參加國際刑警手機法證專家培訓

為持續提升手機法理鑑證效率，強化手機取證方面的技能，本局委派電腦法證處陳思晶處長和關劍飛高級技術員於2016年12月5日至9日前往以色列，修讀“國際刑警手機法證專家培訓課程”。參加課程的學員分別來自英國、法國、意大利、日本、白俄羅斯、巴西、捷克、丹麥、以色列、約旦、墨西哥、新加坡、西班牙及中國澳門等多個國家及地區。

現今的智能手機隨着全球移動通訊技術的快速發展而普及，從以往僅僅作為通訊溝通的工具轉變成能獲取各種資訊的小型個人電腦。許多手機應用程式推陳出新，儲存於手機內的資料大增，這些資料很可能成為調查刑事犯罪案件時不可或缺的關鍵證據，因此智能手機已成為當今各類犯罪最常見的證物之一。是次培訓課程內容主要是應對智能手機法理鑑證領域所面臨的挑戰，介紹智能手機主流作業系統iOS及Android之手機取證流程，以及手機常用數據庫取證及分析方法等。

課程第一部份主要講解智能手機上最常用的數據庫SQLite database，內容包括數據庫結構及資料記錄儲存機制、各資料表的關聯分析方法、資料記錄從數據庫刪除的原理、資料記錄被破壞的成因、資料庫日誌檔案的運用等。

課程核心則是聚焦於智能手機作業系統iOS和Android的取證及分析方法，內容包括各版本作業系統的特點、系統的檔案結構、使用相關手機鑑證軟件對相關作業系統進行取證及分析的方法、遇到智能手機啟動鎖屏功能時如何獲取證據的方法，以及iOS作業系統Plist檔案的分析、iTunes備份及iCloud備份的資料夾結構、備份被加密的處理方法、如何對Android作業系統上的惡意程式進行檢測、分析等。

課程的最後部份則是介紹智能手機取證時容易被忽略的重要資料提取及分析方法、對智能手機進行解焊晶片Chip Off的技術、如何處理新型及不支援的手機品牌，特別是如何分辨出證據可能存在的區域及其相關技術，以及透過關鍵詞搜尋和逆向工程來進行資料復原與分析的技術等。

是次培訓課程能提高法證人員的鑑識能力及對智能手機的取證技巧，導師除了教導理論知識外，也加插實務練習，使參加者能將理論及實際操作融會貫通，有利於法理鑑證人員更好地把相關取證技巧運用到工作上，對於本局提升手機法理鑑證工作成效有積極作用。