

SCP Log Program

Contents

Window Log Analysis



Evtx Log Parsing Search Keyword



Evtx Log Parsing Log



At the end of the Personal Study

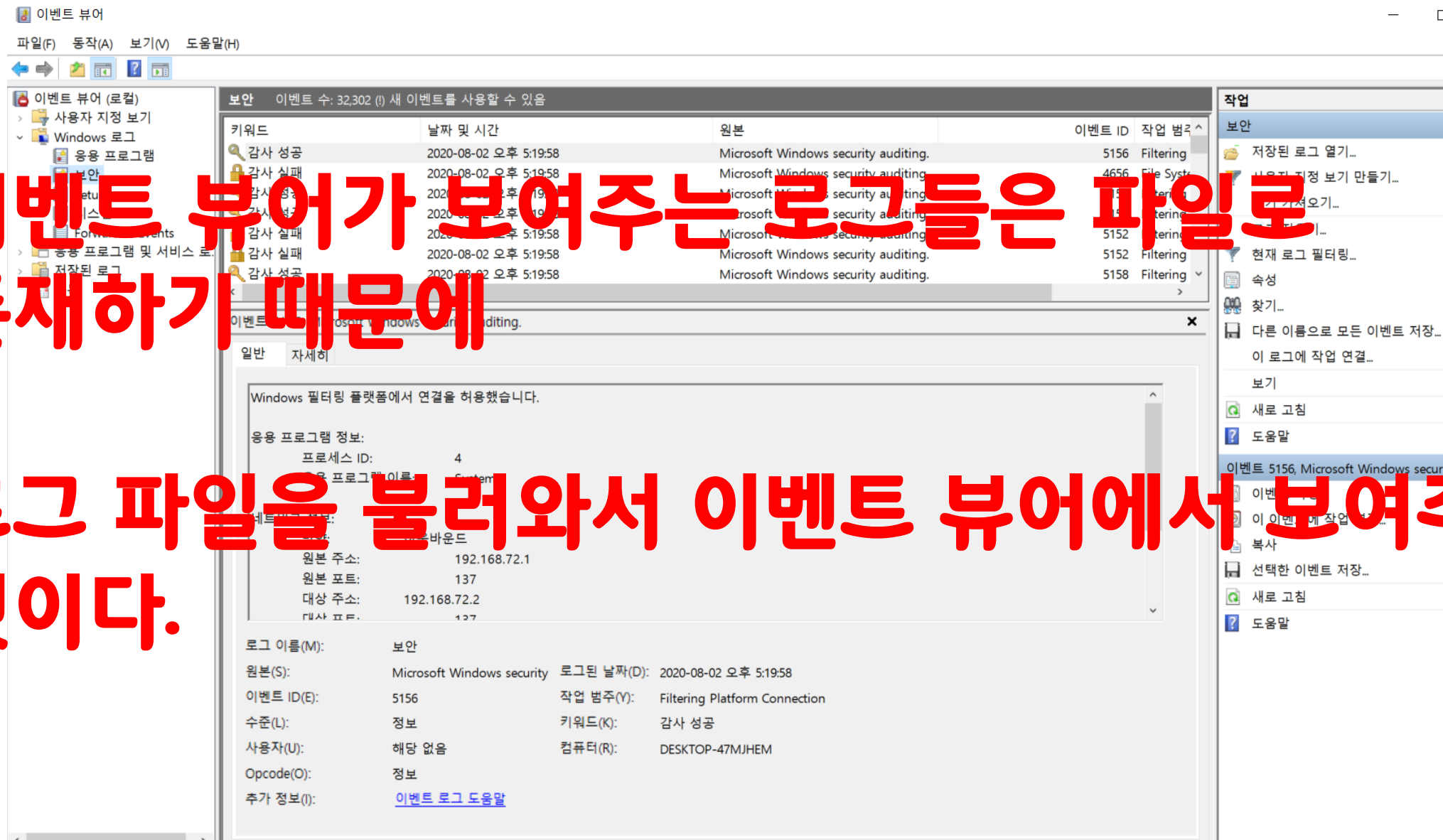
Window Log Analysis

WHY Window Log Analysis?

π

이벤트 뷰어가 보여주는 로그들은 파일로 존재하기 때문에


























로그 파일을 불러와서 이벤트 뷰어에서 보여주는 것이다.



Window 10 Log Path

π

– C:\Windows\System32\winevt\Logs

 Security.evtx	2020-08-02 오후 4:02	이벤트 로그	20,484KB
 Microsoft-Windows-Resource-Exhaustion-Resolver%4Operational.evtx	2020-08-02 오후 12...	이벤트 로그	1,028KB
 Application.evtx	2020-08-02 오전 11...	이벤트 로그	14,404KB
 Microsoft-Windows-Bits-Client%4Operational.evtx	2020-08-02 오전 11...	이벤트 로그	1,028KB
 Microsoft-Windows-Kernel-WHEA%4Errors.evtx	2020-08-02 오전 10...	이벤트 로그	1,028KB
 Microsoft-Windows-NlaSvc%4Operational.evtx	2020-08-02 오전 10...	이벤트 로그	1,028KB
 Microsoft-Windows-WindowsSystemAssessmentTool%4Operational.evtx	2020-08-02 오전 6:24	이벤트 로그	1,028KB
 Microsoft-Windows-Time-Service%4Operational.evtx	2020-08-02 오전 4:27	이벤트 로그	1,028KB
 Microsoft-Windows-Application-Experience%4Program-Compatibility-Assistant.evtx	2020-08-02 오전 2:58	이벤트 로그	1,028KB
 Microsoft-WindowsPhone-Connectivity-WiFiConnSvc-Channel.evtx	2020-04-26 오후 8:52	이벤트 로그	68KB
 Microsoft-Windows-Program-Compatibility-Assistant%4CompatAfterUpgrade.evtx	2020-04-26 오후 8:52	이벤트 로그	68KB
 Microsoft-Windows-Windows Firewall With Advanced Security%4Firewall.evtx	2020-08-01 오후 2:24	이벤트 로그	1,028KB
 Microsoft-Windows-Winlogon%4Operational.evtx	2020-08-01 오후 2:24	이벤트 로그	1,028KB
 Microsoft-Windows-WLAN-AutoConfig%4Operational.evtx	2020-08-01 오후 2:24	이벤트 로그	1,028KB
 System.evtx	2020-08-01 오후 2:24	이벤트 로그	20,484KB
 Microsoft-Windows-AppModel-Runtime%4Admin.evtx	2020-08-01 오후 2:23	이벤트 로그	1,028KB
 Microsoft-Windows-Shell-Core%4Operational.evtx	2020-08-01 오후 2:23	이벤트 로그	1,028KB
 Microsoft-Windows-Diagnosis-PCW%4Operational.evtx	2020-08-01 오후 2:23	이벤트 로그	1,028KB
 Microsoft-Windows-SMBServer%4Operational.evtx	2020-08-01 오후 2:23	이벤트 로그	2,116KB
 Microsoft-Windows-TerminalServices-LocalSessionManager%4Admin.evtx	2020-04-26 오후 8:52	이벤트 로그	68KB
 Microsoft-Windows-UserPnp%4ActionCenter.evtx	2020-04-26 오후 8:52	이벤트 로그	68KB
 Microsoft-Windows-Windows Defender%4WHC.evtx	2020-04-26 오후 8:52	이벤트 로그	68KB
 Microsoft-Windows-Windows Firewall With Advanced Security%4ConnectionSecurity.evtx	2020-04-26 오후 8:52	이벤트 로그	68KB
 Microsoft-Windows-Windows Firewall With Advanced Security%4FirewallDiagnostics.evtx	2020-04-26 오후 8:52	이벤트 로그	68KB
 Microsoft-Windows-WPD-ClassInstaller%4Operational.evtx	2020-04-26 오후 8:52	이벤트 로그	68KB

Window Log Analysis

› 폴더 생성 후 감사정책 적용

SCP 고급 보안 설정

이름: C:\Users\wallti\Desktop\SCP

소유자: Administrators (DESKTOP-47MJHEM\Administrators) 변경(C)

사용 권한 감사 유효한 액세스

자세한 내용을 보려면 감사 항목을 두 번 클릭하세요. 감사 항목을 수정하려면 항목을 선택하고 [편집]을 클릭하세요 (사용 가능한 경우).

감사 항목:

유형	보안 주체	다음에서 상속됨	적용 대상
성공	Everyone	없음	이 폴더, 하위 폴더 및 파일

추가(D) 제거(R) 편집(E)

감사정책 미적용시 로그가 남지 않음

Window Log Analysis

- › 폴더 생성 후 감사정책 적용
- › 감사정책 적용 폴더에 폴더 및 파일을
 - 생성
 - 수정
 - 삭제
 - 접근

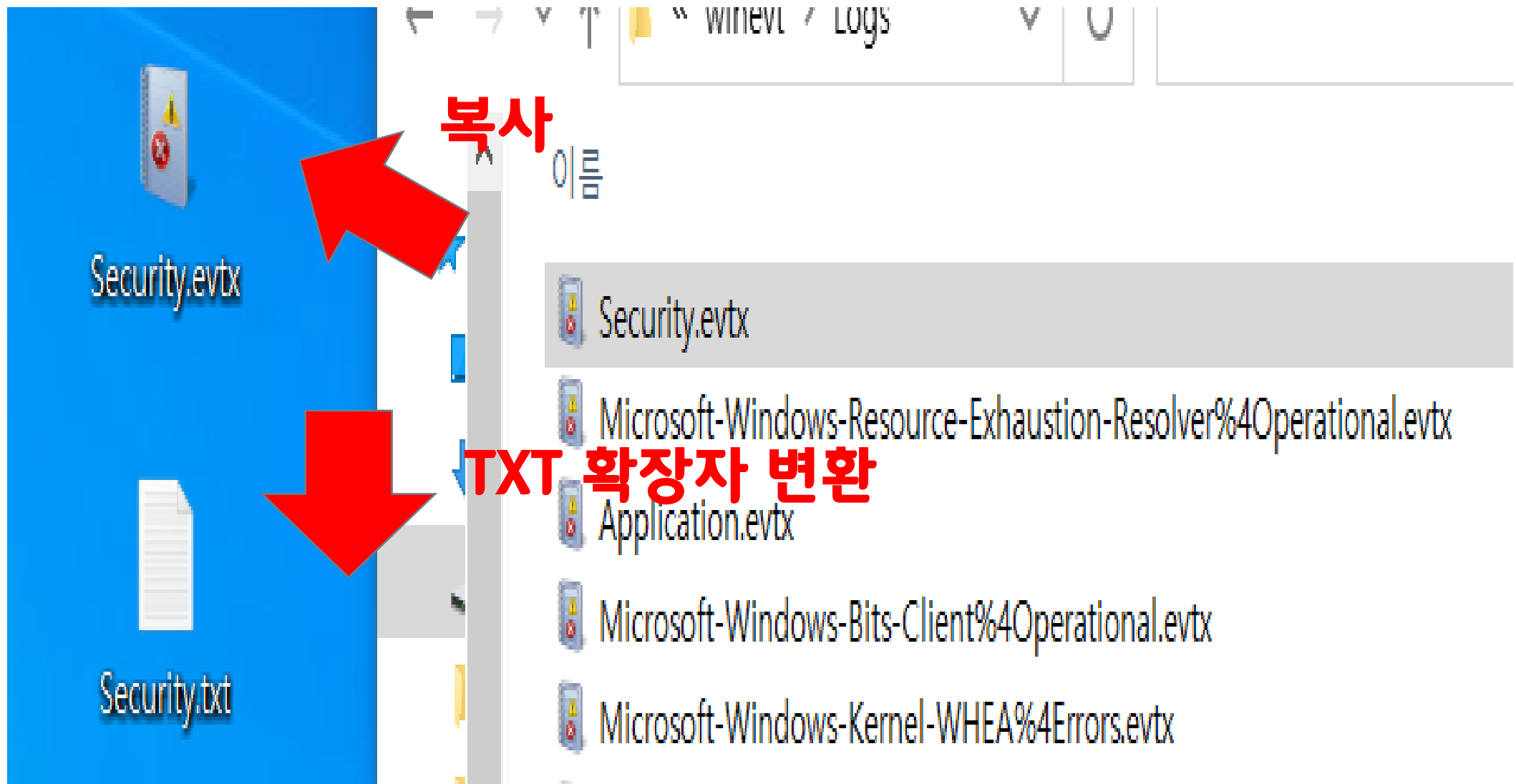
언급된 개수가 늘어남 = 로그가 남는다



하며 기록되는 로그확인(**언급되는 횟수 확인**)

Window Log Analysis

π



Window Log Analysis

π

ElfFileXW...
SystemTime...
EventRecordID...

0713SCP 폴더를 만들지 않았으니

Correlation\FF|
ActivityID... RelatedActivityID...

찾기

찾을 내용(N): 0713SCP

다음 찾기(F)

취소

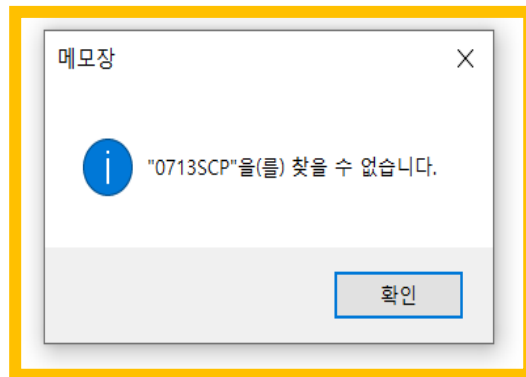
방향

☐ 위로(U) ☒ 아래로(D)

☐ 대/소문자 구분(C)

☐ 주위에 배치(B)

BF-?;nComputer | DESKTOP-47MJHEM A B??Security-?fL-UserID...
Security-Auditing%TxT... (?Security... 6P?... EventData A



검색결과가 없음

SourcePort
DestAddress
DestPort
Protocol
FilterRTID
LayerName
LayerRTID

RemoteUserID
RemoteMachineID

Window Log Analysis

π

> SCP > **0713SCP 폴더 생성**

이름	수정된 날짜	유형	크기
0713SCP	2020-08-02 오후 7:39	폴더	

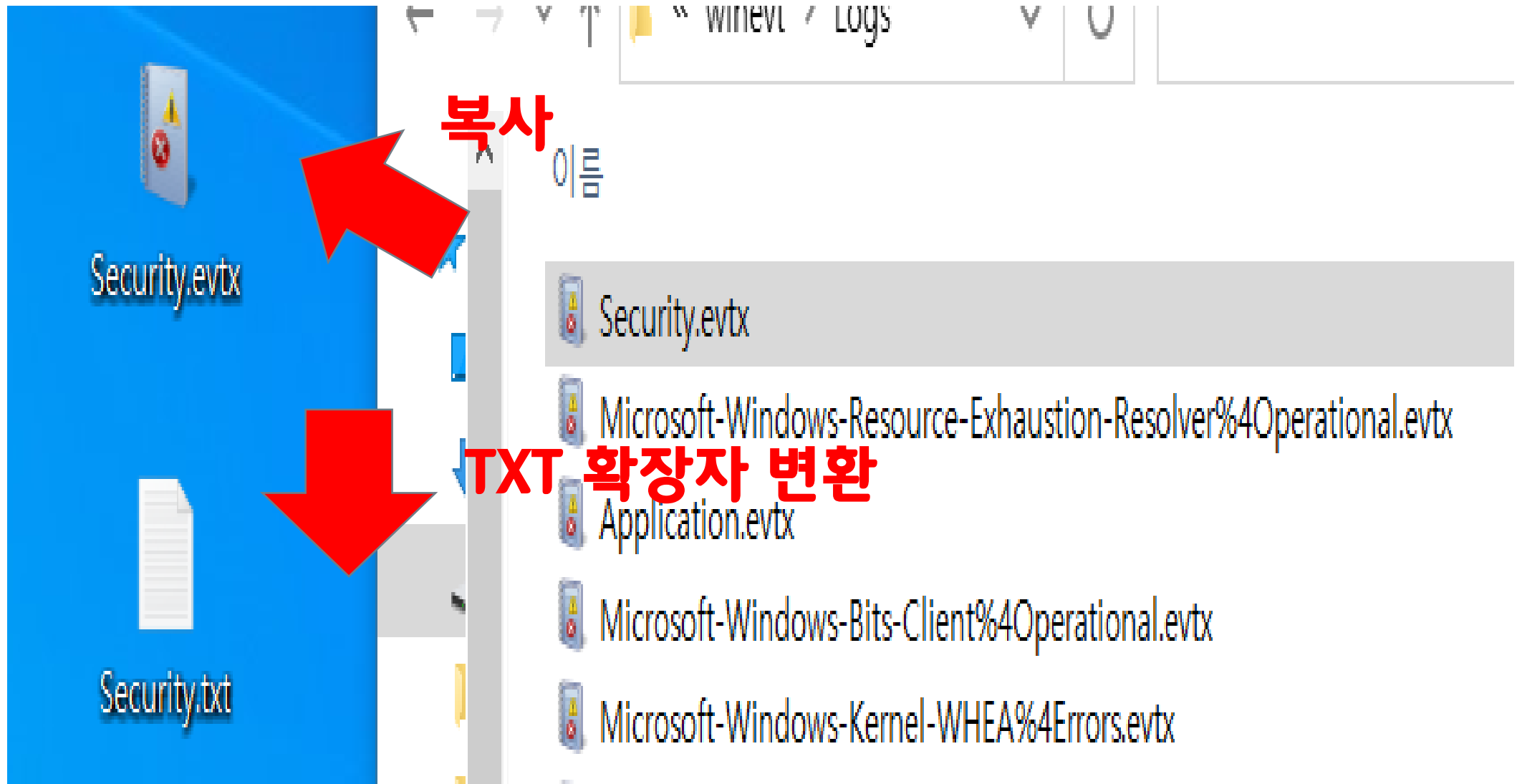


> SCP **0713SCP 폴더 삭제**

이름	수정된 날짜	유형	크기
이 폴더는 비어 있습니다.			

Window Log Analysis

π



Window Log Analysis

π

주체: 보안 ID: 계정 이름: 계정 도메인: 로그인 ID:

개체: 개체 서버: 핸들 ID: 0x20bc

프로세스 정보:

프로세스 ID: 0x276c

프로세스 이름: C:\Windows\explorer.exe

트랜잭션 ID: {00000000-0000-0000-0000-000000000000}

프로세스 정보:

프로세스 ID: 0x276c

프로세스 이름: C:\Windows\explorer.exe

트랜잭션 ID: {00000000-0000-0000-0000-000000000000}

Sec

ecu

주위에 배치(R)

Security

s\allti\Desktop\SCP\0713SCP?%%1537

%%1538

%%1541

%%4423

%%1537: %%1801 D:(A;OICI;0x1301bf;;;BU)

%%1538: %%1804

%%1541: %%1801 D:(A;OICI;0x1301bf;;;BU)

%%4423: %%1801 D:(A;OICI;0x1301bf;;;BU)

C:\Windows\explorer.exe-x**p

WINDOW LOG ANALYSIS

**** Event viewer ****

Forder	security.evtx	system.evtx	File
A 폴더 생성 감사 x	x	x	
A 폴더 생성 감사 o	A : 1	x	
A 폴더 안 R 폴더 생성	A : 4 R : o	x	

☐ 모든 권한

☐ 폴더 트래버스 / 파일 실행

☐ 폴더 목록 / 데이터 읽기

☐ 특성 읽기

☐ 확장 특성 읽기

☐ 파일 만들기 / 데이터 쓰기

☐ 폴더 만들기 / 데이터 추가

☐ 특성 쓰기

☐ 확장 특성 쓰기

☐ 삭제

☐ 사용 권한 읽기

☐ 사용 권한 변경

☐ 소유권 가져오기

B : 약 35

B 텍스트 파일 수정

A : 많음
B : 많음

?

A 폴더 안
B 텍스트 파일 삭제

B : 늘어남

?

B 텍스트 파일 열기
(접근)

Evtx Log Parsing Search

Evtx Log Parsing Search Keyword

- › Evtx text decoder
- › Evtx text Decryption
- › (Python, C) Evtx log parsing (example)
- › (Python, C) Evtx log parser
- › Python evtX import (moudule)

- › python window log parsing
 - win32evt모듈을 이용한 이벤트 로그 추출

Evtx Log Parsing

π

```
Python 3.8.5 (tags/v3.8.5:580fbb0, Jul 20 2020, 15:43:08) [MSC v.1926 32 bit (Intel)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
= RESTART: E:\Samsung_T5\University\SCP\SCP_Project\2020_Summer Project\SCP SCP Summer Project.py
<< SCP LOG PROGRAM >>
```

```
Event Category: 12810
Time Generated: 2020-08-03 10:33:13
Source Name: Microsoft-Windows-Security-Auditing
Event ID: 5156
Event Type: 8
Event Data:
13848
\device\harddiskvolume2\users\allti\appdata\local\programs\python\python38-32\pythonw.exe
%%14592
127.0.0.1
50171
127.0.0.1
50169
6
75125
%%14610
44
S-1-0-0
S-1-0-0
*****
Traceback (most recent call last):
  File "E:\Samsung_T5\University\SCP\SCP_Project\2020_Summer Project\SCP SCP Summer Project.py", line 35, in <module>
    time.sleep(3)
KeyboardInterrupt
>>> |
```

```
import win32evtlog as wevt
import datetime
import Evtx.Evtx as evt
import time

today = datetime.datetime.now().date()
day_ago = today - datetime.timedelta(days=1)

server = 'localhost'
logtype = 'Security'
hand = wevt.OpenEventLog(server, logtype)
flags = wevt.EVENTLOG_BACKWARDS_READ|wevt.EVENTLOG_SEQUENTIAL_READ
total = wevt.GetNumberOfEventLogRecords(hand)

while True:
    events = wevt.ReadEventLog(hand, flags, 0)
    if events:
        for evt in events:
            if str(evt.TimeGenerated)[:10] == str(today):
                print("\t\t<< SCP LOG PROGRAM >>\n")
                print('Event Category:', evt.EventCategory)
                print('Time Generated:', evt.TimeGenerated)
                print('Source Name:', evt.SourceName)
                print('Event ID:', evt.EventID)
                print('Event Type:', evt.EventType)
                data = evt.StringInserts

                if data:
                    print('Event Data:')

                    for msg in data:
                        print(msg)

                print('*' * 50)
                time.sleep(3)

            elif str(evt.TimeGenerated)[:10] == str(day_ago):
                break
```

EVTX LOG PARSING CODE

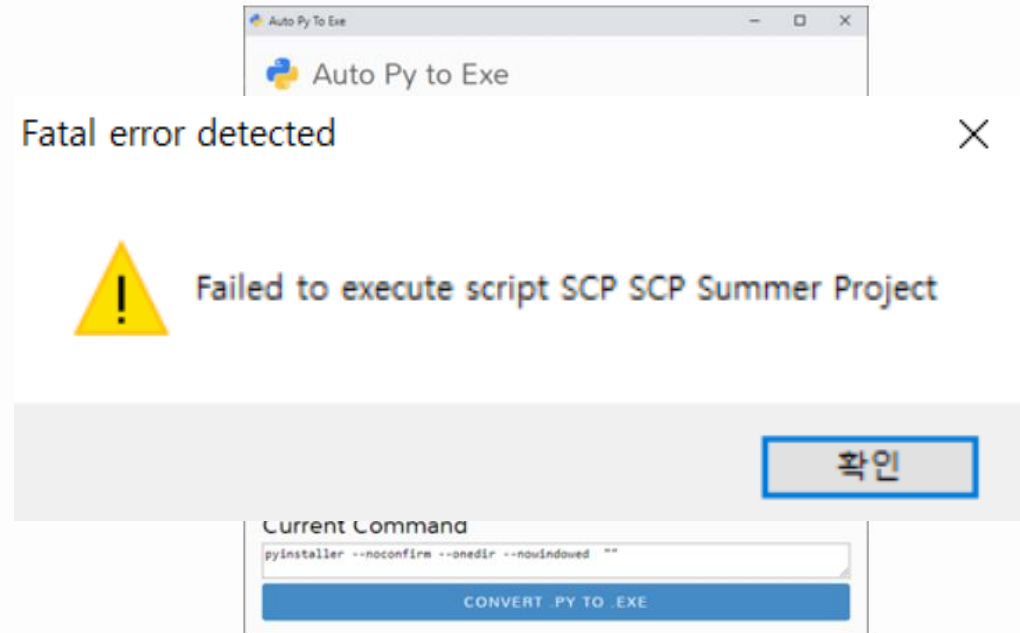
값	의미
win32evtlog.EVENTLOG_FORWARDS_READ	로그를 옛날 거부터 읽는다.(old to new)
win32evtlog.EVENTLOG_BACKWARDS_READ	로그를 최신 거 부터 읽는다.(new to old)

```
9 server = 'localhost'
10 logtype = 'Security'
11 hand = wevt.OpenEventLog(server, logtype)
12 flags = wevt.EVENTLOG_BACKWARDS_READ | wevt.EVENTLOG_SEQUENTIAL_READ
13 total = wevt.GetNumberOfEventLogRecords(hand)
14
15 while True:
16     events = wevt.ReadEventLog(hand, flags, 0)
17     if events:
18         for evt in events:
19             if str(evt.TimeGenerated)[:10] == str(today):
20                 print("\t\t\t<< SCP LOG PROGRAM >>\n")
21                 print('Event Category:', evt.EventCategory)
22                 print('Time Generated:', evt.TimeGenerated)
23                 print('Source Name:', evt.SourceName)
24                 print('Event ID:', evt.EventID)
25                 print('Event Type:', evt.EventType)
26                 data = evt.StringInserts
27
28                 if data:
29                     print('Event Data:')
30
31                     for msg in data:
32                         print(msg)
33
34                     print('!!! * 30')
35                     time.sleep(3)
36
37             elif str(evt.TimeGenerated)[:10] == str(day_ago):
38                 break
39
40
```

EXE

Auto PY to EXE

A .py to .exe converter using a simple graphical interface and [PyInstaller](#) in Python.



pypi [v2.7.5](#) python [2.7](#) | [3.5](#) | [3.6](#) | [3.7](#) license [MIT](#) downloads [325k](#) platform [windows](#) | [linux](#) | [macos](#)

At the end of the Personal Study

At the end of the Personal Study



WHY? → MOTIVATION



삽질보다는 길을 넓히는 과정



할 수 있다는 마인드

Thankyou

도움주신 조재현, 정재훈 선배님께
감사드립니다.