~~KAPE 스크립트 작성~~ KAPE 스크립트 보고서~~하기~~ 보고서

KAPE target 스크립트 작성하기! BOB 포렌식 트랙_ 정현덕

- **SETUP API 스크립트 작성**

Setup API(Setup Application Programming Interface)는 두 가지 기능을 제공하는 시스템 구성요소.

- 일반적인 설정 기능
- 장치 설치 기능

장치 설치 소프트웨어는 이러한 기능을 사용하여 클래스 설치 관리자, 공동 설치 관리자 및 장치 설치 응용 프로그램에서 사용자 지정 작업을 수행할 수 있다.

KAPE에서는 기본적으로 SETUP API를 수집하지 않기 때문에 TARGET의 여러 스크립트를 참고하여 수집할 수 있도록 스크립트를 작성한다.

```
Description: Setupapi
Author: Troy Larson
Version: 2.0
Id: 701573f6-0ce1-454d-af41-612713e22af5
RecreateDirectories: true
Targets:
    -
        Name: Setupapi
        Category: Logs
        Path: C:\Windows\INF\
        FileMask: '*.log'


# Documentation
# https://www.sumologic.com/blog/iis-log-files-location/
```

[setupapi.tkape 파일]

서식 지정함: 글꼴: 17 pt

서식 지정함: 글꼴: 17 pt

서식 지정함: 글꼴: 10 pt

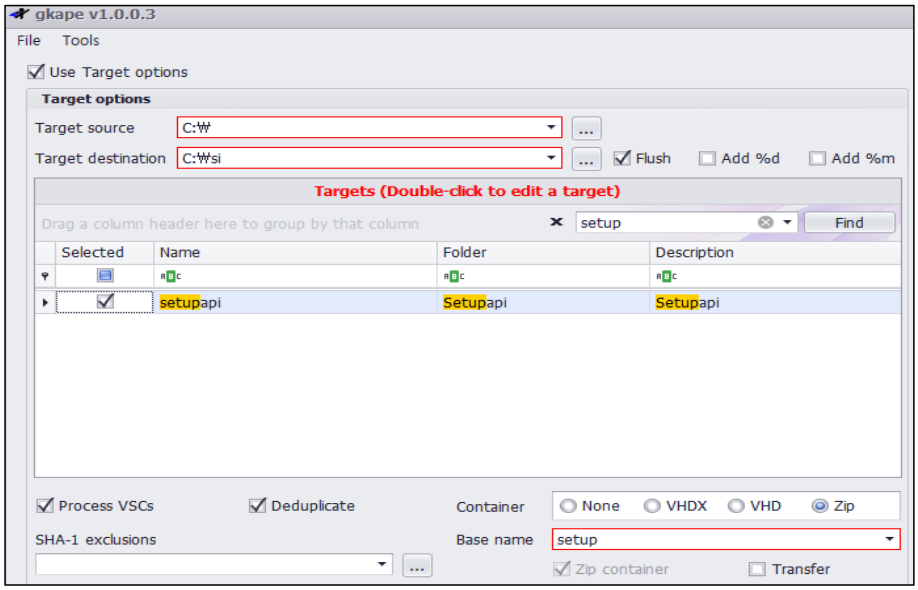
서식 있음: 강한 인용, 테두리: 아래쪽: (테두리 없음)

서식 지정함: 글꼴: 굵게

서식 있음: 목록 단락, 글머리 기호 + 수준:1 + 맞춤 위치: 0.71 cm + 들여쓰기 위치: 1.34 cm

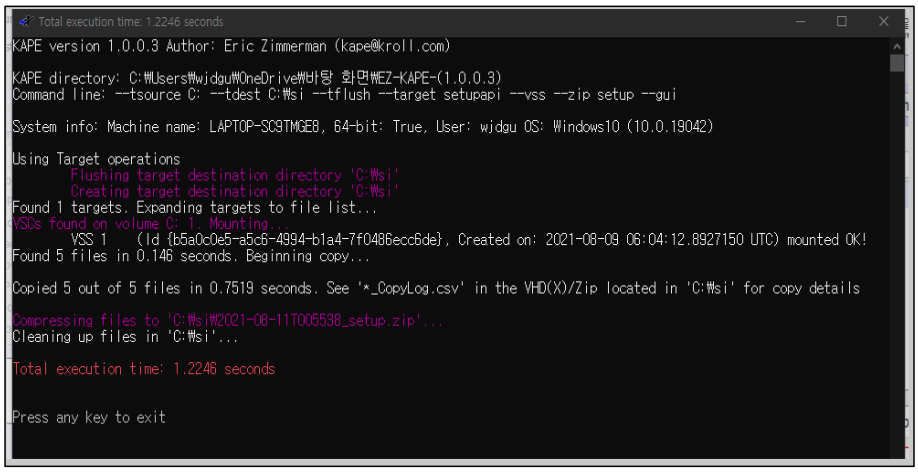
서식 지정함: 글꼴: 10 pt

서식 지정함: 글꼴: 10 pt



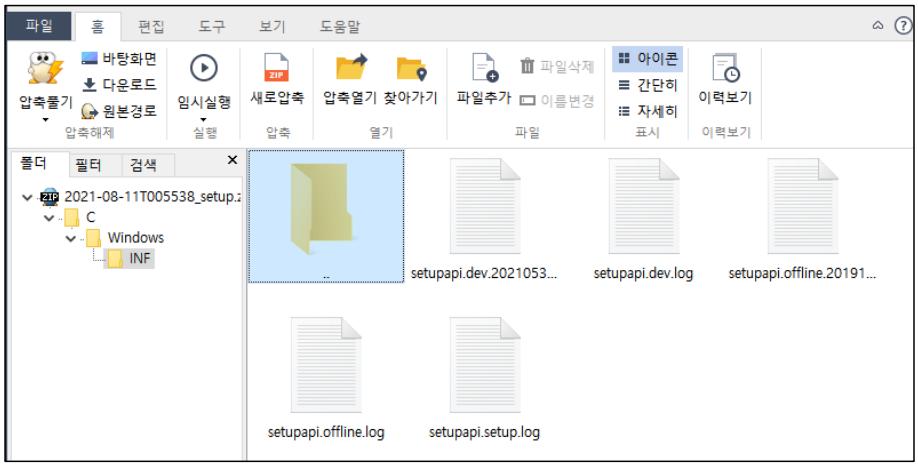
[KAPE에서 작성한 스크립트가 적용된 모습]

Setupapi 스크립트를 이용해서 정보를 들고 와서 zip파일로 저장할 수 있도록 설정 후 Excute버튼을 눌러준다.



[스크립트 정상 실행]

수집이 완료되었다면 지정한 경로로 이동하여 파일이 잘 저장되었는지 확인한다.



[정상적으로 파일을 불러온 것을 확인 가능]

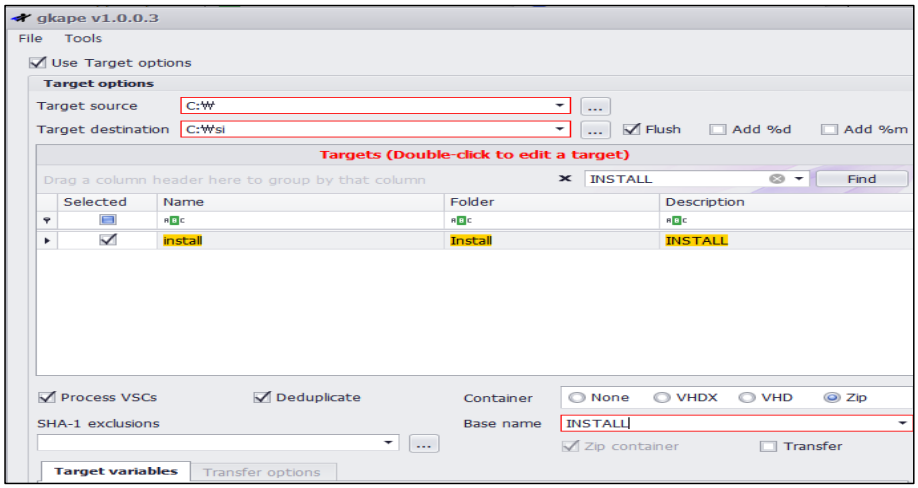
- **Install 스크립트 작성**

C:₩Windows₩appcompat₩Programs₩Install₩ 안에 있는 프로그램 설치 로그를 들고 올 수 있도록 스크립트를 작성 후 실행한다.

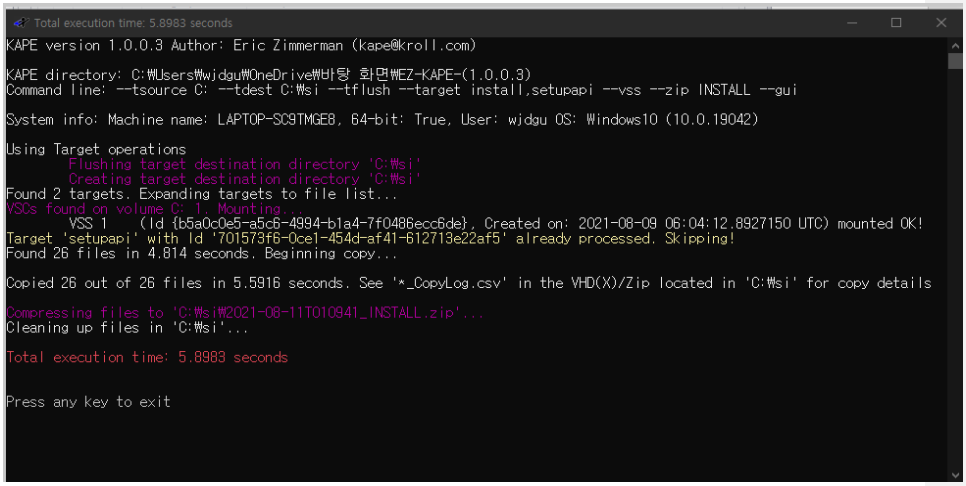
```
Description: INSTALL
Author: Troy Larson
Version: 2.0
Id: 701573f6-0ce1-454d-af41-612713e22af5
RecreateDirectories: true
Targets:
    -
        Name: INSTALL
        Category: Logs
        Path: C:\Windows\appcompat\Programs\Install\
        FileMask: 'Install_*.txt'


# Documentation
# https://www.sumologic.com/blog/iis-log-files-location/
```

[작성된 Install 스크립트]

INSTALL_로 시작하는 TXT파일을 가져 올 수 있도록 스크립트를 작성한 후 앞과 동일한 방법으로 EXCUTE를 실행한다.

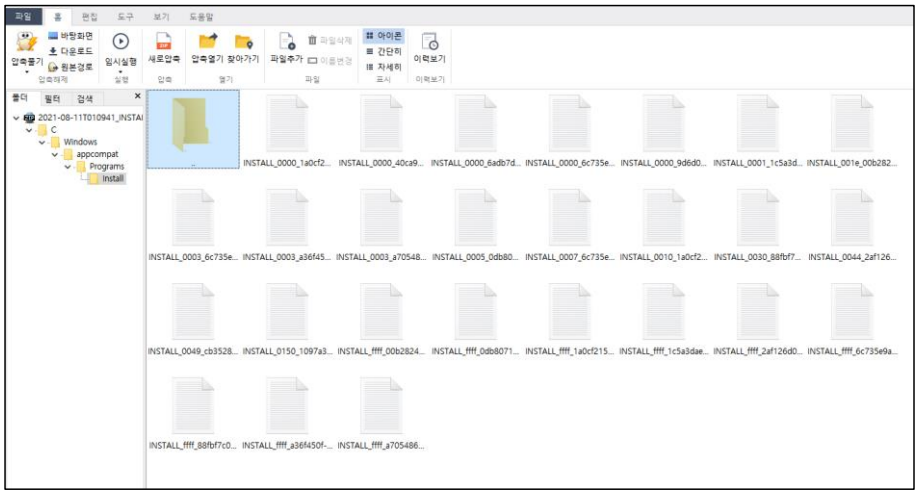


[저장된 스크립트가 검색 됨]



[정상 실행]

앞서 Setup api 를 실행 한 것 과 동일한 방식으로 진행이 되었고 , excute 후 지정한 경로에 들어가 파일이 잘 저장 되었는지를 확인 한다.



[정상적으로 파일이 저장되었다.]

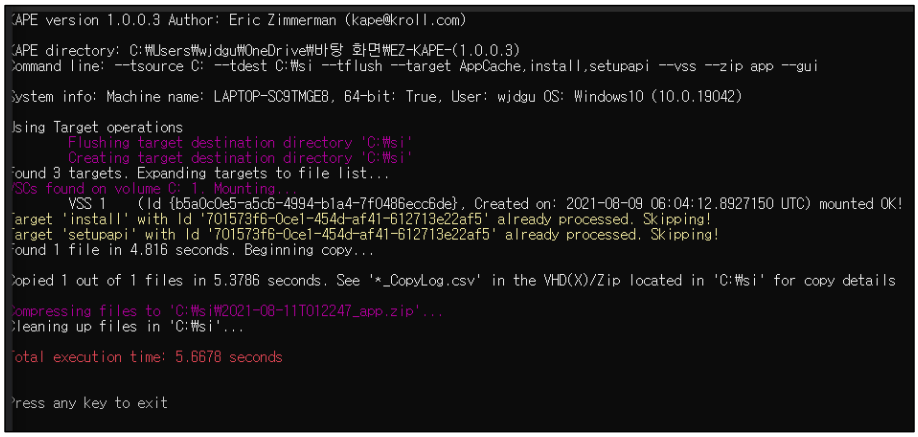
- **Cortana MRU (앱 실행 이력)**

C:₩Users₩wjdgu₩AppData₩Local₩Packages₩Microsoft.Windows.Search_cw5n1h2txyewy₩LocalState₩DeviceSearchCache₩ 안에 있는 앱 실행 이력을 들고 오는 스크립트를 위와 동일한 형태로 작성한 후 실행.

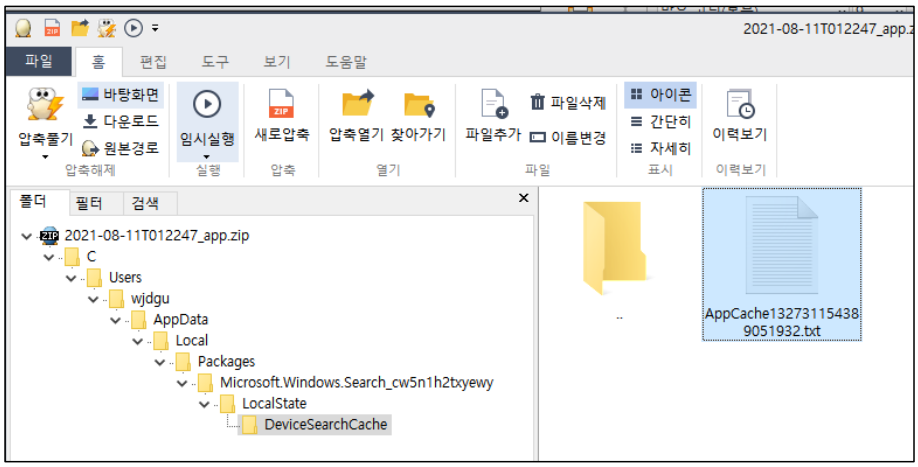
```
Description: AppCache
Author: Troy Larson
Version: 2.0
Id: 701573f6-0ce1-454d-af41-612713e22af5
RecreateDirectories: true
Targets:
    -
        Name: AppCache
        Category: Logs
        Path: C:\Users\wjdgu\AppData\Local\Packages\Microsoft.Windows.Search_cw5n1h2txyewy\LocalState\DeviceSearchCache\
        FileMask: 'AppCache*.txt'


# Documentation
# https://www.sumologic.com/blog/iis-log-files-location/
```

[작성된 수집 스크립트]

앞과 동일한 방식으로 excute 후 결과를 확인.



[스크립트 실행]



[정상 실행]

스크립트가 정상 실행되었고 앱 실행 이력을 들고 오는 것을 확인할 수 있다.

수집한 아티팩트들에 대한 의미

- Setupapi
- 장치 드라이버, 서비스 팩 등이 설치될 때 남기는 텍스트 로그
- 저장장치 최초 연결 시 장치 드라이버 설치 흔적이 남는다 ➔ 최초 연결시간 확인 가능

수집된 setupapi.dev.log 를 확인해 보면 저장 장치 설치 흔적을 확인할 수 있다.

```
>>>  [Device Install (Hardware initiated) -INTELAUDIOWSGPC_FUNC_01&VEN_8086&DEV_2812&SUBSYS_80860101&REV_1000₩5&10ce174c&0&0201]
>>>  Section start 2021/06/24 13:29:11.611
    utl: {Select Drivers - INTELAUDIOWSGPC_FUNC_01&VEN_8086&DEV_2812&SUBSYS_80860101&REV_1000₩5&10ce174c&0&0201} 13:29:11.631
      utl:        Driver Node:
      utl:              Status          - Selected
      utl:              Driver INF      - oem11.inf
                                                                .
                                                                .
                                                                .

dvi:                    Start: INTELAUDIOWSGPC_FUNC_01&VEN_8086&DEV_2812&SUBSYS_80860101&REV_1000₩5&10CE174C&0&0201
      dvi:              {Restarting Devices exit} 13:29:12.495
      dvi:        {Configure Device - exit(0x00000000)} 13:29:12.496
      dvi: {Core Device Install - exit(0x00000000)} 13:29:12.496
<<<  Section end 2021/06/24 13:29:12.501
<<<  [Exit status: SUCCESS]
```

위와 같이 여러가지 정보를 확인해 볼 수 있다. 이러한 정보를 통해서 기밀 정보 유출, 내부문건 유출 등의 사고가 발생하였을 경우 이동저장매체의 연결흔적과 다른 외부 매체의 사용여부를 확인 가능 하다.

- INSTALL
- 여러 프로그램 설치에 대한 로그

```
StartTime=07/23/2021 06:00:53
Name=ALZip1130.exe
Path=C:₩Users₩wjdgu₩Downloads
Size=0x1295888
Magic=0x10b
SizeOfImage=0x1e9000
PeChecksum=0x129f859
LinkDate=12/01/2010 05:20:35
LinkerVersion=6.0
BinFileVersion=21.6.23.1
BinProductVersion=21.6.23.1
BinaryType=PE32_I386
Created=07/23/2021 05:51:40
Modified=07/23/2021 05:52:05
LastAccessed=07/23/2021 06:00:51
VerLanguage=0
Id=000009f6ab78586ba020a6941f0e5c4088f23fecf363
```

FileVersion=21.6.23.1
CompanyName=ESTsoft Corp.
FileDescription=알집 v11.30 공개용 설치 프로그램
LegalCopyright=Copyright (C) 2021 ESTsoft Corp. All rights reserved.
ProductName=ALZip Setup
ProductVersion=11.30.0.1
PeImageType=0x14c
PeSubsystem=2
CrcChecksum=0xc099cc37
FileSize=0x0000000001295888
LongName=ALZip1130.exe
OneProcess=1
MsiDetected=0.

.

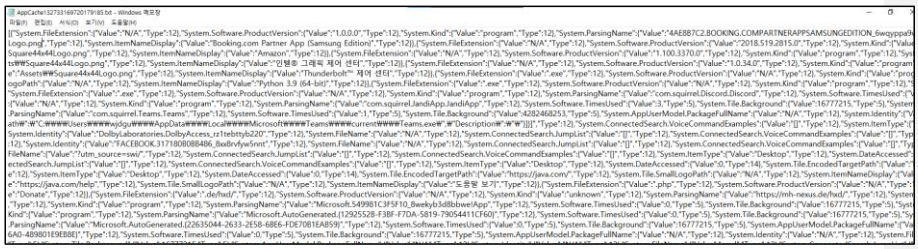
FileCreate=C:₩Program Files (x86)₩ESTsoft₩ALUpdate₩ALUpProduct.exe
FileCreate=C:₩Program Files (x86)₩ESTsoft₩ALUpdate₩ALUpExt.exe
FileCreate=C:₩Program Files (x86)₩ESTsoft₩ALUpdate₩ALUpdateEx.dll
FileCreate=C:₩Program Files (x86)₩ESTsoft₩ALUpdate₩ALAd.dll
FileCreate=C:₩Program Files (x86)₩ESTsoft₩ALUpdate₩unins000.exe
FileCreate=C:₩Users₩wjdgu₩AppData₩Local₩Microsoft₩Windows₩INetCache₩IE₩O1N8X1QB₩ALSee914[1].exe
FileCreate=C:₩Program Files (x86)₩ESTsoft₩Common₩ALSTSCollector.exe
ArpCreate=SOFTWARE₩WOW6432Node₩Microsoft₩Windows₩CurrentVersion₩Uninstall₩ALZip_is1
ArpCreate=SOFTWARE₩WOW6432Node₩Microsoft₩Windows₩CurrentVersion₩Uninstall₩ALUpdate_is1
StopTime=07/23/2021 06:01:44

위처럼 install 파일에서 알집을 설치한 정보에 대해서 확인할 수 있었다.

알 수 있는 정보는 시작 시간, 설치 경로, 사이즈, 매직 넘버, 함께 생성된 파일의 목록, 버전정보 외에도 다양한 정보를 확인할 수 있다. 이를 이용해서 어떤 파일이 언제 설치가 되었으며 생성시간, 수정시간 등의 다양한 정보를 확인할 수 있다.

App cache

- 앱 캐시들이 들어있는 로그



앱 캐시 로그의 경우 수많은 데이터 들이 들어있긴 하지만, 가독성이 떨어지는 형태로 저장되었다.