# 參加進階惡意軟體分析培訓課程

隨着涉及惡意軟體的電腦犯罪個案數字不斷上升，電腦法證檢驗人員及偵查人員必須深入理解惡意軟體的運作原理，掌握電子證據的獲取方法，以有效打擊犯罪。為此，本局委派首席刑事偵查員鍾錦良和一等高級技術員歐陽永昌於2018年8月5日至11日前往菲律賓馬尼拉，參加由國際刑警網絡犯罪處主辦的“國際刑警進階惡意軟體分析培訓”。參加是次培訓的學員還有來自澳洲、斐濟、西班牙、加納等國家及地區的代表共15人。

惡意軟體分析培訓課程為期五天，主要內容有：

（一）惡意軟體的靜態分析原理及檢驗方法。通常惡意代碼會對惡意軟體進行“加殼”，以便隱藏其執行過程的惡意代碼，在課堂上，導師介紹了多種“加殼”的特徵及其檢驗工具的使用方法，並安排學員進行實際操作練習。

（二）惡意軟體的動態分析原理及檢驗方法。動態分析方法是將惡意軟體樣本置於獨立的電腦運行環境中運行，監控分析其惡意行為，導師介紹了各種監控及分析工具，以及惡意軟體的開機自動啟動機制，講解如何深入追蹤並分析其惡意行為的電子證據。

（三）漏洞攻擊套件（Exploit Kits）及無文件感染。首先介紹了漏洞攻擊套件經常會利用的漏洞類型（零日漏洞、N日漏洞及多重漏洞）及攻擊產品對象，然後介紹了無文件感染技術的程式自動啟動方法，以及惡意代碼存活並運作於電腦內存的機制，並以實例演示病毒勒索程式利用漏洞攻擊套件及無文件感染技術，在電腦使用者不知情的狀況下通過瀏覽器攻擊並感染使用者電腦的整個過程。

（四）POS惡意軟體的分析。POS，全稱是Point of Sale，即銷售時點情報系統。課程主要介紹常見的POS惡意軟體如何監控連接着POS設備的電腦，從電腦內存中搜集用戶的銀行卡信息及個人信息，並將信息發送至命令及控制服務器。在練習操作中，導師利用上述的靜態及動態分析工具，講解如何分析出與惡意軟體進行通訊的地址。

本局人員透過是次培訓，學習到不同類型的惡意軟體的運行機制及分析方法，以及各種分析工具的使用技巧，對於本局打擊電腦犯罪很有幫助。