DOI: 10.6482/ECPCR.201910.0014

建立整合性行動鑑識標準作業程序（iDEFSOP-MF）與實際案例驗證之研究—以刑事警察局破獲之實際案例及驗證為例

林宜隆*

目　次

摘　要

我國政府除了 2011 年訂定個人資料保護法外，並於 2016 年以捍衛國家數位國土、防護數位經濟為號召，召開「資安即國安」策略會議、且 2016 年 8 月設置行政院資通安全處，並著手推動「資通安全管理法」立法（2018 年 5 月 11 日立法院三讀通過條文 , 並已於 2019/01/01 施行），以期針對政府機關和部份民間企業提出明確的資通安全規範與相關子法（建議要符合相關國際標準如 ISO27003+ISO27701+ISO27035+ISO27017+ISO27037+ISO27041~43 等）。2016 年總統府國家安全會議更和行政院一起召開第一次的「資安即國安」策略會議，主要是透過整合資安人力、資安產業和科研資源，以提升資安基礎整備、產業能量和數位防衛能力，最終希望可以達成：打造**國家級的資安機制**；建立國家級資安團隊，確保數位國土安全；以及推動國防資安自主研發，強化產業發展等三大目標。（建議其資安相關作為應提升其資安鑑識機制能量及資安技術能力 , 且進一步應符合國際資安鑑識標準如 ISO27005+ISO27009+ISO27037+ISO27041+ISO27042+ISO27043+I

* 林宜隆，元培醫事科技大學資訊管理系教授，台灣數位鑑識發展協會（ACFD）創會理事長，前中央警察大學教授，法務部調查局資通安全諮詢委員，消基會資通訊委員會副召集人，Email: cyberpaul747@gmail.com。

SO27050 等）。

有鑑於我國的現行法規制度下，數位（資安）鑑識尚未明確專章立法（雖然資通安全管理法於去（107）年 05 月 11 日立法院三讀通過，今（108）年 01 月 01 日施行），偵查機關對於數位（資安）鑑識之規範、標準、程序及方法論亦無從遵循，藉由蒐集國內外數位（資安）證據、數位（資安）鑑識機制（如 DEFSOP, Forensics Computing 4P's Model）、國際標準作業程序等文獻，並參考 ISO/IEC27037:2012、ISO/IEC27041:2015、ISO/IEC 27042:2015 及 ISO/IEC 27043:2015 等國際標準程序之管理要項及指引，整合數位鑑識作業程序進行研究及探討對應，以國內學者林宜隆教授所提出數位證據鑑識標準程序（DEFSOP）四個階段（原理概念階段、準備階段、操作階段、報告階段）為基礎，建立一套整合性行動鑑識標準作業程序（iDEFSOP for Mobile Forensics, iDEFSOP-MF），透過刑事警察局破獲之實際案例加以驗證，並使用國際大廠 Cellebrite UFED 鑑識軟體，輔以標準作業程序來驗證、還原整個資安（犯罪）事件，希冀讓偵查及資安人員從整個案件之偵查流程（What to do）、偵查作為（How to do），來瞭解鑑識的重點及方向（Why to do），提供資安（犯罪）事件處置的原則與準則證明不僅強化數位（資安）證據蒐集和舉證，並確保資安落實，提升數位（資安）證據在法庭上之有效性（含證據能力及證據證明力）及公信力之目標外，更可在未來針對資安事件（如 ISIM:ISO27035:2016）做有效之預防機制及應變處置。

關鍵字：iDEFSOP-MF、數位證據、數位（資安）鑑識、行動鑑識、國際標準作業程序

Establishing an Integrated Digital Evidence Forensics Standard Operating Procedure for Mobile Forensics (iDEFSOP-MF) and Actual Cases Verification Research—taking the actual cases and verification of the Criminal Investigation Bureau as an example

I-Long Lin*

Abstract

In addition to the personal information protection law in 2011, the government has called for the protection of the national digital homeland and the protection of the digital economy in 2016. The “Cyber Security is National Security” strategy meeting was held, and the Department of Cyber Security of the Executive Yuan was set up in August 2016. And proceeded to promote the " Cyber Security Management Act" which was implemented at 2019/01/01, with a view to making clear cybersecurity recommendations for government agencies and some private enterprises. The codes of Cybersecurity and related sub-laws (It is recommended that must comply with relevant international standards such as ISO27003+ISO27701+ISO27035+ISO270 17+ISO27037+ISO27041~43, etc.). In 2016, the National Security Council of the Presidential Office held the first "Cyber Security, is National Security" strategy meeting with the Executive Yuan, mainly through the integration of cybersecurity manpower, cybersecurity industry and scientific research resources to improve the cybersecurity infrastructure, the cybersecurity industrial energy and the digital defense capabilities, the ultimate hope can be achieved: to build a national-level cybersecurity mechanism; to establish a national-level cybersecurity team to ensure digital homeland security; and to promote independent research and development of defense cybersecurity, and strengthen industrial development and the three goals. (It is recommended that its cybersecurity as a related should enhance its cyber forensics mechanism and cybersecurity technology capabilities, and should further

* I-Long Lin, Professor, Department of Information Management/Master's Program in Digital Technology Innovation and Management of Yuanpei University of Medical Technology, E-mail: cyberpaul747@gmail.com

comply with international cyber forensics standards such as ISO27005+ISO27009 +ISO27037+ISO27041+ISO27042+ISO27043+ISO27050… etc.).

In view of national current laws and regulations, the digital (cyber) forensic has not yet clear the special chapter legislation (although the Cyber Security Management Act was passed on the Legislative Yuan on May 11, 2018,was implemented on January 01,2019). The police investigative agency has no way to follow the norms, standards, procedures and methodology of digital (cyber) forensic knowledge, by collecting domestic and foreign digital (cyber) evidence, digital (cyber) forensic mechanisms (such as DEFSOP, Forensics Computing, 4P's Model), international standard operating procedures and other documents, and refer to ISO/IEC27037:2012, ISO/IEC27041:2015, ISO/IEC 27042:2015 and ISO/IEC 27043:2015 and other international standard procedures management requirements and guidelines, integrated digital forensic operation procedure conducts research and explores the correspondence, and establishes an integrated the Digital Evidence Forensics Standard Operating Procedure (DEFSOP) for Mobile Forensics (iDEFSOP for Mobile Forensics, iDEFSOP-MF) based on the four stages of proposed by the domestic scholar Professor Lin I-long (the principle concept stage, the preparation stage, the operation stage, and the reporting stage). In view of the standard operating procedures (iDEFSOP for Mobile Forensics, iDEFSOP-MF), verified by the actual cases cracked by the Criminal investigation Bureau(CIB), and using the international company Cellebrite UFED In view of the software, supplemented by standard operating procedures to verify and restore the entire cybersecurity(crime) incident, hope that the investigation and cybersecurity professionals from the entire case of the investigation process (What to do), detection as (How to do), to learn about the focus and direction of cyberforensics (Why to do), the principles and guidelines for the provision of cybersecurity (crime) incidents prove that not only strengthen the digital (cyber) evidence collection and proof, but also ensure the implementation of the cybersecurity, improve the digital (cyber) evidence in court In addition to the effectiveness of the evidence (including the admissibility of the evidences and the weight of the evidences) and the credibility of the goal, it can also be an effective preventive mechanism and response for future events (such as ISIM: ISO27035:2016).

Key Words: iDEFSOP-MF, Digital Evidence, Digital (Cyber Security) Forensics, Mobile Forensics, International Standard Operating Procedures

緒論

近年來，行動互聯網（Mobile Internet）及行動裝置（Mobile Devices）的出現讓人們生活對它的依賴度與日俱增，大量網路使用者湧入網路世界（如2019年06月止全球人口約76億人，而全球網際網路用戶已突破41億人大關，其所占全球人口之比例已超52%，且全球行動網路用戶（Global Mobile Internet Users）已突破38.5億人大關，另FaceBook用戶已突破24億，LINE用戶已突破11億），各行各業無不透過行動互聯網及行動裝置方式來進行資料的輸入、處理、儲存、保管及使用，使得人類與各類資訊零距離，然而「水能載舟，亦能覆舟」，經過電腦數位化處理後，網路資通安全事件（ISIM）亦隨之不斷發生，嚴重影響人民智慧生活。

因此，如何在資安事件（ISIM）發生前建立及妥善保存數位證據的準備，以及事件發生中和發生後，透過各種管道蒐集有利之數位證據、資安現場、鑑識資安事件之本質與歷程，對於維護我國整體網際網路（互聯網）安全之必要性與急迫性甚為重要。以目前我國的執法現況，符合國際標準的蒐證程序尚未明確建立，使得司法官對於蒐集數位證據的證據能力及證明力明顯不足（如107年2月11日台灣高檢署開始在8個地檢署，成立〈**數位採證中心**〉），以致無法由蒐證的數位證據中直接判斷，導致法庭上之爭議不斷，再加上目前我國對於數位行動鑑識方面，較少有相關研究及標準作業程序。

近年來，許多重要資通訊安全事件接連發生，很多都造成企業與社會的衝擊。隨著網際網路技術（ICT）的提升與網際空間（Cyberspace）的擴大，手機不再是傳統的通話功能，透過智慧型手機，可以使用通訊軟體互相聯絡（如LINE、Messenger、Wechat、Juiker）、上網瀏覽網頁與交易、儲存個人相關資訊數位記錄（如照片、記事等），如同行動電腦。手機帶來的便利性，成為有心人士的網路（數位）犯罪工具（如2016年07月第一銀行ATM盜領案、2016年中華郵政商城網路個資外洩案、2017年2月臺灣史上第一次券商集體遭DDoS攻擊勒索事件、2017年5月新型勒索病毒WannaCry重創臺灣、2017年6月全球多個國家遭受新一輪Petya勒索病毒攻擊、2017年10月駭客入侵遠東銀行SWIFT系統 、2016年網路詐欺、2017年智慧型手機詐欺、2018/2019年個資外洩等），以及鴻海、聯發科、台塑化與長春等企業之內賊竊取商業機密事件等。面對層出不窮的資通訊安全事件。

智慧型手機如同行動電腦存在大量的電磁記錄（即數位證據），這些記錄是具備鑑識價值的數位證據。基於資通訊安全事件偵測及偵查（如國際標

準 ISO27043），以及司法訴訟舉證（如國際標準 ISO27037 及 ISO27041）之需求，證據保全及數位鑑識將扮演非常重要角色。數位鑑識乃針對資安事件進行事前蒐證、事中分析與事後報告（如國際標準 ISO27041、ISO27043 及 ISO27050），在事件發生後鑑識報告可作為法律訴訟證據，並符合 DEFSOP（Digital Evidence Forensics Standard Operation Procedure by Paul Paul and Jill Slay）數位證據鑑識標準作業程序及 CIAC（Consistence, Integrity, Accuracy, Compliance by paul Lin）鑑識基本原則，並透過調整公司資安政策達到預防企業機密資料外洩、保護個人資訊資料、避免駭客攻擊等符合資安鑑識科學 4P'S Model（Prevention, Protection, Preservation and Presentation）資安防護機制措施，有助於揪出企業內外的有心人士，協助政府及企業保護相關機敏資料與資安鑑識人才培育。

本文探討整合數位鑑識作業程序進行研究及探討對應，以國內學者林宜隆教授所提出數位證據鑑識標準程序（DEFSOP）四個階段（原理概念階段、準備階段、操作階段、報告階段）為基礎，並整合國際標準作業程序 ISO 27037:2012、ISO 27041:2015、ISO 27042:2015 及 ISO 27043:2015 比較分析，藉此強化及整合數位證據鑑識標準作業程序的有效性（含證據能力及證明力），進而建立一套整合性行動鑑識標準作業程序（Integrated Digital Evidence Forensics Standard Operating Procedure for Mobile Forensics, iDEFSOP for MF），透過刑事警察局破獲之實際案例加以驗證，並使用國際大廠 Cellebrite UFED 鑑識軟體，輔以標準作業程序來驗證、還原整個資安（犯罪）事件，希冀讓偵查及資安人員從整個案件之偵查流程（What to do）、偵查作為（How to do），來瞭解鑑識的重點及方向（Why to do），提供資安（犯罪）事件處置的原則與準則證明不僅強化數位（資安）證據蒐集和舉證，並確保資安落實，提升數位（資安）證據在法庭上之有效性（含證據能力及證明力）及公信力之目標外，更可在未來針對資安事件做有效之預防機制及應變處置。

iDEFSOP-MF 進一步供檢、警、調偵查人員在處理數位證據時的參考，最終目的在協助執法單位對於數位證據之處理時遵循之依據，確保所蒐集到的證據具有效性（含證據能力及證據證明力），使其證據在法庭上更具公信力外，更可在未來針對資安事件（如 ISIM:ISO27035:2016）做有效之預防機制及應變處置。

壹、文獻探討與理論基礎

一、數位證據與行動鑑識

（一）數位證據

數位證據具有易修改性、無限複製性、不易個化性、無法直接以感官知覺和理解等特性，呈現之方式亦有多種型態，另外，數位證據係網路犯罪案件中非常重要的線索對於數位證據概念的界定，常存在不同認識，國外學者 Casey 在其著述「Digital Evidence and Computer Crime」一書中談論到有關於數位證據的定義，認為任何使用電腦儲存或傳輸的數據資料，用於支持或反證犯罪，或可以用來表達犯罪動機、犯罪現場等關鍵要素，為物理證據的一種，包含文字、圖片、聲音、影像等類型，具有可無限無差異複製、不易銷毀、原始作者不易確定、資料完整性驗證等性質，亦稱電腦證據或電子證據。1998 年加拿大在統一數位證據法中認為”電子記錄”是指保存在電腦系統或其他類似裝置的任何媒介上，能夠被個人和計算機系統以及其他類似裝置瀏覽或察覺的數據。

我內學者林宜隆教授認為數位證據係：「任何使用電腦或相關電子設備儲存、傳輸的電磁記錄，包含：文字、聲音、影像、圖片、符號或其他資料，凡是可以透過適當設備讀取出來的電磁記錄，可用於支持或反證犯罪，或可以用來表達犯罪動機、犯罪現場等關鍵要素都可稱為數位證據」。根據我國法律及學者的定義，將其定義為藉由電腦或網路設備儲存或傳送可供證據使用，稱之為數位證據，即包括電子文件、電子紀錄及電磁紀錄。因此，唯有專業的鑑識人員，嚴謹的鑑識流程，以及專業的鑑識工具，才能確保蒐集到的數位證據具有法律效力及避免同樣的證據產生不同的解讀。

（二）數位鑑識

數位鑑識（Digital Forensics），又稱資安鑑識（Cyber Forensics），統稱為資安數位鑑識科學，主要是針對數位裝置中的內容進行調查與復原，提到資安數位證據鑑識不單僅限於電腦鑑識、網路鑑識，凡是以數位方式儲存的相關設備都應包含在數位鑑識的領域中，數位鑑識包括涉及不同技術的各個領域，包括：電腦、手機、iPad、數位相機、記憶卡、網路設備等數位設備，另外亦包含通訊軟體 LINE、FB Messenger、Skype Messenger、Twitter 等。我國學者林宜隆教授認為資安數位鑑識範圍應該包含電腦鑑識

（Computer Forensics）、軟體鑑識（Software Forensics）、資料鑑識（Data Forensics）、網路鑑識（Network Forensics）、行動鑑識（Mobile Forensics）以及雲端鑑識（Cloud forensics）等 6 大類（林宜隆，2012）（如圖 1）。數位鑑識工作除了必須具備高水準的鑑識工具及相當程度的網路犯罪手法的分析外，還必須熟悉各種複雜的數位鑑識工作、流程，因此，對於數位鑑識人員而言，數位鑑識的知識管理及精進訓練課程顯得相當重要。

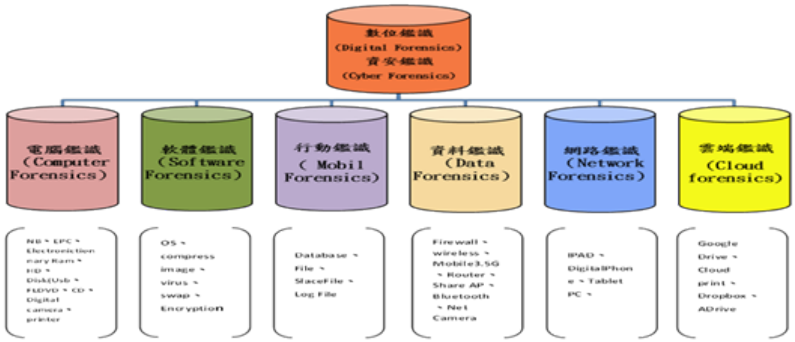


圖 1　資安數位鑑識類型

（三）行動鑑識

行動鑑識（Mobile Forensics）屬於數位鑑識的其中一部份，指所有對行動裝置上的數位資料進行保存、識別、萃取、分析及鑑定的行為。數位鑑識（Digital Forensics）又稱電腦鑑識（Computer Forensics）或資安鑑識（Cyber Forensics）屬於鑑識科學的分支，用以取得數位資料中存在的數位化法律證據。數位鑑識可以定義為：利用科學驗證的方式調查數位證據，經由數位證據的擷取、分析、還原等過程，還原事件原貌，以利事件調查，並提供法庭訴訟之完整依據。手機中儲存的資料，以電磁紀錄存在，此即所謂的數位證據，手機上的證據，屬於數位證據在行動鑑識的延伸。

「資安鑑識（Cyber Forensics）」為台灣數位鑑識發展協會（ACFD）創會理事長林宜隆教授所提出最新名詞，資安鑑識廣義領域包括「資安預防（Prevention）、資安防護（Protection）、證據保全（Preservation）及專業鑑識（Presentation）」等四大階段，由國內學者林宜隆教授與澳洲 Jill Slay 教授所提出之 4P's Model 理論，於資安鑑識領域中要如何建立需具備強大資安鑑識機制能量與資安技術防護能力，其應包括 CyberLab 實驗室（如符合 ISO17025）、標準作業程序 SOP（如符合 ISO27037）與國際專業鑑識人才（如符合 ISO17024）。[資安鑑識機制能量 =ICT（Lab.）+SOP+ 專業（國際證照）人才，by Paul Lin]

二、標準作業程序

（一）ISO 27037:2012（Digital Evidence Handling Process）數位證據處理程序

國際標準 ISO/IEC 27037 係針對資訊安全事件發生時，對於調查數位證據各個階段提供明確的具體實作及證據價值的保護準則，處理數位證據程序分成四個階段（如圖 2），分別為識別階段（Identification）、蒐集階段（Collection）、萃取階段（Acquisition）及保存階段（Preservation）。

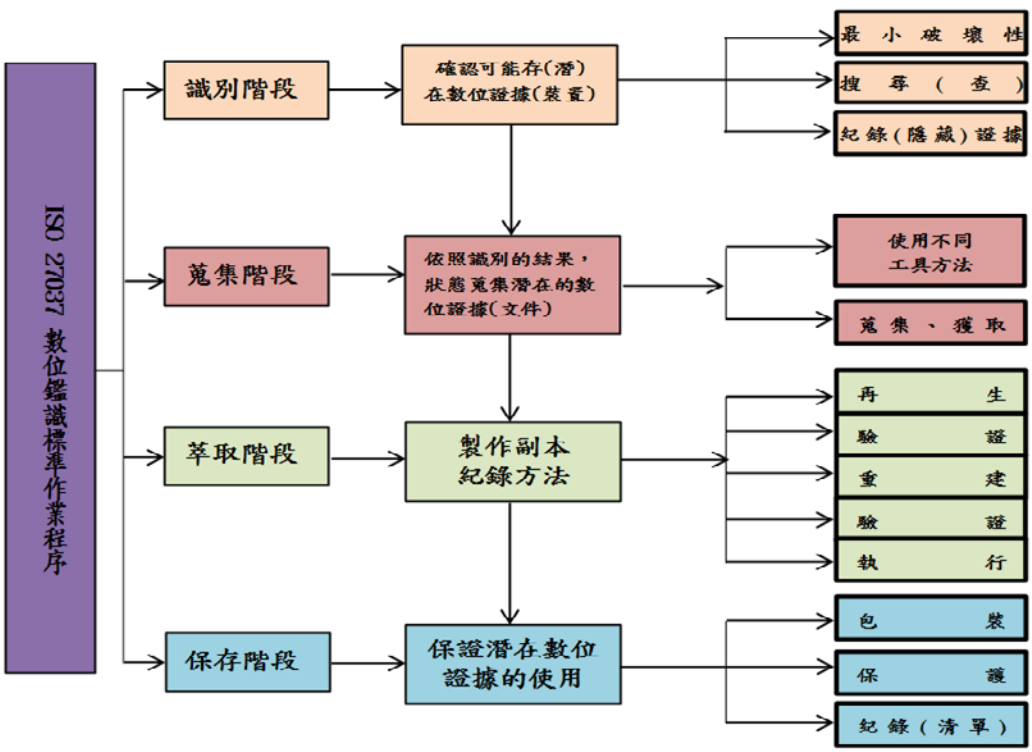


圖 2　ISO/IEC 27037: 2012 數位證據處理程序

1. 識別階段（Identification）

此階段必須在同一個準則之中，在對證據最小程度破壞且能取得最好證據的方式進行蒐集、萃取。任何形態的數位裝置都可能包含了潛在的數位證據。

2. 蒐集階段（Collection）

蒐集是一個裝置在數位證據處理程序的流程，包含潛在數位證據的裝置可能有多個狀態，它可能是正在運作或是關閉的狀態。

3. 萃取階段（Acquisition）

處理人員必須依據不同的情況、損失、時間、文件以判斷採取合適的萃取方式。且應該在最少侵入的方式獲得的潛在數位證據，以避免任何會破壞的行為。

4. 保存階段（Preservation）

必須保證潛在的數位證據在整個調查期間是可以使用的，保存程序應該開始和維持遍及整個數位證據處理程序，並開始於數位裝置、潛在數位證據的識別。

（二）ISO/IEC 27041:2015（Guidance on assuring suitability and adequacy of incident investigative method）資安事件調查方法指引

國際標準 ISO/IEC 27041 提出資訊安全事件調查方法指引，以確保調查中所使用的過程和方法是適當的，包括如何使用提供廠商和第三方之測試，以保證過程的審查。為確保調查事件中使用的方法及流程，其開發和部署程序包括需求獲取和分析、工具設計、程序實行、程序驗證（可選擇與非必要）、過程驗證、確認、部署、檢討和維護等共 8 階段（如圖 3），各階段分述如下：

1. 需求獲取與分析（Requirements capture and analysis）

審查過去使用的設計工具，應依照良好的實作，提出正確和完整記錄的需求，每個需求應該是必要、自由執行、明確、完整與一致，以符合程序的要求。

2. 程序設計（Process design）

程序設計應考慮要求獲取和分析，並確定所有要求如何實現，同時接受非功能性需求，以指出選擇哪種工具應須執行。

3. 程序實行（Process implementation）

完成設計後，應實施記錄詳細的工作指令，提供每一步正確操作過程的說明的形式。

4. 程序驗證（Process verification）

在驗證過程中，審查過程可以修改，以反映實施過程的變化。驗證通常使用「白箱測試」實行，以便考量與設計程序的比較。

5. 過程驗證（證明）（Process validation）

在工作指導驗證示範定義的程序，應符合客戶的要求，在可能的情況下，驗證過程應確定範圍條件和錯誤率。

6. 確認（Confirmation）

依照過去的調查，確認是驗證或重新驗證的最後一步，或是接續進行

下一階段。

7. 部署（Deployment）

一旦部署程序被接受，便可在調查中完成審查。

8. 審查和維護（Review and maintenance）

其目的係在維護各個階段的完成，以確保處理程序的完整性與一致性，使數位證據具有證明力及證據力。

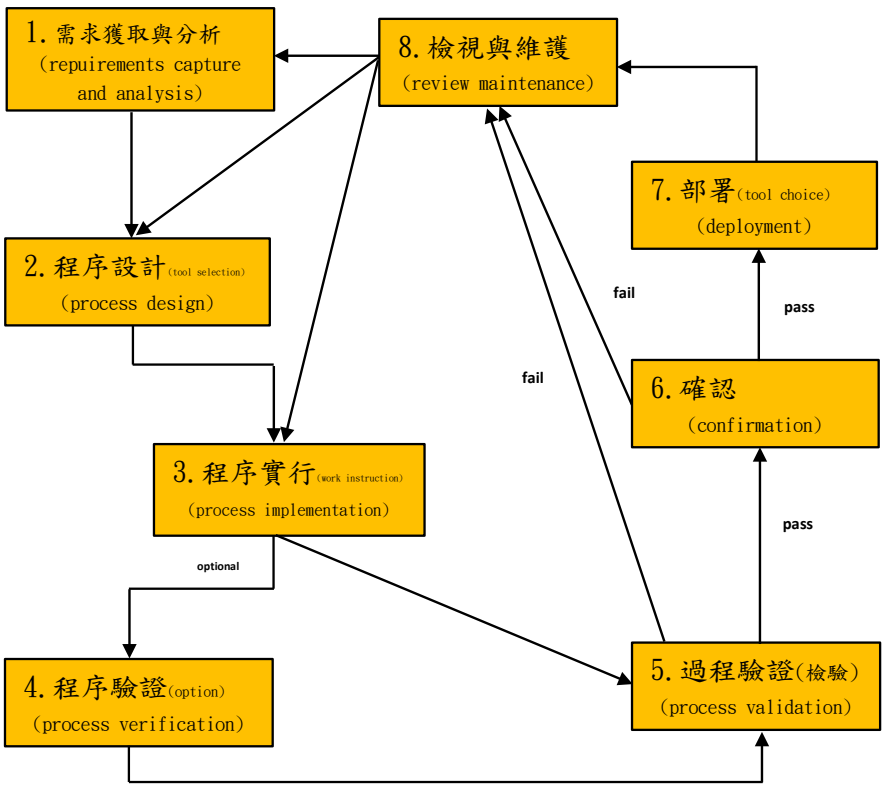


圖 3　ISO/IEC 27041: 2015 資安事件調查方法指引

（三）ISO/IEC 27042:2015（guidelines for the analysis and interpretation of digital evidence）數位證據分析與解釋指引

國際標準 ISO27042:2015 提供對於數位證據分析與解釋方式的指引，適用於每個案件的證據分析過程，並作適當的資訊記錄，使提出這些程序時受到獨立的審查（如圖 4）。

1. 調查（investigation）

主要目的是針對事件發展的理解，在進行調查時，應對事件進行全面性的理解以確定採取什麼行動，包括民事或刑事訴訟事件發生後提起

的法律行動。

2. **分析（analysis）**

分析需要從潛在的數位證據的來源來識別與評估，可以作為確定每個數位證據案件反覆運作的過程，並重新審查其他數位證據。

3. **解釋與審查（interpretation）**

解釋的目的是透過實現資料評價和分析而產生數位證據的意義，透過檢查和分析的過程找出事實真相。

4. **報告（reporting）**

報告應包含適合當地的政策或法律所需的所有資訊。相關報告文件的描述是使用範本、標準化的格式、下拉式選單。

5. **資格能力（Competence）**

沒有能力的人參與的事件調查可能會影響或延誤以致產生不正確的結果。

6. **熟悉程度（Proficiency）**

測試能力與熟練度的程序，可以由獨立的第三方證明

圖 4　ISO/IEC 27042 數位證據分析與解釋指引

（四）國際標準標準作業程序 ISO/IEC 27043:2015（Incident investigation principles and processes）資安事件調查原則與程序

國際標準 ISO/IEC 27043 提供基於常見事故調查程序理想化模型與涉及各種事件數位證據調查方案的指導方針，包含準備程序、開始程序、獲取程序、調查程序、及其各項子程序（如圖 5），各項執行程序如下：

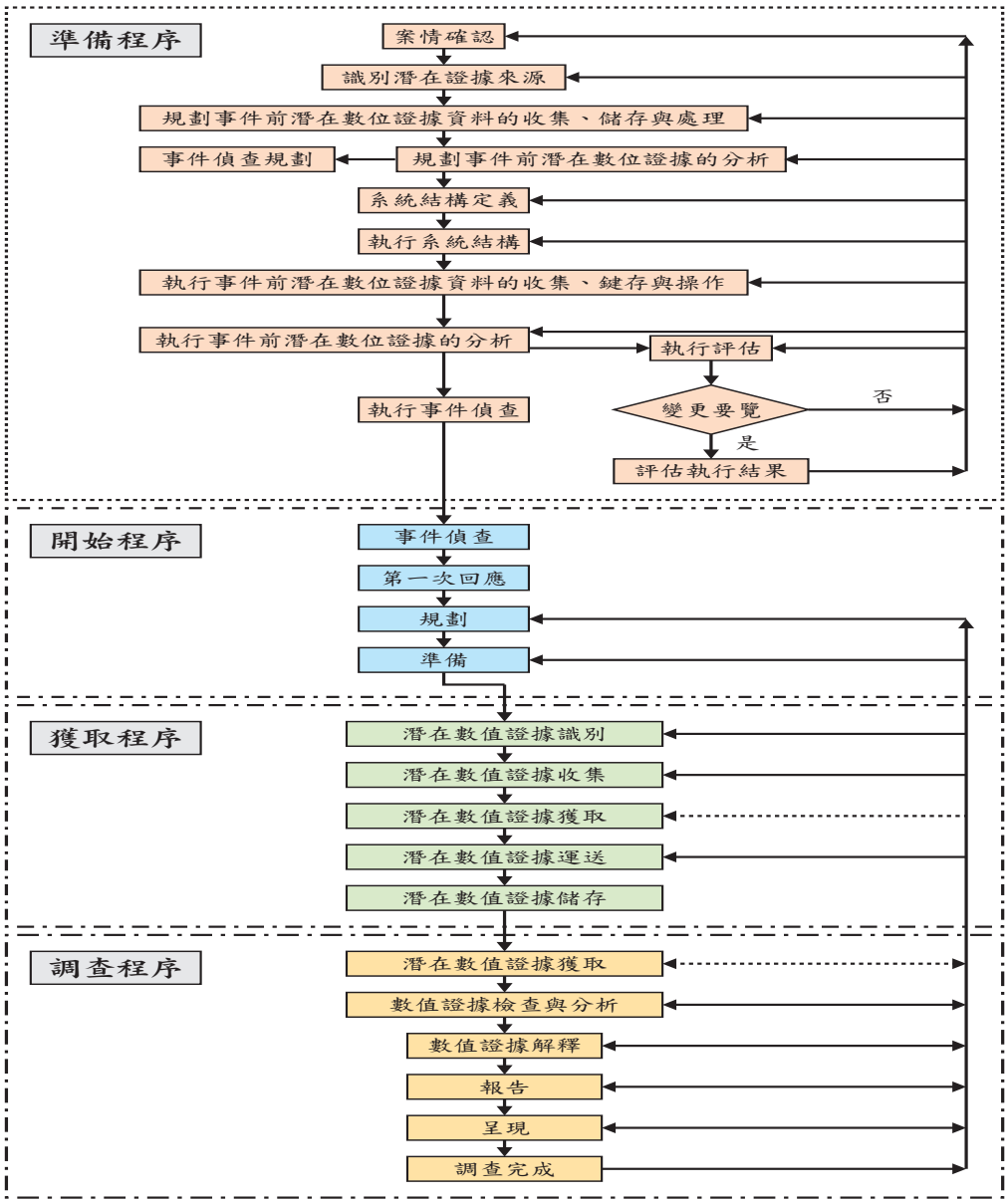


圖 5　ISO/IEC 27043 資安事件調查原則與程序

1. 準備程序

程序是數位調查程序可選擇性的，因為它本是組織執行的特定權力，而不是研究人員的任務。

2. 開始程序

包括處理事件的第一次反應和規劃，以及其他數位事件調查程序的準備。

3. 獲取程序

獲取的程序類包括與潛在數位證據蒐集的有關程序。

4. 調查程序

調查程序類型包括事件調查、數位原因的調查。

三、數位證據鑑識標準作業程序

由國內學者林宜隆教授所提出的數位證據鑑識標準作業程序（DEFSOP），可分為原理概念階段、準備階段、操作階段及報告階段等四大階段（如圖 6）：

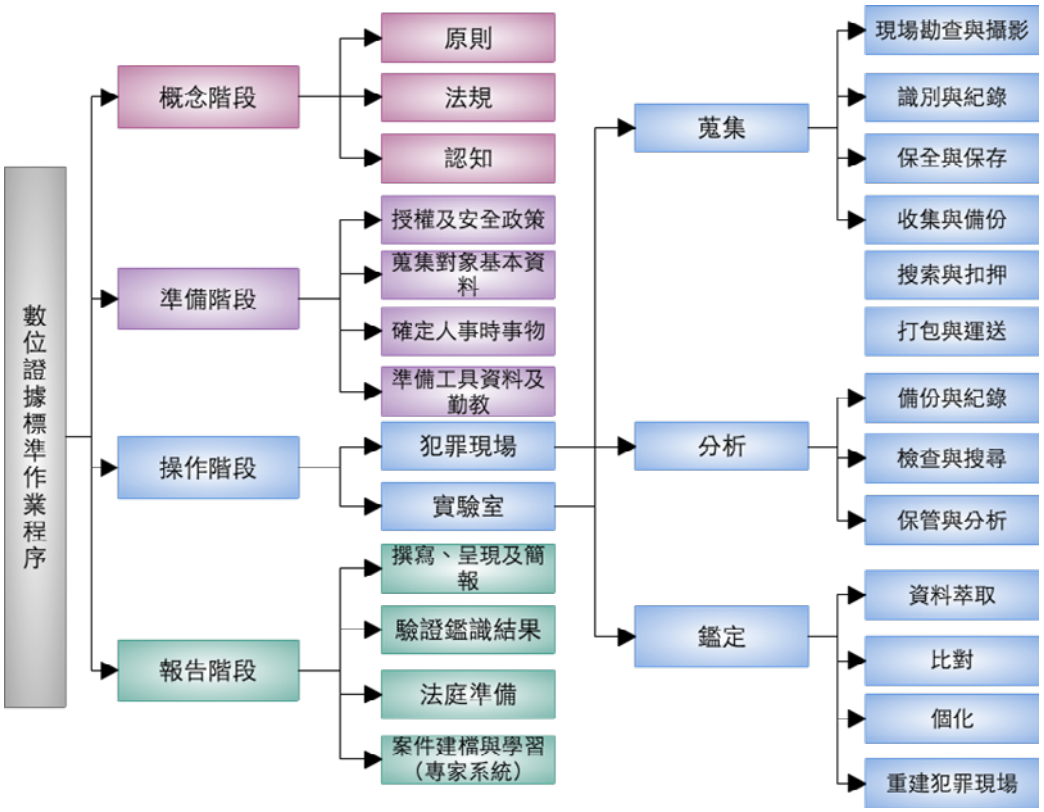


圖 6　數位鑑識標準作業程序（林宜隆，2012）

（一）原理概念階段：本階段分為原則、法規及認知三項規範，說明如下：

1. 原則

數位證據鑑識工作（Digital Evidence Forensic）的指導原則如下：

(1) 應制定大方向之原則，不宜過度細膩。（ex.ISO/IEC 27041: 2015 之 5.1General Principles of Requirements）

(2) 不變更、影響數位證據內容或之原則。（ex.ISO/IEC 27037: 2012 之 5.4.4 Acquisition and Preservation and ISO/IEC 27041: 2015 之 Requirements capture and analysis）

(3) 電腦鑑識程序完整記錄原則。（ex.ISO/IEC 27037: 2012 之 5.4.2 Identification、ISO/IEC 27043: 2015 之 11.3 documentation process）

(4) 鑑識人員必須具有專業性原則。

(5) 電腦鑑識工具必須獲得國際標準鑑識專業機構認可。（ex.ISO/IEC 27041: 2015 之 5.8.3 verification of tool）

(6) 最佳證據原則。（ex.ISO/IEC 27037: 2012 之 5.4.2 Identification）

(7) 最小侵害性原則（比例原則）。（ex.ISO/IEC 27037: 2012 之 5.4.2 Identification）

(8) 運送與保存應符合安全性原則，須用安全設備保護。（ex.ISO/IEC 27037: 2012 之 5 4.5 Preservation and 27043: 2015 之 potential digital evidence transportation process）

(9) 確保原始證據的完整性、不可變動性，由專業人員操作及負責（監管鍊）。（ex.ISO/IEC 27037: 2012 之 5.4.3 Collection and ISO/IEC 27041: 2015 之 6 assurance）

2. 法規

(1) 法規規範是重要的且程序合法始有證據能力。（刑法、刑事訴訟法）

(2) 符合證據法中對於真實性、可靠性之要求。（傳聞法則、自白法則）

(3) 應規範人員資格、設備及鑑定環境之要件。

(4) 視個案情形，以刑事訴訟法、行政訴訟法及民事訴訟法為最低要求，來做為證據之規範。

3. 認知

數位證據鑑識不應限於資訊犯罪發生後，才來做數位證據鑑識，應該是把數位證據鑑識當作是資安犯罪預防的一項重要的工作，且分為：

(1) 事前鑑識：安全防護機制及應變計畫。

(2) 事中鑑識：處置及保留證據。

(3) 事後鑑識：鑑定及資料復原。

（二）準備階段

實施程序包括：授權執法人員或系統管理人員在執行數位證據、資訊安全政策、蒐集對象基本資料、確定人、事、時、地、物及理由及準備工具、資料及勤教。

（三）操作階段

人員到達現場依其任務展開蒐集、分析及鑑定的工作，本階段是展開鑑識流程及數位鑑識實驗室數位證據鑑識標準作業程序流程。

1. 蒐集：現場勘查與攝影、識別與記錄、保存與保全、收集與備份、搜索與扣押。
2. 分析：備份及記錄、檢查與搜尋、分析與保管。
3. 鑑定：資料萃取、比對、個化、重建犯罪現場。

（四）報告階段

DEFSOP 報告階段可分為：撰寫報告、呈現及簡報、驗證鑑識結果、法庭準備、案件建檔及學習。

貳、數位證據鑑識標準作業程序（DEFSOP）與國際標準 ISO/IEC 27041、ISO/IEC 27042、ISO/IEC 27043 比較分析

由於網路犯罪是隨著科技及技術不斷的進步，對於違法數位證據的蒐集必須由執行人員依法全程投入證據的調查，主動蒐集對被告不利的證據，做到認真地收集證據，縝密地分析證據，恰當地運用證據，來揭示案件真相，若調查人員辛苦蒐集、分析之資料因沒有按照標準程序而使之無法為法官所合法的運用，那麼所有的努力將付諸流水，因此，各國也紛紛定訂數位證據相關的法律以及標準，本研究就以最新國際標準 ISO27041: 2015、ISO27042: 2015 以及 ISO27043:2015 作為驗證國內學者林宜隆教授所提出的數位證據鑑識標準作業程序（DEFSOP）的基礎。

一、DEFSOP 原理概念階段與 ISO27041: 2015、ISO27042: 2015 與 ISO27043:2015 比較分析

DEFSOP 在原理概念階段分為原則（不變更數位證據原則、電腦鑑識程

序完整記錄原則、最佳證據原則、確保原始證據的完整性）、法規（法規規範是重要的且程序合法始有證據能力、符合證據法中對於真實性、可靠性、應規範人員資格、設備及鑑定環境之要件）及認知（1. 事前鑑識：安全防護機制及應變計畫、2. 事中鑑識：處置及保留證據、3. 事後鑑識：鑑定及資料復原等三階段的鑑識認知）三項規範，以事件的處理分成前、中、後的不同層面來處理。經過比較後發現（如表 1 所示）：

（一）ISO27042 標準注重在發現事件發生後之執行、調查、審查與驗證程序，缺少與 DEFSOP 原理概念中相同原則，等於沒有事前鑑識準備原則，因此排除在此一比較分析項目之外。

（二）ISO27041、ISO27043 準備程序中的各項子程序及共同進行程序完全符合 DEFSOP 原理概念階段，依據整體蒐證程序前、中、後完整的呈現於法庭上，即具有證據能力及證明力之證物都要呈現。

表 1　DEFSOP 原理概念階段與 ISO27041、ISO27042 與 ISO27043 比較分析

標準 / 原則（方法）	DEFSOP	ISO/IEC 27043	ISO/IEC 27042	ISO/IEC 27041
完整記錄原則	◎	◎	x	◎
最佳證據原則	◎	◎	x	x
最小侵害原則	◎	◎	x	◎
證據的完整性	◎	◎	x	◎
適法性	◎	◎	x	◎
事前原則	◎	◎	x	◎
事中原則	◎	◎	◎	◎
事後原則	◎	◎	◎	◎

[資料來源：本研究整理]

二、DEFSOP 準備階段與 ISO27041、ISO27042 與 ISO27043 比較分析

經過比較後發現 ISO27042 國際標準注重在案件發生後之鑑識、保管、儲存、運送與報告呈現法院等程序，在準備階段僅提及鑑識、驗證工具及報告前之準備，因此將 ISO27042 排除在此一比較分析項目之外。DEFSOP 準備階段的授權及資訊安全政策、蒐集對象基本資料、確定人、事、時、地、

物及理由、準備工具、資料及勤教等各項原則，均係依案件類型、特性及可疑潛在數位證據事先計畫整備，並透過調查小組先行測試、規劃與評估後實施，在ISO27041處理程序設計（Process design） 中說明提供實作方法的詳細資料，選擇合適的工具，清楚定義執行的流程及獲得證據的步驟以及在ISO27043開始程序中提到調查程序的準備、事件檢測程序、第一次回應程序、規劃程序與準備程序等各項實施步驟相吻合（如表2所示）。

表2　DEFSOP準備階段與ISO27041、ISO27042與ISO27043比較分析

標準 原則（方法）	DEFSOP 準備階段	ISO/IEC 27043	ISO/IEC 27042	ISO/IEC 27041
準備工具及勤前教育	◎	◎	x	◎
確定人事時地物	◎	◎	x	x
蒐集對象基本資料	◎	◎	x	◎
授權及資安政策	◎	◎	x	◎

[資料來源：本研究整理]

三、DEFSOP操作階段與ISO27041、ISO27042與ISO27043比較分析

蒐集犯罪現場所有可能的證據（包括物理、化學、數位、影音等）之前，可以依照ISO27043所規定的項目和狀態，在網路的環境、現場調查過程、雲環境和具有大量的資料環境中的潛在數位證據的進行採集。Eoghan Casey在其「Digital Evidence and Computer Crime」的書中提到，在蒐集的過程中也要確認所有實體證據之中（軟、硬體）是否可能包含了潛在的數位證據。操作的過程都做好紀錄或錄影存證並確實遵守鑑據監管鏈流程原則，且每項證據都要讓相關之人員簽名捺印，以示負責。

分析需要從潛在的數位證據的來源來識別與評估，可以作為確定每個數位證據案件反覆運作的過程，並重新審查其他數位證據。因此，調查和支援操作人員，必須有能力進行分析，在分析的過程中，工具（軟體、硬體和元件的組合）的選擇應該是基於執行分析的程序與要求。使用者應當有能力在相關過程的範圍內使用工具，涉及新工具程序應該在通過驗證和部署之前確認，在驗證過程中選擇使用的工具，應遵循在ISO/IEC 27041中指定的程式。

鑑定階段分別為資料萃取、比對及個化、重建犯罪現場，在比對及個

化，整理出數位資料該用何種工具來進行鑑識，建議調查人員應使用熟悉的工具或程序，加上有效率的訓練、常規水準測試和穩定性比例重疊的設計，以確保數位證據並減少額外錯誤發生的機會。

本階段對映林宜隆教授所提出之 DEFSOP，發現操作階段之中的蒐集、分析與鑑定三個部分，可以完全符合 ISO27041、ISO27042、ISO 27043 的各項操作程序及方式（如提供詳細實作方法、靜態與現場的分析、選擇合適的工具、提供正確的工作清單、詳細說明操作步驟、針對程序或工具、來回進行驗證等），將鑑定完成的證據接續報告階段實行（如表 3 所示）。

表 3　DEFSOP 操作階段與 ISO27041、ISO27042 與 ISO27043 比較分析

標準 原則（方法）	DEFSOP 操作階段	ISO/IEC 27043	ISO/IEC 27042	ISO/IEC 27041
現場勘查與攝影	◎	◎	◎	◎
識別與紀錄	◎	◎	◎	◎
保存與保全	◎	◎	◎	◎
收集與備份	◎	◎	◎	◎
搜索與扣押	◎	◎	◎	◎
備份及記錄	◎	◎	◎	◎
檢查與搜尋	◎	◎	◎	◎
分析與保管	◎	◎	◎	◎
資料萃取	◎	◎	◎	◎
比對	◎	◎	◎	◎
個化	◎	◎	◎	◎
犯罪現場重建	◎	◎	◎	◎

[資料來源：本研究整理]

四、DEFSOP 報 告 階 段 與 ISO27041:2015、ISO27042:2015 與 ISO27043:2015 比較分析本階段大致分四個部分，分為：

（一）撰寫呈現及簡報：必須視證據之內容與使用者之目的，正確及平衡的就查核之事實提出報告。

（二）驗證鑑識結果：為保證據之有效性、一致性與完整性，對於證據之鑑

識結果尚需進行驗證，無論是書證或數位證據，都需要進行驗證程序。

（三）法庭準備：報告撰寫、呈現、與，其內容重點必須視證據之內容與使用者之目的，依照所鑑識得到的證據針對其客觀平衡及完整正確的以查核之結果事實提出方案報告。

（四）案件建檔及學習：由於數位證據鑑識是不斷進步的科技及技 術，每件案件應依案件類型分類，建立每件案 件的卷宗及經驗、技術分享，最好建立專家知 識庫，供下次他人偵辦案件參考。

對照 ISO27041 中之驗證、確認、部署、檢視與維護；ISO27042 中提到報告文件的描述是使用範本、標準化的格式，有助於確認包含在報告中足夠的資訊，包括事件發生的時間和持續時間、事件的位置、調查小組的成員、調查的時間、持續時間和位置、在調查期間發現數位證據的事實與細節、發現到任何損壞潛在的數位證據的影響；ISO 27043 中潛在數位證據的審查、解釋、呈現法庭報告、文件與情況彙整和經驗學習等實施步驟與流程。上述三項國際標準均符合林宜隆教授所提出之 DEFSOP 報告階段（如表 4）。

表 4　DEFSOP 報告階段與 ISO27041、ISO27042 與 ISO27043 比較分析

標準 / 原則（方法）	DEFSOP 報告階段	ISO/ IEC27043	ISO/ IEC27042	ISO/ IEC27041
撰寫、呈現及簡報	◎	◎	◎	◎
驗證鑑識結果	◎	◎	◎	◎
法庭準備	◎	◎	◎	◎
案件建檔與學習	◎	◎	◎	◎

[資料來源：本研究整理]

歸納以上，ISO27041 是為確保資訊安全調查事件所使用的方法及程序的適當性，並且要求處理結果符合預期，其定義需求，說明方法，提供證據，透過第三方檢驗確保處理程序（事前、事中、事後）；ISO27042 是提供對於數位證據分析與解釋方式的指引，側重於解決問題的連續性、有效性、再現性及可重複性，適用於每個案件的證據分析過程，並作適當的資訊記錄，使提出這些程序時受到獨立的審查，以作為展現研究團隊執行的能力，並提供調查小組的熟練程度和能力適當的指導機制（事中、事後），與數位證據鑑識標準作業程序（DEFSOP）中之操作與報告階段相符合。另外，ISO27043 是提出全面、協調的程序實現標準化領域應遵循執行電腦

取證調查時的模型，以供數位證據調查程序高等級及明確的指導方針，包含準備程序、開始程序、獲取程序、調查程序及其各項子程序（事前、事中、事後），對照國內學者林宜隆教授所提出的數位證據鑑識標準作業程序（DEFSOP）是從事件發生前的預防，到事件發生後將數位證據蒐集、分析、鑑定、報告之後進入法院與案件建檔為止，其各項處理程序規範均與DEFSOP四大階段完全符合（如圖7）。

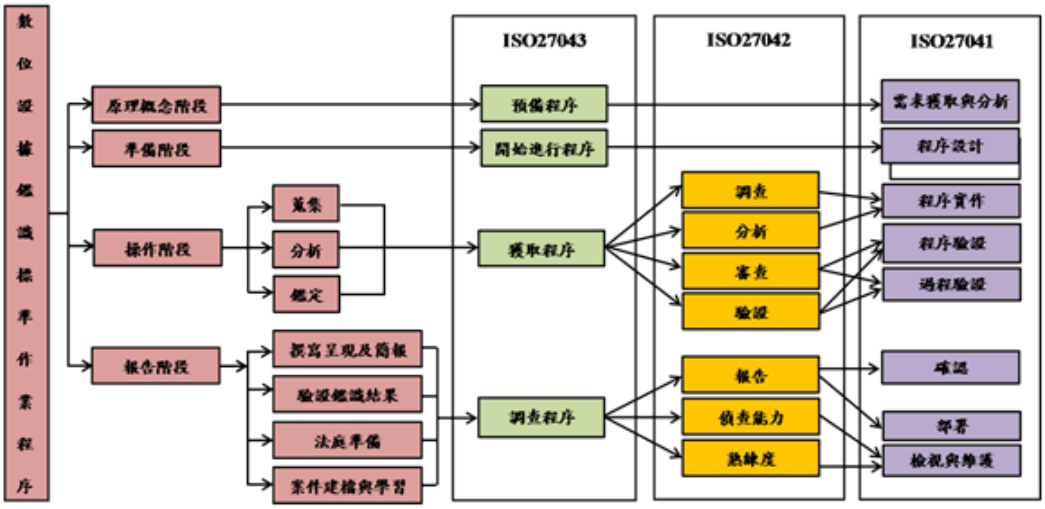


圖7　DEFSOP與ISO27043、ISO27042、ISO27041對照圖

五、建立整合性行動鑑識標準作業程序架構雛型（iDEFSOP for MF）

本研究參照數位證據鑑識標準作業程序（DEFSOP），以及整合國際標　準ISO/IEC 27037、ISO/IEC 27041、ISO/IEC 27042、ISO/IEC 27043等標準作業程序，以建立整合性行動鑑識標準作業程序架構雛型（Integrated Digital Evidence Forensics Standard Operating Procedure for Mobile Forensics, iDEFSOP for MF），並分別對原理概念階段、準備階段、操作階段及報告階段作探討，以提供未來資安鑑識人員在偵查犯罪的流程、方向和準則（如圖8）。

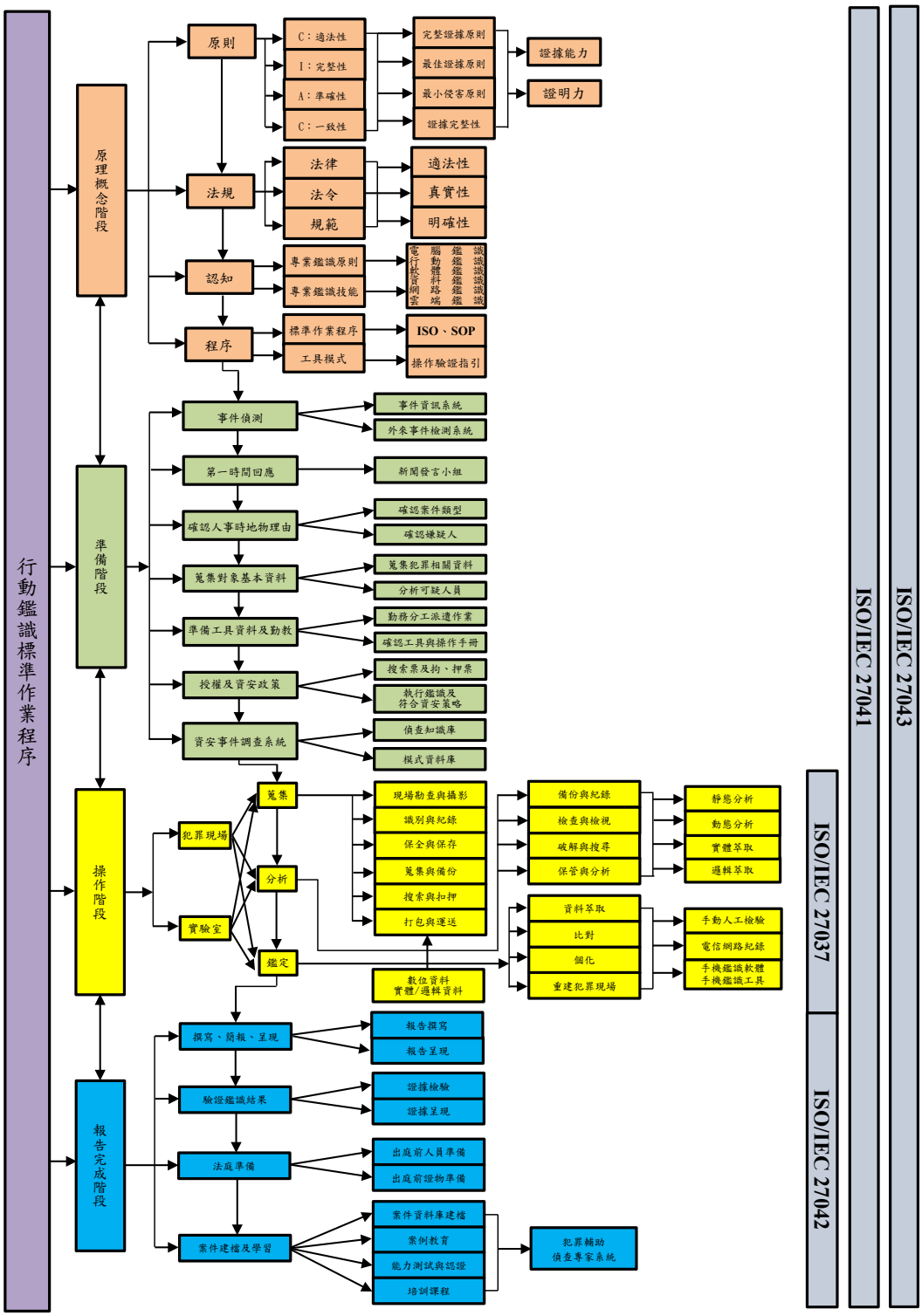


圖 8　行動鑑識標準作業程序（DEFSOP for Mobile Forensics）

參、實際案例驗證與案例分析

本文以刑事警察局破獲之實際案例，並使用國際大廠Cellebrite UFED鑑識軟體，對行動裝置iOS及Android等2大系統的數位證據進行萃取分析，取得手機內，如聯絡人、照片、上網資料、座標點…等相關的證據，來證明犯罪。

一、案例分析

偵破臺女與奈及利亞籍男子共組跨境詐騙集團（如表5）

本案例使用Cellebrite UFED 6.1.6.10工具軟體，針對Snmsung M560 Galaxy Tab J（Android 5.1系統）進行鑑識，鑑識對象為Facebook Messenger聊天軟體、SMS（簡訊）、通話紀錄、通訊錄、照片等證據，蒐集有效跡證，分析個化，找到犯罪證據。

表 5　偵破臺女與奈及利亞籍男子共組跨境詐騙集團案例分析

犯罪時間	2016 年 2 月間（破獲時間 2016/12/26）
犯罪地點	臺中市、新北市
犯罪事實	新加坡籍女子專程自新加坡搭機至臺灣報稱自己遭愛情詐騙，今（105）年 2 月間被害人透過 Tinder 交友網站，認識 1 名自稱美國籍白人男子 John，該名男子僅以模糊的大頭貼、偽造的證件照片取得被害人信任，用甜言蜜語追求被害人，除每天透過通訊軟體噓寒問暖，更承諾將自美國搬至新加坡與被害人同居，兩人未曾見面即以情侶的身分於網路交往。4 月間 John 謊稱寄送即將定居新加坡的行李包裹要求被害人代收，2 日後被害人接獲李嫌假冒物流公司人員，向被害人謊稱包裹遭臺灣海關留置，需要支付相關罰金、行政費用、清關費用等，另被害人亦接獲來自「物流公司」所發出的客服信件，使被害人信以為真，在 John 和李嫌等人輪流誆騙下，被害人陸續依指示共匯出美金 36 萬多元（折合約新臺幣 1 千 1 百多萬元）。
犯罪者剖析	警方調查後發現，該集團係由奈及利亞籍嫌犯 John 於各個交友或英語學習網站和手機 APP 以甜言蜜語騙取各國被害女性個資，再交由李姓女嫌仗恃高學歷與流利英文協助發送詐騙簡訊或撥打詐騙電話，詐騙簡訊均向被害人謊稱有來自該網友的禮物或包裹遭海關扣留，需支付相關費用以順利取得包裹，簡訊發送多達 12 國，其中臺灣、中國、香港、澳門、新加坡、印尼、馬來西亞等地數十被害人受騙，輕鬆詐得新臺幣將近 2 千萬元。
犯罪損害	美金 36 萬多元（折合約新臺幣 1 千 1 百多萬元）
起訴移送	刑法第 339 條詐欺罪移送。
犯罪流程	如圖 12。
偵辦流程	如圖 13。
查獲贓證物	現金 40 多萬元、作案用手機 4 支、存摺 20 本、提款卡 10 餘張、匯款單據百餘張、電郵紀錄。
偵辦單位	臺灣臺中地方法院檢察署、高雄市政府警察局新興分局、刑事局國際刑警科。

二、犯罪流程

本案例犯罪流程從透過交友網站平臺認識被害人、或取信任，在取得被害人個資後，透過手機發送詐騙簡訊或撥打詐騙電話，並利用物流公司發送客服信件詐騙被害人，使被害人信以為真，將金錢匯出，詐騙得手，其犯罪流程如圖 9。

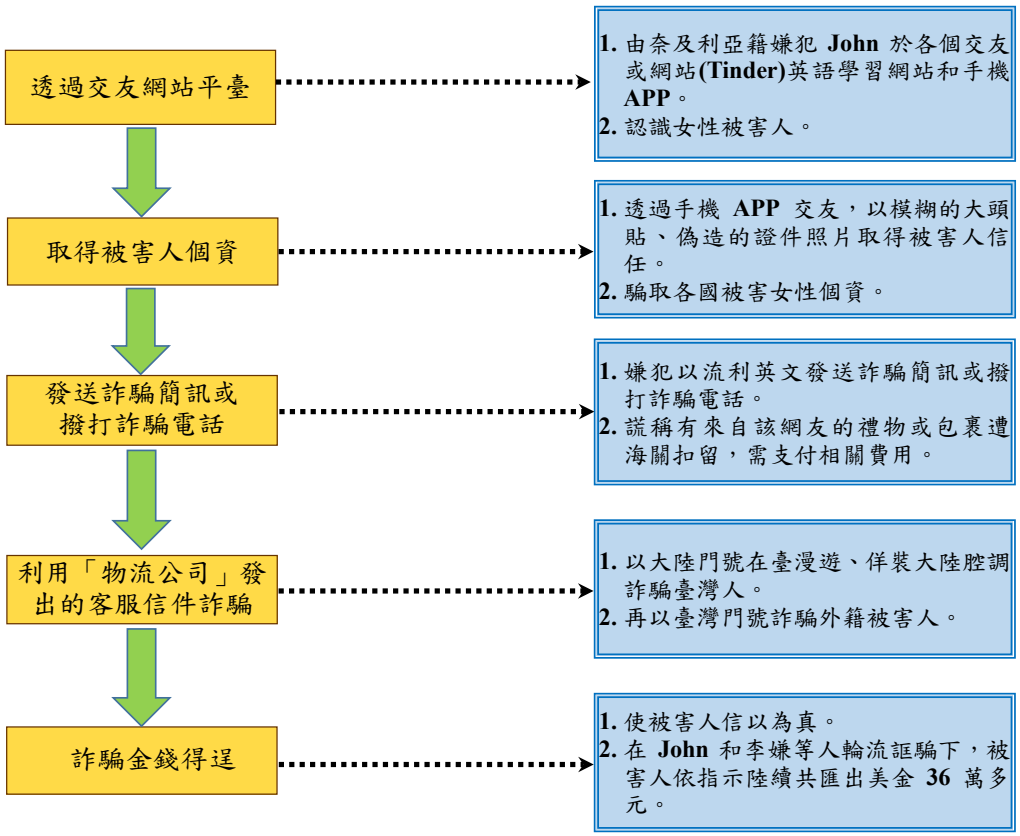


圖 9　犯罪流程圖

三、偵查流程

發現犯罪事實，利用工具（UFED）鑑識於網路或行動裝置搜尋追查犯罪證據，確認犯罪方式、犯罪來源、行為模式，逮捕嫌犯移送偵辦，其偵查流程如圖 10 所示。

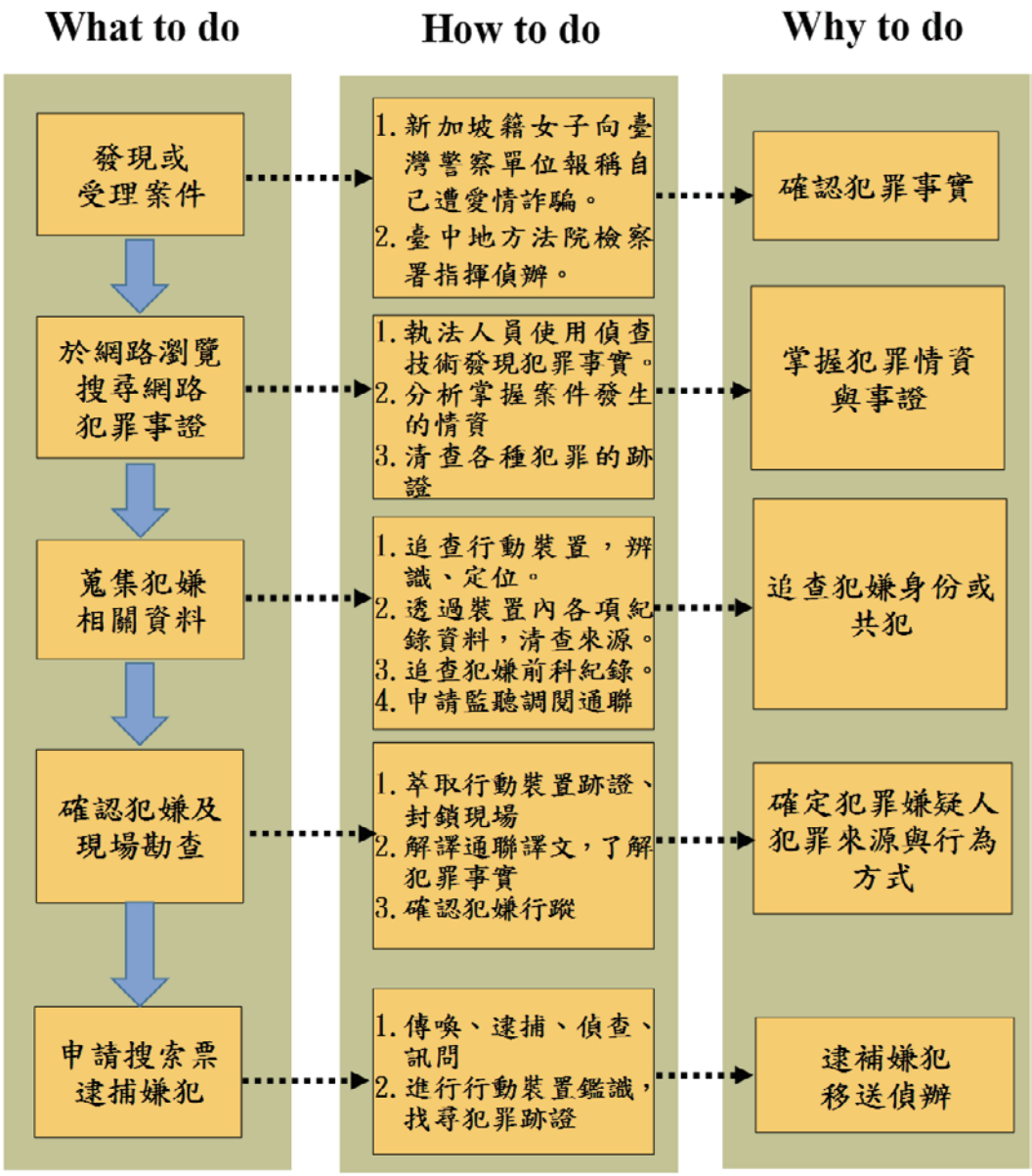


圖 10　偵查流程圖

四、依據 iDEFSOP For Mobile Forensics 操作流程，模擬實際案例，執行以下作業程序：

（一）原理概念階段：

1. 原則：

(1) 適法性（Compliance）：符合當地的法律、規範、政策，如資安鑑識相關法律。

(2) 完整性（Integrity）：在不改變或破壞證物的情況下取得原始證物，保持證據完整性，保持現場不被破壞。

(3) 準確性 （Accuracy）：證明所擷取的數位證據來自扣押的證物，並簽名確認。

(4) 一致性（Consistency）：在不改變證物的情況下，利用程式連結進行分析。

2. 法規：數位證據的取得要遵守合法、真實的原則，證據取得的途徑必須依循數位證據鑑識法律、法令、規範（例如刑法、刑事訴訟法、犯罪偵查手冊、刑事鑑識手冊、電子簽章法），以法律允許的形式規定取得數位證據的程序及許可權。

3. 認知：透過平日的訓練，建立數位偵查及鑑識概念與認知，初步研判是利用 APP 聊天網站和手機詐騙個資金錢案，立即向上級報告，展開偵查。

4. 程序：要求執行人員在操作偵查時，除須遵守專業鑑識原則、鑑識技能外，更需符合國際標準作業程序（SOP）及工具模式，以期獲得的數位證據為法院所接受。

（二）準備階段：

1. 案件偵測：當詐欺案件發生時，即開始針對案件實施偵查、檢視，找到明確實施調查之線索。

2. 第一時間回應：針對發生案件，如本詐欺案件受社會關注案件或涉及重大社會安危，需要民眾加以防範時，應立即由機關負責人召開記者說明會，向社會大眾說明案件之來龍去脈、重大進展，但設牽涉個資或其他保密部份應遵守刑事訴訟法偵查不公開原則。

3. 確定人、事、時、地、物、理由：由相關線索，確認犯罪人員（數）、地點、時間、工具、手機或相關網站資訊等資料。

4. 蒐集對象基本資料：偵查機關向 ISP 追查 IP 註冊相關資料，調閱路口、嫌犯住所監視錄影器、金融機關 ATM 錄影、資訊流程、金錢流

向，以便鎖定嫌疑及其共犯。

5. **準備工具及勤教：**依據數位證據鑑識重點工作任務表立即開專案會議，分析案情，選派適合專業人員及相關鑑識設備前往犯罪現場，填寫資料表、聲請搜索票。
6. **授權及資安政策：**依據數位證據鑑識計畫，填寫資安事件調查資料表，向法院聲請搜索票、監聽票，報請檢察官指揮相關單位聯合偵辦。
7. **資安事件系統：**調閱資安調查系統是否有類似涉案人、案件或是相牽連案件，作為案件偵查之參考。

（三）操作階段：

1. **蒐集：**依據數位證據蒐集計畫資料表紀錄與備份（計算 Hash 值），依表 3- 鑑識關鍵重點資料彙整表蒐集通話紀錄、FB 對話紀錄、網頁瀏覽紀錄、匯款紀錄、通訊錄、照片及影像等檔案數位證物並保全蒐集及備份、搜索與扣押運送至鑑識實驗室分析資料。
   (1) 識別與紀錄：
      a. 利用數位鑑識工具，蒐集與案情相關資料，包含通訊紀錄、FB 聊天紀錄、購物紀錄、轉帳資料、媒體裝置、照片。
      b. 蒐集的數位證據應填寫扣押物品一覽表，如手機、手機配件、儲存裝置（USB、硬碟）、轉帳資料（紙本）、紀錄筆記本、被害人資料。
      c. 了解並填寫目標物規格明細內容紀錄及備份保存原始證物（如手機、平板電腦、GPS、SIM 卡、記憶卡、媒體播放機、連接線等配件等）。
   (2) 現場勘查與攝影：犯罪現場、相關場所或使用車輛勘查，瀏覽行動裝置內容及拍照存證。
   (3) 保全與保存：利用鑑識工具或設備備份及保存原始數位證物，並確保不被破壞（完整證據鏈）。
   (4) 蒐集與備份：透過連結服務（Connectivity Services），以鑑識工具將行動裝置連結電腦，萃取、蒐集、保存原始數位證物。
   (5) 搜索與扣押：依法院核發之搜索票及拘押票，發現犯罪證物後扣押必要罪證。
   (6) 打包與運送：以保護袋（防止電磁影響）或設備將證據封存及運送犯罪證物。

2. 分析：本階段為行動裝置鑑識程序

以 UFED 鑑識軟體進行程式連結，以獲取相關跡證後分析，搜尋關鍵資料，如電話通聯記錄（嫌犯對話紀錄）、FB 通訊軟體聊天紀錄、簡訊紀錄、網路瀏覽紀錄、下載應用程式紀錄、匯款帳號（轉帳紀錄）、電子郵件（找出聯絡訊息）、交易地點、行動地區（利用 GPS 定位）等，紀錄並備份關鍵資料。

(1) 紀錄與備份：紀錄備份關鍵資料，如 FB 通話紀錄、E-mail、SMS、MMS、行經地點（Google 地圖）、Log 檔、登錄檔及其他紀錄。

(2) 檢查與破解：檢查破解關鍵資料，如 FB 通話紀錄、E-mail、SMS、MMS、行經地點（Google 地圖）、Log 檔、登錄檔及其他紀錄。

(3) 保管與分析：保管關鍵資料並加以分析，如 FB 通話紀錄、E-mail、SMS、MMS、行經地點（Google 地圖）、Log 檔、登錄檔及其他紀錄。

3. 鑑定：填寫數位證據鑑定資料表及交叉分析關鍵資料，選定鑑識工具，備份數位證據，透過還原證據，分析比對、個化，確定犯罪事實。在查扣相關證物後，發現手機設有密碼，且疑似有部分證據已遭刪除。調查人員將其交由鑑識人員進行分析，利用手機鑑識軟體 UFED 進行連結行動裝置擷取通訊軟體的通訊資料，選定裝置型號，利用檔案系統連結萃取方式，萃取手機內 summary 檔案資料，加以分析，首先了解被害人係透過交友 APP 與嫌犯認識，在嫌犯與被害人通訊軟體（Facebook Messenger）及電話聊天紀錄，知道被害人透露電話給嫌犯後，嫌犯利用假冒快遞公司名義發送詐騙簡訊給被害人，騙取信任，在匯出金錢後，便由車手將錢提領走，因此，必須確認在嫌犯行動裝置中找到可疑的聯繫資訊，確認詐騙訊息與匯款紀錄等證據。

(1) 資料萃取：

a. 使用工具、系統

(a) 手機裝置：Sumsung M560 Galaxy Tab J

(b) 作業系統：Android 5.1

(c) 鑑識對象：FB Messenger 聊天紀錄、SMS（刪除簡訊）、通話紀錄、通訊錄

(d) 鑑識工具：選擇 Cellebrite UFED（版本 : UFED 4PC 6.1.0.140）

b. 操作步驟如下：

(a) 在操作介面上選擇手機廠牌（圖 11）及型號（圖 12）

(b) 萃取方式選擇 File System Extraction （圖 13）

(c) 選擇模式 Backup and AFC（all），備份所有數位證據（圖 14）

(d) 成功完成萃取（圖 15）、所有檔案資料（圖 16）

圖 11　選擇手機廠牌

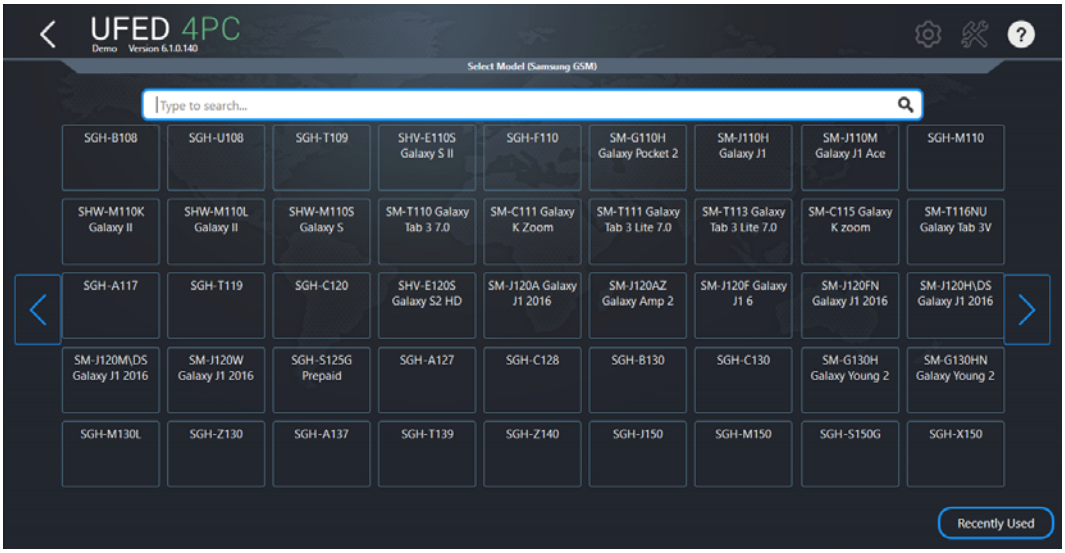


圖 12　選擇手機型號

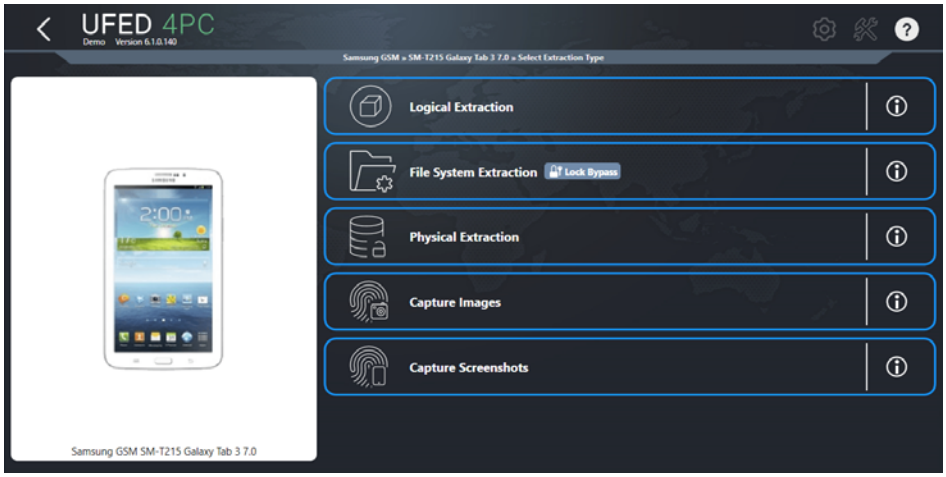


圖 13　選擇進行萃取資料方式 File System Extraction

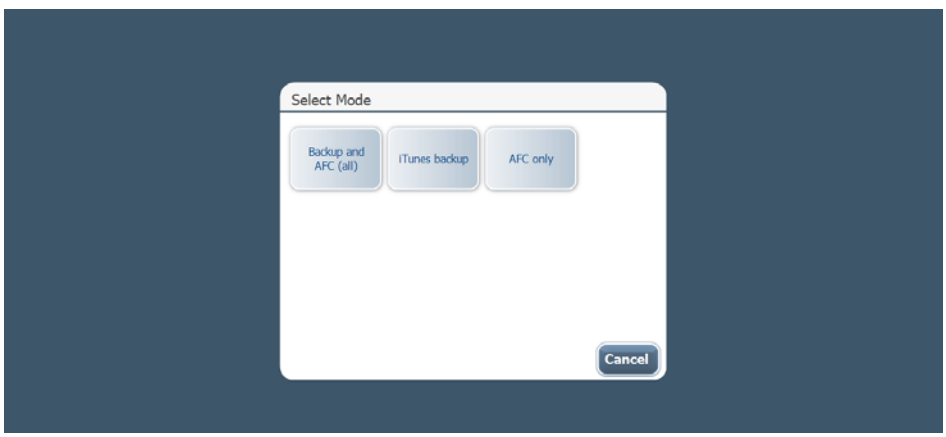


圖 14　選擇模式 Backup and AFC（all）

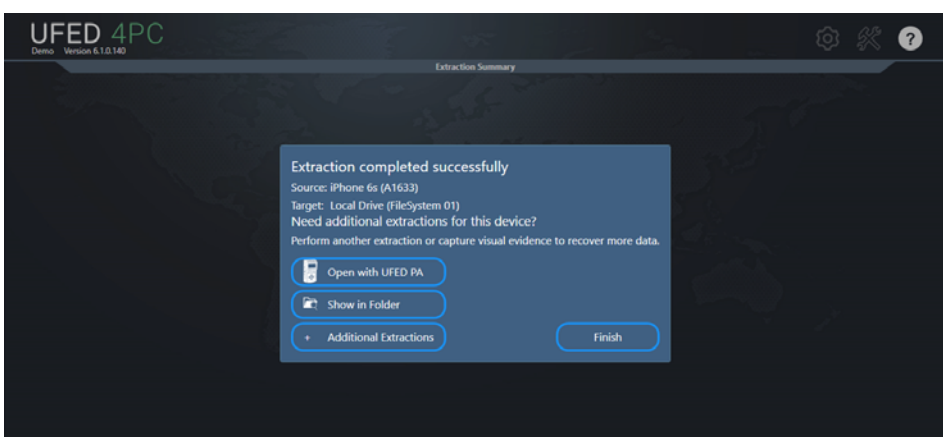


圖 15　完成萃取模式

圖 16　UFED 完成分析資料

(2) 比對：針對以下數位證據做比對

a. 嫌犯利用熱門交友 APP 騙取女子感情，並透過 FB 社群網站與配害人聊天藉機取得電話及個資（如圖 17）。

b. 藉由通聯紀錄，發現犯嫌與受害者有短暫且密集聯絡的紀錄（如圖 18）（找出犯罪證明）。

c. 從已刪除簡訊資料，找到嫌犯想消滅證據的資料 （可疑犯罪紀錄）（如圖 19）。

d. 雙方對談紀錄，研判可能藉此騙取受害者個資並相約見面（確認犯罪紀錄） （如圖 20）。

e. 從被害人匯款紀錄，找到證明嫌犯要求被害人匯款證據（詐欺證明）（如圖 21）。

f. 從其他通訊錄與通話紀錄找出能一同作案的共犯或是主持人、車手等（如圖 22）。

(3) 個化：利用通訊軟體（FB Messenger）或刪除簡訊（SMS）、上網檔案資料及聊天通話等紀錄，檔案分析、邏輯分析、關聯分析、時序分析個化特徵以研判單一目標或其他共犯。

(4) 重建犯罪現場：利用數位鑑識工具所蒐集之資料，還原犯罪現場，找到可能遺留之蛛絲馬跡，亦是模擬現場犯罪情境，對所有相關訊息進行系統且合乎邏輯的思維後，使人認知案件形成過程和犯罪行為，所得出的對犯罪行為過程的合理解釋，此程序準確

完整地收集行動裝置內被害人及其他知情人的各種形式的數位跡證，做好發現、記錄、固定、提取、保存工作和識別評估工作。

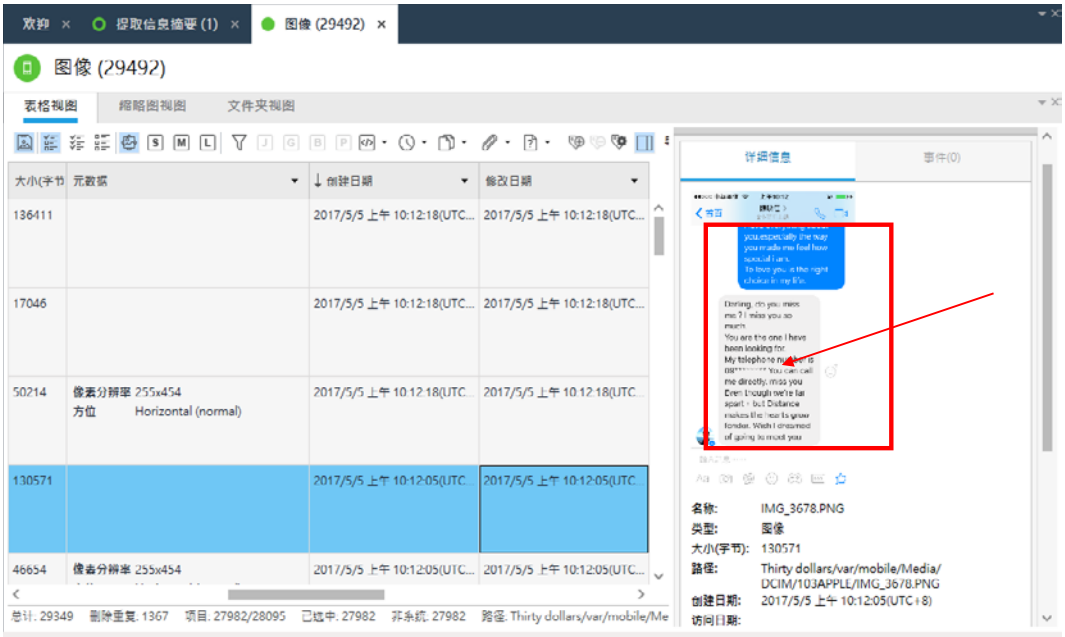


圖 17　與被害人 FB 聊天紀錄

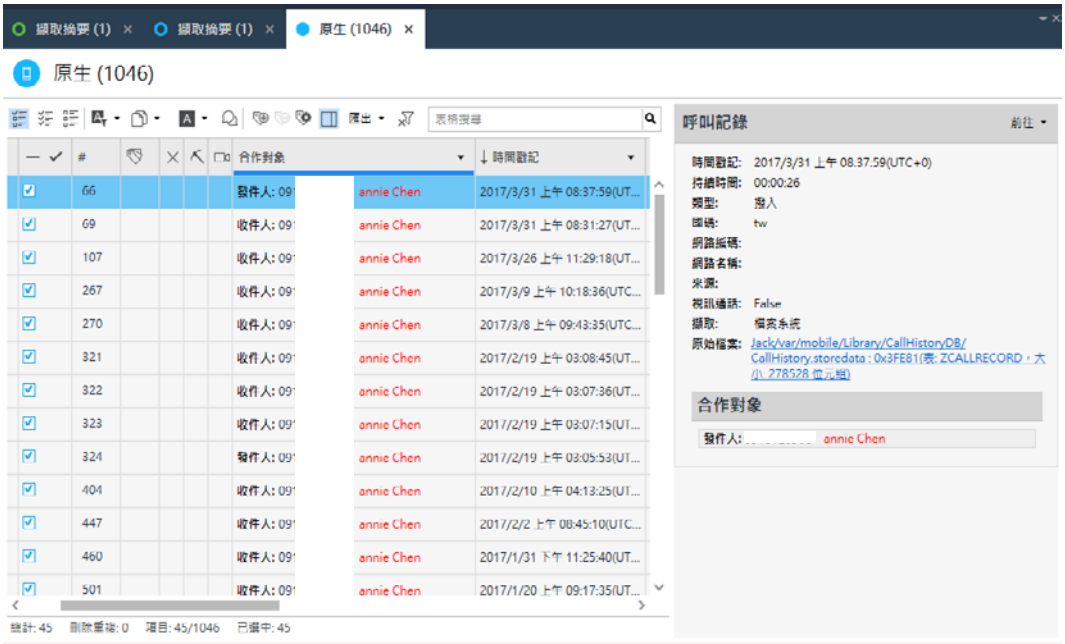


圖 18　與被害人通話紀錄

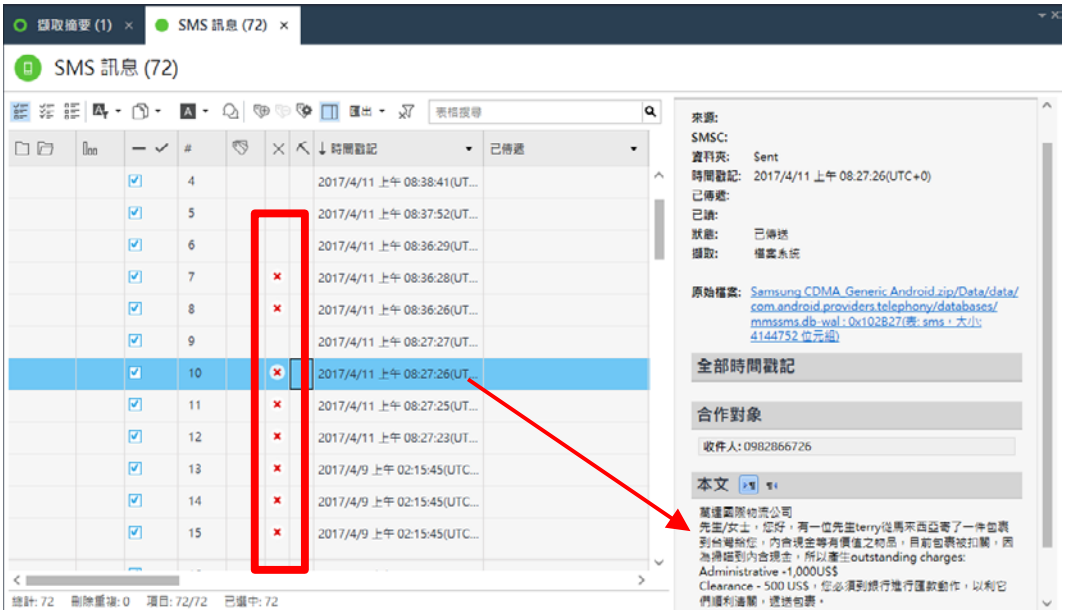


圖 19　遭刪除詐騙簡訊

圖 20　詐騙簡訊內容

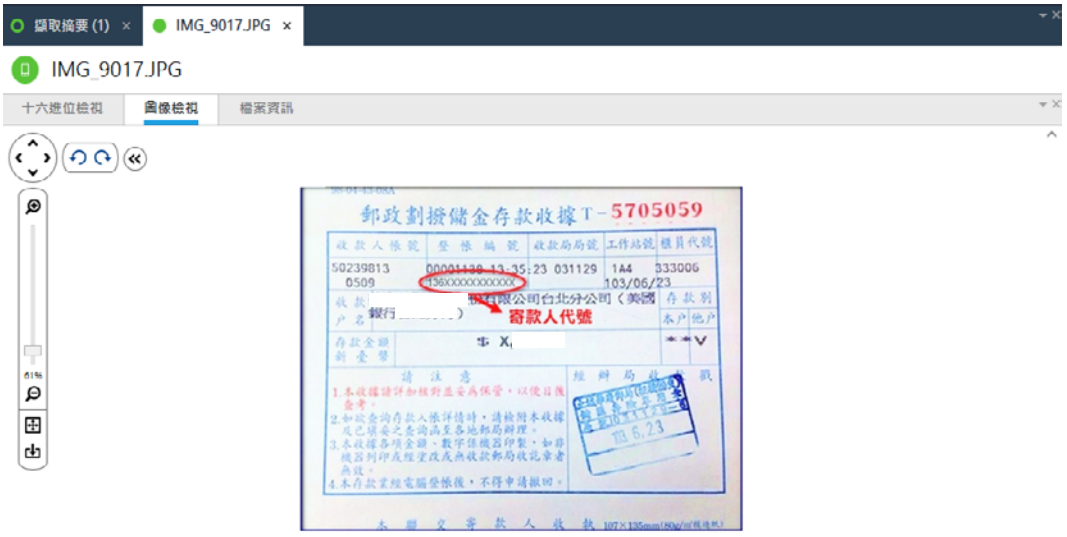


圖 21　要求傳送匯款證明

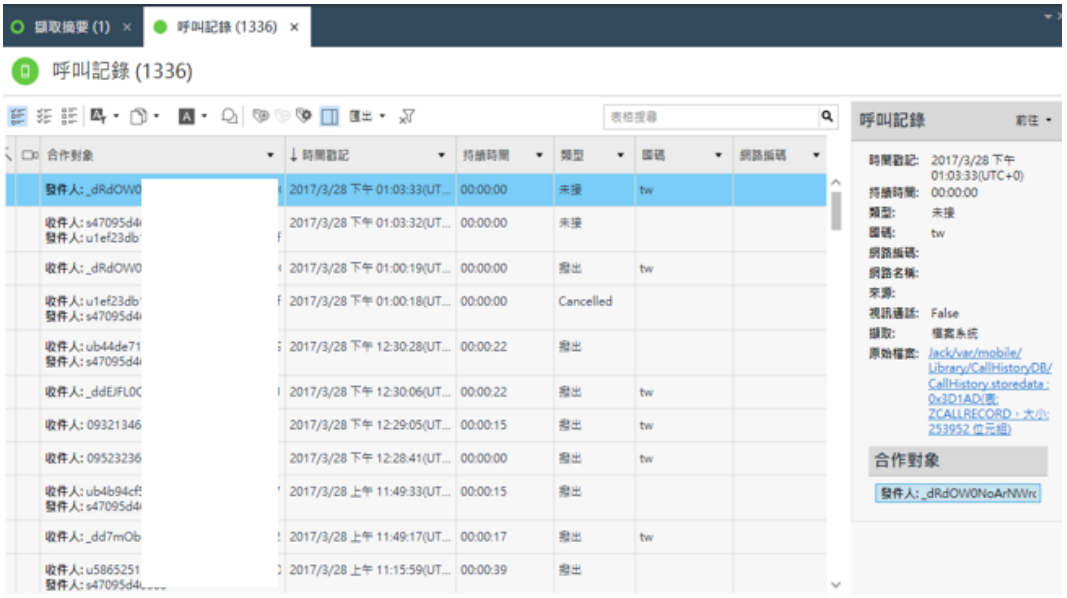


圖 22　共犯（車手）通話紀錄

（四）報告階段：

1. 撰寫呈現簡報：

(1) 呈現鑑識結果如圖 23。

(2) 易讀圖表之簡報，以 excel、html、xml、ufdr、Word 或 PDF 呈現（建議採 PDF 並鎖碼較不易被修改且清晰明瞭）如圖 24。

(3) 鑑識基礎說明，如案例資訊、案例名稱、部門、鑑識人員資格、鑑識工具及環境如圖 25。

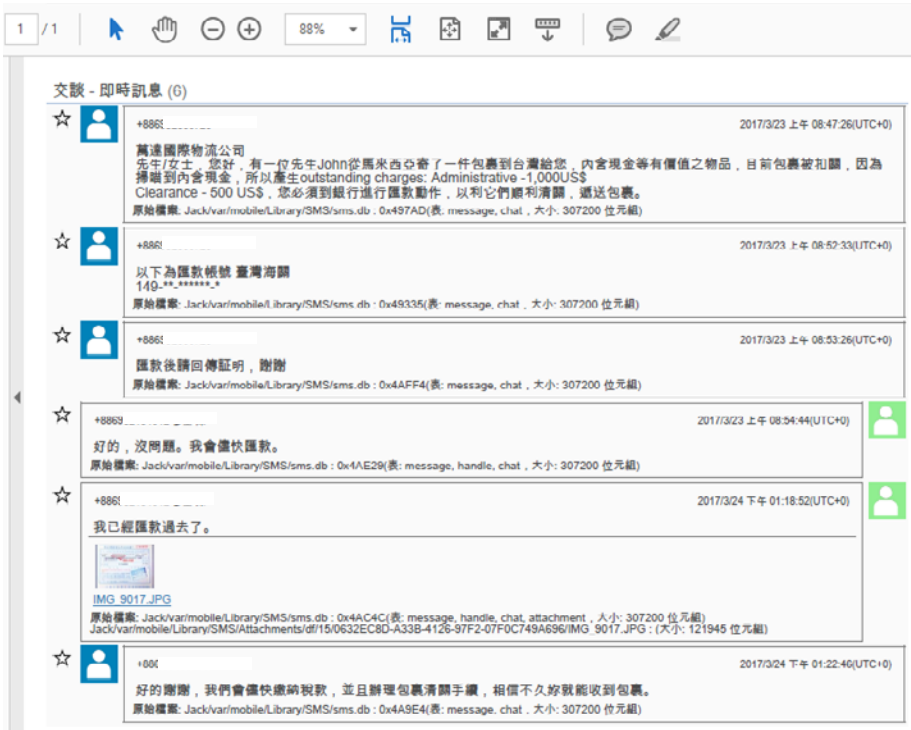


圖 23　全部交談訊息資料

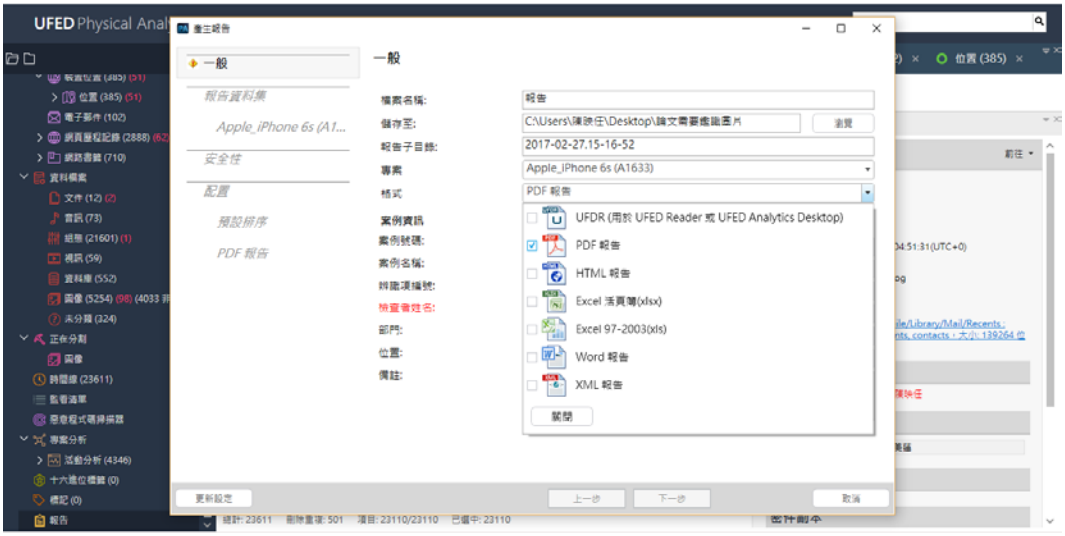


圖 24　匯出報告（建議 PDF 格式）

擷取報告
Apple iPhone

摘要

UFED Physical Analyzer 版本	6.0.0.128
報告建立時間	2017/4/3 下午 03:14:46 +08:00
時區設定(UTC)	原始 UTC 值
案例編號	01
案例名稱	[illegible]
證物編號	01
檢查者姓名	POLICE
部門	POLICE
位置	Police department

來源擷取

檔案系統	
擷取開始日期/時間	2017/3/29 上午 09:04:13(UTC+8)
擷取結束日期/時間	2017/3/29 上午 09:07:19(UTC+8)
UFED 版本	6.1.0.140
內部版本	4.5.2.140
選取的製造商	Apple
選取的裝置名稱	iPhone 6s (A1633)
連線類型	Cable No. 210
擷取類型	檔案系統
擷取 ID	3205FE96-922A-40CF-9CC5-E58E7BOD6783

裝置資訊

名稱	數值
檔案系統	
Jack	
檢測到的電話廠商	iPhone 6s
序號	DNPRV88UHFLT
MSISDN	+886 902-866-726
唯一 ID	24b5828b1dc31c32cf5ea5b2cf56ba57c1407abd
ICCID	89886971608760179193
作業系統版本	10.2.1
檢測到的電話型號	iPhone8,1
IMEI	353799083028894
擁有者名稱	Jack
已加密	True
備份密碼	881102
iCloud 帳戶存在	True
藍牙裝置位址	88:66:a5:2c:56:bf
序號	DNPRV88UHFLT
IMSI	466977600357932
IMEI	353799083028894
ICCID	89886971608760179193
唯一 ID	24b5828b1dc31c32cf5ea5b2cf56ba57c1407abd
WiFi 位址	88:66:a5:2c:56:be
檢測到的型號	iPhone (N71mAP)
電話日期/時間	2017/3/29 上午 01:04:45(UTC+0)
檢測到的電話型號	iPhone8,1
檢測到的電話型號	iPhone 6s
作業系統版本	10.2.1
Apple ID	jack_0508@yahoo.com.tw
上個使用者 ICCID	89886971608760179193
MSISDN	886902866726
[illegible]	
上次使用時間	2017/3/28 下午 12:21:14(UTC+0)
Sync Data	
同步主機名	Computer: DESKTOP-Q4F6AGM\User: [illegible]
同步主機名	Computer: JACK-PC\User: jack
Phone Settings	
位置服務已啟用	True
已啟用「尋找我的 iPhone」	True

圖 25　完整鑑識報告

2. 驗證鑑識結果：

(1) 撰寫鑑識作業流程符合標準。

(2) 註明使用工具及方法符合程序。

(3) 透過第三機關或第三人複驗，證明結果符合法規。

3. 法庭準備：

(1) 證物呈現分類。

(2) 交互詰問資料準備。

(3) 數位證據符合規範、ISO 標準作業程序。

(4) 符合當地法庭、法律需求及規定。

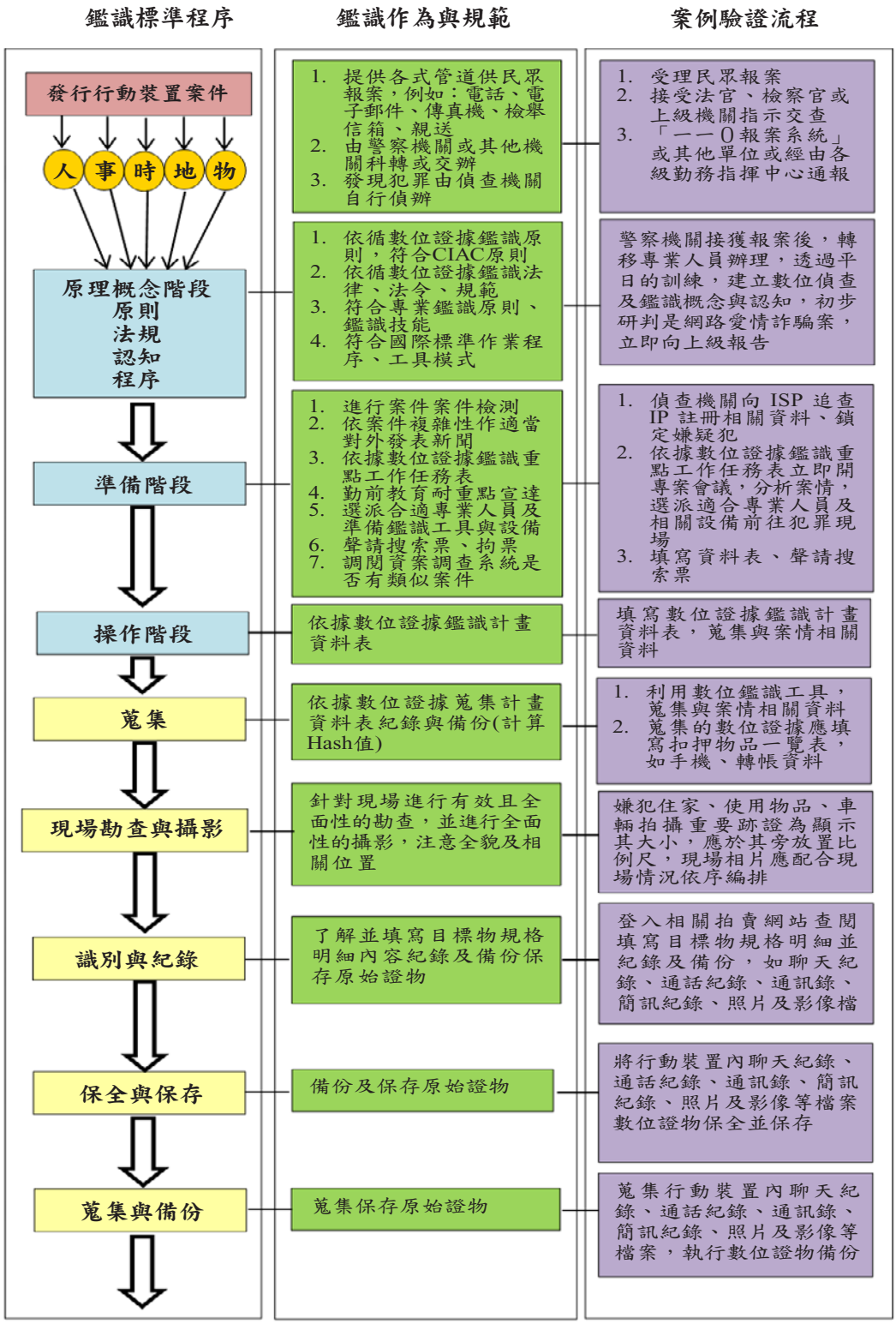
4. 案件建檔及學習：

(1) 案件依資訊犯罪類型分類，建檔於刑事案件資料庫，將鑑識技術及經驗與其他偵查人員分享。

(2) 透過刑事知識庫建檔學習，建立犯罪輔助偵查專家系統，利於事後人員訓練、考試測驗、證照。

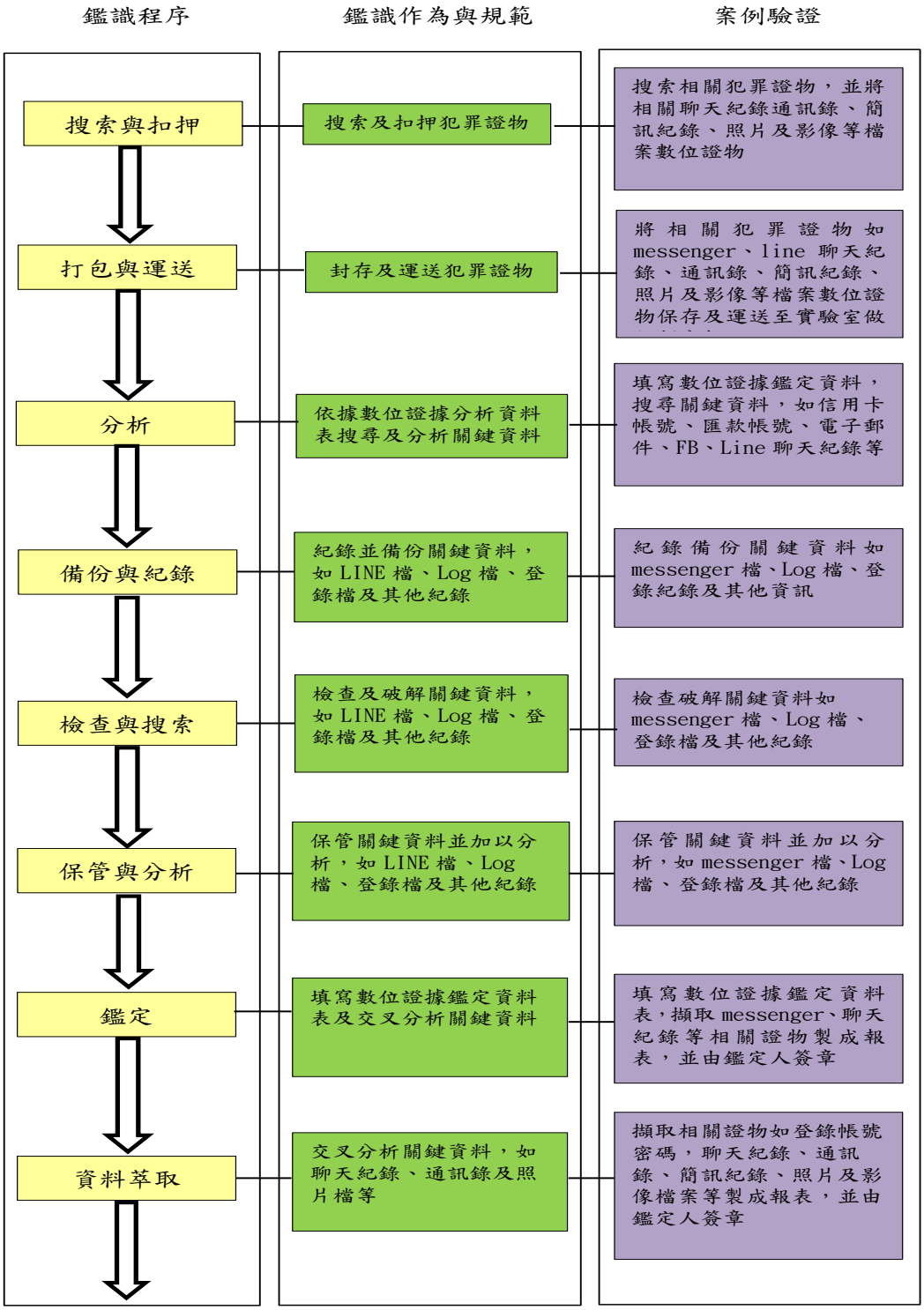
五、案例驗證：

在 Google 及 iOS 系統的 App 商店中，手機中社交 App（Social Networking App），尤其是交友網站，是時下年輕族群下載的熱門軟體之一。但是行動網路蓬勃的發展，年輕人使用社交 App 來進行資訊分享與交流之際，卻被有心人士利用軟體的便利性、即時性、可隱藏性及人性弱點，透過社交軟體聊天中來進行非法活動，達到犯罪的目的，因此，鑑識裝置中的通訊紀錄就成為檢調偵查的重要跡證，由上述案例二，分析其鑑識程序與所需規範暨相關知識，用以驗證所建構之整合性行動鑑識標準作業程序架構雛型（iDEFSOP for MF）具有可行性及可操性，符合我國現行偵查流程，案例驗證如圖 26 所示。


鑑識標準程序
鑑識作為與規範
案例驗證流程
發行行動裝置案件
人
事
時
地
物
原理概念階段
原則
法規
認知
程序
準備階段
操作階段
蒐集
現場勘查與攝影
識別與紀錄
保全與保存
蒐集與備份
1. 提供各式管道供民眾報案，例如：電話、電子郵件、傳真機、檢舉信箱、親送
2. 由警察機關或其他機關科轉或交辦
3. 發現犯罪由偵查機關自行偵辦
1. 受理民眾報案
2. 接受法官、檢察官或上級機關指示交查
3. 「一一0報案系統」或其他單位或經由各級勤務指揮中心通報
1. 依循數位證據鑑識原則，符合CIAC原則
2. 依循數位證據鑑識法律、法令、規範
3. 符合專業鑑識原則、鑑識技能
4. 符合國際標準作業程序、工具模式
警察機關接獲報案後，轉移專業人員辦理，透過平日的訓練，建立數位偵查及鑑識概念與認知，初步研判是網路愛情詐騙案，立即向上級報告
1. 進行案件案件檢測
2. 依案件複雜性作適當對外發表新聞
3. 依據數位證據鑑識重點工作任務表
4. 勤前教育耐重點宣達
5. 選派合適專業人員及準備鑑識工具與設備
6. 聲請搜索票、拘票
7. 調閱資案調查系統是否有類似案件
1. 偵查機關向ISP追查IP註冊相關資料、鎖定嫌疑犯
2. 依據數位證據鑑識重點工作任務表立即開專案會議，分析案情，選派適合專業人員及相關設備前往犯罪現場
3. 填寫資料表、聲請搜索票
依據數位證據鑑識計畫資料表
填寫數位證據鑑識計畫資料表，蒐集與案情相關資料
依據數位證據蒐集計畫資料表紀錄與備份(計算Hash值)
1. 利用數位鑑識工具，蒐集與案情相關資料
2. 蒐集的數位證據應填寫扣押物品一覽表，如手機、轉帳資料
針對現場進行有效且全面性的勘查，並進行全面性的攝影，注意全貌及相關位置
嫌犯住家、使用物品、車輛拍攝重要跡證為顯示其大小，應於其旁放置比例尺，現場相片應配合現場情況依序編排
了解並填寫目標物規格明細內容紀錄及備份保存原始證物
登入相關拍賣網站查閱填寫目標物規格明細並紀錄及備份，如聊天紀錄、通話紀錄、通訊錄、簡訊紀錄、照片及影像檔
備份及保存原始證物
將行動裝置內聊天紀錄、通話紀錄、通訊錄、簡訊紀錄、照片及影像等檔案數位證物保全並保存
蒐集保存原始證物
蒐集行動裝置內聊天紀錄、通話紀錄、通訊錄、簡訊紀錄、照片及影像等檔案，執行數位證物備份

（接下頁）

（承上頁）


鑑識程序
鑑識作為與規範
案例驗證
搜索與扣押
搜索及扣押犯罪證物
搜索相關犯罪證物，並將相關聊天紀錄通訊錄、簡訊紀錄、照片及影像等檔案數位證物
打包與運送
封存及運送犯罪證物
將相關犯罪證物如messenger、line聊天紀錄、通訊錄、簡訊紀錄、照片及影像等檔案數位證物保存及運送至實驗室做
分析
依據數位證據分析資料表搜尋及分析關鍵資料
填寫數位證據鑑定資料，搜尋關鍵資料，如信用卡帳號、匯款帳號、電子郵件、FB、Line聊天紀錄等
備份與紀錄
紀錄並備份關鍵資料，如LINE檔、Log檔、登錄檔及其他紀錄
紀錄備份關鍵資料如messenger檔、Log檔、登錄紀錄及其他資訊
檢查與搜索
檢查及破解關鍵資料，如LINE檔、Log檔、登錄檔及其他紀錄
檢查破解關鍵資料如messenger檔、Log檔、登錄檔及其他紀錄
保管與分析
保管關鍵資料並加以分析，如LINE檔、Log檔、登錄檔及其他紀錄
保管關鍵資料並加以分析，如messenger檔、Log檔、登錄檔及其他紀錄
鑑定
填寫數位證據鑑定資料表及交叉分析關鍵資料
填寫數位證據鑑定資料表，擷取messenger、聊天紀錄等相關證物製成報表，並由鑑定人簽章
資料萃取
交叉分析關鍵資料，如聊天紀錄、通訊錄及照片檔等
擷取相關證物如登錄帳號密碼，聊天紀錄、通訊錄、簡訊紀錄、照片及影像檔案等製成報表，並由鑑定人簽章

（接下頁）

（承上頁）

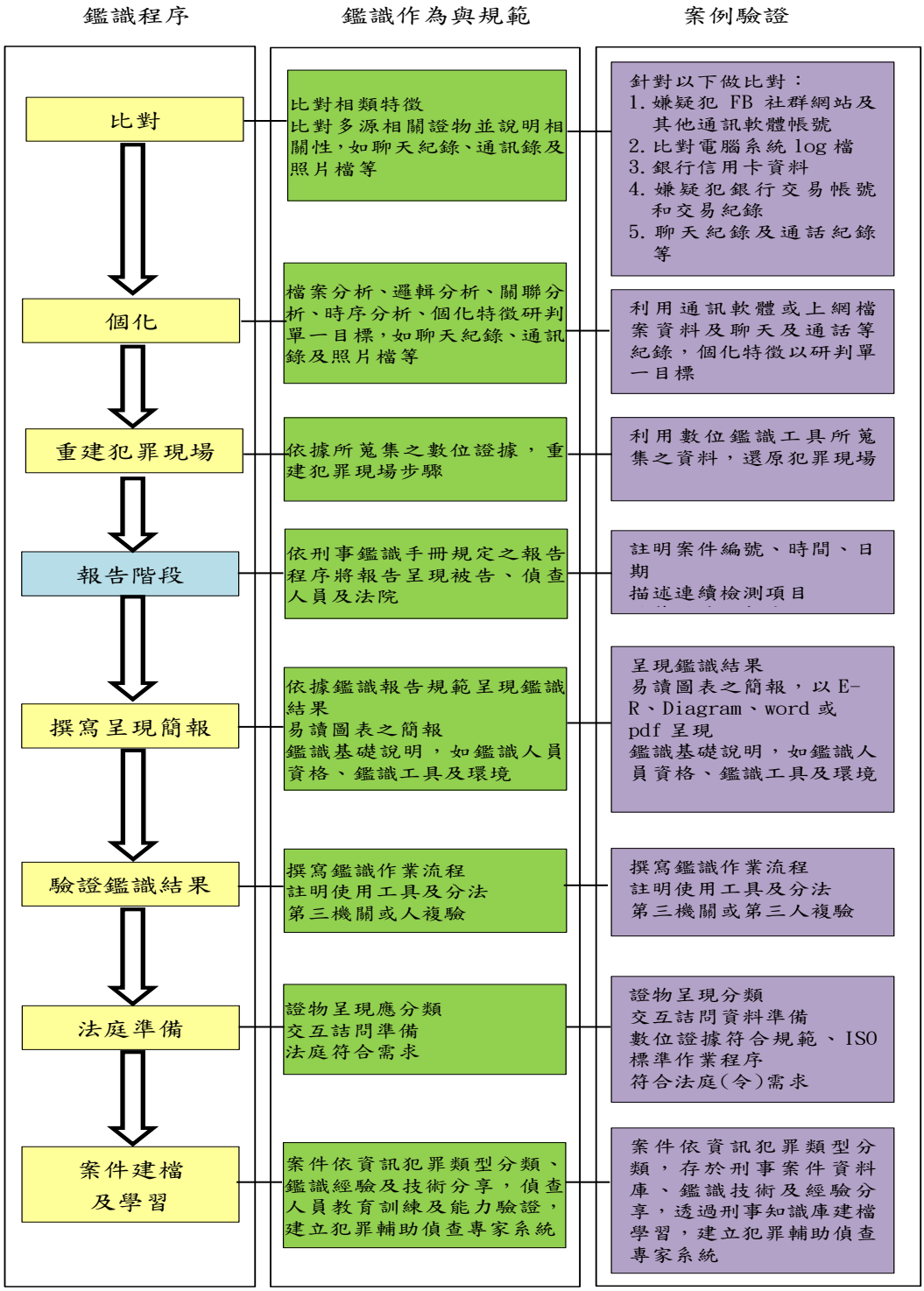


圖 26　整合性行動鑑識標準作業程序架構（iDEFSOP for MF）驗證圖

肆、結論

犯罪案件調查，著重在整個調查的程序及步驟，資安犯罪亦是如此，在現今數位鑑識領域上，各專家學者針對數位鑑識執行程序提出不同之見解，認為數位鑑識之執行與過程應遵守哪些注意事項。基此，數位證據鑑識標準作業程序（DEFSOP）是否符合規範，其鑑識過程對於證據能力有極大的影響，本研究所提出 iDEFSOP For Mobile Forensics（iDEFSOP-MF）整合性行動鑑識標準作業程序，透過鑑識行動裝置工具與數位證據分析程序來加強鑑識結果及公信力，以強化司法鑑識單位之能力及法庭上公信力，再者，瞭解數位證據的特性及其在證據法上的地位，讓其作業規範及流程能更契合證據法的需要，不僅強化數位（資安）證據蒐集和舉證，並確保資安落實，提升數位（資安）證據在法庭上之證據能力、證明力及公信力之目標外，更可在未來針對資安事件（如 ISIM:ISO27035:2016）做有效之預防機制及應變處置。

參考文獻

中文文獻

方彥霏，2016，建構行動裝置數位證據鑑識標準作業程序之研究 - 從智慧型手機萃取數位證據分析，國立宜蘭大學多媒體網路通訊數位學習碩士在職專班碩士論文。

林宜隆、藍添興，2003，『數位證據蒐證程序之初探』，資訊管理學術暨警政資訊 實務研討會 , 中央警察大學主辦。

林宜隆，2006，建構網路犯罪行為模式之探討，檔案與微縮，第 82 期，頁 9-22。

林宜隆，2007，數位證據標準作業程序（DESOP）之建構，電腦稽核，第十六期。

林宜隆、歐啟銘，2008，手持式行動通訊裝置數位鑑識工具比之較與案例分析，第十屆「網際空間：資安、犯罪與法律社會」學術研究暨實務研討會，輔仁大學主辦。

林宜隆，2009，網路犯罪理論與實務第三版，中央警察大學出版，桃園。

林宜隆、顏雲生、吳柏霖、蕭勝方，2010，「VoIP 攻擊分析與數位證據鑑識機制之研究」，第二十一屆國際資訊管理學術研討會（ICIM 2010），台南市：成功大學。

林宜隆、李政謙、陳靜玉、張志宗，「數位證據鑑識標準作業程序與 ISO27037 數位證據處理程序之比較分析」，2013 第十九屆資訊管理暨實務研討會。

林宜隆，「建構數位證據鑑識標準作業程序」，司法新聲 101 期 _ 第 4 篇，2012，1 月。

林宜隆、張文耀、劉耿旭，「建構個人資料保護之數位證據鑑識標準作業程序」，電腦稽核 27 期，2013 年 1 月。

劉秋伶，2010，數位證據之刑事證據調查程序，國立政治大學法律學研究所碩士論文。

陳聖文、楊中皇、陳世仁，2012，Android Live SD 資料還原系統設計與實作，資訊、科技與社會學報，頁 51-65。

陳威棋，“談數位鑑識－從國內外實際案例看數位鑑識之重要性”，財金資訊季刊，勤業眾信聯合會計師事務，2014 年 7 月。

陳詰昌，2016，數位鑑識「原件不可變動原則」之適用—由行動裝置鑑識與電腦鑑識差異探討，第 119 期司法新聲季刊。

黃志龍，2006，建構數位證據鑑識標準作業程序規範之研究，中央警察大學碩士論文。

黃敬博，2011，因應個資法之數位鑑識案例，第十屆台北國際資訊安全科技展暨亞太資訊安全論壇。

楊鴻正，2003，我國資通安全鑑識科技能量規劃之研究，中央警察大學資訊管理所論文。

蔡旻峰、陳志誠，2004，數位鑑識實驗室建構標準之芻議，第六屆「網際空間：資訊、法律與社會」學術研究暨實務研討會。

外文文獻

ISO/IEC 27041:2015, “Information technology — Security techniques — Guidance on assuring suitability and adequacy of incident investigative method”, international standard, 2015.

ISO/IEC 27042:2015,“Information technology — Security techniques — Guidelines for the analysis and interpretation of digital evidence”, international standard, 2015.

ISO/IEC 27043:2015, “Information Technology — Security Techniques — Investigation principles and processes”, international standard, 2015.

Timothy Wright, The Field guide for investigation Computer Crime: search and seizure basic part three, security focus, 2000.

United States of Justice, Federal Guidelines for Searching and Seizing Computers, 1994.

Weber, R. P. (1990). Basic Content Analysis, 2nd (ed.). California: SAGE Publications, Inc., 1-87.

Waldron, 2004,Public policy Analysis:An Introduction, Englewood Gliffs, N.J.:Prentice-Hall Inc, pp.32-55.

Waldron, 2004,Public policy Analysis:An Introduction, Englewood Gliffs, N.J.:Prentice-Hall Inc, pp.32-55.

Warren G. Kruse II and Jay G. Heiser, Computer forensics-Incident Response Essentials, 2002, Addison-Wesley corporation.

(Waldron, 2004) M. Waldron, Adopting Electronic Management: European Strategic Initiatives, Information Management Journal, Jul/Aug. 2004, ABI/INFORM 14 Global, p.30-34.