

The Forensic Science in Cloud Computing

DOP Shiuh-Jeng WANG / 王旭正

- 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>



C'est La Via

- HAKUNA MATATA
- Information/Network Security
- Authentication and Forensics
- Computer/Network Forensics



Outline

- ICCL-FROG
- Introduction to Cloud Computing
(雲端運算介紹)
- Apply Forensics to Cloud Computing
(雲端鑑識之應用)
- Case Study
- Conclusions

MY FROG and the FROG with you

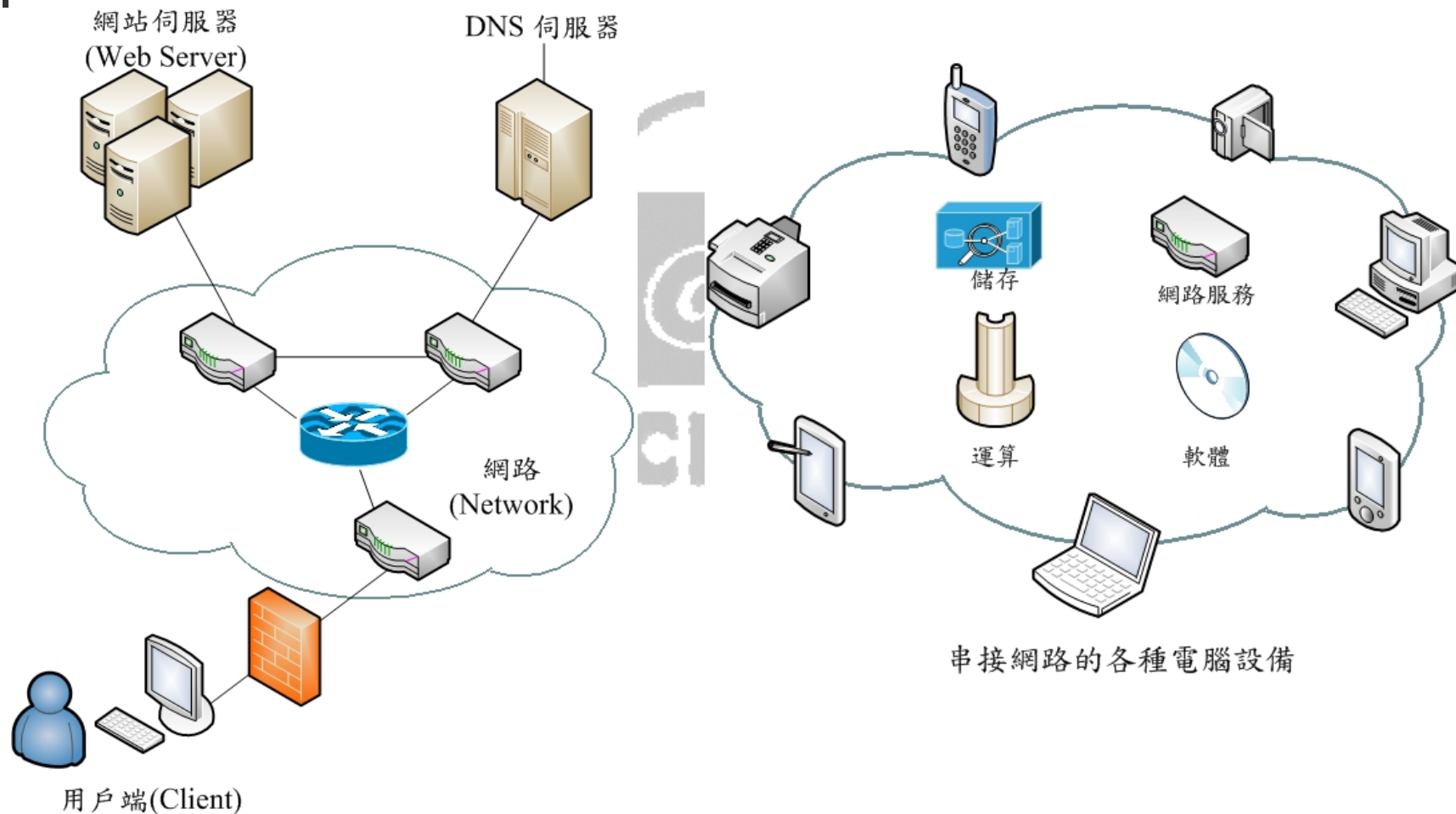




Outline

- ICCL-FROG
- Introduction to Cloud Computing
(雲端運算介紹)
- Apply Forensics to the Cloud Computing
(雲端鑑識之應用)
- Case Study
- Conclusions

Update to Cloud Environments



What is the cloud computing?

- NIST's **Definition**
 - Ubiquitous(無所不在)
 - Convenient(便利性)
 - On-demand (隨選即用)
- Key **Factors** to the Cloud Computing
 - 硬體與軟體皆是資源，透過網際網路提供服務
 - 資源動態調整
 - 分散虛擬架構
 - 依時付費，以量計價



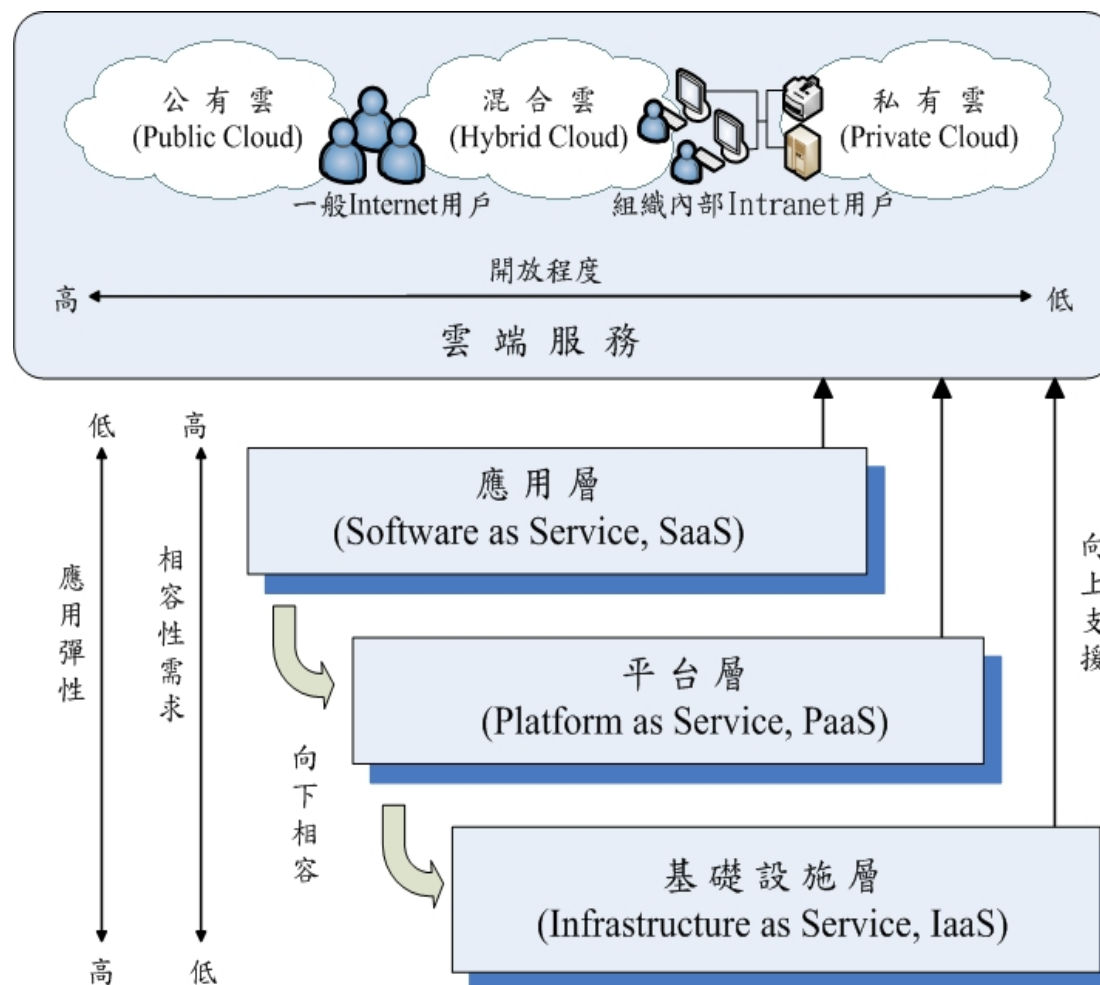
The **Evolution** of Cloud Computing

- Distributed Computing(分散式運算)
- Grid Computing(網格運算)
- Utility Computing(公用運算)
- Software as a Service(軟體即服務)
- Cloud Computing(雲端運算)

Classification of Cloud Computing

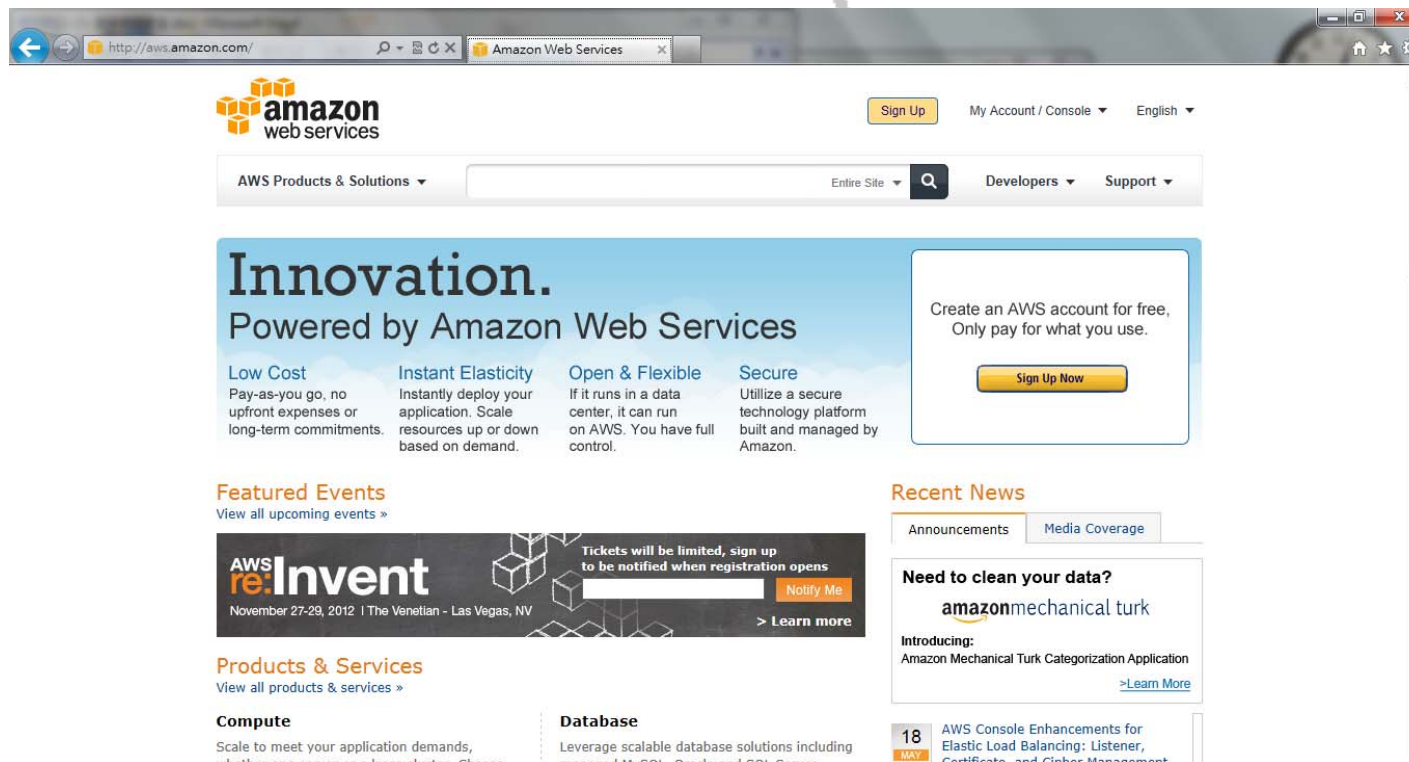
- 依提供者與使用者關係
 - Public Cloud(公有雲)
 - Private Cloud(私有雲)
 - Hybrid Cloud(混合雲)
- 依提供服務種類
 - Infrastructure as a Service (IaaS, 基礎設施雲)
 - Platform as a Service (PaaS, 平台雲)
 - Software as a Service (SaaS, 應用雲)

Classification of Cloud Computing



Cloud Service Application – Amazon

- EC2(Elastic Comput Cloud)- IaaS
- AWS(Amazon Web Service) : S3 、 RDS 、 Cloud Player(SaaS)



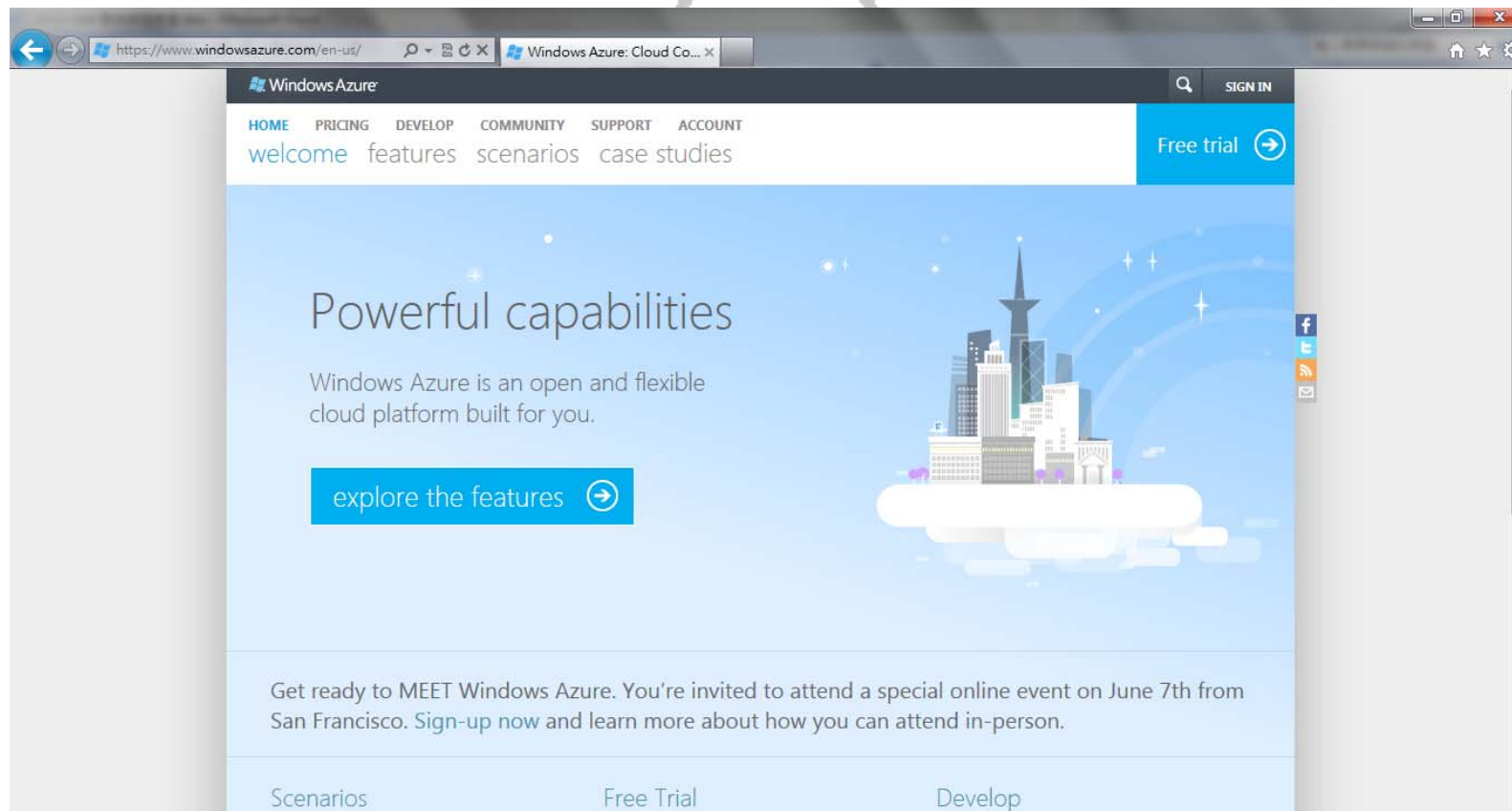
Cloud Service Application – Google App Engine

- GAE- PaaS
- Eclipse : Python, Java, Go



Cloud Service Application – Windows Azure

- PaaS
- Visual Studio 2010 – Tools for Azure





Outline

- ICCL-FROG
- Introduction to Cloud Computing
(雲端運算介紹)
- **Apply Forensics to Cloud Computing**
(雲端鑑識之應用)
- Case Study
- Conclusions

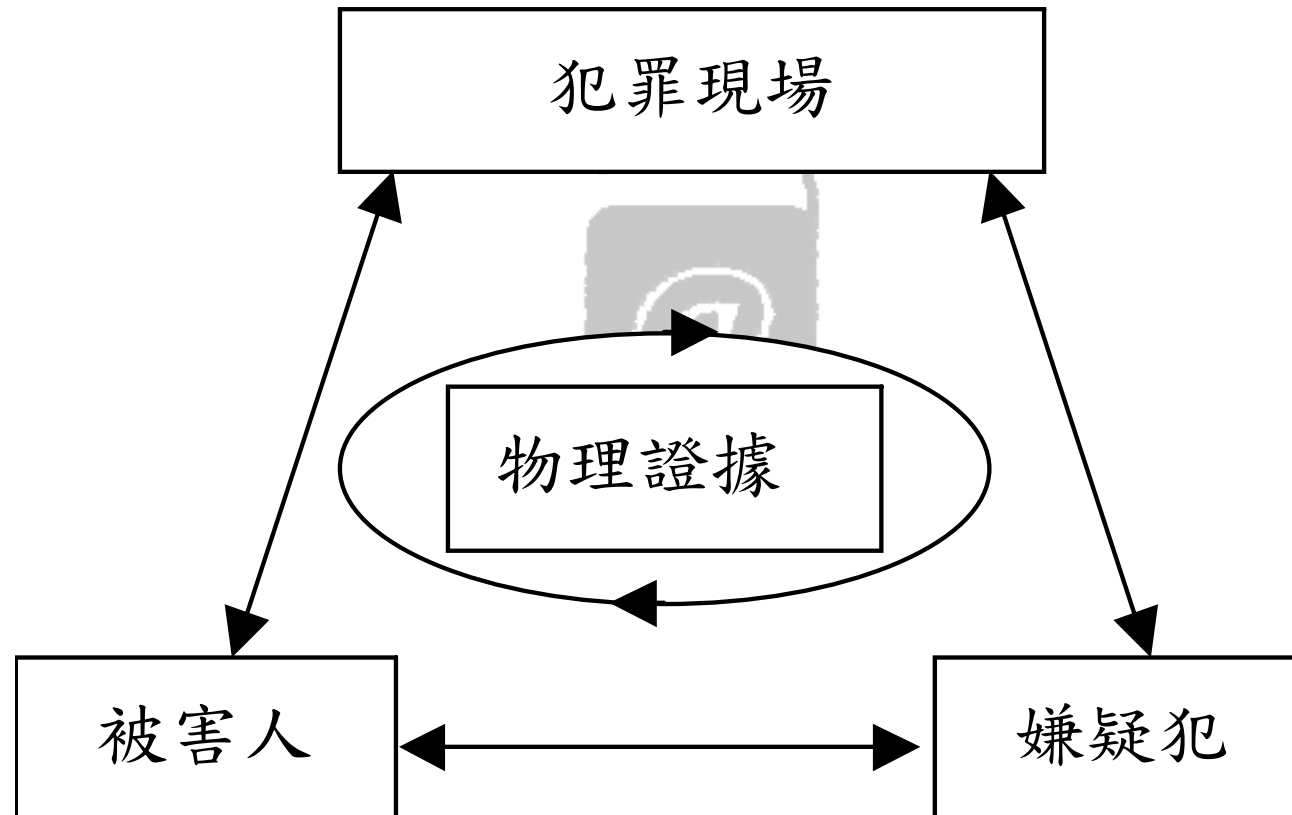


Forensic Science

- 定義
 - 運用科學於執法
 - 科學: 化學, 生物學, 物理學, 地理學, ...
- 目標: 確定**犯罪現場及相關證物之證據能力**

ICCL@B

Forensic Science (Locards's Exchange Principle)



Computer Forensics

(Warren, G. Kruse ii and Jay G. Heiser, 2002, *Computer Forensics – Incident Response Essentials*, Addison Wesley)

- 定義：
 - 以周延的方法及程序保存, 識別, 抽取, 記載, 及解讀電腦媒體證據與分析其成因之科學
- 方法與基本原則：
 - 在不改變或破壞證物的情況下取得原始證物
 - 證明所抽取的證物來自扣押的證物
 - 在不改變證物的情況下進行分析

Example to Digital Information

- 通聯紀錄
- 交易紀錄(如提款、購物、轉帳等等)
- 電子郵件備份
- 網路連線紀錄
- BBS 備份
- 機密文件



Digital Forensics

- 數位鑑識工作的目的為擷取、整理、分析這些和犯罪行為有關的資訊，並讓這些資訊在調查程序中還原真相，而使之具有證據能力。
- 數位鑑識的程序，目前的法律還沒有一定之規範，因此，如何讓鑑識的程序合法化一直是目前數位鑑識工作者努力的目標。



The purpose of Digital Forensics

- 確認嫌犯
- 起訴犯罪者
- 保護無辜
- 了解犯罪行為與動機



Digital Evidence

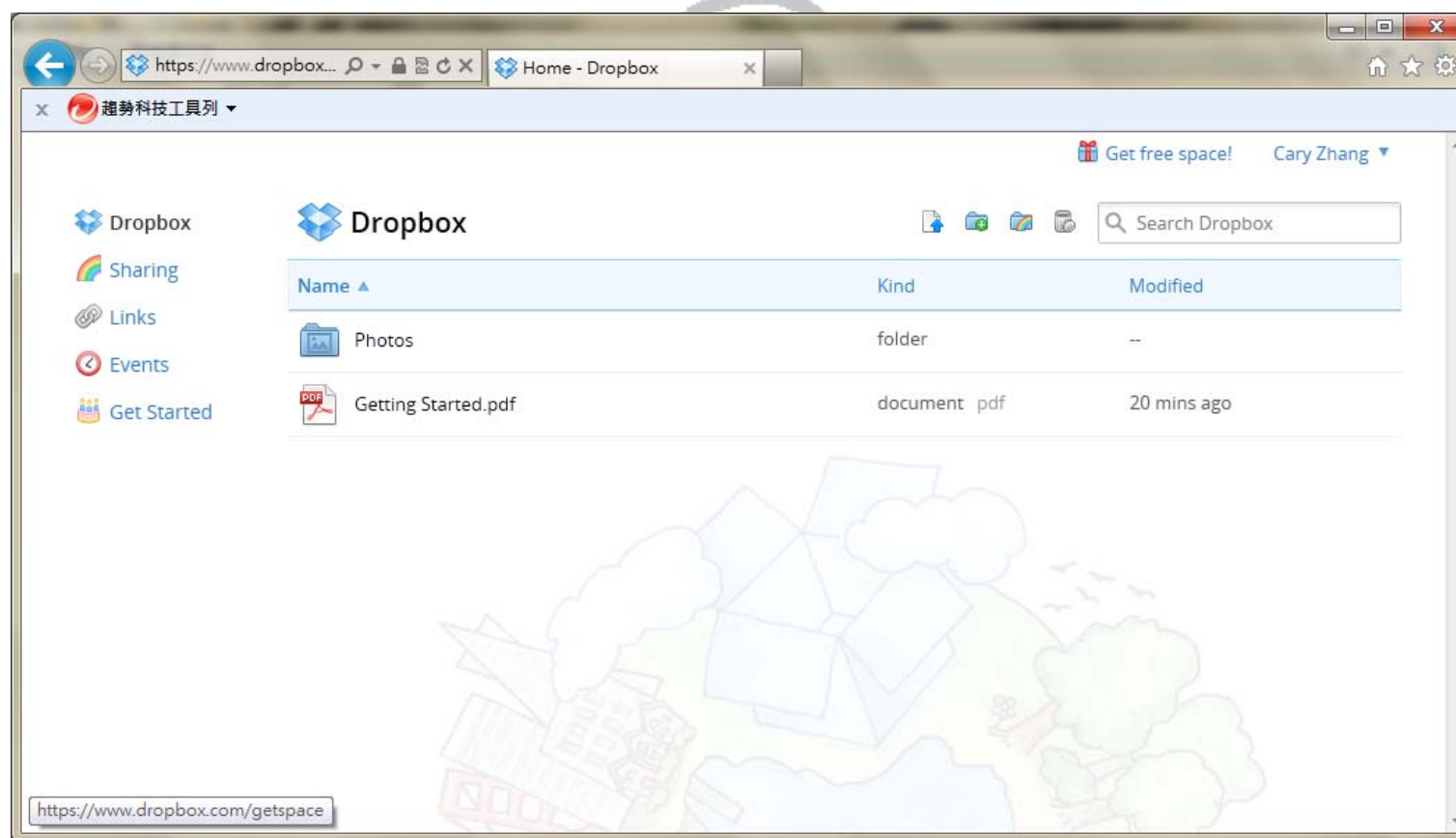
- 「數位證據」指存在於電子儲存媒體中的**磁性狀態、數位訊號**等資料，憑藉這些證據可與電腦犯罪做連結。
- 數位證據具有下列幾項特色：
 - 現代化
 - 多樣化
 - 不穩定性

Digital Evidence vs. Physical Evidence

- 為物理證據之一種
- 易於複製與修改
- 不易證實其來源及完整性
- 無法直接被人類所感知、理解的內容

Apply Forensic Science to Cloud Computing

■ A Cloud Service – Dropbox



Apply Forensic Science to Cloud Computing

- Dropbox Services
 - Storing files in Cloud(檔案儲存與同步)
 - Sharing folders(檔案共享)
 - Back up files(檔案備份)
 - Safety and Privacy(安全及隱私)
 - Mobile Access(手機存取)
- Question : How to apply Forensic Science to Dropbox?



Outline

- ICCL-FROG
- Introduction to Cloud Computing
(雲端運算介紹)
- Apply Forensics to Cloud Computing
(雲端鑑識之應用)
- Case Study
- Conclusions

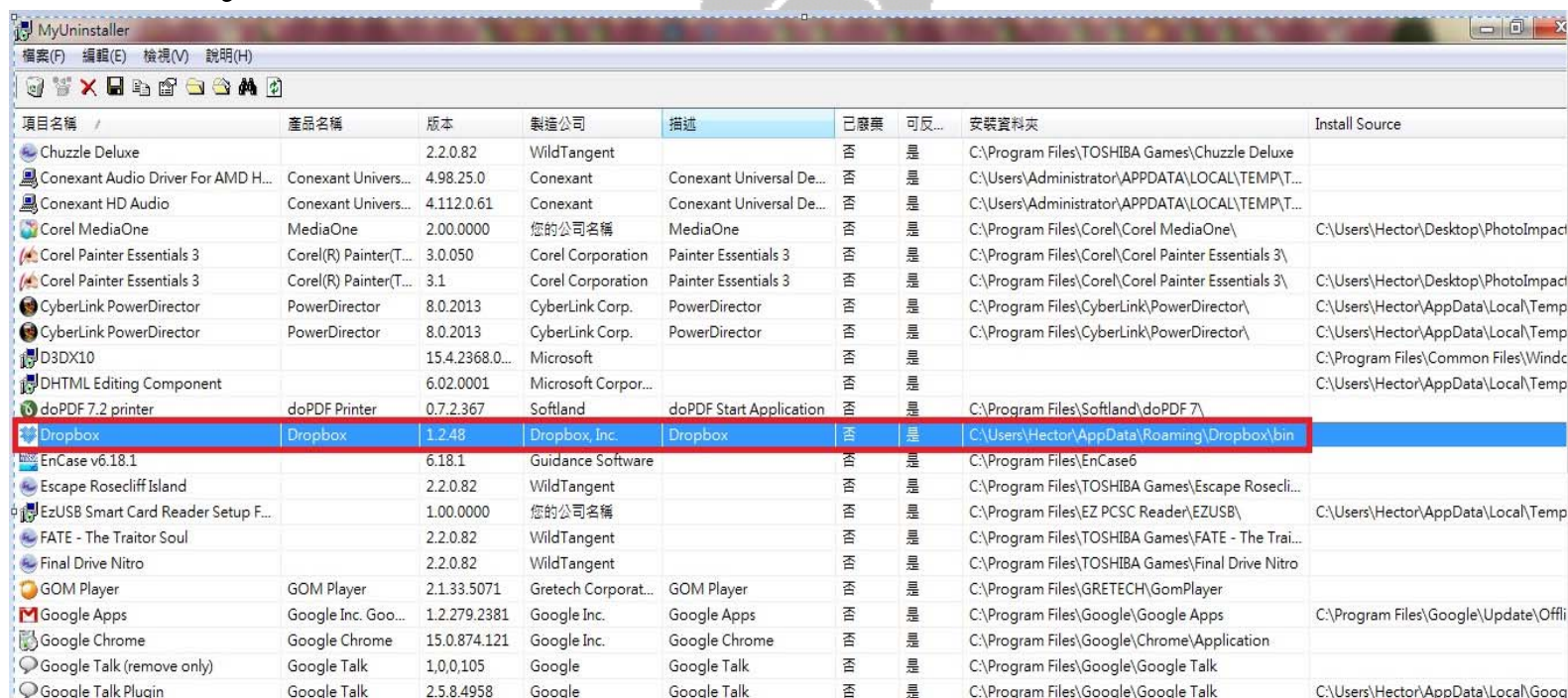
Case Study

■ 案例說明：

- 執法單位偵辦一起手機販毒案，嫌犯利用手機上網功能，將販毒交易明細儲存至網路空間，以利隨時掌握毒品買賣狀況。
- 鑑識人員要將手機進行扣押鑑識時，嫌犯竟將手機破壞，使之鑑識人員無法從手機中萃取相關數位跡證。
- 鑑識人員遂往嫌犯住處，扣押嫌犯平日所使用的電腦，進行鑑識。在鑑識過程中，發現嫌疑犯有安裝 Dropbox，判斷嫌犯應是利用此軟體進行網路毒品交易。

Case Study (Cont.)

- 檢視數位跡證
 - 檢查Dropbox的捷徑或連結檔。(使用MyUninstaller)



項目名稱	產品名稱	版本	製造公司	描述	已廢棄	可反...	安裝資料夾	Install Source
Chuzzle Deluxe		2.2.0.82	WildTangent		否	是	C:\Program Files\TOSHIBA Games\Chuzzle Deluxe	
Conexant Audio Driver For AMD H...	Conexant Univers...	4.98.25.0	Conexant	Conexant Universal De...	否	是	C:\Users\Administrator\AppData\LOCAL\TEMP\T...	
Conexant HD Audio	Conexant Univers...	4.112.0.61	Conexant	Conexant Universal De...	否	是	C:\Users\Administrator\AppData\LOCAL\TEMP\T...	
Corel MediaOne	MediaOne	2.00.0000	您的公司名稱	MediaOne	否	是	C:\Program Files\Corel\Corel MediaOne\	C:\Users\Hector\Desktop\PhotoImpact
Corel Painter Essentials 3	Corel(R) Painter(T...	3.0.050	Corel Corporation	Painter Essentials 3	否	是	C:\Program Files\Corel\Corel Painter Essentials 3\	C:\Users\Hector\Desktop\PhotoImpact
Corel Painter Essentials 3	Corel(R) Painter(T...	3.1	Corel Corporation	Painter Essentials 3	否	是	C:\Program Files\Corel\Corel Painter Essentials 3\	C:\Users\Hector\Desktop\PhotoImpact
CyberLink PowerDirector	PowerDirector	8.0.2013	CyberLink Corp.	PowerDirector	否	是	C:\Program Files\CyberLink\PowerDirector\	C:\Users\Hector\AppData\Local\Temp
CyberLink PowerDirector	PowerDirector	8.0.2013	CyberLink Corp.	PowerDirector	否	是	C:\Program Files\CyberLink\PowerDirector\	C:\Users\Hector\AppData\Local\Temp
D3DX10		15.4.2368.0...	Microsoft		否	是		C:\Program Files\Common Files\Windc
DHTML Editing Component		6.02.0001	Microsoft Corpor...		否	是		C:\Users\Hector\AppData\Local\Temp
doPDF 7.2 printer	doPDF Printer	0.7.2.367	Softland	doPDF Start Application	否	是	C:\Program Files\Softland\doPDF 7\	
Dropbox	Dropbox	1.2.48	Dropbox, Inc.	Dropbox	否	是	C:\Users\Hector\AppData\Roaming\Dropbox\bin	
EnCase v6.18.1		6.18.1	Guidance Software		否	是	C:\Program Files\EnCase6	
Escape Rosecliff Island		2.2.0.82	WildTangent		否	是	C:\Program Files\TOSHIBA Games\Escape Rosecli...	
EzUSB Smart Card Reader Setup F...		1.00.0000	您的公司名稱		否	是	C:\Program Files\EZ PCSC Reader\EZUSB\	C:\Users\Hector\AppData\Local\Temp
FATE - The Traitor Soul		2.2.0.82	WildTangent		否	是	C:\Program Files\TOSHIBA Games\FATE - The Trai...	
Final Drive Nitro		2.2.0.82	WildTangent		否	是	C:\Program Files\TOSHIBA Games\Final Drive Nitro	
GOM Player	GOM Player	2.1.33.5071	Gretech Corporat...	GOM Player	否	是	C:\Program Files\GRETECH\GomPlayer	
Google Apps	Google Inc. Goo...	1.2.279.2381	Google Inc.	Google Apps	否	是	C:\Program Files\Google\Google Apps	C:\Program Files\Google\Update\Offi
Google Chrome	Google Chrome	15.0.874.121	Google Inc.	Google Chrome	否	是	C:\Program Files\Google\Chrome\Application	
Google Talk (remove only)	Google Talk	1.0.0.105	Google	Google Talk	否	是	C:\Program Files\Google\Google Talk	
Google Talk Plugin	Google Talk	2.5.8.4958	Google	Google Talk	否	是	C:\Program Files\Google\Google Talk	C:\Users\Hector\AppData\Local\Goo

Case Study (Cont.)

- 檢查上網紀錄
 - 瀏覽歷程、cookie



The screenshot shows the CNET Download.com page for 'Web Historian'. The page features a red header with the CNET logo and navigation links. A green box highlights the 'Start Download' button. Below this, a list of steps for installation is provided. The main content area includes a 'Download Now' button, a 'CNET Editors' review' section with a 5-star rating, and a detailed description of the software's features and requirements.

3 Steps for a faster install & scan

1. Click "Start Download"
2. Run the quick scan
3. Scan & Fix up to 100 errors

Start Download

Home > Windows Software > Security Software > Corporate Security Software > Web Historian

Web Historian

Download Now
CNET Secure Download

CNET Editors' review
by: CNET Staff on February 27, 2009

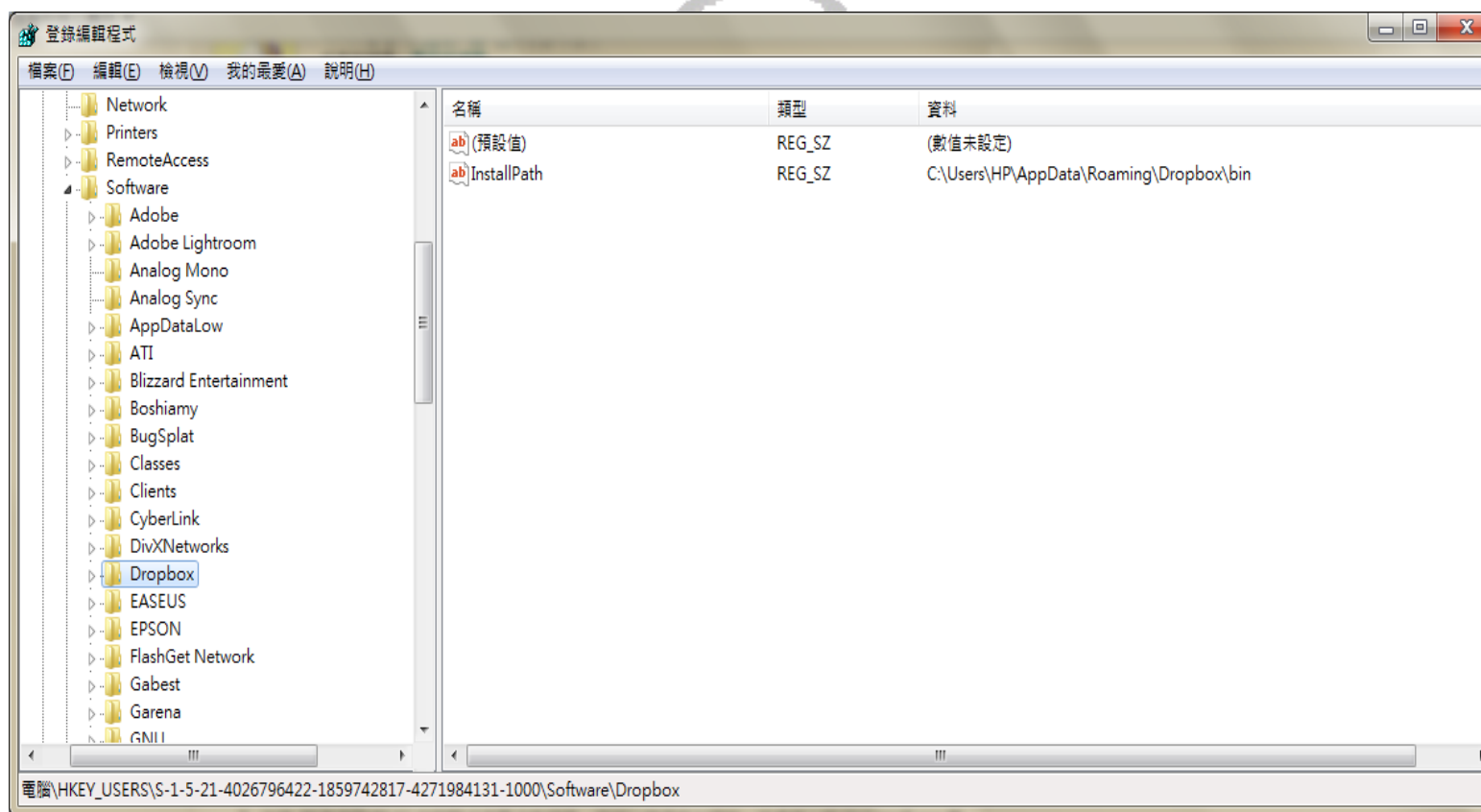
CNET Editors' Rating:
★★★★★
Good

Average User Rating:
★★★★★

Web Historian gives a detailed report of browser history, although it locked up repeatedly before spitting out the facts. The program needs nearly 20MBs to download, and requires a quick registration during the installation. The small, unimaginative interface cuts to the chase with two simple options: you can search by specific browser history files, or search a directory and its subdirectories.

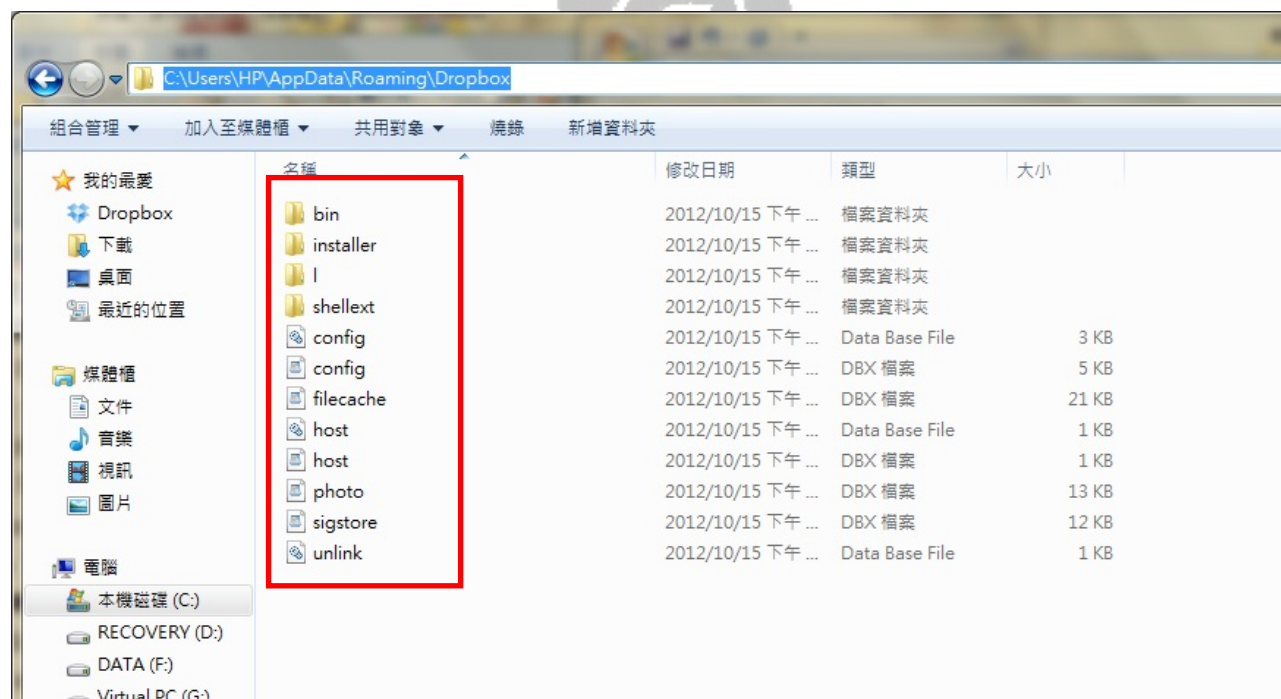
Case Study (Cont.)

■ 檢查註冊機碼(Registry)



Case Study (Cont.)

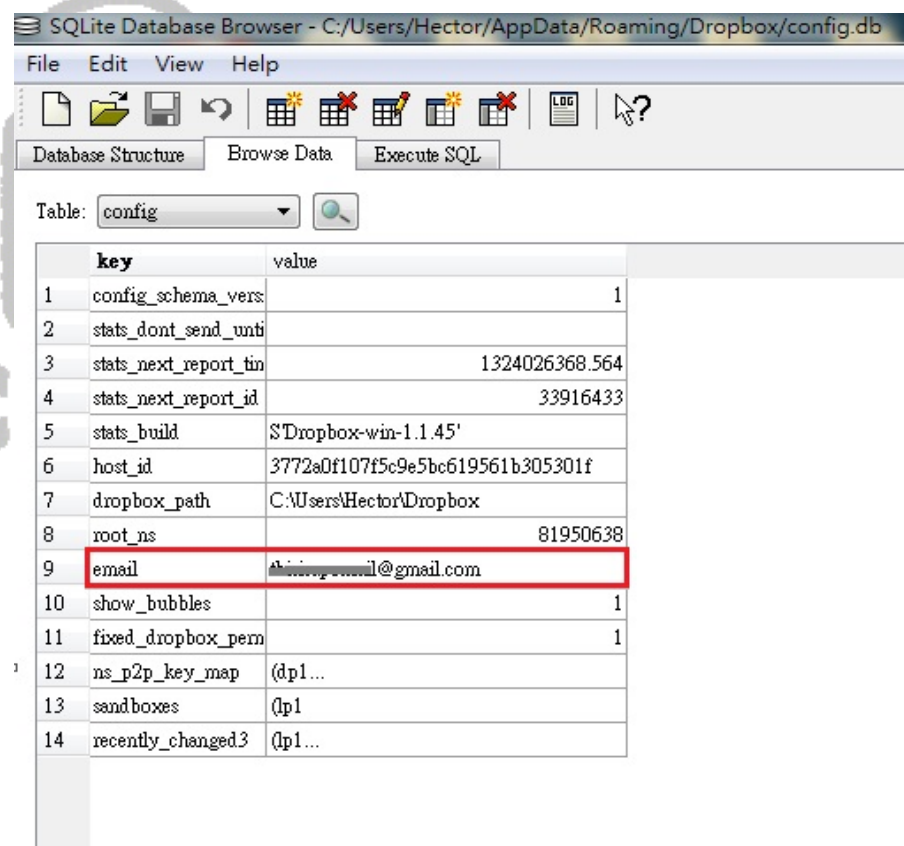
- 檢查安裝紀錄路徑
 - WinXP：「Documents and Settings/username/Application Data/Dropbox」
 - Win7：「Users/username/AppData/Roaming/Dropbox」



Case Study (Cont.)

■ 檢視Dropbox系統資訊

- config.db
- SQLite Database Browser



SQLite Database Browser - C:/Users/Hector/AppData/Roaming/Dropbox/config.db

File Edit View Help

Database Structure Browse Data Execute SQL

Table: config

	key	value
1	config_schema_vers	1
2	stats_dont_send_until	
3	stats_next_report_time	1324026368.564
4	stats_next_report_id	33916433
5	stats_build	'SDropbox-win-1.1.45'
6	host_id	3772a0f107f5c9e5bc619561b305301f
7	dropbox_path	C:\Users\Hector\Dropbox
8	root_ns	81950638
9	email	thirup@gmail.com
10	show_bubbles	1
11	fixed_dropbox_perm	1
12	ns_p2p_key_map	(dp1...
13	sandboxes	(p1
14	recently_changed3	(p1...

Case Study (Cont.)

- 檢視Dropbox系統資訊
- filecache.db

SQLite Database Browser - C:/Users/Hector/AppData/Roaming/Dropbox/filecache.db

File Edit View Help

Database Structure Browse Data Execute SQL

Table: file_journal

	id	server_path	parent_path	extra_pending_d	local_sjid	local_filename	local_blocklist	local_size	local_mtime	local_ctime
1	1	81950638:/photos	81950638:/		4376917934	Photos		0	1322122697	1322122697
2	2	81950638:/public	81950638:/		8671885230	Public		0	1322743271	1322122697
3	3	81950638:/photos/sample album	81950638:/photos		12966852526	Sample Album		0	1322122697	1322122697
4	9	81950638:/photos/sample album/boston city flow.jpg	81950638:/photos/sample album		17261819822	Boston City Flow.jpg	7GWhCh6IZM638	339773	1322122092	1322122697
5	10	81950638:/photos/sample album/pensive parakeet.jpg	81950638:/photos/sample album		21556787118	Pensive Parakeet.jpg	HM183nQwcIF6t1Pr	480098	1322122092	1322122697
6	11	81950638:/photos/sample album/costa rican frog.jpg	81950638:/photos/sample album		25851754414	Costa Rican Frog.jpg	kubgE06V6VVeGjII	354633	1322122092	1322122697
7	12	81950638:/getting started.pdf	81950638:/		30146721710	Getting Started.pdf	in2XAozYmKJ7yQz	246000	1322122092	1322122697
8	13	81950638:/photos/how to use the photos folder.txt	81950638:/photos		34441689006	How to use the Photos folder.txt	VI97MyT2ml15950	567	1322122092	1322122697
9	23	81950638:/accl	81950638:/		339384367022	ICCL		0	1323085420	1323085420
10	39	81950638:/memories	81950638:/		433873647534	memories		0	1322474881	1322474881
11	81	81950638:/雙桃小丸子	81950638:/		713046521774	雙桃小丸子		0	1326676743	1326676743
12	82	81950638:/雙桃小丸子/藥丸頭兒.docx	81950638:/雙桃小丸子		725931423662	藥丸頭兒.docx		0	1326676803	1326676803
13	83	81950638:/雙桃小丸子/那一天，我們一起嗑藥的日子.docx	81950638:/雙桃小丸子		738816325550	那一天，我們一起嗑藥的日子.docx		0	1326676852	1326676852
14	84	81950638:/雙桃小丸子/翻滾吧，小丸.docx	81950638:/雙桃小丸子		751701227438	翻滾吧，小丸.docx		0	1326676938	1326676938
15	85	81950638:/accl/丸子歷史.rar	81950638:/accl	("mount_request": n	0	丸子歷史.rar	p3ULZiTLjtKvMY8	32772678	1326677283	1326677277
16	86	81950638:/memories/大伏兒的錢.rar	81950638:/memories	("mount_request": n	0	大伏兒的錢.rar	LSMPCoDHazXGIsX	3980278	1326677434	1326677434
17	87	81950638:/public/不能說的秘密.rar	81950638:/public		949269723054	不能說的秘密.rar	V1M2xAvllG_OuIV	28985817	1325751233	1325751260

Case Study (Cont.)

■ 利用連線狀態檢查

- netstat -an
- TCPView

TCPView - Sysinternals: www.sysinternals.com

File Options Process View Help

Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Packets	Sent Bytes	Rcvd Packets	Rcvd Bytes
chrome.exe	4480	TCP	hector-pc	49884	nut19s17-in-f26.1e10...	http	ESTABLISHED				
chrome.exe	4480	TCP	hector-pc	49885	nut19s17-in-f26.1e10...	http	ESTABLISHED				
chrome.exe	4480	TCP	hector-pc	49886	202.169.174.219	https	ESTABLISHED				
Droptbox.exe	5596	TCP	Hector-PC	17500	Hector-PC	0	LISTENING	10	1,110	10	1,110
Droptbox.exe	5596	TCP	Hector-PC	19872	localhost	49165	ESTABLISHED				
Droptbox.exe	5596	TCP	Hector-PC	49165	localhost	19872	ESTABLISHED				
Droptbox.exe	5596	TCP	hector-pc	49166	v-client-3a.sjc.droptb...	https	CLOSE_WAIT				
Droptbox.exe	5596	TCP	hector-pc	49167	sjo-not2.sjc.droptbox...	http	ESTABLISHED	1	192	1	179
Droptbox.exe	5596	UDP	Hector-PC	17500	*	*					
dsNcService.exe	1912	TCP	Hector-PC	4242	Hector-PC	0	LISTENING				
GoogleDesktop...	3920	TCP	Hector-PC	4664	Hector-PC	0	LISTENING				
GoogleDesktop...	3920	TCP	hector-pc	49811	64.4.11.252	http	ESTABLISHED				
hasplms.exe	912	TCP	Hector-PC	1947	Hector-PC	0	LISTENING			4	160
hasplms.exe	912	UDP	Hector-PC	1947	*	*					
hasplms.exe	912	UDP	Hector-PC	50520	*	*		4	160		
hasplms.exe	912	TCPV6	hector-pc	1947	hector-pc	0	LISTENING				
hasplms.exe	912	UDPV6	hector-pc	1947	*	*					
lsass.exe	592	TCP	Hector-PC	49155	Hector-PC	0	LISTENING				
lsass.exe	592	TCPV6	hector-pc	49155	hector-pc	0	LISTENING				
services.exe	564	TCP	Hector-PC	49156	Hector-PC	0	LISTENING				
services.exe	564	TCPV6	hector-pc	49156	hector-pc	0	LISTENING				
SfCtlCom.exe	2320	TCP	Hector-PC	37848	Hector-PC	0	LISTENING				

Case Study (Cont.)

■ 案例說明

- 手機販毒案，嫌犯利用手機上網功能，將販毒交易明細儲存至網路空間，以利隨時掌握毒品買賣狀況。
- 鑑識人員逐往嫌犯住處，扣押嫌犯平日所使用的電腦，進行鑑識。在鑑識過程中，發現嫌疑犯有安裝Dropbox，判斷嫌犯應是利用此軟體進行網路毒品交易。

鑑識方法	數位跡證
MyUninstaller	Dropbox捷徑及安裝紀錄
Web Historian	網路瀏覽歷程、cookie
Registry	程式安裝或反安裝紀錄
搜尋安裝路徑	應用程式執行檔、組態檔
Dropbox系統資訊分析 - config.db	E-mail帳號
Dropbox系統資訊分析 - filecache.db	上傳/下載檔案紀錄、存取位置
netstat - an TCPView	Dropbox服務連線運作情形

Conclusions

- **雲端概念**改變了應用程式的使用方式，透過網路連線至雲端平台，用戶可**隨時**取得各種**服務資源**。
- 新型態的網路應用使得嫌犯在利用雲端服務從事犯罪時，**犯罪跡證**易隱藏，增加辦案人員鑑識的困難度。
- 鑑識人員採取各種鑑識方法，發現相關數位痕跡，描繪犯罪流程，提供**關鍵鑑識報告**。



- **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 (Forensic Research development task force Group)
- 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/uicuiipm2012/> 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)