

IR-1 Tutorial

Step By Step으로 문제 접근하기

문제 확인

랜섬웨어에 걸린 것 같다.

최초로 감염된 파일명과 감염 시간, 어떤 파일에 의해 감염되었는지 입력하라.

파일명은 소문자로 입력, 띄어쓰기는 언더바(_) 처리, 타임스탬프는 한국 시간인 UTC+9를 따르며, ISO 8601 표준에 의해 날짜와 날짜 사이에 T 문자를 입력한다.

ex: KEEPER{asdf.asd_2024-12-23T12:34:56_example.exe}

Download Link: <https://drive.google.com/file/d/1KhkiZXagtpBXRQ63et2ZCyDtpvAlko87>

E01이 뭘까?

Google Drive에서 파일에 바이러스가 있는지 검사할 수 없습니다

240103.E01(6.3G) 파일이 너무 커서 바이러스 검사를 할 수 없습니다. 그래도 파일을 다운로드하시겠습니까?

무시하고 다운로드

- 문제 파일을 보면 E01이라는 확장자와 용량(6.3G)이 큰 것을 확인할 수 있다.

Introduction

Developed by ASR Data, the Expert Witness file format (aka E01 format aka EnCase file format) is an industry standard format for storing “forensic” images. The format allows a user to access arbitrary offsets in the uncompressed data without requiring decompression of the entire data stream. The specification does **NOT** provide for quantifiable assurance of integrity, it is up to the implementation to provide meaningful authentication for **any** data contained in an “evidence file”.

- E01은 Guidance software¹에서 개발한 압축 포맷이며, 하드디스크 백업본을 파일의 형태로 저장할 수 있다. 대부분의 포렌식 이미징 도구에서 E01 파일 포맷을 지원한다.^{2 3 4}

¹ https://en.wikipedia.org/wiki/Guidance_Software

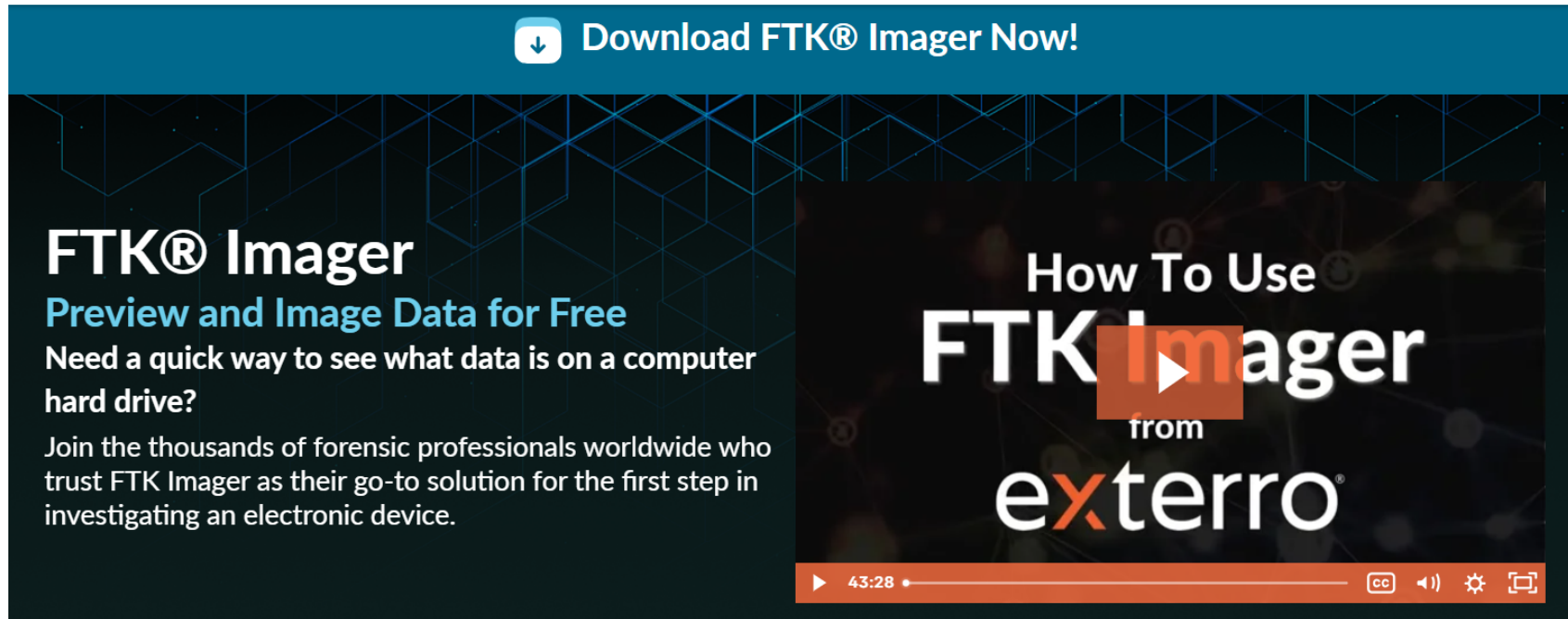
² https://forensics.wiki/encase_image_file_format/

³ <https://blog.naver.com/happymaru11/222102005996>

⁴ http://www.asrdata.com/?page_id=1566

FTK Imager 사용하기

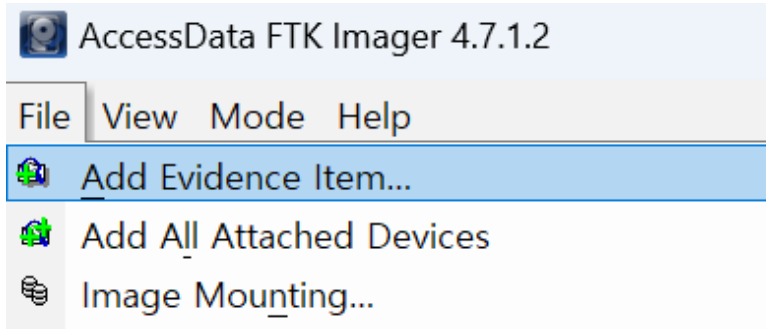
- E01 파일을 열기 위해서 해당 포맷을 해석해주는 도구를 사용해야 한다.
- 다양한 이미징 도구 중에서 무료인 FTK Imager를 많이 사용한다.¹
- Download Link: <https://www.exterro.com/ftk-imager>



¹ https://en.wikipedia.org/wiki/Digital_forensic_process#Acquisition

FTK Imager 사용하기

- File → Add Evidence Item → Image File → E01 파일 열기



Add Evidence Item 클릭

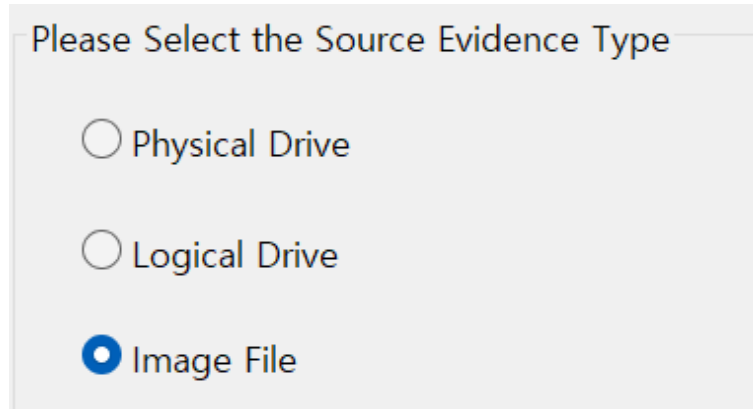
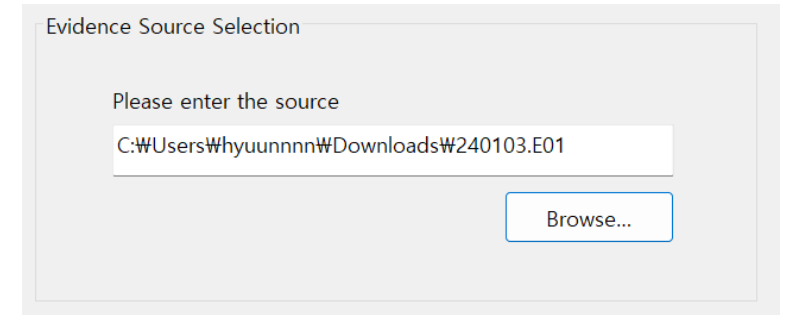


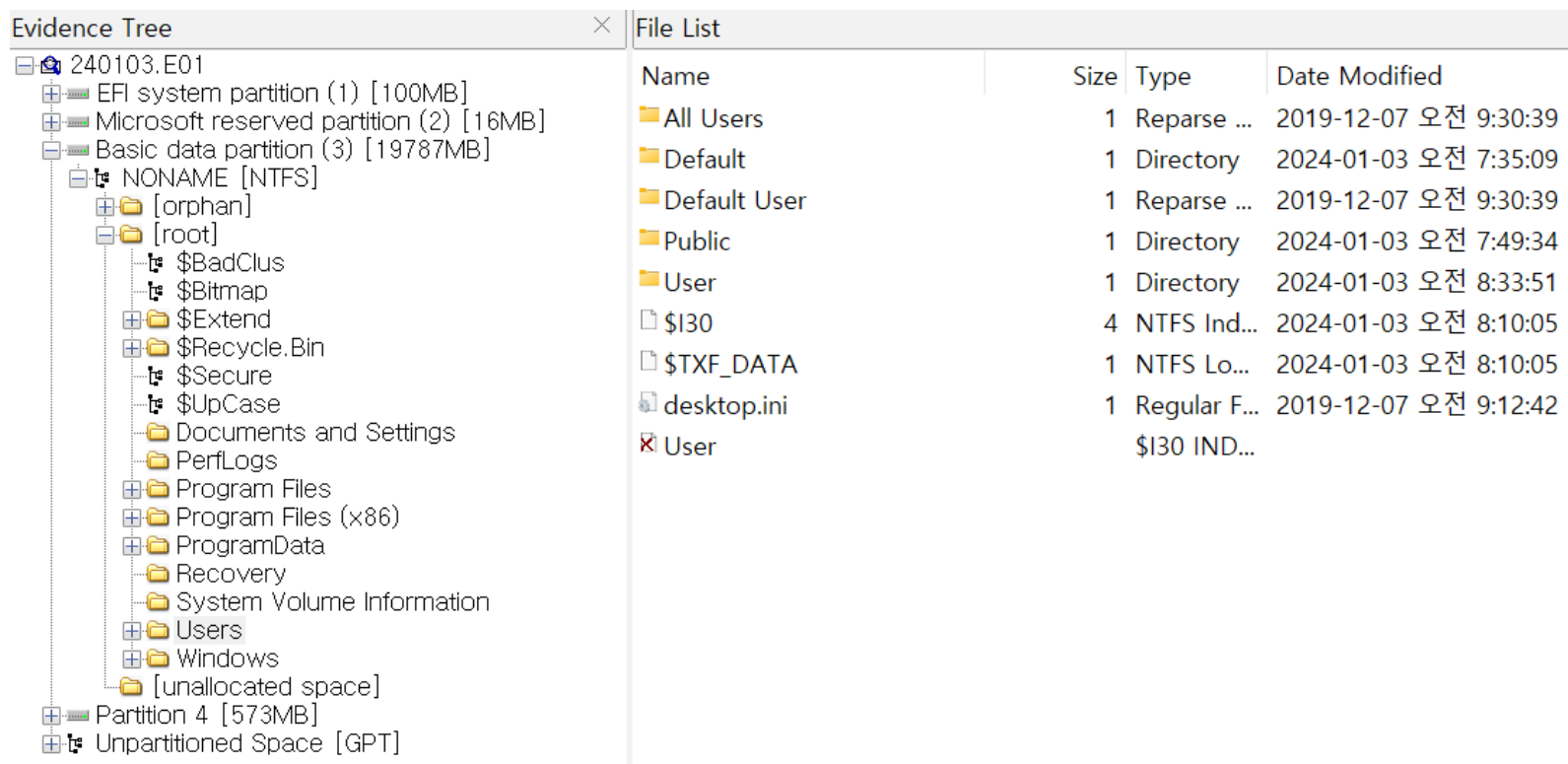
Image File 클릭



E01 파일 열기

FTK Imager 사용하기

- 윈도우를 포맷할 때 사용되는 파티션 외에도 시스템 예약 파티션과 같은 추가 파티션이 생성된다.
- 그 중에서 C 드라이브의 파티션을 확인해보자. (용량이 가장 큰 파티션을 누르면 된다.)



The screenshot displays the FTK Imager interface with two main panes: 'Evidence Tree' on the left and 'File List' on the right.

Evidence Tree:

- 240103.E01
 - EFI system partition (1) [100MB]
 - Microsoft reserved partition (2) [16MB]
 - Basic data partition (3) [19787MB]
 - NONAME [NTFS]
 - [orphan]
 - [root]
 - \$BadClus
 - \$Bitmap
 - \$Extend
 - \$Recycle.Bin
 - \$Secure
 - \$UpCase
 - Documents and Settings
 - PerfLogs
 - Program Files
 - Program Files (x86)
 - ProgramData
 - Recovery
 - System Volume Information
 - Users
 - Windows
 - [unallocated space]
 - Partition 4 [573MB]
 - Unpartitioned Space [GPT]

File List:

Name	Size	Type	Date Modified
All Users	1	Reparse ...	2019-12-07 오전 9:30:39
Default	1	Directory	2024-01-03 오전 7:35:09
Default User	1	Reparse ...	2019-12-07 오전 9:30:39
Public	1	Directory	2024-01-03 오전 7:49:34
User	1	Directory	2024-01-03 오전 8:33:51
\$I30	4	NTFS Ind...	2024-01-03 오전 8:10:05
\$TXF_DATA	1	NTFS Lo...	2024-01-03 오전 8:10:05
desktop.ini	1	Regular F...	2019-12-07 오전 9:12:42
User		\$I30 IND...	

NTFS Log Tracker 사용하기

- 문제를 보면 랜섬웨어의 행위를 분석해야 한다.
- 윈도우는 일반적으로 NTFS 파일 시스템¹을 사용하는데, NTFS의 경우 \$MFT, \$LogFile, \$UsnJrnl:\$J라는 메타데이터 파일들이 존재한다. 이를 추출하여 윈도우에서 발생한 기록, 정보들을 분석할 수 있다.^{2 3 4 5}
- 위 파일들을 분석하는 여러 도구들이 있는데 그 중에서 NTFS Log Tracker를 사용해보자.
- 다른 도구들이 궁금하다면 [ArtifactParsers](#), [awesome-forensics](#) 등을 참고해보자.
- Download Link: <https://sites.google.com/site/forensicnote/ntfs-log-tracker>

¹ <https://ko.wikipedia.org/wiki/NTFS>

² http://forensic.korea.ac.kr/DFWIKI/index.php/로그_%26_저널_분석/NTFS

³ <http://forensic.korea.ac.kr/DFWIKI/index.php/메타데이터/NTFS>

⁴ <https://www.igloo.co.kr/security-information/행위-분석을-위한-구조-분석-및-추출-방안-데이터-런/>

⁵ <http://forensicinsight.org/wp-content/uploads/2013/06/F-INSIGHT-NTFS-Log-TrackerKorean.pdf>

NTFS Log Tracker 사용하기

Basic data partition (3) [19787MB]

NONAME [NTFS]

[orphan]

[root]

\$BadClus

\$Bitmap

\$Extend

\$Recycle.Bin

\$Secure

\$UpCase

Documents and Settings

PerfLogs

Program Files

Program Files (x86)

ProgramData

Recovery

System Volume Information

Users

Windows

[unallocated space]

Partition 4 [573MB]

Unpartitioned Space [GPT]

Program Files

Program Files (x86)

ProgramData

Recovery

System Volume Information

Users

Windows

\$AttrDef

\$BadClus

\$Bitmap

\$Boot

\$I30

\$LogFile

\$MFT

\$MFTMirr

1 Directory

1 Directory

1 Directory

1 Directory

1 Directory

1 Directory

1 Directory

3 Regular F...

0 Regular F...

619 Regular F...

8 Regular F...

4 NTFS Ind...

29,648 Regular F...

123,136 Regular F...

4 Regular F...

2024-01-03 오전 8:20:25

2024-01-03 오전 8:04:13

2024-01-03 오전 7:53:32

2024-01-03 오전 7:35:15

2024-01-03 오전 7:37:25

2024-01-03 오전 8:10:05

2024-01-03 오전 8:20:53

2024-01-03 오전 7:28:34

2024-01-03 오전 7:28:34

2024-01-03 오전 7:28:34

2024-01-03 오전 7:28:34

2024-01-03 오전 8:20:28

2024-01-03 오전 7:28:34

2024-01-03 오전 7:28:34

2024-01-03 오전 7:28:34

[root] 경로에서 \$LogFile, \$MFT 추출

240103.E01

EFI system partition (1) [100MB]

Microsoft reserved partition (2) [16MB]

Basic data partition (3) [19787MB]

NONAME [NTFS]

[orphan]

[root]

\$BadClus

\$Bitmap

\$Extend

\$Deleted

\$ObjId

\$Reparse

\$RmMetadata

\$UsnJrnl

Name	Size	Type	Date Modified
\$J	29,354	Alternate...	2024-01-03 오전 7:33:11
\$J.FileSlack	23	File Slack	
\$Max	1	Alternate...	2024-01-03 오전 7:33:11

[root]\\$Extend\\$UsnJrnl 클릭 후 \$J 추출

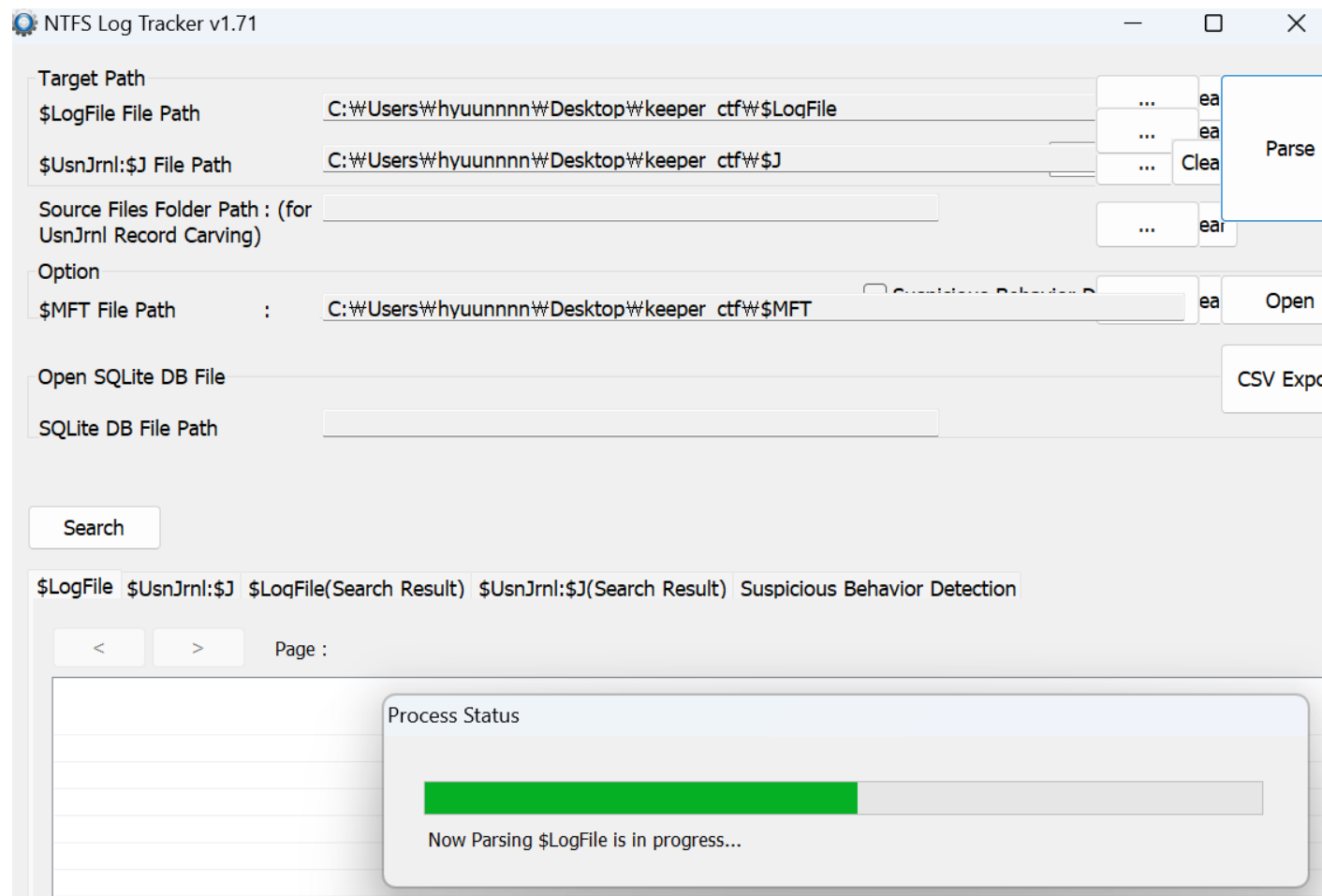
NTFS Log Tracker 사용하기

- 위 파일들은 운영체제 관련 파일들이기 때문에 탐색기를 열었을 때 보이지 않는데, 아래와 같이 설정해주면 된다.
- 파일 탐색기 옵션 검색 → 보기 클릭 → 보호된 운영 체제 파일 숨기기(권장) 체크 해제
- 나머지 옵션은 추가로 숨겨진 파일 확인이나 확장자 수정에 용이하기 때문에 일반적으로 모두 보이게 설정한다.

- ☐ 보호된 운영 체제 파일 숨기기(권장)
- ☒ 빈 드라이브 숨기기
- ☒ 상태 표시줄 표시
- ☒ 숨김 파일 및 폴더
 - ☐ 숨김 파일, 폴더 또는 드라이브 표시 안 함
 - ☒ 숨김 파일, 폴더 및 드라이브 표시
- ☐ 아이콘은 항상 표시하고 미리 보기는 표시하지 않음
- ☐ 알려진 파일 형식의 파일 확장명 숨기기

NTFS Log Tracker 사용하기

- 추출한 3개의 파일을 올린 후 Parse 버튼 클릭 → SQLite 파일명 및 경로는 아무 곳이나 상관 없음



NTFS Log Tracker 사용하기

- 분석이 완료되었다면 아래와 같은 결과가 보이는데, 더욱 편하고 의미있는 분석을 하기 위해 CSV 추출
CSV Export → 경로 설정 후 확인

Open SQLite DB File

SQLite DB File Path

Search

CSV Expo










\$LogFile \$UsnJrnl:\$J \$LogFile(Search Result) \$UsnJrnl:\$J(Search Result) Suspicious Behavior Detection

< > Page : (1 / 1)

LSN	EventTime(UT...	Event	Detail	File/Directory Name	Full Path(from \$MFT)
181081698		Writing Content of No...	Data Runs(in Volume)...		
181082147	2024-01-03 17...	Directory Creation		th	
181082456	2024-01-03 17...	File Creation		FileSync.LocalizedRes...	
181082764		Writing Content of No...	Data Runs(in Volume)...	FileSync.LocalizedRes...	
181083208	2024-01-03 17...	Directory Creation		ti	
181083517	2024-01-03 17...	File Creation		FileSync.LocalizedRes...	
181083822		Writing Content of No...	Data Runs(in Volume)...	FileSync.LocalizedRes...	
181084287	2024-01-03 17...	Directory Creation		tk-TM	
181084599	2024-01-03 17...	File Creation		FileSync.LocalizedRes...	
181084908		Writing Content of No...	Data Runs(in Volume)...	FileSync.LocalizedRes...	
181085358	2024-01-03 17...	Directory Creation		tn-ZA	
181085670	2024-01-03 17...	File Creation		FileSync.LocalizedRes...	
181085975		Writing Content of No...	Data Runs(in Volume)...	FileSync.LocalizedRes...	

NTFS Log Tracker 사용하기

- 지금까지의 모든 단계를 따라왔다면 아래 사진과 같은 파일들을 확인할 수 있다.
- CSV 파일들을 분석하여 랜섬웨어의 행위를 분석하고 답을 찾아보자.

 \$J	2024-01-03 오후 4:33	시스템 파일	29,354KB
 \$LogFile	2024-01-03 오후 4:28	시스템 파일	29,648KB
 \$MFT	2024-01-03 오후 4:28	시스템 파일	123,136KB
 NLT_LogFile_2024-01-14 00-22-27.csv	2024-01-14 오전 12:22	Microsoft Excel 싼표...	2,522KB
 NLT_LogFile_Search_2024-01-14 00-22-27.csv	2024-01-14 오전 12:22	Microsoft Excel 싼표...	1KB
 NLT_Suspicious_Behavior_Detection_2024-01-14 00-22-27.csv	2024-01-14 오전 12:22	Microsoft Excel 싼표...	1KB
 NLT_UsnJrnl_2024-01-14 00-22-27.csv	2024-01-14 오전 12:22	Microsoft Excel 싼표...	51,069KB
 NLT_UsnJrnl_Search_2024-01-14 00-22-27.csv	2024-01-14 오전 12:22	Microsoft Excel 싼표...	1KB
 test_2024-01-14 00-17-35.db	2024-01-14 오전 12:17	Data Base File	131,035KB

- Excel 프로그램, [Timeline Explorer](#) 등 자신에게 편리한 프로그램으로 CSV 분석

CSV 파일 분석 꿀팁

- 첫 번째 라인 클릭 (사진 왼쪽에 1을 누르면 된다.) → 홈 → 정렬 및 필터 → 필터 클릭
 - 각 카테고리에 원하는 데이터만 볼 수 있게 필터링하거나 정렬하는 방법을 활용해보자.

	A	B	C	D	E	F	G	H	I	J
1	TimeStamp(UTC+9)	USN	File/Dir	FullPath	EventIn	Source	FileAttr	Carving	FileRef	ParentFileReferenceNumber
2	2024-01-03 16:33	88	shell32.dll	\\Window	File_Close	Normal	Archive		0x00010000	0x000100000000446B
3	2024-01-03 16:33	176	psapi.dll	\\Window	File_Close	Normal	Archive		0x00010000	0x0001000000001FE3
4	2024-01-03 16:33	256	setupapi.dll	\\Window	File_Close	Normal	Archive		0x00010000	0x0001000000004418

- 타임스탬프 설정
 - Office Excel의 경우 타임스탬프로 보여주는 값이 미흡하다.
 - A 클릭 (A열 전체 드래그) → 오른쪽 클릭 → 셀 서식 → 사용자 지정 → 아래 사진과 같이 세팅

	A
1	TimeStamp(UTC+9)
2	2024-01-03 16:33:11
3	2024-01-03 16:33:11
4	2024-01-03 16:33:11
5	2024-01-03 16:33:11
6	2024-01-03 16:33:11

회계
날짜
시간
백분율
분수
지수
텍스트
기타
사용자 지정

형식(I):
yyyy-mm-dd hh:mm:ss
h:mm:ss AM/PM
h:mm
h:mm:ss
h"시" mm"분"
h"시" mm"분" ss"초"
yyyy-mm-dd h:mm

CSV 파일 분석 꿀팁

- Timeline Explorer
 - 중복되는 내용들을 그룹핑하여 로그를 볼 수 있다.

20240116153350_EvtxECmd_Output.csv							
Map Description ▾							
	Line	Tag	Record Number	Event Record Id	Event Id	Time Created ▲	Level
⌵	=	■	=	=	=	=	Info
> Map Description: Pipeline executed (Count: 12)							
> Map Description: Performing Create VHD (Count: 12)							
> Map Description: Performance summary for Storport Device (Count: 2,834)							
> Map Description: Path of executed program (Count: 985)							
▼ Map Description: OS was started (Count: 60)							
	381135	□	85815	85815	12	2023-10-04 08:58:51	Info
	382128	□	86808	86808	12	2023-10-07 09:09:16	Info
	382675	□	87355	87355	12	2023-10-09 22:39:18	Info
	383626	□	88306	88306	12	2023-10-12 00:08:16	Info
	384827	□	89507	89507	12	2023-10-16 06:37:55	Info
	385107	□	89787	89787	12	2023-10-16 09:03:44	Info
	385299	□	89979	89979	12	2023-10-16 09:05:09	Info

CSV 파일 분석 꿀팁

- 랜섬웨어가 어떤 행위를 할까?
 - 랜섬웨어는 특정 파일들을 암호화시킬 때 특정 확장자로 변하지 않던가?
 - 랜섬웨어 동작이 끝나면 무엇을 하지?
 - 랜섬노트가 생성되지 않나?
- 이러한 행위들을 생각하고, 분석하여 랜섬웨어의 전체적인 동작 흐름을 분석해보자.

주의사항

- 랜섬웨어를 실행하지 않게 조심하자. - 랜섬웨어 바이너리 자체를 분석하는 문제는 없다.
- 랜섬웨어 파일을 추출했을 때 백신이 켜져있다면 자동으로 삭제되므로 백신을 꺼두자.

바이러스 및 위협 방지 설정

Microsoft Defender 바이러스 백신에 대한 바이러스 및 위협 방지 설정을 보고 업데이트할 수 있습니다.

실시간 보호 기능

맬웨어를 찾고 디바이스에서 설치되거나 실행하는 것을 방지합니다. 이 설정을 잠시 동안 끌 수 있습니다. 그러면 자동으로 다시 켜집니다.



컴