數位科技安全與鑑識

-

序

數位科技安全與鑑識(Forensics and Security in Computer Systems) —高科技犯罪預防與數位證據偵蒐。本書—**數位科技安全與鑑識:**為作者所主持的資訊密碼暨建構實驗室-數位鑑識研究工作室(**I**nformation **C**ryptology and **C**onstruction **L**ab.-**F**orensic **R**esearch devel**O**pment task force **G**roup, **ICCL-FROG**)的第二本有關在高科技犯罪趨勢裡,如何提供技術與工具操作使用的因應之道與專業叢書。

本書除延續數位鑑識研究第一本書(**電腦鑑識與數位證據，ISBN：CNE0007，博碩文化**)的電腦犯罪、網路安全、鑑識理論與數位證據偵蒐程序之外，更進一步以實務的觀念加入在各種可能情境下，如何於不同的作業系統平台(Windows/Unix/Linux),探討電腦高科技犯罪的趨勢與偵防之道。本書—**數位科技安全與鑑識**，全文包含十二章，內容如下：

- **第一章：數位證據與數位鑑識**
- **第二章：電腦與網路犯罪**

閱讀此兩章，可對證據於電腦犯罪的判定能有概觀的了解。並尋求合法的追蹤與偵蒐途徑(即鑑識的精義)，使得呈現的數位證據力值得採信。

- **第三章：偽裝與鑑識**
- **第四章：密碼學與資訊安全**
- **第五章：網路安全機制**

此三章將鑑識與資訊安全的關係加以整理與闡述。數位鑑識的學習，不只是概念與操作的了解，也該能具備深厚紮實安全理論基礎。多能體會密碼安全機制的原理，可加深鑑識工作的研究與推動。

- **第六章：網路資料危機與鑑識**

本章裡，介紹在許多電腦犯案後，將會留下的證據在網路系統中。就鑑識工作的使用，將可助爾後的犯罪事件調查，保障網路使用者的隱私權益與爭議性犯罪身份的認定。

- **第七章：Windows 系統主機偵查**
- **第八章：Unix 系統主機偵查**
- **第九章：Windows 工具軟體**
- **第十章：Linux 系統鑑識工具**

上述四章，乃基於不同作業系統平台所需要的鑑識工作之進行，所撰寫的偵查／工具的程序／操作。期能因應在重要系統的資安入侵事件發生後，能在第一時間紀錄入侵點，以保留最後的數位證據。

- **第十一章：遠端數位鑑識與數位證據蒐集**

本章介紹網路環境的適度佈施／設置，可使得數位鑑識工作得以動態進行。此章提供遠端鑑識中心的建立雛形。藉由遠端鑑識中心的建置可突破時空受限的鑑識作業，強化高科技犯罪的蔓延。

- **第十二章：科技犯罪與鑑識工作**

本章討論因應高科技犯罪的防範措施與數位證據偵蒐的基本作業程序。並以現代通訊科技產品 PDA 為例，說明如何結合鑑識工作。使得科技的使用不只便利，而且可以適時地在犯罪入侵行為發生時掌握線索、還原真相。

本書章節的編撰，是結合中央警察大學數位鑑識研究工作室(ICCL)與東海大學資訊工程系資訊安全實驗室(ISLAB)的研究群之合作結果。在群策群力、積極規劃與共同合作下終得呈現給讀者。要感謝中央警察大學資訊密碼暨建構實驗室-數位鑑識研究工作室的伙伴/研究人員陳晉煒、吳晉緯、張瑋志、張晃瑜、江文雅與劉心玫的全力參與，以及東海大學資訊工程系資訊安全實驗室的楊宗哲、鄭懋樺、鄭掄元、李衍緯、林育瑩等同學得協助，使得本書得以順利附梓。另外，柯宏叡的網路安全與鑑識技術的實驗編入，適時地對本書的發揮事半功倍的效果。藉此對 ICCL 及 ISLAB 所有人員的努力表達深摯的感謝。

最後我們以網站裡(http://hera.im.cpu.edu.tw)對生活的期許與讀者分享：

「學習 as well as 忘」;「研究 as well as 痴」;

「做事 as well as 心」;「生活 as well as 混」;

「情感 as well as 容」;「持處 as well as 后」;

「成就 as well as 慟」。

並盼此書得以為科技發展/研究之文獻做粗淺整理，以為此相關領域的參酌。

ICCL –FROG
http://hera.im.cpu.edu.tw

ISLAB
http://islab.csie.thu.edu.tw

王旭正、林祝興 謹識

Mid-Jan. 2009

Visit at **S**ung**k**yun**k**wan **U**niversity (成均館大學, SKKU)

Korea