FINSEC Forum

通往金融網路安全之事件反應和數位鑑識路徑

高大宇 教授/博士

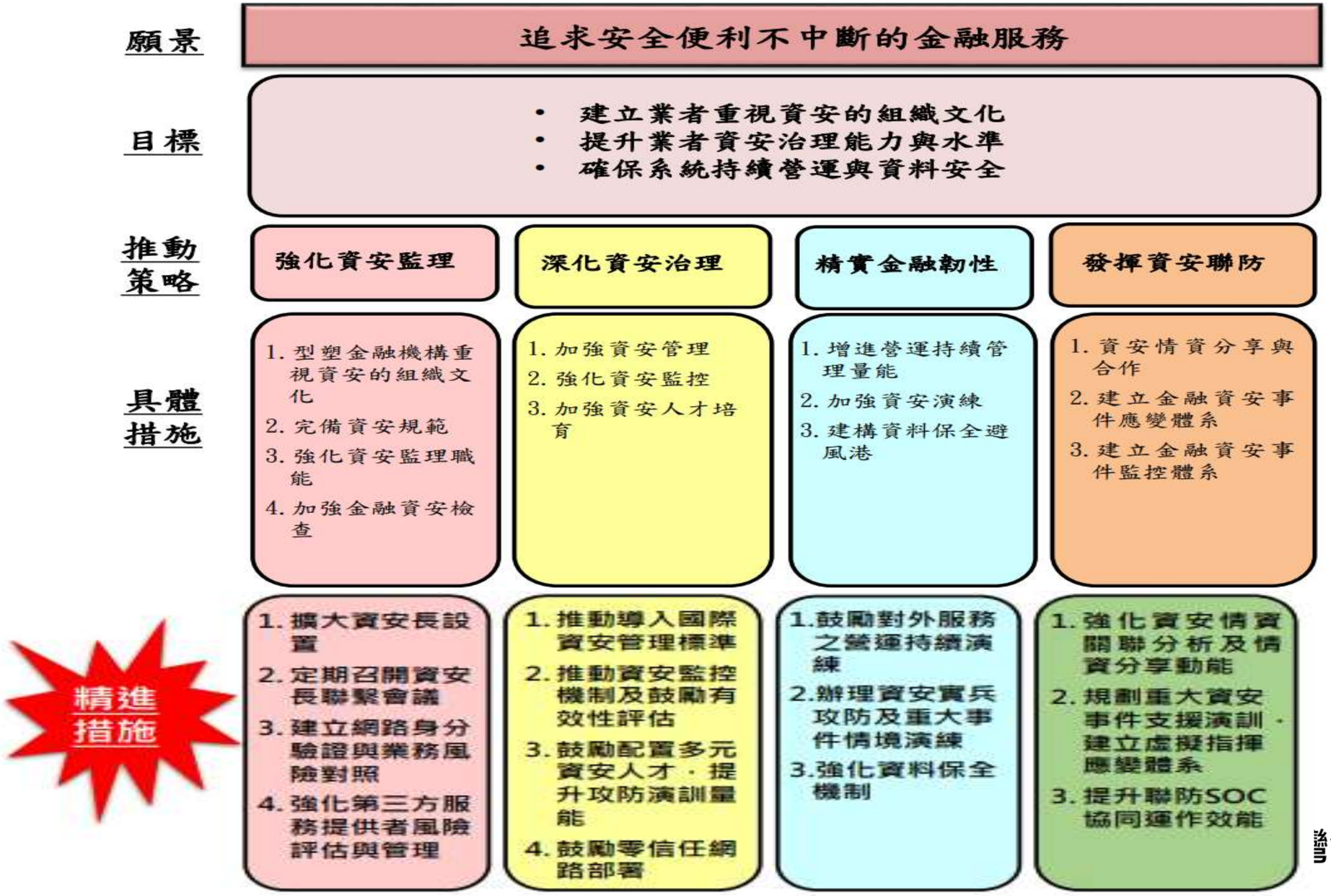
永豐銀行資訊安全處 副總經理/副處長
台灣資安主管聯盟 副會長

大綱

1.金融網路安全
2.數位鑑識
3.資安事件反應
4.案例分析
5.結語

1.金融網路安全

金融資安行動方案1.0->2.0



來源：金管會

2.數位鑑識

追查嫌犯的稽核紀錄四要件

編號	要件	理由	目標
1	來源網址 (IP addresses)	追查來源電腦帳號或電話號碼	鎖定涉案嫌犯的犯罪行為
2	時間戳記(timestamp)		
3	數位動作 (digital action)	檢查犯罪構成要件的該當或合致	
4	系統訊息 (system response)		

數位證據的特性

格式多樣性	• 數位資料存於各種電腦儲存媒體 • 聲音檔、影像檔、文字檔或其他格式檔案
資料發散性	• 網際網路網網相連，數位紀錄散置全世界 • 執法機關跨國合作，7天24小時熱線合作。
難辨真實性	• 數位記錄容易修改、複製或刪除 • 不易證明數位資料的來源真實性。
證據動態性	• 數位資料易變動，加深調查困難度。 • 特殊知識(專業)、技術(工具)與能力(訓練)。
關係連結性	• 常缺充分、完整的軌跡、紀錄、線索。 • 將特定人事時地物資料交叉驗證/比對(Cross-reference)，放在一起(Put it all together) • 輔以時間(Temporal)、功能(Functional)或關聯性(Relational)分析，找前後脈絡，還原(重建)事件原貌

3.資安事件反應

(1)三道防線-內外部問責制度的差異分析

	人員差異	情資分享	程序防弊
犯罪預防 內部 詐欺舞弊 理專十誡	內部業務人員 (職員、實習生)	具私密性 資訊交流不足	熟悉內部程序 規避相關規範
外部 洗錢風險	外部人員 (客戶、廠商)	眾多指導文件 可疑交易行的 為監控態樣	透過程序規範 有效防制

來源： https://www.pwc.tw/zh/topics/risk-management/risk-management-20201030.html

(2)資安事件通報主管機關

資安事件通報性質 1

勒索病毒、個人資料或財務資料被洩漏，可能會影響個人隱私或金融安全。如含敏感資料，具更高的通報必要性。

應通報門檻程度 2

應律定通報門檻程度，如機密性、完整性及可用性(營運中斷期間)。

通報時機與方式 3

通報主管機關的時機與方式，依據當地法律與規定進行判斷。

法律責任 4

某些國家，企業須在一定時間內報告相關情況。未及時通報，可能面臨法律責任或罰責。

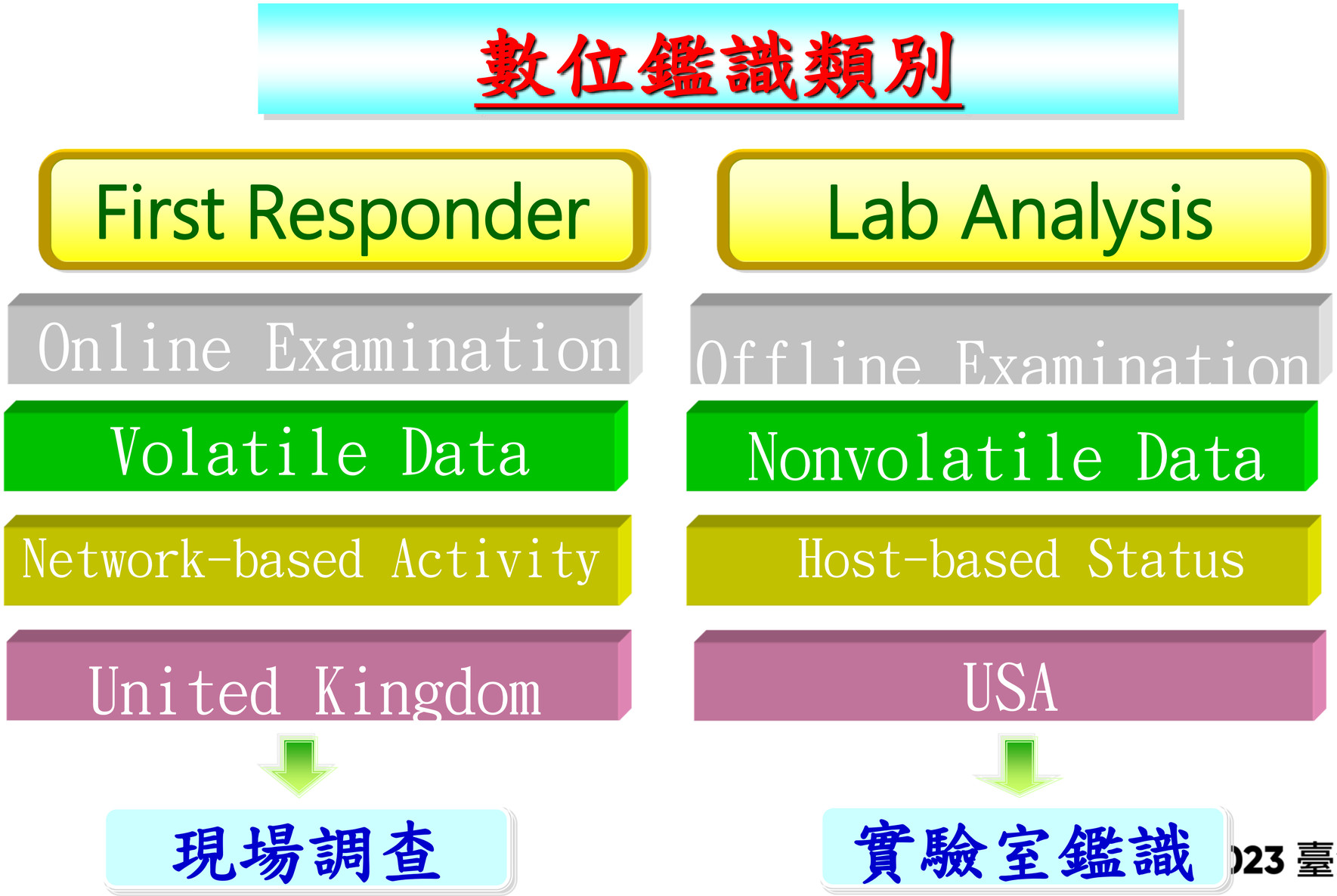
獲得專業協助與指導 5

可進一步調查與追蹤，有助提高事件處理效率與準確性。

例外管理 6

若未達通報門檻，依企業自身資安政策，內部處理及調查，降低類似復發風險。

(3)數位鑑識：類別-現場調查與實驗室鑑識



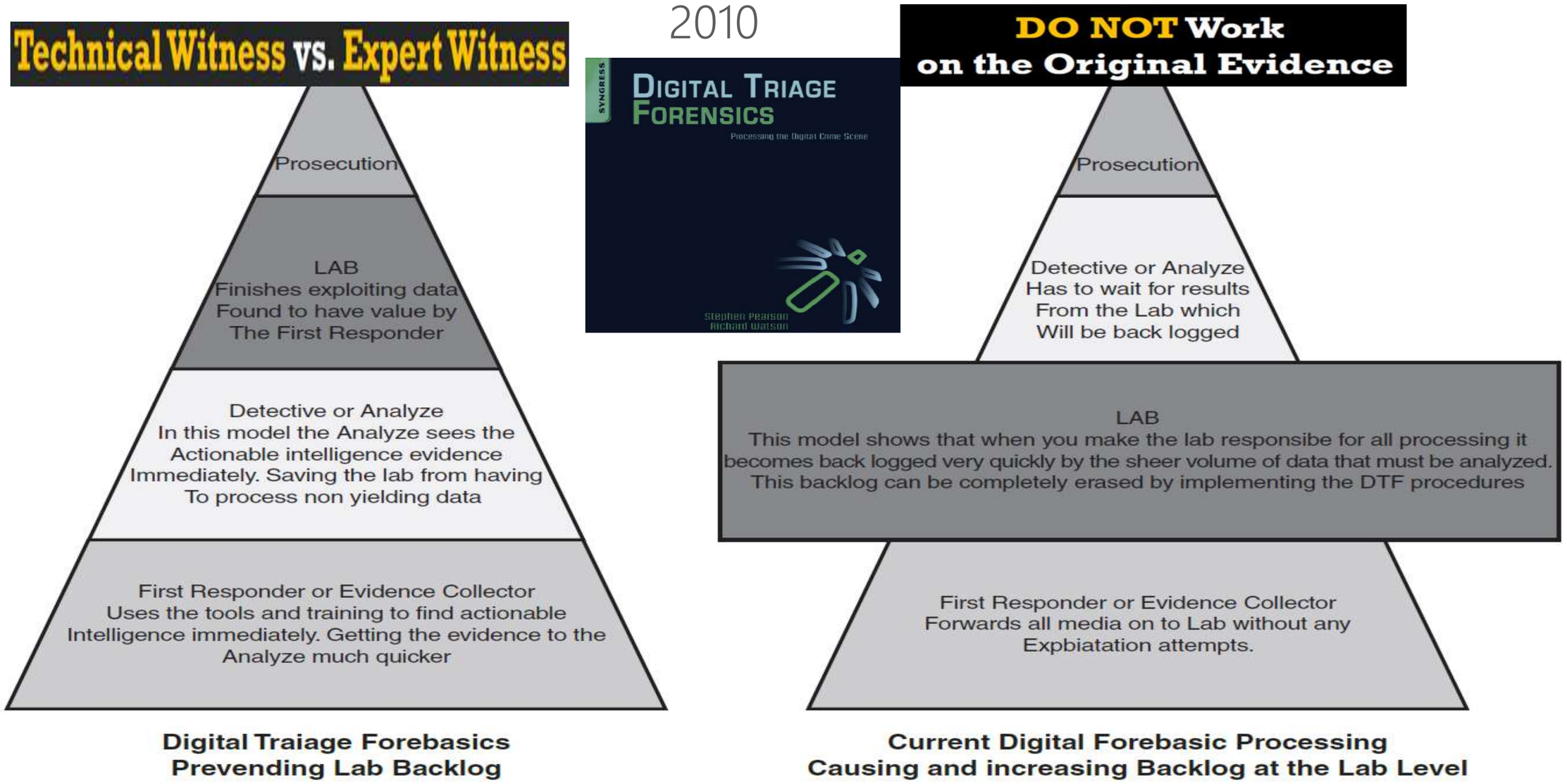
(3)數位鑑識：警察觀點-數位證據的處理準則

數位證據的處理準則

1.不得修改電腦內容	保持現場原始狀態
2.某些狀況存取原件	有能者解釋動作意涵
3.確立方法保留紀錄	相同程序相同結果
4.遵守法律規範原則	承辦人擔負全責

來源： Good Practice Guide for Computer-Based Electronic Evidence by the Association of Chief Police Officers(ACPO) , UK

(3)數位鑑識：軍事觀點-數位分類鑑識



■ **FIGURE 1** Processing pyramid.

(3)數位鑑識：ISO/IEC 27043:2015資安事件調查原則與程序

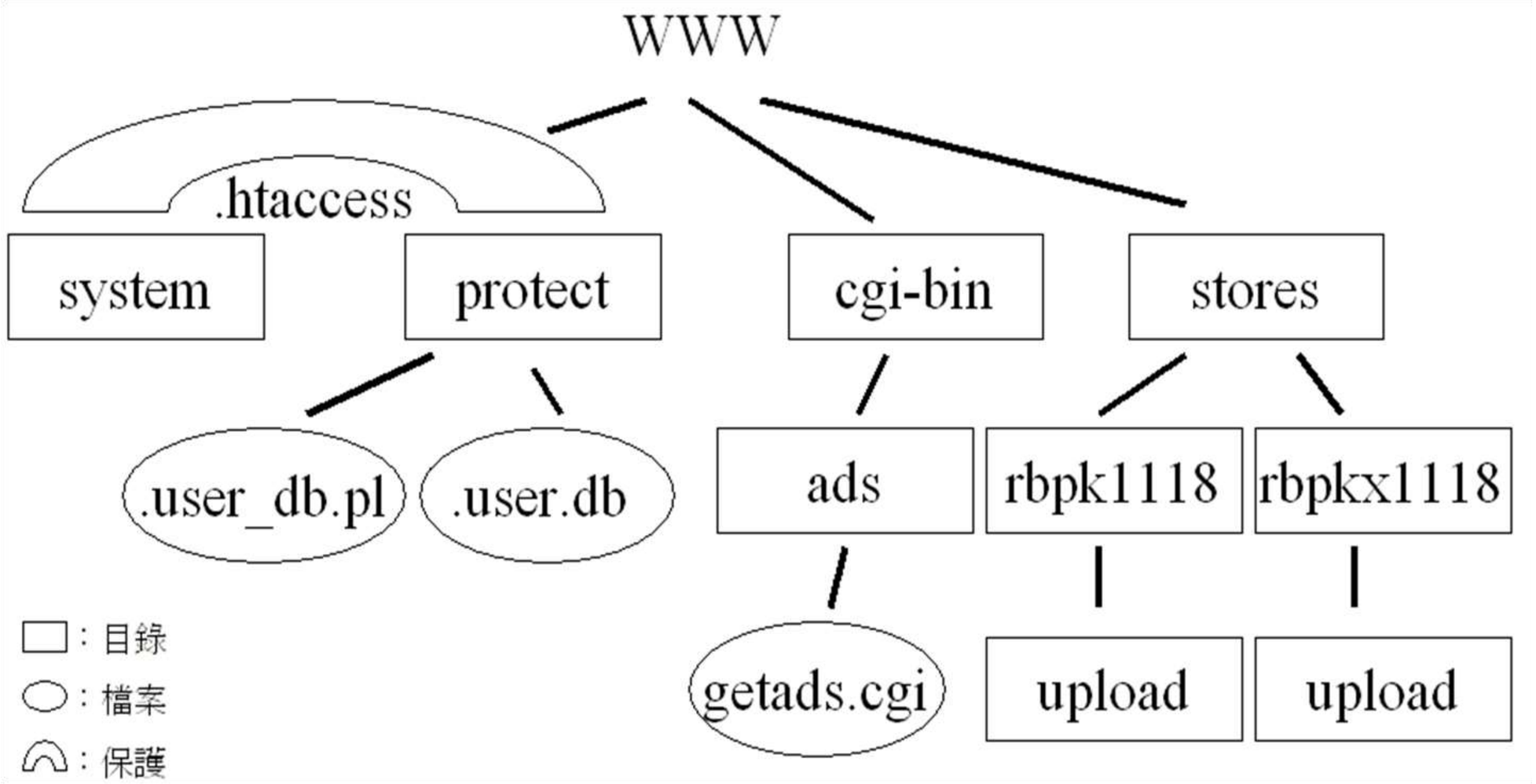
階段程序 Process Class	準備就緒 Readiness Processes	啟始程序 Initialization Processes	獲取程序 Acquisitive Processes	調查程序 Investigative Processes
活動 Activity	計畫 Plan 準備 Prepare	反應 Respond	識別 Identify 蒐集 Collect 獲取 Acquire 保存 Preserve	了解 Understand 報告 Report 結案 Close

同時進行程序 Concurrent Process

1.獲取授權(Obtaining Authorization)
2.資料文件化(Documentation)
3.管理資訊流(Managing Information Flow)
4.維持證物監管鏈(Preserving Chain-of-custody)
5.保存數位證據(Preserving Digital Evidence)
6.與實體調查相互參考(Interaction with Physical Investigation)

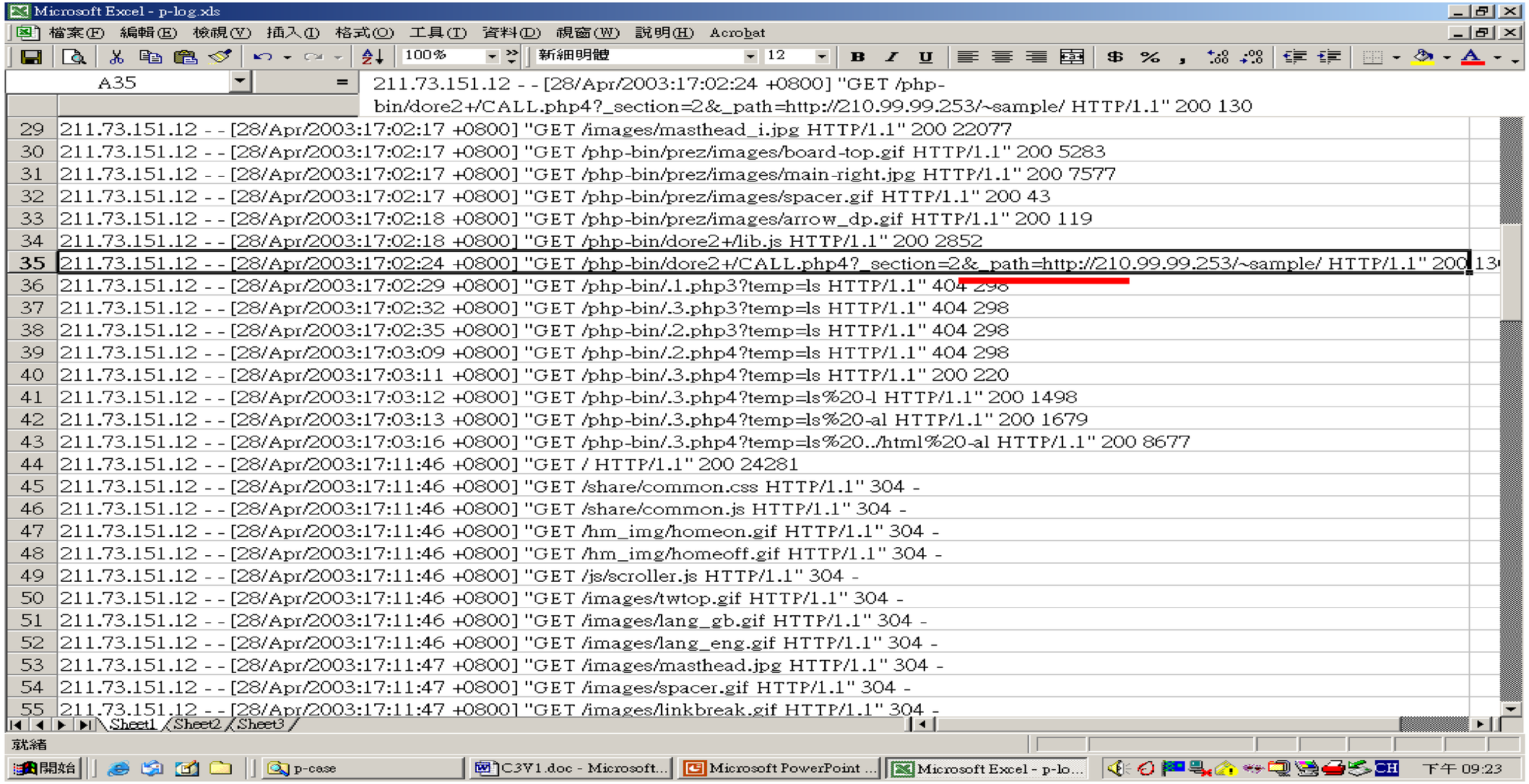
4.案例分析

(1)個案：離職員工入侵

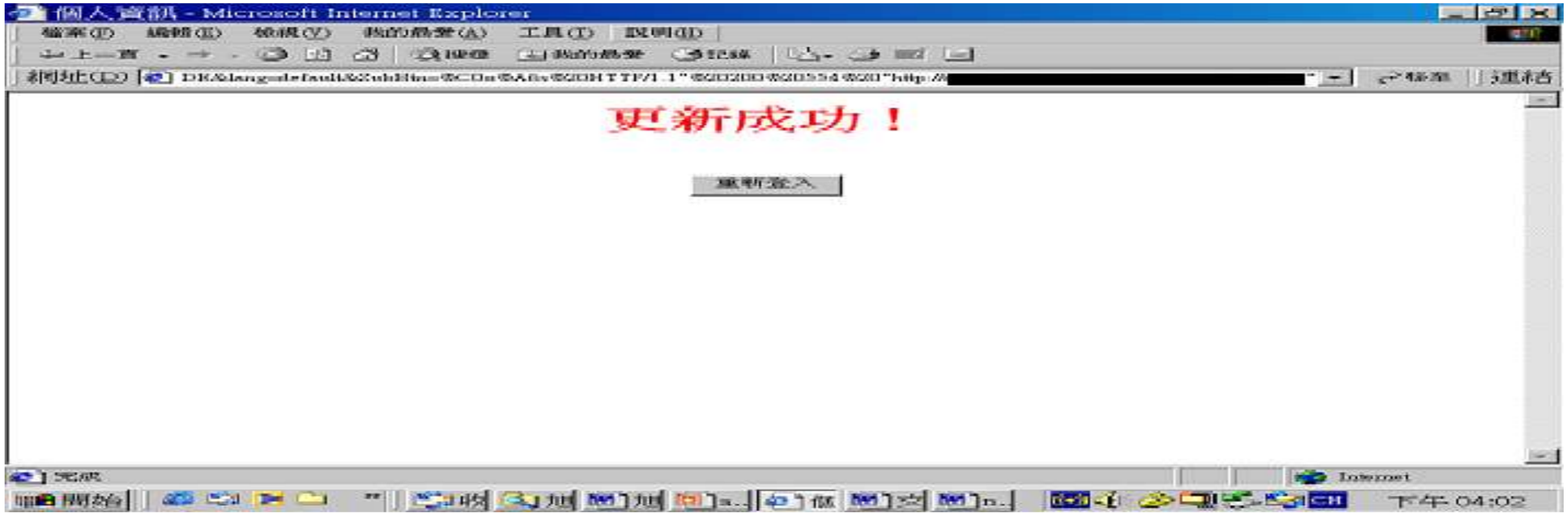

WWW
.htaccess
system
protect
cgi-bin
stores
.user_db.pl
.user.db
ads
rbpk1118
rbpkx1118
getads.cgi
upload
upload
：目錄
：檔案
：保護

(1)個案：Peep反彈式木馬

(1)個案：異常行為(設定路徑)



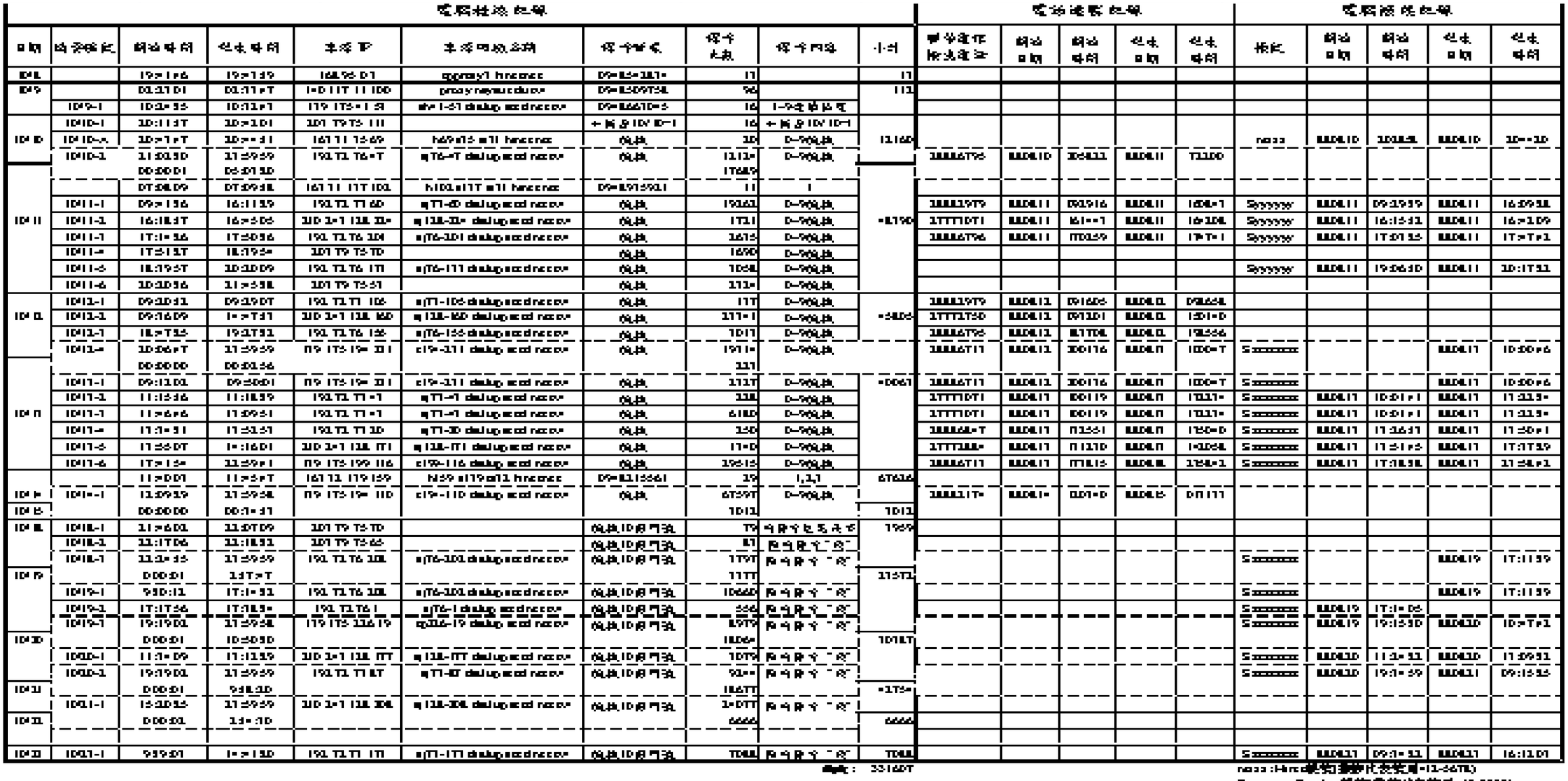
(2)情資、紀錄與證據：利用程式漏洞更新帳密



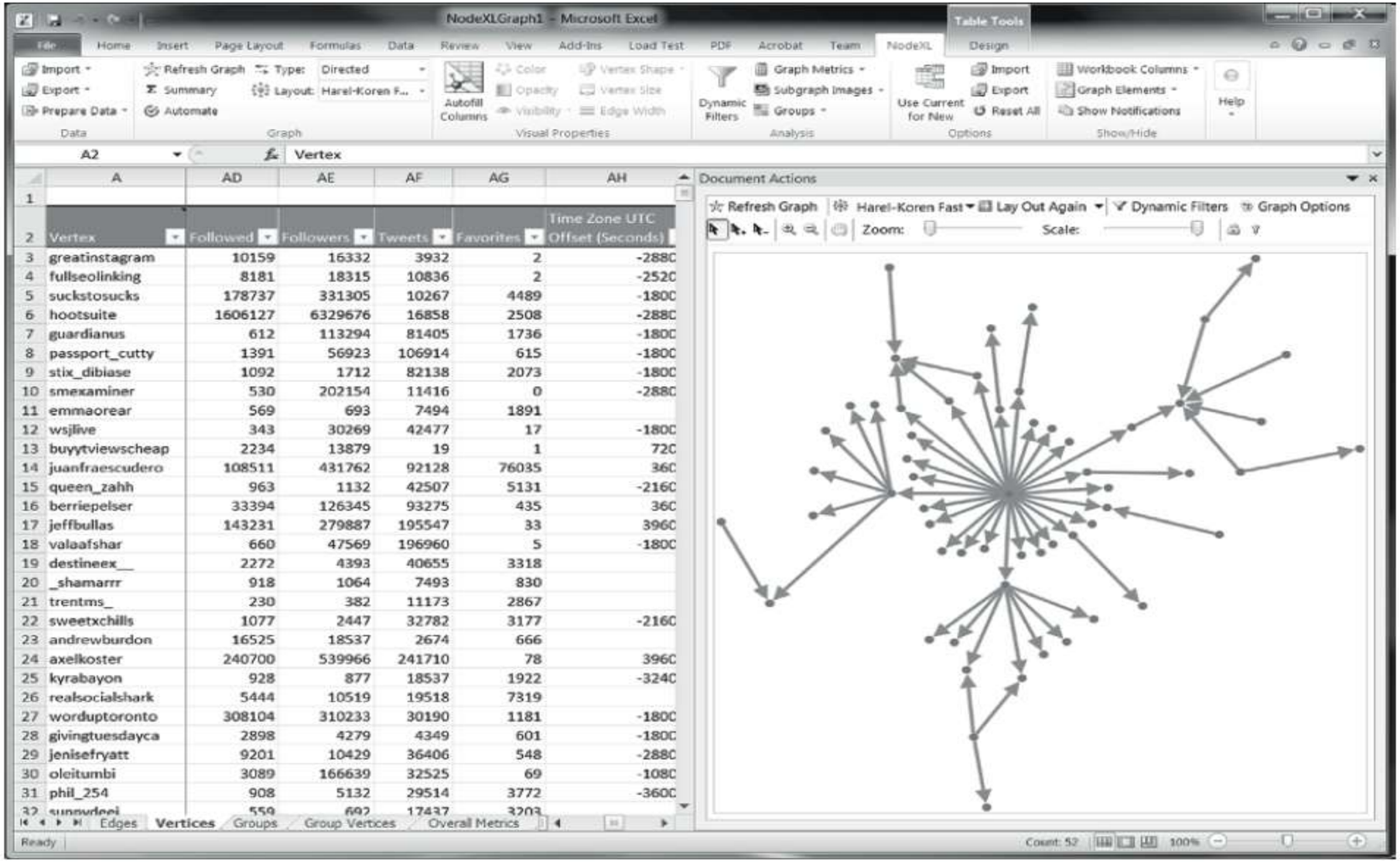
218.160.154.13 - - [22/Apr/2003:22:16:39 +0800] "GET
/newuser**/login.php?username=administrator**&gotourl=&no=&passwd=aaa&**repasswd=aaa**&name=%BA%F4%A4j%A8%B5%B0%F3%A7U%B1%D0&sex=0&year=2001&month=1&day=5&pid=a123456789&mail=service@mail.smaple.com.tw&myhome=&address=Chang+Rong+RD.+Sec.+2%2C+Taipei%2C+Taiwan%2C+R.O.C&tel=06-1234567&mobile=&job=%A6%B0%C1p%AC%EC%A7%DE&lang=default&SubBtn=%C0x%A6s HTTP/1.1“ **200** 554 "http://www.sample.com.tw/newuser/login.php" "Mozilla/4.0 (compatible; MSIE 5.01; Windows NT 5.0)"

(3)交叉比對：事件重建(Temporal時間)

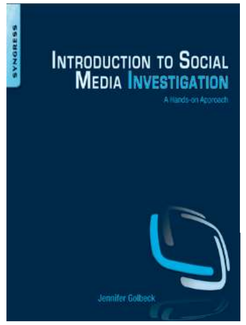
Log1 **Log2** **Log3**



(3)交叉比對：事件重建(Relational相關)



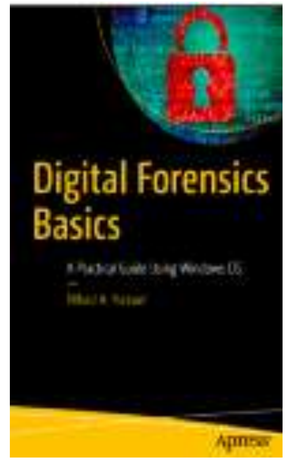
	A	AD	AE	AF	AG	AH
1						
2	Vertex	Followed	Followers	Tweets	Favorites	Time Zone UTC Offset (Seconds)
3	greatinstagram	10159	16332	3932	2	-288(
4	fullseolinking	8181	18315	10836	2	-252(
5	suckstosucks	178737	331305	10267	4489	-180(
6	hootsuite	1606127	6329676	16858	2508	-288(
7	guardianus	612	113294	81405	1736	-180(
8	passport_cutty	1391	56923	106914	615	-180(
9	stix_dibiase	1092	1712	82138	2073	-180(
10	smexaminer	530	202154	11416	0	-288(
11	emmaorear	569	693	7494	1891	
12	wsjlive	343	30269	42477	17	-180(
13	buyytviewscheap	2234	13879	19	1	72(
14	juanfraescudero	108511	431762	92128	76035	36(
15	queen_zahh	963	1132	42507	5131	-216(
16	berriepelser	33394	126345	93275	435	36(
17	jeffbullas	143231	279887	195547	33	396(
18	valaafshar	660	47569	196960	5	-180(
19	destineex__	2272	4393	40655	3318	
20	_shamarrr	918	1064	7493	830	
21	trentms_	230	382	11173	2867	
22	sweetxchills	1077	2447	32782	3177	-216(
23	andrewburdon	16525	18537	2674	666	
24	axelkoster	240700	539966	241710	78	396(
25	kyrabayon	928	877	18537	1922	-324(
26	realsocialshark	5444	10519	19518	7319	
27	worduptoronto	308104	310233	30190	1181	-180(
28	givingtuesdayca	2898	4279	4349	601	-180(
29	jenisefryatt	9201	10429	36406	548	-288(
30	oleitumbi	3089	166639	32525	69	-108(
31	phil_254	908	5132	29514	3772	-360(
32	sunnydeei	559	692	17437	3203	



(4)關鍵問題：資安滲透的法律/道德界線-公/私部門調查的差異？事先授權？

Private sector investigation

(p14)Always treat a private investigation as if it will end up in court. This will force you to follow strict investigatory procedures when building your case and thus protect your organization's private assets if the case ends up in court.

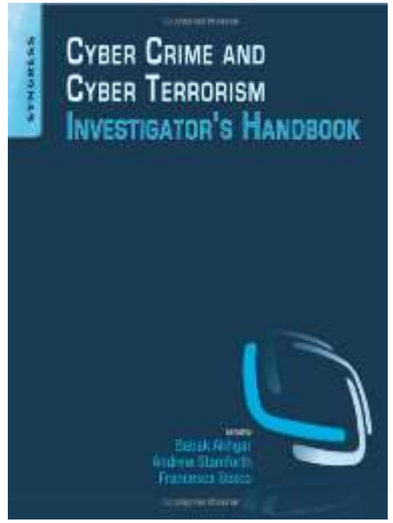


General public sector criminal investigation flow

5.結語

網路犯罪調查者的黃金守則

- ***'ABC' principle throughout the life of an investigation as follows:***
  - **A. Assume nothing不預設任何事情**
  - **B. Believing nothing不輕易相信任何事情**
  - **C. Challenge and check everything質疑挑戰並檢查所有事情**



2014

金融資安事件的應變聯防機制

聯盟願景及推動目標

台灣資安主管聯盟
Taiwan Chief Information Security Officer Alliance

願　景

提升台灣產業資安韌性，促使企業永續發展

目標1：專業資安人才培訓整備
透過資安人才培訓機制，辦理資安長研習課程、產學交流、企業實習、人才媒合等活動，並建置虛實學習平台，促使企業完善專業資安人才。

目標5：資安服務資源鏈結
結合資安專業服務資源，辦理資安事件個案研析、資安治理顧問諮詢、資安解決方案引介等，有效排除資安問題。

目標2：供應鏈資安韌性建立
運作供應鏈資安機制，辦理資安個案、資安治理分享活動，及資安威脅情資分析與示警，強化產業資安韌性。

目標4：重大資安事件應變協助
因應資安事件發生之應變諮詢、協處，並發展事前示警情資服務。

目標3：資安管理制度合規建立
辦理政策法規宣導、法遵諮詢服務等活動，協助企業建立資安管理制度符合相關規範。

金融資安事件的應變聯防機制

聯盟組織架構

台灣資安主管聯盟
Taiwan Chief Information Security Officer Alliance

台灣CISO聯盟
金慶柏 會長
(華碩集團 資安長)

專家顧問群

推動委員會

秘書處
台北市電腦公會

人才培訓委員會
蘇清偉 副會長
(富邦金資安長)

- ◆ 資安主管研習
- ◆ 資安人員培訓
- ◆ 人才媒合活動

政策與法規委員會
曾立峰 副會長
(台達電資訊長)

- ◆ 產業資安治理需求調查
- ◆ 政策法規建言

推廣服務委員會
葉正明 副會長
(欣興電資安長)

- ◆ 資安實務研討
- ◆ 產業 SIG 交流

供應鏈資安委員會
朱建國 副會長
(遠傳電信資安長)

- ◆ 供應鏈資安交流

重大資安事件偵防應變委員會
高大宇 副會長
(永豐金副總經理)

- ◆ 應變諮詢
- ◆ 連結公私部門
- ◆ 接軌國際
- ◆ 威脅示警

金融資安事件的應變聯防機制

聯盟組織運作策略

處理聯盟共通性需求之委員會

處理特定領域需求之委員會

角色：盤點並統籌本聯盟政策或法規建言，及辦理資安政策法規相關活動

角色：盤點並統籌本聯盟可以與外部哪些單位合作，並進行相關合作之連結及初步洽談

政策與法規委員會
曾立峰 副會長
(台達電資訊長)

推廣服務委員會
葉正明 副會長
(欣興電資安長)

相互合作 發揮綜效

人才培訓委員會
蘇清偉 副會長
(富邦金資安長)

角色：辦理人才培訓課程、媒合相關活動；審議提供會員之培訓課程或相關資源內容

供應鏈資安委員會
朱建國 副會長
(遠傳電信資安長)

角色：運作供應鏈資安機制，辦理資安個案、資安治理分享活動，及資安威脅情資分析與示警，強化產業資安韌性

重大資安事件偵防應變委員會
高大宇 副會長
(永豐金副總經理)

角色：因應資安事件發生之應變諮詢、協處，並發展事前示警情資服務

台灣資安主管聯盟
Taiwan Chief Information Security Officer Alliance