

## 參加“互聯網及網絡調查課程”



為使執法人員及時掌握最新的互聯網及網絡調查技巧，香港警務處網絡安全及科技罪案調查科與香港警察學院於2017年12月11日至22日，在香港灣仔警察總部合辦“互聯網及網絡調查課程”。參加課程的學員分別來自公安部網絡安全保衛局、香港警務處、香港廉政公署、香港出入境事務處，以及新加坡、芬蘭和中國澳門的執法機關。本局委派資訊罪案調查處二等刑事偵查員江家偉和電腦法證處一等技術員林健城前往參加培訓。

是次課程由網絡安全及科技罪案調查科多位經驗豐富的警察擔任導師。培訓內容包括互聯網基礎、路由概念、TCP/IP協議和網址轉移的技術；TCP/IP協議和端口（Port）的作用，利用軟件工具查看自身電腦所啟用的端口；電子郵件標頭（Email Header）的分析方法，查看發送電郵的源頭IP地址；域名/IP註冊人或公司的資料追查；利用網絡代理伺服器（Proxy）隱藏自身的IP地址；網絡封包截取工具Wireshark的使用及其封包過濾（filter）功能；網頁伺服器的調查及取證方法，以及日誌的分析技巧；利用NMAP軟件掃描目標網絡中的電腦及查看目標電腦所開啟的端口、服務

和操作系統類型；使用Python、Volatility軟件進行電腦取證的技術；數據庫的入侵技術SQL Injection；殭屍網絡（Botnet）的種類及其運作方式；使用CISCO的Packet Tracer模擬網狀環境；介紹Darknet及示範tor browsers 訪問；網絡入侵事件的偵查和分析。



除了理論學習外，導師還安排多個模擬案例讓學員們演習，包括電郵標頭（Email Header）中IP地址及其所在地的查看和分析、伺服器日誌分析、網絡封包分析，最後由香港警務處主管人員講解、示範及分享真實案例。本局人員通過培訓，學習到網絡案件偵查的流程及各個環節，增加了網絡偵查的知識及技能，鞏固並提升了對網絡罪案的調查和分析能力。

網絡罪案具有跨地域特點，由於各地法律體系、調查程序不同，相關地區的執法人員需要良好的溝通，才能合作打擊網絡犯罪。本局人員透過參加培訓，與相關地區人員就網絡調查經驗及技術進行交流，增進了友誼，有助於日後在工作上更深入地溝通合作，高效打擊網絡犯罪。