tsc 德欣
TSC CAPITAL GROUP
The Bridge to the Asia Pacific Region

國立臺南藝術大學

數位鑑識

講師：邱立德

德欣寰宇科技股份有限公司 TSC TECHNOLOGIES, INC.

台北公司：台北市10059新生南路一段50號5樓500室　TEL: 886 2 2358 2775 · FAX:886 2 2358 3775

新竹公司：新竹市30046四維路130號2樓之2　TEL: 886 3 522 9570 · FAX:886 3 524 7507

課程大綱

1. 何謂數位鑑識
2. 數位鑑識流程
3. 工具之使用
4. Q & A

常見電腦犯罪類型

- 以電腦為犯罪工具
  - 非法販賣—販賣違禁品(毒品、槍枝等)
  - 煽惑犯罪—網路三七仔、六合彩明牌
  - 網路詐騙—拍賣詐欺、網路男蟲
  - 非法言論—千面人恐嚇、妨害名譽
  - 非法傳輸—P2P

常見電腦犯罪類型(續)

- 以電腦為犯罪場所
  - 侵害著作權—盜版光碟
  - 妨害風化—色情網站
  - 網路賭博—賭博網站
- 以電腦為犯罪標的
  - 入侵主機—竊取資料庫、破壞系統
  - 電腦病毒—破壞電腦、植入後門
  - 盜用帳號—小額付款、遊戲裝備、網路銀行轉帳、下單

何謂數位鑑識(Computer Forensics)

- 電腦鑑識是利用科學的方法對電腦等資訊科技設備進行犯罪蒐證，以提供有力的線索，來幫助犯罪案件的偵查或是法庭的審訊。
- 電腦鑑識也是有關於電腦鑑識分析、電子資料發掘、電子證據發掘、數位資料發掘、資料回復、資料發掘、電腦分析和檢查的工作，是一種有條不紊的鑑定電腦相關媒體之處理程序。

何謂數位鑑識(續)

- 由於數位資料的任何新增、刪除與修改動作，相關的紀錄都會儲存在電腦設備（系統）中，因為它有所謂「凡走過必留下痕跡」的特性，即使是被有人心士蓄意刪除，還是可透過鑑識工具軟體還原，這也就是電腦鑑識在高科技犯罪偵查過程中不可或缺的重要原因。

何謂數位鑑識(續)

- 「數位證據」係指電腦儲存媒體中任何足以證明犯罪構成要件或關聯的電子數位資料，為物理證據的一種，包括有文字、圖片、聲音、影像等型態，具有可無限無差異性複製、不易銷毀、原始作者不易確定、資料完整性驗證等性質，亦稱電腦證據或電子證據，其以電磁紀錄方式儲存於電腦儲存媒體上

何謂數位鑑識(續)

- 數位證據在實務上是扮演輔助證據的角色，是用來加強罪犯的犯罪事實
  - 數位證據是否與原始的記錄相同，是否曾遭他人篡改或其它因素變更原始內容，即所謂「證據能力」的問題。
  - 數位證據如未被篡改或變更其內容，該證據能證明什麼，即所謂「證明力」的問題。

數位鑑識

- 數位鑑識作業程序：
  - 蒐集
  - 證據保存
  - 檢驗 & 分析
  - 報告
  - 法庭呈現
- 重點在於防止證據被污染
- 所有步驟需要錄影、兩人以上在場

數位鑑識(續)

- 數位證據的特性：
  - 易於複製與修改，但不易保留其原始狀態
  - 不易證實其來源及完整性
- 來源種類繁多
- 介質規格不盡相同
- 儘管取證困難，但證據無所不在

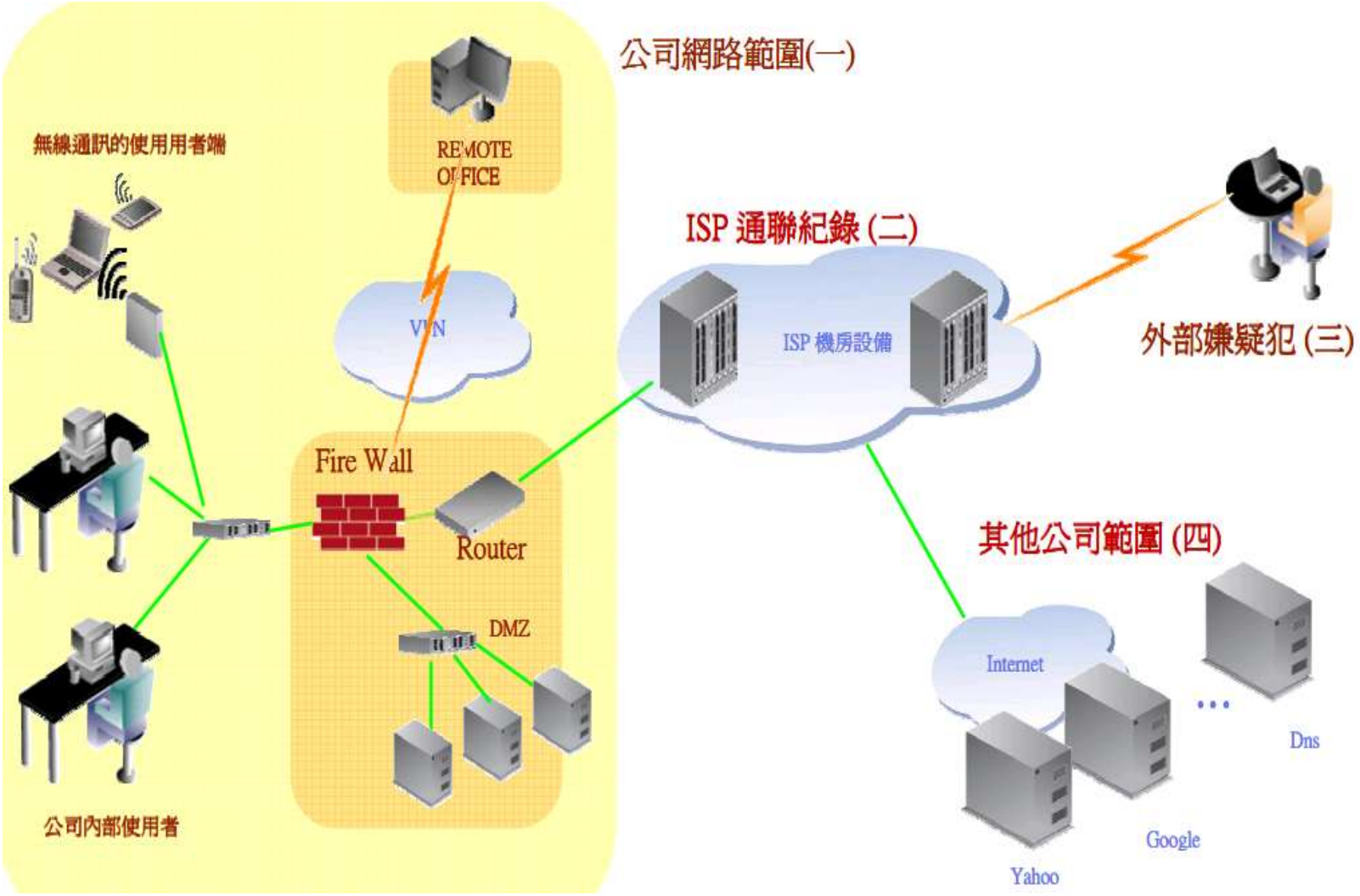
電腦現狀及趨勢

- 電腦消逝性資料愈來愈多
  - RAM 增加
- 硬碟的容量愈來愈大
- 資料加密的狀況愈來愈普及
- 網路通訊的加密

數位證據有哪些

- 個人隨身資訊產品例如：
  - 智慧型手機、PDA 、 MP3 Player 、 Mobile Phone 、 USB Disk 、 Digital Camera 、電子書及電子相簿等
- 各型式電腦：
  - 例如平板電腦、個人電腦、筆記型電腦、掌上型電腦、工業用電腦等
- 網路設備：
  - 防火牆、路由器、交換器及各型式網路匝道設備
- 大型伺服器系統：
  - AIX，Solaris，HP Unix，AS 400等
- 資料貯存媒體：
  - Tape，SAN，NAS，DAS，光碟(CD、DVD、BlueRay)等

數位證據可能存在的位置



數位鑑識開始

- 開始之前，應先考慮下列幾點：
  - 鑑識人員須準備攝影照相等器材，紀錄所有鑑識過程，以及證物的相關資訊
  - 所有的證物接入鑑識主機前一定要確保防寫機制有效
  - 將證物收進證物室之前必須標記清楚並做好門禁管制，所有進出入的文件可一併附在鑑識報告之後，以供查驗
  - 結案之後的證據檔及相關報告需留存一年以上
- 誰掌握了資料庫及知識分析智能，誰就掌握了優勢

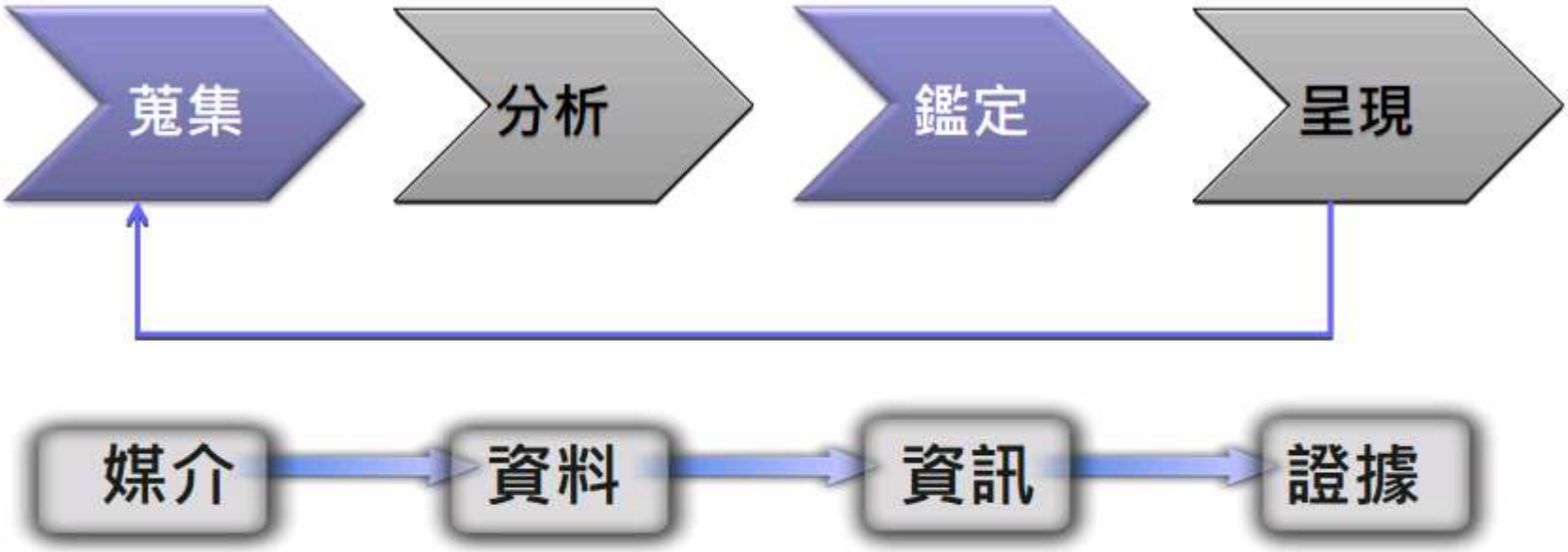
現場採証主要類型

- 原始證物封存帶離現場
- 現場製作映像檔或位元串流式(Bit-stream)複製
- 只做邏輯檔案的複製
- 開機狀況下消逝性資料採證及資訊分析
- 網路及通訊內容的即時蒐證

課程大綱

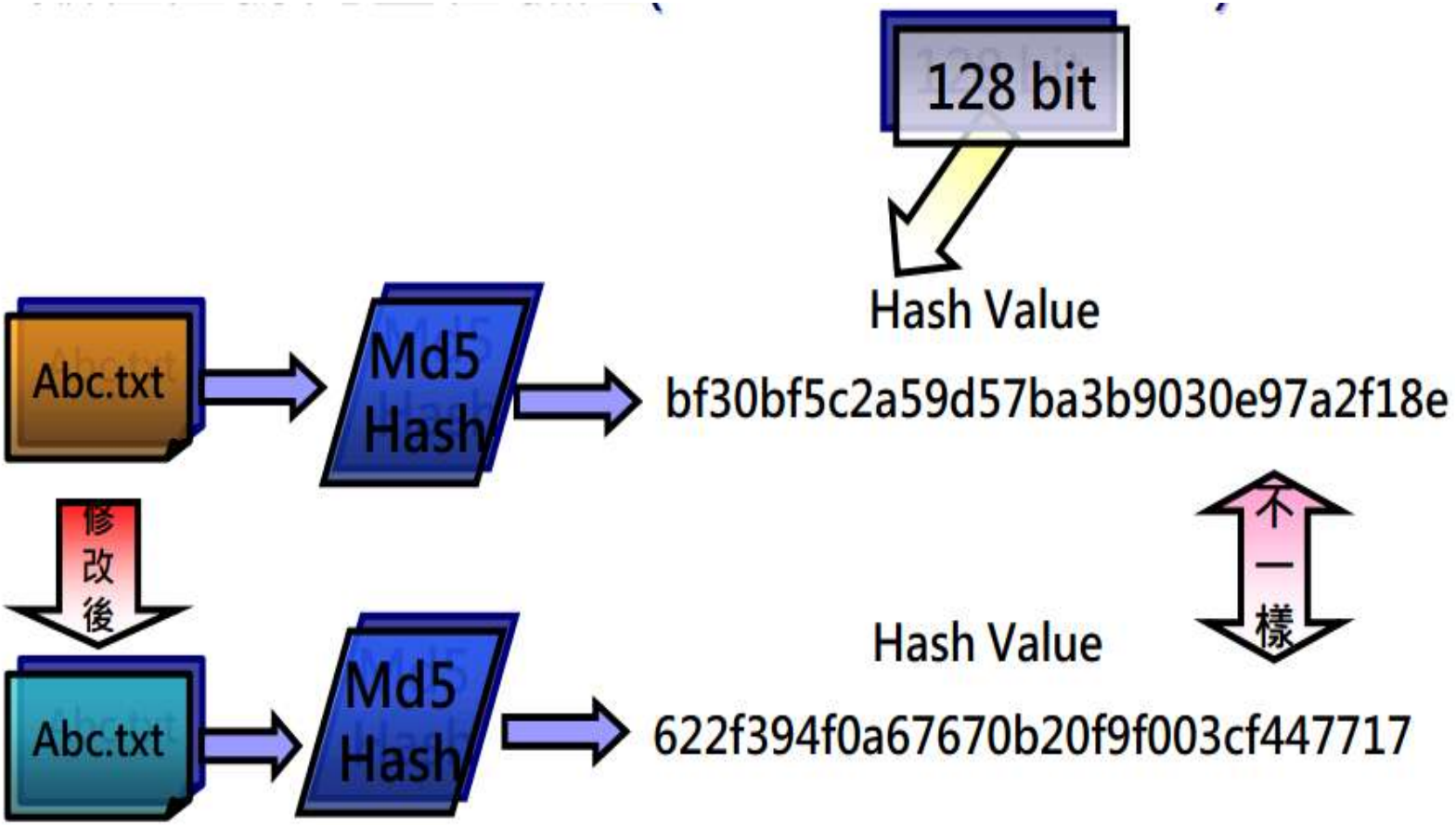
1. 何謂數位鑑識
2. 數位鑑識流程
3. 工具之使用
4. Q & A

數位鑑識流程



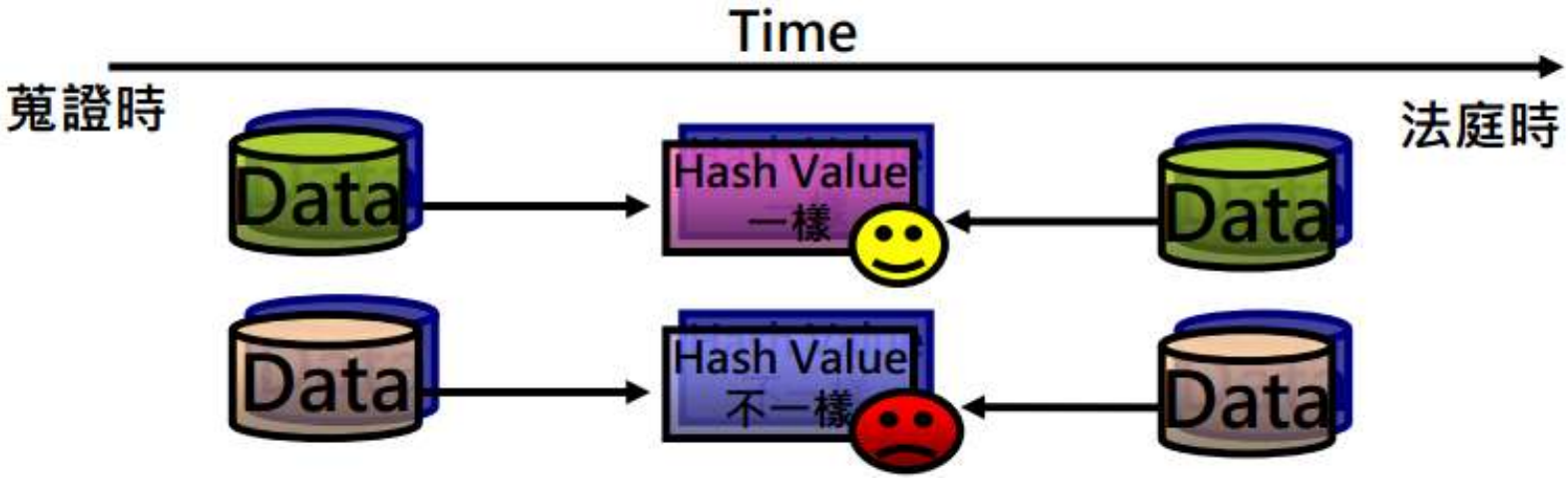
Evidence Viability=Data Preservation+ Data Integrity+ Documentation

數位證據完整性之驗證


128 bit
Hash Value
Abc.txt
Md5 Hash
bf30bf5c2a59d57ba3b9030e97a2f18e
修改後
不一樣
Hash Value
Abc.txt
Md5 Hash
622f394f0a67670b20f9f003cf447717

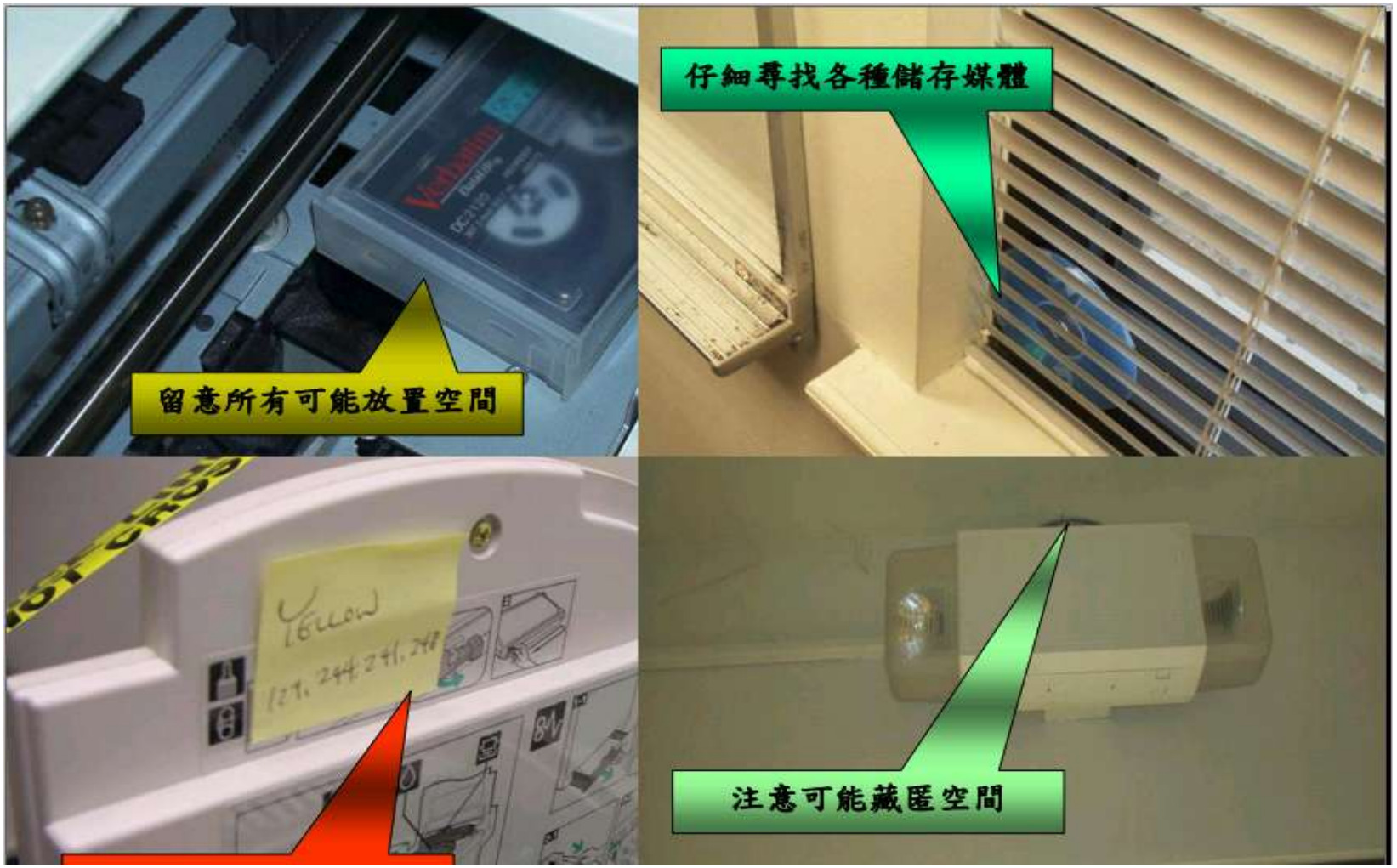
數位證據完整性之驗證(續)

- 數位證據蒐證時必須對所蒐集到的資料做完整性驗證並記錄Hash值於相關表單中。
- 在法院時如對交付之證據有疑議時，可以對原始資料做一次完整性驗證，如果Hash值與蒐證時所記錄的數值一樣的話表示數位證據從蒐證到法院的期間並未受到任何修改。

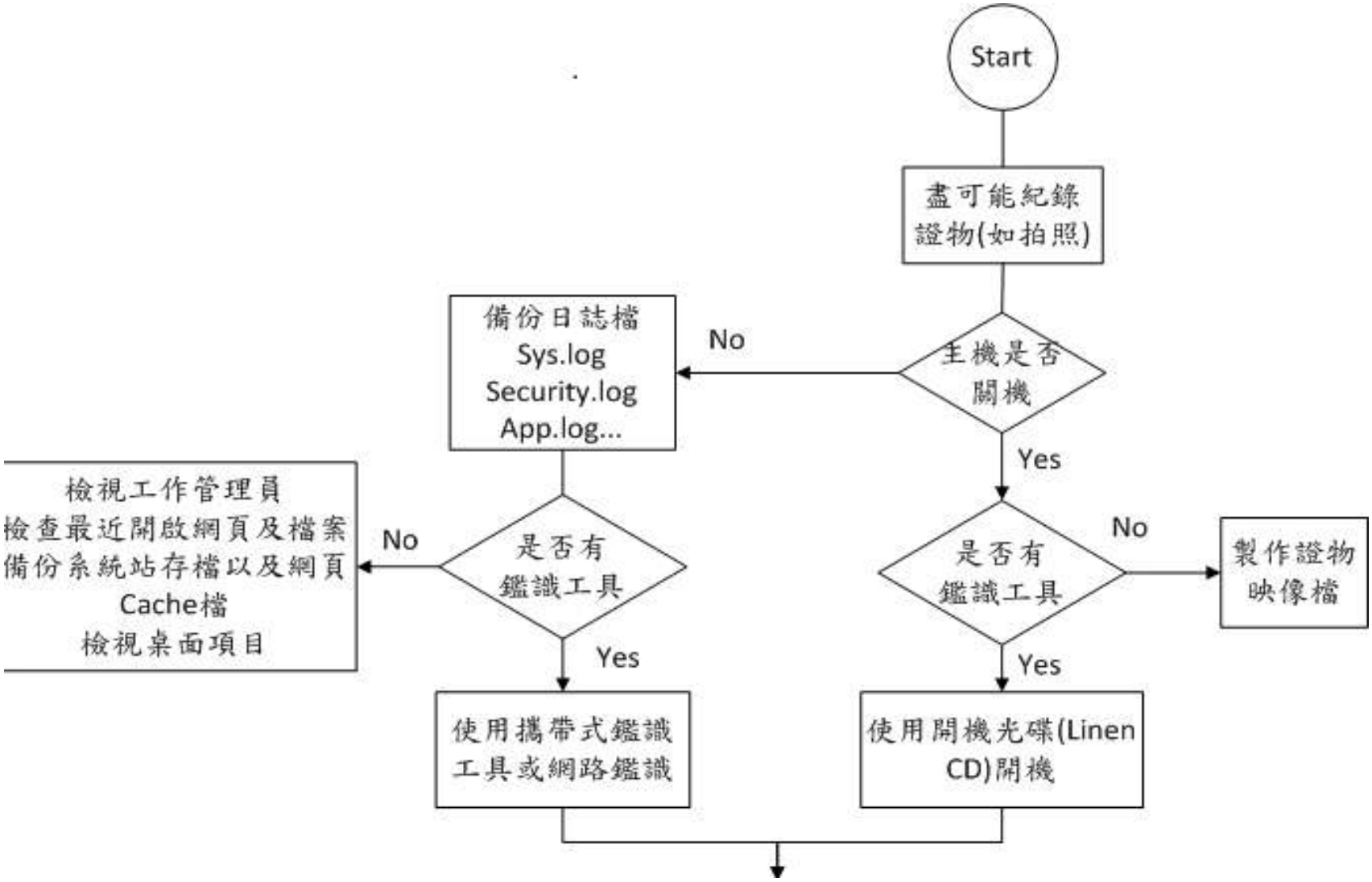


現場資訊蒐集

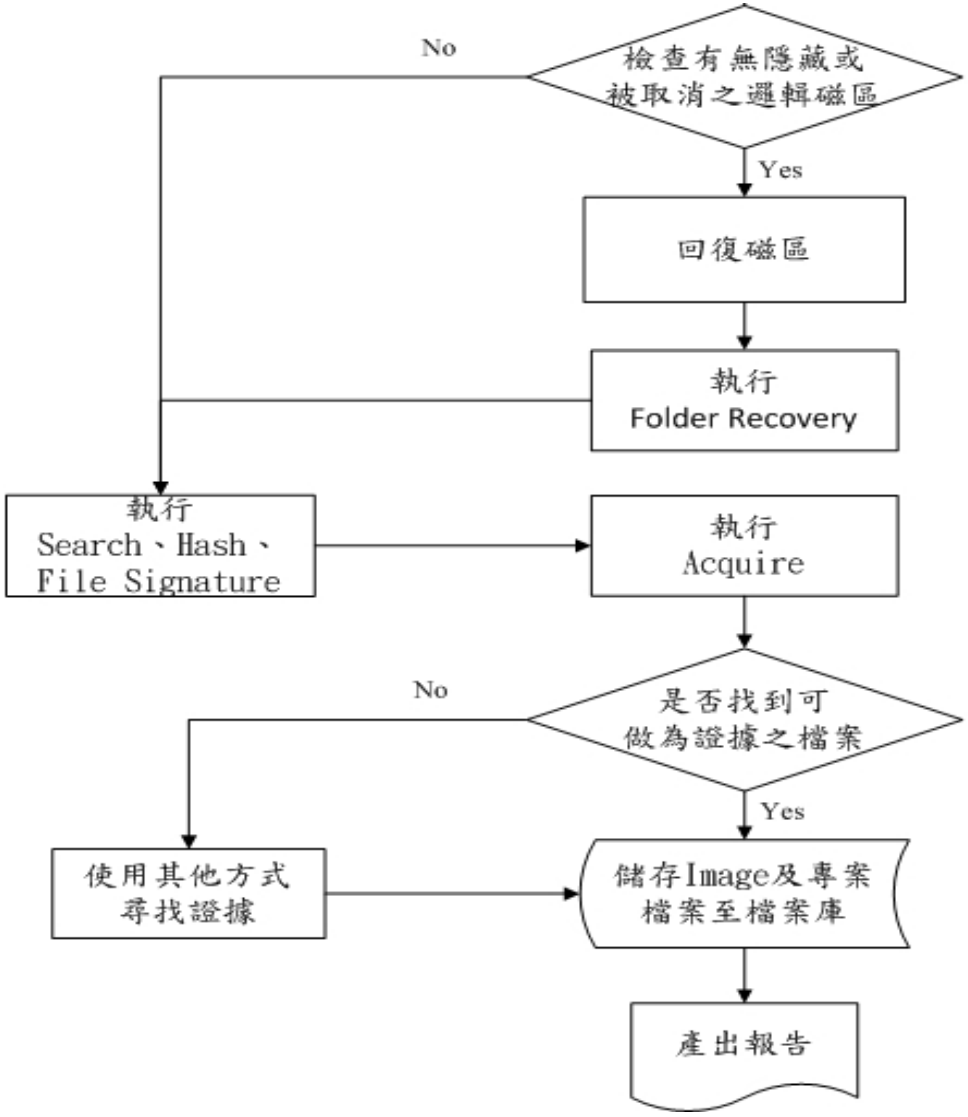
現場資訊蒐集(續)



數位鑑識流程


Start
盡可能紀錄
證物(如拍照)
主機是否
關機
No
備份日誌檔
Sys.log
Security.log
App.log...
Yes
是否有
鑑識工具
No
製作證物
映像檔
Yes
使用開機光碟(Linen
CD)開機
是否有
鑑識工具
No
檢視工作管理員
檢查最近開啟網頁及檔案
備份系統站存檔以及網頁
Cache檔
檢視桌面項目
Yes
使用攜帶式鑑識
工具或網路鑑識

數位鑑識流程(續)


No
檢查有無隱藏或
被取消之邏輯磁區
Yes
回復磁區
執行
Folder Recovery
執行
Search、Hash、
File Signature
執行
Acquire
No
是否找到可
做為證據之檔案
Yes
使用其他方式
尋找證據
儲存Image及專案
檔案至檔案庫
產出報告

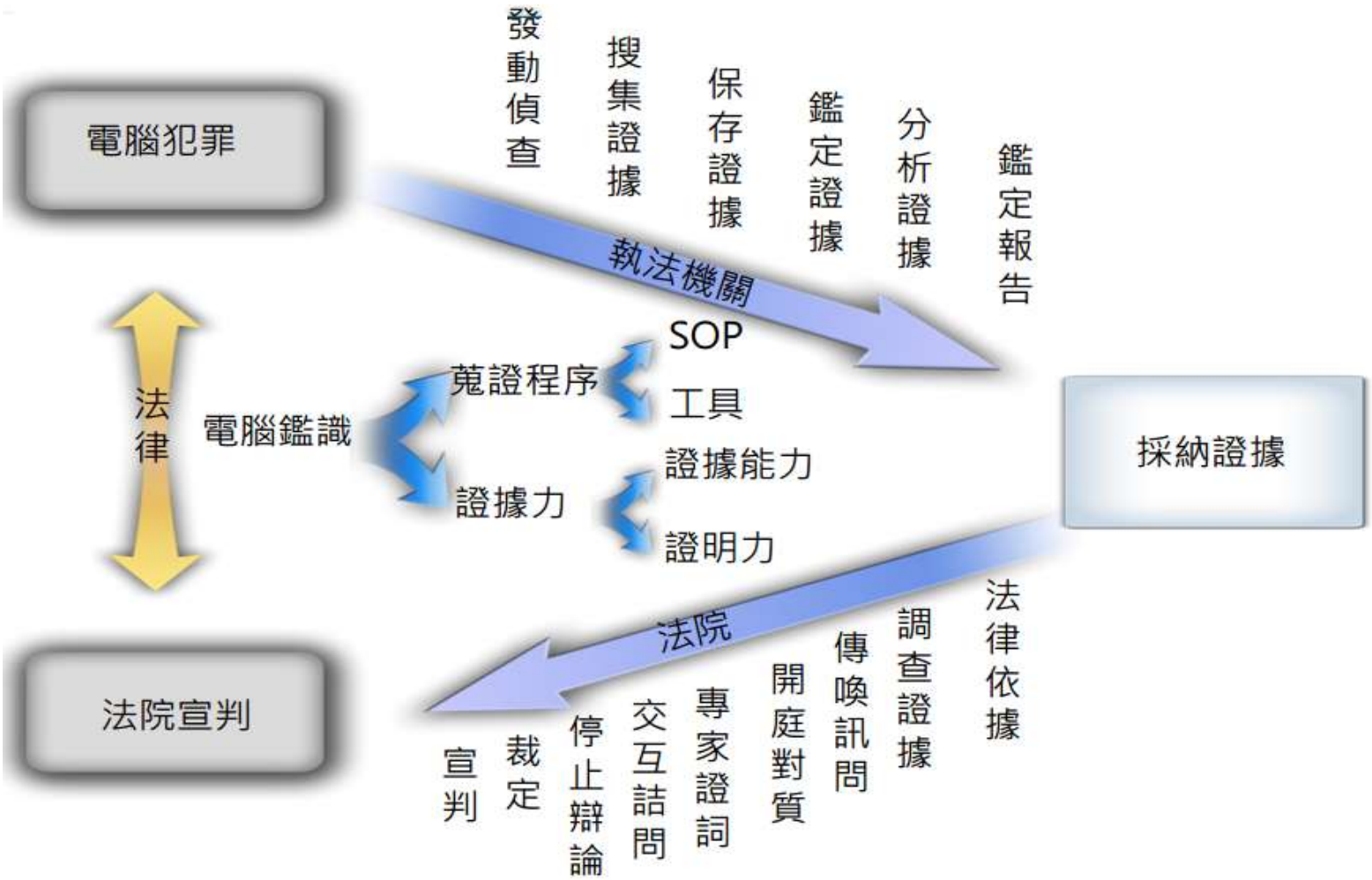
硬碟資料復原與解析

- 製作硬碟副本
  - 為維護電腦系統的持續運作，硬碟無法帶離現場，或需要鑑定硬碟資料，且不可修改或破壞原始硬碟資料時。
  - dd、dcfldd、encase、ftk imager、Forensic Talon、OSForensics
- 硬碟鑑識分析
  - 將映像檔載入鑑識軟體分析->EnCase、FTK、OSForensics
  - 將映像檔掛載成一個或多個虛擬磁碟機->Mount Image Pro、OSFmount
  - 利用VMware軟體掛載成虛擬磁碟並啟動作業系統->LiveView、Vmware Player

硬碟資料復原與解析(續)

- 常遇到的挑戰
  - Encrypted File System
  - Steganographic(資訊影藏)
  - Partition table、FAT、MFT損毀
  - RAID 故障或設定錯誤

電腦犯罪與數位鑑識


電腦犯罪
發動偵查
搜集證據
保存證據
鑑定證據
分析證據
鑑定報告
執法機關
SOP
工具
證據能力
證明力
採納證據
法律
電腦鑑識
蒐證程序
證據力
法院
法律依據
調查證據
傳喚訊問
開庭對質
專家證詞
交互詰問
停止辯論
裁定
宣判
法院宣判

課程大綱

1. 何謂數位鑑識
2. 數位鑑識流程
3. 工具之使用
4. Q & A

儲存媒體

- 硬碟是眾多實體儲存媒體中的一種其中能分割成多個邏輯磁碟區

分割磁區

- 硬碟是眾多實體儲存媒體中的一種其中能分割成多個邏輯磁碟區

s Overwritten: No

Volume

File System:	NTFS	Drive Type:	Fixed
Sectors per cluster:	4	Bytes per sector:	512
Total Sectors:	3,894,849	Total Capacity:	1,994,162,176 bytes (1.9GB)
Total Clusters:	973,712	Unallocated:	192,303,104 bytes (183.4MB)
Free Clusters:	93,898	Allocated:	1,801,859,072 bytes (1.7GB)
Volume Name:		Volume Offset:	63
Driver Information:	NTFS 3.1 Chkdsk 0		

Is Internal: No
Is Overwritten: No

Volume

File System:	FAT32	Drive Type:	Fixed
Sectors per cluster:	8	Bytes per sector:	512
Total Sectors:	1,104,705	Total Capacity:	564,486,144 bytes (538.3MB)
Total Clusters:	137,814	Unallocated:	490,704,896 bytes (468MB)
Free Clusters:	119,801	Allocated:	73,781,248 bytes (70.4MB)
Volume Name:	DATA	Volume Offset:	3,894,975
OEM Version:	MSWIN4.1	Serial Number:	3956-1108
Heads:	128	Sectors Per Track:	63

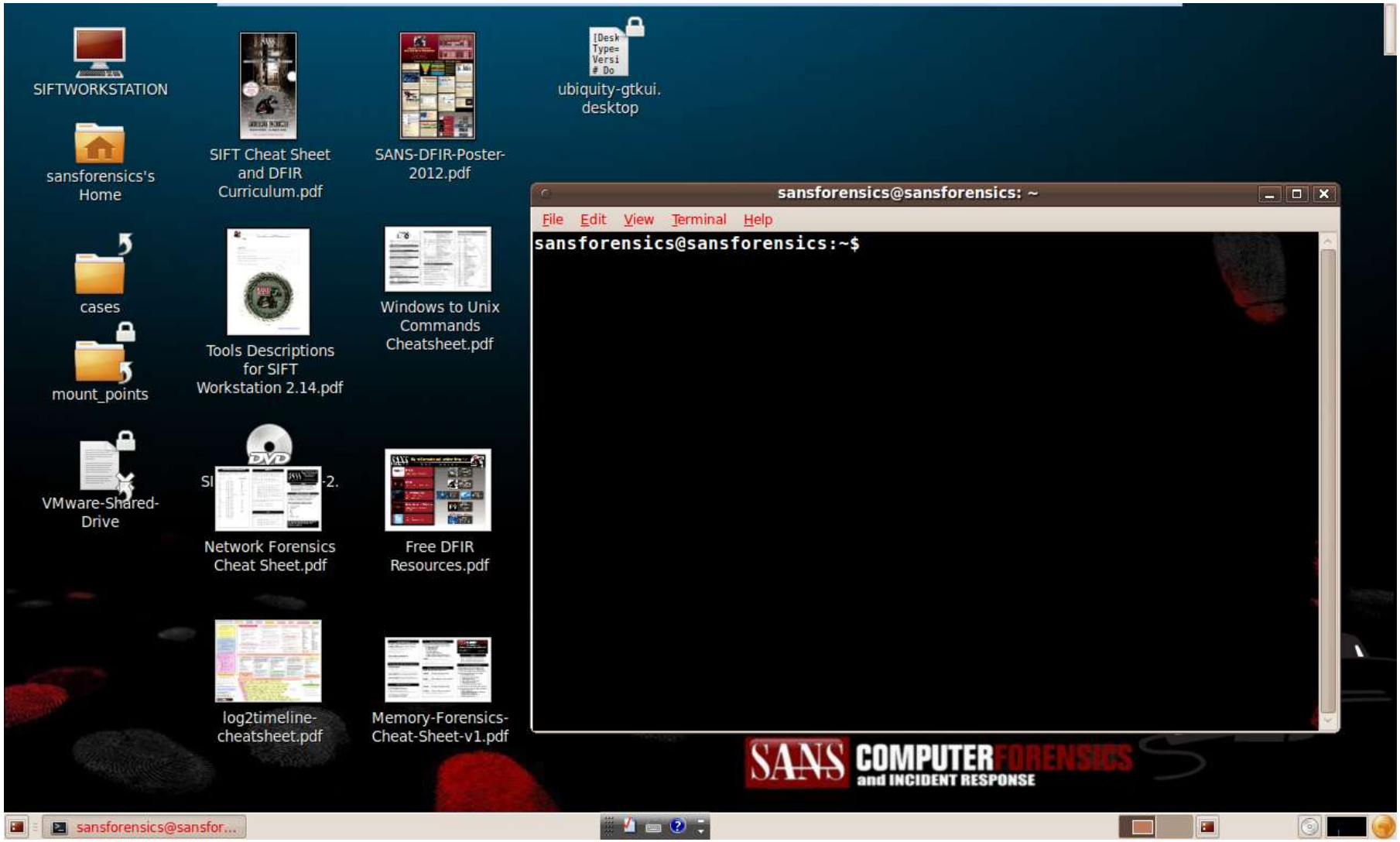
鑑識工具介紹

- 開機光碟(LiveCD)
  - Helix
  - SANS Investigate Forensic Toolkit (SIFT) Workstation
  - Back Track
  - DEFT
  - CAINE (Computer Aided INvestigative Environment)
  - **FCCU GNU/Linux Forensic Boot CD**

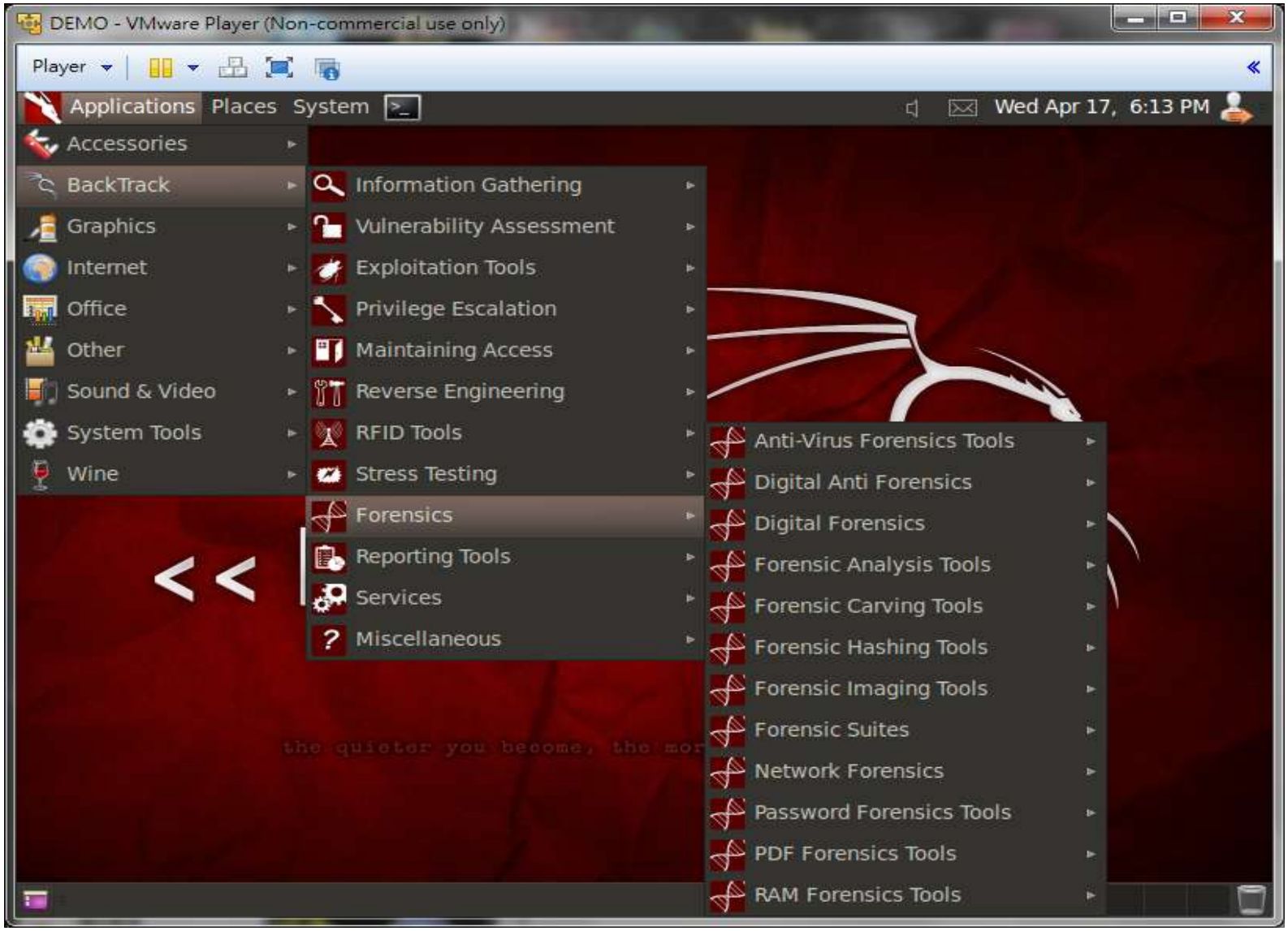
鑑識工具介紹(續)


Applications
Places
System
Wed Apr 17, 7:19 PM
Accessories
Forensics & IR
Graphics
Internet
Office
Sound & Video
System Tools
Add/Remove...
Adepto
Autopsy
Bless Hex Editor
GtkHash
HFS Volume Browser
Linen
Meld Diff Viewer
Ophcrack
Registry Viewer
Retriever
Root Terminal
TrueCrypt
Virus Scanner
Wireshark (root)
Xfprot
INCIDENT RESPONSE
HELIX3
COMPUTER FORENSICS
ELECTRONIC DISCOVERY

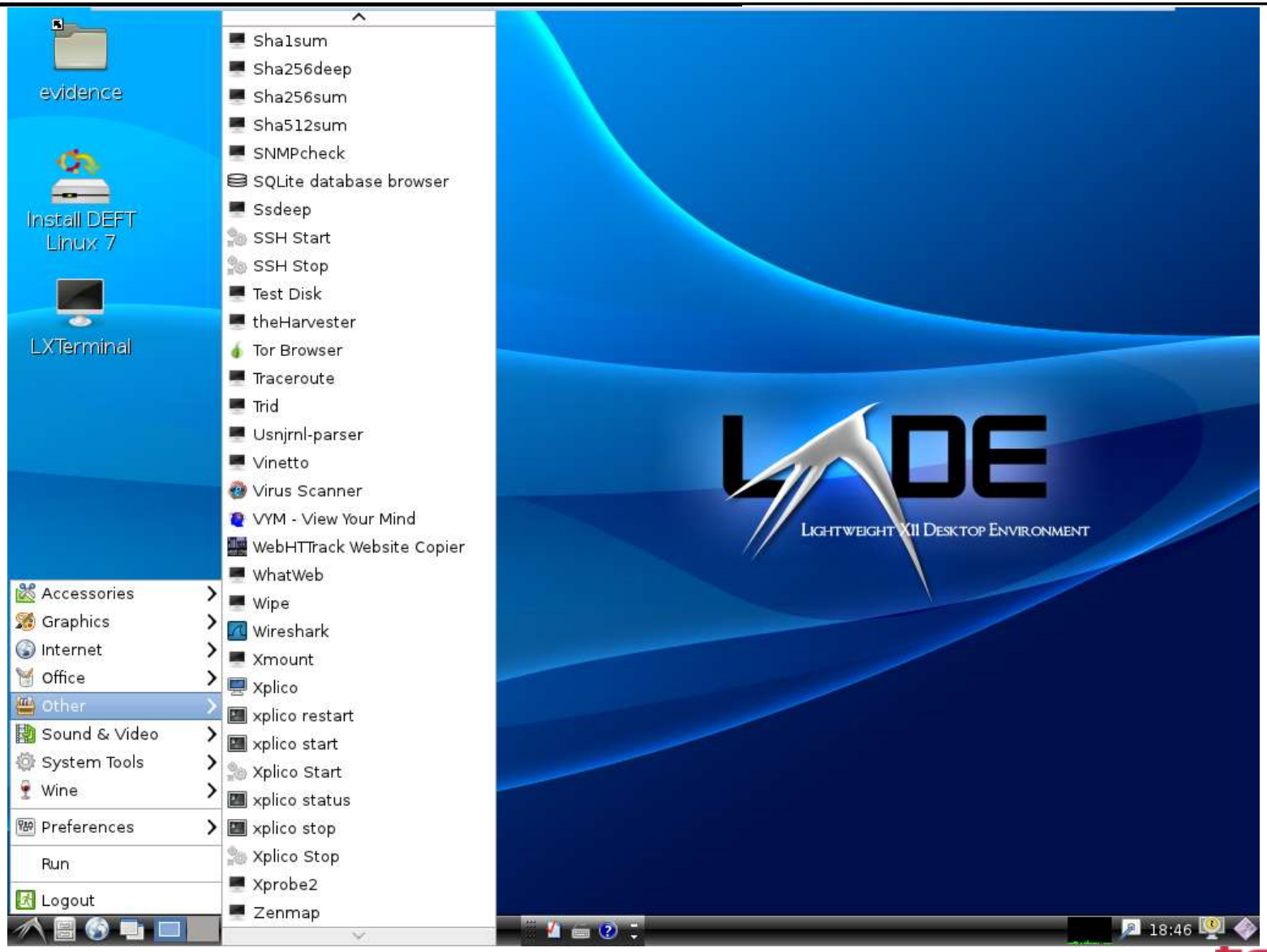
鑑識工具介紹(續)


SIFTWORKSTATION
sansforensics's Home
cases
mount_points
VMware-Shared-Drive
SIFT Cheat Sheet and DFIR Curriculum.pdf
SANS-DFIR-Poster-2012.pdf
ubiquity-gtkui.desktop
Tools Descriptions for SIFT Workstation 2.14.pdf
Windows to Unix Commands Cheatsheet.pdf
Network Forensics Cheat Sheet.pdf
Free DFIR Resources.pdf
log2timeline-cheatsheet.pdf
Memory-Forensics-Cheat-Sheet-v1.pdf
sansforensics@sansforensics: ~
File Edit View Terminal Help
sansforensics@sansforensics:~$
SANS COMPUTER FORENSICS and INCIDENT RESPONSE
sansforensics@sansfor...

鑑識工具介紹(續)


DEMO - VMware Player (Non-commercial use only)
Player
Applications
Places
System
Wed Apr 17, 6:13 PM
Accessories
BackTrack
Graphics
Internet
Office
Other
Sound & Video
System Tools
Wine
Information Gathering
Vulnerability Assessment
Exploitation Tools
Privilege Escalation
Maintaining Access
Reverse Engineering
RFID Tools
Stress Testing
Forensics
Reporting Tools
Services
Miscellaneous
Anti-Virus Forensics Tools
Digital Anti Forensics
Digital Forensics
Forensic Analysis Tools
Forensic Carving Tools
Forensic Hashing Tools
Forensic Imaging Tools
Forensic Suites
Network Forensics
Password Forensics Tools
PDF Forensics Tools
RAM Forensics Tools

鑑識工具介紹(續)

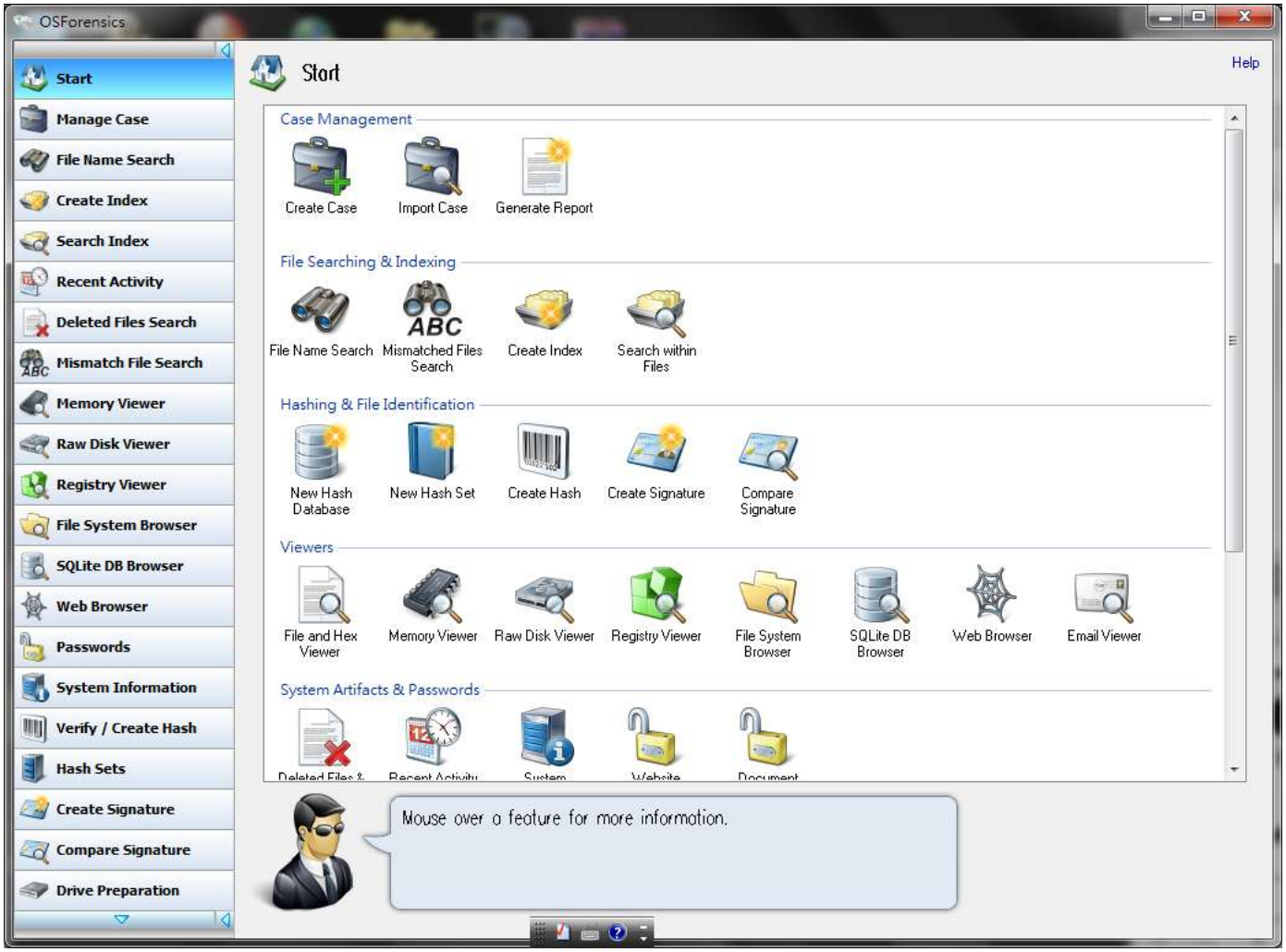

evidence
Install DEFT Linux 7
LXTerminal
Sha1sum
Sha256deep
Sha256sum
Sha512sum
SNMPcheck
SQLite database browser
Ssdeep
SSH Start
SSH Stop
Test Disk
theHarvester
Tor Browser
Traceroute
Trid
Usnjrnl-parser
Vinetto
Virus Scanner
VYM - View Your Mind
WebHTTrack Website Copier
WhatWeb
Wipe
Wireshark
Xmount
Xplico
xplico restart
xplico start
Xplico Start
xplico status
xplico stop
Xplico Stop
Xprobe2
Zenmap
Accessories
Graphics
Internet
Office
Other
Sound & Video
System Tools
Wine
Preferences
Run
Logout
LXDE
Lightweight X11 Desktop Environment
18:46

鑑識工具介紹(續)


DEMO - VMware Player (Non-commercial use only)
Player
DEMO - VMware Player (Non-commercial use only)
Accessories
Education
Forensic Tools
Graphics
Internet
Office
Other
Programming
Sound & Video
System Tools
Universal Access
Places
System
Lock Screen
Log Out caine...
Shut Down...
Mobile forensics
Network forensics
Mounter
Caine Interface
Guymager
AIR
Autopsy
Bash Scripts Tools
File Browser ROOT MODE
GTKHash
DVDisaster
Hex Editor
NBTempo
Remote Filesystem Mounter
Photorec
Fred
Mobius
QuickHash
Testdisk
PULSAR
C.A.IN.E.
Computer Aided for INvestigative Environment
en
0 B/s
0 B/s
Thu Apr 18, 01:44

鑑識工具介紹(續)

- OSForensics

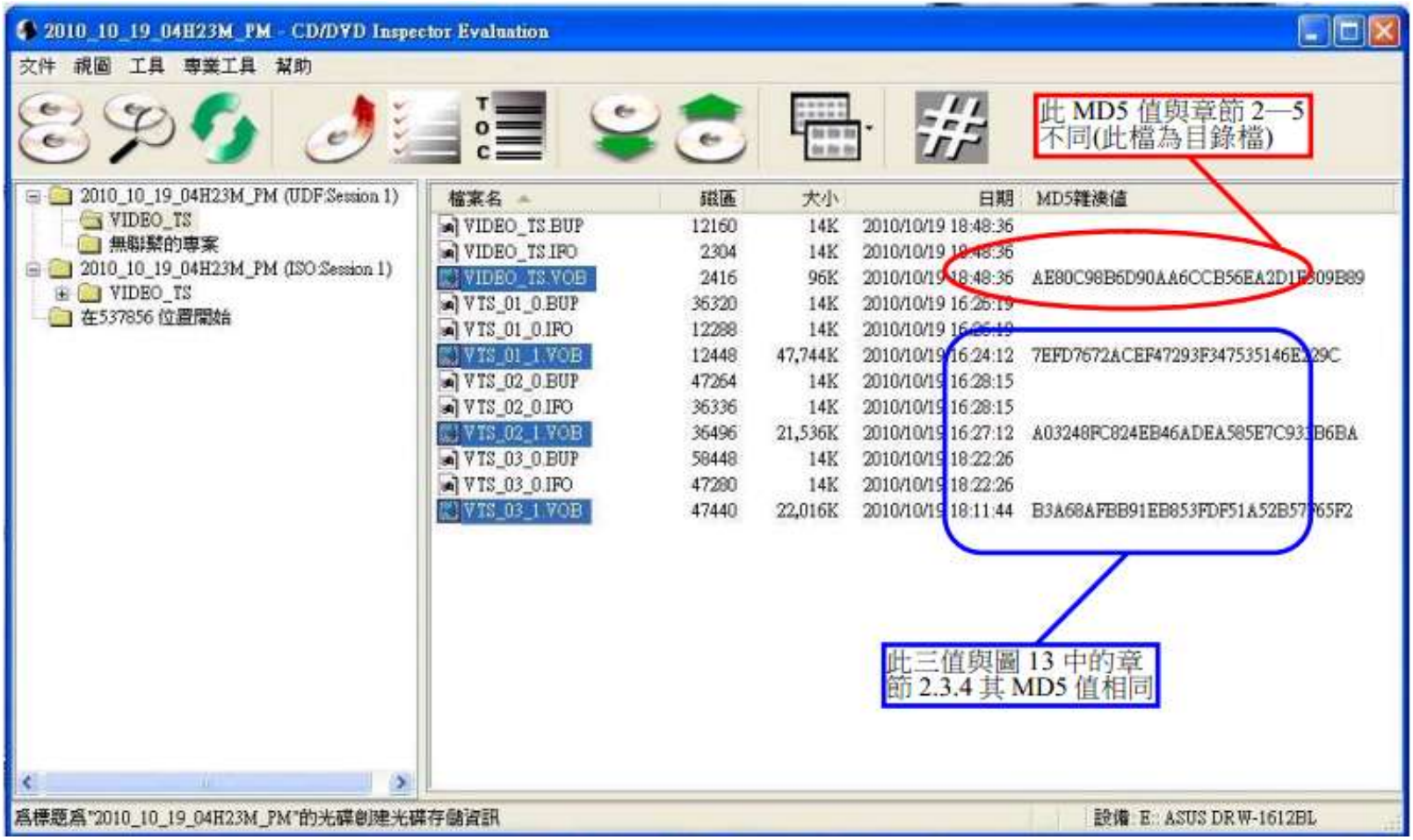


鑑識工具介紹(續)

- CD/DVD Inspector
  - 是一套光碟資料的回復及鑑識軟體，是由InfinaDyne公司發表

	CD/DVD Inspector	EnCase	FTK	ISO Buster	Fernico PRO Imager
Designed for optical media	✓			✓	✓
Supports all disc formats, all types – any disc	✓		✓	✓	✓
Automatically recovers lost and inaccessible data	✓			✓	
Accepts image files from a variety of sources	✓		✓	✓	
Extensive analysis showing when and how the disc was recorded	✓				
Court tested, reliable tool	✓	✓	✓		
Comprehensive built-in reporting	✓	✓	✓		
Knowledgeable telephone technical support	✓				
Supports automatic disc collection	✓				✓

鑑識工具介紹(續)


2010_10_19_04H23M_PM - CD/DVD Inspector Evaluation
文件 視圖 工具 專業工具 幫助
此 MD5 值與章節 2—5 不同(此檔為目錄檔)
2010_10_19_04H23M_PM (UDF Session 1)
VIDEO_TS
無關聯的專案
2010_10_19_04H23M_PM (ISO Session 1)
VIDEO_TS
在537856 位置開始
檔案名 磁區 大小 日期 MD5雜湊值
VIDEO_TS.BUP 12160 14K 2010/10/19 18:48:36
VIDEO_TS.IFO 2304 14K 2010/10/19 18:48:36
VIDEO_TS.VOB 2416 96K 2010/10/19 18:48:36 AE80C98B6D90AA6CCB56EA2D1F309B89
VTS_01_0.BUP 36320 14K 2010/10/19 16:26:19
VTS_01_0.IFO 12288 14K 2010/10/19 16:26:19
VTS_01_1.VOB 12448 47,744K 2010/10/19 16:24:12 7EFD7672ACEF47293F347535146E229C
VTS_02_0.BUP 47264 14K 2010/10/19 16:28:15
VTS_02_0.IFO 36336 14K 2010/10/19 16:28:15
VTS_02_1.VOB 36496 21,536K 2010/10/19 16:27:12 A03248FC824EB46ADEA585E7C93 B6BA
VTS_03_0.BUP 58448 14K 2010/10/19 18:22:26
VTS_03_0.IFO 47280 14K 2010/10/19 18:22:26
VTS_03_1.VOB 47440 22,016K 2010/10/19 18:11:44 B3A68AFBB91EB853FDF51A52B57 65F2
此三值與圖 13 中的章節 2.3.4 其 MD5 值相同
為標題爲"2010_10_19_04H23M_PM"的光碟創建光碟存儲資訊
設備: E: ASUS DRW-1612BL

Q & A

Thanks for your direction and advices.

We are delighted to discuss any question with you.

tsc 德欣
TSC CAPITAL GROUP
The Bridge to the Asia Pacific Region

Thank you

德欣寰宇科技股份有限公司 TSC TECHNOLOGIES, INC.

台北公司：台北市10059新生南路一段50號5樓500室
TEL: 886 2 2358 2775 · FAX:886 2 2358 3775

新竹公司：新竹市30046四維路130號2樓之2
TEL: 886 3 522 9570 · FAX:886 3 524 7507