數位鑑識簡介

中央警察大學資訊系教授　吳國清

享譽國際之刑事鑑識專家──李昌鈺博士，在民國 96 年 11 月 23 日由台灣科技大學資通安全與教學中心、中央警察大學、財團法人李昌鈺博士物證科學教育基金會所共同籌辦的「電腦犯罪防治與資安技術發展」國際學術研討會中指出：「未來電腦犯罪將會成為主要犯罪，治安工作需要科技的配合，尤其現今電腦犯罪情形普遍，故而應如何從技術層面上去做研究，讓警察、鑑識等工作人員能應用在犯罪現場偵查與鑑識上。」

世界各國數位鑑識相關專家學者們均不約而同的指出，數位鑑識相對於傳統鑑識，它是一個亟待開發的新鑑識領域，然各國對於這類人才與技術之質與量均明顯嚴重不足，加上電腦網路通訊應用十分普及、產品廉價，已為人類日常生活和活動的主要部分，政府和民間企業、機關等加速推動業務 e 網路化，再者網路虛擬社會行為的跨地域性、隱密性和犯罪時機無時空性限制，導致電腦犯罪猖獗，犯罪黑數有增無減。尤甚者，全球惡意網站的高倍速成長，合法網站常遭受惡意程式碼的攻擊，社交型網站(包括網誌、微網誌等)已為垃圾郵件和廣告等業者的鎖住目標，同時它也是駭客發動網路攻擊的主要對象之一。鑑此，世界各國應攜手同心，積極偵辦電腦犯罪案件和提升數位鑑識之質與量水準，以有效對抗全世界共通犯罪類型──電腦犯罪。

電腦鑑識（Computer Forensics）和數位鑑識（Digital Forensics）二詞常被交換使用，其觀念源自於刑事鑑識，可謂鑑識科學的分支，只是鑑識的標的物不同。數位（電腦）鑑識需要大量的資訊科技加以輔助，用以蒐集、鑑定、分析和呈現電磁紀錄。數位（電腦）鑑識分

兩個部分，一為現場鑑識，另一為實驗室鑑識。數位（電腦）鑑識程序大致分成：（1）準備，（2）蒐集，（3）檢驗，（4）分析（含重建），（5）報告等五個步驟。其方法與原則為（1）完整性：在不改變或破壞證據的情況下取得原始證據；（2）正確性：證明所萃取的證據是來自於扣押的證據；（3）一致性：在不改變證據的情況下進行分析。數位（電腦）證據保管鏈良窳對於法定證據證明力有決定性影響。

現今數位（電腦）鑑識的理論基礎、方法論、標準作業程序和鑑定用軟硬體工具等，不斷在精益求精中；它的分支領域，如有線和無線網路鑑識、多媒體鑑識、影像鑑識、數位內容鑑識、手機或行動載具鑑識……等，也在持續發展中。未來如何將它們導入資訊應用系統以完成鑑識程序之全自動化或半自動化，亦是發展重點。總之，數位（電腦）鑑識是鑑識科學分支，其發展歷史相當短，值得大家去研究。