IOAF를 이용한 안티 포렌식 도구 탐지

wormhole

wormhole1313@gmail.com

1. **IOAF**
    - IOAF 란?
    - IOAF를 이용한 안티 포렌식 도구 탐지
    - IOC와 IOAF
2. **안티 포렌식 탐지 지표 생성**
3. **안티 포렌식 도구 탐지**
4. **활용 방안 고찰에 대한 질문**

IOAF란?

- IOAF의 줄인 말
  - Indicators of Anti Forenscics으로 안티포렌식 탐지 지표
- IOC를 안티 포렌식에 접목
  - Indicators Of Compromise로 침해사고 탐지 지표 의미
  - 안티 포렌식의 지표를 이용하여 안티 포렌식을 탐지

IOAF를 이용한 안티 포렌식 도구 탐지

- 각 안티 포렌식 도구에 대한 지표를 생성하여 도구를 탐지
  - 안티 포렌식 도구가 설치, 단순 실행, 기능 실행 되었을 때 나오는 고유한 흔적을 지표로 수립
- 안티 포렌식 행위 자체의 탐지는 자동화 하기 어려움
  - 데이터 완전 삭제 등의 대다수의 안티 포렌식 기법들은 패턴으로 만들기 어려움
  - 안티 포렌식의 탐지는 보통 수동으로 이루어짐
  - 도구를 탐지 하게 되면 안티 포렌식 탐지를 자동화 할 수 있음

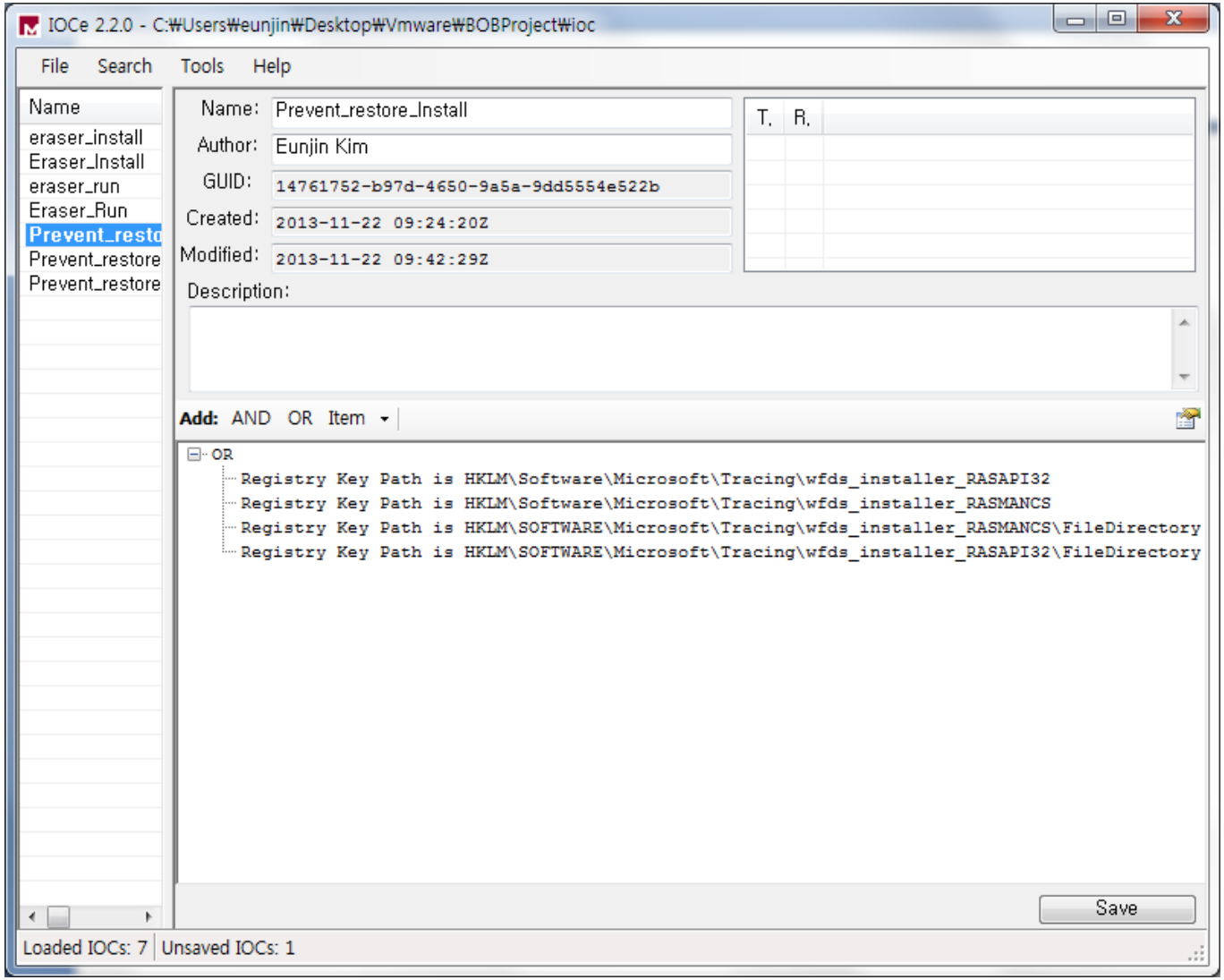
IOAF를 이용한 안티 포렌식 도구 탐지

- 안티 포렌식 기술 사용시 직접 만든 도구를 사용하는 경우가 적음
  - 안티 포렌식 기술이 비 전문가에게 대중화
    - ✓ 인터넷 등에 게시된 도구를 많이 사용
    - ✓ 전문가에 의한 안티 포렌식 보다 비전문가에 의한 안티 포렌식이 많음
- 분석관에게 분석 방향 제시
  - 분석 전에 간단히 안티 포렌식 사용 여부 점검
  - 안티 포렌식이 적용 유무에 따라 분석 방향이 달라짐

IOC와 IOAF

- **IOC**
  - XML 포맷으로 만들어 짐
  - AND, OR 등의 논리 연산자를 이용
  - 다양한 종류의 흔적 지원
    - ✓ Prefetch, registry , file item, driver list, logfile 등

IOC와 IOAF


IOCe 2.2.0 - C:₩Users₩eunjin₩Desktop₩Vmware₩BOBProject₩ioc
File
Search
Tools
Help
Name
eraser_install
Eraser_Install
eraser_run
Eraser_Run
Prevent_resto
Prevent_restore
Prevent_restore
Name: Prevent_restore_Install
Author: Eunjin Kim
GUID: 14761752-b97d-4650-9a5a-9dd5554e522b
Created: 2013-11-22 09:24:20Z
Modified: 2013-11-22 09:42:29Z
T.
R.
Description:
Add: AND OR Item
OR
Registry Key Path is HKLM\Software\Microsoft\Tracing\wfds_installer_RASAPI32
Registry Key Path is HKLM\Software\Microsoft\Tracing\wfds_installer_RASMANCS
Registry Key Path is HKLM\SOFTWARE\Microsoft\Tracing\wfds_installer_RASMANCS\FileDirectory
Registry Key Path is HKLM\SOFTWARE\Microsoft\Tracing\wfds_installer_RASAPI32\FileDirectory
Save
Loaded IOCs: 7
Unsaved IOCs: 1

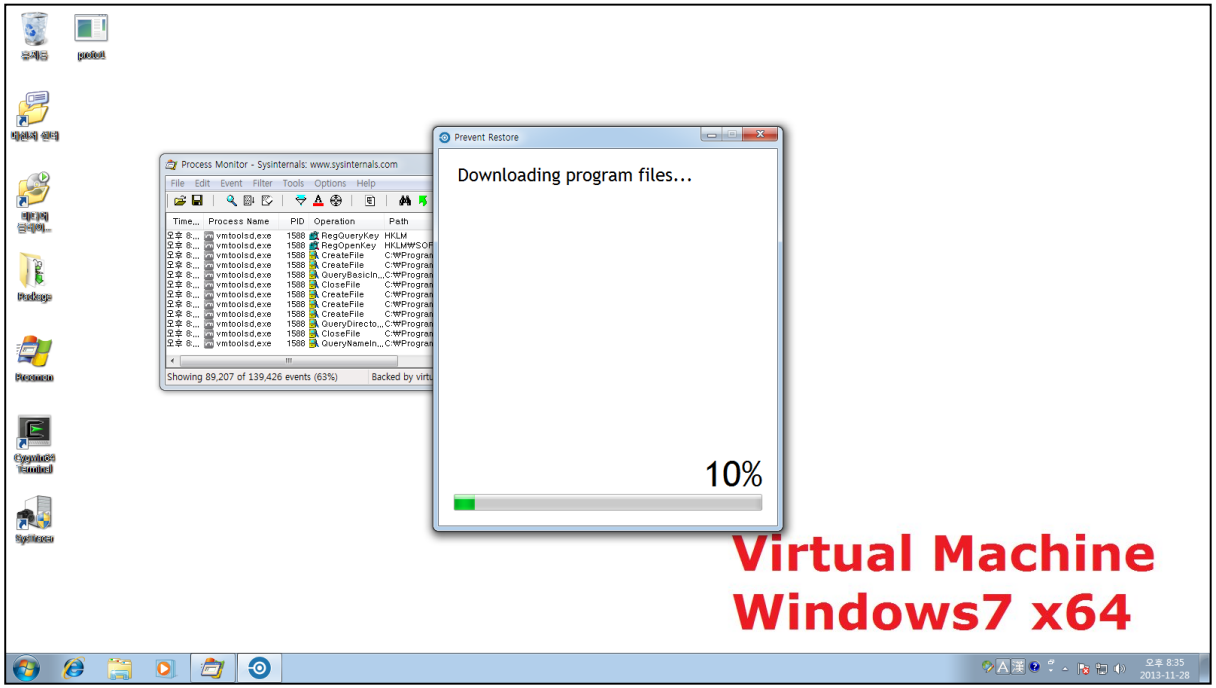
IOC와 IOAF

- **안티포렌식 도구 탐지를 위한 IOAF**
  - 지표 타입이 install, run(단순실행), use(기능 실행), uninstall 등으로 나누어짐
  - 지표 타입이 파일과 레지스트리로 2개임
    - ✓ 여러 도구에서 가장 많고 공통되는 흔적을 선별

```
<signs type="install">
    <and>
        <sign type="file" weight="0.3">.*?/AppData/LocalLow/Microsoft/CryptnetUrlCache/MetaData/CE4CFAB51DB3F9AB265C1526D1E6F12F_FC8C5CB969BCDC8ACE4FEF989663C7A4</sign>
        <sign type="file" weight="0.3">.*?/AppData/LocalLow/Microsoft/CryptnetUrlCache/Content/CE4CFAB51DB3F9AB265C1526D1E6F12F_FC8C5CB969BCDC8ACE4FEF989663C7A4</sign>
    </and>
</signs>
<signs type="run">
    <and>
        <sign type="reg" weight="0.2">^HKCU/Software/Eraser/Eraser 6$</sign>
        <sign type="reg" weight="0.2">^HKCU/Software/Eraser/Eraser 6/3460478d-ed1b-4ecc-96c9-2ca0e8500557$</sign>
        <sign type="reg" weight="0.2">^HKCU/Software/Eraser/Eraser 6/9977d7c4-c940-4b73-a02a-33c9ee2d47fe$</sign>
        <sign type="reg" weight="0.2">^HKCU/Software/Eraser/Eraser 6/e2e55c15-f188-4293-a4b2-1d8a016103b5$</sign>
        <sign type="reg" weight="0.2">^HKCU/Software/Eraser$</sign>
    </and>
</signs>
```

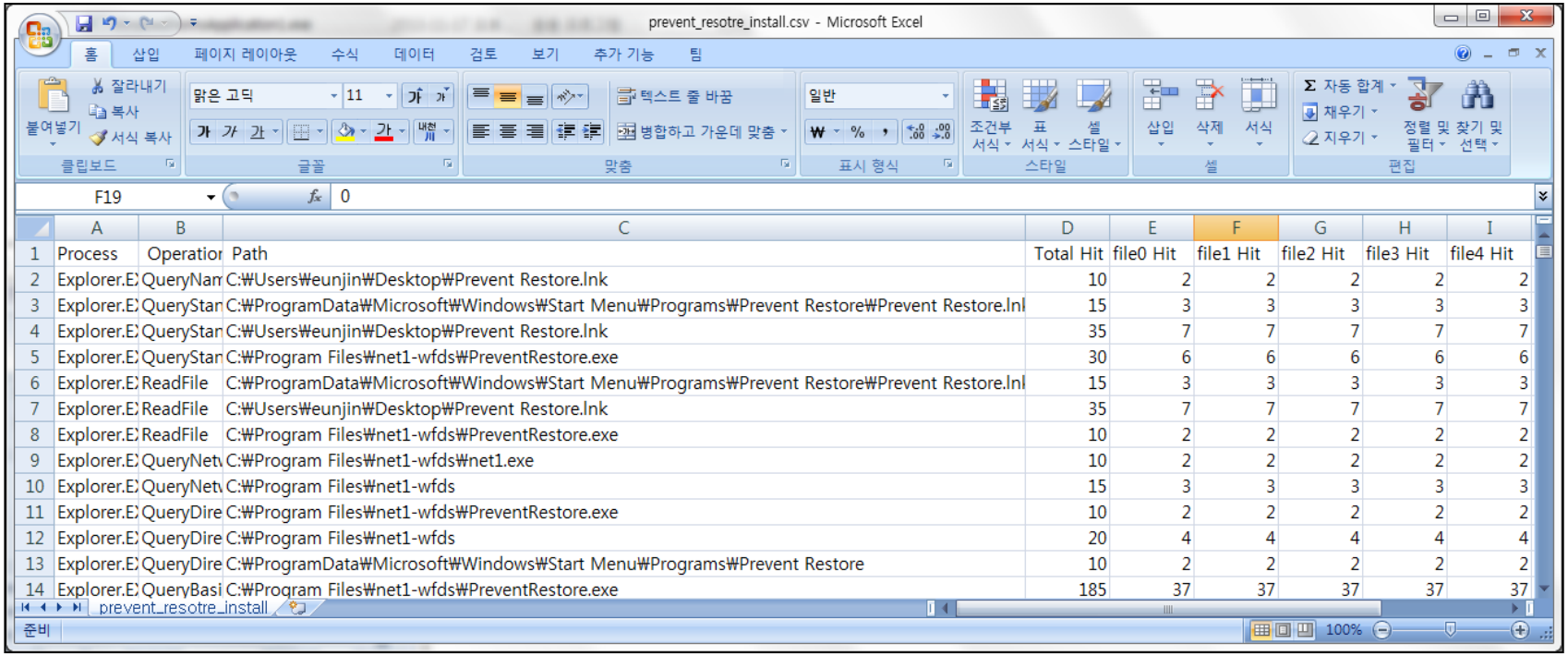
안티 포렌식 도구 지표 생성

- **Process Monitor로 안티 포렌식 도구의 설치, 실행, 삭제에 대한 로그 수집**
  - 가상 머신 에서 스냅샷 등을 이용하여 반복하여 로그 수집



안티 포렌식 도구 지표 생성

- **각 로그 파일에서 반복되어 나타나는 로그 항목 선별**
  - 동일한 로그가 계속 중복되어 나타나는 경우, 도구의 고유한 로그일 확률이 큼



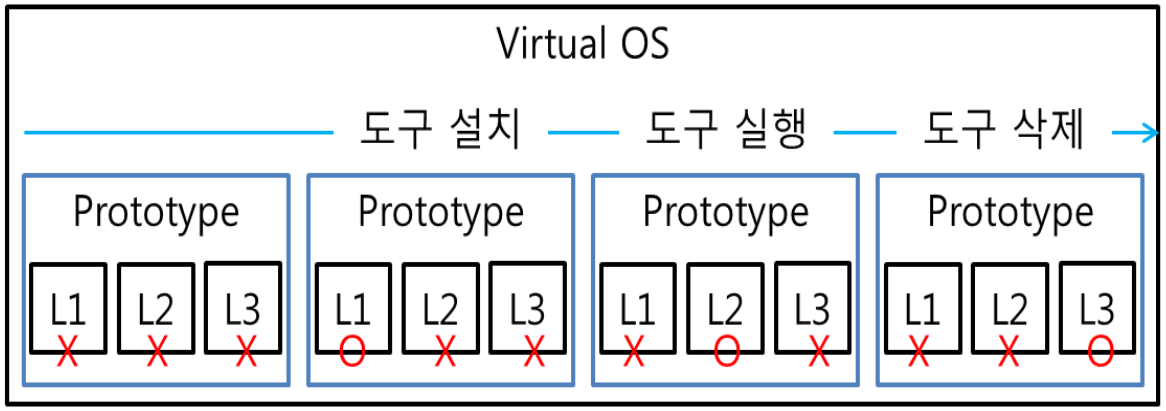
prevent_resotre_install.csv - Microsoft Excel

F19 | 0

	A	B	C	D	E	F	G	H	I
1	Process	Operation	Path	Total Hit	file0 Hit	file1 Hit	file2 Hit	file3 Hit	file4 Hit
2	Explorer.E	QueryNam	C:₩Users₩eunjin₩Desktop₩Prevent Restore.lnk	10	2	2	2	2	2
3	Explorer.E	QueryStan	C:₩ProgramData₩Microsoft₩Windows₩Start Menu₩Programs₩Prevent Restore₩Prevent Restore.lnk	15	3	3	3	3	3
4	Explorer.E	QueryStan	C:₩Users₩eunjin₩Desktop₩Prevent Restore.lnk	35	7	7	7	7	7
5	Explorer.E	QueryStan	C:₩Program Files₩net1-wfds₩PreventRestore.exe	30	6	6	6	6	6
6	Explorer.E	ReadFile	C:₩ProgramData₩Microsoft₩Windows₩Start Menu₩Programs₩Prevent Restore₩Prevent Restore.lnk	15	3	3	3	3	3
7	Explorer.E	ReadFile	C:₩Users₩eunjin₩Desktop₩Prevent Restore.lnk	35	7	7	7	7	7
8	Explorer.E	ReadFile	C:₩Program Files₩net1-wfds₩PreventRestore.exe	10	2	2	2	2	2
9	Explorer.E	QueryNet	C:₩Program Files₩net1-wfds₩net1.exe	10	2	2	2	2	2
10	Explorer.E	QueryNet	C:₩Program Files₩net1-wfds	15	3	3	3	3	3
11	Explorer.E	QueryDire	C:₩Program Files₩net1-wfds₩PreventRestore.exe	10	2	2	2	2	2
12	Explorer.E	QueryDire	C:₩Program Files₩net1-wfds	20	4	4	4	4	4
13	Explorer.E	QueryDire	C:₩ProgramData₩Microsoft₩Windows₩Start Menu₩Programs₩Prevent Restore	10	2	2	2	2	2
14	Explorer.E	QueryBasi	C:₩Program Files₩net1-wfds₩PreventRestore.exe	185	37	37	37	37	37

안티 포렌식 도구 지표 생성

- **반복적으로 나타나는 로그를 실제 시스템에서 확인**
  - 도구 설치 전, 도구 설치, 도구 실행, 도구 삭제가 된 상태에서 각각 테스트
  - X는 일치되는 로그 항목 삭제
  - O는 일치되지 않는 로그 항목 삭제



안티 포렌식 도구 지표 생성

- 지표 검증

종류	시그니처	적합 여부
파일	C:₩Program Files₩net1-wfds₩PreventRestore.exe	Yes
레지스트리	HKCU₩Software₩Microsoft₩Windows NT₩CurrentVersion₩AppCompatFlags	NO
레지스트리	HKLM₩SOFTWARE₩Microsoft₩Tracing₩wfds_installer_RASMANCS₩FileDirectory	YES
파일	C:₩Program Files₩net1-wfds₩Languages₩el.ini	YES
레지스트리	HKLM₩Software₩Microsoft₩Tracing₩wfds_installer_RASMANCS	YES
파일	C:₩Users₩eunjin₩AppData₩Roaming₩net1-wfds₩settings.ini	YES
파일	C:₩ProgramData₩Microsoft₩Windows₩Start Menu₩Programs₩Prevent Restore₩Prevent Restore.lnk	YES

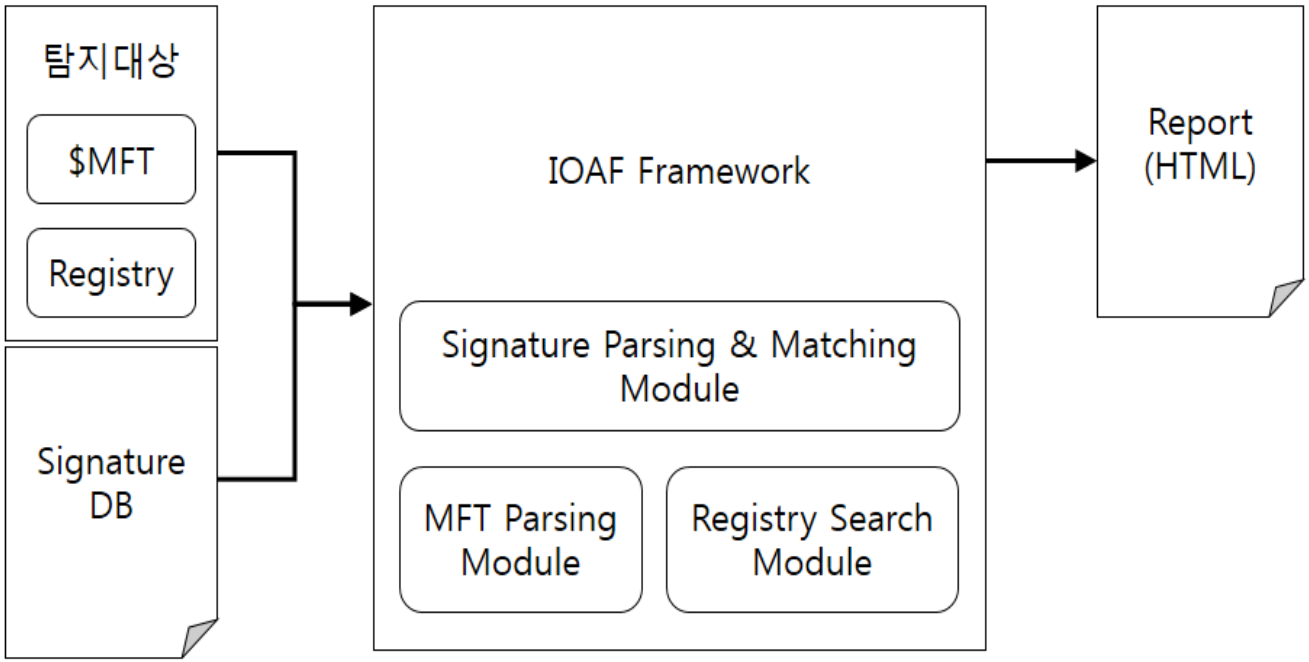
안티 포렌식 도구 지표 생성

- **정규표현식으로 변경**
  - User name
  - Download 경로
  - Program file

안티 포렌식 도구, Prevent Restore의 탐지 지표
.*?₩ProgramData₩Microsoft₩Windows₩Start Menu₩Programs₩Prevent Restore
.*?₩ProgramData₩Microsoft₩Windows₩Start Menu₩Programs₩Prevent Restore₩Visit our web site.url
.*?₩ProgramData₩Microsoft₩Windows₩Start Menu₩Programs₩Prevent Restore₩Help us translate.url
.*?₩ProgramData₩Microsoft₩Windows₩Start Menu₩Programs₩Prevent Restore₩Search for free updates.lnk
.*?₩ProgramData₩Microsoft₩Windows₩Start Menu₩Programs₩Prevent Restore₩Upgrade to PRO version.lnk
.*?₩AppData₩LocalLow₩Microsoft₩CryptnetUrlCache₩Content₩8AECE3B546DB08679345E5CEC4511FFC
.*?₩net1-wfds₩wfds.index
.*?₩Desktop₩setup_prevent_restore.exe
HKLM₩Software₩Microsoft₩Tracing₩wfds_installer_RASAPI32
HKLM₩Software₩Microsoft₩Tracing₩wfds_installer_RASMANCS

안티 포렌식 도구 탐지

- MFT와 Registry를 이용하여 탐지
- Signature DB와 비교하여 일치하는 항목이 있는지 검사



안티 포렌식 도구 탐지

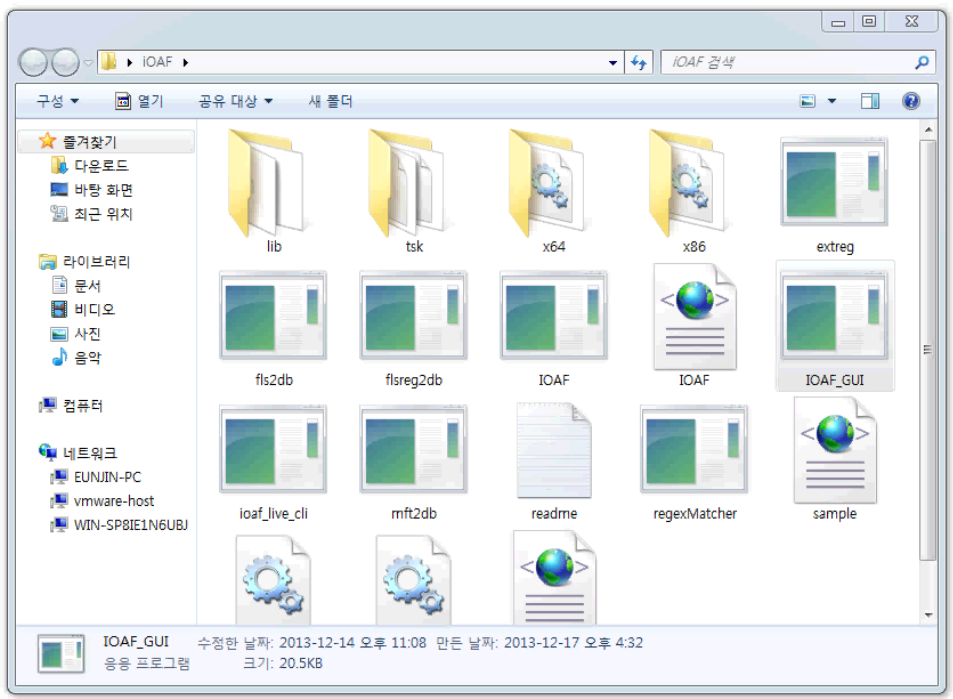
- **안티 포렌식 도구 지표의 일치 여부를 리포트로 출력**
  - 안티 포렌식 도구에 대한 버전, 다운로드 경로, 설명 비용 등의 정보 제공
    - ✓ 안티 포렌식을 사용한 사람의 숙련도 등을 파악할 수 있음

Eraser

type : Data destruction
importance : ★★★★★
URL : http://eraser.heidi.ie/
version : 6.0.10
Eraser is an advanced security tool for Windows which allows you to completely remove sensitive data form your hard drive by overwriting several times with carefull
fee : free
*** if run operation is detected, It also have posibility of run the function on the system.**

Group	Regex	Result
INSTALL +/-		
0	.*?/AppData/LocalLow/Microsoft/CryptnetUrlCache/MetaData/CE4CFAB51DB3F9AB265C1526D1E6F12F_FC8C5CB969BCDC8ACE4FEF989663C7A4	
0	.*?/AppData/LocalLow/Microsoft/CryptnetUrlCache/Content/CE4CFAB51DB3F9AB265C1526D1E6F12F_FC8C5CB969BCDC8ACE4FEF989663C7A4	
RUN +/-		
0	^HKCU/Software/Eraser/Eraser 6$	
0	^HKCU/Software/Eraser/Eraser 6/3460478d-ed1b-4ecc-96c9-2ca0e8500557$	
0	^HKCU/Software/Eraser/Eraser 6/9977d7c4-c940-4b73-a02a-33c9ee2d47fe$	
0	^HKCU/Software/Eraser/Eraser 6/e2e55c15-f188-4293-a4b2-1d8a016103b5$	
0	^HKCU/Software/Eraser$	
REMOVE +/-		

- DEMO



Anti-Forensic Tool Detection

- Live Mode -

활용 방안 고찰에 대한 질문

- DB화 된 파일 및 레지스트리 데이터를 다른 용도로 사용 한다면?
- 출력 되는 안티포렌식 도구 탐지 레포트에 포함되어야 할 내용?
- 안티포렌식 도구 탐지 및 타임라인 정보 등 제공 시, 시간과 활용성의 관계?
- 분석대상 PC의 안티포렌식 도구 유입 경로?
- 현재 탐지 지표 사용된 레지스트리, 파일시스템 외, 추가 되면 좋은 아티펙트는?

Question and Answer