

附件 4.基本數位證據保存工具使用說明

數位證據可推測出遭受的攻擊種類，找出入侵的原因。有利於未來規範上的改善或資安漏洞的修補。建議保存以下資訊。

1. Registry 機碼

(1) 按下 Win+R 彈出執行視窗並輸入 regedit

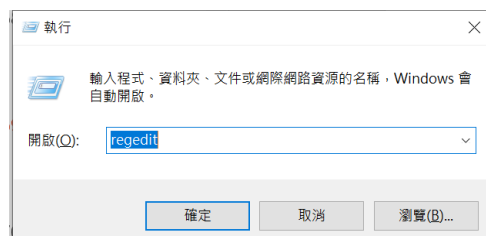


圖 1 開啟機碼編輯視窗

(2) Regedit 會看到此畫面，點選「電腦」→「檔案」→「匯出」

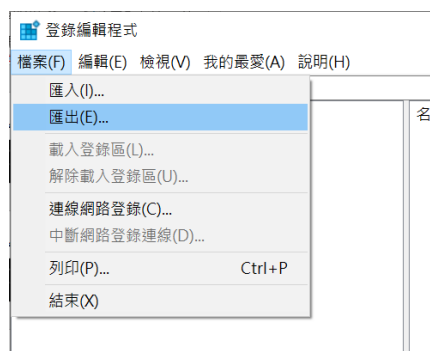


圖 2 點選機碼匯出按鈕

(3) 選擇要匯出的路徑與檔名即可匯出此電腦所有的機碼

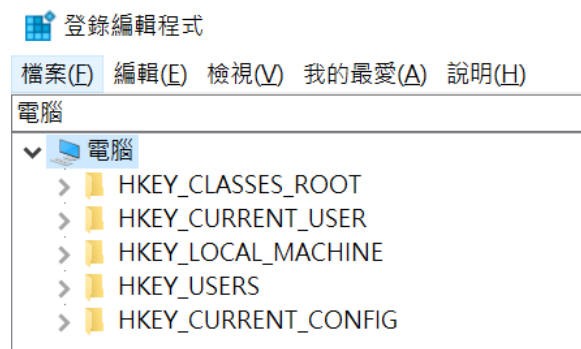


圖 3 選擇匯出的路徑

2. USB 使用紀錄(需管理員權限)

- (1) reg query HKLM\System\currentcontrolset\enum\usbstor /s > 你要匯出的路徑.txt
- (2) 尋找 FriendlyName 可發現此電腦有 Kingston 的 USB 曾經連接過(此範例為：Kingston DataTraveler 3.0 USB Device)

```
C:\Users\twnic\Desktop\新增資料夾 (3)>reg query HKLM\System\currentcontrolset\enum\usbstor /s
HKEY_LOCAL_MACHINE\System\currentcontrolset\enum\usbstor\Disk&Ven_Kingston&Prod_DataTraveler_3.0&Rev_
HKEY_LOCAL_MACHINE\System\currentcontrolset\enum\usbstor\Disk&Ven_Kingston&Prod_DataTraveler_3.0&Rev_160A44C4138F0F2C02
9D5B04&0
DeviceDesc REG_SZ @disk.inf,%disk_devdesc%;Disk drive
Capabilities REG_DWORD 0x10
Address REG_DWORD 0xf
ContainerID REG_SZ {c4163120-f014-5bfe-b59a-50bbf9cbf313}
HardwareID REG_MULTI_SZ USBSTOR\DiskKingstonDataTraveler_3.0_\USBSTOR\DiskKingstonDataTraveler_3.0_\USBST
R\DiskKingston\USBSTOR\KingstonDataTraveler_3.0_\0KingstonDataTraveler_3.0_\USBSTOR\GenDisk\0GenDisk
CompatibleIDs REG_MULTI_SZ USBSTOR\Disk\USBSTOR\RAW\0GenDisk
ClassGUID REG_SZ {4d36e967-e325-11ce-bfcl-08002be10318}
Service REG_SZ disk
Driver REG_SZ {4d36e967-e325-11ce-bfcl-08002be10318}\0004
Mfg REG_SZ @disk.inf,%genmanufacturer%;(Standard disk drives)
FriendlyName REG_SZ Kingston DataTraveler 3.0 USB Device
ConfigFlags REG_DWORD 0x0
```

圖 4 USB 使用紀錄查詢

3. Event log

(1) 以「系統管理員」開啟 cmd 輸入「eventvwr.exe」

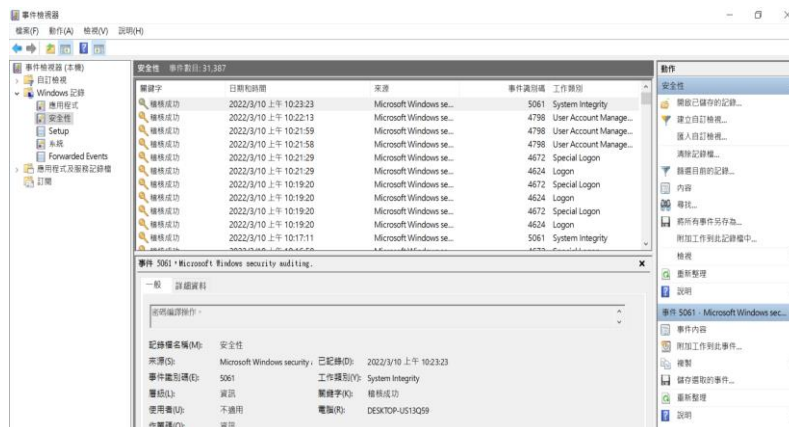


圖 5 事件紀錄檢視器

(2) 點選「Windows 紀錄」→「應用程式、系統、安全性」→「將所有事件另存為...」

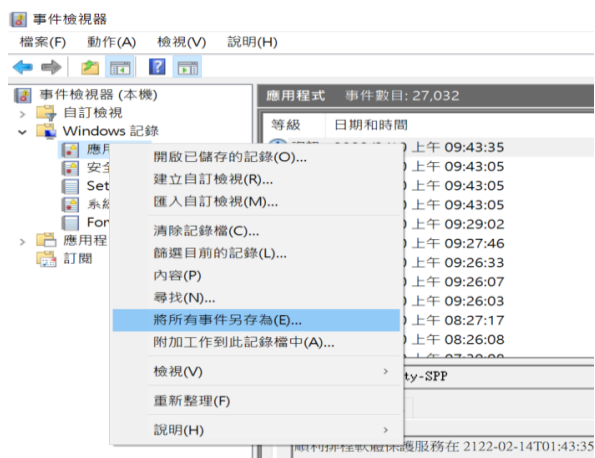


圖 6 匯出事件紀錄

(3) 常見重要事件編碼

表 1 常見重要事件編碼

項次	事件編號	說明
1	4624	帳號登入成功
2	4625	帳號登入失敗
3	4657	機碼註冊表遭修改

(4) 亦可透過 cmd 的指令將 log 匯出，亦可透過 cmd 的指令將 log 匯出

1. wevtutil.exe epl application .\evtxapp.evtx
2. wevtutil.exe epl Security .\evtxsec.evtx
3. wevtutil.exe epl System .\evtxsys.evtx

(5) Linux 系統日誌系統位於/var/log/

1. Message：包含 Kernel 錯誤訊息、網路錯誤、I/O 錯誤
2. Cron：包含排程任務訊息
3. Lastlog：各用戶最近登入事件

4. 記憶體匯出(需額外工具)

當發生資安事故時，當下的記憶體狀態相當珍貴，因為執行中的程式會在記憶體中。常見的採證工具為 FTK Imager，值得注意的是要 dump 的電腦記憶體大小若為 16G 存放的媒體需大於 16G 較為妥當。

(1) 點選 File→capture Memory

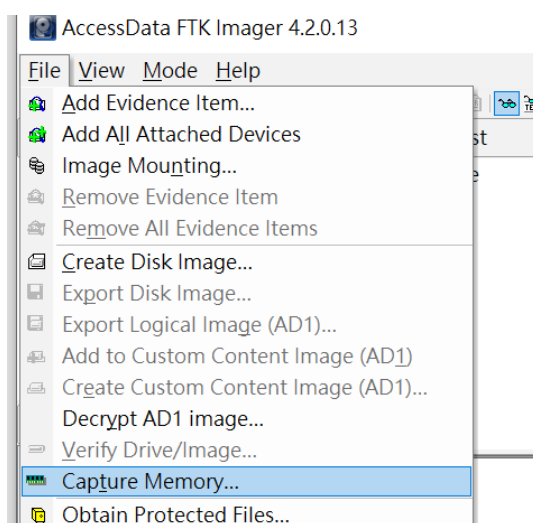


圖 7 擷取記憶體

(2) 選擇儲存位置與命名

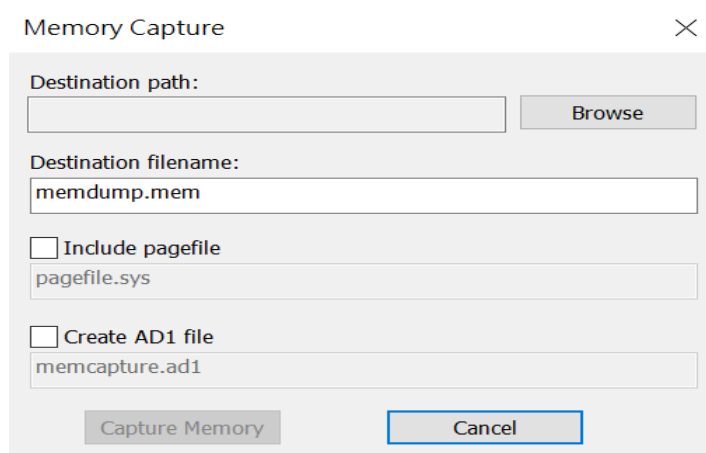


圖 8 記憶體儲存的位置

(3) 匯出記憶體

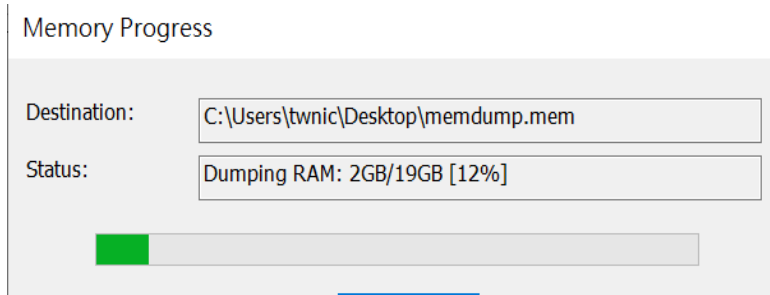


圖 9 正在匯出記憶體的画面

5. 系統使用狀態資訊

系統管理員身分開啟 cmd 將以下資訊另存檔案，如 Systeminfo > C:\Systeminfo.txt 即可將相關資訊另存為文字檔

- (1) Systeminfo：顯示有關電腦及其作業系統的詳細設定資訊，包括作業系統設定、安全性資訊、產品識別碼和硬體內容（例如 RAM、磁碟空間和網路卡）

```

主機名稱: DESKTOP-US13Q59
作業系統名稱: Microsoft Windows 10 家用版
作業系統版本: 10.0.19043 N/A 組建 19043
作業系統製造商: Microsoft Corporation
作業系統設定: 獨立工作站
作業系統組建類型: Multiprocessor Free
註冊的擁有者: twnic
註冊公司: N/A
產品識別碼: 00325-96643-84424-AAOEM
原始安裝日期: 2021/3/22, 下午 05:05:30
系統開機時間: 2021/12/16, 上午 12:54:21
系統製造商: Dell Inc.
系統型號: Inspiron 7490
系統類型: x64-based PC
處理器: 已安裝 1 處理器。
[01]: Intel64 Family 6 Model 142 Stepping 12 GenuineIntel ~1803 Mhz
BIOS 版本: Dell Inc. 1.4.1, 2020/3/3
Windows 目錄: C:\WINDOWS
系統目錄: C:\WINDOWS\system32
開機裝置: \Device\HarddiskVolume1
系統地區設定: zh-tw;中文(台灣)

```

圖 10 Systeminfo 資訊

- (2) net user：顯示使用者帳戶訊息，USER 可建立和修改電腦上的使用者帳戶。使用時不加上參數,便會列出該台電腦的使用者帳戶。使用者帳戶資訊是儲存在使用者帳戶資料庫中。[檢查是否有被建立未知的帳戶]

```

-----
Administrator          DefaultAccount          Guest
twnic                   WDAGUtilityAccount
命令已經成功完成。

```

圖 11 net user 資訊

- (3) `ipconfig /all`：顯示所有目前的 TCP/IP 網路設定值，並重新整理動態主機設定通訊協定 (DHCP) 和網域名稱系統 (DNS) 設定。在不使用參數的情況下使用，`ipconfig` 會顯示第四版網際網路協定 (IPv4) 和 IPv6 位址、子網路遮罩，以及所有介面卡的預設閘道。

```

連線特定 DNS 尾碼 . . . . . : Intel(R) Wi-Fi 6 AX201 160MHz
描述 . . . . . : C0-B8-83-3F-46-89
實體位址 . . . . . : 是
DHCP 已啟用 . . . . . : 是
自動設定啟用 . . . . . : 是
連結-本機 IPv6 位址 . . . . . : fe80::987:ee75:47c8:f6ef%12(偏好選項)
IPv4 位址 . . . . . : 192.168.121.9(偏好選項)
子網路遮罩 . . . . . : 255.255.255.0
租用取得 . . . . . : 2022年3月9日 下午 01:35:19
租用到期 . . . . . : 2022年3月9日 下午 06:29:55
預設閘道 . . . . . : 192.168.121.228
DHCP 伺服器 . . . . . : 192.168.121.228

```

圖 12 `ipconfig/all` 資訊

- (4) `Netstat -ano`：顯示作用中 TCP 連線、電腦正在接聽的埠、乙太網路統計資料、IP 路由表、IP、ICMP、TCP 資訊

```

TCP 192.168.121.9:139 0.0.0.0: LISTENING 4
TCP 192.168.121.9:13204 52.114.40.59:443 ESTABLISHED 4456
TCP 192.168.121.9:13211 20.43.70.166:443 ESTABLISHED 15972
TCP 192.168.121.9:13547 20.198.162.78:443 ESTABLISHED 29896
TCP 192.168.121.9:13578 52.111.232.14:443 ESTABLISHED 18692
TCP 192.168.121.9:14655 108.177.97.188:5228 ESTABLISHED 37644
TCP 192.168.121.9:14658 52.114.7.165:443 ESTABLISHED 31920
TCP 192.168.121.9:15084 117.18.232.200:443 CLOSE_WAIT 17404
TCP 192.168.121.9:15085 117.18.232.200:443 CLOSE_WAIT 17404

```

圖 13 `netstat -ano` 資訊

6. 可疑檔案加密封存

- (1) 透過內建指令產生檔案 Hash:certutil -hashfile 檔案路徑 MD5/SHA1/SHA256
- (2) 使用壓縮軟體加密

```
C:\Users\twnic\Desktop\Hash>certutil -hashfile .\myfile.TXT MD5
MD5 的 .\myfile.TXT 雜湊:
50b7748612b28db487d115f220bb77ab
CertUtil: -hashfile 命令成功完成。

C:\Users\twnic\Desktop\Hash>certutil -hashfile .\myfile.TXT SHA1
SHA1 的 .\myfile.TXT 雜湊:
2d533b9d9f0f06ef4e3c23fd496cfeb2780eda7f
CertUtil: -hashfile 命令成功完成。
```

圖 14 執行 Hash 指令