新興科技環境的數位鑑識科技與策略

2024.10

唐雍為 執行董事

pwc 資誠

重要聲明

1.本文件僅單獨提供　貴公司及周邊單位內部參考使用。

2.本文件內容本公司不對前述資料的真實性進行驗證，同時本公司亦不保證前述資料之完整性及正確性。

3.本文件為機密文件，在未取得本公司書面同意下，本文件不得複製或提供第三人使用，亦不得作為其他用途。對於任何人因違反前述規定，任意傳閱、複製或使用本份報告所引發之任何損失，本公司將不負任何義務及責任。

唐雍為　執行董事

資誠 / 風險及控制服務
☎ (02) 2729 6093
✉ yung-wei.w.tang@pwc.com

| 經歷 |

- 資誠聯合會計師事務所 風險管理及內部控制服務部 副總經理
- 資誠聯合會計師事務所 風險管理及內部控制服務部 協理/經理/顧問
- 曾任 星展(臺灣)商業銀行股份有限公司 資訊安全服務部 協理暨資安長
- 曾任 中華民國銀行商業同業公會全國聯合會 金融業務電子化委員會 技術分組 委員
- 國際資訊安全系統專家(CISSP)、國際電腦稽核師(CISA)
- 國際道德駭客認證(CEH) 、國際滲透測試專家(LPT)
- 國際資安分析專家(ECSA) 、國際數位鑑識專家(CHFI)
- 國際加密貨幣專家(CCE)

| 學歷 |

- 英國華威大學資訊管理碩士
- 交通大學管理科學系(輔修資訊工程、電腦軟體、半導體製程、財務工程)

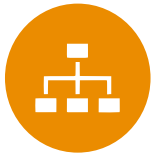
| 服務實績 |

- 資安風險與資安維運評估與諮詢 / 資安治理與縱深防禦輔導與諮詢
- 資訊安全檢測與評估服務與諮詢 / 資安事件系統導入與規劃諮詢
- 資料庫活動管理系統導入與規劃諮詢 / 資訊安全管理制度(ISMS)輔導諮詢
- 個人資訊管理系統(PIMS)輔導諮詢 / 資訊系統專案管理輔導與諮詢
- 區塊練應用分析與諮詢 / 加密貨幣發行 / 證券型代幣發行
- 資訊系統一般控制、應用系統及企業流程之稽核或診斷諮詢
- 內部控制及作業流程優化 / 企業流程再造及數位轉型

Agenda

01 資訊安全威脅趨勢

02 數位鑑識科技發展變革



03 數位鑑識實務介紹

04 新興科技與數位鑑識

1

資訊安全威脅趨勢

2024全球數位信任洞察報告

因**資料外洩**財務損失金額超過百萬美元的比例增加，從前一年的27%升至今年的 **36%**。

仍有超過三分之一企業**未實行風險管理措施**。

52% 認為未來12個月，生成式AI可能導致**災難性網路攻擊**。

PwC 發布《全球數位信任洞察報告》針對全球71個國家或地區、共3,876位高階主管進行調查，探討企業在未來12至18個月可能遭遇的資安挑戰與機會。

全球企業對於生成式人工智慧可能產生的風險準備不足。另外，**因資料外洩，蒙受財務損失超過百萬美元的企業，在過去一年比例有增加的趨勢**。

資料來源：2024 PwC 全球數位信任洞察報告

資安事件案例分享

電信商傳出**資料外洩**，我國國安單位內部資料流入暗網

本資料由　(上市公司)　公司提供

序號	1	發言日期	113/02/29	發言時間	12:43:34
發言人		發言人職稱	執行副總經理兼財務長	發言人電話	
主旨	說明本公司疑似資訊外流事件				
符合條款	第	26	款	事實發生日	113/02/29
說明	1.事實發生日：113/02/29 2.發生緣由：媒體報導 3.處理過程： 本公司資安團隊於查知有疑似資訊外流事件時，已全面啟動相關檢視與資安防禦機制，積極展開調查，藉以釐清問題發生原因，並與外部資安技術專家共同合作處理，同時通報政府部門，保持密切連繫。 4.預計可能損失或影響：目前評估對公司營運尚無重大影響。 5.可能獲得保險理賠之金額：不適用。 6.改善情形及未來因應措施： 本公司資安團隊於查知有疑似資訊外流事件時，立即啟動相關檢視與資安防禦機制。 本公司將持續強化網路資安管控以確保資料安全。 7.其他應敘明事項：無。				

近期暗網出現電信商與國安單位之間往來的**機密文件**和公文，賣家聲稱握有1.7 TB資料，內容涵蓋內部文件、逾7千個資料庫，政府採購合約等。

國防院戰略資源研究所長認為，很有可能是相關人士的**手機遭到入侵**造成。

資料來源：iThome (2024)

2024全球企業領袖調查報告

01 41% 企業認為生成式AI可為企業營收帶來正面影響

02 70% 全球CEO認為，生成式AI未來三年將為價值創造帶來重大改變

03 **採用生成式AI的企業領袖中，擔憂生成式AI 帶來之資安風險比例達 68%**

- 生成式AI（Generative AI）是利用人工智慧技術生成包括圖像、音檔與影片。
- 生成式AI可以用來創建高度逼真的假圖像和視頻，這被稱為深偽技術（Deepfakes），這些假圖像和影片可用來進行**身份偽冒、詐欺等舞弊行為**。

資料來源：
PwC 第27屆全球企業領袖調查報告 2024

詐騙事件案例分享

跨國企業遭 Deepfake**視訊會議詐騙**，損失金額達 2億港幣

香港警方接獲跨國公司報案，報案人於上月收到假冒該公司英國總部首席財務官的訊息，對方聲稱要進行機密交易，邀請報案人參與一個多人視訊會議。

當時參與視訊會議的各成員，**顯示與真實人物相同的面貌**，雖報案人曾有懷疑，但最終不虞有詐，按指示匯款共2億港元，報案人向總公司查詢後，才驚覺被詐騙。

資料來源：iThome (2024)

2024全球經濟犯罪調查報告

55%

受訪企業表示採購舞弊為當地常見的犯罪。

01

42%

企業未進行**第三方風險管理或評估**。

02

03

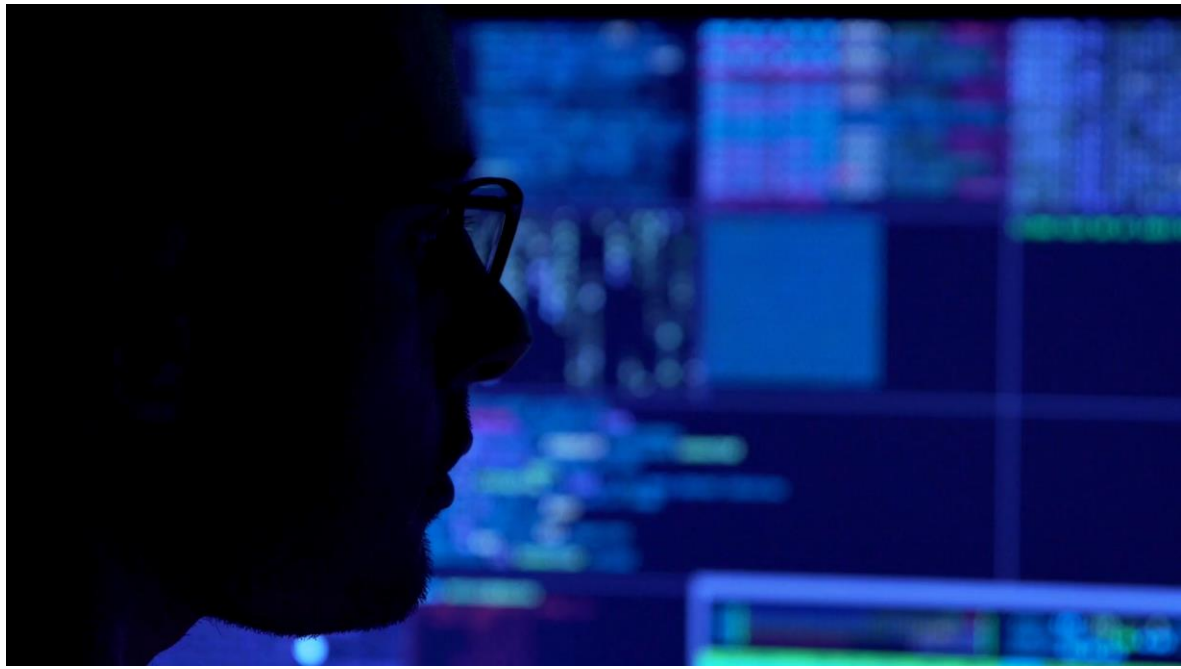
32%

企業從未計算過**舞弊造成的損失**。

04

74%

企業未有可辨識或對抗採購舞弊的工具



資料來源：PwC 全球經濟犯罪調查報告 2024

現今技術的創新，導致舞弊案件的調查困難度逐漸提高。

數位鑑識

- 當發生**舞弊事件**或**資安事件**時，因犯罪型態手段日趨複雜，傳統偵查方法已難以因應。

- 現實世界中，對企業關鍵資產感興趣的除駭客外，**競爭同業**及**企業內部員工**也是威脅企業資安的重要來源。

- 科技犯罪的成本及門檻低、具隱匿性及偵查不易等特點，不少企業開始著重經濟犯罪的偵防。然而，在**案件發生時結合數位鑑識**，**做好證據保全**，**在必要時透過司法維護自身權益**，資安投資才能發揮最大效益。

資料來源：PwC 數位轉型下資安與數位鑑識

2

數位鑑識科技發展變革

國際數位鑑識發展趨勢

起步階段

- 數位鑑識剛起步，主要集中於簡易數據恢復與基本硬碟分析。
- 主要涉及電腦犯罪，如未經授權的系統侵入和數據盜竊。
- 最早設立防治電腦犯罪的法條為：**佛羅里達電腦犯罪防治法**

電子揭證興起/網絡與移動設備普及

- 隨著互聯網與手機普及，網絡犯罪成為數位鑑識的重要領域，如：網絡釣魚與金融詐騙。
- **新工具和技術不斷開發**，以處理不同類型的數位證據，如手機取證工具。

人工智慧與大數據

- AI技術在數位鑑識中的應用變得更加普遍，**用於模式識別、異常檢測和自動化數據分析**。
- 資料量的爆炸性增長，要求更先進的大數據分析技術，以處理、分析海量數據。
- 區塊鏈技術的應用，帶來新的鑑識需求，如：分析加密貨幣交易和智能合約。

數位鑑識科技產業變革及法規影響

- 開始建立相關法律框架與標準，如：美國的《計算機詐欺和濫用法》(Computer Fraud and Abuse Act)。
- 成立專業鑑識機構與學術研究團體，如：美國的HTCIA (High Technology Crime Investigation Association)。

雲端計算與物聯網

- 雲端服務廣泛應用，使雲端數據成為鑑識的重點，涉及多租戶環境和數據存儲位置的複雜性。
- 物聯網設備普及，帶來新鑑識挑戰，包括：如何提取和分析來自各種智能設備的數據。
- **人工智能和機器學習技術開始應用於數位鑑識**，以提高分析效率和準確性。

預測與展望

- 將出現更智能化的鑑識系統，自動化處理大部分的鑑識流程，提供更精確的分析結果。
- 雲端數位鑑識可能對數位鑑識產生重大影響，包括**加密技術破解與更高效的數據處理能力**。
- 數據來源多樣化與分佈式計算普及，數位鑑識將需處理更複雜和分散的數據環境。

數位鑑識科技產業變革及法規影響

1980 1990 2000 2010 2020 2030

數位鑑識的根本需求來自解決法律的需求，法規在這十年間的發展主因來自於國安及公司治理危機。

危機過後，法案持續成為產業發展的依據，許多直接或間接涉及數位資訊處理的法規不勝枚舉。

國安軍事面

2001年發生紐約世貿911恐怖攻擊，及2005年發生倫敦地鐵炸彈攻擊後，各國意識到數位鑑識在反恐戰爭的重要性，除了**發展相關鑑識技術，也頒佈了相關法案**。

重要法案：2001，《美國愛國者法案》

刑事偵查面

電腦網路科技的興起，使得傳統的犯罪偵查方法難以抑制高科技犯罪，促成**數位鑑識技術被大量應用在犯罪的偵查**上。

重要文件：2003，《英國ACPO數位證據取證實戰指南》

重要鑑識工具測試方法：2004，NIST's CFTT

資訊治理面

商業交易與相關活動日漸依賴資通技術，由於企業資料逐漸數位化，相關安全防護也變得異常重要。數位鑑識技術因此常被應用在智財保護、訴訟支援、責任釐清等支援上，相關法令規範陸續被發佈。

重要法規：計算機詐欺和濫用法，1986 ； HTCIA，1986 ； 1996，HIPPA；2001，IFRS；2002，Sarbannes-Oxley；2004，Basel II；2006，FRCP； 2010，PCI DSS、個資法

電子揭證(e-Discovery)興起

1980 1990 2000 2010 2020 2030

Discovery 是美國訴訟程序上的一種程序，類似國內的準備程序，讓訴訟雙方交換各自掌握的證據，促進提前合解，避免進入冗長的法律訴訟程序，而 **e-Discovery 是用於訴訟或調查的電子內容搜索**。

美國於2006年11月修法通過電子蒐證法，即針對「電子儲存資訊」ESI (Electronically Stored Information)定義了法律認定的相關發現程序和原則。

電子郵件是主要的數位證據之一，在法律訴訟佔有重要地位。

美國於2002年所通過的沙賓法案(Sarbanes-Oxley Act)，及日本2008開始實施的日本版沙賓法案(J-SOX)中均**明文規定企業有責任保存電子郵件記錄**，其適用範圍遍及所有在美國或日本上市的公司。

因此近年來許多的科技訴訟案例中，如何**有效利用電子郵件進行舉證**已成為訴訟成敗的主要關鍵因素。

雲端計算與物聯網的普及

1980 ····· 1990 ····· 2000 ····· 2010 ····· 2020 ····· 2030 ····· ▸

隨著雲端服務與物聯網技術的發展帶來了新的挑戰和機會，促使數位鑑識採用新的技術和方法來應對這些變化。

美國於2018年頒布美國《雲端法》，更新《1986年儲存通訊紀錄法》，並釐清海外資料合法取得，無論資料儲存地在美國境內或境外執法機構均可**合法請求相關紀錄的保存或揭露**。

解決跨國數據存取的法律和技術挑戰，以便迅速取得存儲在境外的數據，確保數據存取的合法性和合規性。

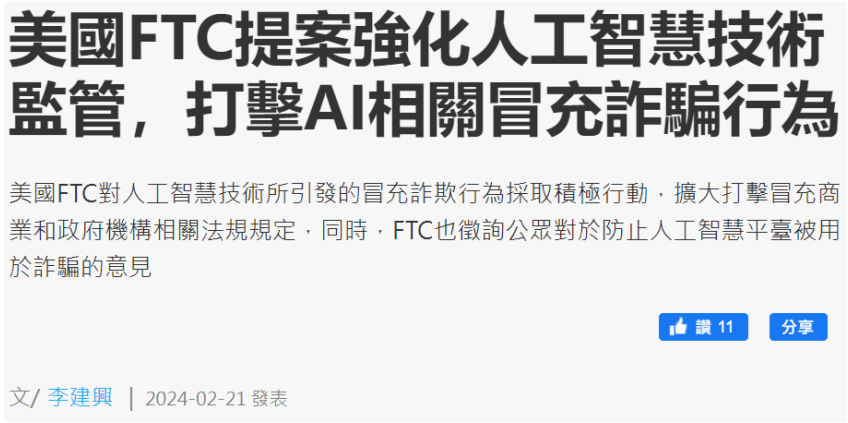
澳大利亞政府於2018年頒布《1997年電信法案》的修正法案，此法案授權執法和國家安全機構發出技術協助要求，**強制科技公司提供技術支援**，包括：解密數據與開發技術。

人工智慧與大數據興起

1980 1990 2000 2010 2020 2030

隨著AI技術的迅猛發展，其應用範圍和影響力日益擴大，但也帶來了新的風險和挑戰。特別是AI生成的假冒內容和自動化詐騙行為，對消費者和市場秩序構成了嚴重威脅。

- AI生成的深度偽造（deepfake）視頻和音頻、假信息和自動化詐騙行為等，對消費者和企業構成了新的威脅。
- 聯邦貿易委員會（FTC）法案：FTC對涉及AI和大數據技術的詐騙行為進行監管，包括AI在數據分析過程中的透明度和公平性。
- 通過加強監管和合作，提升透明度和責任制，並加強消費者教育，希望能夠有效地打擊AI相關的冒充和詐騙行為，促進AI技術的健康發展。



美國FTC提案強化人工智慧技術監管，打擊AI相關冒充詐騙行為

美國FTC對人工智慧技術所引發的冒充詐欺行為採取積極行動，擴大打擊冒充商業和政府機構相關法規規定，同時，FTC也徵詢公眾對於防止人工智慧平臺被用於詐騙的意見

讚 11 分享

文/ 李建興 | 2024-02-21 發表

其他國外相關法規趨勢

隨著數位技術的快速發展，數位鑑識在刑事調查、反恐、網絡安全和企業合規等領域的重要性日益增強，

法規的改革趨勢反映了技術進步、隱私保護需求和國家安全考量之間的不斷平衡。

證據完整性及合法性 (2012/2023)

英國ACPO數位證據取證實戰指南：

- 更新數位證據搜集的標準操作程序。強化證據展示與報告要求。

美國聯邦刑事訴訟規則：

- 因電子證據在刑事訴訟中的重要性不斷增加，確保電子證據的搜集、保存與展示符合法律要求。

增加透明度及問責制 (2015)

美國自由法案：

- 要求機構揭露其資料搜集和處理方法，使公眾能夠瞭解並監督。
- 限制大規模資料搜集

加強隱私保護 (2018)

通用數據保護條例:

- 要求機構只能搜集和處理完成特定任務所需之最小數據。
- 數據處理過程中，使用去識別化技術。

加強跨國數據和國際司法合作 (2022)

布達佩斯網路犯罪公約 (第二附加議定書)：

加強國際執法合作，確保跨國網絡犯罪案件的有效調查和起訴。

臺灣數位鑑識發展趨勢

初步意識與概念引入

- 數位鑑識和電腦犯罪的概念在臺灣逐漸被認識，但尚未形成系統性的法律架構。
- 學術界開始進行研究，但缺乏明確的法規支持。

網絡犯罪與法規完善

- 2001年實施的《電子簽章法》促進了電子商務的發展，同時也規範了電子證據的法律效力。
- 2003年通過的《通訊保障及監察法》規範了通訊數據的保護和監控，為數位證據的合法搜集提供了法規依據。
- 刑事局於2006年成立「**科技犯罪防制中心**」以因應通訊、科技技術不斷發展以及**電腦犯罪**、**白領犯罪**、**經濟犯罪之上升**。

人工智慧與機器學習

- 隨著人工智能技術的應用，政府已逐步制定與AI技術相關之框架，如：金管會《金融業運用人工智慧(AI)指引》
- 針對人工智慧於數位鑑識領域，目前臺灣並未有相關法規依循。

1980 · 1990 · 2000 · 2010 · 2020 · 2030 ▸

法規初步制定

- 成立電腦犯罪防制中心，研擬電腦犯罪（含網路犯罪）政策。
- 初步標準化：初步制定了一些數位證據搜集和保存的標準和流程。

雲端服務與數據隱私法規

- 2012年修訂的《個人資料保護法》強化了對個人數據的保護，對個人資料搜集有了更高要求。
- 隨著雲端服務的廣泛應用，政府於2019-2023年逐步增定雲端服務相關法規，如：《金融機構作業委託他人處理內部作業制度及程序辦法》第19條

預測與展望

預計持續依據新興技術，如人工智慧與機器學習應用方向進行規範制定。

網路犯罪與法規完善

隨著資訊通信科技的快速發展，我國警政當局也注意到其帶來的犯罪問題，以及運用新科技打擊犯罪的重要性。

環境背景：

- 2000年開始，網路犯罪比率逐年上升。為應對網路犯罪行為，修訂刑法以包括透過電子通訊或電腦系統進行詐欺的行為，使網路詐騙可依法定罪並進行懲處，如：《刑法》第339-4條。
- 2003年制定的《電腦處理犯罪條例》也針對電腦相關犯罪進行了明確的規範，包括未經授權存取電腦系統、破壞資料等行為。
- 2010年政府規劃「科技犯罪防制工作中程計畫」，實施六項重要工作，其中一項為：**成立電腦鑑識及科技偵查實驗室**。

執法情況：

符合國際標準的蒐證程序尚未明確建立，使得司法官對於搜集數位證據的證據能力不足，以致法庭上爭議不斷。

- 2018年刑事訴訟法第122條，分別對被告、第三人的**電磁紀錄搜索**進行規範。
- 2018年開始陸續於8個地檢署，成立「數位採證中心」，進行數位採證、判斷、解讀數位證據或報告。

資料來源：2013 資訊通信科技對臺灣縣市犯罪率的影響
2018 TWNIC 建構行動鑑識標準作業程序

雲端服務與數據隱私法規

1980 ····· 1990 ····· 2000 ····· 2010 ····· 2020 ····· 2030 ▸

行動設備的普及與成長，不但帶動了雲端服務發展，也使得數位鑑識調查更為複雜。

《個人資料保護法》強化了對個人數據的保護，對個人資料的搜集、處理、使用和儲存的規定，以及**跨境傳輸**，有了更高的要求。

隨不斷增長的數位犯罪威脅、司法和企業安全的需要，進行雲端鑑識並解析雲端服務存取足跡的需求越來越多。

基於雲端服務的特性，數據可能儲存在不同國家。數位鑑識可以幫助解決跨境調查的挑戰，確保資料在不同法域間的傳輸處理符合相關法律法規。

對行動裝置做雲端鑑識　解析雲服務存取足跡

2017-11-22 中央警察大學資訊密碼暨建構實驗室（ICCL）

人工智慧與機器學習

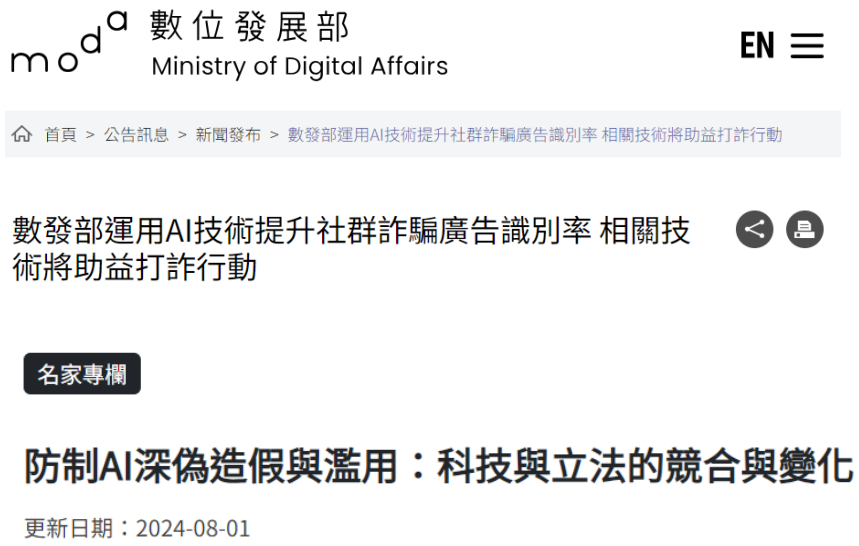
1980 1990 2000 2010 2020 2030

隨著網絡詐騙手法日益複雜和多樣化，傳統的防詐技術已難以應對新興威脅。為更有效保護消費者和企業免受詐騙侵害，投入了大量資源和技術力量，運用AI技術準確偵測網絡上的各類詐騙廣告，從而提升網絡安全防護能力。

通過科技與法律的競合與變化，可以有效保護個人隱私、維護社會秩序，並促進AI技術發展。

臺灣於2024年頒布「金融業運用人工智慧(AI)指引」與「人工智慧基本法」草案，參考國外法規建立隱私保護、資料治理及資安防護相關規範。

促進AI技術的創新和應用，同時保障數據隱私和安全，確保技術發展符合倫理和法律標準。



臺灣相關法規趨勢

隨著數位技術的快速發展，數位鑑識在刑事調查、反恐、網絡安全和企業合規等領域的重要性日益增強，

法規的改革趨勢反映了技術進步、隱私保護需求和國家安全考量之間的不斷平衡。

電子簽章和數位證據 (2014)

電子簽章法：

規範電子簽章和電子文件的法律效力，並要求使用數位鑑識技術檢測和驗證電子簽章的真實性和完整性。

增加透明度和問責制 (2018)

通訊保障及監察法 ：

法規保障秘密通訊自由及隱私權，**要求執法機構於進行通訊監察時，需遵循的程序**，並增加對監察活動的監督，以確保其合法性和透明度。

加強隱私保護 (2023)

個人資料保護法：

強調數據最小化原則，要求機構僅能搜集與處理完成特定任務所需之最少數據。

證據完整性及合法性 (2024)

刑事訴訟法：

刑事訴訟法對數位證據的搜集、保存和使用提出具體要求，確保數位鑑識技術在刑事案件中的應用符合法律程序。

數位鑑識技術演進

過去的數位鑑識

01 **手動分析**
資料量小，依賴調查人員之經驗與直覺，透過基本的資料恢復與檢索工具進行調查，且速度較慢。

02 **有限的自動化**
有限的自動化工具，主要用於基本資料篩選排序，且報告通常是手動製作的，耗時且易犯錯。

03 **過度依賴特定硬體**
數位鑑識技術依賴於特定的硬體設備，如硬碟克隆器和磁帶讀取器，難以擴展處理大量數位證據

參考來源： The Future of Digital Forensic Investigations, 2024

處理**大規模資料集**，包括：電子郵件、照片、視頻。依賴於機器學習技術自動識別和分類數據，**大幅提高處理速度**，減少了人力資源需求。

利用AI進行模式識別、自然語言處理和行為分析，**快速識別關鍵證據**，並自動進行分類。

利用雲端計算資源處理和存儲**大量數據**，提供更高的**可擴展性和靈活性**，同時從大量的數據中提取有用的資訊，提高調查效率。

數位鑑識社群，成員能於社群內自發性學習，並**與其他專家學者進行交流，或是舉行專業論壇**，使專業人員能夠快速掌握數位鑑識之新技術與挑戰。

3

數位鑑識實務介紹

為什麼要瞭解數位鑑識？

根據實務經驗，當發生科技犯罪時，**企業要做的第一件事**，通常**是保全證據**，而不是讓受害的主機**恢復正常運作**。

以個資外洩為例，要證明無故意或過失，需要證據，事發時立即拔除網路、關機、重灌系統，將導致**證據被湮滅**，造成**舉證困難**。

建議以數位鑑識方式保全證據後，再恢復系統較為妥適。

科技犯罪回應方式

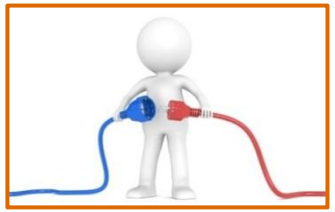
發生科技犯罪當下，**應該**：

Step 1 以數位鑑識方法保全證據

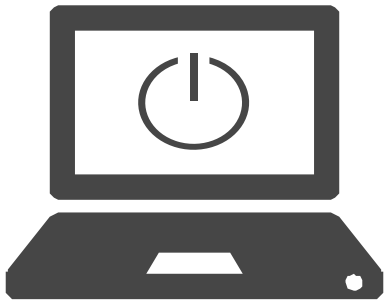
Step 2 追查問題根源
讓被入侵的系統恢復正常運作

- 要證明無故意或過失，需要證據。
- 若事發時立即拔除網路、關機或重灌系統，將導致證據被湮滅，造成舉證困難。

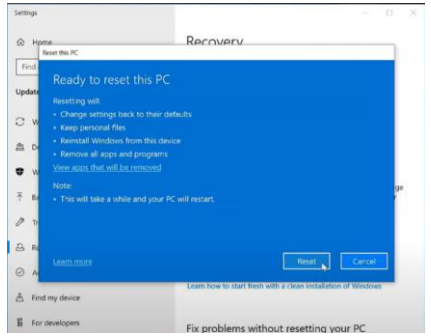
發生科技犯罪當下，**不應**：



立刻拔網路線



關機



重灌系統

數位鑑識標準作業程序

數位鑑識係利用科學驗證方法調查數位證據，經由資料還原、擷取、分析等過程，還原案情原貌，作為後續處理之依據

訪談(Identification)

1. **瞭解案情**
2. **系統分布與資料量**
3. **作業時程**
4. **...**

- 個資外洩、駭客侵入
- 未授權使用、智慧財產權竊取
- 破壞資料安全、惡意軟體侵襲等
- 違約/侵權損害賠償認定及計算
- 不合常規交易等疑似舞弊行為的內部調查等

01 蒐證
錄影/拍照、現場處理、映像檔製作、證物封存 (Acquisition)

02 保全
確認數位證據完整搜集、資料一致性 (Preservation)

03 分析
利用數位鑑識方法，確保分析過程證據不受污染 (Analysis)

04 呈現
提供客觀的數位鑑識報告，供後續處理 (Presentation)

訪談階段作業內容

1 瞭解案情

於鑑識作業開始前，透過專案會議，邀請鑑識團隊成員、客戶代表、律師等，**瞭解案件背景、目的及鑑識目標**等。

2 確認證據所在

透過案件背景，分析證據可能之所在處 (例如：個人電腦、郵件伺服器、手機等)。並依過往經驗，建議**蒐證之順序及方法**。

3 系統與資料量

系統版本、所在地及資料量，為蒐證作業前的關鍵資訊。鑑識團隊將依該資訊攜帶經認證的鑑識設備前往蒐證。

訪談階段作業內容

4 作業時程

蒐證作業過程中，客戶或律師會全程陪同，故需花費多少時間蒐證、分析，乃至出具鑑定報告，皆會在**專案會議中說明清楚**，確保各方期待一致。

5 瞭解目標

瞭解鑑識目標

訪談階段應辦事項

鑑識人員

- 透過專案會議，**瞭解案件背景、目的及鑑識目標**。
- 分析證據可能之所在處 ，並依過往經驗，建議**蒐證之順序及方法**。
- 攜帶經認證的鑑識設備前往蒐證。
- **評估鑑識作業時程**。

被蒐證人員及公司

- **確保所有蒐證活動符合法律和公司政策**。取得必要的搜索令或法律授權。
- 如果法律要求，通知相關人員即將進行的蒐證活動，並解釋其權利和義務。
- **確保蒐證環境的安全**，防止數據被篡改或損壞。
  - **勿**拔除網路線。
  - **勿**關機。
  - **勿**重灌系統。

數位鑑識工具準備

於訪談階段瞭解系統與資料量背景時，便可進行硬體準備作業

硬碟

目標儲存設備之蒐證應一式二份，且攜帶之硬碟數量應足夠。

防靜電手套

避免鑑識人員身上靜電導致電子設備損壞。

硬碟複製機

若目標硬碟沒有加密(Disk Encryption)，則可以透過硬碟複製機，快速進行證據映像檔製作，可同時一式二份，並驗證映像檔製作結果與原始資料一致。

阻寫器

避免在讀取證據資料時，污染原始資料，造成不可逆的資料破壞。

電波時鐘

用以證明目標主機時間與標準時間的實際差異，以便在還原案發現場時，能用正確的時序呈現之。

照相機/攝影機

用以證明所有蒐證及鑑定作業是在監控環境下進行，以確保鑑定結果之正確性與有效性。

手電筒

於光源不足環境下清楚辨識目標主機所處 狀況、其條碼序號、財產管理編號等。

數位鑑識工具準備

筆電

通常搭配防寫器一起使用，用以檢查原目標硬碟的內容、進行活體鑑識使用，或現場分析使用。

Dongle

部份鑑識軟體需要搭配Dongle方能使用其完整的功能，如Encase、FTK等。

電源延長線

蒐證現場的電源插座常有不足的情況，電源延長線是必備設備之一。

螺絲起子

依目標主機類別及型號，準備相對應之螺絲起子，避免到了現場後卻發現目標主機的螺絲拆不下來。

螺絲收納盒

於蒐證拆卸目標主機時，將卸下的螺絲收好，避免安裝回去時發現缺件的窘境。

便利貼

用以辦別原目標主機或物品的正確位置，方便於蒐證完成後再原物擺放回原位置，避免鑑識目標人物發現異常。

氣泡紙

在運送過程中，避免鑑識設備及硬碟等電子設備，因不慎碰撞而導致損壞。

蒐證與保全階段作業內容

1 錄影/拍照

於蒐證開始前、進行中及完成後，皆需對作業進行拍照及錄影，**確保所有過程禁得起檢驗**。

2 現場處理

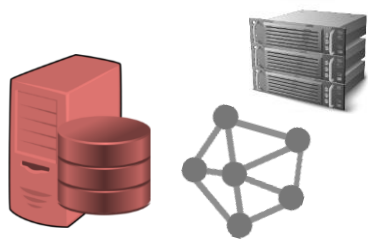
為**確保鑑識目標無察覺**，將目標主機移至他處進行蒐證後，應減少碰觸目標位置物品，如：椅子、鍵盤及滑鼠。且應記錄所有排線連接方式，避免誤接引起懷疑。

3 映像檔製作

依據訪談內容對鑑識目標主機進行蒐證，將硬碟及記憶體內容進行映像檔備份，一式二份。

蒐證順序

電子郵件/網路記錄
/Server記錄

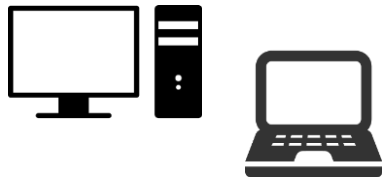


為避免打草驚蛇，蒐證作業不會直接與嫌疑人接觸的證據可能所在處開始進行。

僅需IT人員配合提供出入機房及存取伺服器權限。

蒐證方式多為針對資料所在磁區或資料夾，製作成映像檔。

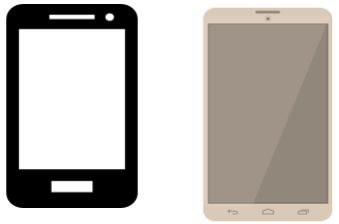
個人主機/筆電
(含USB隨身碟、外接式硬碟、光碟等)



當鑑識人員從前類設備找不到證據時，或需要更多的證據佐證，會對嫌疑人所使用的主機設備蒐證，嘗試發掘更多證據。

對個人主機/筆電蒐證需十分謹慎，避免當事人發現而滅證，造成後續重建犯罪現場的困難。

個人手機能否進行蒐證？



蒐證與保全階段作業內容

4 映像檔內容檢驗

映像檔備份完成後，須**確保結果與原證物內容一致**，且映像檔內容可正確讀取。

5 證物攜回

證物是鑑識的核心，必須小心保全攜帶，**避免運輸過程受損或遺失**，盡量避免搭乘大眾運輸工具，降低運送風險。

蒐證與保全階段應辦事項

鑑識人員

- 對作業期間之行為進行拍照及錄影。
- 將目標主機移至他處進行蒐證，並記錄所有排線連接方式。
- **依據訪談內容對鑑識目標主機進行蒐證**，並將硬碟及記憶體內容進行映像檔備份。
- 須**確保結果與原證物內容一致**，且映像檔內容可正確讀取。
- **避免證物運輸過程受損或遺失。**

被蒐證人員及公司

- **應確保相關設備（如電腦、手機、伺服器等）處於原始狀態，勿關機、重新啟動或於蒐證過程中使用相關設備。**
- 提供必要的存取權限和密碼。
- 協助鑑識人員進行映像檔備份。
- 回答鑑識人員的問題，提供設備和資料的相關訊息。

分析階段作業內容

1 已刪除資料回復

回復已刪除資料通常是分析作業的第一個動作。鑑識人員對這些被刪除的資料很感興趣，例如它們與案件之間的關係、何時被刪、為何被刪等。

2 關鍵字搜尋

鑑識人員從訪談過程中掌握的關鍵字，及對本案的瞭解所引發的關鍵字進行搜尋，並在過程中不斷刪除及增加可能的關鍵字，直到找到相關的證據為止。

3 檔案解密

檔案加密是常見的證據隱匿手段之一。然而解密可能是一個十分消耗資料的過程。鑑識人員會依據經驗判斷並建議客戶是否提撥額外的預算進行解密。

分析階段作業內容

4 登錄檔/日誌分析

嫌疑人曾經安裝或刪除何種軟體、隨身碟使用紀錄、最近存取之檔案紀錄、曾拜訪的網站等，皆可透過分析登錄檔及日誌得知。

5 時序分析

檔案的建立、修改及存取時間是識別證據是否與案件有關的重要資訊之一。

透過分析各個證據的發生時間序，鑑識人員得以重建犯罪現場。

Hypothesis and proof

分析階段應辦事項

鑑識人員

- 回復已刪除資料並進行關鍵字搜尋。
- 判斷並建議客戶是否提撥額外的預算進行解密。
- **登錄檔、日誌、時序分析。**

被蒐證人員及公司

- 提供被蒐證設備和資料的背景訊息，幫助鑑識人員理解資料的上下文。
- 評估是否提撥額外的預算進行解密。

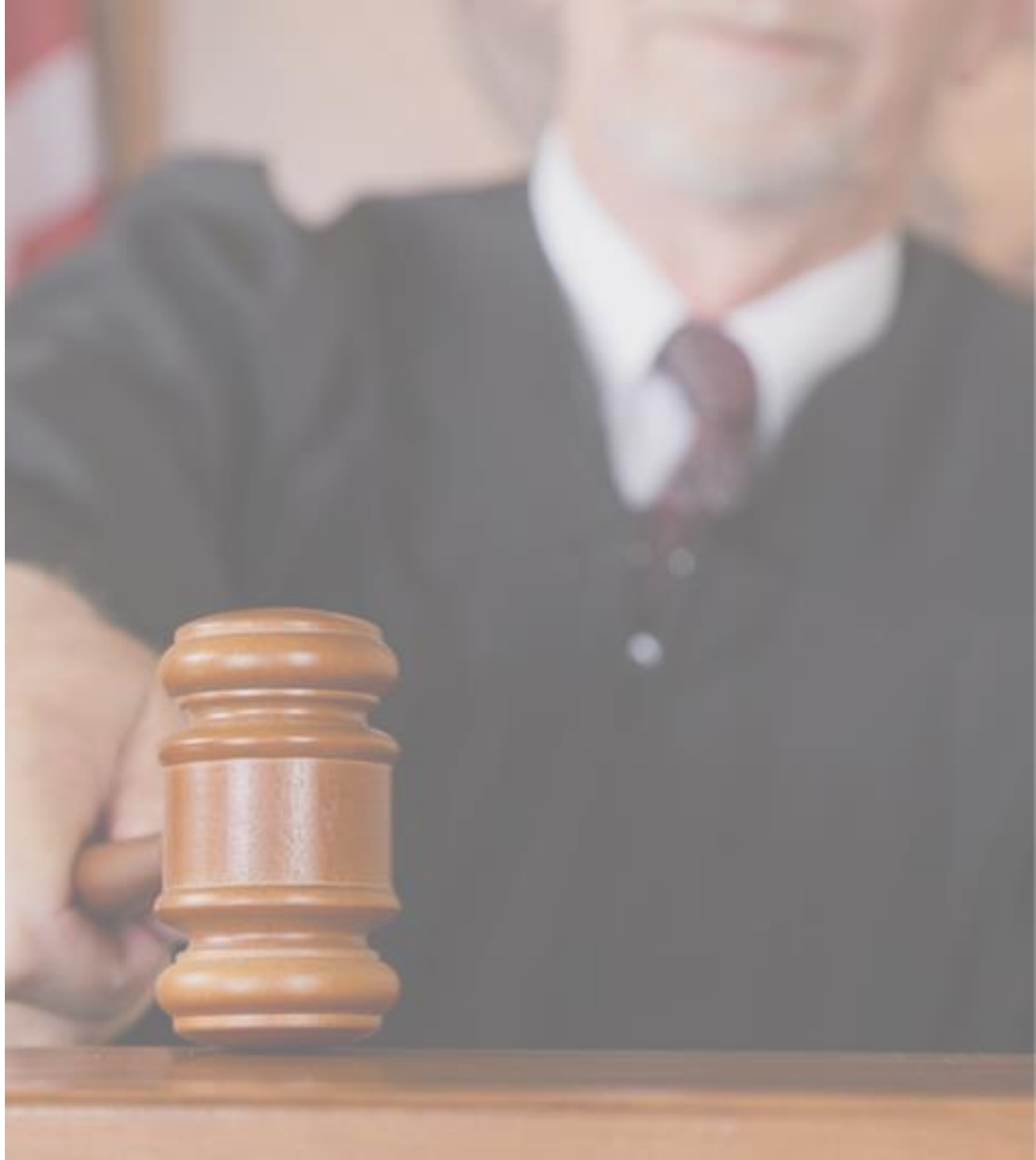
呈現階段作業內容

4 為了保障當事人的防禦權，鑑定者有出庭接受交互詢問之必要。

1 鑑定者針對鑑定事項，必須具有**專業的證明能力**。

2 對於所使用的鑑定儀器或方法，須有精確性，並依照**公認的標準程序**進行，以保證鑑定結果。

3 **鑑定結果不會因人、時、地而改變，且可讓其他專業者有重現相同結果的可能。**



呈現階段應辦事項

鑑識人員

- 對於所使用的鑑定儀器或方法，須有精確性，並依照**公認的標準程序**進行。
- 提供客觀的數位鑑識報告，並確保鑑定結果**可讓其他專業者有重現相同結果的可能**。
- 出庭接受交互詢問。

被蒐證人員及公司

- 在法律允許的範圍內，審查數位鑑識報告，確認其準確性。
- 配合法律團隊，準備必要的法律文件和證據提交。
- 確保報告和提交的證據中不包含不相關或敏感的個人資料。

過去，數位鑑識大多仰賴人工作業及特定硬體設備，耗時且難以擴展處理大量數位證據

如今，該如何提升數位鑑識之效率及觸及更多潛在數位證據？

4

新興科技與數位鑑識

新興科技於數位鑑識各階段應用

- **人工智慧(AI)**：利用語音識別技術，AI可以將訪談的錄音自動轉錄為文字，節省手動轉錄的時間和勞力。

- **人工智慧 (AI) 和機器學習 (ML)**：自動化數據搜集，識別和標記關鍵數據。
- **物聯網 (IoT)**：搜集各種IoT設備的數據。
- **雲端服務**：提供安全的資料儲存和備份。

- **區塊鏈技術**：提供不可篡改的證據記錄。
- **雲端服務**：安全且易於存取的證據儲存。

- **人工智慧(AI) 和機器學習 (ML)**：自動化分析，識別異常行為和模式。
- **大數據分析技術**：從大量數據中提取有價值的訊息。
- **區塊鏈技術**：確保資料的完整性和不可篡改性。

- **人工智慧(AI)**：利用自然語言生成（NLG）技術，根據分析結果自動生成包含圖表之可視化鑑識報告。
- **虛擬現實 (VR) 和擴增實境 (AR)**：重建犯罪現場和模擬情境。

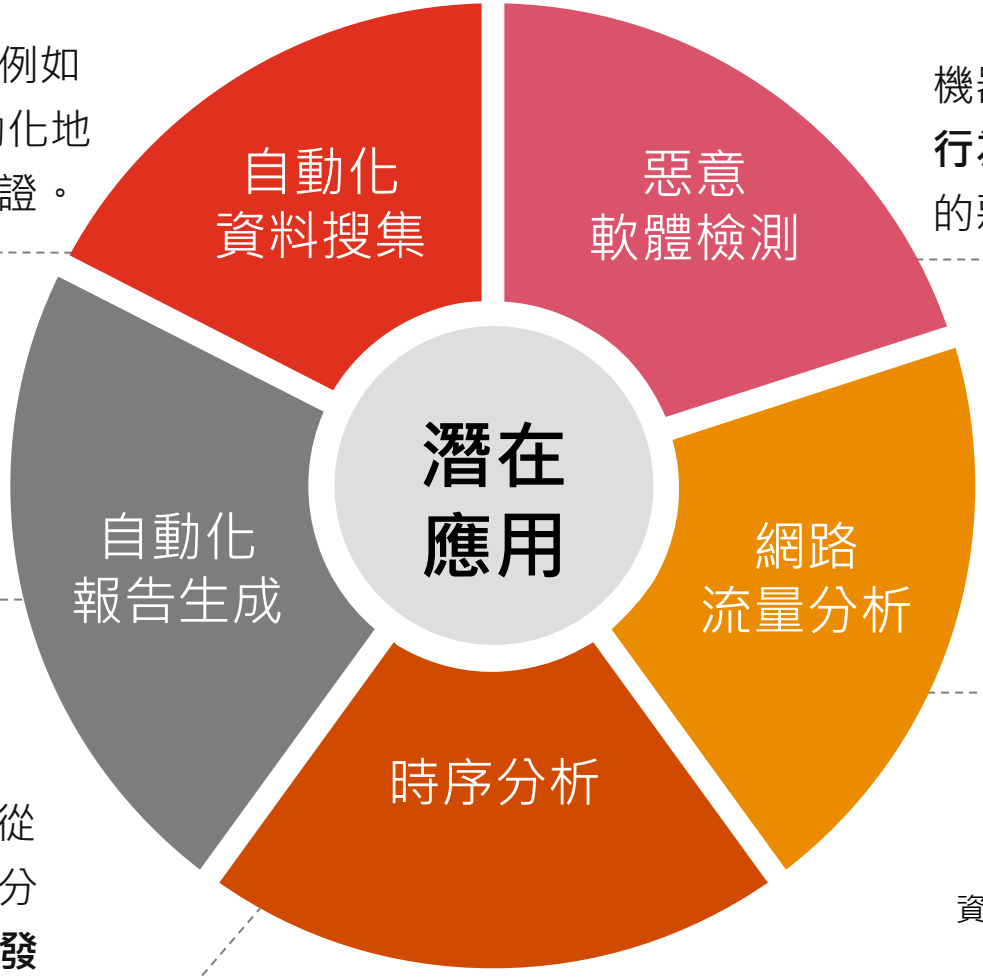
資料來源：Preservation Of Digital Forensic Evidence Using Blockchain Technology (2024)
Dark Reading (2023)
The Future of Digital Forensics: Trends and Technologies (2024)

人工智慧於數位鑑識潛在應用

數位鑑識往往需要**處理大量的資料**，例如硬碟、手機、網路流量。AI 可以自動化地從這些資料中提取有用的資訊進行蒐證。

利用自然語言生成（NLG）技術，AI可以根據分析結果**自動生成包含圖表之可視化鑑識報告**，提高效率與準確性，並同時減少人力錯誤。

AI技術協助構建事件發生的時間線，從而更好地理解事件的發展過程，通過分析不同事件之間的關聯性，**構建事件發生的時間線**。



機器學習算法可以快速**自動化分析軟體的行為模式，識別異常行為**，從而檢測潛在的惡意軟體。

分析網絡流量，以檢測和應對網絡攻擊，這在數位鑑識中也是一個重要的應用領域。**透過實時監控網絡流量，識別異常活動，從而及時發現潛在的網絡攻擊**。

資料來源：Dark Reading (2023)
RCS cybersecurity
oxygenforensics(2024)

於數位鑑識應用人工智慧之挑戰

1 誤報和偏見

人工智慧可能會產生誤報，或因訓練資料中的偏見而無法公平地分析數據。

2 依賴性

過度依賴人工智慧，可能會導致調查人員忽視他們自己的專業判斷和直覺。

3 法律挑戰

人工智慧計算出的證據可能在法律上面臨挑戰，特別是在計算的透明度和可解釋性。

資料來源：ACEDS (2024)

建議：基於人工智慧產製之數位鑑識結論，仍需要由調查員驗證。

對新興科技執行數位鑑識

社群媒體

利用社群媒體上的互動記錄，尋找潛在的犯罪證據或行為模式。

行動裝置/行動應用

分析其通訊紀錄、地理位置、應用程式、API等。

FIDO (Fast Identity Online)

分析FIDO 協議流量，確保內容沒有被篡改過。

物聯網（IoT）

分析IoT設備的通訊模式，確保設備未被攻擊或篡改。

雲端計算

分析雲端環境中的活動日誌，並查找異常行為。

大數據技術

使用資料分析技術分析數據，發現潛在異常模式與威脅

對新興科技執行數位鑑識 – 社群媒體

01
- 社群媒體帳號的公開資訊
- 私人訊息
- 使用者活動紀錄

02
利用社群媒體上的互動記錄、貼文內容、網路好友關係等，尋找潛在的犯罪證據或行為模式。

03
利用工具搜集網路社群媒體證據、調查犯罪活動並追蹤嫌疑犯，如：Maltego, Social-Engineer Toolkit 與 WebPreserver。

資料來源：ADF News (2023)
controlrisks (2022)

對新興科技執行數位鑑識 – 行動裝置

01
- 行動裝置的文件系統、通訊記錄、應用程式數據
- 應用程式的安裝檔(APK或IPA)、應用程式執行時的數據流量。

02
利用社群媒體上的互動記錄、貼文內容、網路好友關係等，尋找潛在的犯罪證據或行為模式。

03
- 分析來自不同行動裝置的資料，並支援多種裝置型號和作業系統，如：Cellebrite、XRY
- 用於逆向工程、惡意軟體分析，如：JEB、IDA Pro

資料來源： splunk (2024)
salvationdata (2024)

對新興科技執行數位鑑識 – FIDO (Fast Identity Online)

01

用戶身份驗證記錄、FIDO 認證設備、使用模式、失敗嘗試、密鑰資訊。

02

- 分析FIDO U2F或FIDO2/WebAuthn協議的流量，確保沒有被篡改。
- FIDO使用的公鑰加密技術，可以保護數據的完整性，這在數位鑑識中非常重要。確保數據未經篡改是電子證據有效性的關鍵。

03

- 需要使用專門分析FIDO協議的工具，這些工具可以解碼和分析FIDO的認證過程。
- 使用日誌分析工具：Splunk、ELK Stack (Elasticsearch, Logstash, Kibana)，分析對註冊和身分驗證操作記錄。

資料來源： cybersecurityasia (2024)

對新興科技執行數位鑑識 – 物聯網（IoT）

01 透過擷取IoT設備的韌體、日誌、使用者行為數據、位置數據、環境數據、圖片和視頻數據、感應器數據和網路流量。

02 分析IoT設備的通訊模式、韌體更新歷史，確保設備未被攻擊或篡改。

03 IoT設備通常會記錄時間戳，這些時間戳可以用來重建事件的時間線。此外，可使用IoT設備專用工具，解碼各種IoT協議，如：MQTT、CoAP等。

資料來源： briskinfosec (2024)

對新興科技執行數位鑑識 – 雲端計算

01 搜集雲端伺服器上的日誌、存儲數據、虛擬機快照等。

02 分析雲端環境中的活動日誌、文件存取記錄，並查找異常行為。

03 透過專門的雲端鑑識工具，如AWS CloudTrail、Azure Security Center等，可用於監控和檢測潛在的安全事件、搜集證據並分析，以進行進一步調查。

資料來源：eccouncil (2022)

advantage-tech (2024)

對新興科技執行數位鑑識 – 大數據技術

01 可搜集分散在多個不同來源的大規模資料集。

02 使用資料分析技術與機器學習模型，進行數據分析，從數據中發現潛在異常模式與威脅。

03 透過大數據分析平台，如：Hadoop、Spark、 SAS 視覺化分析等，可以有效提升數據處理和分析的效率和準確性，更快速地找到關鍵證據。

資料來源： largitdata（2024）

數位鑑識於新興科技環境中，需結合各種專業工具與方法，針對不同領域的需求，進行量身定制的分析。

每個領域都有其獨特的挑戰與解決方式，鑑識人員需要具備相關領域知識與技能，才能有效進行數位鑑識活動。

Thank you

pwc.tw