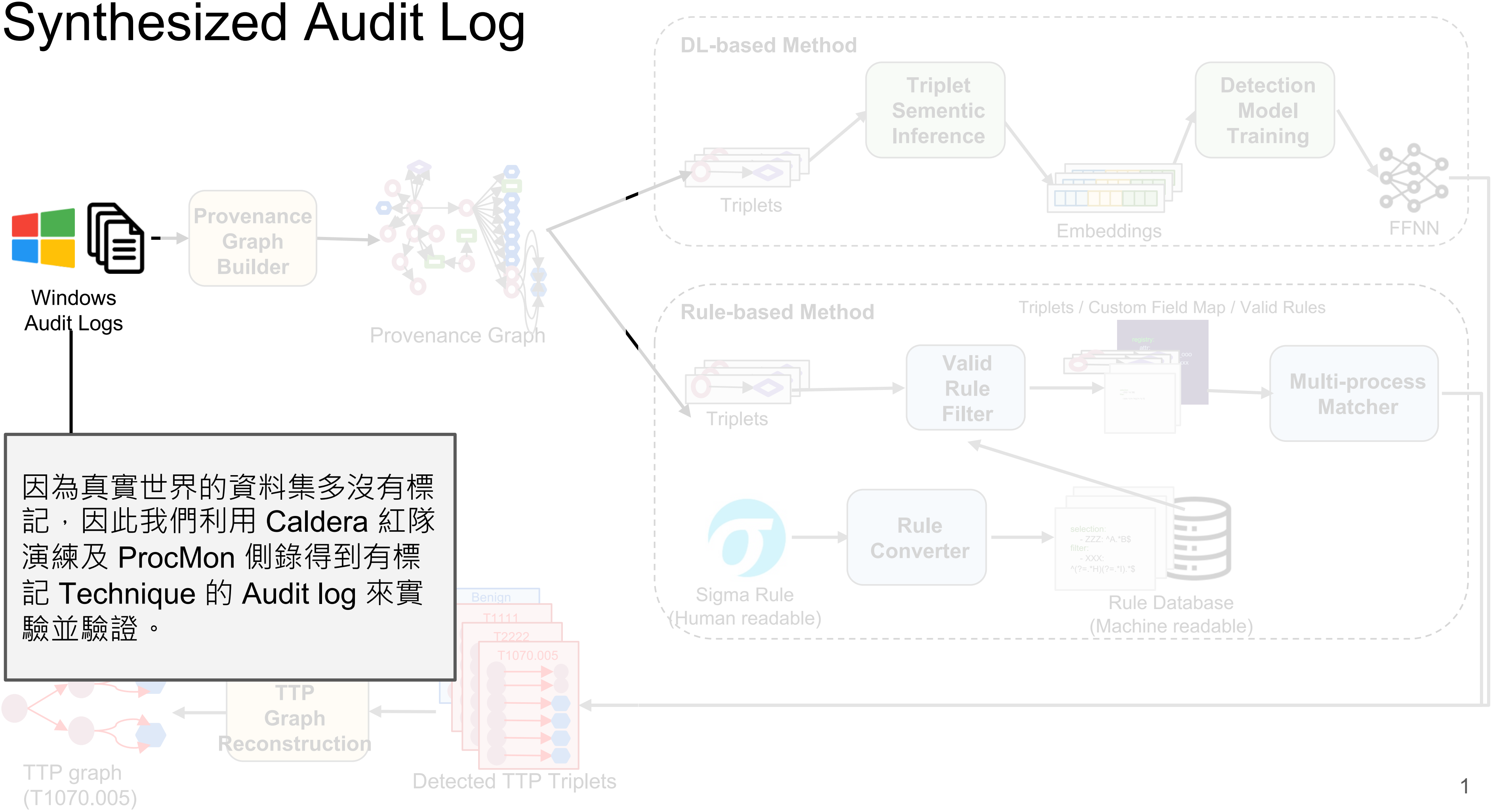
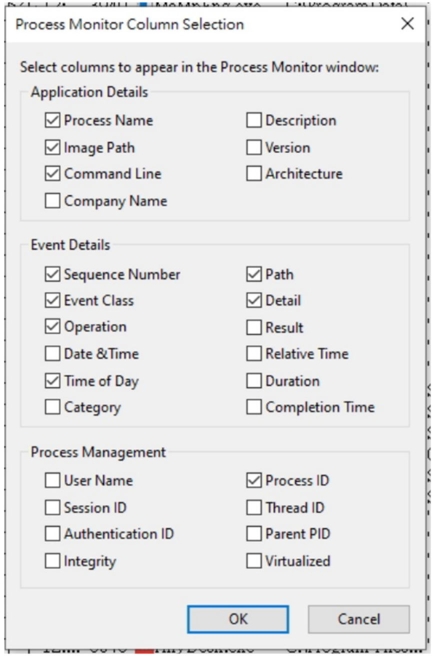
Synthesized Audit Log



因為真實世界的資料集多沒有標記，因此我們利用 Caldera 紅隊演練及 ProcMon 側錄得到有標記 Technique 的 Audit log 來實驗並驗證。

Process Monitor Columns

Process Monitor Columns



Process Monitor Column Selection

Select columns to appear in the Process Monitor window:

Application Details

☑ Process Name
☑ Image Path
☑ Command Line
☐ Company Name
☐ Description
☐ Version
☐ Architecture

Event Details

☑ Sequence Number
☑ Event Class
☑ Operation
☐ Date &Time
☑ Time of Day
☐ Category
☑ Path
☑ Detail
☐ Result
☐ Relative Time
☐ Duration
☐ Completion Time

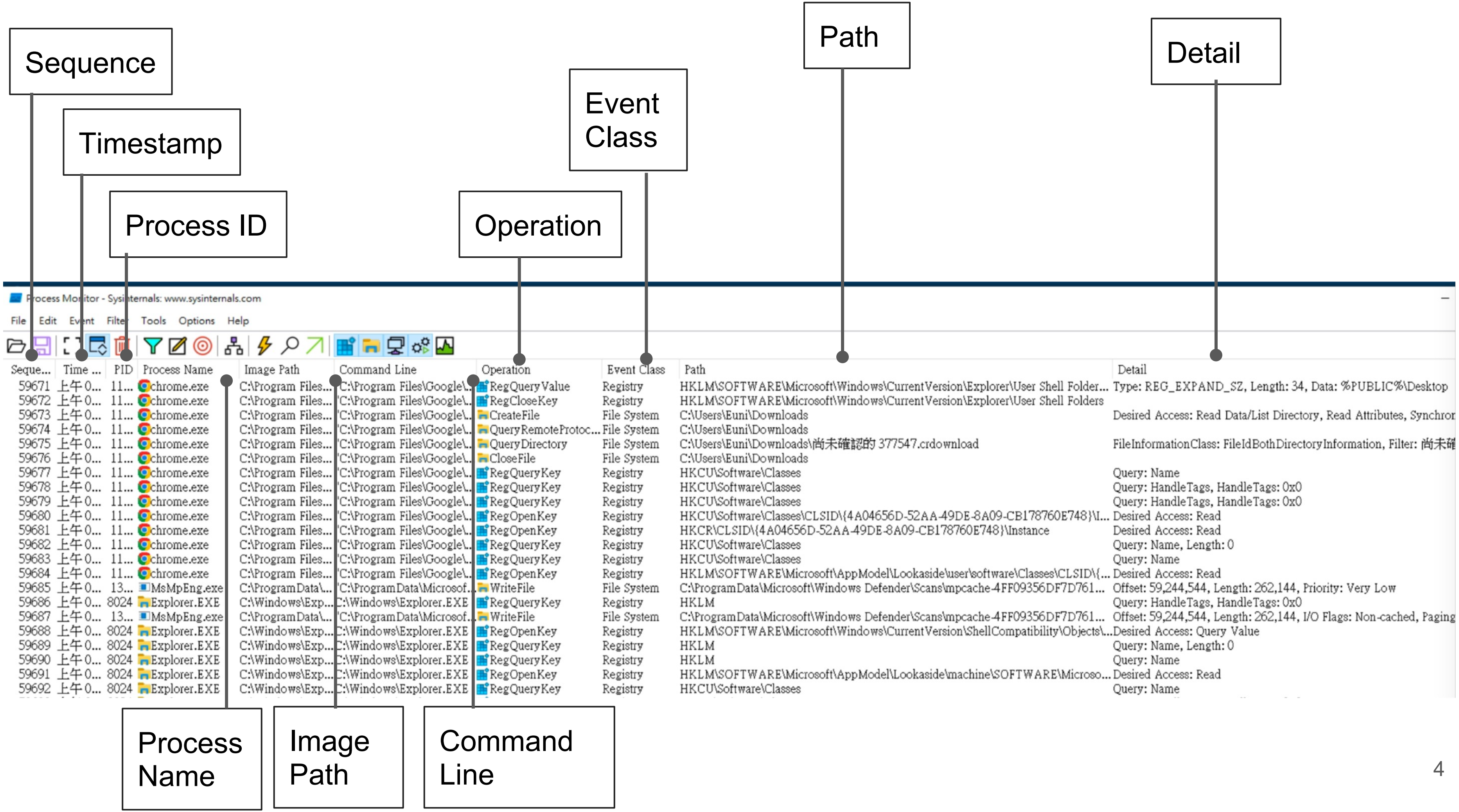
Process Management

☐ User Name
☐ Session ID
☐ Authentication ID
☐ Integrity
☑ Process ID
☐ Thread ID
☐ Parent PID
☐ Virtualized

Fig. Columns in ProcMon

We selected and organized useful log information to JSON format from 10 of 27 columns in ProcMon.

- **Process:** Name The name of the process in which an event occurred.
- **Image Path:** The full path of the image running in a process.
- **Command Line:** The command line used to launch a process.
- **Sequence Number:** The relative position of the operation with respect to all events included in the current filter.
- **Event Class:** The class (File, Registry, Process) of the event.
- **Operation:** The specific event operation
- **Time of Day:** Time of an operation.
- **Process ID:** The Process ID (PID) of the process that executed an operation.
- **Path:** The path of the resource that an event references.
- **Detail:** Additional information specific to an event.



Sequence

Timestamp

Process ID

Operation

Event Class

Path

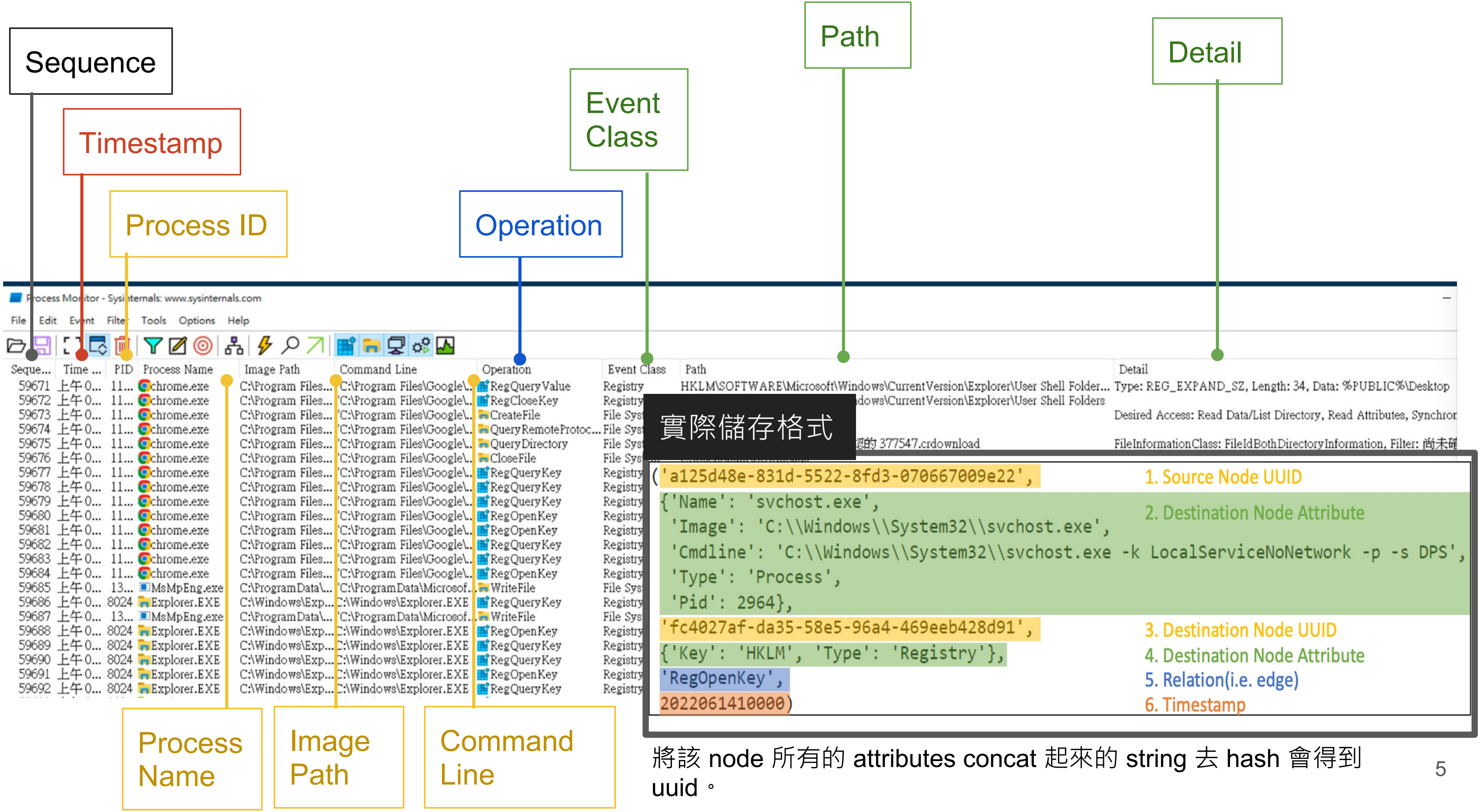
Detail

Process Name

Image Path

Command Line

Seque...	Time ...	PID	Process Name	Image Path	Command Line	Operation	Event Class	Path	Detail
59671	上午 0...	11...	chrome.exe	C:\Program Files...	"C:\Program Files\Google\..	RegQueryValue	Registry	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folder...	Type: REG_EXPAND_SZ, Length: 34, Data: %PUBLIC%\Desktop
59672	上午 0...	11...	chrome.exe	C:\Program Files...	"C:\Program Files\Google\..	RegCloseKey	Registry	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders	
59673	上午 0...	11...	chrome.exe	C:\Program Files...	"C:\Program Files\Google\..	CreateFile	File System	C:\Users\Euni\Downloads	Desired Access: Read Data/List Directory, Read Attributes, Synchron
59674	上午 0...	11...	chrome.exe	C:\Program Files...	"C:\Program Files\Google\..	QueryRemoteProtoc...	File System	C:\Users\Euni\Downloads	
59675	上午 0...	11...	chrome.exe	C:\Program Files...	"C:\Program Files\Google\..	QueryDirectory	File System	C:\Users\Euni\Downloads\尚未確認的 377547.crdownload	FileInformationClass: FileIdBothDirectoryInformation, Filter: 尚未確
59676	上午 0...	11...	chrome.exe	C:\Program Files...	"C:\Program Files\Google\..	CloseFile	File System	C:\Users\Euni\Downloads	
59677	上午 0...	11...	chrome.exe	C:\Program Files...	"C:\Program Files\Google\..	RegQueryKey	Registry	HKCU\Software\Classes	Query: Name
59678	上午 0...	11...	chrome.exe	C:\Program Files...	"C:\Program Files\Google\..	RegQueryKey	Registry	HKCU\Software\Classes	Query: HandleTags, HandleTags: 0x0
59679	上午 0...	11...	chrome.exe	C:\Program Files...	"C:\Program Files\Google\..	RegQueryKey	Registry	HKCU\Software\Classes	Query: HandleTags, HandleTags: 0x0
59680	上午 0...	11...	chrome.exe	C:\Program Files...	"C:\Program Files\Google\..	RegOpenKey	Registry	HKCU\Software\Classes\CLSID\{4A04656D-52AA-49DE-8A09-CB178760E748}\I...	Desired Access: Read
59681	上午 0...	11...	chrome.exe	C:\Program Files...	"C:\Program Files\Google\..	RegOpenKey	Registry	HKCR\CLSID\{4A04656D-52AA-49DE-8A09-CB178760E748}\Instance	Desired Access: Read
59682	上午 0...	11...	chrome.exe	C:\Program Files...	"C:\Program Files\Google\..	RegQueryKey	Registry	HKCU\Software\Classes	Query: Name, Length: 0
59683	上午 0...	11...	chrome.exe	C:\Program Files...	"C:\Program Files\Google\..	RegQueryKey	Registry	HKCU\Software\Classes	Query: Name
59684	上午 0...	11...	chrome.exe	C:\Program Files...	"C:\Program Files\Google\..	RegOpenKey	Registry	HKLM\SOFTWARE\Microsoft\AppModel\Lookaside\user\software\Classes\CLSID\{...	Desired Access: Read
59685	上午 0...	13...	MsMpEng.exe	C:\ProgramData\...	"C:\ProgramData\Microsof..	WriteFile	File System	C:\ProgramData\Microsoft\Windows Defender\Scans\mpcache-4FF09356DF7D761...	Offset: 59,244,544, Length: 262,144, Priority: Very Low
59686	上午 0...	8024	Explorer.EXE	C:\Windows\Exp...	C:\Windows\Explorer.EXE	RegQueryKey	Registry	HKLM	Query: HandleTags, HandleTags: 0x0
59687	上午 0...	13...	MsMpEng.exe	C:\ProgramData\...	"C:\ProgramData\Microsof..	WriteFile	File System	C:\ProgramData\Microsoft\Windows Defender\Scans\mpcache-4FF09356DF7D761...	Offset: 59,244,544, Length: 262,144, I/O Flags: Non-cached, Paging
59688	上午 0...	8024	Explorer.EXE	C:\Windows\Exp...	C:\Windows\Explorer.EXE	RegOpenKey	Registry	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellCompatibility\Objects\...	Desired Access: Query Value
59689	上午 0...	8024	Explorer.EXE	C:\Windows\Exp...	C:\Windows\Explorer.EXE	RegQueryKey	Registry	HKLM	Query: Name, Length: 0
59690	上午 0...	8024	Explorer.EXE	C:\Windows\Exp...	C:\Windows\Explorer.EXE	RegQueryKey	Registry	HKLM	Query: Name
59691	上午 0...	8024	Explorer.EXE	C:\Windows\Exp...	C:\Windows\Explorer.EXE	RegOpenKey	Registry	HKLM\SOFTWARE\Microsoft\AppModel\Lookaside\machine\SOFTWARE\Microso...	Desired Access: Read
59692	上午 0...	8024	Explorer.EXE	C:\Windows\Exp...	C:\Windows\Explorer.EXE	RegQueryKey	Registry	HKCU\Software\Classes	Query: Name



Seque...	Time ...	PID	Process Name	Image Path	Command Line	Operation	Event Class	Path	Detail
59671	上午 0...	11...	chrome.exe	C:\Program Files...	C:\Program Files\Google\...	RegQueryValue	Registry	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folder...	Type: REG_EXPAND_SZ, Length: 34, Data: %PUBLIC%\Desktop
59672	上午 0...	11...	chrome.exe	C:\Program Files...	'C:\Program Files\Google\...	RegCloseKey	Registry	dows\CurrentVersion\Explorer\User Shell Folders	
59673	上午 0...	11...	chrome.exe	C:\Program Files...	'C:\Program Files\Google\...	CreateFile	File Syst		Desired Access: Read Data/List Directory, Read Attributes, Synchron
59674	上午 0...	11...	chrome.exe	C:\Program Files...	'C:\Program Files\Google\...	QueryRemoteProtoc...	File Syst		
59675	上午 0...	11...	chrome.exe	C:\Program Files...	'C:\Program Files\Google\...	QueryDirectory	File Syst	認的 377547.crdownload	FileInformationClass: FileIdBothDirectoryInformation, Filter: 尚未確
59676	上午 0...	11...	chrome.exe	C:\Program Files...	'C:\Program Files\Google\...	CloseFile	File Sys		
59677	上午 0...	11...	chrome.exe	C:\Program Files...	'C:\Program Files\Google\...	RegQueryKey	Registry		
59678	上午 0...	11...	chrome.exe	C:\Program Files...	'C:\Program Files\Google\...	RegQueryKey	Registry		
59679	上午 0...	11...	chrome.exe	C:\Program Files...	'C:\Program Files\Google\...	RegQueryKey	Registry		
59680	上午 0...	11...	chrome.exe	C:\Program Files...	'C:\Program Files\Google\...	RegOpenKey	Registry		
59681	上午 0...	11...	chrome.exe	C:\Program Files...	'C:\Program Files\Google\...	RegOpenKey	Registry		
59682	上午 0...	11...	chrome.exe	C:\Program Files...	'C:\Program Files\Google\...	RegQueryKey	Registry		
59683	上午 0...	11...	chrome.exe	C:\Program Files...	'C:\Program Files\Google\...	RegQueryKey	Registry		
59684	上午 0...	11...	chrome.exe	C:\Program Files...	'C:\Program Files\Google\...	RegOpenKey	Registry		
59685	上午 0...	13...	MsMpEng.exe	C:\ProgramData\...	'C:\ProgramData\Microsof...	WriteFile	File Sys		
59686	上午 0...	8024	Explorer.EXE	C:\Windows\Exp...	C:\Windows\Explorer.EXE	RegQueryKey	Registry		
59687	上午 0...	13...	MsMpEng.exe	C:\ProgramData\...	'C:\ProgramData\Microsof...	WriteFile	File Sys		
59688	上午 0...	8024	Explorer.EXE	C:\Windows\Exp...	C:\Windows\Explorer.EXE	RegOpenKey	Registry		
59689	上午 0...	8024	Explorer.EXE	C:\Windows\Exp...	C:\Windows\Explorer.EXE	RegQueryKey	Registry		
59690	上午 0...	8024	Explorer.EXE	C:\Windows\Exp...	C:\Windows\Explorer.EXE	RegQueryKey	Registry		
59691	上午 0...	8024	Explorer.EXE	C:\Windows\Exp...	C:\Windows\Explorer.EXE	RegOpenKey	Registry		
59692	上午 0...	8024	Explorer.EXE	C:\Windows\Exp...	C:\Windows\Explorer.EXE	RegQueryKey	Registry		

```
('a125d48e-831d-5522-8fd3-070667009e22',
 {'Name': 'svchost.exe',
  'Image': 'C:\\Windows\\System32\\svchost.exe',
  'Cmdline': 'C:\\Windows\\System32\\svchost.exe -k LocalServiceNoNetwork -p -s DPS',
  'Type': 'Process',
  'Pid': 2964},
 'fc4027af-da35-58e5-96a4-469eeb428d91',
 {'Key': 'HKLM', 'Type': 'Registry'},
 'RegOpenKey',
 2022061410000)
```

將該 node 所有的 attributes concat 起來的 string 去 hash 會得到 uuid。

Synthesized 資料集描述

Synthesized 資料集中總事件數量：17,346,525

其中是 TTP 的事件數量：18,334

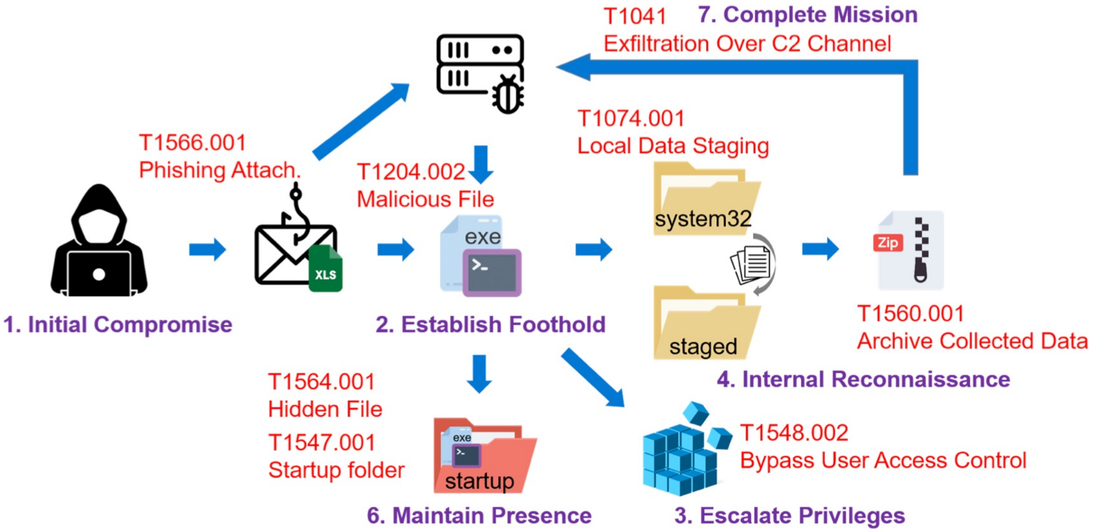
TTP 的數量是？

各個 TTP 對應的事件數量

其中是 Benign 的事件數量：17,328,191

Entity / Relation 數量

Synthesized attack campaign - case study



T1041
7. Complete Mission
Exfiltration Over C2 Channel
T1074.001
Local Data Staging
T1566.001
Phishing Attach.
T1204.002
Malicious File
system32
exe
XLS
Zip
staged
1. Initial Compromise
2. Establish Foothold
T1560.001
Archive Collected Data
4. Internal Reconnaissance
T1564.001
Hidden File
T1547.001
Startup folder
exe
startup
T1548.002
Bypass User Access Control
6. Maintain Presence
3. Escalate Privileges