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

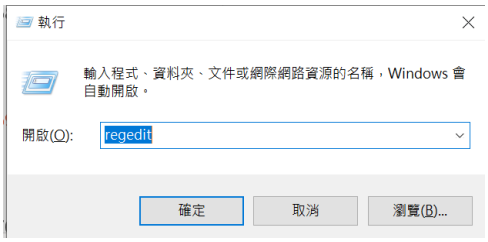

圖 1 開啟機碼編輯視窗

(2) Regedit 會看到此畫面，點選「電腦」→「檔案」→「匯出」

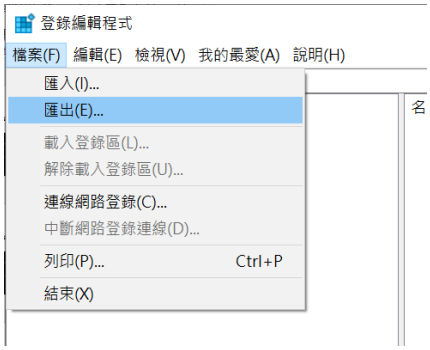

圖 2 點選機碼匯出按鈕

(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)

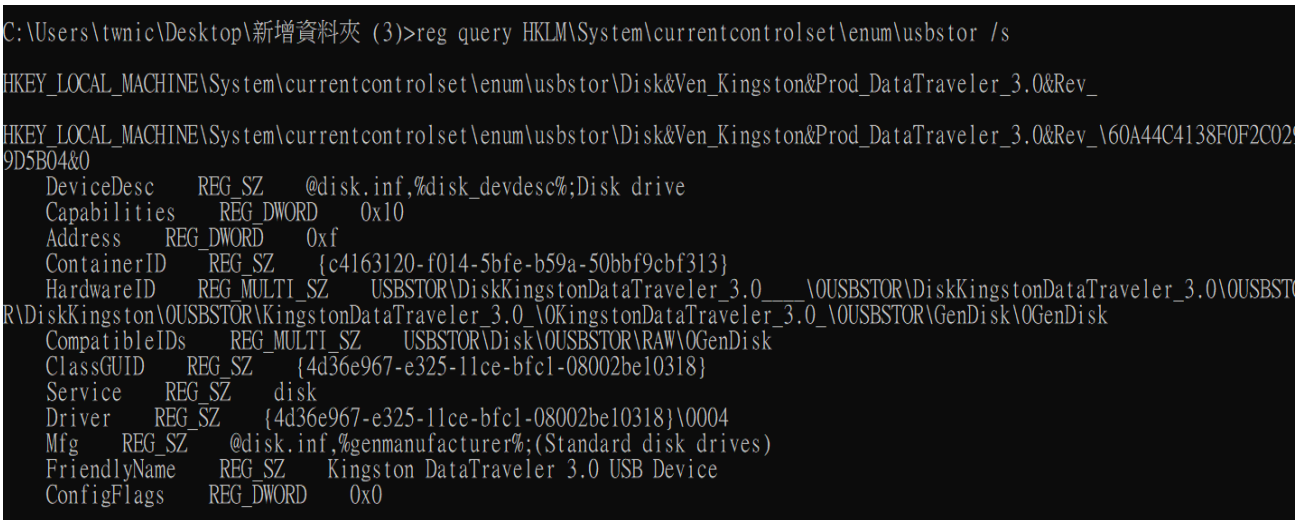

圖 4 USB 使用紀錄查詢

3. Event log

(1) 以「系統管理員」開啟 cmd 輸入「eventvwr.exe」

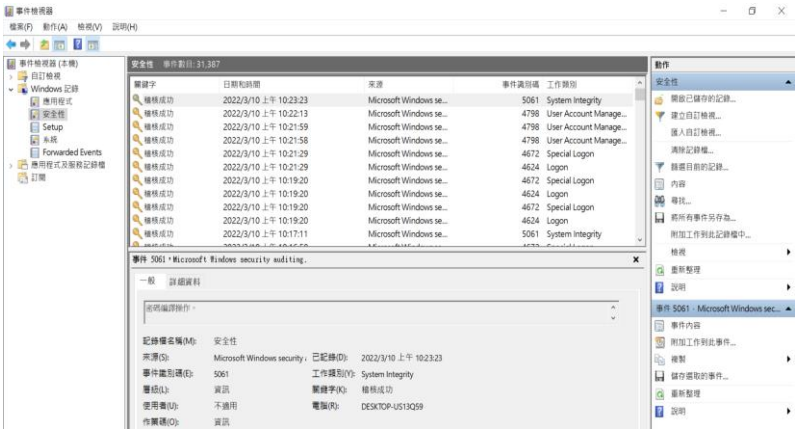

圖 5 事件紀錄檢視器

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

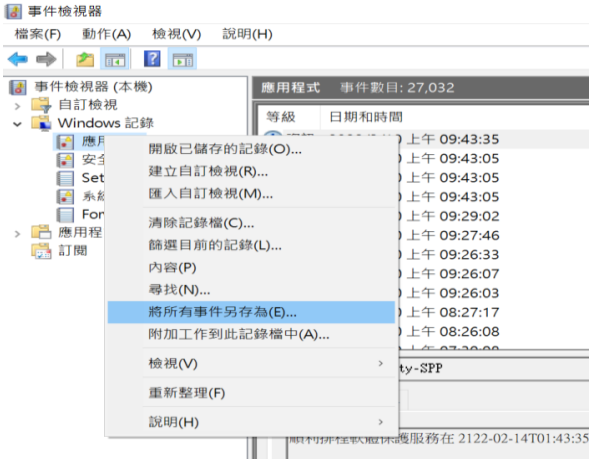

圖 6 匯出事件紀錄

(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

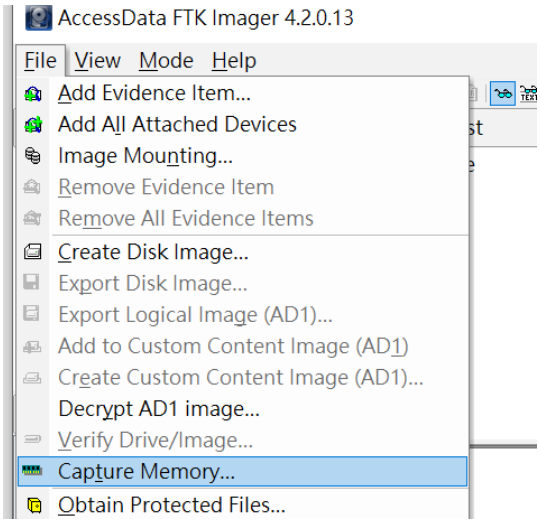

圖 7 擷取記憶體

(2) 選擇儲存位置與命名

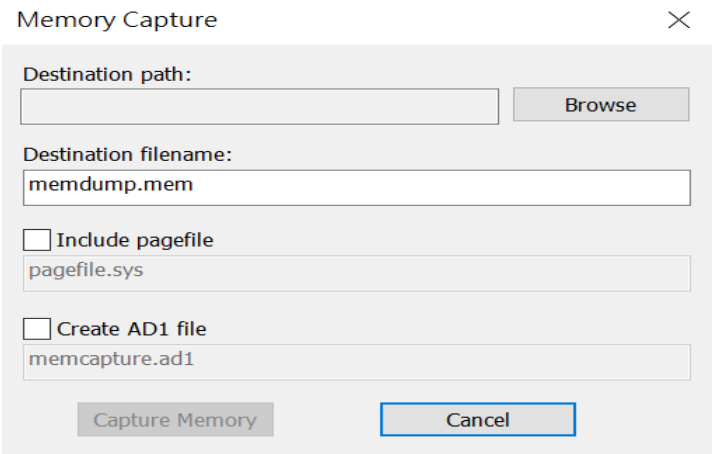

圖 8 記憶體儲存的位置

(3) 匯出記憶體

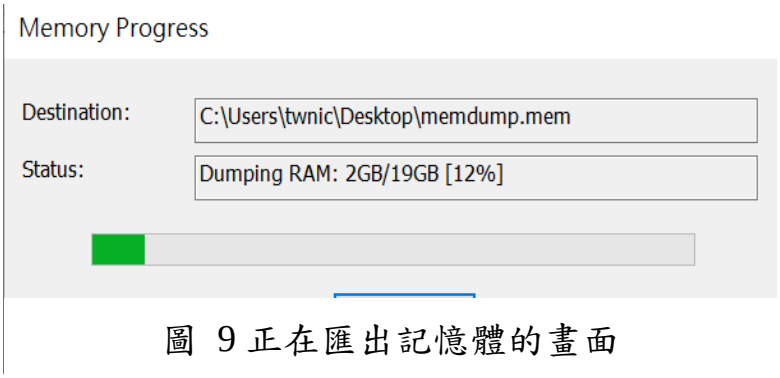

圖 9 正在匯出記憶體的畫面

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)

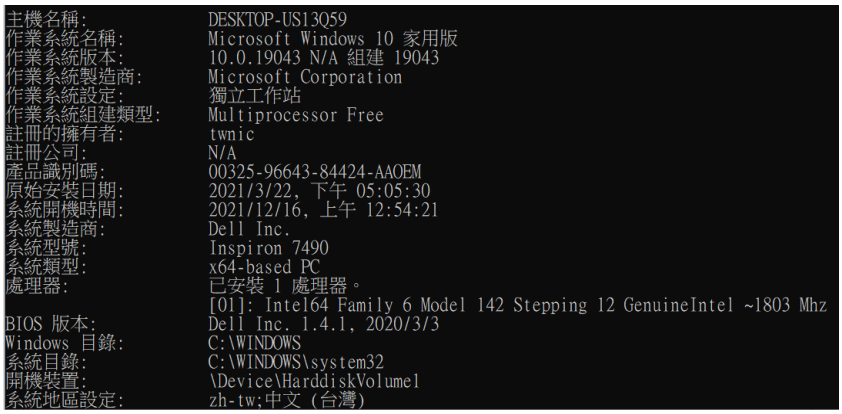

圖 10 Systeminfo 資訊

(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]

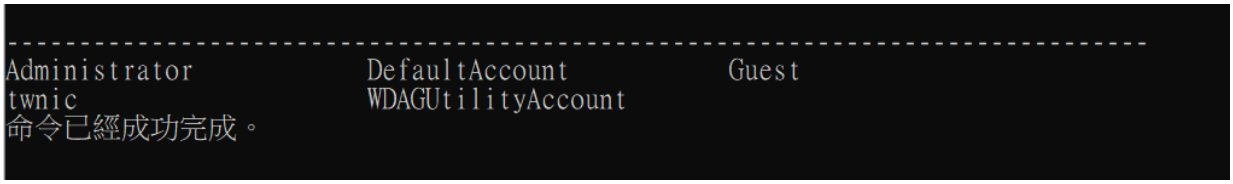

圖 11 net user 資訊

(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。

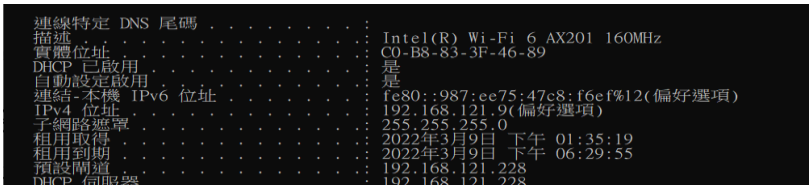

圖 12 ipconfig/all 資訊

(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

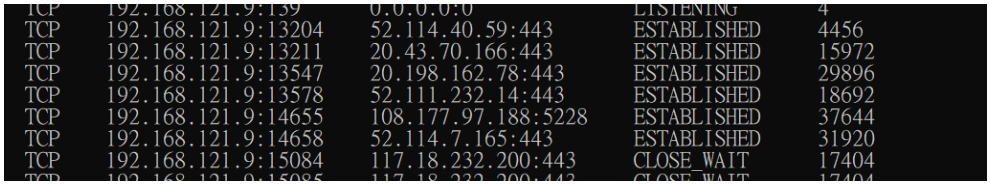

圖 13 netstat -ano 資訊

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

圖 14 執行 Hash 指令