GEnCCFI Guidance EnCase v7 CF1國際專業鑑識認證課程

Guidance EnCase v7 Computer Forensics I

時數：32 小時 ｜ 費用：68,000 元 ｜ 點數：20 點 ｜ 教材：Guidance 原廠英文教材

適合對象 執法人員、資安從業人員、資訊系統管理者、或對電腦鑑識技術有興趣者

課程內容
1. 數位證據是什麼、數位證據的組成，以及電腦如何運作
2. EnCase v7電腦犯罪鑑識方法概論及導覽
3. 如何準備一個可以在法院成為呈堂證供之證物
4. FAT與NTFS檔案系統基本架構介紹
5. 建立專案、預覽及取得數位證據映像檔
6. 如何使用內建之軟體防寫機制蒐集證據
7. 如何使用光碟開機和網路線進行證據蒐集
8. 關鍵字搜尋功能、參數簡介
9. 檔案特徵值分析並檢視原始檔案
10. 如何使用時間軸檢視變動檔案
11. 如何建立及運用Hash資料庫幫助調查
12. 如何運用分析流程將製作的證據檔案與資料蒐集歸檔
13. 如何使用標籤標記檔案以及匯出網頁格式之標籤檢視檔
14. 如何復原被刪除、隱藏、覆蓋之檔案
15. 從檔案殘存區(Files Slack、Ram Slack)取得有價值之證據
16. 驗證證據檔案持有人及還原使用者設定、資源回收桶內資訊
17. 如何有效的利用Encase v7提供之範本產出報告

備註事項 課程結束後將頒發原廠結訓證書及CPE 32小時之證書

GEnCCFI

EnCE認證

CPE積分

GEnCCFII Guidance EnCase v7 CF2國際專業鑑識認證課程

Guidance EnCase v7 Computer Forensics II

時數：32 小時 ｜ 費用：68,000 元 ｜ 點數：20 點 ｜ 教材：Guidance 原廠英文教材

適合對象 執法人員、資安從業人員、資訊系統管理者、或對電腦鑑識技術有興趣者

課程內容
1. 還原刪除之分割區及資料夾
2. 複合檔案簡介及如何檢視、操作
3. Windows之註冊檔案簡介及其在鑑識上的應用
4. 如何利用時間函數適當調整專案設定
5. 了解NTFS檔案系統概觀
6. 了解如何使用Encase Evidence Processor
7. 如何還原被刪除檔案、運用建立索引進階搜尋
8. 了解單一與邏輯證物檔之差別，並知道如何產出及利用邏輯證物檔
9. 如何使用Encase Virtual File System(VFS)與Physical Disk Emulator(PDE)模組
10. 如何利用關鍵字搜尋與如何利用GREP進階搜尋
11. 如何使用Hash值確認為同一個證物檔案並建立Hash查詢系統
12. 如何辨識Windows 7作業系統架構(連結檔、垃圾桶、使用者資料夾)
13. 檢視網頁瀏覽器暫存檔、Cookie、Email
14. 搜尋Email及Email附加檔案
15. 如何由垃圾桶還原資料
16. 產出專業並具法律效用之報告與證物做為呈堂證供

備註事項
1. 課程結束後將頒發原廠結訓證書及CPE 32小時之證書
2. 完成基礎CF1及CF2課程後即可申請EnCE®認證考試，考試分別為線上筆試和實際案例分析操作兩個部份；通過考試後約1個月左右，將會收到原廠核發的EnCE®(EnCase Certified Examiner)國際證書

GEnCCFII

EnCE認證

CPE積分