Cuckoo Sandbox and Noriben

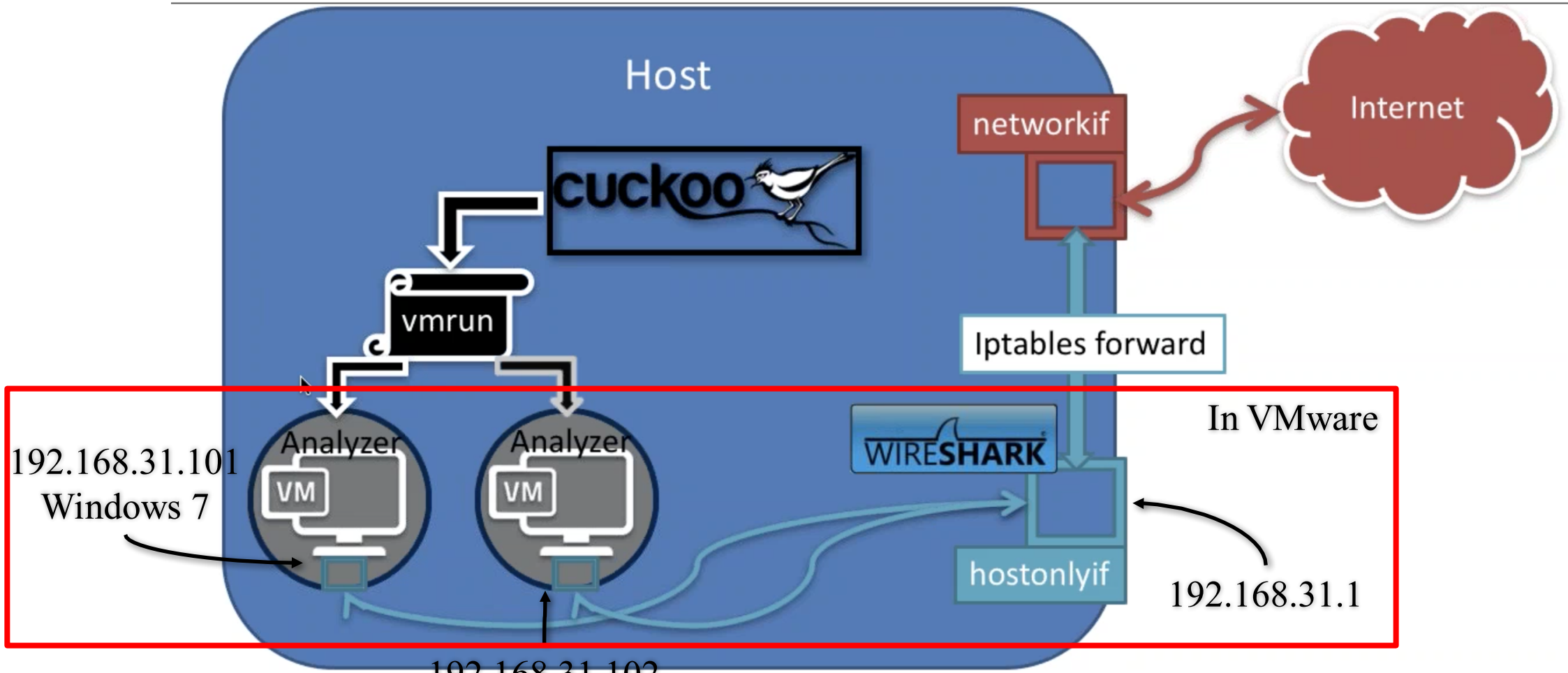
賴家民 SENALAI@III.ORG.TW

1. Cuckoo SandBox
2. Procmon
3. Noriben

Cuckoo Sandbox

- Traces of calls performed by all processes spawned by the malware.
- Files being created, deleted and downloaded by the malware during its execution.
- Memory dumps of the malware processes.
- Network traffic trace in PCAP format.
- Screenshots taken during the execution of the malware.
- Full memory dumps of the machines.

Architecture



Requirements

- Virtual Machine : VMware Fusion
- Host : Mac OS X 10.12.6
- Client : Windows 7 x64

Preparing Client

- Drop agent.py to Guset Client

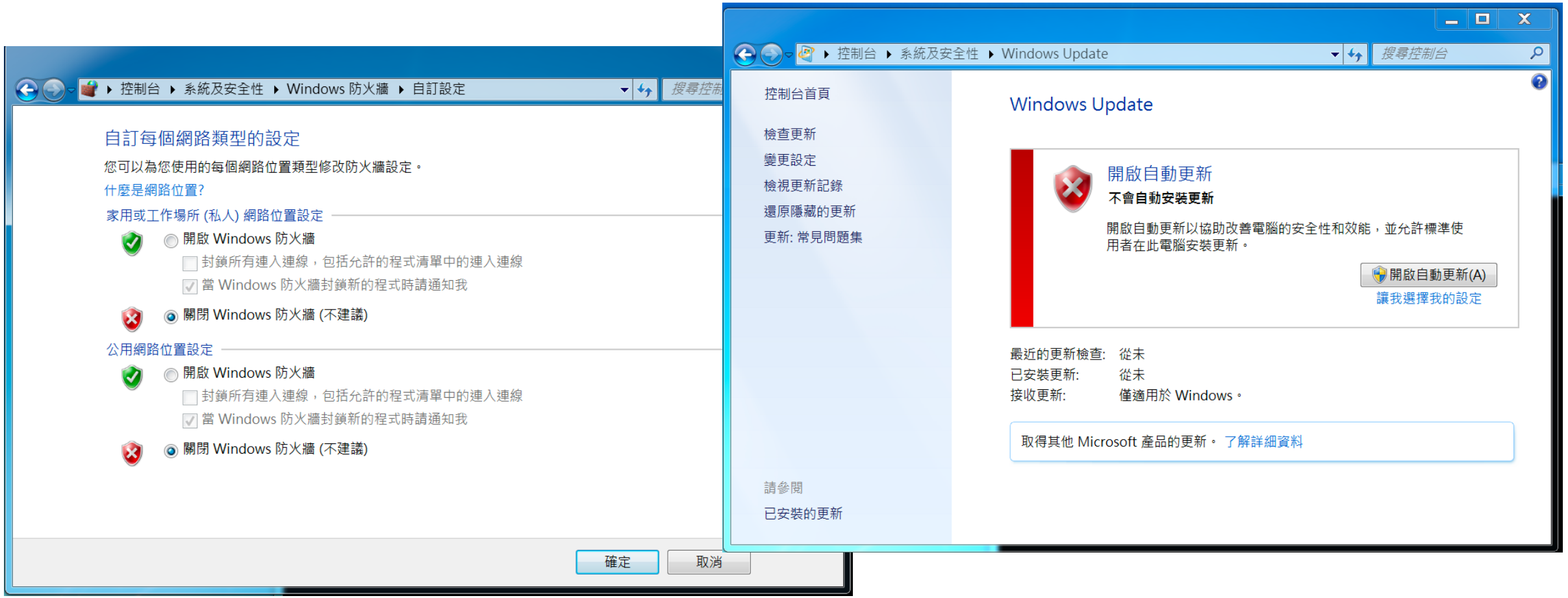
- Python 2.7
  - https://www.python.org/ftp/python/2.7.13/python-2.7.13rc1.msi
  - For agent.py
  - Rename the file from agent.py to **agent.pyw** which will prevent the console window from spawning.

- Python Pillow
  - http://effbot.org/downloads/PIL-1.1.7.win32-py2.7.exe
  - For screenshot

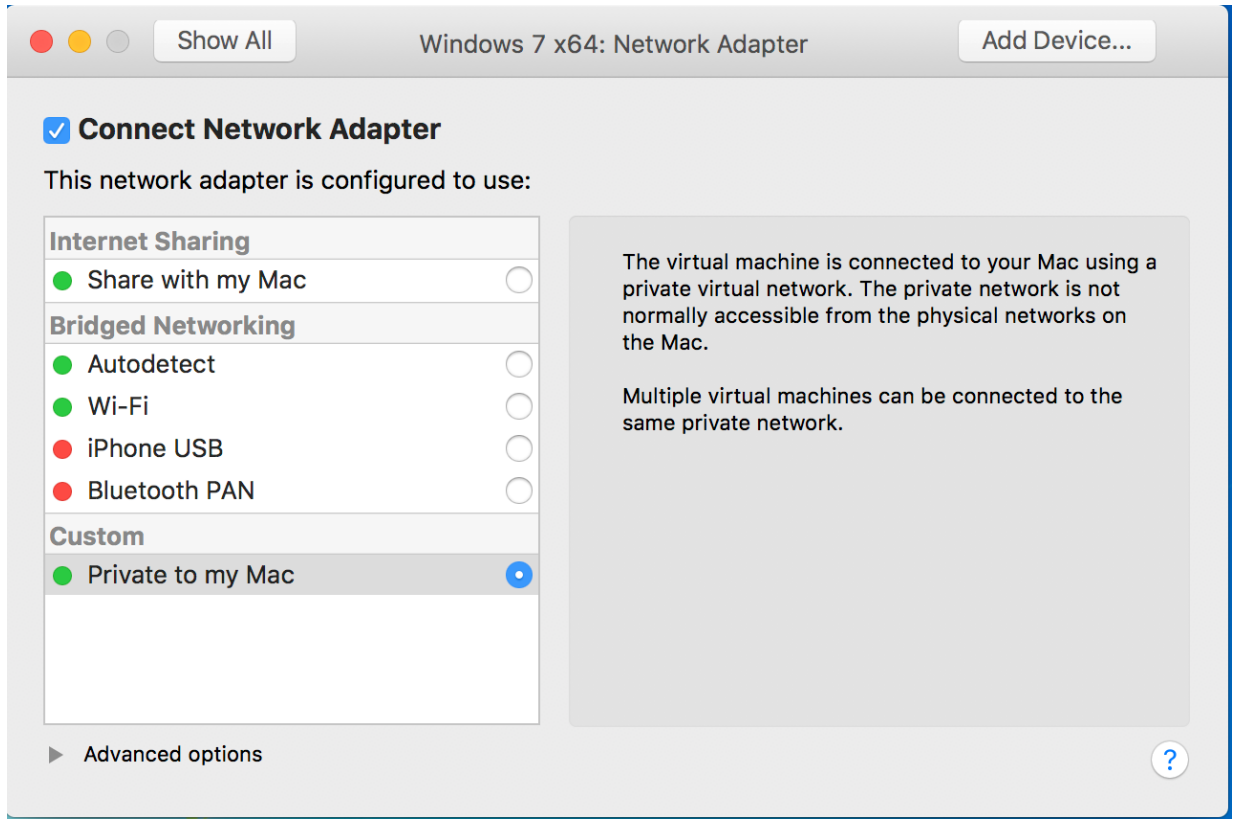
Preparing Client

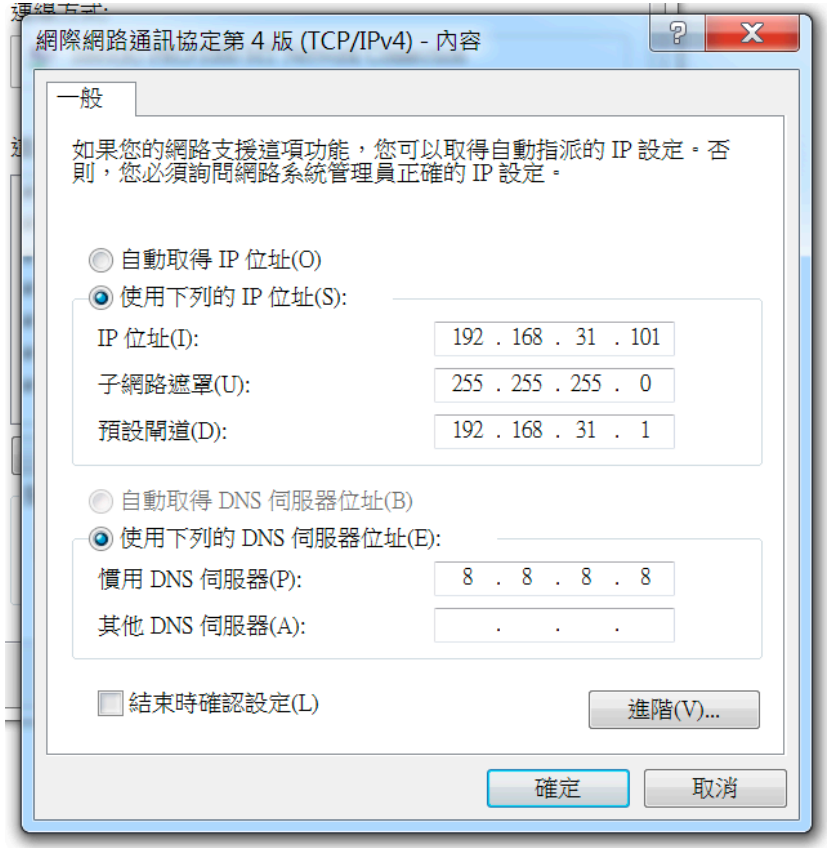
- Enable auto-logon
  - reg add "hklm\software\Microsoft\Windows NT\CurrentVersion\WinLogon" /v DefaultUserName /d <USERNAME> /t REG_SZ /f
  - reg add "hklm\software\Microsoft\Windows NT\CurrentVersion\WinLogon" /v DefaultPassword /d <PASSWORD> /t REG_SZ /f
  - reg add "hklm\software\Microsoft\Windows NT\CurrentVersion\WinLogon" /v AutoAdminLogon /d 1 /t REG_SZ /f
  - https://support.microsoft.com/zh-tw/help/324737/how-to-turn-on-automatic-logon-in-windows

Preparing Client

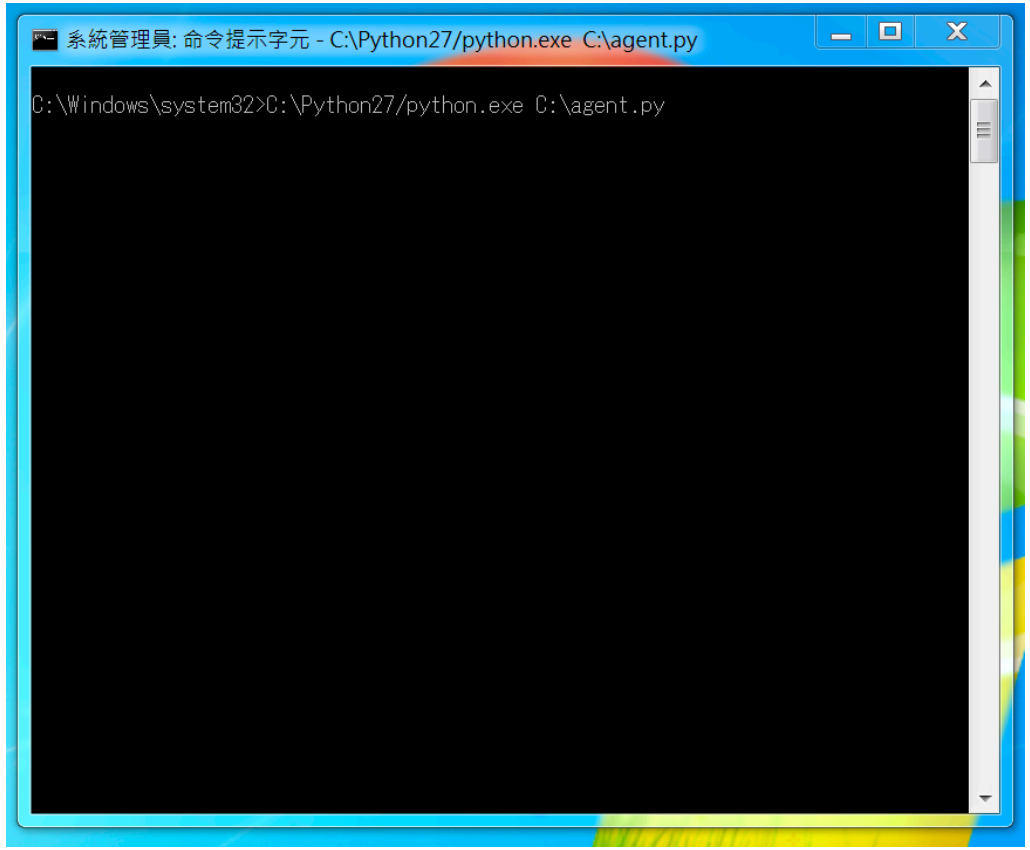


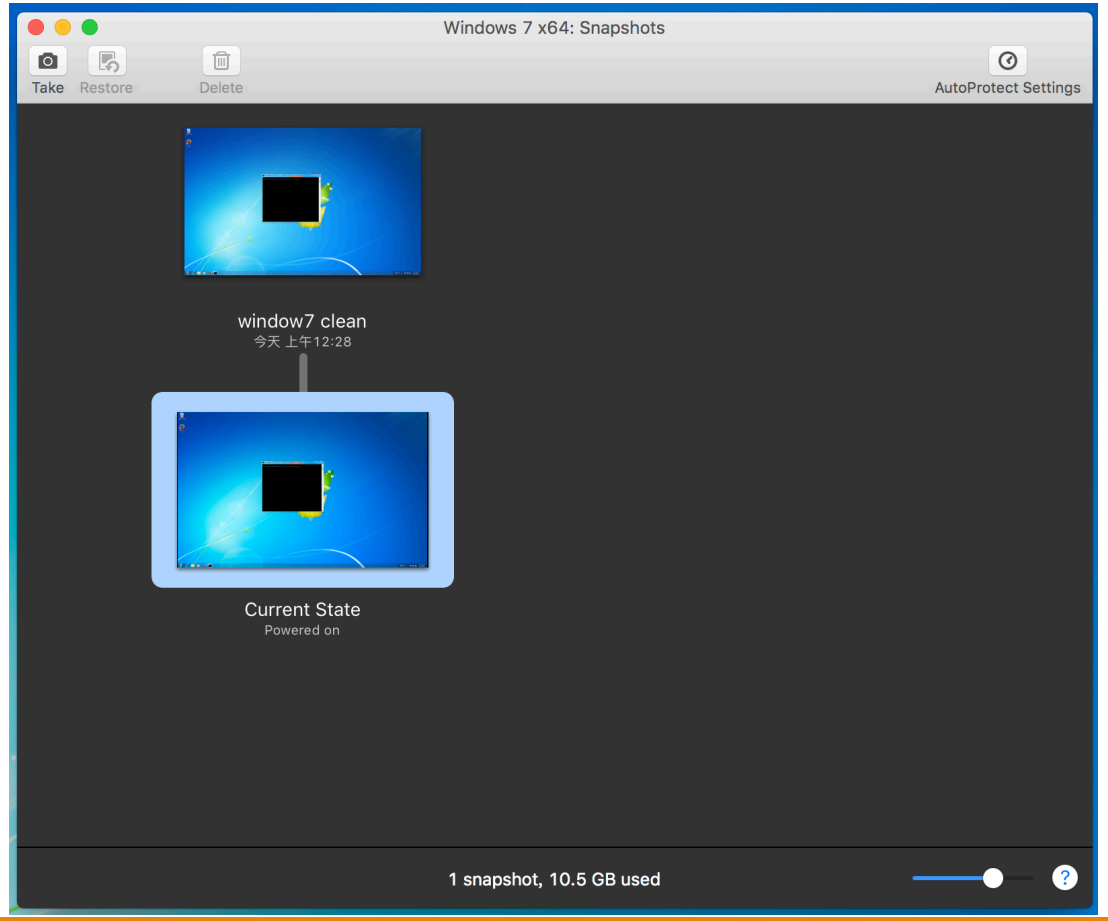
Preparing Client





Preparing Guest Client





Preparing Host

$ sudo pip install -U pip setuptools

$ sudo pip install -U cuckoo

or

$ virtualenv cuckoo

$ source cuckoo/bin/activate

(cuckoo)$ pip install -U pip setuptools

(cuckoo)$ pip install -U cuckoo

Preparing Host(Ubuntu)

$ sudo apt-get install python python-pip python-dev libffi-dev libssl-dev

$ sudo apt-get install python-virtualenv python-setuptools

$ sudo apt-get install libjpeg-dev zlib1g-dev swig

$ sudo apt-get install mongodb

$ sudo apt-get install tcpdump apparmor-utils

$ sudo aa-disable /usr/sbin/tcpdump

$ sudo setcap cap_net_raw,cap_net_admin=eip /usr/sbin/tcpdump

(http://blog.csdn.net/mark20170902/article/details/53422384)

Preparing Host(Ubuntu)

- Setting IP Forwarding

```
1 iptables -A FORWARD -o ens33 -i ens38 -s 192.168.31.0/24 -m conntrack --ctstate NEW -j ACCEPT
2
3 iptables -A FORWARD -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
4
5 iptables -A POSTROUTING -t nat -j MASQUERADE
6
7 sysctl -w net.ipv4.ip_forward=1
```

Preparing Host (Mac)

$ brew install libmagic

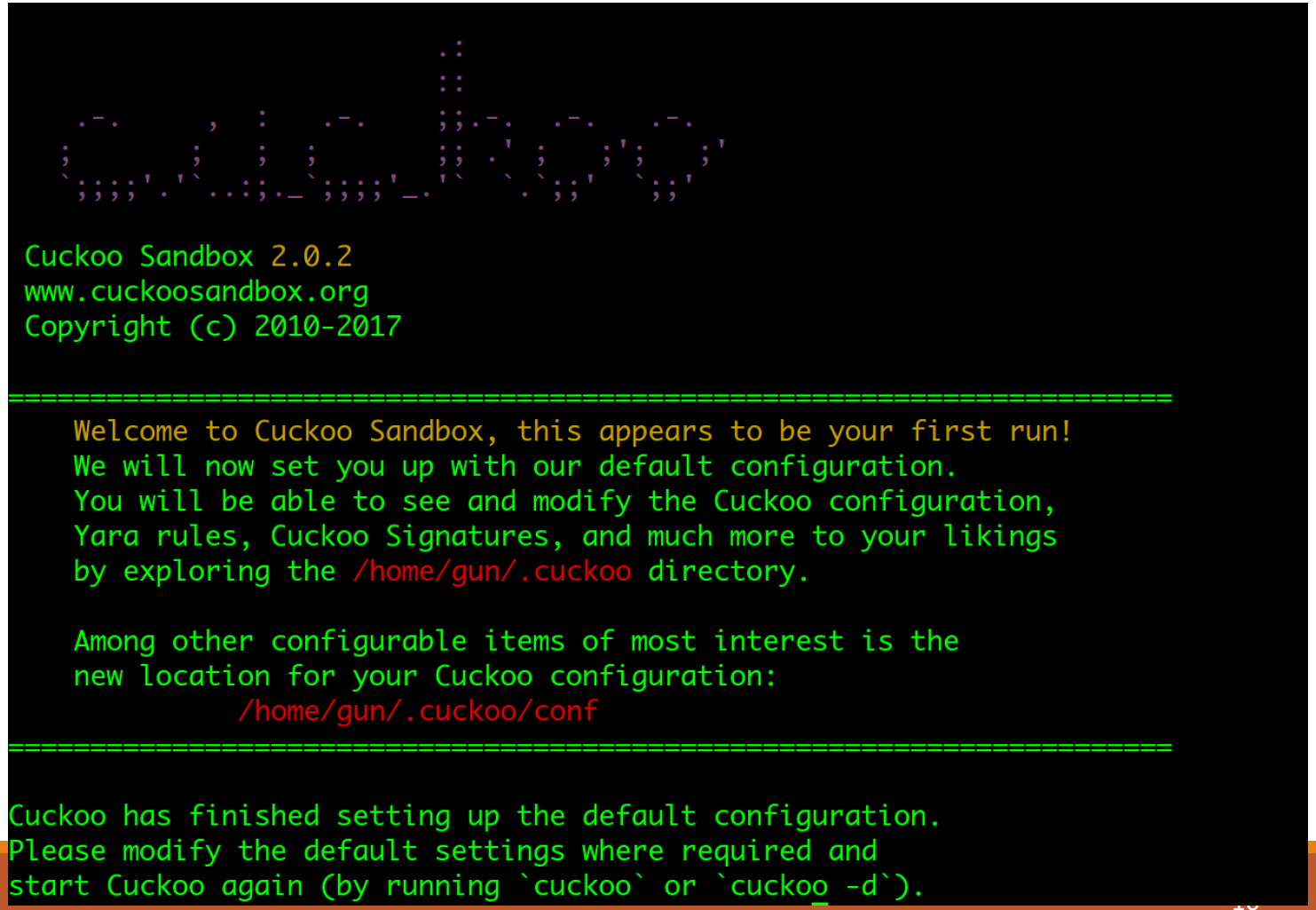
Preparing Host (Mac)

- Setting ip Forwarding

```
sudo sysctl -w net.inet.ip.forwarding=1 #setting mac os x port forwarding
rules="nat on en0 from vmnet2:network to any ->(en0)
pass inet proto icmp all
pass in on vmnet2 proto udp from any to any port domain keep state
pass quick on en0 proto udp from any to any port domain keep state"
echo "$rules" > ./pfrules
sudo pfctl -e -f ./pfrules
```

Preparing Host

- Initial Cuckoo
  - (cuckoo) $ cuckoo -d



Preparing Host

- Configuring general behavior and analysis options
  - (cuckoo) $ vim ~/.cuckoo/conf/cuckoo.conf

- Modify part
  - ip = 192.168.31.1
  - machinery = vmware

Preparing Host

- Enabling and configuring auxiliary modules
  - (cuckoo) $ vim ~/.cuckoo/conf/auxiliary.conf

- Modify part
  - None

Preparing Host

- Volatility configuration
  - (cuckoo) $ vim ~/.cuckoo/conf/memory.conf

- Modify part
  - None

Preparing Host

- Enabling and configuring processing modules
  - (cuckoo) $ vim ~/.cuckoo/conf/processing.conf
- Modify part
  - [Virustotal]
    - enable = yes

Preparing Host

- Enabling or disabling report formats
  - (cuckoo) $ vim ~/.cuckoo/conf/reporting.conf

- Modify part
  - [mongodb]
    - enable = yes

Preparing Host

- Enabling or disabling report formats
  - (cuckoo) $ vim ~/.cuckoo/conf/vmware.conf
- Modify part
  - path = /Applications/VMware Fusion.app/Contents/Library/vmrun
  - interface = vmnet2
  - machines = windows7
  - [windows7]
    - vmx_path = /Users/scml/Documents/VirtualMachines.localized/Cuckoo.vmwarevm/Cuckoo1.vmx
    - Snapshot = Cuckoo Clean
    - ip = 192.168.31.101

Preparing Host

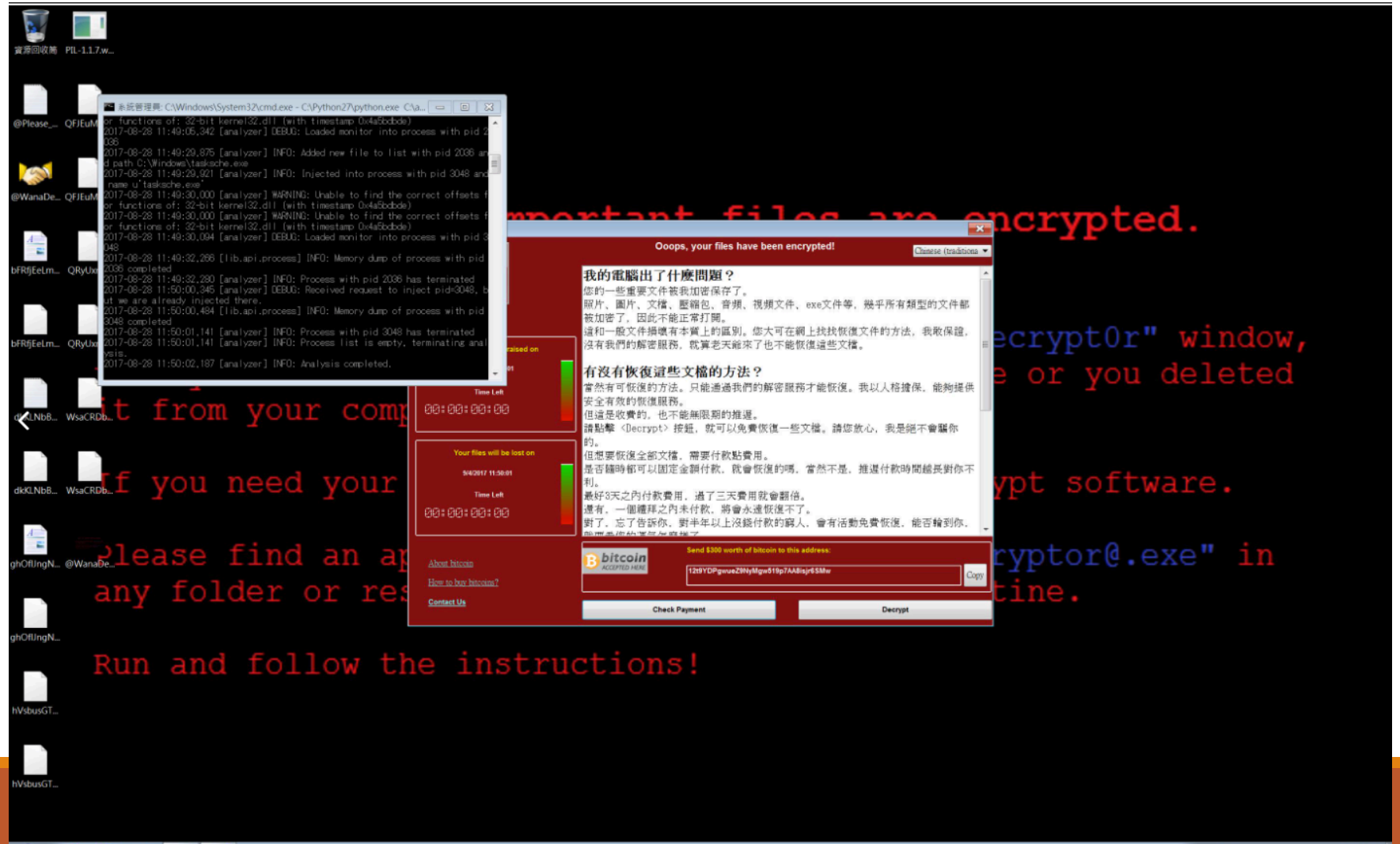
```
(cuckoo) scml@MBPR [~/Documents/cuckoo]: cuckoo

  .-----------------.
  | Cuckoo Sandbox? |
  |     OH NOES!    |\  '-.__.-'
  '-----------------' \  /oo |--.--,--,--.
                      \_.-'._i__i__i_.'
                         """""""""""


 Cuckoo Sandbox 2.0.3
 www.cuckoosandbox.org
 Copyright (c) 2010-2017

 Checking for updates...
 You're good to go!
2017-08-26 15:58:16,585 [cuckoo.core.startup] WARNING: Unable to import yara (install with `pip install yara-python==3.5.0`)
2017-08-26 15:58:16,586 [cuckoo] WARNING: It appears that you haven't loaded any Cuckoo Signatures. Signatures are highly recommended and improve & enrich t
he information extracted during an analysis. They also make up for the analysis score that you see in the Web Interface - so, pretty important!
2017-08-26 15:58:16,586 [cuckoo] WARNING: You'll be able to fetch all the latest Cuckoo Signaturs, Yara rules, and more goodies by running the following com
mand:
2017-08-26 15:58:16,586 [cuckoo] INFO: $ cuckoo community
2017-08-26 15:58:16,588 [cuckoo.core.scheduler] INFO: Using "vmware" as machine manager
CuckooConfigurationError: Option Cuckoo is not found in configuration
```

Preparing Host

- (cuckoo) $ cuckoo community

- (cuckoo) $ git clone --recursive https://github.com/VirusTotal/yara-python
- (cuckoo) $ cd yara-python
- (cuckoo) $ python setup.py build
- (cuckoo) $ python setup.py install

Wannacry @ Cuckoo



Process Monitor

Process Monitor

Process Monitor是windows系統的即時監控程式, 可以對process , activity, File, Registry, Network…等等進行分析

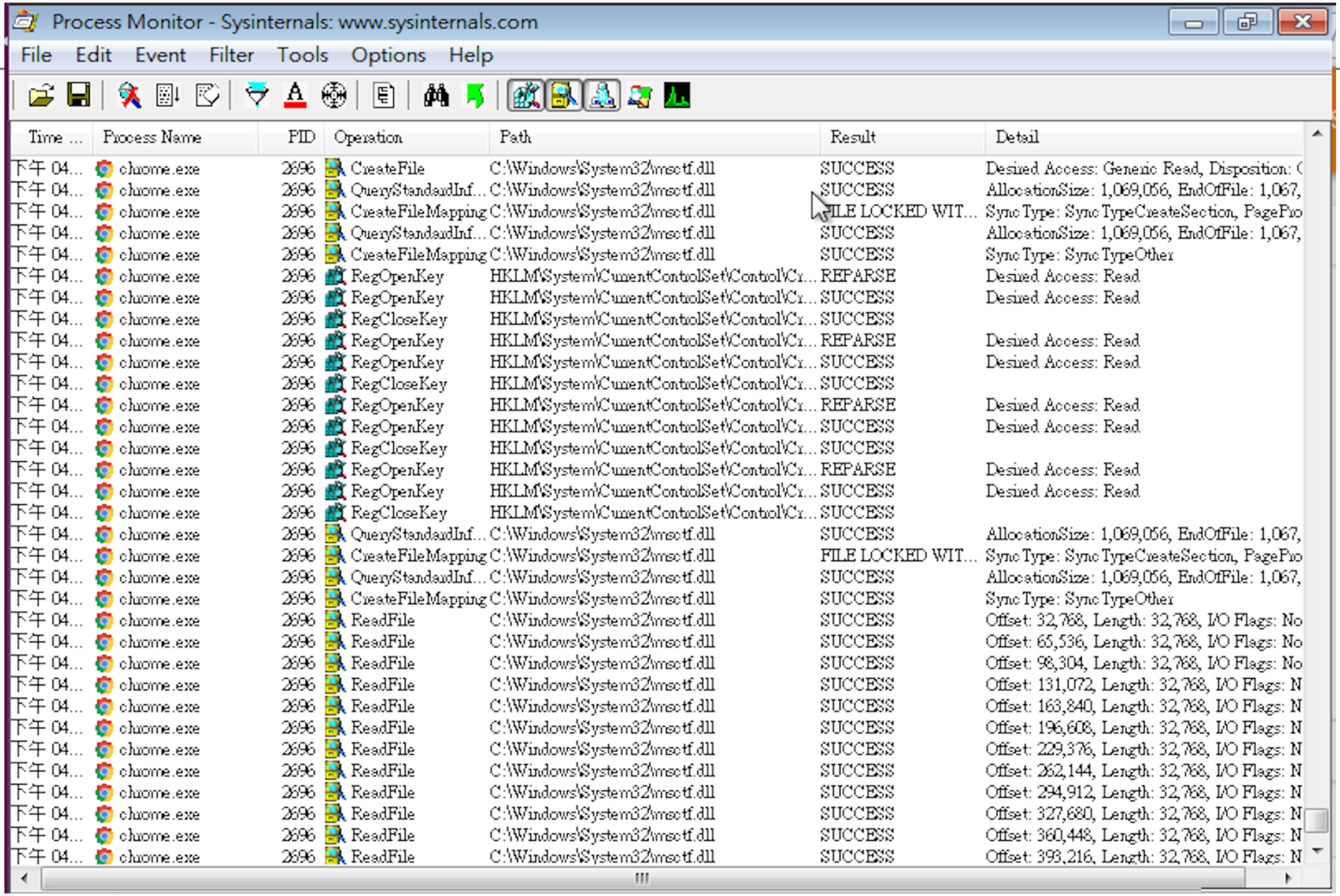
- 同時監控Registry和Process

Process Monitor v3.33

免安裝, 直接執行exe檔

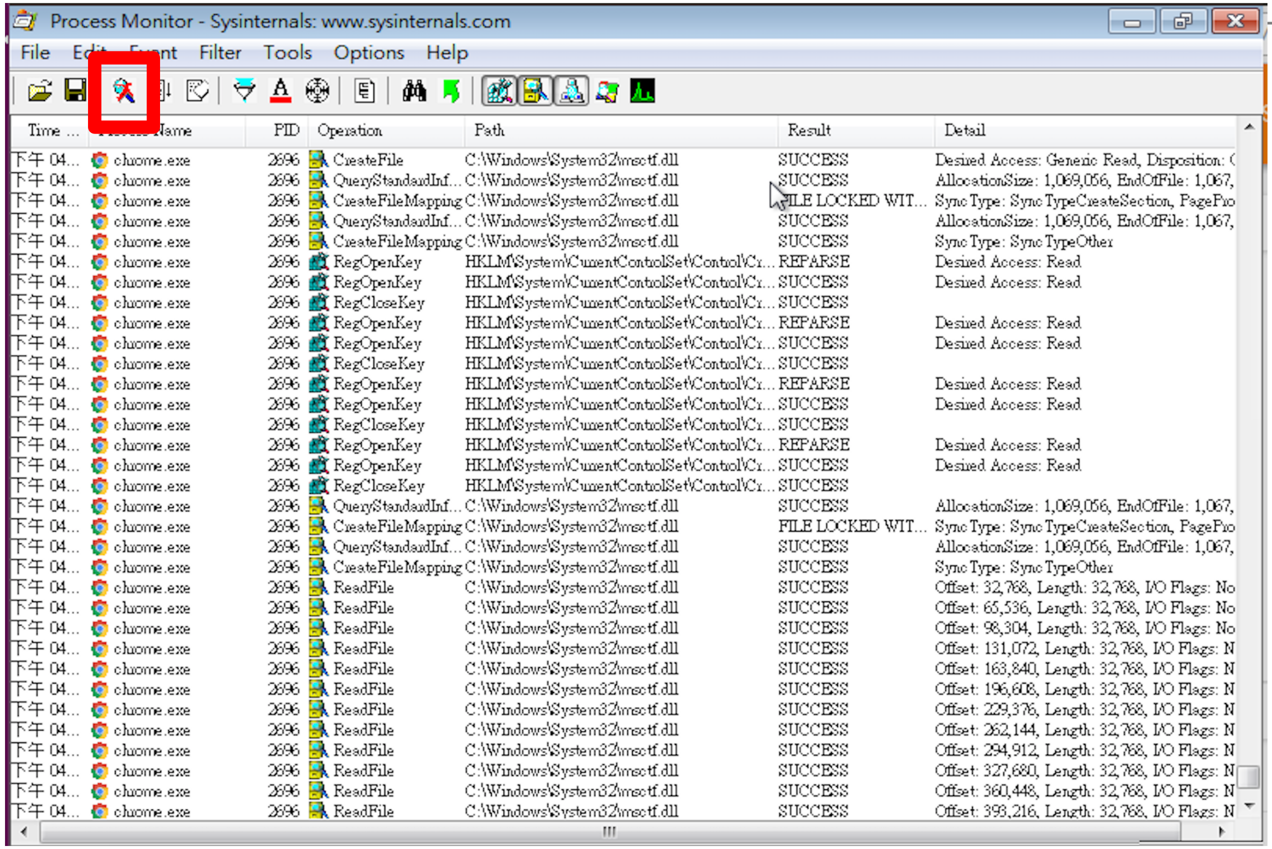
下載網址: https://technet.microsoft.com/en-us/sysinternals/processmonitor.aspx

主畫面



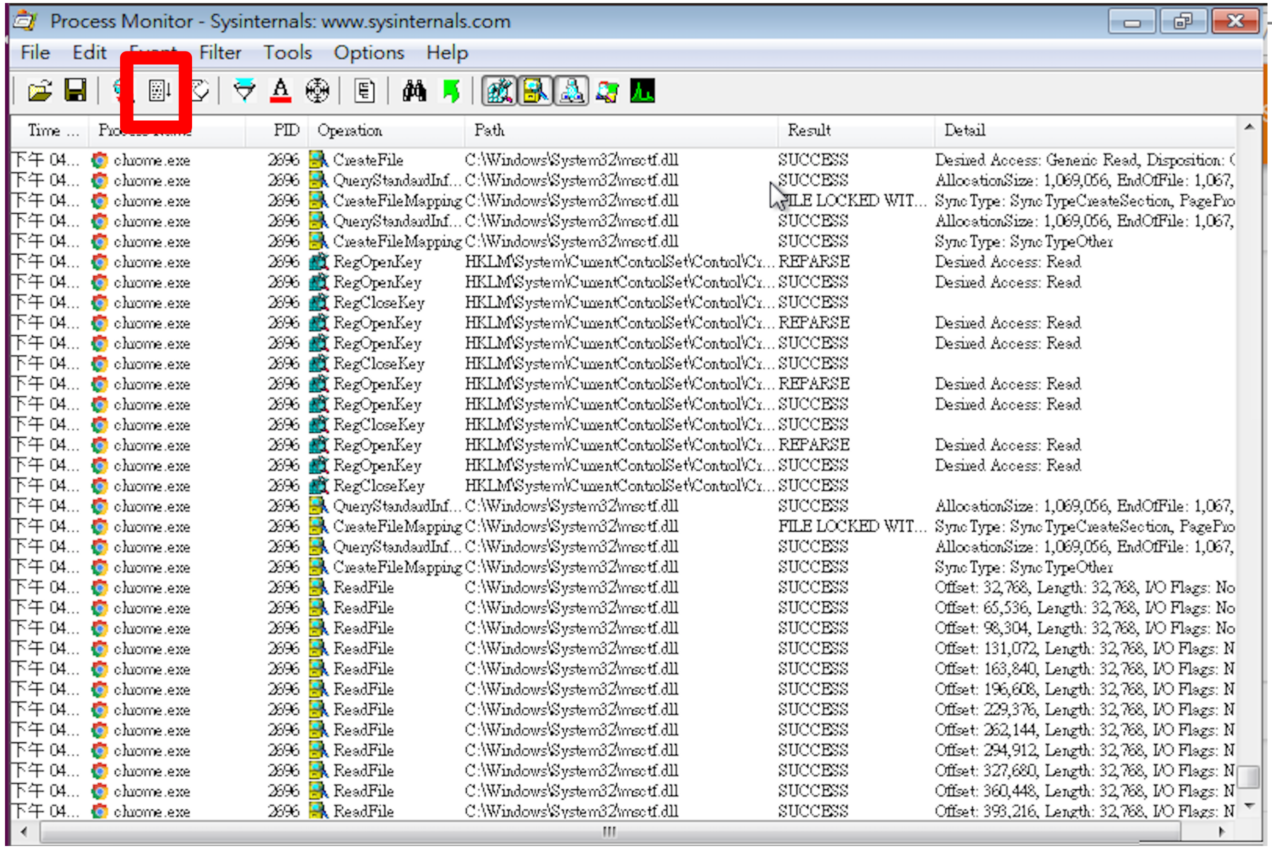
Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Time ... Process Name PID Operation Path Result Detail
下午 04... chrome.exe 2696 CreateFile C:\Windows\System32\msctf.dll SUCCESS Desired Access: Generic Read, Disposition: (
下午 04... chrome.exe 2696 QueryStandardInf... C:\Windows\System32\msctf.dll SUCCESS AllocationSize: 1,069,056, EndOfFile: 1,067,
下午 04... chrome.exe 2696 CreateFileMapping C:\Windows\System32\msctf.dll FILE LOCKED WIT... SyncType: SyncTypeCreateSection, PageProt
下午 04... chrome.exe 2696 QueryStandardInf... C:\Windows\System32\msctf.dll SUCCESS AllocationSize: 1,069,056, EndOfFile: 1,067,
下午 04... chrome.exe 2696 CreateFileMapping C:\Windows\System32\msctf.dll SUCCESS SyncType: SyncTypeOther
下午 04... chrome.exe 2696 RegOpenKey HKLM\System\CurrentControlSet\Control\Cr... REPARSE Desired Access: Read
下午 04... chrome.exe 2696 RegOpenKey HKLM\System\CurrentControlSet\Control\Cr... SUCCESS Desired Access: Read
下午 04... chrome.exe 2696 RegCloseKey HKLM\System\CurrentControlSet\Control\Cr... SUCCESS
下午 04... chrome.exe 2696 RegOpenKey HKLM\System\CurrentControlSet\Control\Cr... REPARSE Desired Access: Read
下午 04... chrome.exe 2696 RegOpenKey HKLM\System\CurrentControlSet\Control\Cr... SUCCESS Desired Access: Read
下午 04... chrome.exe 2696 RegCloseKey HKLM\System\CurrentControlSet\Control\Cr... SUCCESS
下午 04... chrome.exe 2696 RegOpenKey HKLM\System\CurrentControlSet\Control\Cr... REPARSE Desired Access: Read
下午 04... chrome.exe 2696 RegOpenKey HKLM\System\CurrentControlSet\Control\Cr... SUCCESS Desired Access: Read
下午 04... chrome.exe 2696 RegCloseKey HKLM\System\CurrentControlSet\Control\Cr... SUCCESS
下午 04... chrome.exe 2696 RegOpenKey HKLM\System\CurrentControlSet\Control\Cr... REPARSE Desired Access: Read
下午 04... chrome.exe 2696 RegOpenKey HKLM\System\CurrentControlSet\Control\Cr... SUCCESS Desired Access: Read
下午 04... chrome.exe 2696 RegCloseKey HKLM\System\CurrentControlSet\Control\Cr... SUCCESS
下午 04... chrome.exe 2696 QueryStandardInf... C:\Windows\System32\msctf.dll SUCCESS AllocationSize: 1,069,056, EndOfFile: 1,067,
下午 04... chrome.exe 2696 CreateFileMapping C:\Windows\System32\msctf.dll FILE LOCKED WIT... SyncType: SyncTypeCreateSection, PageProt
下午 04... chrome.exe 2696 QueryStandardInf... C:\Windows\System32\msctf.dll SUCCESS AllocationSize: 1,069,056, EndOfFile: 1,067,
下午 04... chrome.exe 2696 CreateFileMapping C:\Windows\System32\msctf.dll SUCCESS SyncType: SyncTypeOther
下午 04... chrome.exe 2696 ReadFile C:\Windows\System32\msctf.dll SUCCESS Offset: 32,768, Length: 32,768, I/O Flags: No
下午 04... chrome.exe 2696 ReadFile C:\Windows\System32\msctf.dll SUCCESS Offset: 65,536, Length: 32,768, I/O Flags: No
下午 04... chrome.exe 2696 ReadFile C:\Windows\System32\msctf.dll SUCCESS Offset: 98,304, Length: 32,768, I/O Flags: No
下午 04... chrome.exe 2696 ReadFile C:\Windows\System32\msctf.dll SUCCESS Offset: 131,072, Length: 32,768, I/O Flags: N
下午 04... chrome.exe 2696 ReadFile C:\Windows\System32\msctf.dll SUCCESS Offset: 163,840, Length: 32,768, I/O Flags: N
下午 04... chrome.exe 2696 ReadFile C:\Windows\System32\msctf.dll SUCCESS Offset: 196,608, Length: 32,768, I/O Flags: N
下午 04... chrome.exe 2696 ReadFile C:\Windows\System32\msctf.dll SUCCESS Offset: 229,376, Length: 32,768, I/O Flags: N
下午 04... chrome.exe 2696 ReadFile C:\Windows\System32\msctf.dll SUCCESS Offset: 262,144, Length: 32,768, I/O Flags: N
下午 04... chrome.exe 2696 ReadFile C:\Windows\System32\msctf.dll SUCCESS Offset: 294,912, Length: 32,768, I/O Flags: N
下午 04... chrome.exe 2696 ReadFile C:\Windows\System32\msctf.dll SUCCESS Offset: 327,680, Length: 32,768, I/O Flags: N
下午 04... chrome.exe 2696 ReadFile C:\Windows\System32\msctf.dll SUCCESS Offset: 360,448, Length: 32,768, I/O Flags: N
下午 04... chrome.exe 2696 ReadFile C:\Windows\System32\msctf.dll SUCCESS Offset: 393,216, Length: 32,768, I/O Flags: N

功能介紹



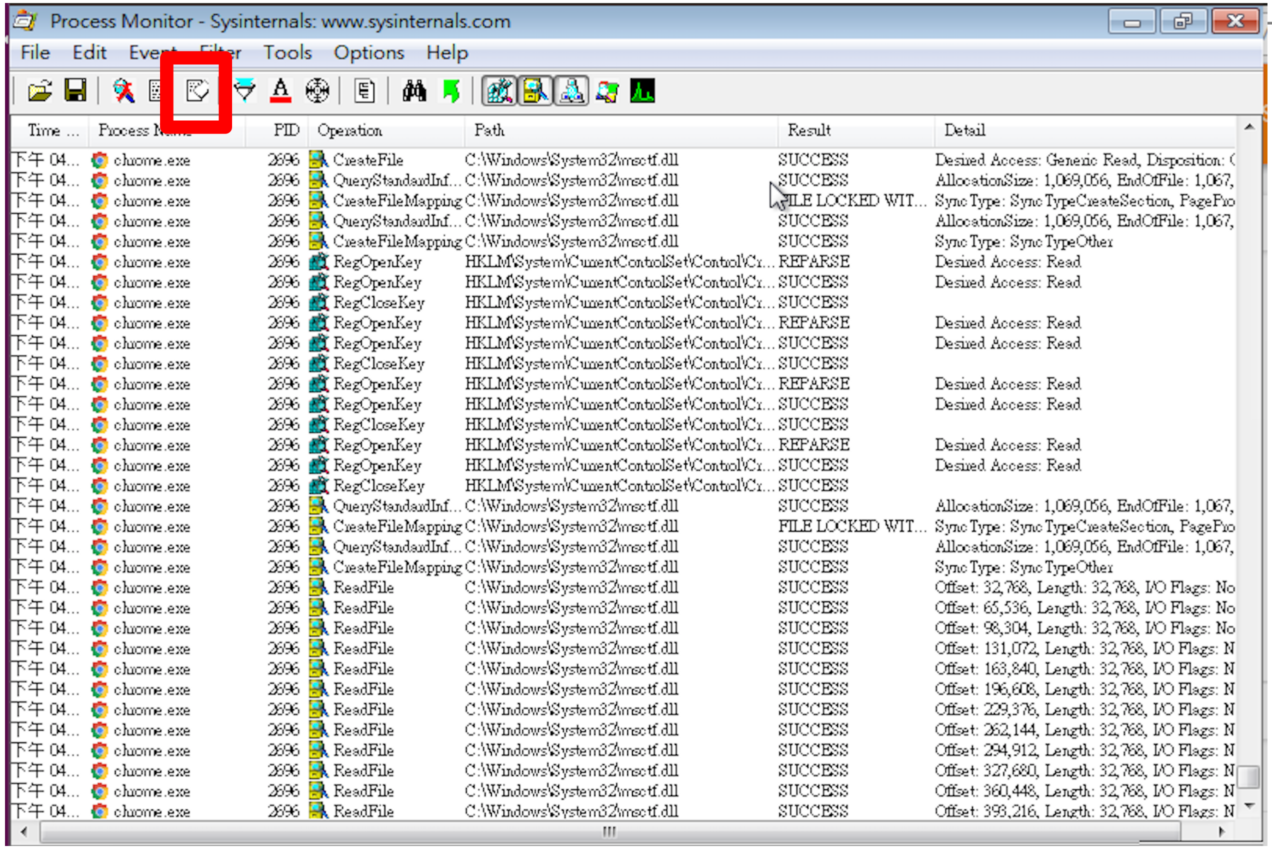
開啟/停止捕捉: 開始/停止捕捉行為

功能介紹



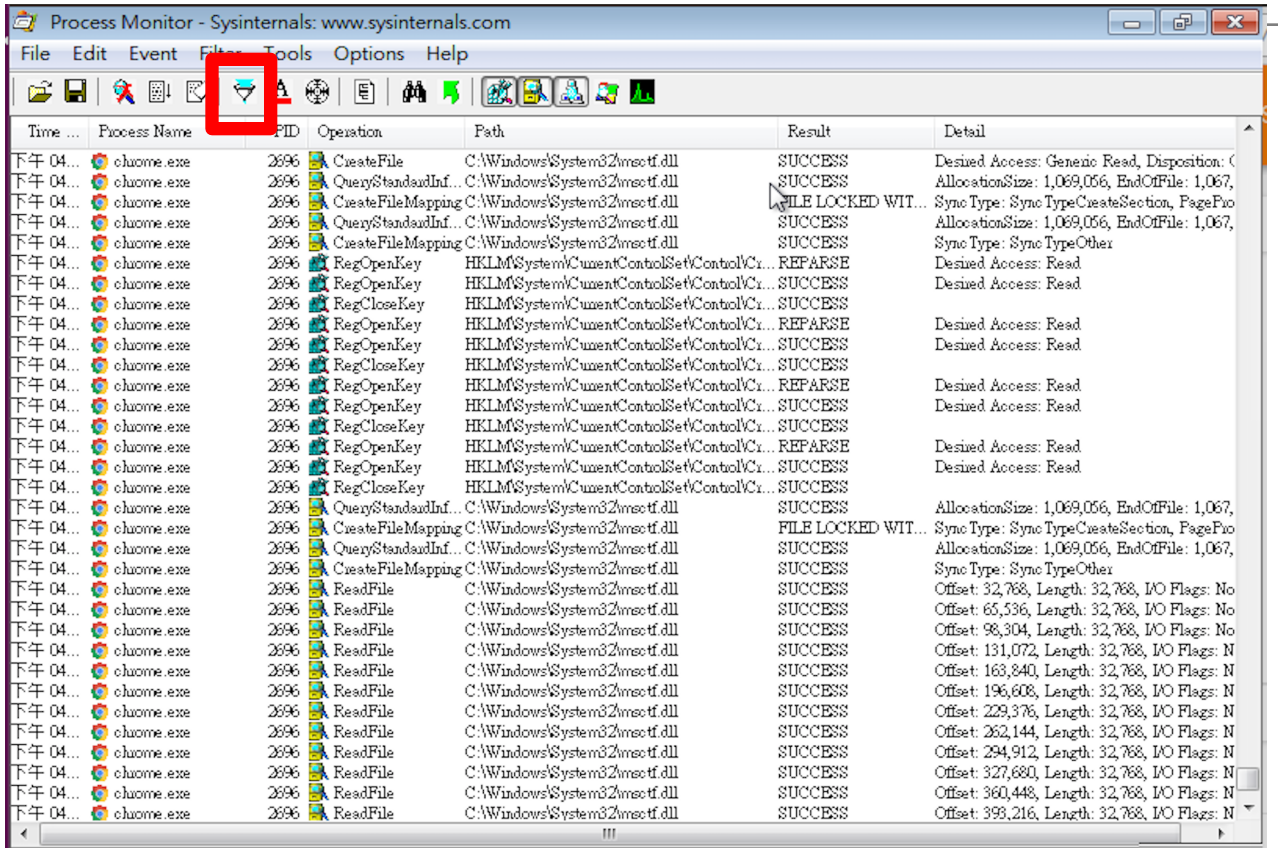
自動下拉: 保持在最下(新)的紀錄

功能介紹



清除記錄: 清除目前的紀錄

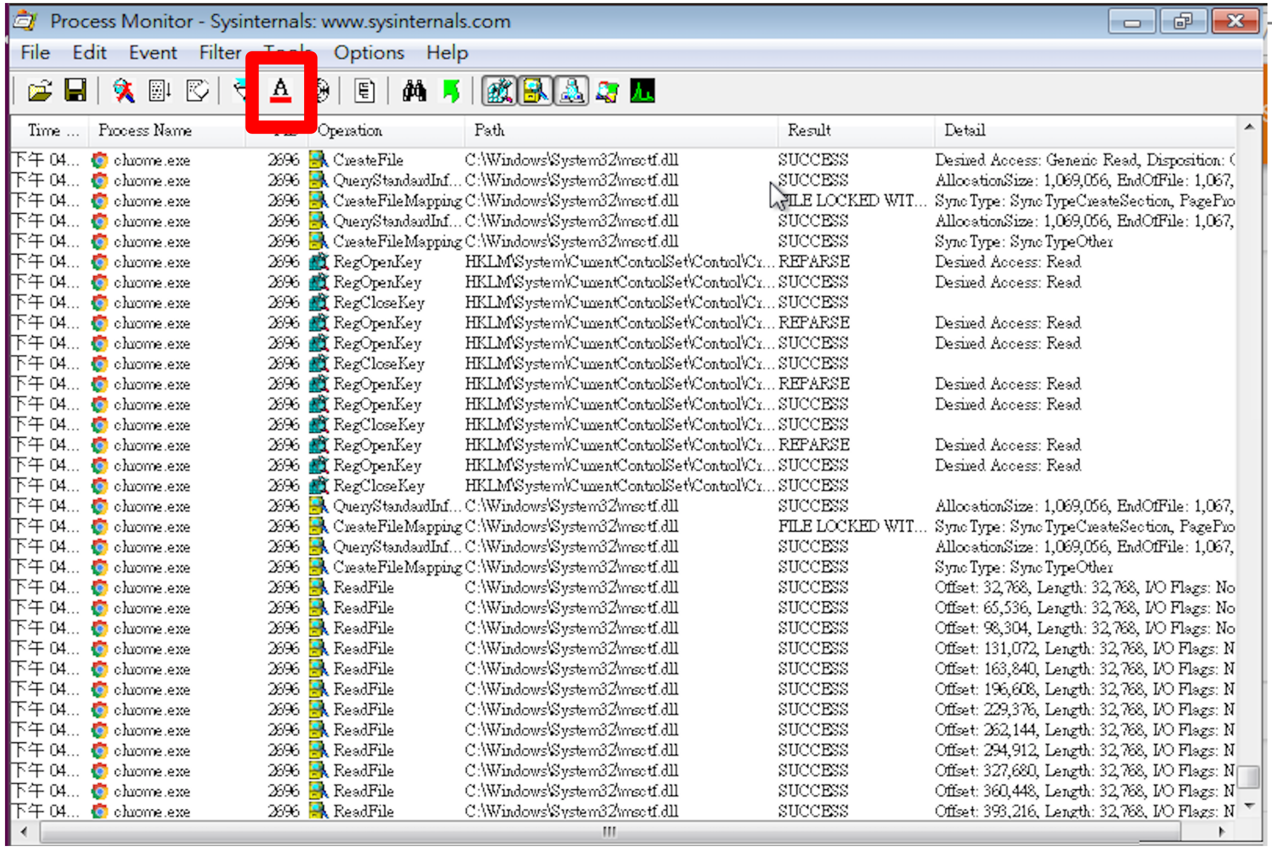
功能介紹



設定過濾: 可用PID, Operation, Process Name…等等來設定過濾紀錄

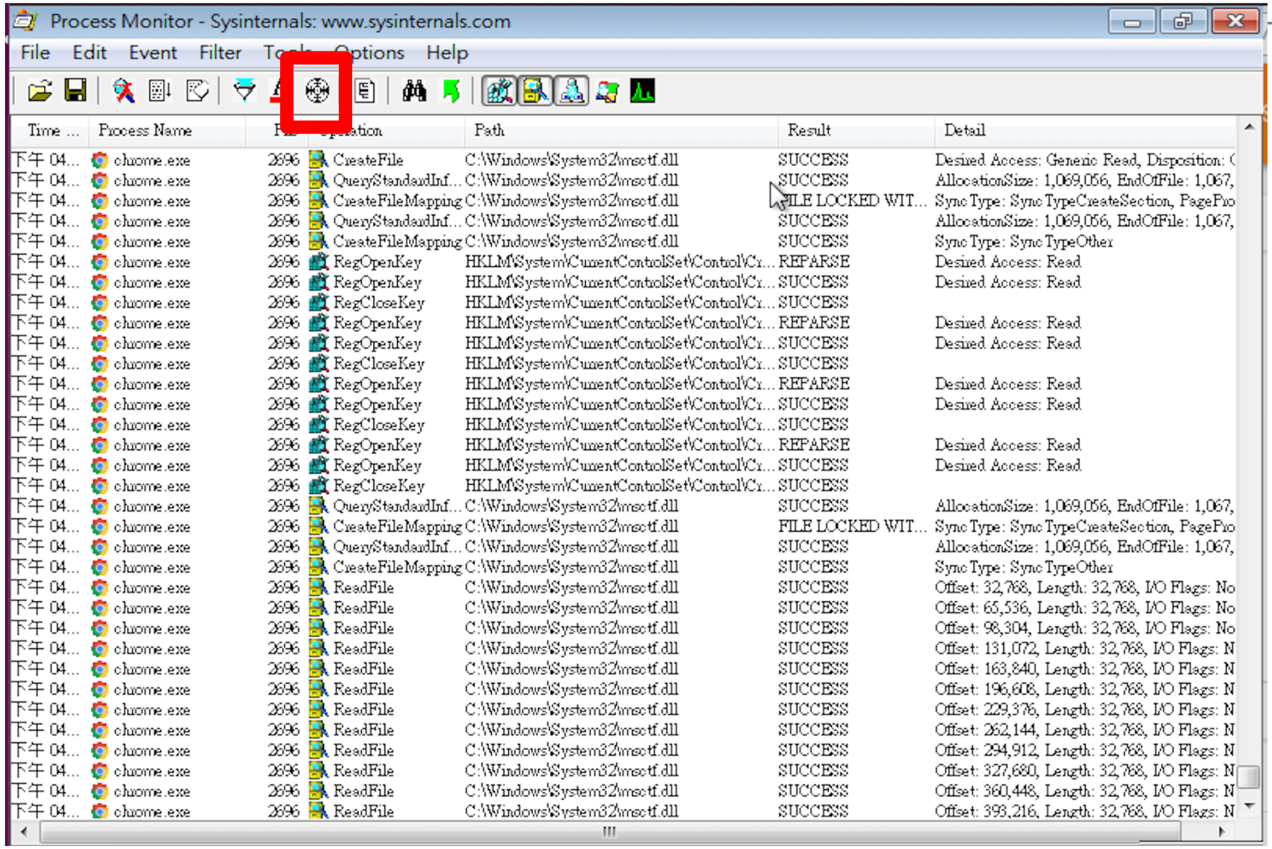
- Operation is “TCP Connect”
- Operation is “RegSetValue”
- Operation is “WriteFile”
- “Category” is “Write”

功能介紹



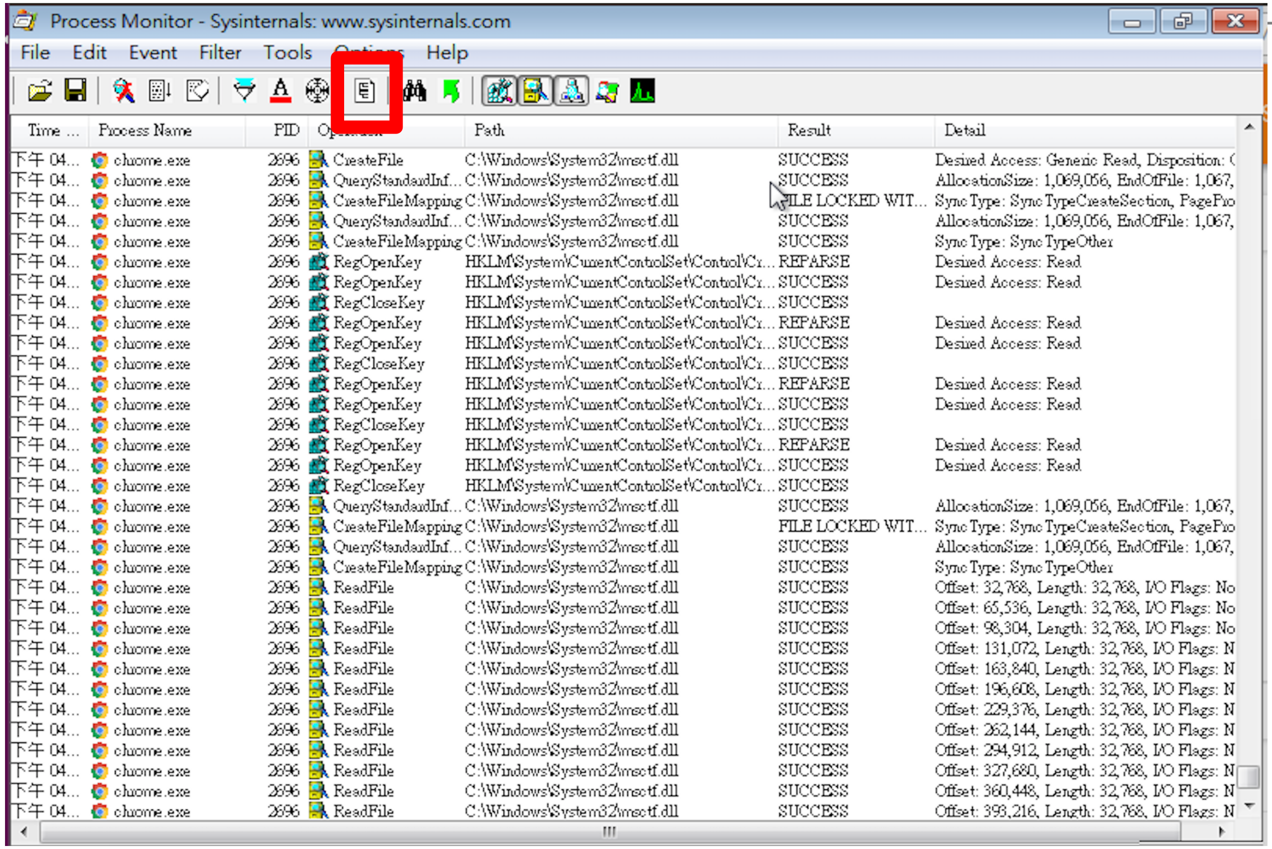
突出標示: 標示出所設定的紀錄

功能介紹



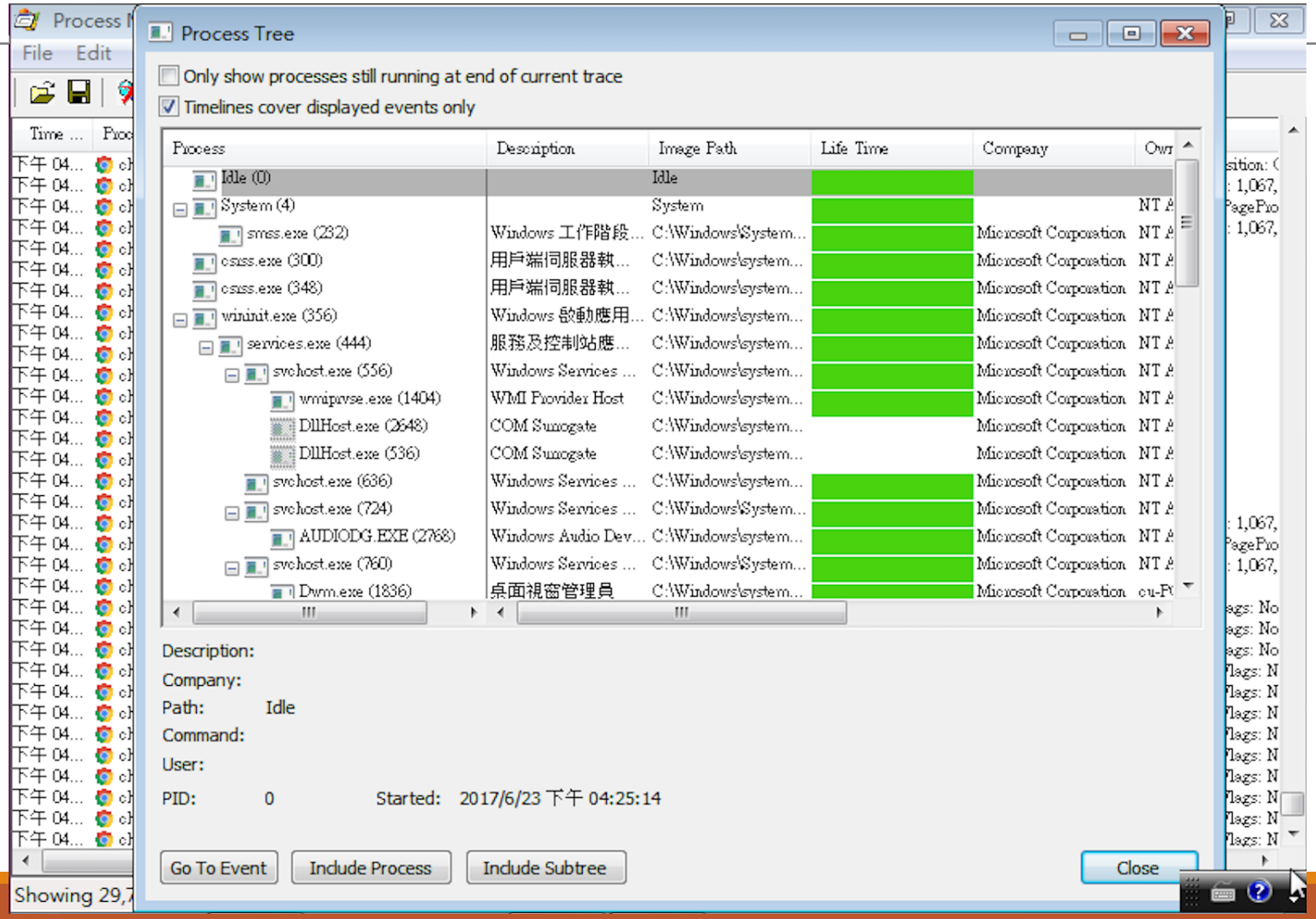
指定程式: 直接拖曳到指定的程式，Procmon會過濾此程式的紀錄

功能介紹

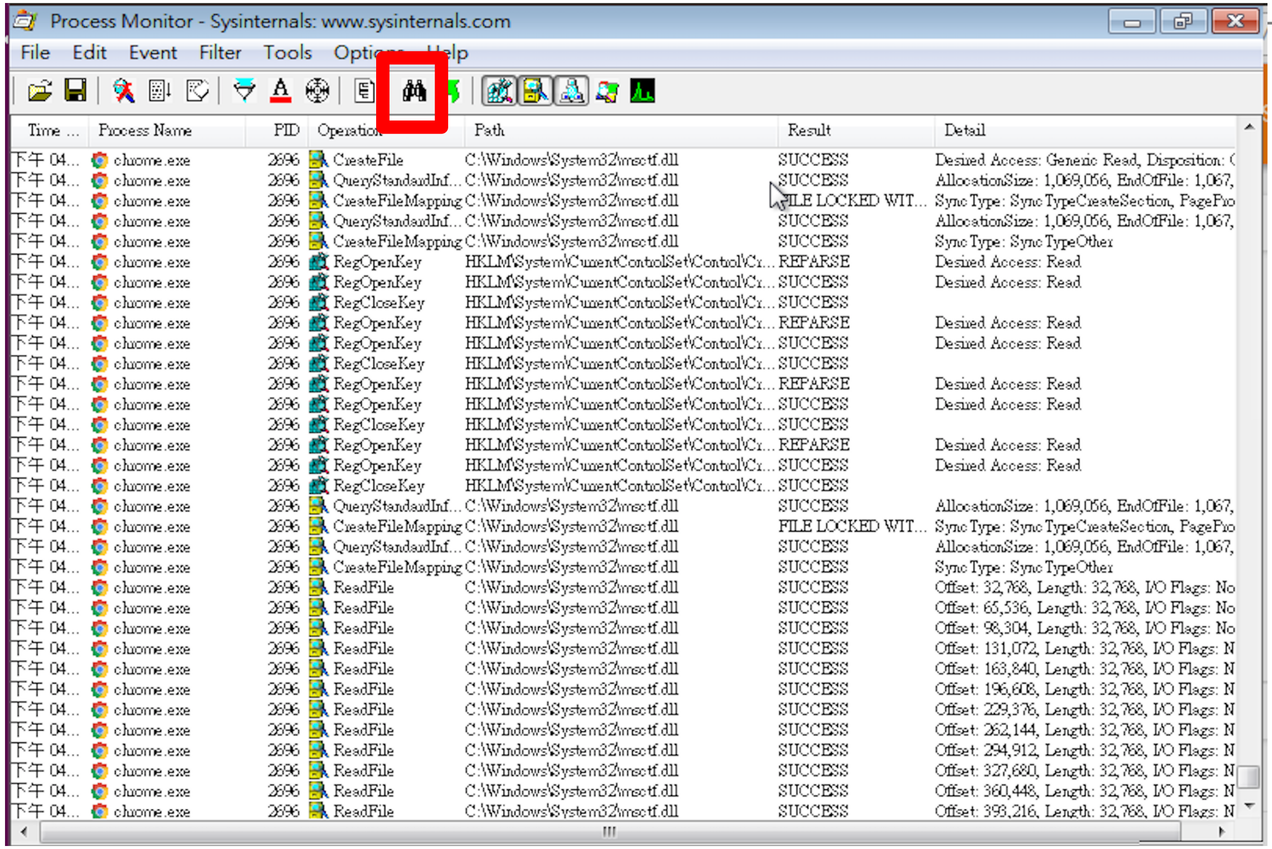


Process樹: 畫出Process樹

功能介紹

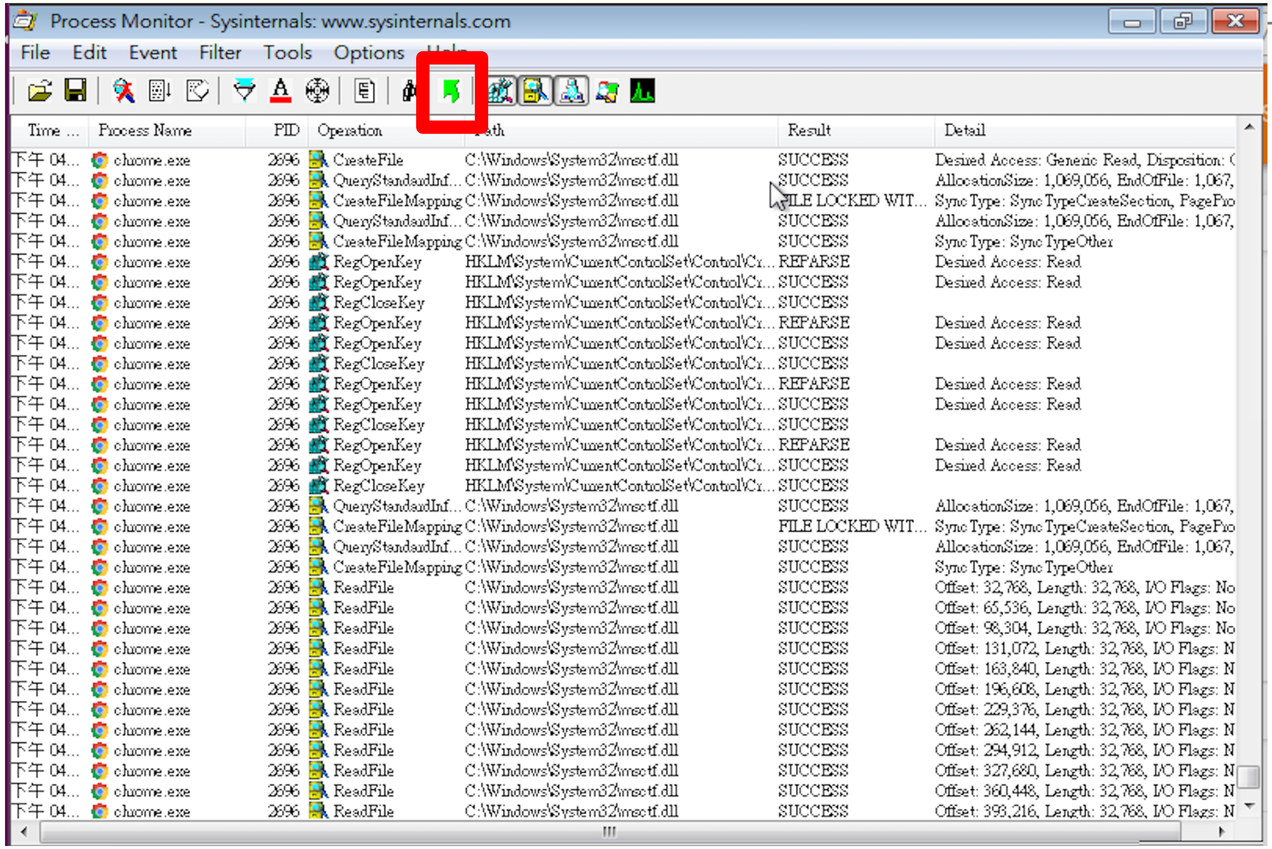

Process Tree
Only show processes still running at end of current trace
Timelines cover displayed events only
Process
Description
Image Path
Life Time
Company
Idle (0)
System (4)
smss.exe (232)
csrss.exe (300)
csrss.exe (348)
wininit.exe (356)
services.exe (444)
svchost.exe (556)
wmiprvse.exe (1404)
DllHost.exe (2648)
DllHost.exe (536)
svchost.exe (636)
svchost.exe (724)
AUDIODG.EXE (2768)
svchost.exe (760)
Dwm.exe (1836)
Description:
Company:
Path: Idle
Command:
User:
PID: 0
Started: 2017/6/23 下午 04:25:14
Go To Event
Include Process
Include Subtree
Close

功能介紹



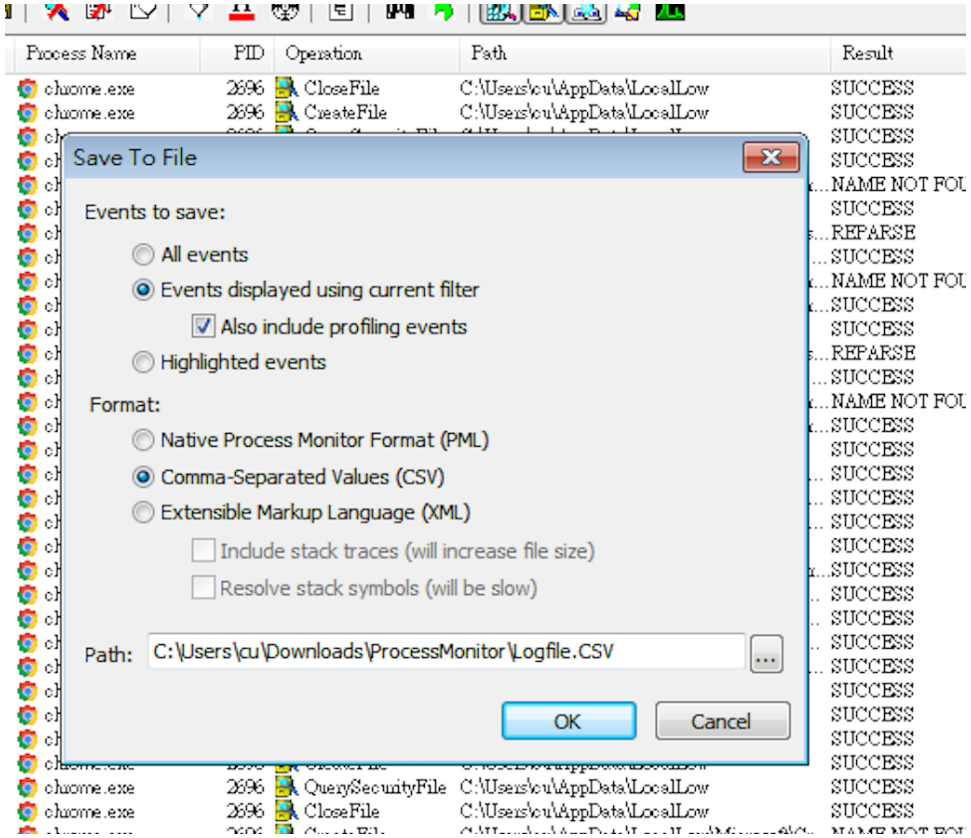
搜尋: 搜尋指定文字

功能介紹



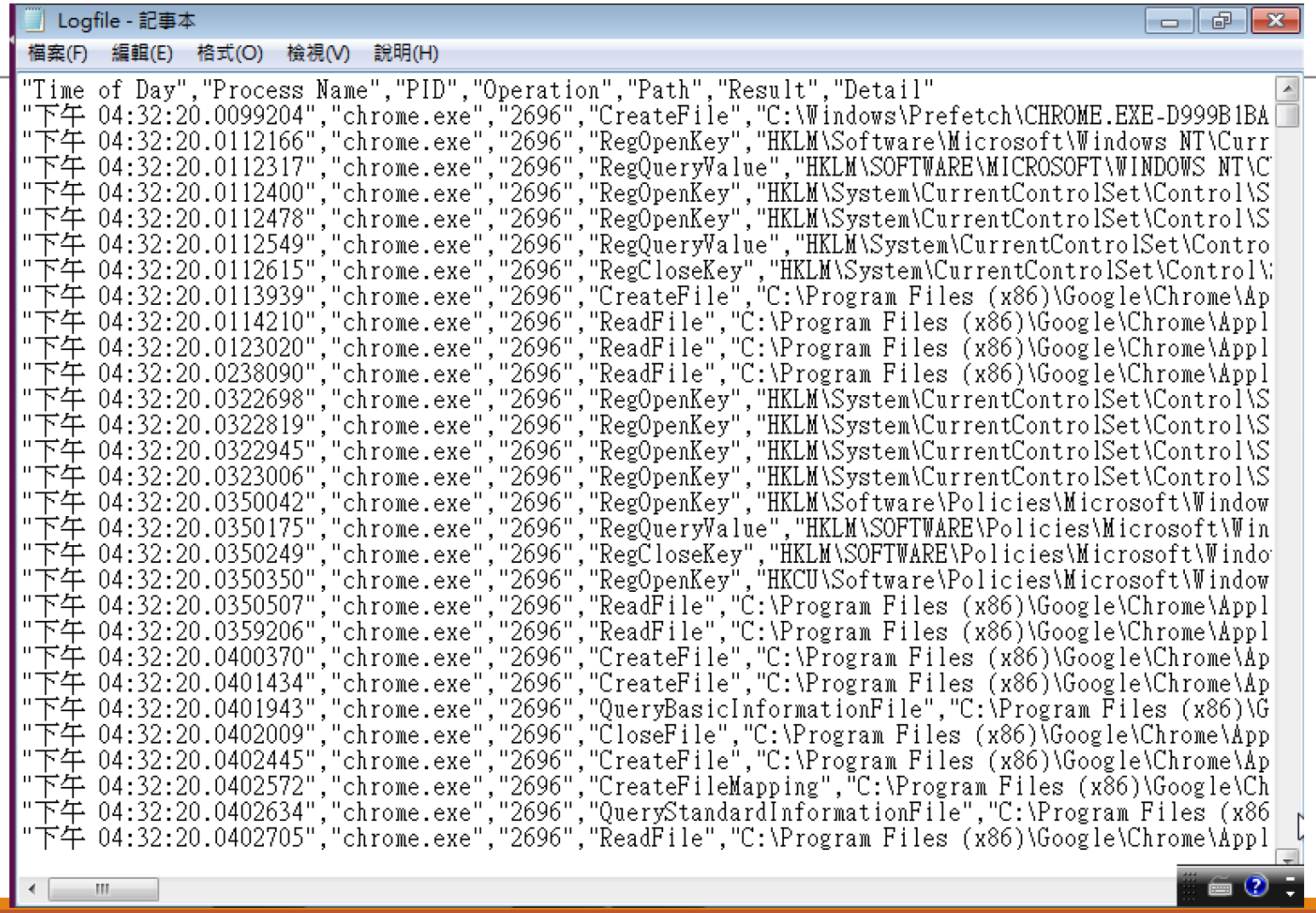
跳至File/ Registry: 跳至File檔案位置/登陸編輯程式該Registry Key

檔案儲存



可以將所有或部分的紀錄儲存, 可以儲存為不同的格式(PML, CSV, XML)

儲存結果


Logfile - 記事本
檔案(F) 編輯(E) 格式(O) 檢視(V) 說明(H)
"Time of Day","Process Name","PID","Operation","Path","Result","Detail"
"下午 04:32:20.0099204","chrome.exe","2696","CreateFile","C:\Windows\Prefetch\CHROME.EXE-D999B1BA
"下午 04:32:20.0112166","chrome.exe","2696","RegOpenKey","HKLM\Software\Microsoft\Windows NT\Curr
"下午 04:32:20.0112317","chrome.exe","2696","RegQueryValue","HKLM\SOFTWARE\MICROSOFT\WINDOWS NT\C
"下午 04:32:20.0112400","chrome.exe","2696","RegOpenKey","HKLM\System\CurrentControlSet\Control\S
"下午 04:32:20.0112478","chrome.exe","2696","RegOpenKey","HKLM\System\CurrentControlSet\Control\S
"下午 04:32:20.0112549","chrome.exe","2696","RegQueryValue","HKLM\System\CurrentControlSet\Contro
"下午 04:32:20.0112615","chrome.exe","2696","RegCloseKey","HKLM\System\CurrentControlSet\Control\
"下午 04:32:20.0113939","chrome.exe","2696","CreateFile","C:\Program Files (x86)\Google\Chrome\Ap
"下午 04:32:20.0114210","chrome.exe","2696","ReadFile","C:\Program Files (x86)\Google\Chrome\Appl
"下午 04:32:20.0123020","chrome.exe","2696","ReadFile","C:\Program Files (x86)\Google\Chrome\Appl
"下午 04:32:20.0238090","chrome.exe","2696","ReadFile","C:\Program Files (x86)\Google\Chrome\Appl
"下午 04:32:20.0322698","chrome.exe","2696","RegOpenKey","HKLM\System\CurrentControlSet\Control\S
"下午 04:32:20.0322819","chrome.exe","2696","RegOpenKey","HKLM\System\CurrentControlSet\Control\S
"下午 04:32:20.0322945","chrome.exe","2696","RegOpenKey","HKLM\System\CurrentControlSet\Control\S
"下午 04:32:20.0323006","chrome.exe","2696","RegOpenKey","HKLM\System\CurrentControlSet\Control\S
"下午 04:32:20.0350042","chrome.exe","2696","RegOpenKey","HKLM\Software\Policies\Microsoft\Window
"下午 04:32:20.0350175","chrome.exe","2696","RegQueryValue","HKLM\SOFTWARE\Policies\Microsoft\Win
"下午 04:32:20.0350249","chrome.exe","2696","RegCloseKey","HKLM\SOFTWARE\Policies\Microsoft\Windo
"下午 04:32:20.0350350","chrome.exe","2696","RegOpenKey","HKCU\Software\Policies\Microsoft\Window
"下午 04:32:20.0350507","chrome.exe","2696","ReadFile","C:\Program Files (x86)\Google\Chrome\Appl
"下午 04:32:20.0359206","chrome.exe","2696","ReadFile","C:\Program Files (x86)\Google\Chrome\Appl
"下午 04:32:20.0400370","chrome.exe","2696","CreateFile","C:\Program Files (x86)\Google\Chrome\Ap
"下午 04:32:20.0401434","chrome.exe","2696","CreateFile","C:\Program Files (x86)\Google\Chrome\Ap
"下午 04:32:20.0401943","chrome.exe","2696","QueryBasicInformationFile","C:\Program Files (x86)\G
"下午 04:32:20.0402009","chrome.exe","2696","CloseFile","C:\Program Files (x86)\Google\Chrome\App
"下午 04:32:20.0402445","chrome.exe","2696","CreateFile","C:\Program Files (x86)\Google\Chrome\Ap
"下午 04:32:20.0402572","chrome.exe","2696","CreateFileMapping","C:\Program Files (x86)\Google\Ch
"下午 04:32:20.0402634","chrome.exe","2696","QueryStandardInformationFile","C:\Program Files (x86
"下午 04:32:20.0402705","chrome.exe","2696","ReadFile","C:\Program Files (x86)\Google\Chrome\Appl

Noriben

Nori-Ben = seaweed lunchbox

Simplest "box" to make

Cheap

Minimal ingredients

Noriben

- Simple Malware Anlysis Sandbox:
  - Wrapper for Microsoft SysInternals Process Monitor(ProcMon)
- Build a Sandbox VM with just:
  - Noriben.py
  - Procmin.exe

Optional:

- Extra Procmon binary filter
- YARA signature files
- Virustotal API Key
- Add new filter to the script

Goal of Noriben

- Quick malware analysis results
- Flexibility for open-ended runs(manually stopped analysis)
- Allow for user interaction
- Analysis of
  - GUI apps
  - Command line args
  - Malware requiring debugging(Z-flag, code/men altering)
  - Long sleeps(hours, days)

Noriben focus on:

- Processes, File activaity, Registry Activity, Network Activity
- Log high level API calls while filtering out known noise
  - Thumbnail creation
  - Prefetch creation
  - Explorer registry key(MRUs)
  - RecentDocs
  - Malware analysis tools (CaptureBat, IDA, FakeNet)
  - VMWare tools
  - Java updater

Strat Noriben

Open "CMD" with administration

Run path/to/python.exe path/to/noriben.py

Compare with cuckoo sandbox

	Cuckoo Sandbox	Noriben
Spend time(sample/sec) time-out 120s	140s	230s
Simulate human activity	Yes(just random move mouse)	No
Memory dump	Plugin(volatility)	No
Static Analysis(Strings, PE header, ...)	Yes	No
Interface	Web and console	Just console
Network Analysis	Use wireshark catch package and analysis	Just analysis windows api
Report	Json and use web present	Just CSV
Portable	Slightly complicated	Very easy to use
Analysis range	Only Malware and process spawned by Malware	Whole systems