Jan. 2007

–State of the Art –

Computer Forensics and Digital Evidence

Anti-cyber-crime with Security Tactics, Computer Crime Prevention, Authentication and Re-construction of Venue

FORWORDS

The present book entitled as **Computer Forensics and Digital Evidence- State of the Art in the Anti-cyber-crime with Security Tactics, Computer crime Prevention and Re-construction of Venue** provides an introduction to the concepts regarding the theory and practice of information security/ internet security and technological crimes/ forensics and evidence, which are very important in the 21st century. With the coming of the internet era, it is no longer about traditional criminal traces at the crime scene, and traditional equipment is no longer sufficient for the forensic staff to collect evidence at the crime scene. In a high-tech modern society, for similar cases, there are additional related objects of evidence such as hardware and software and digital electronic equipment: monitors, computers, PDA, flash devices, email, MSN, Skype etc. When dealing with these novel computer crime cases, the traditional forensics staff is unable to comprehensively collect evidence, and would require the support of computer forensics technology. Consequently, a scientific approach towards the handling of cases has become an indispensable and crucial factor in investigations in the criminal justice process in various countries.

In the present book **Computer Forensics and Digital Evidence**, the following topics are introduced and discussed:

- **The changes over the course of time**
- **Cyber crimes and investigation of cyber crimes**
- **Digital evidence on the Internet**
- **Digital forensics**
- **Establishing the environment for digital forensics**
- **Technologies of concealing information**
- **Information security**

I. **The changes over the course of time**: Introduces the evolution of concepts regarding computers, the internet, digital evidence and digital forensics, such that a reader who does not come from the information technology industry would be able to grasp the theoretical foundations for the present book, and explore the ideas surrounding cyber crimes and digital evidence that are hidden within the world of the internet.

II. **Cyber crimes and investigation of cyber crimes**: Carries out an in-depth and practical discussion on the issues of information security risks/ cases/ applications that are confronted by an information technology society, e.g. cyber crime: fraud, gambling, money laundering and other information security issues in the new wave of cyber crimes. By analyzing the various current trends in cyber crimes and introducing the technologies for investigation of cyber crimes, the book seeks to provide a timely response to the various criminal acts that are growing in their online presence and technological scope.

III. **Digital evidence on the internet**: The contents broadly discuss the potential

existence of various types of digital evidence in cyber crimes, including the contents of information that are stored in computer systems, computer peripheral equipment for the internet or other electronic installations and storage media. It also introduces the technology and tools for the collection of digital evidence, as well as the potential problems and bottlenecks that may be encountered in the process of collecting information. It serves not only as a point of reference for investigators when they are handling cases, but also enables the general public and corporations to be aware of the real-time evidence for the crime that may be preserved when they encounter losses on the internet, so that such evidence may become relevant and admissible evidence to be used in the courts to protect the rights and interests of the individual or the corporation.

IV. **Digital forensics**: The present section broadly divides the technologies for digital forensics into two units for exploration: “computer forensics” and “online forensics”. In an era where the recognition of information security risks is increasing, in order for digital evidence to have probative value before the judge in the court in the future, it is necessary to establish a standardized evidence authentication procedure, and to merge it with the technologies developed in information security, so that the digital forensics activities would be complaint with the law, thereby increasing the admissibility and probative value of digital evidence. Digital forensics technology has become an interesting new academic domain that is worth exploring further.

V. **Establishing the environment for digital forensics**: A further discussion is carried out on the growing trend of high technology crime in Taiwan and the national forensics laboratories that are being established internationally. It further discusses the need to establish the environment for digital forensics in Taiwan in the future, and considers the various technologies that need to be cultivated, the

purchase and research and development of tools and equipment, and the nurturing of forensics talents. It also proposes a concrete structure and organization for a digital forensics laboratory, in order to carry out the planning and preparation to create an environment for implementing digital forensics and analysis of evidence, so as to meet the need of the times.

VI. **Technologies of information hiding**: The present topic is directed at introducing the technologies of information hiding within the field of digital forensics technology, including digital watermarking, steganography and visual cryptography, thereby enabling the reader to appreciate the process of analyzing digital evidence in a more concrete manner and to see the areas of difficulties involved.

VII. **Information security**: After introducing the various novel cyber crime methods, the book finally cautions the corporations to establish a comprehensive online security system, carry out effective risk management internally and externally, and set up a standard operating procedure for dealing with the occurrence of information security incidents. It is also hoped that general internet users would be able to rely on the present section to enable themselves to set up the basic preventive measures, in order to avoid becoming the next victim of cyber crime.

In the present book, the Chapter one entitled as In-progress Computers and Communications on the Internet results in the introductory topic on the **"Changes over the Course of Time"**, and concludes with the Chapter twelve entitled as Network Security under the topic on **"Information Security"**. The contents deal with the earliest notions of internet security to the most recent trends on cyber crimes on the internet, as well as the related issues such as the collection of digital evidence and computer forensics technologies. With active planning and cooperation within the entire team, the farsighted

project was finally presented as a comprehensive work. Although there are some twists and turns in the process, it has also shown forth the path of flexible application of change management. Y.**H**. CHANG and Patric **U**.C. KU, my partners/ researchers at Information Cryptology & Construction Lab. (ICCL) probably share the above sentiments the most. Following the comprehensive preparations, things finally turned out well, and the project was completed smoothly. The elaborate experiments of my student H.J. **K**E on forensic technologies were compiled and included into the book, thereby enabling us to achieve the maximum results. Therefore, putting "**K-U-H**" on the cover page of the book is a way of expressing the heartfelt thanks and appreciation of the hard work of the staff at ICCL.

Family is absolutely the most important pillar of support behind hard work, in particular Rebecca, G.Y., G.R., my wife, and my children – my love is with all of them. Finally, I would like to share with readers my expectations of ICCL/Life:

*"Think **why** you are here".*

*"Find **where** you are interested in here".*

*"Marry **whom** you look for here".*

*"Get **what** you want to have here".*

*"Honor here **when** you own something special with knowledge".*

I hope this book can be used as a preliminary attempt for the literature of technology development/research, and a reference for related fields.

ICCL –FROG
(Information Cryptology and Construction Lab.-
Forensic Research develOpment task force Group)
http://hera.im.cpu.edu.tw
http://163.25.10.166

Shiuh-Jeng Wang
Late Jan. 2007
Visit at CMU, Pittaburgh
Pennslyvania, USA

電腦鑑識與數位證據

---資安技術、科技犯罪的預防、鑑定與現場重建----

序

本書**電腦鑑識與數位證據-資安技術、科技犯罪的預防、鑑定與現場重建**

(Computer Forensics and Digital Evidence: State of the Art in the Anti-cyber-crime with Security Tactics、 Computer Crime Prevention、Authentication and Re-construction of Venue)為現代二十一世紀重要的資訊安全/網際網路安全與科技犯罪/鑑識與證據的相關理論與實務上所涉及的概念作介紹。網路時代的來臨，刑事案件現場不再只是傳統犯罪跡證,鑑識人員透過傳統的設備工具已不足以採集犯罪現場的證據。高科技的現代化社會，同樣的案件，犯罪現場多了許多軟硬體及數位電子設備等相關證物，如：監視器、電腦、PDA、隨身碟(Flash Device)、EMAIL、MSN、Skype 等。面對如此新興的電腦犯罪案件，傳統的鑑識人員已無法完整的採證、因此需要電腦鑑識技術的輔助，科學化的辦案已成為各國刑事司法偵審中不可或缺的關鍵因素。

在本書**電腦鑑識與數位證據**中，相關的議題介紹/討論如下:

- **時代的變遷**
- **網路犯罪與網路犯罪偵查**
- **網路數位證據**
- **數位鑑識**
- **數位鑑識環境建置**
- **資訊隱藏技術**
- **資訊安全**

I. **時代的變遷**: 介紹電子計算機、網際網路、數位證據與數位鑑識演進之概念，使得非資訊專業領域的讀者亦能具備本書相關理論基礎，一同來窺探這隱藏著許多網路犯罪與數位證據在其中的網路世界。

II. **網路犯罪與網路犯罪偵查**: 為資訊科技社會所得面臨的資訊安全危機/事件/應用問題，諸如 CYBER-CRIME：詐欺/賭博/洗錢/…等新興網路犯罪的資訊安全議題，進行深入/實務的討論。藉由分析現今各類網路犯罪趨勢與介紹網路犯罪偵查技術，為求能夠及時因應泛網路化且技術日新月異的各類犯罪行為。

III. **網路數位證據**: 內容泛談在各種網路犯罪中各種數位證據可能的所在，包括存在於電腦系統、網路設備電腦週邊設備或其它電子裝置、存儲媒體中的資訊內容。並介紹數位證據蒐集的技術與工具，以及在蒐集數位證據過程中可能遭遇的困難與瓶頸，提供偵查人員辦案的參考，亦能提供一般大眾或企業於網路上遭受損失時，知道可以保存哪些即時的犯罪證據，將來可作為有力的呈堂證供以保護個人或公司的權益。

IV. **數位鑑識**: 此部分將數位鑑識技術大致分成「電腦鑑識」與「網路鑑識」二單元來探討。在資安危機意識逐漸高漲的時代，為了將來數位證據能在法庭上受到法官的採信，如何建立一套標準的證據鑑定程序，並與資訊安全所發展的技術結合，使一切數位鑑識行為合乎法律要求，提高數位證據的證據力與證明力,數位鑑識技術儼然已成為一門有趣且值得深入探究的新領域學問。

V. **數位鑑識環境建置**: 進一步討論了台灣地區高科技犯罪亦日益增加的趨勢與國際上已紛紛建立國家級鑑識實驗室，探討台灣未來建置數位鑑識環境的必要性，並考量其所需具備的各種技術培養、設備工具的採購研發、與鑑識人才的培訓等，提出一個具體的數位鑑識實驗室架構與組織，為實施數位鑑識與證據分析的完善環境做規畫與準備，以符合時代的需求。

VI. **資訊隱藏技術**: 本議題針對數位鑑識技術中的資訊隱藏技術部分作深入介

紹，包括數位浮水印、偽裝學與視覺密碼，使讀者能更為具體感受分析數位證據的過程與其困難的地方。

VII. **資訊安全**: 在介紹了那麼多的新興網路犯罪手法後，最後提醒企業建立一個完善的網路安全機制，做好內部及外部的風險管理，並建立資安事件發生之標準處理流程；也希望一般網路使用者能藉由本章節建構起自己基本的防護能力，以避免自己成為下一個網路上的受害者。

本書，由第一章裡網路的演進勾勒出 **“時代的變遷”** 的議題，並結束於**第“資訊安全”**議題下的網路全機制。由最原始的網際網路安全概念直至近來 Internet 上最新網路犯罪趨勢、以及與之因應之數位證據採集與電腦鑑識技術皆囊括於其中。一件具前瞻性的工程在群策群力的積極規劃與帷幄下終得以決勝於完整一面的呈現。過程雖有些曲折，但亦突顯了「**窮**」、「**變**」、「**通**」的靈活運用之道。此番心情的雜陳/歷練，Information Cryptology & Construction Lab.（ICCL，資訊密碼暨建構實驗室)的伙伴/研究人員之一的張躍翰與古永昌或許最有滋味上心頭。最後亦在「萬事全，東風起」的催波助瀾下，工程計畫得以順利附梓，我的學生柯宏叡的鑑識技術實驗編入，適時地對本書的發揮事半功倍的效果。藉此，將書之編撰以「柯永翰」列名於書封面頁，是對 ICCL 所有人員努力下真實深刻的感謝與感動。

努力的背後，Family 絕對是最重要的支柱，In Particular for **Rebecca/G.Y./G.R.**， my wife, my kids, my loves with them。 最後吾人以經常對 ICCL/生活的期許(禪語)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」。

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

(Information Cryptology and Construction Lab.-

Forensic Research develOpment task force Group)

http://hera.im.cpu.edu.tw

http://163.25.10.166

王旭正

Late Jan. 2007

Visit at Carnegie Mellon University (CMU)

Pittsburgh, Pennsylvania, USA