6.5.3. sqlparse

6.5.4. 應用分析行動裝置sqlite db分析

7. 注意事項

7.1. 工作坊時間 至少要12小時

7.2. 參與者會送andrid +ios forensic 軟硬體+chip 取證硬體設備 市價5萬元

7.3. 參考書

7.3.1. Practical Mobile Forensics

7.3.2. Android Forensics: Investigation, Analysis and Mobile Security for Google Android

7.3.3. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf