參加“第二屆國際刑警進階手機法證培訓”

隨着移動通訊技術的高速發展，傳統的手機通話功能已不能滿足人們需求，促使越來越多的應用程式（Apps）相繼推出，儲存在手機內的資料越來越多，這些資料有可能不經意地成為揭露事件真相的關鍵證據。因此，執法人員需要不斷學習最新的手機取證技術，研討手機取證在法律和技術上的難點。2017年5月15日至19日，國際刑警組織在中國福建省廈門市舉辦“第二屆國際刑警進階手機法證培訓”，參加培訓的專業取證人員為分別來自法國、西班牙、巴西、馬來西亞、新加坡、印度、墨西哥、阿爾及利亞、摩洛哥、多明尼加共和國、孟加拉、斯里蘭卡、秘魯、摩爾多瓦、科威特、約旦、加納、斐濟、黎巴嫩、尼日利亞、蘇丹，以及中國內地、香港和澳門合共24個國家或地區的36位代表，其中包括本局電腦法證處首席高級技術員謝嘉健和二等技術員張小聰。

手機取證是從手提電話及流動設備中固定、收集、保全和分析相關的電子證據，並最終獲得具有法律效力的、能被法庭所接受的證據的過程。是次培訓專為從事手機取證的專業人員而舉辦，主要內容圍繞當前主流手機系統的運作模式和系統安全結構、各手機系統的取證難點和最新取證方式，以及一些新興便攜物聯網（IoT，亦即Internet of Things）的取證研究成果，包括： Android系統和iOS系統的手機取證技術及分析方法、智能終端（Smart Terminal）取證技術以及無人機取證技術。主辦單位邀請中國內地執法部門的手機取證專家和學者講授最新的手機取證技術和研究成果。第一部份內容主要介紹手機通訊系統的組成以及通訊原理、Android系統的架構、系統啟動模式以及在不同啟動模式下擁有的權限。第二部份內容介紹iOS系統的發展史以及在各個版本的安全機制發展、iOS系統啟動模式和文件結構系統、安全機制、iCloud 備份和iTunes備份的文件結構，分析數據庫的存儲機制，講解應用程式的取證和分析方法。第三部份是講述Android和iOS系統的數據安全保護機制、取證技術和分析方法。第四部份則詳細介紹了Android系統動態和靜態的取證技術，智能終端（Smart Terminal）取證的技術以及手機數據分析，根據獲取的數據總結出具有價值的資料。

為了使課堂上講授的理論與實際相結合，使取證知識得到實踐應用，導師舉辦了手機取證競賽，競賽題目分為兩部份，一部份為取證理論選擇題，另一部份是手機取證實戰，參加人員需要在有限的時間內，分組合作尋找模擬案件所要求的資料，務求將涉案人的犯案計劃、犯案地點時間和所有關聯人士進行全面偵查，以便將有關的電子證據呈交佐證。此外，培訓期間，專家亦分享最新的研究成果，介紹勒索病毒的傳播方式和加密文件的方式、採取的預防措施，以及通過數據恢復技術找回被病毒加密的文件，儘量減低所造成的損失。

參加是次培訓使本局人員學到更多手機取證的相關理論知識，認識最新的手機取證研究成果和取證技巧，加深瞭解執法人員共同存在的難題和共同探求解決的方法，有利於本局人員更好地把相關取證技術運用到實際工作中，提高手機法理鑑證工作的成效。