Communications of the CCISA
Vol. 25 No. 1 Feb. 2019

建構行動鑑識標準作業程序(DEFSOP-MF)與整合國際鑑識標準之研究
－整合 ISO27037、ISO27041、ISO27042 及 ISO27043 比較分析為例

林宜隆 [1,2*]、陳映任 [1]
[1] 元培醫事科技大學 資訊管理系暨數位創新管理碩士班
[2] 台灣數位鑑識發展協會(ACFD)
[1]cyberpaul747@gmail.com

摘要

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 107 年 05 月 11 日立法院三讀通過，並於今(108)年 1 月 1 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，且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，建立一套完整行動鑑識標準作業程序（DEFSOP for Mobile Forensics，DEFSOP-MF），透過刑事警察局局破獲之實際案例加以驗證，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(如 ISIM:ISO27035:2016 及資通安全管理法之六大相關子法)做有效之預防機制及應變處置。

關鍵詞：ISO 27037/27041/27042/27043、數位(資安)鑑識、行動鑑識、行動鑑識標準作業程序

* 通訊作者 (Corresponding author.)

Regular Paper

Communications of the CCISA
Vol. 25 No. 1 Feb. 2019

Research on the Construction of the Mobile Forensics Standard Operating Procedure (DEFSOP-MF) and the Integration of International Forensic Standards
--- Integration of ISO27037, ISO27041, ISO27042 and ISO27043 Comparative Analysis as an Example

I-Long Lin[1,2†*] Yingren Chen[1]
[1]Department of Information Management and Master's Program in Digital Technology Innovation Management, Yuanpei University of Medical Technology
[2]Taiwan Association of Cyber Forensic Development (ACFD)
[1]cyberpaul747@gmail.com

Abstract

In view of our country's current legal system, the digital forensics (cyber) is not clear the special chapter legislation, the investigative agency are not in compliance with the norms, standards and procedures for the identification of digital (cyber), by collecting the literatures of the domestic and foreign digital (cyber) evidence, the digital (cyber) mechanism, the International standard operating procedure, and the ISO/IEC 27037:2012, ISO/IEC 27041:2015, ISO/IEC 27042:2015 and 27043:2015, the management of international standard procedures and guidelines, integrated digital forensics procedures to study the corresponding, based on the four stages (principle concept stage, preparation stage, operation stage, reporting stage) of the Digital Evidence Forensics Standard Operating Procedure (DEFSOP) presented by the domestic scholar Professor I-Long Lin, a complete set of Mobile Forensics standard operating procedures (DEFSOP for Mobile Forensics, DEFSOP- MF) is developed, Expect to the investigators and cyber personnel can understand the focus and direction of forensics (why to do) from the investigation process (what to do) and the investigation action (how to do) of the whole case, not only to strengthen the digital (cyber) evidence and proof, and to ensure the implementation of the security, enhance the digital (cyber) evidence in the court of evidence, proof and credibility of the target, but also in the future for the incidents to do an effective preventive mechanism and contingency disposal.

Keywords: Digital evidence, Digital (Cyber) forensics, Mobile forensics, International Standard Operating Procedures

†* 通訊作者 (Corresponding author.)

壹、前言

近年來，行動互聯網(Mobile Internet)及行動裝置(Mobile Devices)的出現讓人們智慧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 1 月止全球人口約 76 億人，而全球網際網路用戶已突破 42 億人大關，且行動網路用戶(Mobile Users)也已突破 38 億人大關，其所占全球人口之比例已超 50%），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，符合國際鑑識相關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據力明顯不足(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。

本文探討以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)與整合國際鑑識相關標準 ISO27037:2012 、ISO27041:2015 、ISO27042:2015 及 ISO27043:2015 與比較分析**，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)，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(ISIM)做有效之預防機制及應變處置。

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 107 年 05 月 11 日立法院三讀通過，並於今(108)年 1 月 1 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，建立一套完整行動鑑識標準作業程序（DEFSOP for Mobile Forensics，DEFSOP-MF），透過刑事警察局局破獲之實際案例加以驗證，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(如 ISIM:ISO27035:2016 及資通安全管理法之六大相關子法)做有效之預防機制及應變處置。

貳、數位證據與行動鑑識

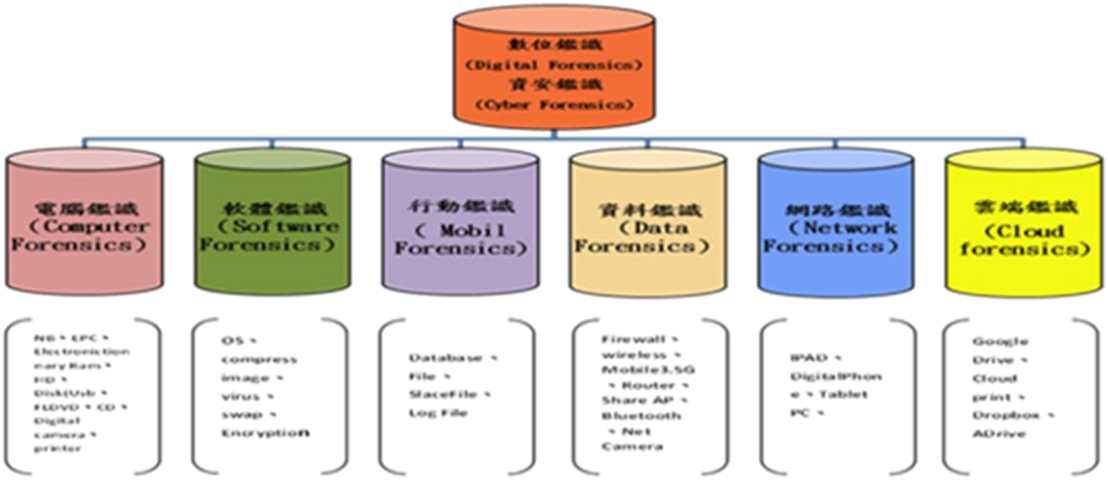
2.1 數位證據

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，國外著名學者 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。

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。

2.2 行動鑑識

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(Cyber Forensics Science)，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，其包括：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 message、FB message、Skype message、Wechat message、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)(如圖一)。行動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。



圖一：資安數位鑑識類型

參、國際鑑識相關標準作業程序

3.1 ISO27037:2012 Guidelines for identification, collection, acquisition and preservation of digital evidence

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(如圖二)，分別為識別階段(Identification)、蒐集階段(Collection)、萃取階段(Acquisition)及保存階段(Preservation)。

(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)

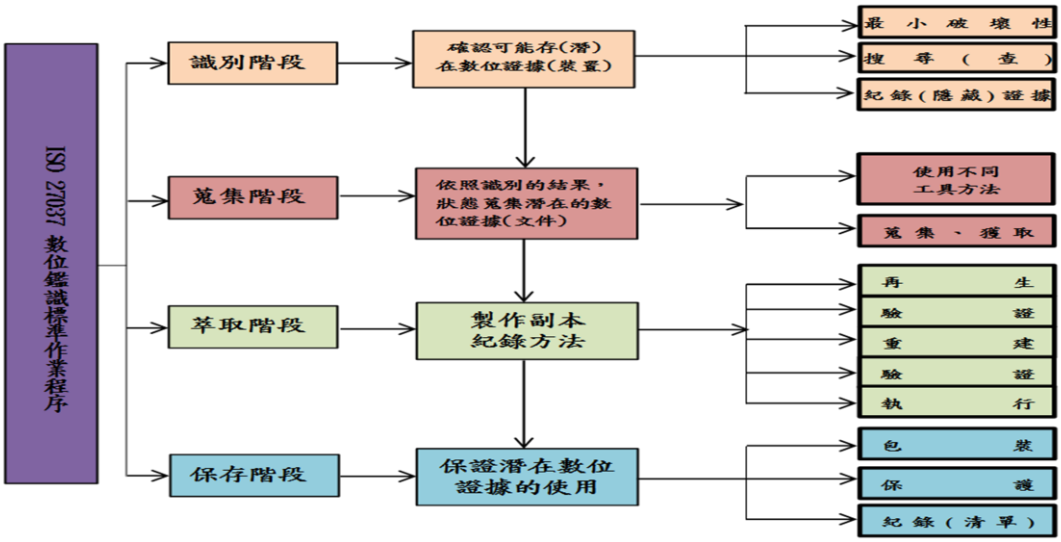
蒐集是一個裝置在數位證據處理程序的流程，包含潛在數位證據的裝置可能有多個狀態，它可能是正在運作或是關閉的狀態。

(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。



圖二：ISO/IEC 27037: 2012 數位證據處理程序

3.2 ISO/IEC27041:2015 Guidance on assuring suitability and adequacy of incident investigative method

國際標準 ISO/IEC 27041 提出資安事件調查方法指引，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(如圖三)，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)

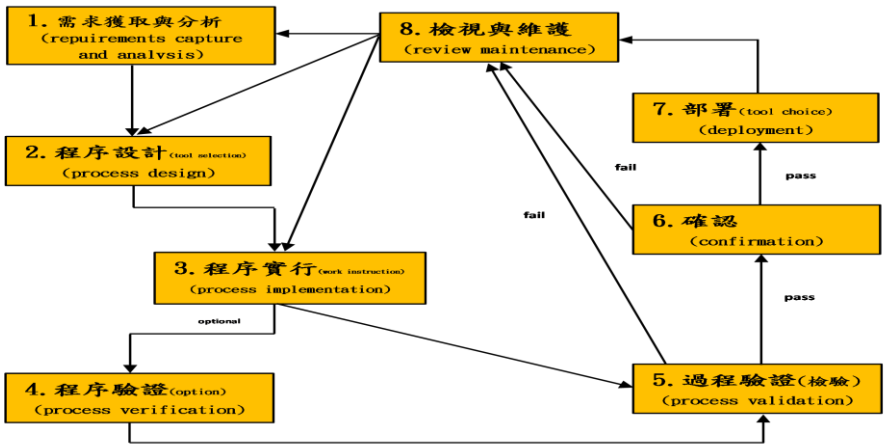
依照過去的調查，確認是驗證或重新驗證的最後一步，或是接續進行下一階段。

(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。



圖三：ISO/IEC 27041: 2015 **資安事件調查方法指引**

3.3 ISO/IEC 27042:2015 guidelines for the analysis and interpretation of digital evidence

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。

(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。

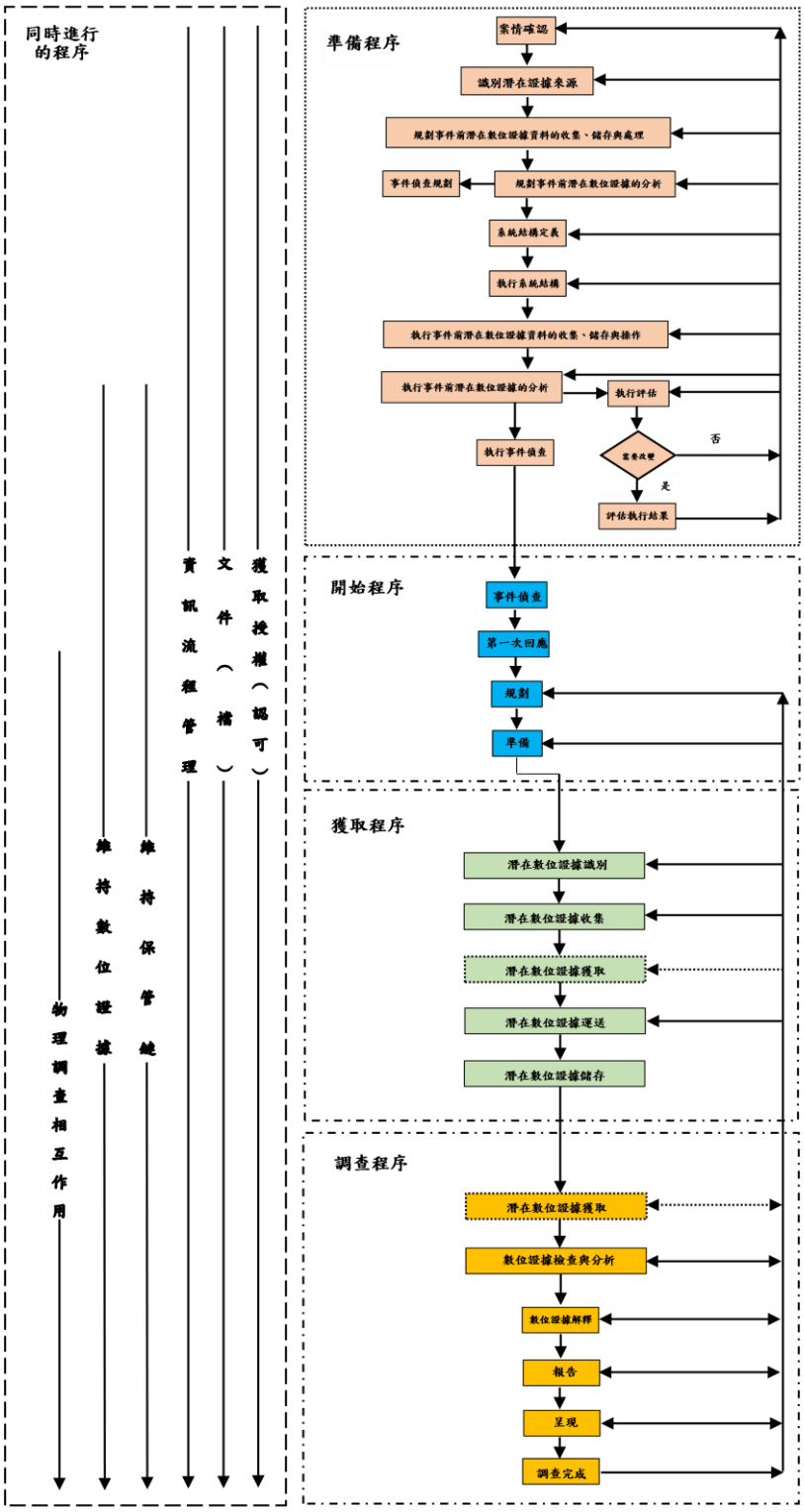
(6) 熟悉程度(Proficiency)

測試能力與熟練度的程序，可以由獨立的第三方證明

圖四：ISO/IEC 27042 數位證據分析與解釋指引

3.4 ISO/IEC27043:2015 Incident investigation principles and processes

國際標準 ISO/IEC 27043 提供基於常見資安事件調查原則與程序理想化模型與涉及各種資安事件(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(如圖五)，各項執行程序如下：



圖五：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。

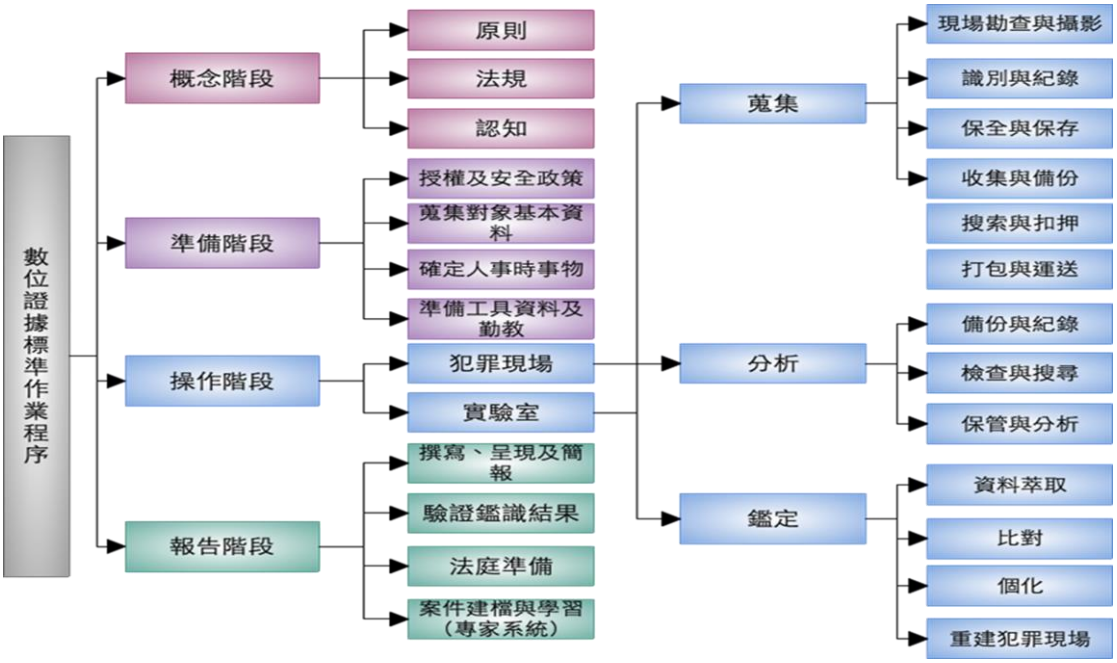
(4) 調查程序

調查程序類型包括資安事件調查、數位原因的調查。

肆、建立行動鑑識標準作業程序(DEFSOP-MF)與整合國際鑑識相關標準

4.1 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)：



圖六：數位鑑識標準作業程序(林宜隆，2012)

1、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 Forensics）的指導原則如下：

a、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)

b、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)

c、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)

d、鑑識人員必須具有專業性原則。

e、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)

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

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

h、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)

i、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

a、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)

b、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)

c、應規範人員資格、設備及鑑定環境之要件。

d、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：

a、**事前鑑識**：安全防護機制及應變計畫。

b、**事中鑑識**：處置及保留證據。

c、**事後鑑識**：鑑定及資料復原。

2、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。

3、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。

a、 **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。

b、 **分析**：備份及記錄、檢查與搜尋、分析與保管。

c、 **鑑定**：資料萃取、比對、個化、重建犯罪現場。

4、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。

4.2 整合國際鑑識相關標準 ISO/IEC 27037、ISO/IEC 27041、ISO/IEC 27042、ISO/IEC 27043 與 DEFSOP 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)四大階段的基礎。

4.2.1 DEFSOP 原理概念階段與 ISO27041: 2015、ISO27042: 2015 及 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(如表一所示)：

1、 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。

2、 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。

表一: DEFSOP 原理概念階段與 ISO27041、ISO27042 及 ISO27043 比較分析

標準 / 原則(方法)	DEFSOP	ISO/IEC27041	ISO/IEC27042	ISO/IEC27043
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

4.2.2 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(如表二所示)。

表二: DEFSOP 原理概念階段與 ISO27041、ISO27042 及 ISO27043 比較分析

標準 / 原則(方法)	DEFSOP 準備階段	ISO/IEC 27041	ISO/IEC 27042	ISO/IEC 27043
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

4.2.3 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(如表三所示)。

表三: 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/IEC27041	ISO/IEC27042	ISO/IEC27043
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

4.2.4 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：

1、 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。

2、 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。

3、 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。

4、 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(如表四)。

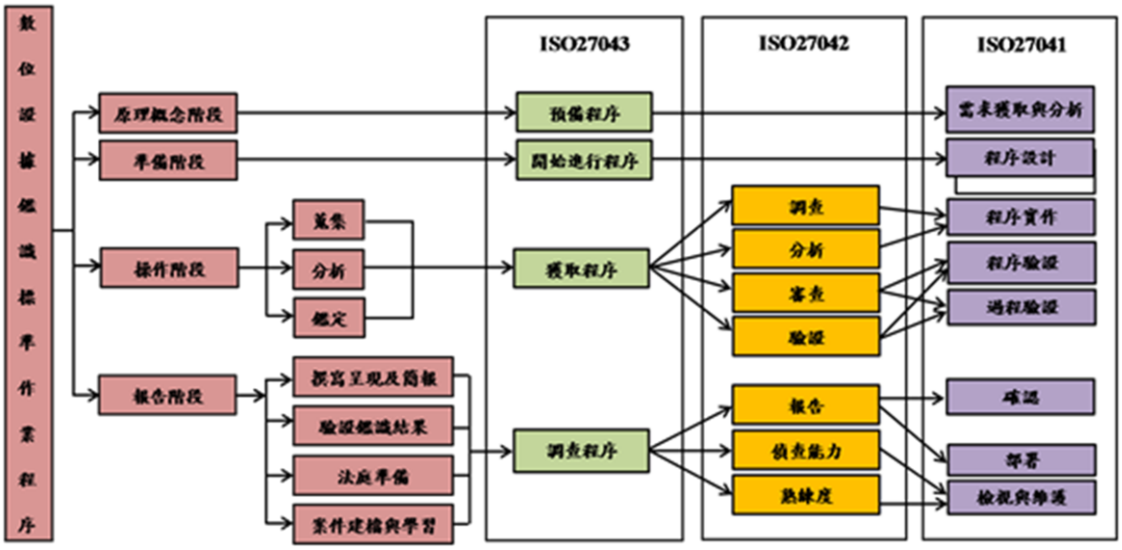
表四: DEFSOP 報告階段與 ISO27041、ISO27042 與 ISO27043 比較分析

標準 / 原則(方法)	**DEFSOP 報告階段**	**ISO/IEC27041**	**ISO/IEC27042**	**ISO/IEC27043**
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(如圖七)。

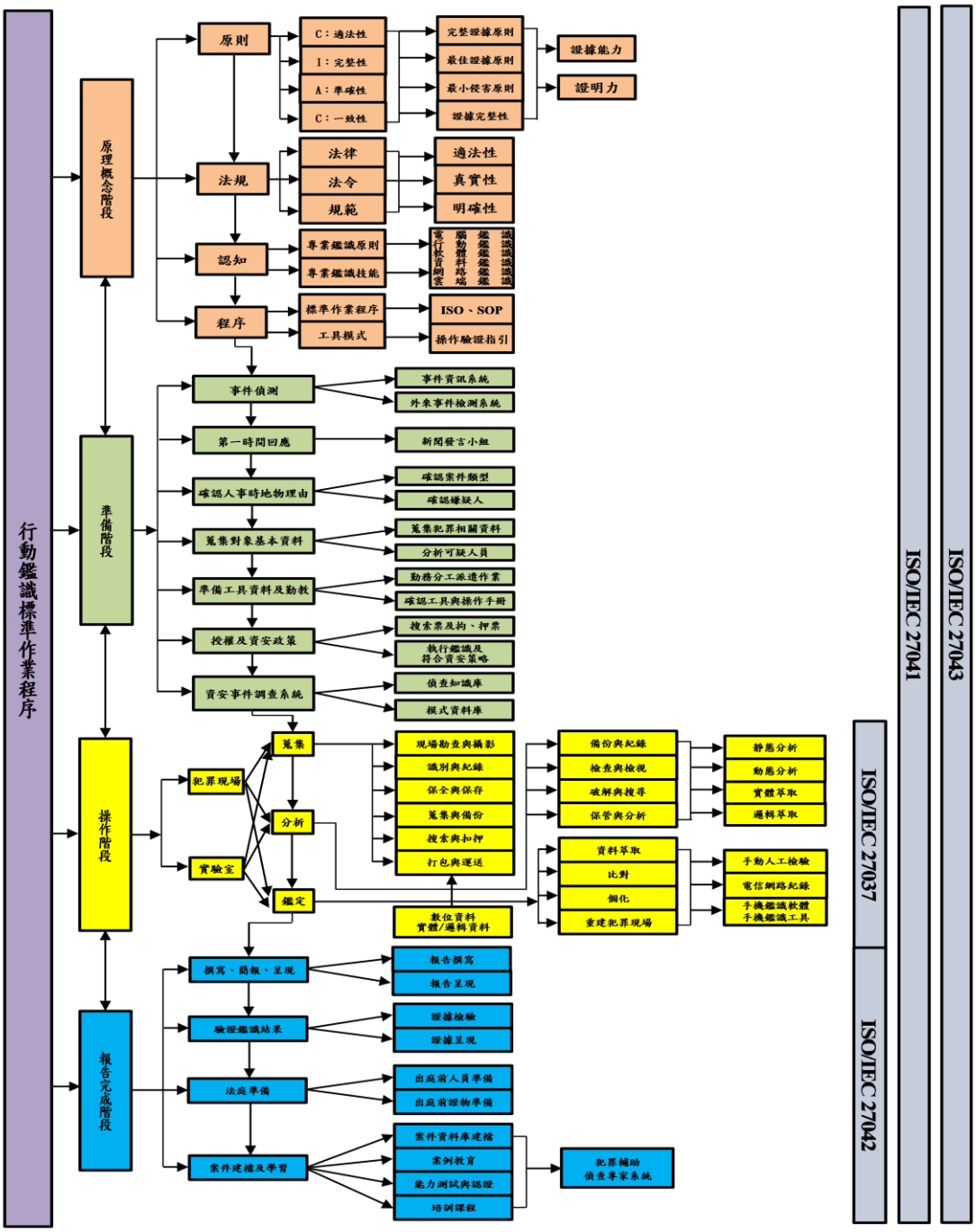


圖七：DEFSOP 與 ISO27041、ISO27042、ISO27043 對照圖

伍、建立整合國際鑑識相關標準之行動鑑識標準作業程序(代結論)

本文參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），以及整合國際鑑識相關標準 ISO/IEC 27037、ISO/IEC 27041、ISO/IEC 27042、ISO/IEC 27043 等作業程序，以**建構行動鑑識標準作業程序架構雛型（Digital Evidence Forensics Standard Operating Procedure , DEFSOP 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等四大階段作探討，以提供未來資安鑑識人員在偵查犯罪的流程、

方向和準則。(如圖八)



圖八：行動鑑識標準作業程序(DEFSOP for Mobile Forensics)

參考文獻

[1] ISO/IEC 27041:2015, “Information technology — Security techniques — Guidance on assuring suitability and adequacy of incident investigative method”, international standard, 2015.
[2] ISO/IEC 27042:2015,“Information technology — Security techniques — Guidelines for the analysis and interpretation of digital evidence”, international standard, 2015.
[3] ISO/IEC27043:2015, “Information Technology — Security Techniques —Investigation principles and processes”, international standard, 2015.
[4] Timothy Wright, The Field guide for investigation Computer Crime: search and seizure basic part three, security focus，2000.
[5] United States of Justice, Federal Guidelines for Searching and Seizing Computers, 1994.
[6] Warren G. Kruse II and Jay G. Heiser, Computer forensics-Incident Response Essentials, 2002, Addison-Wesley corporation.
[7] 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。
[8] 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。
[9] 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。
[10] 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。
[11] 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。
[12] 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。
[13] 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。
[14] 林宜隆、李政謙、陳靜玉、張志欶，「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。
[15] 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。
[16] 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。
[17] 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。
[18] 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。
[19] 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。

[20] 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。
[21] 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。