作業報導

●法務部調查局資安鑑識業務發展及實驗室認證介紹

法務部調查局資通安全處科長 陳受湛

壹、 緣起

科技進步帶動犯罪手法的改變，電腦和網路常被利用作為犯罪工具或進行犯意聯絡，因此如何從犯罪中找出數位證據，並以嚴謹之鑑識機制使之具有證據能力，成為司法單位偵辦犯罪的重要工作。法務部調查局(下稱本局)於民國(下同)93年成立專組受理數位證據之鑑識業務；又依據行政院國家資通安全會報「建立我國通資訊基礎建設安全機制計畫（九十四年至九十七年）」行動方案３２「建立國家級資安鑑識實驗室，提供資安網路犯罪相關技術與實務訓練教材，以及舉辦相關教育訓練」之資通安全政策要求，開始積極規劃建置國家級鑑識實驗室。

經本局向行政院提出「調查局資安鑑識實驗室」建置計畫並獲經費補助，計畫內容包括收集各國對等單位建置之實際經驗，如電腦鑑識實驗室之人員組織、功能架構、經費運用、人才培育計畫等，並藉參與國際研討會及數位鑑識專業訓練課程培育專才，採購各式鑑識軟、硬體工具設備等；另辦理環境建置整修，包含電力系統、空調系統，設置證物室、證物收件室、鑑識分析室、證據討論室等；而於 95 年底完成資安鑑識實驗室建置，並於 98 年於本局資通安全處下成立資安鑑識科，專責實驗室營運。目前實驗室成員 9 人，主要服務對象對內為本局辦案單位，有關電腦犯罪案件之現場搜索、數位證據查扣及鑑識，對外依刑事訴訟法接受院、檢之囑託鑑定。

貳、 鑑識工作項目

一、實驗室業務職掌包括下列各項：

(一) 各類數位證據之檢驗、鑑定：從證物中取得數位證據之相關資料以確認與犯罪相關之時間戳記、行為人帳號、資料存放位置、所使用軟體及版本等。

(二) 支援案件現場與網路環境之罪證擷取、記錄及保全：協助外勤單位於搜索現場取得相關數位證據。

(三) 數位證據還原與事實行為分析：硬碟資料回復及解碼並使用鑑識軟體解釋分析，重現犯罪行為。

(四) 證物管理：在鑑識過程中，對送鑑之扣押物如電腦主機、網路設備、手機、監視系統及儲存媒體進行適當管理並符合證據監管鏈之要求。

(五) 數位證據鑑識技術之研究發展：數位科技與產品發展快速，犯罪行為人會利用最新科技產品做為工具，造成取證上之困難，故實驗室每年均提出數位鑑識技術研究計畫，積極爭取經費，並與國內知名學府、民間研究機構、數位鑑識廠商等合作研究。例如今(104)年特別針對雲端環境與

行動裝置之鑑識技術進行多項合作研究，以提升實驗室之鑑識能量。

二、目前實驗室所受理鑑識之各類品項，包括桌上型電腦、筆記型電腦、伺服器主機、監視錄影器、智慧型手機、平板電腦、隨身碟、外接式硬碟、各式記憶卡及光碟等。為因應此多樣化，故所使用之鑑識工具種類亦夥，常用之資料備份工具有 AccessData 公司之 FTK Imager 及 Guidance Software™ 公司之 EnCase Forensic Imager、資料回復工具有 R-Tools Technology 公司之 R-Studio、鑑識分析工具有 Guidance Software™公司之 EnCase® Forensic Tools、硬體備份工具有 Forensic Dossier、硬碟防寫工具有 Digital Intelligence 公司之 forensic write blockers、手機鑑識工具有 Micro Systemation 公司之 XRY 及 Cellebrite 公司之 UFED 等，另備有各式鑑識平台與工作站供鑑識所需。

三、實驗室鑑識業務每年均大幅成長，無論是送鑑案件數、送鑑證物數及證物儲存容量均是如此，依各單位不同需求，利用不同的鑑識工具及技術，完成各式案件之鑑定分析報告，不只改進實驗室之運作效率，也有效提升案件中數位證據之證明力。

表 1　數位證據送鑑案數統計表

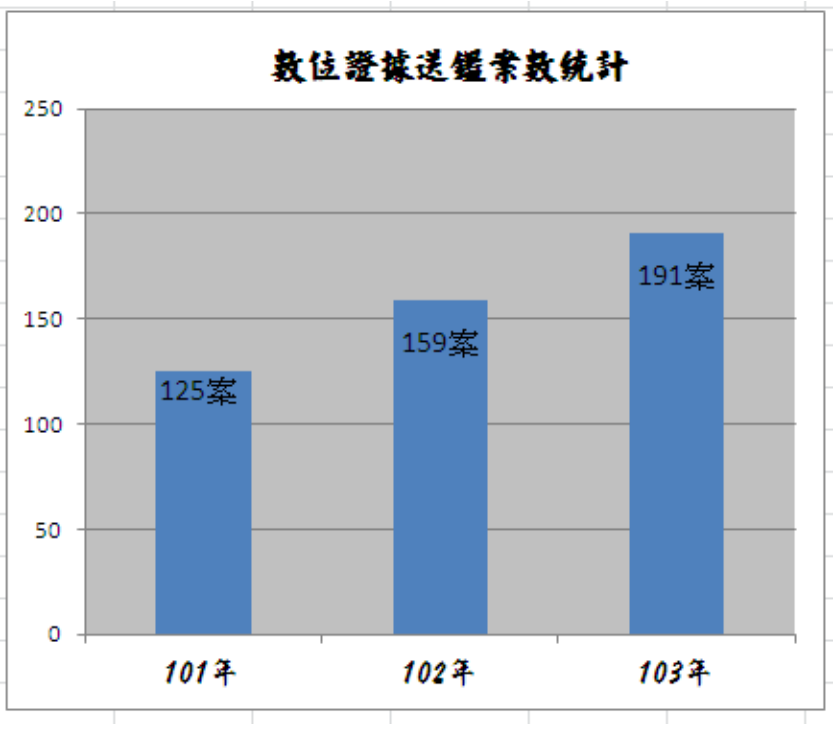


表 2　數位證據送鑑證物數統計表

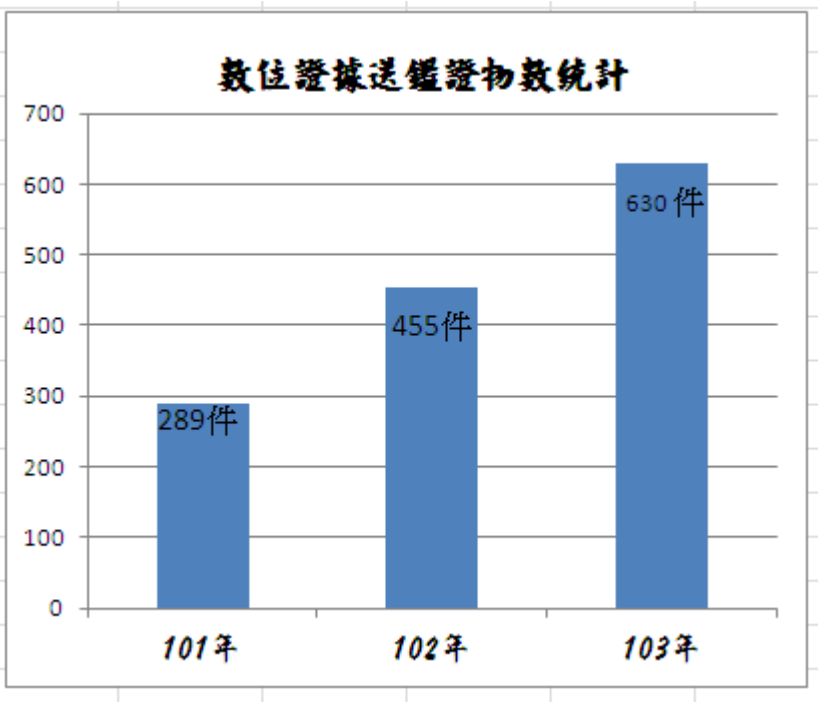
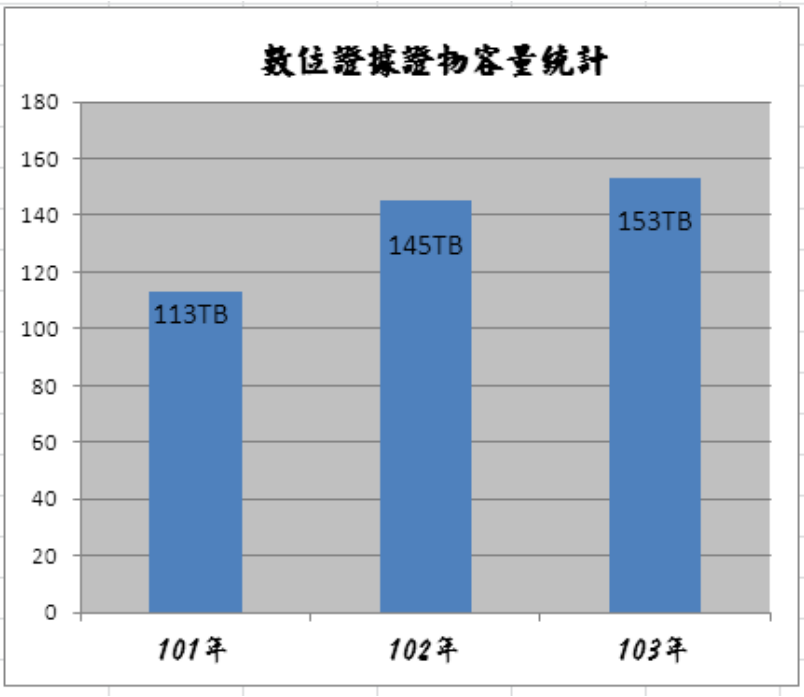


表 3　數位證據證物容量統計表



近年智慧型手機及平板電腦之開發與使用快速成長，也常成為犯罪工具，使得行動裝置之鑑識需求大幅提升；本局為因應此項鑑識需求，導入 Micro

Systemation XRY 及 Cellebrite UFED 等行動裝置鑑識工具，可攜至搜索現場擷取所扣押手機內之通訊錄、簡訊、即時通訊軟體 APP 之通聯紀錄、聲音照片影像等資料，提升可攜式行動裝置設備之現場數位證據蒐證及解讀能力。

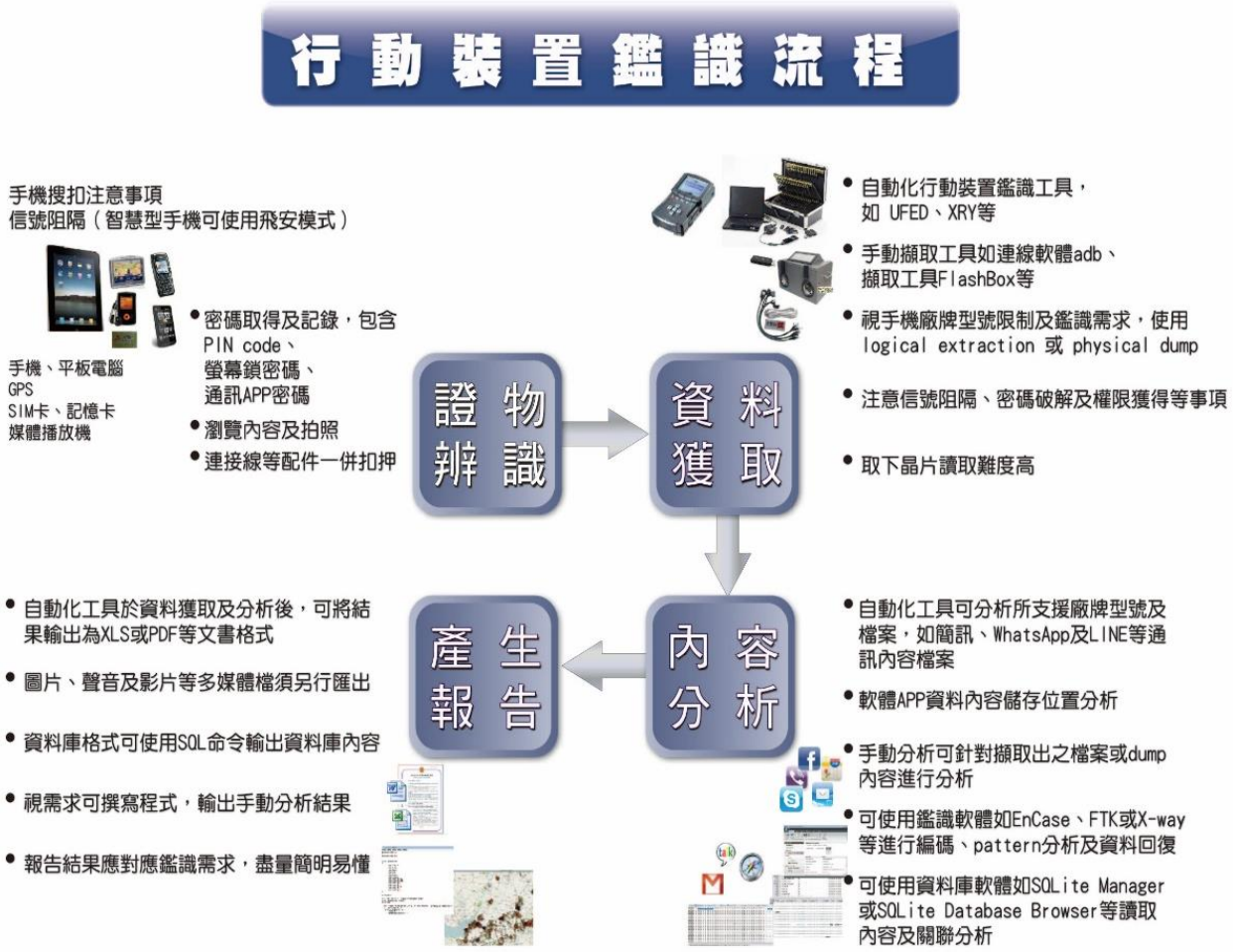


圖 1　行動裝置鑑識流程圖

又因社會上大量使用監視錄影設備，並成為鑑識案件中的需求項目，而建立了簡易及快速之多媒體檔案修復流程與鑑識方法，將已毀損無法讀取並顯示之多媒體 JPEG 影像檔、MP4 多媒體影片檔，呈現為可供檢視之狀態。另首創簡易之鑑識程序與方法，可以分辨多媒體即時通訊軟體所存放之對話紀錄及常見之 PDF 多媒體文件檔所存放之元資料內容是否經過偽變造。

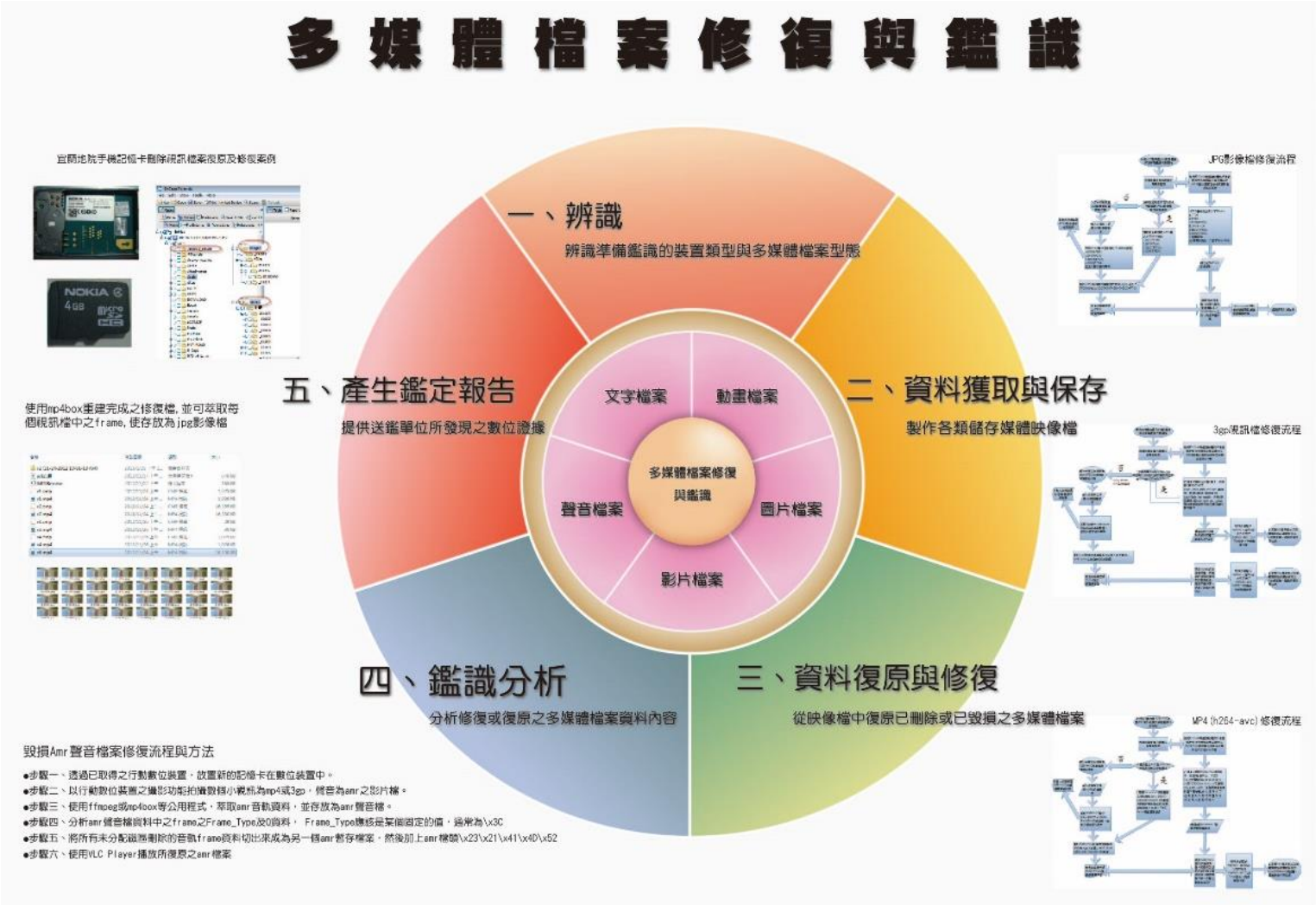


圖 2　多媒體檔案修復與鑑識圖

另針對硬碟遭破壞而無法讀取之情形，專研毀損硬碟資料回復之流程與操作技術，並於實驗室中建置「無塵室」，提供適當作業空間，希望能將硬碟修復至可讀取狀態，以利資料救援、備份，目前已有多次成功修復並將資料復原之案例。

圖 3　硬碟修復案例圖

參、 提升外勤單位鑑識能量

本局為強化外勤第一線調查人員對犯罪現場數位證據蒐證技能、證物保全與數位鑑識能力，將簡易鑑識軟體及常用資料保全工具整合成「調查局現場鑑識工具包」，逐年更新軟體，增強其功能，配發至各外勤單位使用。目前最新之工具包可於現場採集嫌疑人電腦內易揮發性資料、上網紀錄及密碼等資訊，並可快速過濾、檢視硬碟內資料；亦具有邏輯資料回復之功能，可將已刪除檔案之資料，於第一時間復原，對數位證據保存及案件調查，瞭解事實真相，有即時幫助。

同時為了讓調查人員在犯罪現場能正確分辨各式數位證物，並熟悉數位證據之搜索扣押流程及操作方式，本室於 99 年 5 月完成本局「數位證物搜索現場操作手冊」，並配發至各外勤單位參考，其中包含數位證據現場蒐證配備清單、住家型態數位證據現場搜索扣押流程、公司型態數位證據現場搜索扣押流程、數位證據辨識與扣押等。又因數位證據的快速演變與多樣化，手冊內容已不敷所需，復於 103 年 12 月增修完成「數位證據保全標準作業程序規範暨現場數位證據保全操作手冊」，特別強調現場蒐證時之作業程序，包括數位證據之識別標示、蒐集擷取、封緘保管等現場數位證據保全流程，提供外勤單位依循。

又為強化外勤第一線人員現場數位證據保全及鑑識之能量，自 102 年起舉辦組織學習，以台北、新北、台中、台南及高雄五都調查處為軸心，轄下資通安全科為召集單位，聯合周邊縣市站為聯盟，利用講習及實際心得交換方式，發揮群聚效應與聚落效果，推動現場數位證據鑑識工作。本局於 102 年辦理 20 場組織學

習，參加人員超過 500 人次，103 年辦理 15 場組織學習，參加人數亦有 400 人次以上。經過這兩年的訓練，外勤單位對現場數位證據保全及鑑識能力已大幅增強，成為面對現場之第一線主力，實驗室人員支援外勤單位現場數位證據搜索之頻率降低，而能多用心於實驗室鑑識工作及技術突破，成為專注鑑識研究之第二線。

肆、 制定標準作業流程

為使鑑定報告具有證據能力及證明力，前提之一就是自取證迄鑑定報告完成過程沒有暇疵。本室為維護數位證據的完整性(Integrity)與正確性(Correctness)，足以成為具有法律效力的數位證據，能為民眾、法院所能接受，本室經常與產、官、學各界利用委託研究之機會，探討各項「數位證據保全」之安全控管及驗證機制，以確保各送鑑證物不致遭到污染或破壞，次參考國外鑑識機構實際作業流程，結合本局犯罪調查手冊，且經多次研修，訂定本局數位鑑識標準作業程序、以及相關規範，以確實達到數位證據之公正性、合法性、完整性與正確性。

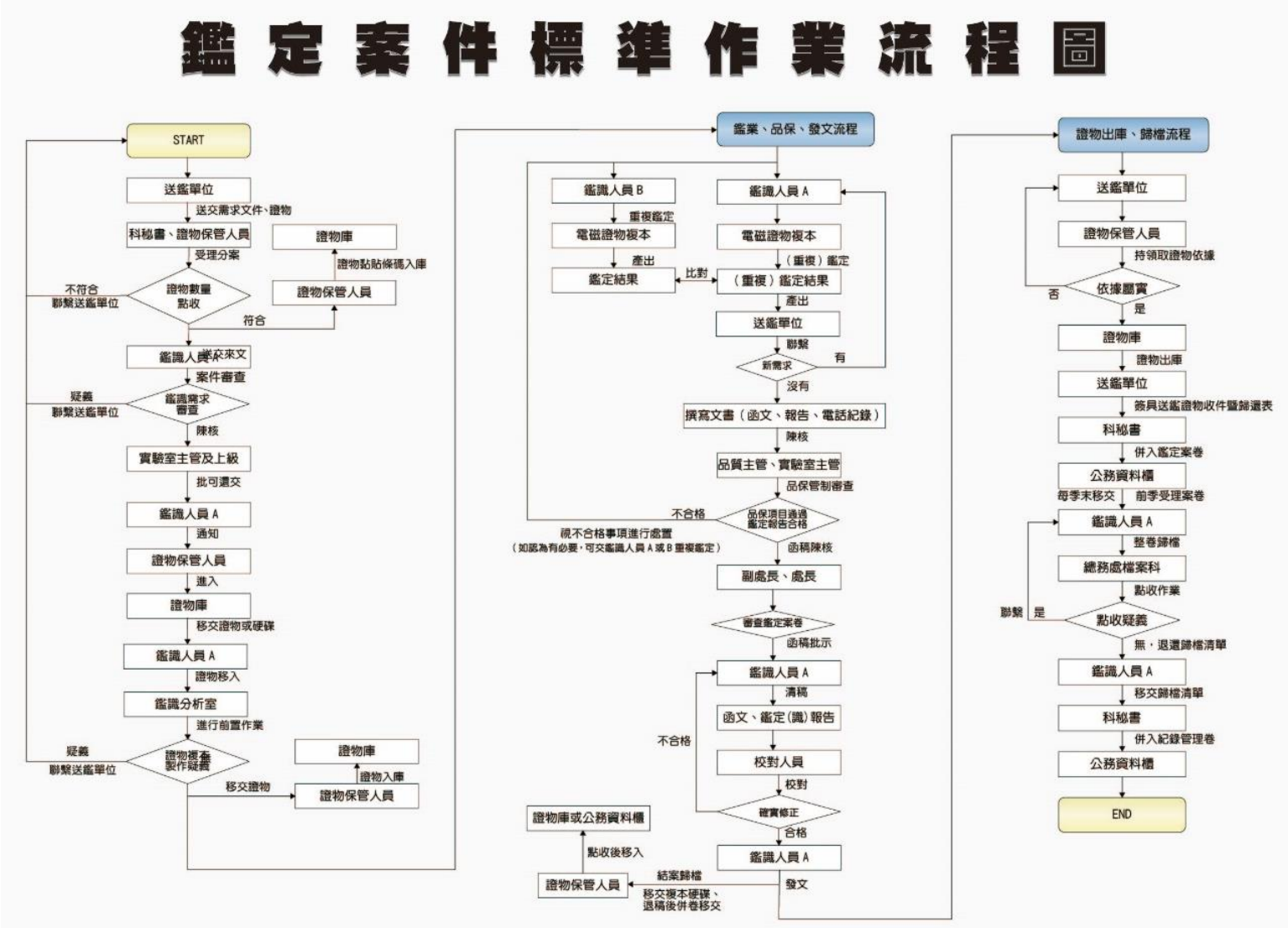


圖 4　鑑定案件標準作業流程圖

伍、 實驗室認證

本室成立之初即為取得認證作準備，先是在 97 年取得英國標準組織（BSI）ISO 27001 之資訊安全管理系統(ISMS)認證，又於 98 年 9 月開始規劃進行實驗室認證整備工作，邀集全國認證基金會(Taiwan Accreditation Foundation，TAF)、本局鑑識科學處「DNA 鑑識實驗室」等單位蒞室講授認證作業須知，並因應認證需要，全員均參加並通過 TAF 實驗室認證規範 ISO/IEC 17025 之教育訓練。因國內尚無已取得認證之同屬性實驗室可供參考，故有關鑑定作業標準流程、方法原理確效、設備功能查核、證物管制程序、人員資格認定、品保管制審查等認證核心項目，僅能由實驗室同仁共同討論訂定實行，並就發現之缺失，逐步調整改善以制訂完善流程，進而完成書面之品質文件，以達到規範中「說」「寫」「作」一致之要求並留存其紀錄。

本實驗室於 101 年 4 月 5 日完成品質文件第 1-1 版，後續亦逐一完成 TAF 所要求之內部稽核、外部稽核、功能確效、管理審查會議等項目，並於 102 年 5 月向 TAF 提出初次認證申請，申請認證領域為測試領域，申請認證項目為 Z078 資訊重現(硬碟、隨身碟、記憶卡、光碟)，包括刪除資料復原及關鍵字搜尋兩項認證項目。TAF 於 10 月 31 日至 11 月 1 日至本局進行現場評鑑，於 11 月 29 日寄發評鑑結果通知書函及認證合格證書，同意本實驗室於出具鑑定報告時，使用認證標誌，並於 103 年 2 月 12 日，由當時擔任行政院政務委員之張副院長善政見證下，TAF 頒發本局「資安鑑識實驗室」認可證書，成為國內第一所取得「資訊重現」項目之鑑識科學實驗室。也因 TAF 為國際實驗室認證聯盟(International Laboratory Accreditation Cooperation，ILAC)簽署會員，在其相互承認協議(Mutual Recognition Arrangement，MRA)機制下，本局資安鑑識實驗室同時取得包括美、英、加等國在內的全球 74 個經濟體與 89 個認證機構之認可。且為維持認證，又於 103 年 10 月 9 日通過該年度之監督評鑑，在新進人員訓練、內部稽核、證據監管鏈執行及使用設備查核上，展現優秀的維持能力獲得評鑑人員肯定，爾後仍將積極規劃行動裝置鑑識等之認證，俾能符合實務所需、與時俱進。

陸、 結語

國際上各執法機構皆十分注重數位鑑識之發展，而在雲端環境鑑識、虛擬主機資料擷取與鑑識、加密資料破解密、手機密碼破解等技術方面，都有許多待努力與解決之處，本局資安鑑識實驗室仍將持續在人才培育、設備更新、創新研究及國際交流等項目上尋求突破，持續為數位證據鑑識工作提供先進而完整之服務。