Process Explorer
工具應用

Process Explorer 工具應用

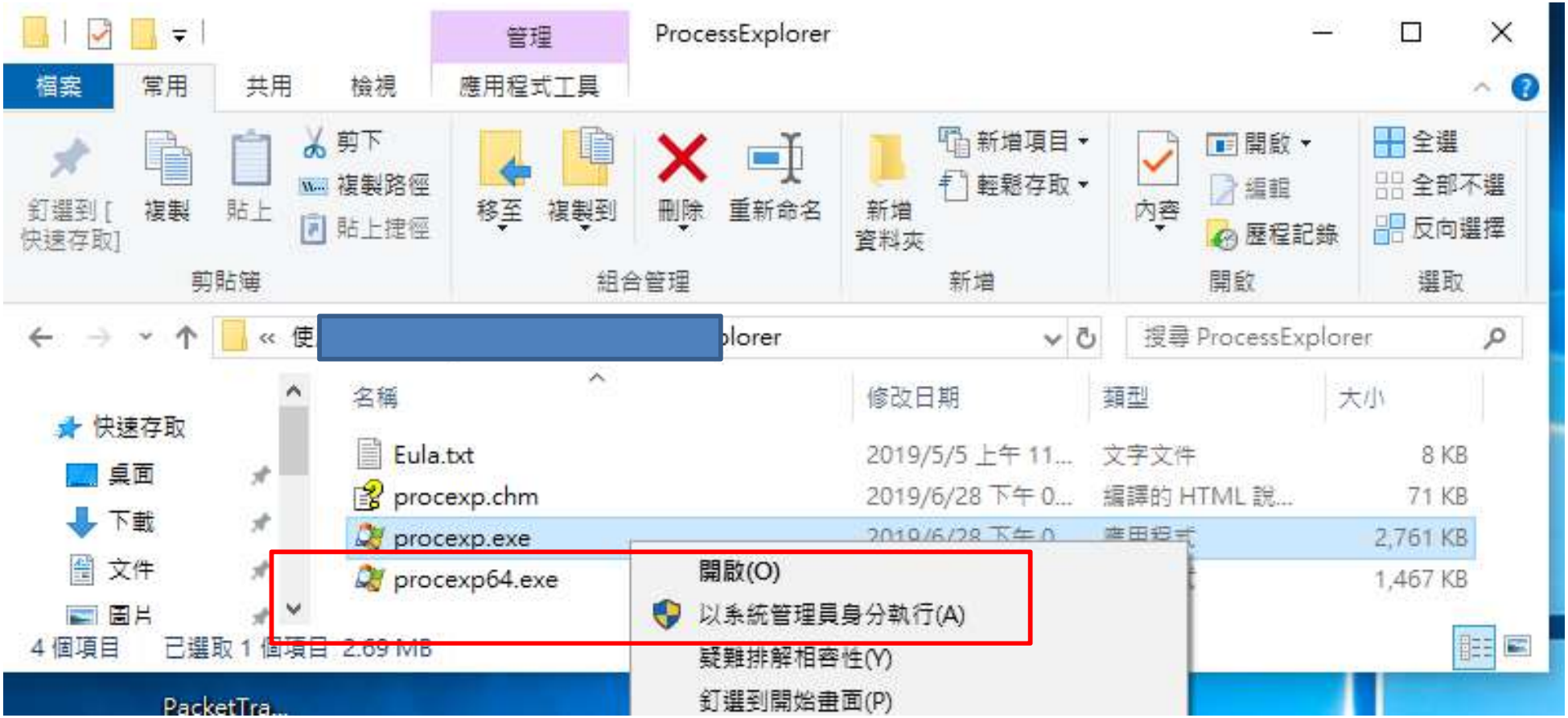
經驗分享

- 開啟方法與下載點：
  - https://docs.microsoft.com/en-us/sysinternals/downloads/process-explorer
  - 目前最新版本 「**Process Explorer v16.32**」
- Process 狀態與種類
- 檢查是否為惡意程序
- 驗證程序簽名檔
- 找出電腦中的惡意程序

啟動程式

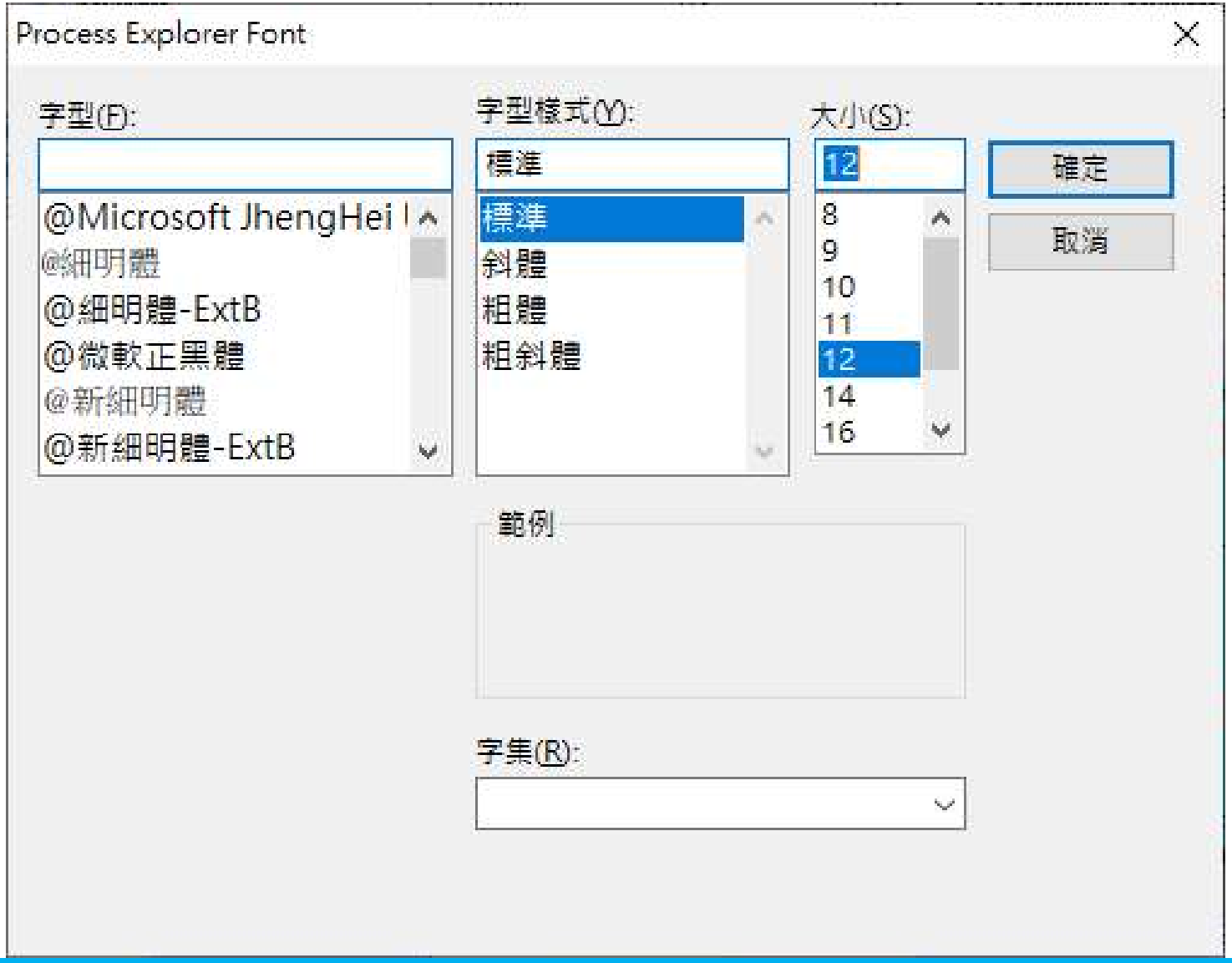
下載後啟動

- 下載完畢，並解壓縮後，使用系統管理者身份執行



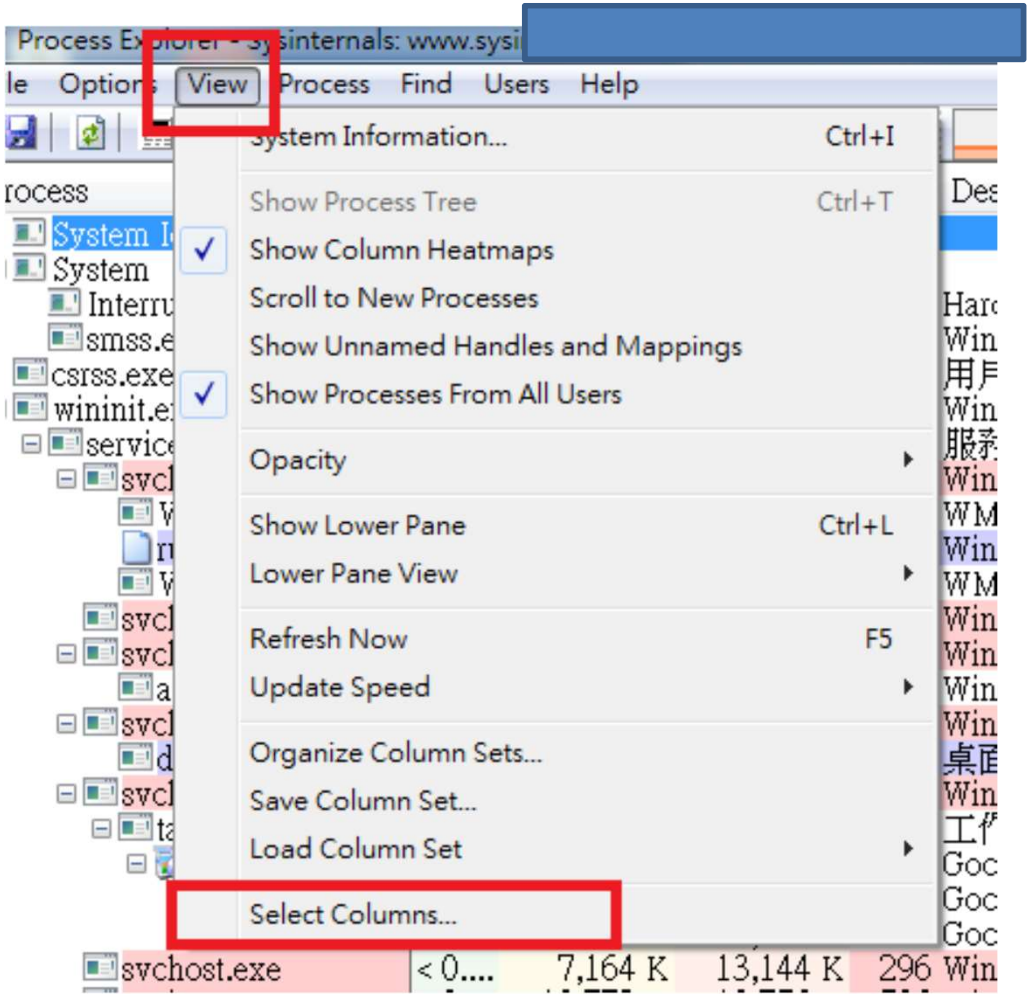
設定字型

- Options →Font

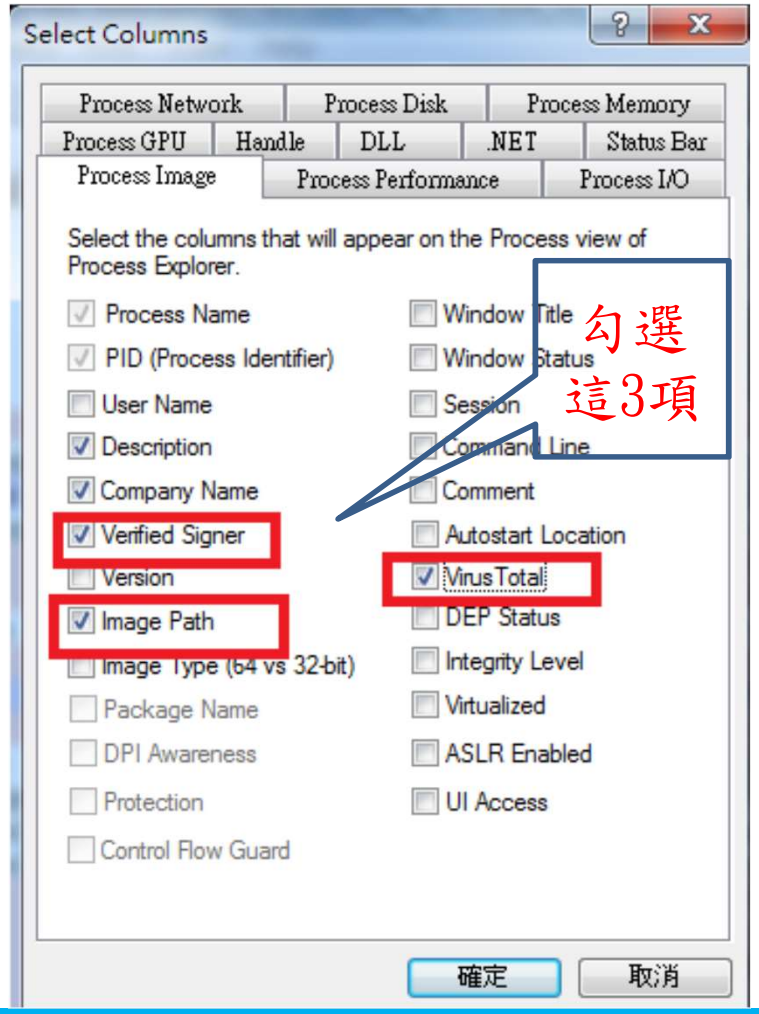


設定顯示欄位

- View →Select Columns



- 勾選下列項目
  - Verfied Singer
  - Image Path
  - Virus Total

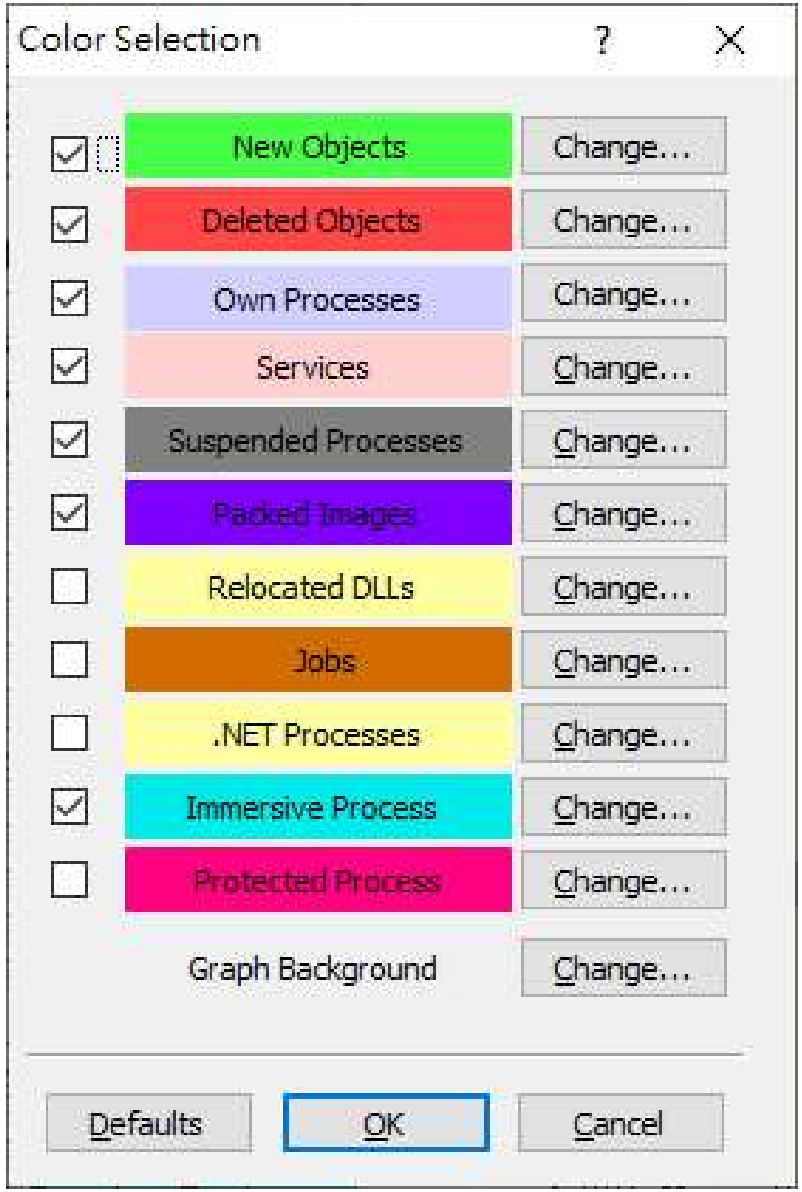


哪些Process 啟動、加密、背景服務執行?

行程類型與顏色 -

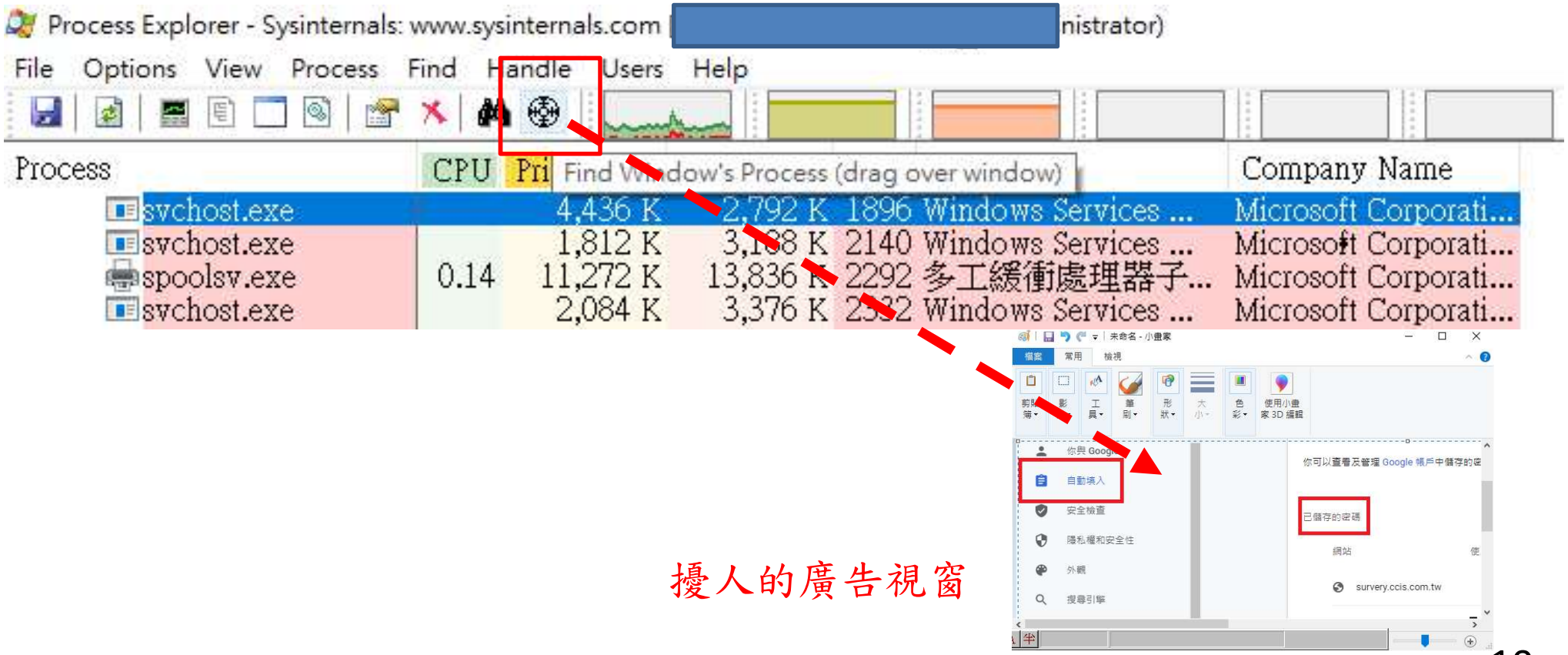
Options→Color Selection

- 紫色 Packed Images: 表示這個 process 有特別的被加密處理過。
  - 通常正常的 process 很少會這樣做。病毒的可能性就很大。
- Process 的啟動與結束：綠色與紅色。
  - 看看是不是有經常性的 process 被啟動。或是莫名的被停止。
- Service 粉紅色：Services 因為一開啟就會自動的在背景執行。所以可以知道系統有哪些背景服務與 process 的關係。
- 淺藍色行程是由啟動Process Explorer的同一帳戶運行的行程



找出流氓軟體位置並停用

- 右下角的彈跳視窗，我們想知道是什麼軟體的彈跳視窗以及他的目標位置在哪裡
- 點擊圖中像是「靶子」圖示(Find Windows Process)，拖動至右下角彈跳視窗



擾人的廣告視窗

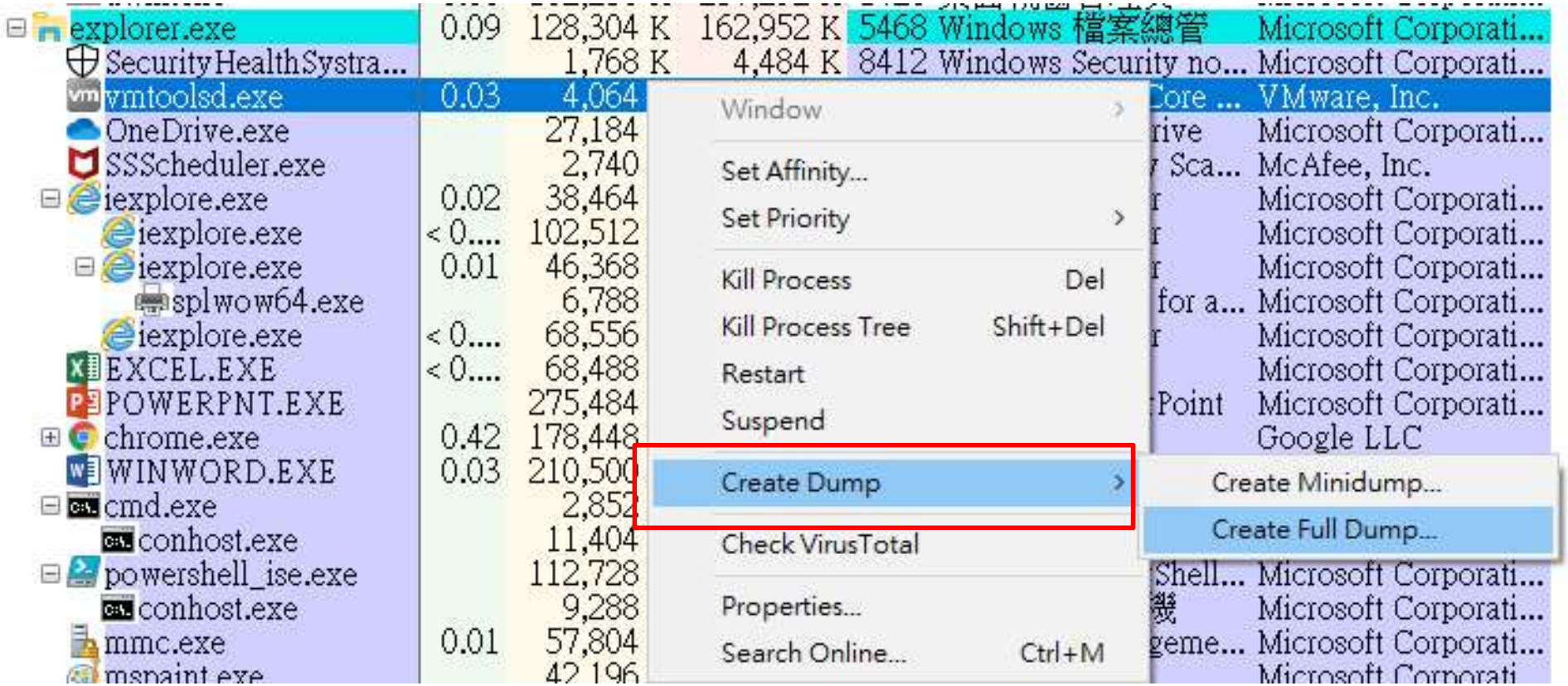
檢視整體電腦的效能

- View > System information (Ctrl + I)

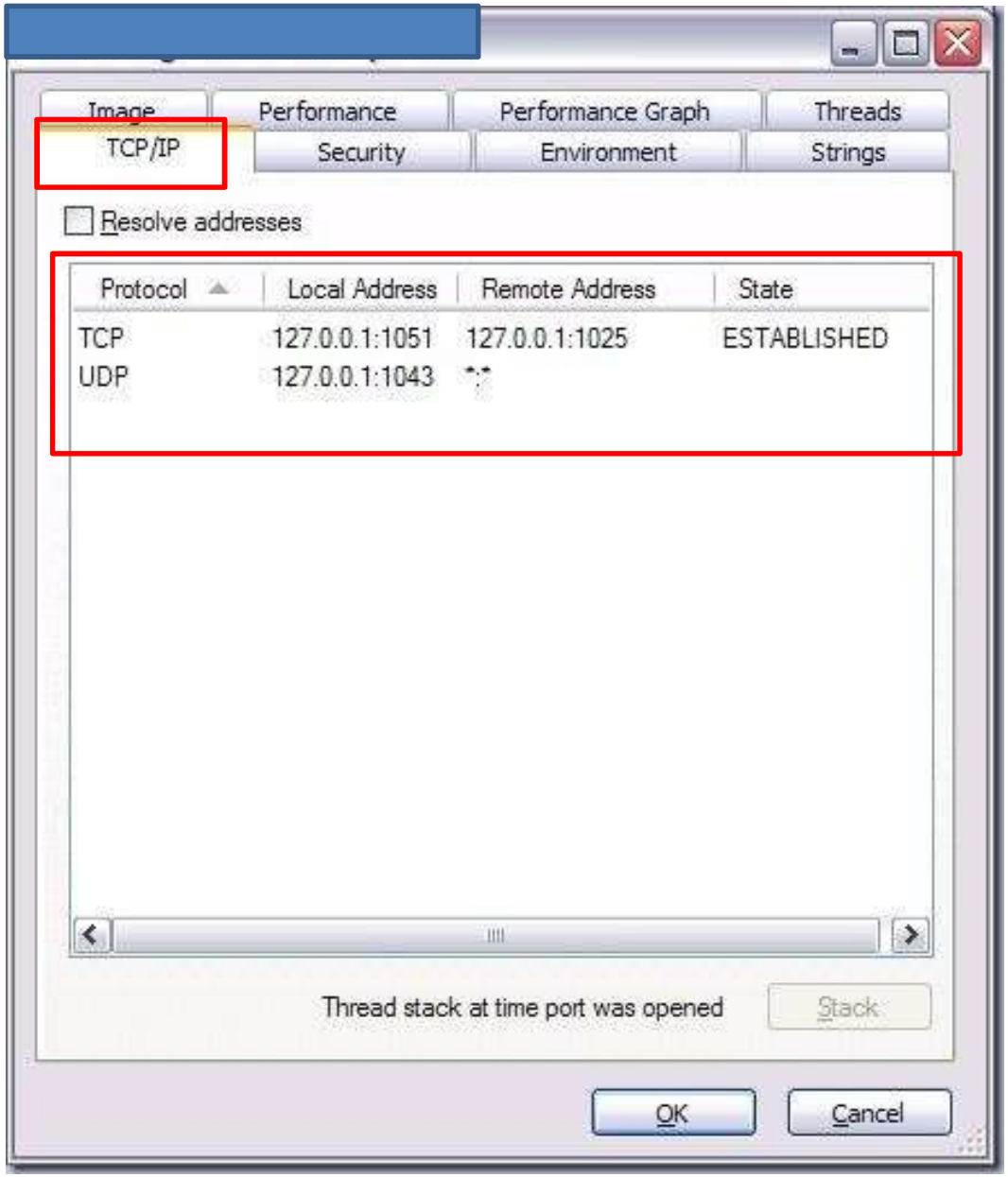
將特定Process 當下的狀態快照事後分析

使用技巧

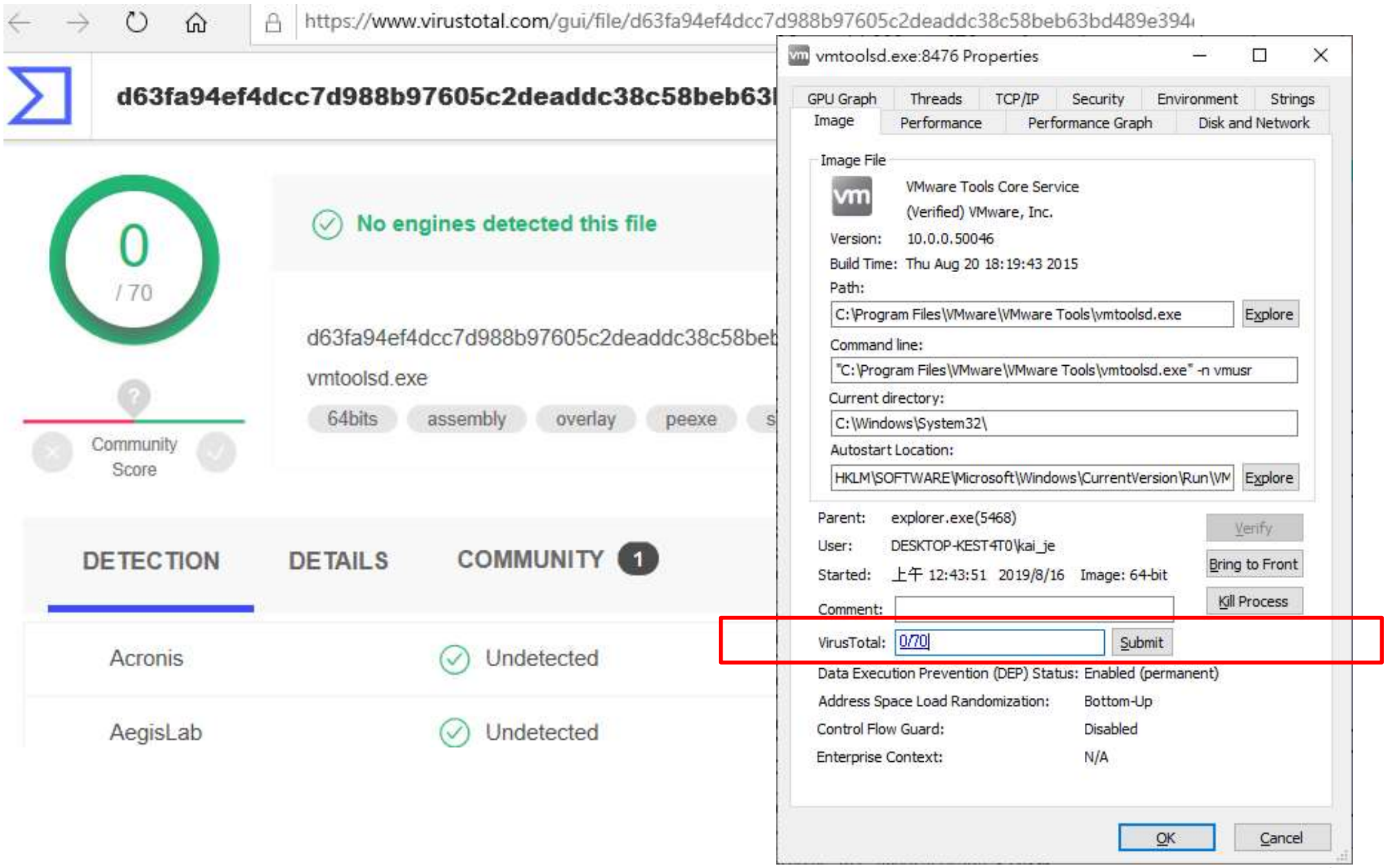
- 利用 “Create Dump” 的功能，將特定 process 當下的狀態儲存
- 產生的 Dump 可以用 windbg or Diagnosis Tool 事後分析(windbg)
  - https://docs.microsoft.com/zh-tw/windows-hardware/drivers/debugger/debugger-download-tools



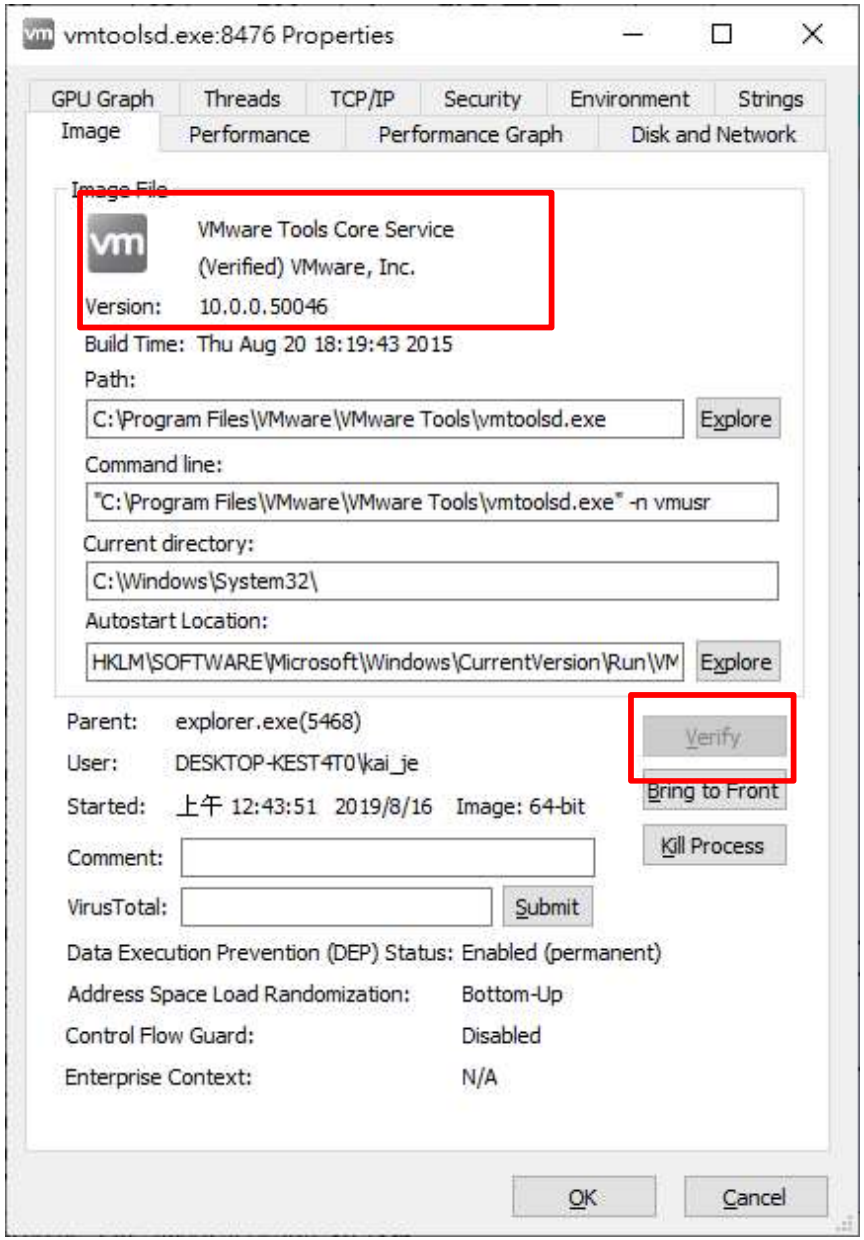
Process 是不是有偷偷往外連



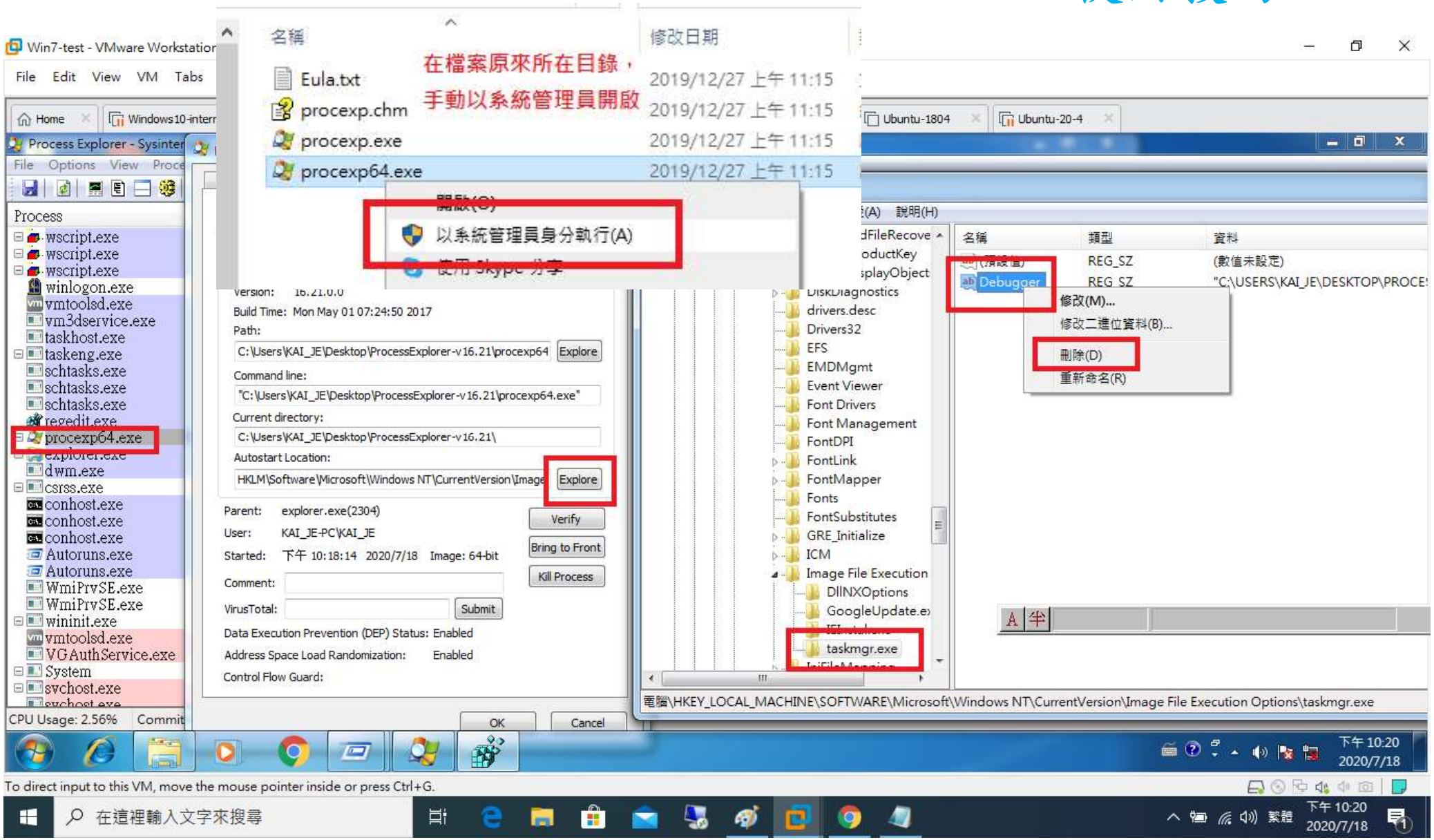
檢查是否為已知病毒?


https://www.virustotal.com/gui/file/d63fa94ef4dcc7d988b97605c2deaddc38c58beb63bd489e394
d63fa94ef4dcc7d988b97605c2deaddc38c58beb63
0
/ 70
No engines detected this file
d63fa94ef4dcc7d988b97605c2deaddc38c58beb
vmtoolsd.exe
64bits
assembly
overlay
peexe
Community Score
DETECTION
DETAILS
COMMUNITY 1
Acronis
Undetected
AegisLab
Undetected
vmtoolsd.exe:8476 Properties
GPU Graph
Threads
TCP/IP
Security
Environment
Strings
Image
Performance
Performance Graph
Disk and Network
Image File
VMware Tools Core Service
(Verified) VMware, Inc.
Version: 10.0.0.50046
Build Time: Thu Aug 20 18:19:43 2015
Path:
C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
Explore
Command line:
"C:\Program Files\VMware\VMware Tools\vmtoolsd.exe" -n vmusr
Current directory:
C:\Windows\System32\
Autostart Location:
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\VM
Explore
Parent: explorer.exe(5468)
User: DESKTOP-KEST4T0\kai_je
Started: 上午 12:43:51 2019/8/16 Image: 64-bit
Comment:
VirusTotal: 0/70
Submit
Verify
Bring to Front
Kill Process
Data Execution Prevention (DEP) Status: Enabled (permanent)
Address Space Load Randomization: Bottom-Up
Control Flow Guard: Disabled
Enterprise Context: N/A
OK
Cancel

驗證是否具有簽名檔

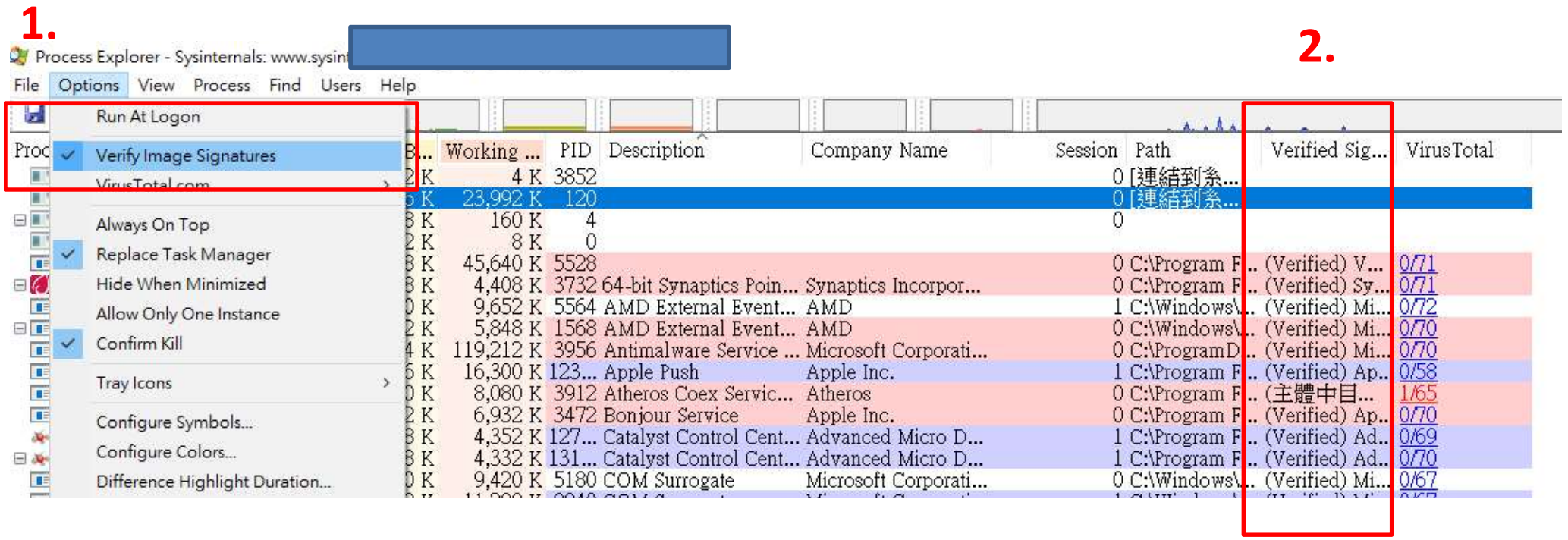

vmtoolsd.exe:8476 Properties
GPU Graph
Threads
TCP/IP
Security
Environment
Strings
Image
Performance
Performance Graph
Disk and Network
Image File
VMware Tools Core Service
(Verified) VMware, Inc.
Version: 10.0.0.50046
Build Time: Thu Aug 20 18:19:43 2015
Path:
C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
Explore
Command line:
"C:\Program Files\VMware\VMware Tools\vmtoolsd.exe" -n vmusr
Current directory:
C:\Windows\System32\
Autostart Location:
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\VM
Explore
Parent: explorer.exe(5468)
User: DESKTOP-KEST4T0\kai_je
Started: 上午 12:43:51 2019/8/16 Image: 64-bit
Comment:
VirusTotal:
Submit
Verify
Bring to Front
Kill Process
Data Execution Prevention (DEP) Status: Enabled (permanent)
Address Space Load Randomization: Bottom-Up
Control Flow Guard: Disabled
Enterprise Context: N/A
OK
Cancel

取代/取消 預設的工作管理員(2)



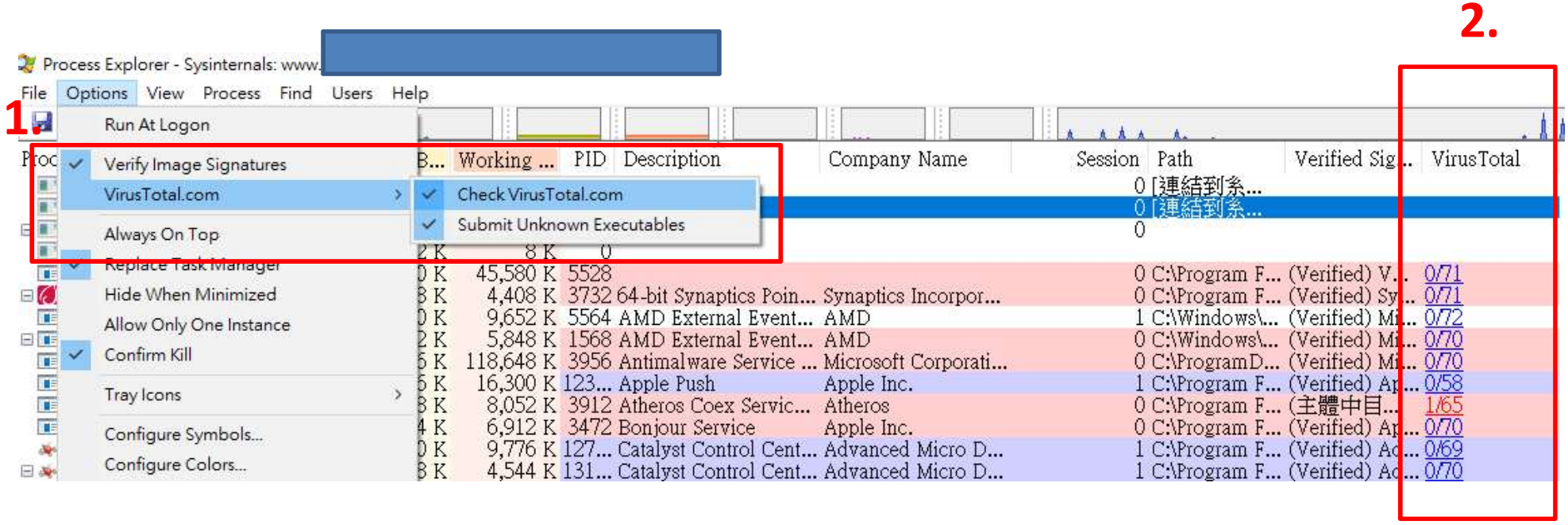
驗證簽名檔(所有行程)

- Options →Verify Image Signatures



檢查是否為惡意程序(所有行程)

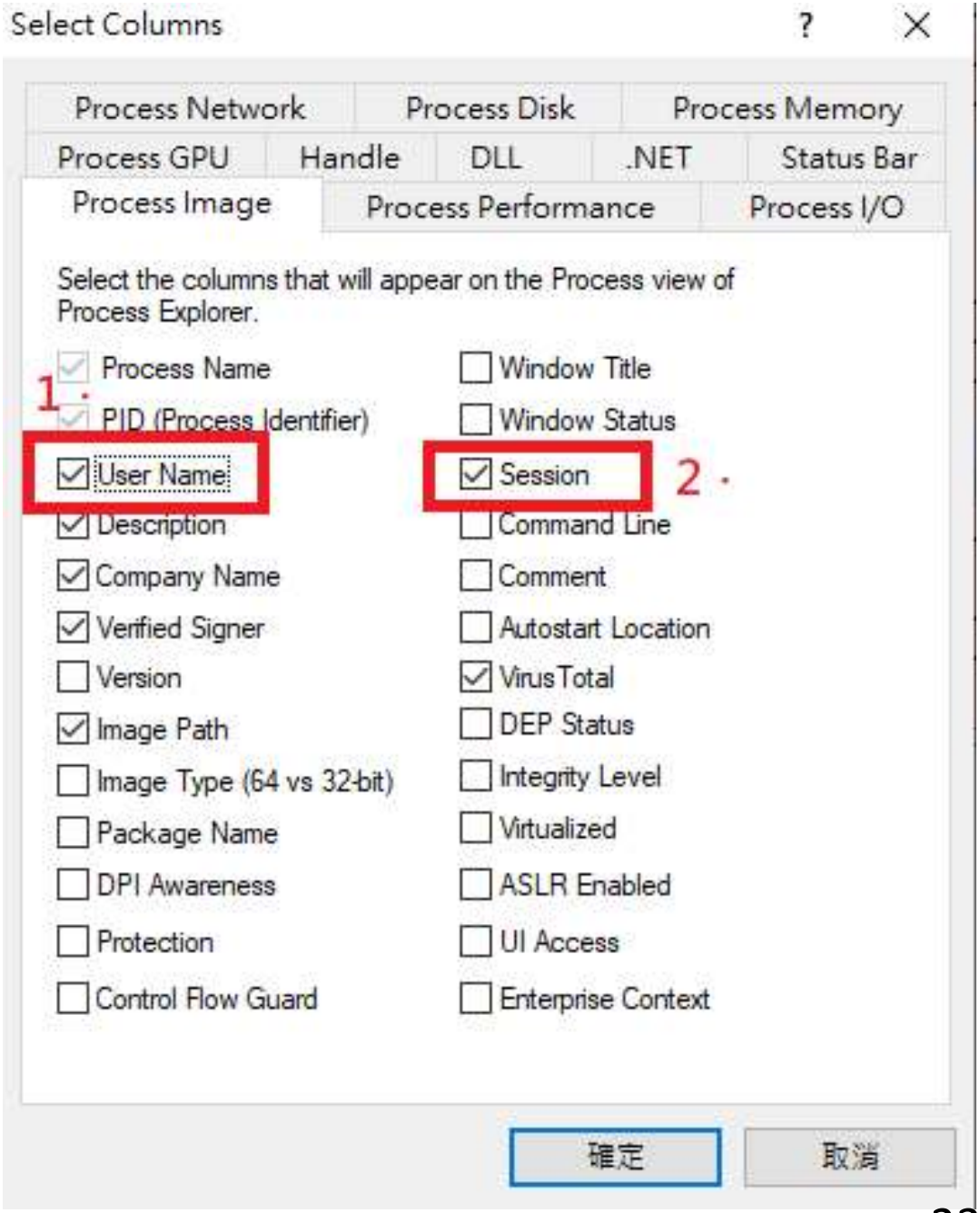
- Options →VirusTotal.com → Check VirusTotal.com



找出可疑程序(2)

- 選用其他欄位項目
  - UserName
  - Session

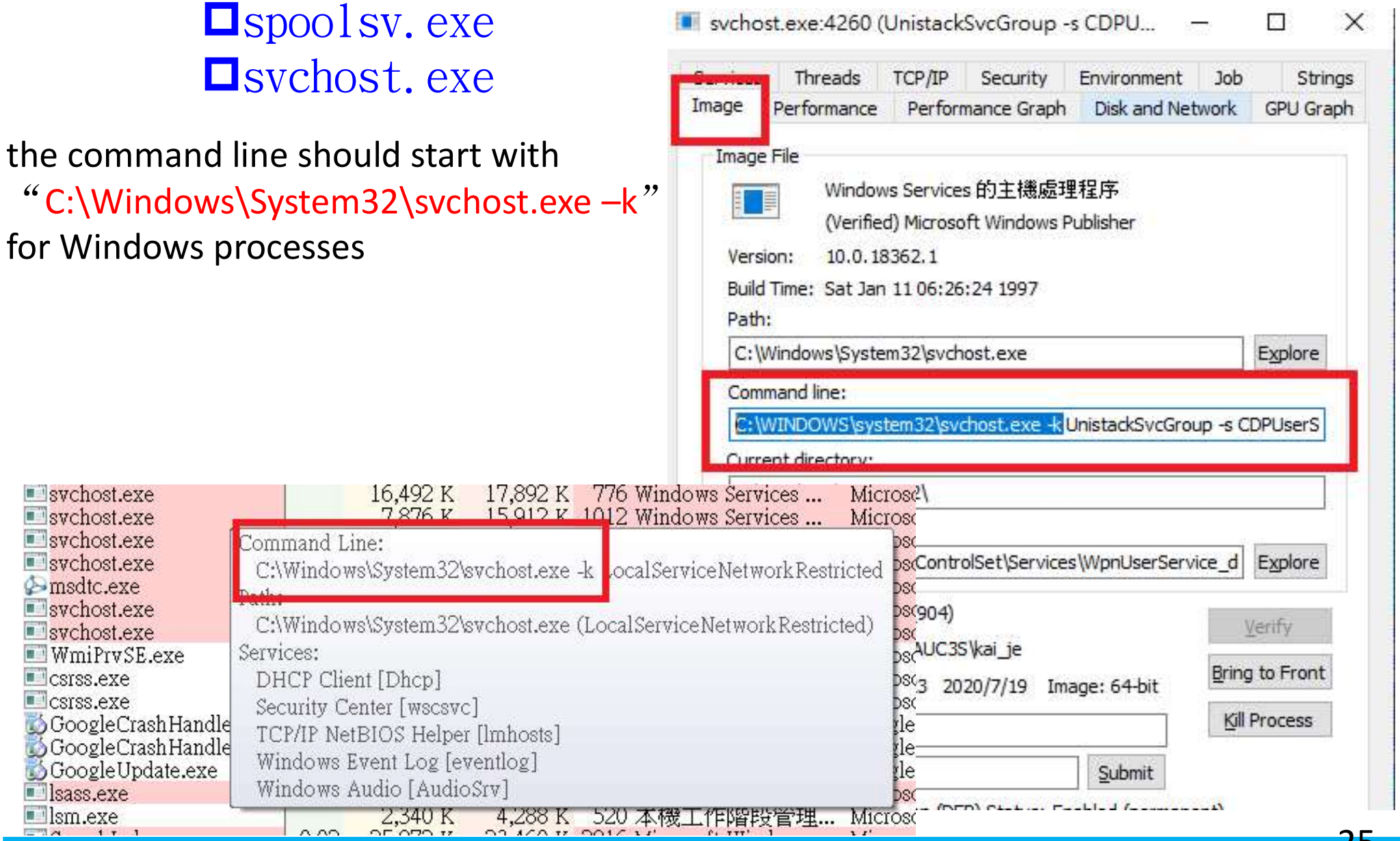
- View →Select Columns



檢視Command Line 參數

- 點擊 Svchost.exe 程序2下，並開啟視窗
  - spoolsv.exe
  - svchost.exe

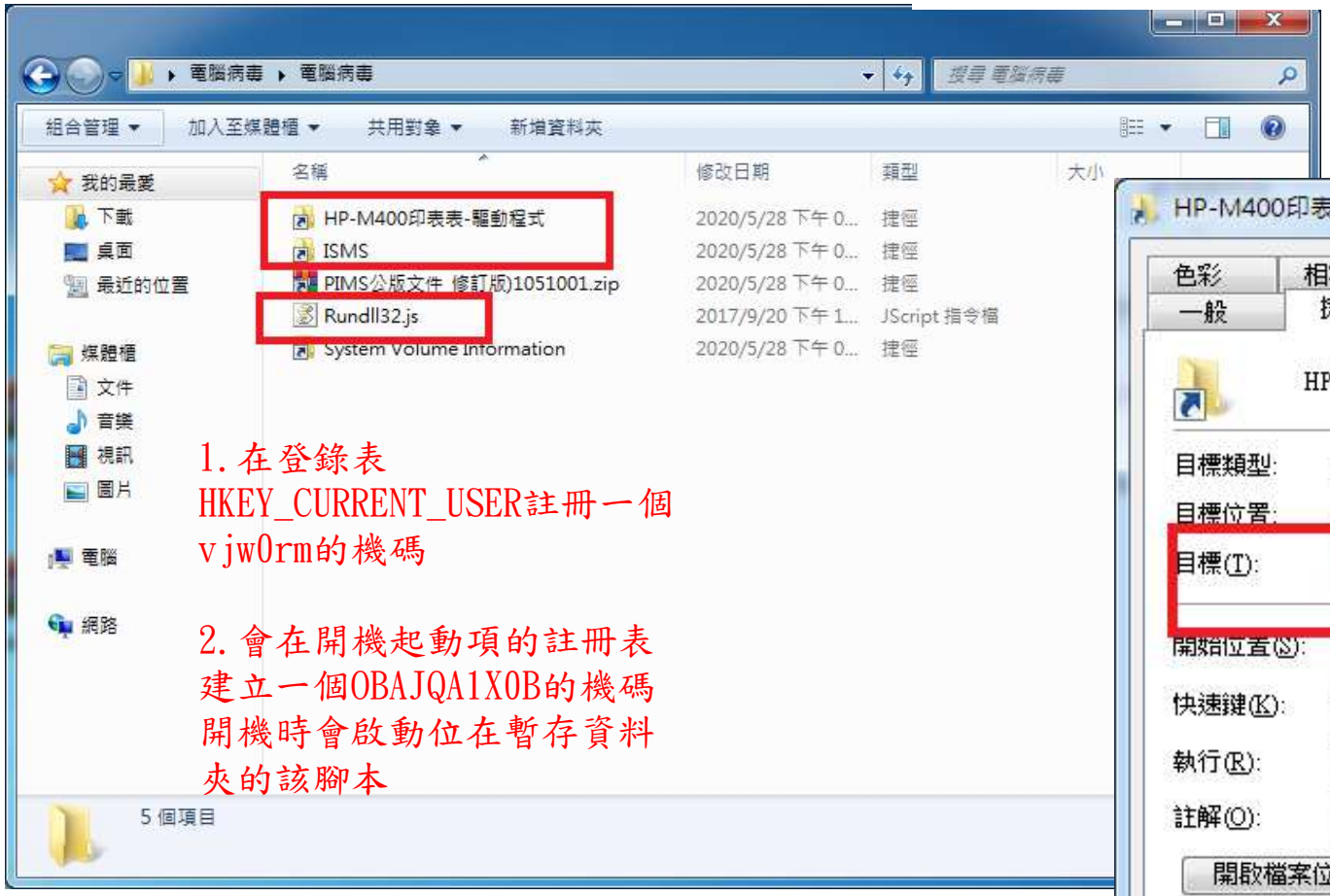
the command line should start with
"C:\Windows\System32\svchost.exe –k"
for Windows processes



- 請先再建立一個系統「還原點」或快照
- 請在虛擬機主練習執行「電腦病毒」，並觀察下列資訊：
  - USB隨身碟中是否產生相關的病毒程式
  - 嘗試刪除USB隨身碟中的「惡意程式」後，有何變化
- 請利用「還原點」/快照還原電腦，再嘗試刪除USB隨身碟中的「惡意程式」，是否會成功
- 成功刪除惡意程式後，還原被隱藏的檔案(解除反白)
- 測試再接入USB時，是否還被寫入惡意程式

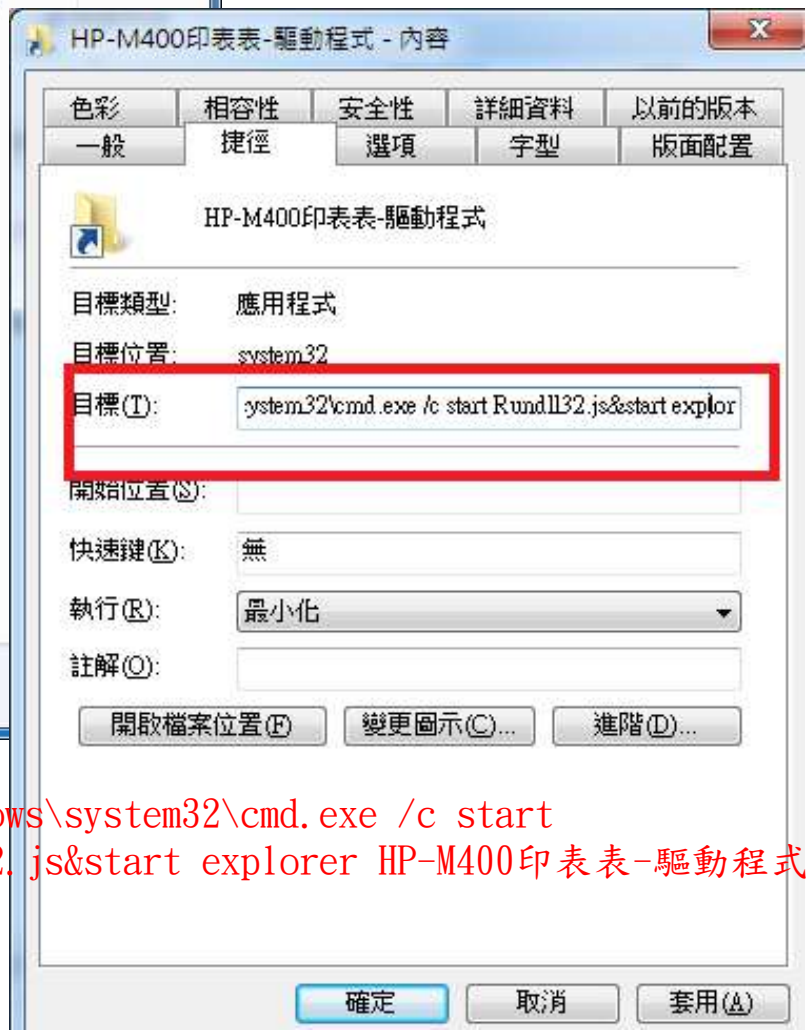
捷徑病毒中毒症狀

Process Explorer 工具應用



1.在登錄表HKEY_CURRENT_USER註冊一個vjwOrm的機碼

2.會在開機起動項的註冊表建立一個OBAJQA1XOB的機碼開機時會啟動位在暫存資料夾的該腳本



C:\Windows\system32\cmd.exe /c start Rundll32.js&start explorer HP-M400印表表-驅動程式 &exit

資料參考網址：

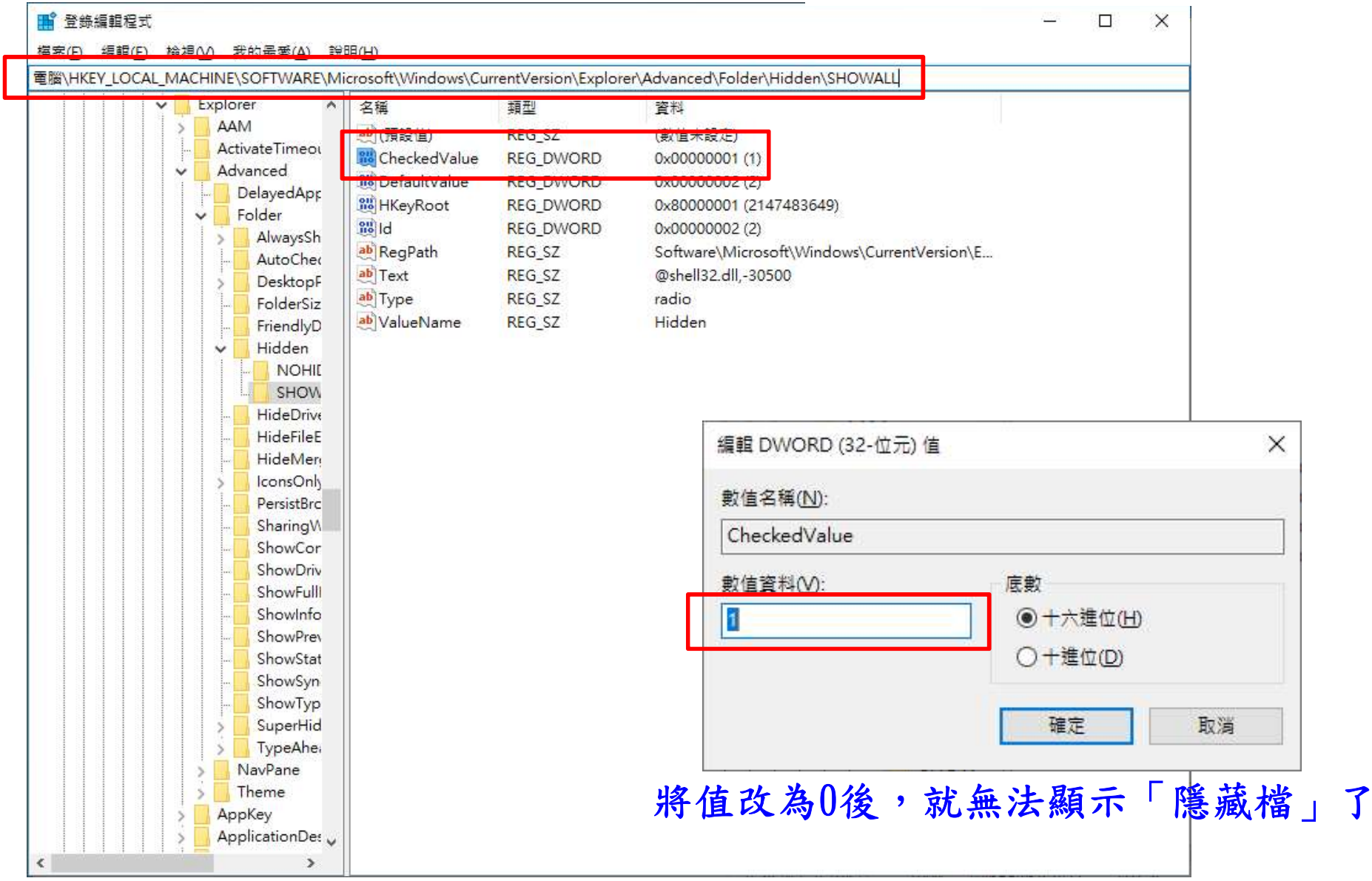
https://gist.github.com/poynt2005/165abc6cdf8d0d1fb9b6c3c98517f2a4

捷徑病毒中毒症狀(2)

- 在USB隨身碟中產生病毒捷徑、隱藏原來的資料與產生rundll32.js病毒檔
- 在登錄表HKEY_CURRENT_USER註冊一個vjw0rm的機碼
- 會在「開機起動項」的註冊表建立一個OBAJQA1X0B的機碼
  - 開機時會啟動位在暫存資料夾的該腳本
- 建立排程(每30分鐘執一次)
- 讓系統無法顯示隱藏檔
- 點選檔案捷徑後，就會感染電腦病毒

解決無法顯示隱藏檔問題

Process Explorer

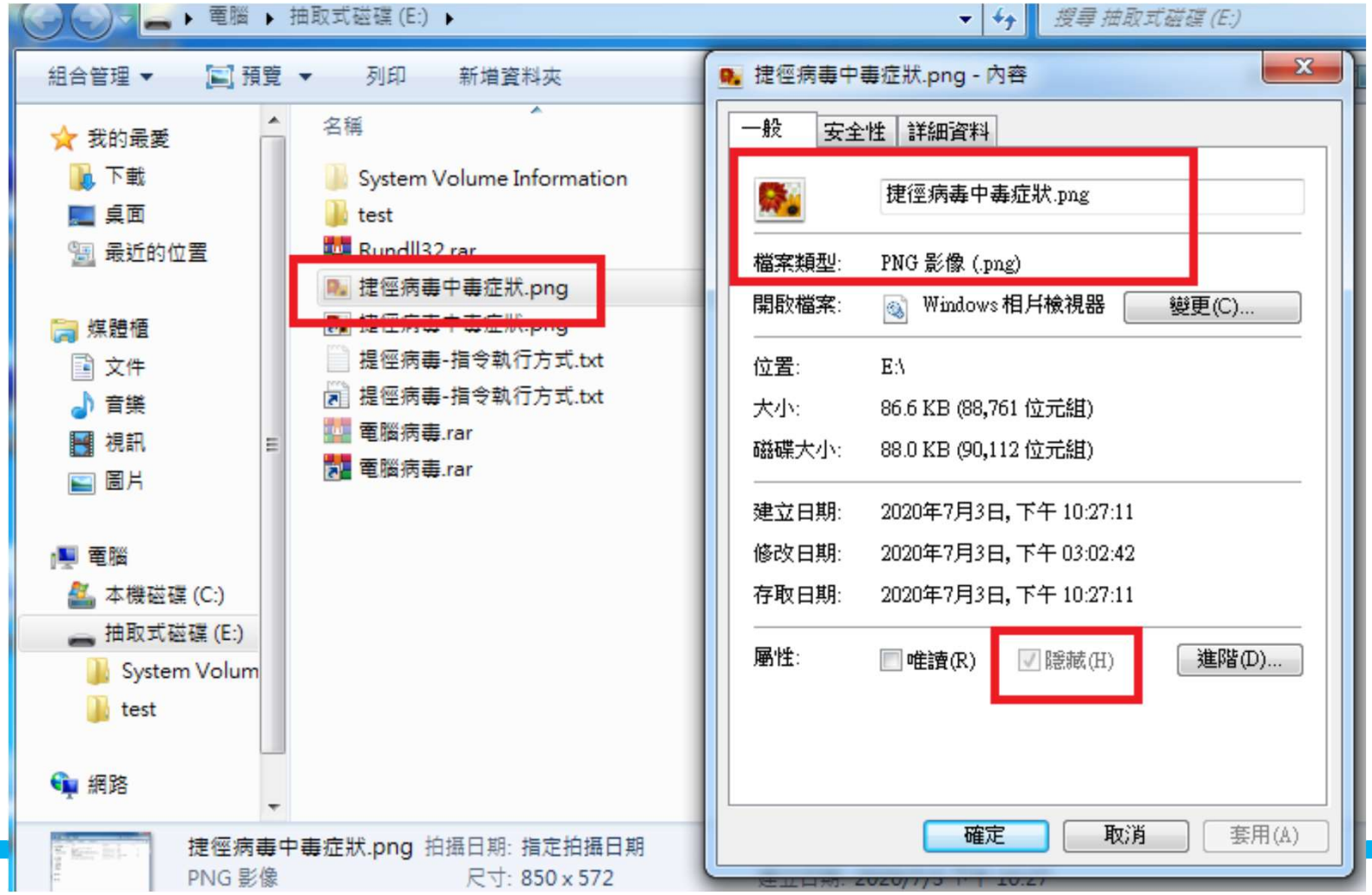


將值改為0後，就無法顯示「隱藏檔」了

電腦
\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Folder\Hidden\SHOWALL

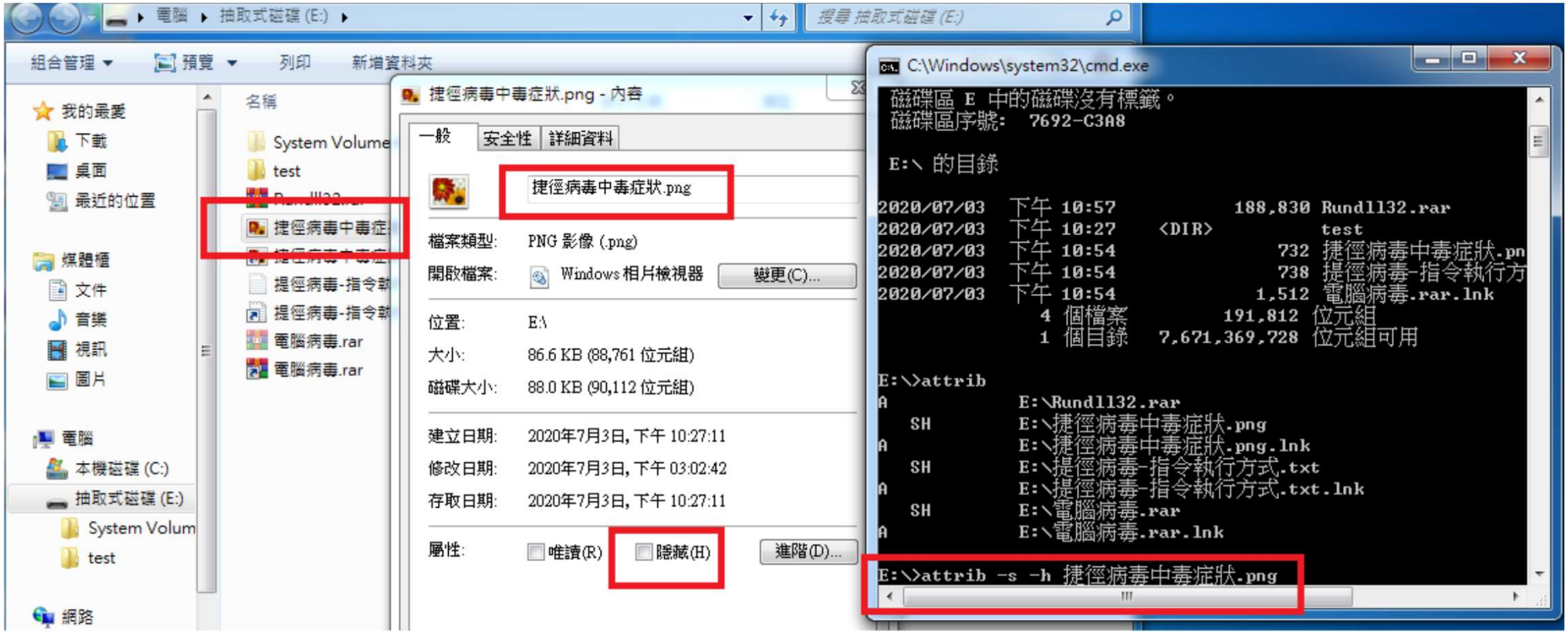
解決無法取消隱藏問題(2)

Process Explorer

- dir/ah　dir/as
- attrib -s -h e:\file　強制解除檔案隱藏指令
- attrib +s +h e:\file　強制進行檔案隱藏指令(GUI)介面會看到反白的
- 

解決無法取消隱藏問題(3) Process Explorer

```
attrib -s -h e:\file      強制解除檔案隱藏指令
attrib +s +h e:\file      強制進行檔案隱藏指令(GUI)介面會看到
```



THANK YOU

~ 簡報結束，謝謝 ~

Thank you for listening