Module – 01
當今世界的電腦鑑識

電腦鑑識在鑑識科學中，就是一門在電腦中找出證據的學科

只要有人存在，就會有犯罪，當今日數位化程度越來越高的情況下（現今生活都與資訊科技綁在一起了），在電腦世界中犯罪的數量就會有所提升

傳統的資安愛怎麼做就怎麼做，但會談到鑑識，就表示要進入司法程序，一切就要合乎法律程序沒辦法隨便做，法律從來就不是追求正義、對錯，法律追求的是，程序的完整，攻防雙方誰的程序越完備誰就獲勝

但有些時候電腦鑑識是幫助危機處理團隊找出一件危機事件發生的真正原因

鑑識科學的模範生 – 日本
日本檢察官起訴率低、定罪率高，因為日本人對於蒐證的謹慎精神
強調完整性，所以常常鐵證如山

LO # 01
了解電腦鑑識的基本知識

電腦鑑識是鑑識科學的一部份，所以法規、流程一樣，技術不一樣

一切由程序開始，這個程序會參照一套方法論和技術（設備、工具、IT...等等），來幫忙辨識、收集、保存、擷取、解釋、紀錄（從頭到尾）和呈現證據

簡單來說，鑑識科學 > 用科學找出證據（要經得起考驗） > 反應事實（是否有發生這件事情，事實不等於真相） > 一連串真相（是否真的是那樣）

普通法的三個精神（保護法律上的弱者，即被告）

- 無罪推定論 > 在還沒找出證據之前，不可以說有罪
- 不溯及既往 > 除非是新發現的證據，否則不可後補證據
- 不能誘導犯罪

要從攻擊者的軌跡中找證據，證據必須要有完整性（Integrity），證據要經得起考驗

為何會需要電腦鑑識?

- 以forensically sound manner的方式取證 > 重複做結果一致，確保可以驗證證據的正確性

- 保護組織在未來免受類似事件影響和最小化有形、無形資產的損失

- 幫助起訴危機事件的肇事者

何時會需要電腦鑑識?

- 違反合約的事情發生、發生版權和知識產權盜竊/濫用、有員工糾紛或對公司不滿的員工、公司資產被損壞的情況下

LO # 02
了解網絡犯罪及其調查程序

網路犯罪的種類

網絡犯罪的定義為，涉及計算設備、網路及系統或應用程式...等任何非法行為來謀取特定利義或單純不爽

可以大概分為兩類

- Internal/Insider Attack（內部攻擊，內賊）
- External Attack（外部攻擊），又可以分成幾類
  - 軍事（網路戰）
  - 犯罪（錢）
  - 激進主義份子（不爽）

幾個網路犯罪種類的例子（舉不完）

- **Espionage** – 間諜
- **Theft of Intellectual Property** - 版權和知識產權的盜竊（通常為內賊）
- **Manipulation of Data** – 資料的操縱
- **Trojans Horse Attack** - 特洛伊木馬攻擊
- **Structured Query Language Attack** – 結構化查詢語言攻擊（SQL Injection）
- **Brute-force Attack** – 暴力攻擊（打驗證機制，想做到非經授權的存取）
- **Phishing/Spoofing** – 網路釣魚/欺騙
- **Privilege Escalation Attacks** - 提權攻擊（水平、垂直）
- **Denial of Service Attack** - 阻斷服務攻擊
- **Cyber Defamation** – 網絡誹謗
- **Cyberterrorism** - 恐怖份子
- **Cyberwarfare** – 網路戰

網路犯罪的調查，不同的種類，程序有些不同

- Civil（民事，有人提告才成案）
- Criminal（刑事，相關單位會主動調查）
- Administrative（行政、內部單位）
  依照美國的法律，行政單位要符合non-criminal in nature（內部不能有刑事案件），如果發生，就一定要對外呈報給執法單位

LO # 03
了解數位證據

數位證據是以數位形式儲存或傳輸的任何有證明（法律）價值的資訊

數位資訊可以在許多地方發現
e.g. 數位儲存媒體、裝置或網路流量，甚至是從鑑識備份中採證時...等

數位證據相對傳統證據是脆弱的、有時效性的

根據羅卡交換定律（Locard's Exchange Principle），行為人（犯罪嫌疑者）必然會帶走一些東西，亦會留下一些東西，現場必會留下微量跡證，所以我們相信證據

萬物皆可鑑，與犯罪有關皆可

數位證據的種類

- Volatile Data，可揮發性資料，只要設備斷電後就會失去資料
  e.g. 記憶體

- Non-volatile Data，不可揮發性資料，存放在輔助儲存裝置，沒有意外會永久留著
  e.g. 硬碟

數位證據的角色，講不完且有點多餘，只要可以用來做數位犯罪都是，而且重點不是證據而是證明

法院三證 > 人證、物證、心證，後者會受到前兩者的影響

潛在證據的來源

- User-Created Files
  e.g. 通訊錄、資料庫檔案、媒體設備、文件...等
- User-Protected Files，每個加密的背後都一定有它的原理
  e.g. zip是軍規等級的加密，幾乎不可能破解，90%以上都是繞過
- Computer-Created Files，最具代表性的為Log files
- 一些其他軟、硬體
  e.g. 硬碟、記憶卡、Dongle（目前以軟體出現較多）、掃描機、網路卡、伺服器、印表機、IoT、穿戴裝置、GPS...等

不同的國家有不同的法律

使用者建立的檔案有些國家認為是相對直接的證據，有些國家認為不會單獨成證，需要有別的證據佐證

電腦建立的檔案有些國家認為是間接證據（傳聞證據），與行為沒有直接的關係，有些國家認為是原則上成證，但還是可以懷疑真實性

證據在法院上要有用要符合

- 證據的三個要求
  - ◎ Authentic > 真實地確定跟案子有關
  - ◎ Reliable / Accurate > 不可被懷疑，可以被驗證
  - ◎ Complete > 可以完整證明一個行為或無行為

- 證據的兩個應用、結果
  - ◎ Admissible > 與Authentic的不同在於法院承認
  - ◎ Understandable / Believable > 清楚明確讓法官理解

最好的證據

符合當地法規就是最好的證據，證據可被當地法院接受

在美國必須出示原始證據，副本有條件被接受

證據要符合程序要求

證據力 > 是否成為證據
證據證明力 > 是否在法院上有幫助

接下來都是為了符合法規的要求而制定的

- Federal Rules of Evidence 美國聯邦證據規則
  - ◎ Rule 102: Purpose > 公平地管理每一道程序，消除不合理的費用和延誤，促進證據法的發展，以達到查明真相和保證公正裁決的目的
  - ◎ Rule 103: Rulings on Evidence > 證據裁決
  - ◎ Rule 104: Preliminary Questions > 初步問題，目擊證人的訪談，不能強迫，所有的回答都有一定的疑慮，但以人性的角度來看第一時間的可信度較高
  - ◎ Rule 105: Limited Admissibility > 有限的可接受性
  - ◎ Rule 801: Hearsay Rule > 傳聞證據的規則（非直接的證據）

Federal Rules of Evidence 美國聯邦證據規則（續）

◎ Rule 801: Statements That Are Not Hearsay > 筆錄並非傳聞證據，傳聞證據達成某些條件就會變成筆錄

以下為傳聞證據的例外
◎ Rule 803: Hearsay Exceptions – Availability of Declarant Immaterial
聲明人無關緊要的可用性

◎ Rule 804: Hearsay Exceptions; Declarant Unavailable
聲明人不可用

以下為文字、錄音和照片的內容定義
◎ Rule 1001: Definitions
注意原始與副本的差異

Scientific Working Group on Digital Evidence（SWGDE） 美國聯邦警察數位鑑識的流程，強調證據的準確性和可靠性

The Association of Chief Police Officers（ACPO） Principles of Digital Evidence 英國警長辦公室數位鑑識的流程

- Principle 1: 持證物單位不可改證物
- Principle 2: 要看原始證物，一定要有專業能力在法院上和法官說明對證據做了什麼
- Principle 3: 稽核紀錄，證據經得起考驗（系統化、可重複、可再現、連續性、有效性）
- Principle 4: 調查員對上面三項負責

LO # 04

了解鑑識準備就緒，危機處理團隊和安全營運中心在電腦鑑識中的角色

鑑識準備就緒

組織在有限的時間內以最低的調查成本優化使用數位證據的能力

偏向組織內部調查，因為沒有身份（為了上法院而做的鑑識，必須要為第三方公正單位，有合法的授權身份），沒有要保存證據

鑑識準備就緒與商業持續營運之間的關係

鑑識準備就緒以快速且輕易的識別受影響的元件，然後取代他讓服務繼續運作來幫助維持商業營運（這麼做本身就是在破壞證據，比較像是危機處理團隊的任務，管理層普遍不太在乎數位鑑識，只想要把事情盡快解決，然後給個交代）

鑑識準備就緒的計畫

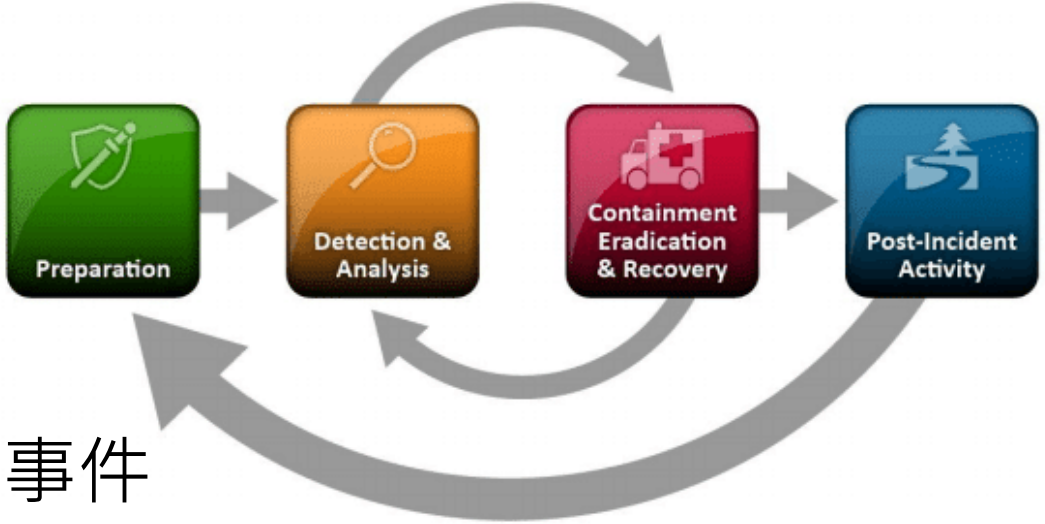
其實就是導入數位鑑識的流程、技術、方法...等，只差保存證據

危機處理團隊（Incident Response Team,IRT）

最大程度地減少損害並減少恢復的時間和成本，透過數位鑑識快速辨識問題，但大部份企業遇到事故只想要回到正常，不在乎背後的真相

沒辦法快速解決就先隔離，還是找不到問題就只能直接殺掉（以IRT的角度，對數位鑑識團隊而言，是破壞證據）

NIST制定的危機處理流程



Step 1 > 所有的一切都從準備開始

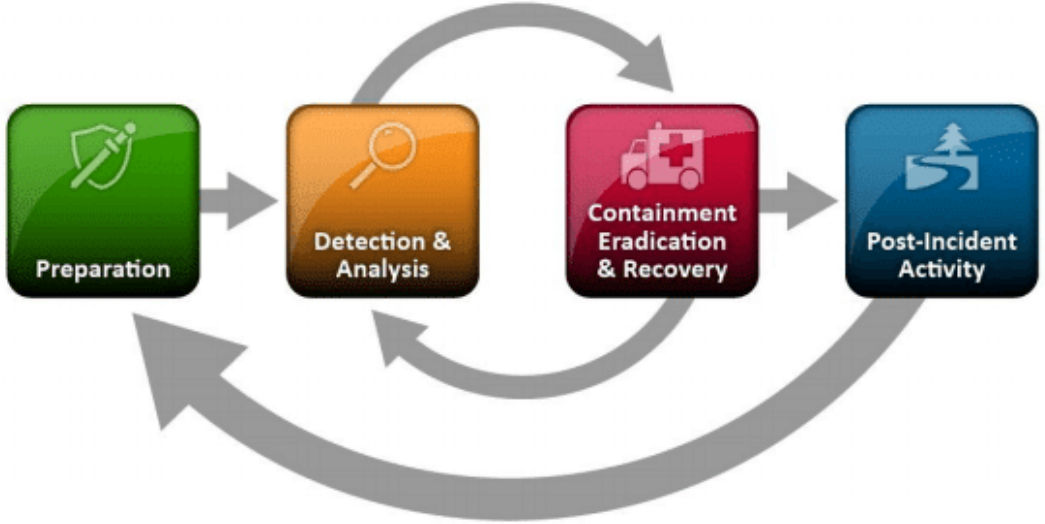
Step 2 > 安全營運團隊做監控，發現有危機事件通報IRT

Step 3 > IRT判斷是否真的為危機事件、做檢傷分類，依照嚴重性排出優先順序

Step 4 > 通知管理部門和其他相關部門（法定、行政通報以獲得授權，因為Step 5可能會影響服務）

Step 5 > 隔離（封鎖），1. 避免災情變大 2. 保留證據

NIST制定的危機處理流程（續）



Step 6 > 鑑識團隊的進入

Step 7 > 解決問題

Step 8 > 恢復

Step 9 > 事後活動，做紀錄、評估事件造成的衝擊、重新檢視和修改政策、結案、是否做揭露?

安全營運團隊（Security Operations Center,SOC）
專門做24小時不間斷的資安監控

Security Prevention 預警（ISAC,威脅情資）
Detection 監控（SOC）
Correction 應變（CERT,IRT）

LO # 05
確認鑑識調查員的角色和責任

以forensically sound manner收集證據

是什麼造就了一個好的電腦鑑識調查員?

訪談技巧、研究技巧、測試的準確度、耐心和意願、撰寫技巧、分析技巧、溝通技巧、熟悉鑑識技術、熟悉不同電腦平台、熟悉不同的技術、軟硬體、誠實、道德感、 遵紀守法、擁有法律的知識、情緒管理、涉及刑事和民事案件的多學科專業知識...等

總而言之，是個充滿挑戰的工作，但哪個工作不具挑戰性呢?

道德規範

在調查過程中，可能會看到一些不該看的，要善盡自己的社會責任
e.g. 營業秘密、智慧財產、隱私...等

要清楚知道什麼該做、什麼不該做

電腦鑑識資源

- Computer Technology Investigators Network
  https://www.ctin.org

- High Technology Crime Investigators Association
  https://www.htcia.org

- Forensic Focus
  https://www.forensicfocus.com/

電腦鑑識資源（續）

- Digital Evidence and Forensics
  https://nij.ojp.gov/digital-evidence-and-forensics
- ForensicsWiki
  https://forensicswiki.xyz/page/Main_Page
- 13Cloud
  https://www.youtube.com/user/davisrichardg?app=desktop
- DFIR Training
  https://www.dfir.training/
- Invoke-IR
  http://www.invoke-ir.com/

電腦鑑識資源（續）

- Forensic Sciences
  https://nij.ojp.gov/topics/forensics

- Topical Publication Collections: Digital Forensics
  https://nij.ojp.gov/taxonomy/term/9131?tags=Forensics%2CElectronic%20Crime%20-%20Cybercrime

- Topical Publication Collections: Computer Forensic Tool Testing
  https://nij.ojp.gov/library/publications/list?tags=Electronic%20Crime%20-%20Cybercrime

- SANS Computer Forensics
  https://www.sans.org/digital-forensics-incident-response/

電腦鑑識資源（續）

- DFRWS
  https://dfrws.org/
- The Scientific Working Group on Digital Evidence
  https://www.swgde.org/
- Computer Forensics World
  https://www.computerforensicsworld.com/
- Invisible Man
  http://jay-fva.blogspot.com/
- Department of Defense Cyber Crime Center
  https://www.dc3.mil/

電腦鑑識資源（續）

- JUSTNET -- Computer/Cybercrime (Digital Evidence and Forensics) https://cjtec.org/
- National Institute of Standards and Technology Computer Forensics Tool Testing (CFTT) Project https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt
- National Software Reference Library NSRL) Project https://www.nist.gov/itl/ssd/software-quality-group/national-software-reference-library-nsrl
- Computer Forensic Reference Data Sets (CFReDS) Project https://cfreds.nist.gov/

電腦鑑識資源（續）

- Top 20 Free Digital Forensic Investigation Tools for SysAdmins https://techtalk.gfi.com/top-20-free-digital-forensic-investigation-tools-for-sysadmins/

LO # 06
了解調查網路犯罪會面臨的挑戰

網絡犯罪對調查人員構成的挑戰

可以先大致分為三個部份

- General > IT技術
- Legal > 法律
- Privacy > 隱私

導致IT技術受到挑戰的因素為

- Speed > 網絡打破了時間和空間的限制
- Anonymity > 查IP不一定準
- Volatile nature of evidence > e.g. 記憶體一斷電後就會失去資料、資料隨著時間的改變而改變
- Evidence Size and Complexity > 檔案太大會浪費時間，檔案格式複雜鑑識工具不一定看得懂
- Anti-Digital Forensics（ADF） > 倒是還好，比較好遇到頂尖的駭客
- Global origin and difference in laws > 各國的法律不同
- Limited legal understanding > 對於法律的了解

電腦鑑識: 隱私問題

The Fourth Amendment of the U.S. Constitution 美國憲法第四修正案

強調 Reasonable Expectation of Privacy

人民對於自己的隱私有合理的期待，不得隨意扣押、搜索，除非有搜索票（search warrant）

沒有搜索票而搜到的證據，是非法搜索，不可成證據

私人入侵不算在內

LO # 07
了解電腦鑑識的法律合規性

- Gramm-Leach-Bliley Act（GLBA） 金融現代化法案，要求所有金融機構向客戶公開隱私權保護政策和措施，而且每年要對這些保密措施進行一次評估，以防客戶資料被竊取

- Federal Information Security Modernization Act of 2014（FISMA） 聯邦資訊安全現代化法，授權給美國國土安全部對於各公務機關進行監督與管理、管制重大資安事件之通報與受到侵害時之處置

- Health Insurance Portability and Accountability Act（HIPAA） 醫療保險攜帶和責任法案，要求醫療單位採用標準的資料格式與和傳輸方式，讓病患的電子醫療記錄能夠跟原先的紙張記錄一樣安全，甚至更好

- Payment Card Industry Data Security Standard（PCI DSS） 支付卡產業資料安全標準，是支付卡產業安全標準協會所制定的標準，是基於保障持卡人資料安全的全球統一規範。凡儲存、處理或傳輸 Visa 持卡人資料的業者，包括金融機構、特約商店與服務提供者都必須遵守

- Electronic Communications Privacy Act（ECPA） 美國電子通訊隱私法，規定了人們在使用電話、電腦、手機或傳真...等其他電子通信時應享有該有的隱私權

- General Data Protection Regulation（GDPR） 一般資料保護規定，歐盟公民享有資料刪除、更改、轉移的權利，且企業需保護用戶個資

- Data Protection Act 2018 資料保護法，參照GDPR法令，讓英國與歐盟之間的資料隱私法令保持一致

- Sarbanes-Oxley Act of 2002（SOX） 原名為2002年上市公司會計改革和投資者保護法案，但目前都稱為沙賓法案，明定企業必須以文件（至少保存5年）記錄各項財務政策與流程、改善財務報告權責制度、提高製作財務報告效率