數位 數位
留下? - E
證明 ? - F
當有線索的時候再去追 - Forensics

DOP Shiuh-Jeng **WANG** /王旭正
with partner-張晃瑜

- 中央警察大學 資訊管理系
- 中華民國資訊安全學會 (www.ccisa.org.tw, 理事 (2000-2012)
- 中華民國資訊安全學會 副理事長 (www.ccisa.org.tw, 2012-)
- Visiting Scholars at FSU and UF in USA, 2002, 2004, 2010.
- Academic tour for International Project Inspection at CMU in USA, 2007
- Columnists of Domestic Information-tech Magazines, http://www.netadmin.com.tw/ 網路通訊/iThome/網管人雜誌, 2002-2006, 2007-至今
- Director of ICCL, http://hera.im.cpu.edu.tw (Information Cryptology and Construction Lab.)
- sjwang@mail.cpu.edu.tw, http://www.wretch.cc/blog/icclsjwang

Outline

- 數位證據
- 數位鑑識之概念
- 數位證據的處理程序
- 數位鑑識工具
- 國外相關規範介紹
- 鑑識與反鑑識
- 案例探討
- 鑑識工具實作

數位證據

- 數位證據(Digital Evidence) 又稱為電子證據(Electronic Evidence)，數位證據與傳統證據不同之處，在於數位證據是以數位的型態儲存或傳輸，它是可以在法庭成為證據的數位/電子資訊。

數位證據

- 特性：

1. 難蒐集
2. 無法直接理解
3. 易竄改與刪除
4. 難證實完整性
5. 難建立連結關係

數位鑑識之概念

- 數位鑑識為一種運用科學的技術與方法，對數位證物實施蒐集、分析、鑑定與保存等作為。
- 換言之，是當事件正發生或發生後，對電腦系統或設備找尋與案件有關的數位證據之系統化活動或作為，而經此系統化之作為所呈現的證據，可做為法庭所接受之證據。

路卡交換原理(Locard’s exchange principle)

「凡接觸必留下痕跡」

意指任何人、物只要進入了犯罪現場，必會帶走現場某些東西；必然也會留下某些東西，亦即所謂微物跡証之相互移轉。

路卡交換原理(Locard’s exchange principle)

以數位證據的角度而言，舉例來說：當使用電腦進行瀏覽網站的動作，本機端必會留下該網站資訊，而該網站伺服器也會留下瀏覽紀錄。

數位證據的處理程序

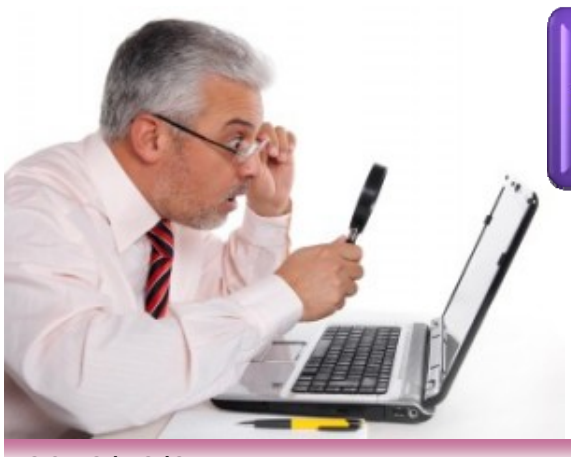
初步分析（Preliminary Analysis）

證據蒐證（Evidence Collection）

證據擷取保存（Preserve Evidence）

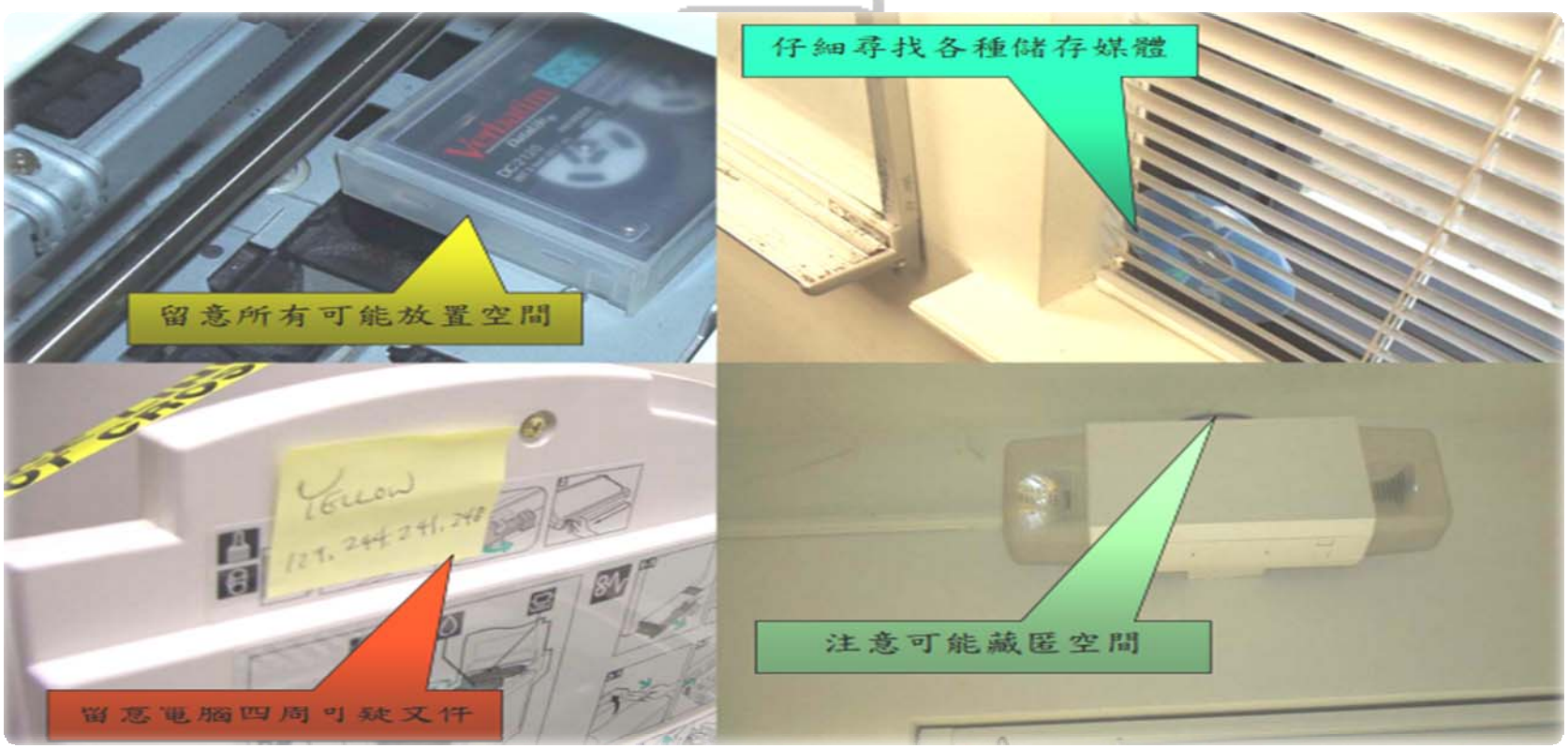
證據檢驗分析（Evidence Analysis）

結果呈現（Case Interpretation）



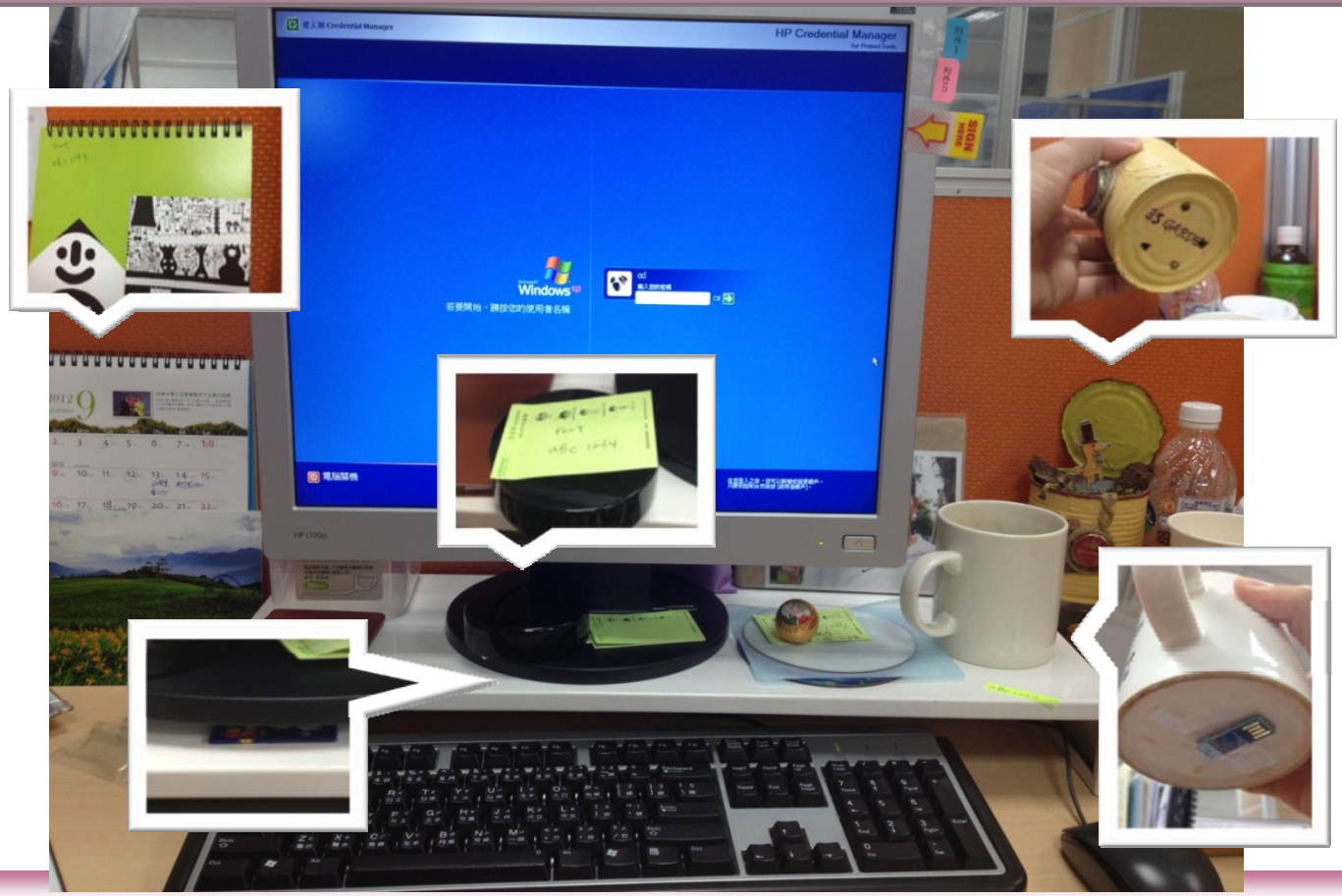
數位證據的處理程序

初步分析（Preliminary Analysis）



數位證據的處理程序

初步分析（Preliminary Analysis）

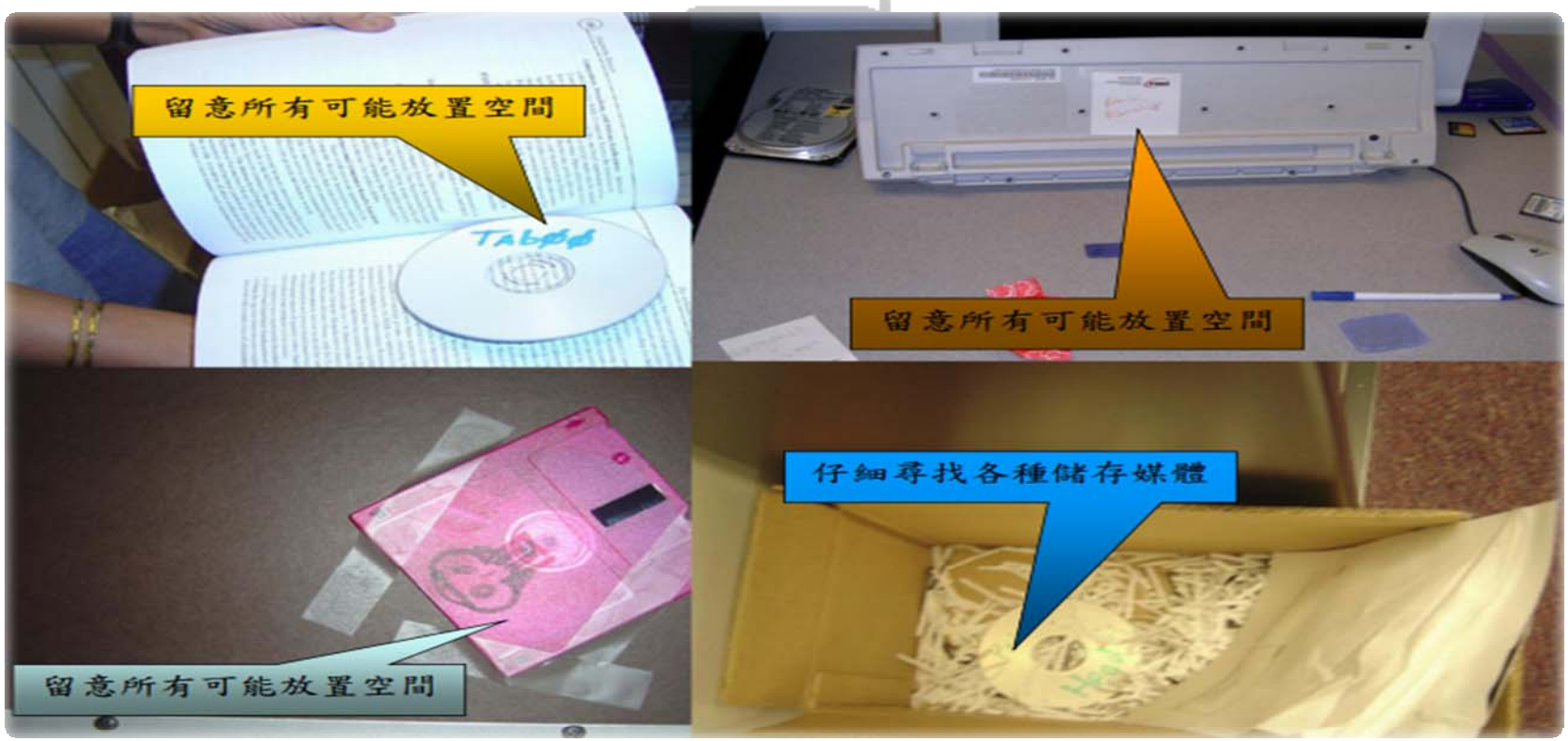


數位證據的處理程序

初步分析（Preliminary Analysis）

數位證據的處理程序

初步分析（Preliminary Analysis）

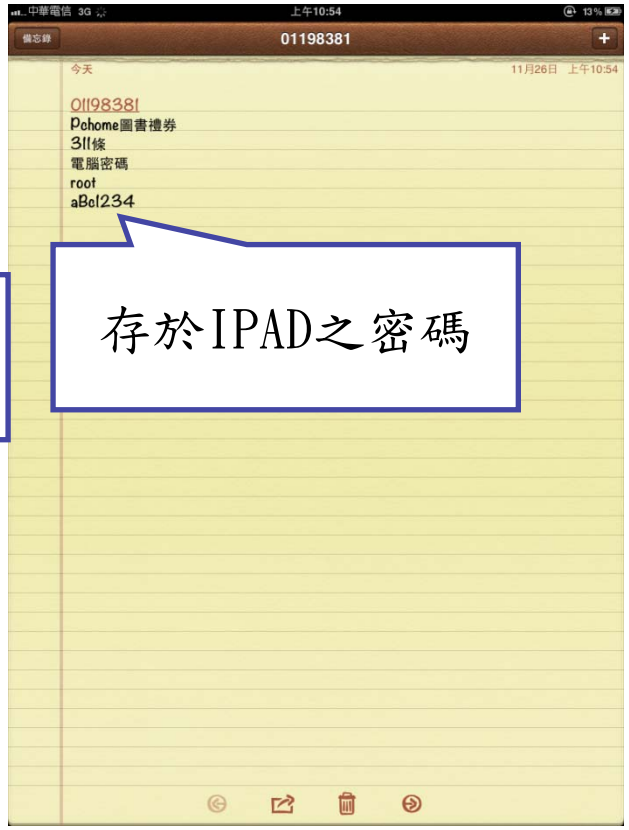


數位證據的處理程序

證據蒐證（Evidence Collection）

數位證據的處理程序

證據蒐證（Evidence Collection）



數位證據的處理程序

證據擷取保存（Preserve Evidence）

證物鏈（Chain of Custody）

數位證據的處理程序

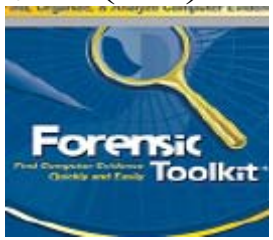
結果呈現 (Case Interpretation)

數位鑑識工具(for Mobile)

- 手機資料蒐集選擇一種的連接方式(Cable、WiFi 、 Bluetooth、IrDA)
- 針對裝置選擇鑑識軟體
  - 非智慧型手機
    - Oxygen Forensicfor Nokia phones
    - MOBILedit!
  - 智慧型手機Windows CE、Palm系列
    - Paraben For PDA(Data Acquisition)
  - Symbian系列
    - Oxygen Forensicfor Symbian OS
  - iOS-ramdisk (Elcomsoft)
  - Andriod-Dalvik VM
- 可攜式行動裝置鑑識設備
  - CellDEK (Software implement)
  - CellDEK TEK (Hardware implement)
  - CellBrite
  - XRY

數位鑑識工具(for Computer)

- Non-Commercial based Solution
  - Unix-Based
    - Live Collecton
      - Trusted System Command (ps，lsof、netstat.,etc.)
      - chkrootkit、rkhunter
    - Forensic Duplication
      - dcfl-dd
    - Network Collection
      - Tcpdump
      - Ethereal、Ettercap
      - tcpxtract、foremost
  - Windows-Based
    - Live Collection
      - Forensic Acquisition Utilities (dd、md5sum.,etc.)
      - Netcat
      - Sysinternals (PsXXX)
      - PTFinder
      - Windows Forensic Toolchest (WFT)
    - Forensic Duplication
      - DD
      - Network Evidence Duplicator(NED)
      - Ftk Imager
    - Network Collection
      - Ethereal 、ettercap
      - windump
- Commercial based Solution
  - EnCase
  - Access Data FTK
  - X-Ways Forensics
  - Paraben P2
  - FinalData



國外相關規範介紹

1. National Institute of Justice

Forensic Examination of Digital Evidence:
A Guide for Law Enforcement

原則：

1） 必須確定保全及採集數位證據的動作不會影響原證據的完整性。

2） 負責檢查的人員必須受過專業訓練。

3） 任何對數位證據的動作如扣押、檢查、儲存、傳輸等過程必須加以記錄、保存並且可供日後調閱。

國外相關規範介紹

鑑識流程：

1)證據評估 Evidence Assessment

2)證據獲取 Evidence Acquisition

3)證據檢查 Evidence Examination

4)紀錄與報告 Documenting and Reporting

國外相關規範介紹

證據檢查：

1)準備 Preparation

2)萃取 Extraction

3)進行萃取資料之分析 Analysis of extracted data

4)結論 Conclusion

ICCL@B

國外相關規範介紹

2. Association of Chief Police Officers

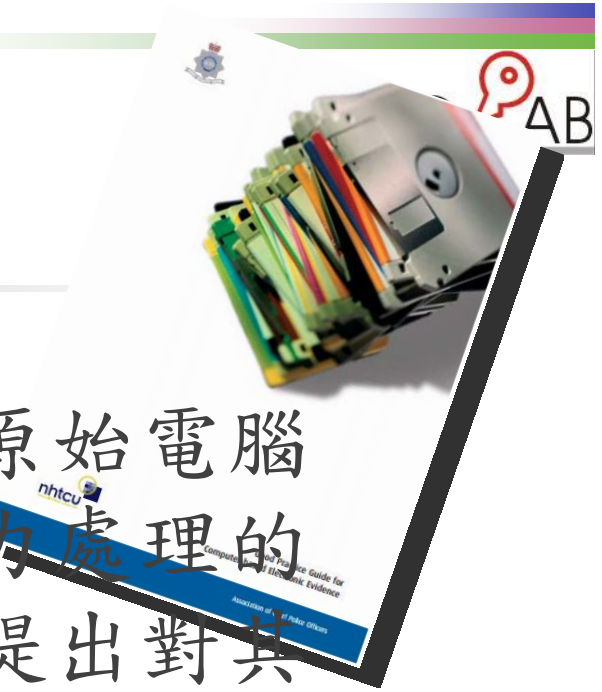
Good Practice Guide for Computer based Electronic Evidence

ICCL@B

原則：

1)為了獲得數位證據在法院中的認可，處理案件的警察人員或其委託代理人，必須維持電腦或其他電子媒體上的資料為犯罪現場中原始的狀態，不得採取任何造成影響之動作。

國外相關規範介紹



2）在特殊情況下，如果需存取原始電腦證據的資料，則必須由有能力處理的人員進行存取的動作，並且提出對其處理的動作解的解釋與說明。

3）對於電腦相關證據的任何稽核資料或其它處理的紀錄，應建立處理與保存方法。使獨立公正的第三者即使進行相同的處理程序，其所得結果亦相同。

國外相關規範介紹

4）案件承辦的負責人必須負責確保法律的規範與以上的處理原則有被遵守，這些規範並適用於案件中所包括的電腦資訊存取。任何人存取電腦資料或使用拷貝設備進行複製都必須遵守法律規範與以上原則。

國外相關規範介紹

共通點：

1）確保數位證據不受外力影響。

2）鑑識人員需經專業訓練。

3）確保證據鏈紀錄完備。

鑑識與反鑑識(偽裝學)

矛(鑑識) 與 盾(反鑑識) 之爭!

鑑識與反鑑識(偽裝學)

反鑑識之策略：

1)Attack on data：刪除或修改潛在的證據，使之難以理解或使之在法院上不具證據力。

2)Attack on tools：利用電腦鑑識工具的弱點，進而產生不實的調查報告。

3)Attack on the analyst: 產生了大量的資料，使分析者懷疑工作內容的有效性。

鑑識與反鑑識(偽裝學)

Attack on analyst

→

Attack on tools

→

Attack on data

→

鑑識與反鑑識(偽裝學)

反鑑識手法：

1)資料隱藏(Data hiding)：使用資料隱藏技術隱藏證據。(關鍵技術)

2)零足跡(Zero footprinting)：有鑑於「凡走過必留下足跡」的道理，那麼就清理足跡！

3)資料混淆(Data obfuscation)：目的是創造資料的混亂與不確定性，鑑識結果產生誤差。

鑑識與反鑑識(偽裝學)

1）熟悉反鑑識技術至為重要，因為犯嫌為掩飾犯罪證據而使用該技術刪除電腦中的跡證。

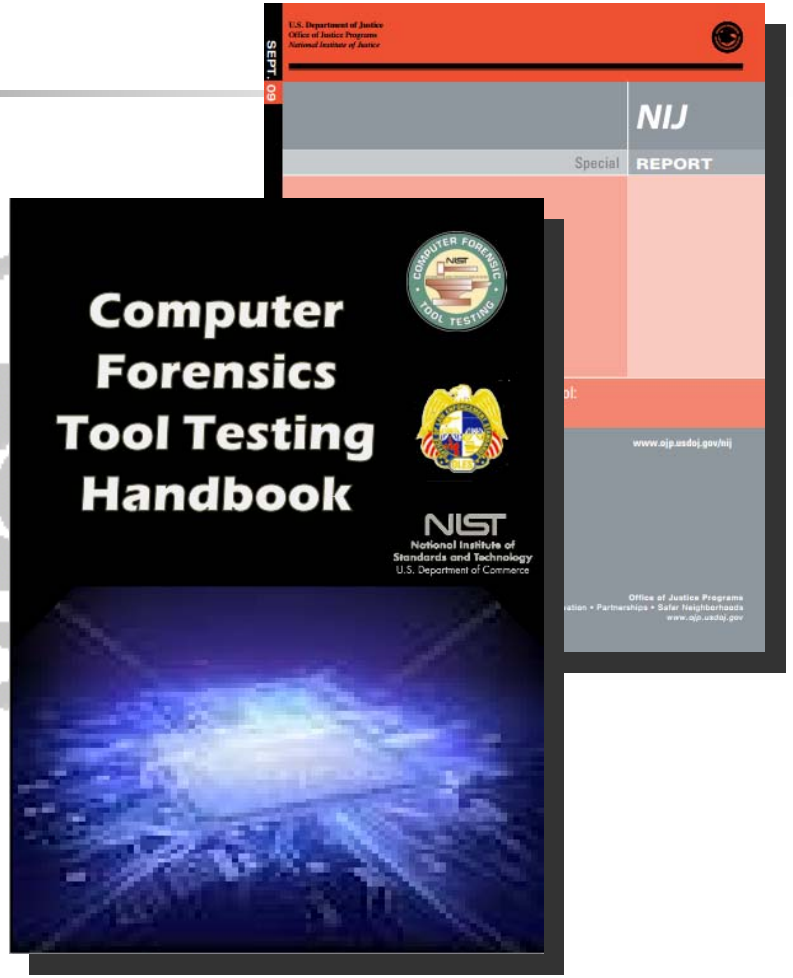
2）數位資料能否成為法庭上的證據(或者證據力強弱)，取決於鑑識人員能否揭開犯嫌之反鑑識技術 。

數位鑑識將面臨的挑戰

- 儲存容量倍數成長，鑑識人員工作吃重。
- 資訊隱藏技術成熟，工具更是隨手可得。
- 犯罪證據備援於國外機房或利用 VPN 連線，造成偵查與蒐證的困難。
- 資料復原觀念普及，犯罪者多使用安全的檔案清除工具。
- 檔案系統加密技術之使用，硬碟分區之解密增加鑑識難度。
- 智慧型手機的價位趨於大眾接受，桌上型電腦的應用快速 轉移至手機上，手機鑑識將成為主流。

鑑識工具評測

美國NIST與NIJ合作規劃執行Computer Forensics Tool Testing (CFTT) Project針對各項電腦鑑識軟體做評測，並將評測結果公執法人員參考使用。

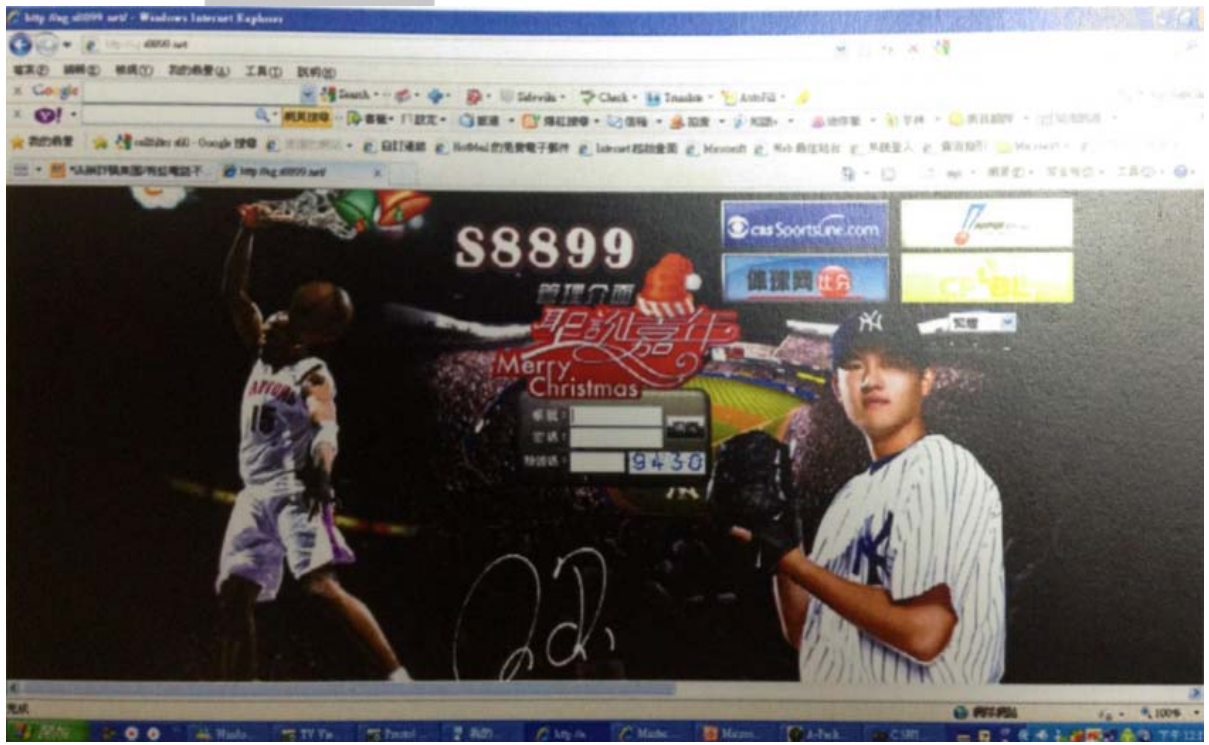


相關網址：http://www.cftt.nist.gov/

案例探討-賭博

- 陳○ ○與吳○ ○以百萬元於95年間在台中成立○ ○運動網，經營至99年4月遭受警方取締。

四年間估計獲利上百億。



案例探討-賭博

- 網路賭博匿名性高

  賭博網站多利用網路匿名性高與無遠弗屆的特性，利用網際網路向國外網路服務業者申請網址註冊，並將網站架設於境外，透過這種法律管轄權不同的優勢，進行跨境犯罪，由於賭客透過網際網路進行對賭，能保持一定隱密性，因此擴張速度快，讓警方查不勝查。

案例探討-賭博

透過臺灣固網ADSL的IP位置順利找到伺服器所在位置後查扣相關主機，並從主機中找到工資記錄與帳務資料，因為所有資料均透過網路傳送，因此從網路傳送紀錄反查其他犯罪處所IP，順利找出賭博網站機房處所及盤口。

案例探討-賭博

第一線偵查人員進入網路賭博盤口發現全部電腦均關閉，開啟電源後會啟動程式立即刪除資料。

鑑識工具評測

MOBILedit!

http://www.mobiledit.com/

手機鑑識工具MOBILedit操作

- IPhone4S手機連接電腦
  - 讀取手機電話簿
  - 讀取手機簡訊
  - 讀取手機存儲之多媒體檔案
  - 讀取手機裡系統資料檔
  - 讀取手機行事曆
  - 讀取手機記事本

- **Dr. Professor Shiuh-Jeng WANG**
- PhD. National Taiwan University, Taiwan, 1996
- Full Professor, Central Police University, Dept. of Information Management
- Director Information Crypto and Construction Lab
- Chair of ICCL-FROG (**F**orensic **R**esearch devel**O**pment task force **G**roup)
- Vice-President, Chinese Cryptography Information Security Association (**www.ccisa.org.tw**)

- Chairs of IEEE-CS/LNCS Proceedings, Internat'l confs.
  http://www.sersc.org/SH08/ http://www.ftrg.org/MPIS2009
  http://ncs2009.ntpu.edu.tw/CI/CI.htm http://www.ftrg.org/futuretech2010
  https://sites.google.com/site/uicuipm2012/ IEEE-sponsored,
  http://www.ftrai.org/music2012
- Editor-in-Chief AT JITAS (http://jitas.im.cpu.edu.tw)
- SCI-Journals, Guest-editors-,
  - IEEE J-SAC, http://www.comsoc.org/livepubs/sac/index.html
    http://hera.im.cpu.edu.tw/sjw_2006/meeting_report/IEEE-GUEST-EDITORIAL-0808-2011-.pdf
  - Journal of Internet Technology (JIT)
    http://jit.ndhu.edu.tw/callforpaper/April-2011-SI-JIT.pdf
  - The Computer Journal, http://comjnl.oxfordjournals.org/
  - Springer Telecommunication Systems
    http://www.springer.com/business/business+information+systems/journal/11235
  - The Journal of Supercomputing,
    http://www.springer.com/computer/swe/journal/11227 (Springer)
  - Peer-to-Peer Networking and Applications,
    http://www.editorialmanager.com/ppna/ (Springer)