2021新課

iFNF 網路鑑識及惡意程式分析

Network Forensics and Malware Analysis

時數：14小時 | 費用：24,000元 | 點數：6點 | 教材：專用教材

適合對象	1. 對資安事件調查領域工作有興趣者 2. 欲充實本身資安鑑識技術能力的人員
預備知識	Windows作業系統基礎操作、網路基礎概念、程式設計基礎概念
課程內容	1. 惡意程式事件之現場蒐證處理方式 2. 網路封包蒐證及分析 3. Windows 惡意程式主機端分析的主要重點資料 4. 資料搜尋、TimeLine及 Log分析 5. 惡意程式記憶體分析暨案例處理 6. 惡意程式反組譯分析
備註事項	1. 白天班之上課時間為09:00~17:00 2. 本課程與鑒真數位合作開班
後續推薦課程	iFApp：智慧型手機APP資安分析

2021新課

iFDC 資安事件損害控制暨資料復原實務

Information Security Incident Damage Control and Data Recovery Practice

時數：14小時 | 費用：24,000元 | 點數：6點 | 教材：專用教材

適合對象	1. 對資安領域工作有興趣者 2. 網商或電商經營者(有個資及交易紀錄) 3. 政府單位或八大關鍵基礎設施之資訊人員
預備知識	資安基礎概念、網路基礎概念
課程內容	1. 資安法對於資安緊急事件之要求 2. 個資法暨 165 網商詐騙通報對於個資外洩之要求 3. 資安事件應建立事前偵測才能把損害有效控制 4. 災損控制暨系統回復重點 5. 事前的防禦措施決定復原及災損的控制能力 6. 資料外洩之災損控制及回復 7. 實體故障/人員因素之災損控制及回復 8. DDOS攻擊/主機遭駭之災損控制及回復 9. 實務綜合演練
備註事項	1. 白天班之上課時間為09:00~17:00 2. 本課程與鑒真數位合作開班
後續推薦課程	iFNF：網路鑑識及惡意程式分析

2021新課

iFApp 智慧型手機APP資安分析

Smartphone APP Information Security Analysis

時數：14小時 | 費用：24,000元 | 點數：6點 | 教材：專用教材

適合對象	想學習App iOS、Android鑑識知識、手機APP開發人員、資安分析人員、欲充實本身資安鑑識技術能力的人員
預備知識	手機封包分析的觀念、程式開發基礎觀念
課程內容	1. 智慧型手機APP的安全問題及目前國際間的分析作法 2. iOS平台 APP分析基本環境架設 3. iOS平台 APP程式反組譯及相關靜態分析 4. Android 平台APP分析基本環境架設 5. Android 平台APP程式反組譯及相關靜態分析 6. Android平台 APP 虛擬平台及Sandbox分析 7. 智慧型手機APP網路封包Man-in-the-middle解密分析
備註事項	1. 白天班之上課時間為09:00~17:00 2. 本課程與鑒真數位合作開班
後續推薦課程	iFNF：網路鑑識及惡意程式分析

2021新課

DF120 Opentext-DF120 Encase國際專業鑑識認證課程

Opentext-DF120 Foundations in Digital Forensics Course

時數：32小時 | 費用：78,000元 | 點數：21點 | 教材：Opentext原廠教材

DF120

適合對象	執法人員、資安從業人員、資訊系統管理者、對電腦鑑識技術有興趣者
預備知識	數位鑑識基礎概念、作業系統基礎概念、網路安全基礎概念
課程內容	Day1 1. 建立新案件 2. 設定環境 3. 學習數位證物格式及硬碟、檔案系統基礎 4. 學習EnCase各項功能包含備份案件、設定檔、圖示、欄位等 Day2 1. 如何製作證物image 2. 執行process分析證物包含檔案特徵值分析、計算Hash值、Email分析、網路分析、關鍵字搜尋、Index搜尋等 3. 學習使用bookmark及report功能 Day3 1. 學習關鍵字及index搜尋 2. 學習檔案複製，磁區掛載 3. 製作logical evidence file 4. 學習檔案特徵值分析原理 5. 學習匯出匯入Project VIC Day4 1. 學習entropy分析原理 2. 手動進行檔案Carving 3. 建立、客製化、匯出報告 4. 學習Reacquiring、Restoring、封裝案件等結案功能
備註事項	1. 白天班之上課時間為9:00-18:00 2. 本課程與鑒真數位合作開班 3. 課程結束後將頒發原廠結訓證書及CPE 32小時之證書
後續推薦課程	DF210：Opentext-DF210 Encase國際專業鑑識認證課程

2021新課

DF210 Opentext-DF210 Encase國際專業鑑識認證課程

Opentext-DF210 Building an Investigation Course

時數：32小時 | 費用：78,000元 | 點數：21點 | 教材：Opentext原廠教材

DF210

適合對象	執法人員、資安從業人員、資訊系統管理者、對電腦鑑識技術有興趣者
預備知識	已完成以下課程所具備技術能力 DF120：Opentext-DF120 Foundations in Digital Forensics
課程內容	Day1 1. 複習案件建立及加入證物 2. 調查被Bitlocker加密之資料 3. 學習MBR相關機制 4. 學習Partition Recovery 功能 5. 了解Compound Files 6. 製作Logical evidence files 7. 了解Windows機碼 Day2 1. 時區更改設定 2. ExFAT、NTFS檔案系統解析 3. 了解Windows Artifacts 4. 使用者帳號資訊分析 5. Thumbnail Cache file功能 6. 系統檔案分析 7. Windows EDB分析 8. GREP練習 Day3 1. LNK Files 分析 2. USB Device分析 3. 學習Windows 資源回收桶 4. Email分析 5. 網際網路歷程分析 Day4 1. 列印檔案救援 2. Unallocated 區域進行關鍵字搜尋 3. 建立、客製化、匯出報告 4. 學習Reacquiring、Restoring、封裝案件等結案功能
備註事項	1. 白天班之上課時間為9:00-18:00 2. 本課程與鑒真數位合作開班 3. 完成基礎DF120及DF210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分。通過考試後約1個月左右，將會收到原廠核發的EnCE(EnCase Cerified Examiner)國際證書 4. 課程結束後將頒發原廠結訓證書及CPE 32小時之證書