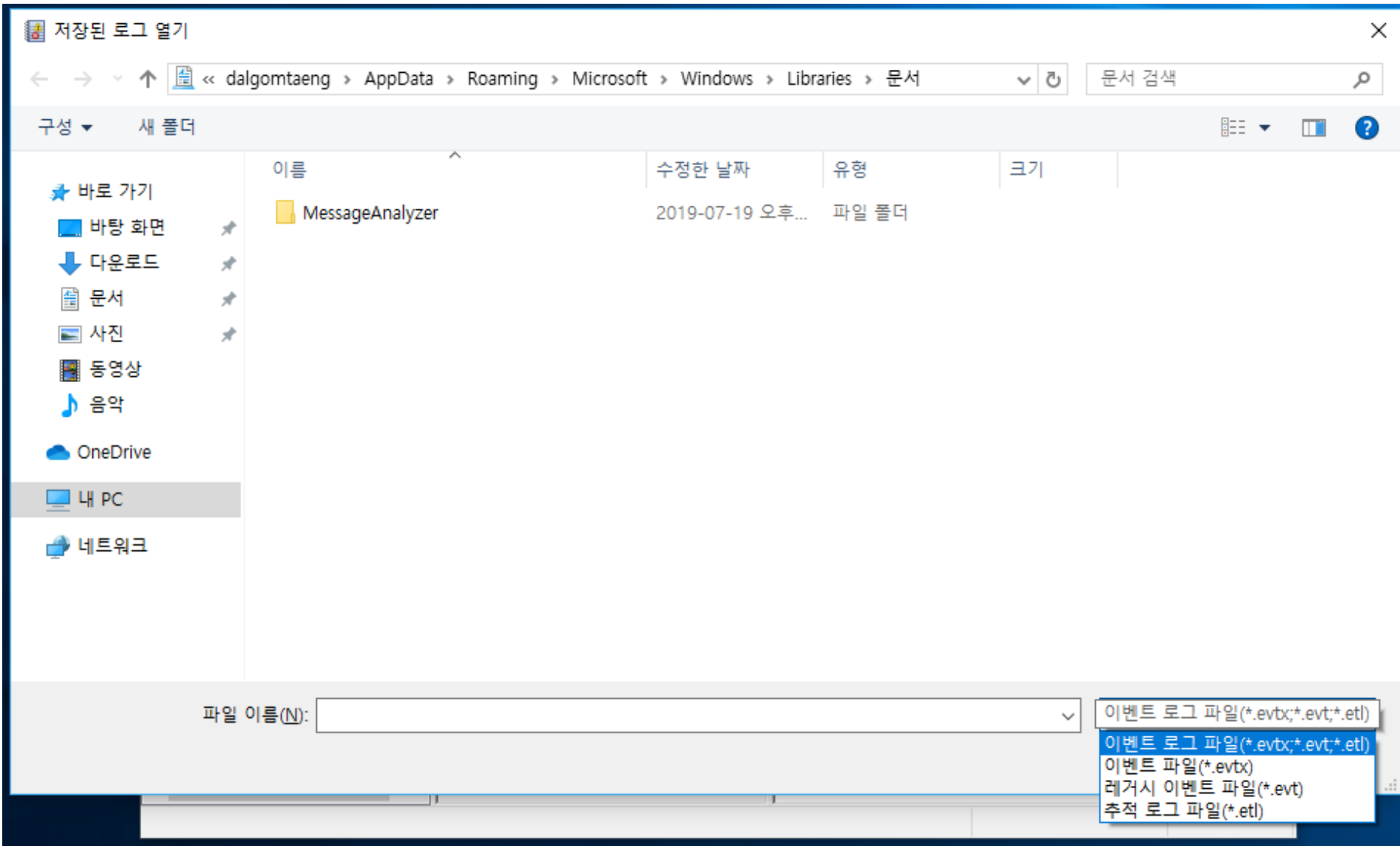


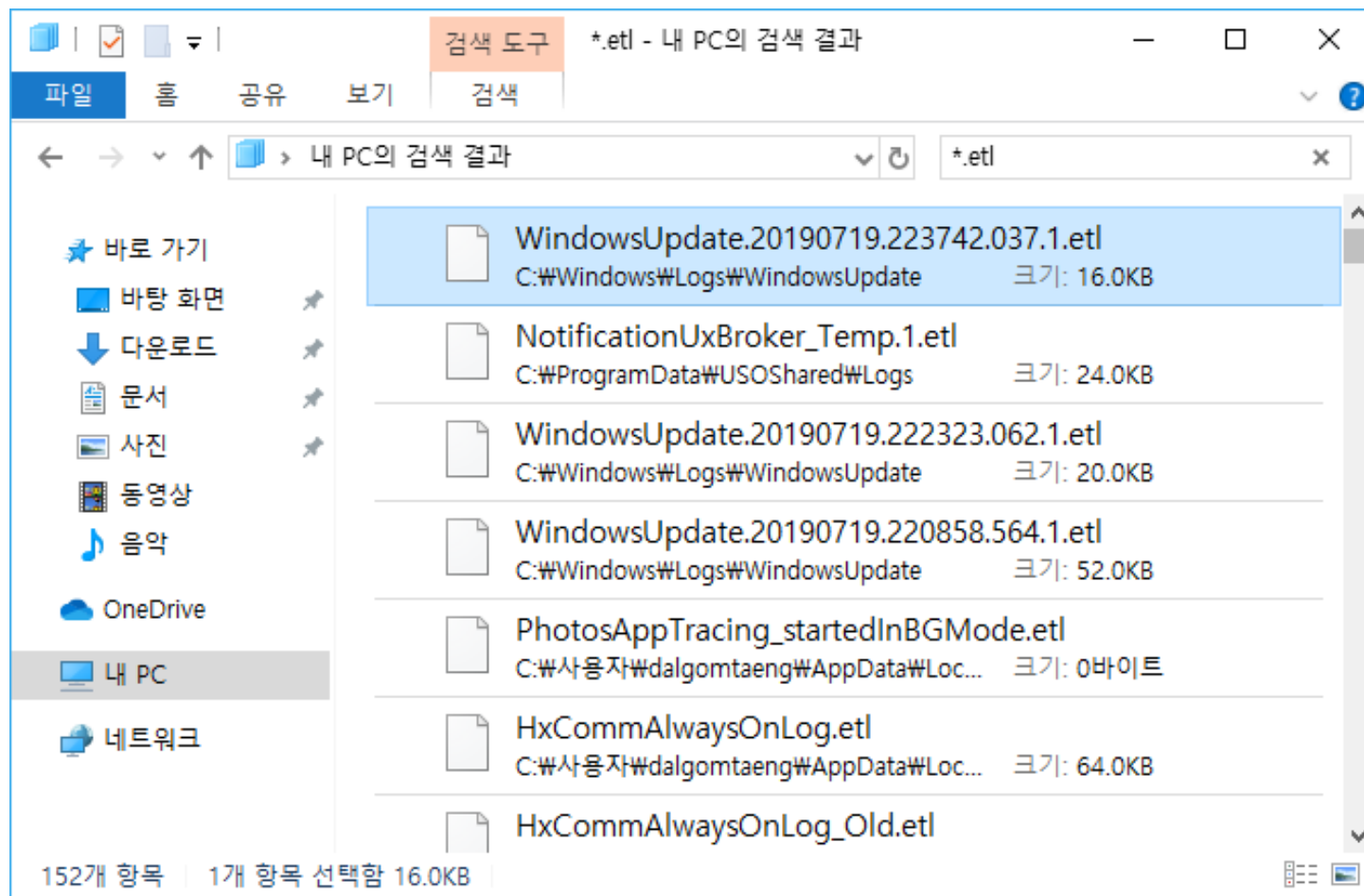
Windows Event Trace Logs

Dalgomtaeng

dalgomtaeng@gmail.com









- 디스크에 저장되는 윈도우용 이벤트 추적(ETW) 세션
 - ETW는 윈도우2000부터 도입
- ETL 확장자
- EVT/EVTX랑 비슷한 구조
- 윈도우 시스템의 다양한 위치에서 찾을 수 있음
- 시스템마다 존재하는 ETL이 다를 수 있음



- **윈도우 성능, 디버깅, 트러블슈팅**
 - 시스템 부팅과 종료시의 커널 작업
 - 전력 진단 및 슬립모드 학습
- **개발자 디버깅**
 - 응용프로그램이 실행하는 동안, 어떤 지점의 어떤 문제든 추적이 가능
 - 스택과 콜
 - 단순한 어플리케이션 크래시가 아니라 개발자가 원하는 것이면 어떤 것이든 모니터 가능
- **관리 작업**
 - 시스템에 대한 이벤트 추적을 수동으로 실행하고 나중에 검토 할 수 있도록 디스크에 저장

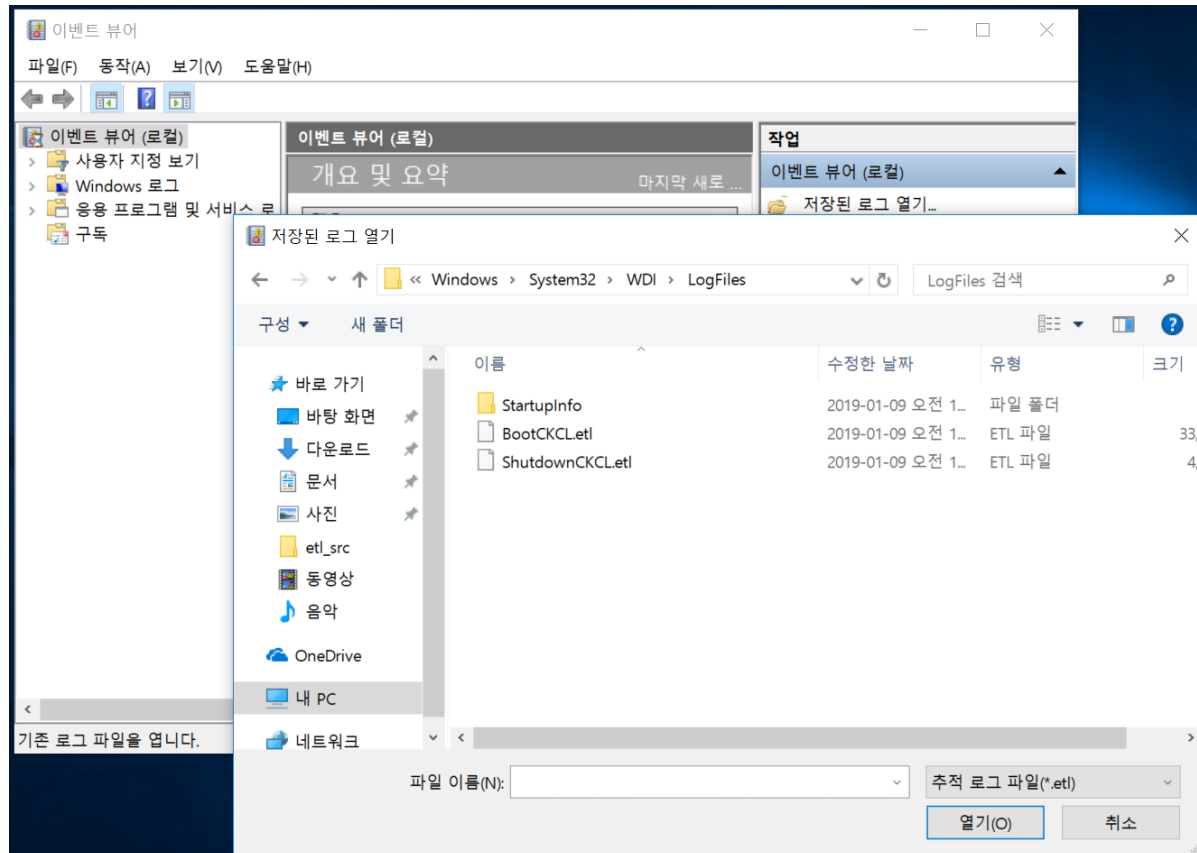


- 코타나 검색부터 WiFi SSID까지 여러 종류의 정보를 가지고 있음
- 헤더 데이터
 - 세션 정보
- 이벤트 데이터
 - 타임스탬프
 - 제공자와 이벤트명
 - 프로세스 및 스레드 ID
 - 등급 및 작업
 - 페이로드



- 윈도우 이벤트 뷰어
- Microsoft Message Analyzer
- 윈도우 SDK 도구들
- ETL Viewer & Parser
- tela
- C#에서 TraceEvent를 Python에서 PyETW 라이브러리 사용 가능
- 모든 도구는 다른 시스템에서 ETL을 복호화하고 파싱하는 것에는 한계가 있음

- "저장된 로그 열기"를 이용하여 열수 있음
 - 기본 데이터는 잘 보임
 - 현재 시스템에 있던 ETL이 아닐 경우, 몇몇 데이터가 잘못 표기됨
 - 페이로드를 늘 해독할 수 있는 건 아님





ShutdownCKCL
이벤트 수: 25,794

수준	날짜 및 시간	원본	이벤트 ...	작업 범...
정보	2019-01-09 오전 9:52:24		0	없음
정보	2019-01-09 오전 9:52:24		0	없음
정보	2019-01-09 오전 9:52:24		0	없음
정보	2019-01-09 오전 9:52:24		0	없음
정보	2019-01-09 오전 9:52:24		0	없음
정보	2019-01-09 오전 9:52:24		0	없음
정보	2019-01-09 오전 9:52:24		0	없음
정보	2019-01-09 오전 9:52:24		0	없음
정보	2019-01-09 오전 9:52:24		0	없음
정보	2019-01-09 오전 9:52:24		0	없음
정보	2019-01-09 오전 9:52:24		0	없음
정보	2019-01-09 오전 9:52:24		0	없음
정보	2019-01-09 오전 9:52:24		0	없음
정보	2019-01-09 오전 9:52:24		0	없음
정보	2019-01-09 오전 9:52:24		0	없음
정보	2019-01-09 오전 9:52:24		0	없음

이벤트 0,

일반

자세히

로그 이름(M):

원본(S):

이벤트 ID(E):

수준(L):

로그된 날짜(D): 2019-01-09 오전 9:52:24

작업 범주(Y): 없음

키워드(K): 없음



- Microsoft 에서 무료로 다운로드 및 설정이 가능
- 이벤트 데이터를 해독하는데 매우 강력함
- 사용이 어려움
- 보고서를 설정하고 출력가능함
- 이벤트 뷰어에 비해서 많은 데이터를 제공함
- 하지만 모든 이벤트를 파싱하지는 못함



Microsoft Message Analyzer

File Session Tools Help

New Session Favorite Scenarios Open Save New Viewer Edit Session Shift Time Aliases New Union Window Layout

Modules Loaded Errors or warnings were found when loading modules. [Show Log](#)

Start Page 1 : ShutdownCK...

Add Filter Viewpoints Flat Message List Add Columns Color Rules Find Message Go To Message Layout Find In Grouping Viewer Export

Remove Apply Enter a filter expression, such as:
tcp.port==80
*address==192.168.1.1

Library History

Right click on any column header and select 'Group' to create a grouping.

MessageNumber	Timestamp	TimeDelta	EventRec	EventRecor	Module	Summary
4	2019-01-09T09...	1,519,363.463...	429496...	4294967...	Windows_Kernel_Trace	Header_Extension_TypeGroup{GroupMask1=0,GroupMask2=0,GroupMask3=0,GroupMask
5	2019-01-09T09...	0.0000496	429496...	4294967...	Windows_Kernel_Trace	Header_Extension_TypeGroup{GroupMask1=7,GroupMask2=0,GroupMask3=0,GroupMask
6	2019-01-09T09...	0.0000025	429496...	4294967...	Windows_Kernel_Trace	Process_V4_TypeGroup1{UniqueProcessKey=EtwPointer{pointerValue=184467352792
7	2019-01-09T09...	0.0000009	0	0	Windows_Kernel_Trace	Thread_V3_TypeGroup1{ProcessId=0,TThreadId=0,StackBase=EtwPointer{pointerVa
8	2019-01-09T09...	0.0000004	0	0	Windows_Kernel_Trace	Thread_V3_TypeGroup1{ProcessId=0,TThreadId=0,StackBase=EtwPointer{pointerVa
9	2019-01-09T09...	0.0000000	0	0	Windows_Kernel_Trace	Thread_V3_TypeGroup1{ProcessId=0,TThreadId=0,StackBase=EtwPointer{pointerVa

Message Stack 1

1 Origin

6 : Windows_Kernel_Trace
Process_V4_TypeGroup1{UniqueProcessKey=EtwPointer{pointerValue=18446735279256979904},ProcessId=0,TThreadId=0,StackBase=EtwPointer{pointerValue=18446735279256979904}}

6 : Etw
{3d6fa8d0-fe05-11d0-9dda-00c04fd7ba7c}, EventID: 0, ProcessID: 0

Details 1

Enter search text here..

Name	Value	Bit Offset	Bit Length
UniqueProcessKey	EtwPointer{pointerValue=18446735279256979904}	0	64
ProcessId	0 (0x00000000)	64	32
ParentId	0 (0x00000000)	96	32
SessionId	4294967295 (0xFFFFFFFF)	128	32
ExitStatus	0 (0x00000000)	160	32
DirectoryTableBase	EtwPointer{pointerValue=1757184}	192	64
Flags	0 (0x00000000)	256	32
UserId_blob	.j)..ÿÿ.....	288	128

Field Data

Field Data Message Data 1

Session Explorer

6: Process_V4_TypeGroup1{UniqueProcessKey=EtwPointer{pointerValue=18446735279256979904},ProcessId=0,TThreadId=0,StackBase=EtwPointer{pointerValue=18446735279256979904}}

Ready Session Total: 25,795 Available: 25,795 Selected: 1 Viewpoint: Default Truncated Session: False Parsing Level: Default Build: 4.0.8112.0



- 단순한 유저인터페이스
- 이벤트 명으로 분류
- 모든 페이로드를 파싱하지는 못함
- 대신 사람이 읽기 쉽게 덤프



ETL Viewer

File

Select Parser

☒ Dynamic/Kernel
 ☐ AllEvents

Get Header Stats

Search

Go

Clear

Event Names

Process/DCStart

Thread/DCStart

Image/DCStart

Event Trace/RundownCompl

Thread/Start

Thread/CompCS

Thread/Stop

Image/Unload

DiskIO/Read

DiskIO/FlushBuffers

DiskIO/Write

FileIO/FileCreate

Image/Load

Process/Start

Process/Stop

FileIO/FileDelete

Thread/DCStop

Process/DCStop

Image/DCStop

Process/Defunct

FileIO/FileRundown

Event Trace Report

Process/Defunct number of events: 12

	ProcessID	ParentID	ImageFileName	PageDirectoryBase	Flags	SessionID	ExitStatus	UniqueProcessKey	CommandLine
▶	696	412	smss.exe	Null	Protected	1	0x00000000	0xFFFFA58C26376580	
	4,520	3,796	cmd.exe	Null	None	0	0x00000000	0xFFFFA58C27583080	
	696	412	smss.exe	Null	Protected	1	0x00000000	0xFFFFA58C26376580	
	4,520	3,796	cmd.exe	Null	None	0	0x00000000	0xFFFFA58C27583080	
	6,820	3,796	cmd.exe	Null	None	0	0x00000000	0xFFFFA58C2820B080	
	7,340	864	userinit.exe	Null	None	1	0x00000000	0xFFFFA58C2867F080	
	8,296	3,796	cmd.exe	Null	None	0	0x00000000	0xFFFFA58C28D08580	
	10,860	3,796	cmd.exe	Null	None	0	0x00000000	0xFFFFA58C2926F080	
	11,176	10,852	HPNetworkCommunicator.exe	Null	None	1	0x00000000	0xFFFFA58C287B84C0	
	2,744	10,852	HPNetworkCommunicator.exe	Null	None	1	0x00000000	0xFFFFA58C2932F580	
	5,492	3,796	cmd.exe	Null	None	0	0x00000000	0xFFFFA58C29365080	
	808	3,796	cmd.exe	Null	None	0	0x00000000	0xFFFFA58C29478080	

```

C:\Users\dalgomtaeng\Downloads>ETLParser.exe -c test -s etl_src -o etl_dst
ETL Parser v0.3, Runtime: 01/09/2019 01:59:15 UTC
=====
Parsing files.....
[BEGIN_PARSE] 01/09/2019 01:59:15 UTC File 1 of 5. Started parsing BootCKCL.etl.
                    
```

File Loaded: E:\06-Presentations\2018\SansDFIR\Tools and Examples\ETLs\20180528-23-00_Asus_Laptop\BootCKCL.etl



- **C:\Windows\System32\WDI\LogFiles**
 - BootCKCL.etl
 - ShutdownCKCL.etl
 - SecondaryLogOnCKCL.etl
 - WdiContext.etl.<###>
- **C:\Windows\System32\WDI<GUID>\<GUID>**
 - snapshot.etl
- **C:\Windows\System32\LogFiles\WMI**
 - Wifi.etl
 - LwNetLog.etl
- **C:\Windows\System32\SleepStudy**
 - UserNotPresentSession.etl
 - abnormal-shutdown-<YYYY>-<MM>-<DD>-<HH>-<MM>-<SS>.etl
 - user-not-present-trace-<YYYY>-<MM>-<DD>-<HH>-<MM>-<SS>.etl
 - ScreenOnPowerStudyTraceSession-<YYYY>-<MM>-<DD>-<HH>-<MM>-<SS>.etl



- C:\Windows\System32\WDI\LogFiles\BootCKCL.etl
- 시스템 부팅 때마다 덮어쓰여짐
- 부팅 과정 동안의 커널 이벤트를 기록함
 - Processes
 - Threads
 - DiskIO
 - FileIO
 - Image loading (DLLs, EXEs, ..)
- 포렌식 관점에서 볼만한 것들
 - 최근 부팅시에 실행된 프로세스
 - 연속성 매커니즘
 - 악성 도구
 - 부팅시나 사용자 로그인시에 동작하게 설정된 스케줄 작업
 - 모든 드라이브에 연결된 파일 핸들
 - 특정 프로세스에 의해 로드된 DLL
 - 명령어 실행



Microsoft Message Analyzer

File Session Tools Help

New Session Favorite Scenarios Open Save New Viewer Edit Session Shift Time Aliases New Union Window Layout

Modules Loaded Errors or warnings were found when loading modules. Show Log

Start Page 1 : BootCKCL : A... 1 : ShutdownCK... 1 : Wifi : Analysi... 1 : LwtNetLog ... 1 : Session 8 : A... 1 : Session 9 : A... 1 : Session 10 ...

Add Filter Viewpoints Flat Message List Add Columns Color Rules Find Message Go To Message Layout Find In Grouping Viewer Export

Remove Apply Windows_Kernel_Trace.FileName == "*.pfi" Library History

Right click on any column header and select 'Group' to create a grouping.

MessageNumber	Timestamp	TimeDelta	EventRec	EventReco	Module	Summary
117410	2019-01-09T11...	-2.8699862	5512	6996	Windows_Kernel_Trace	Process_V4_TypeGroup1{UniqueProcessKey=EtwPointer{pointerValue=1844662482220820608},Proc...

Message Stack 1 1 Origin

117410 : Windows_Kernel_Trace
Process_V4_TypeGroup1(UniqueProcessKey=EtwPointer{pointerValue=1844662482220820608},Proc...

117410 : Etw
{3d6fa8d0-fe05-11d0-9dda-00c04fd7ba7c}, EventID: 0, ProcessID:

Details 1

Name	Value	Bit Offset	Bit Length	Type
UniqueProcessKey	EtwPointer{pointerValue=184466248222...	0	64	E...
ProcessId	10744 (0x000029F8)	64	32	U...
ParentId	5512 (0x00001588)	96	32	U...
SessionId	0 (0x00000000)	128	32	U...
ExitStatus	259 (0x00000103)	160	32	I...
DirectoryTableBase	EtwPointer{pointerValue=8037728256}	192	64	E...
Flags	4 (0x00000004)	256	32	U...
UserId_blob	0cY..0jy.....	288	128	B...
UserId	S-1-5-18 LocalSystem -- An account th...	416	96	D...
ImageFileName	mscorsvw.exe	512	104	S...
CommandLine	C:\Windows\Microsoft.NET\Framework64\...	616	2480	S...
PackageFullName		3096	16	S...
ApplicationId		3112	16	S...

Field Data

C:\Windows\Microsoft.NET\Framework64\Wv4.0.30319
Wmcsorsvw.exe -StartupEvent 1d4 -InterruptEvent 0 -
NGENProcess 204 -Pipe 1e4 -Comment "NGen Worker
Process"

No alternate presentation available.

Field Data Message Data 1

Session Explorer

117410: Process_V4_TypeGroup1(UniqueProcessKey=EtwPointer{pointerValue=1844662482220820608}

Ready Session Total: 186,614 Available: 186,614 Selected: 1 Viewpoint: Default Truncated Session: False Parsing Level: Default Build: 4.0.8112.0



Timeline Explorer v0.8.11.0

File
Tools
Help

f-insight_Parsed_ETL.csv
f-insight_Parsed_ETL.csv x

Find

.pf

1 of 500
First scrollable column
Select a column to pin

Power filter
"Event Name":FileIo

Drag a column header here to group by that column

Index	Payload
186346	'FileObject: 18446693515924693344', 'FileName: \Device\HarddiskVolume4\Windows\Prefetch\NGEN.EXE-383F81D5.pf'
186345	'FileObject: 18446693515924628192', 'FileName: \Device\HarddiskVolume4\Windows\System32\config\systemprofile\AppData\Local\Microso
186344	'FileObject: 18446693515924695040', 'FileName: \Device\HarddiskVolume4\Windows\System32\config\systemprofile\AppData\Local\Microso
186343	'FileObject: 18446693515924705632', 'FileName: \Device\HarddiskVolume4\Windows\System32\config\systemprofile\AppData\Local\Microso
186342	'FileObject: 18446693515851006304', 'FileName: \Device\HarddiskVolume4\Windows\System32\config\systemprofile\AppData\Local\Packag
186341	'FileObject: 18446693515930311472', 'FileName: \Device\HarddiskVolume4\Windows\ServiceProfiles\LocalService\AppData\Local\Package
186340	'FileObject: 18446693515924626432', 'FileName: \Device\HarddiskVolume4\Users\dalgomtaeng\AppData\Local\Microsoft\CLR_v4.0\UsageLo
186339	'FileObject: 18446693515924707760', 'FileName: \Device\HarddiskVolume4\Users\dalgomtaeng\AppData\Local\Microsoft\CLR_v4.0\UsageLo
186338	'FileObject: 18446693515924709728', 'FileName: \Device\HarddiskVolume4\Users\dalgomtaeng\AppData\Local\Microsoft\CLR_v4.0\UsageLo
186337	'FileObject: 18446693515924424256', 'FileName: \Device\HarddiskVolume4\Users\dalgomtaeng\AppData\Local\Microsoft\CLR_v4.0\UsageLo
186336	'FileObject: 18446693515924711408', 'FileName: \Device\HarddiskVolume4\Users\dalgomtaeng\AppData\Local\Microsoft\CLR_v4.0\UsageLo
186335	'FileObject: 18446693515924487168', 'FileName: \Device\HarddiskVolume4\Users\dalgomtaeng\AppData\Local\Microsoft\CLR_v4.0\UsageLo
186334	'FileObject: 18446693515930716976', 'FileName: \Device\HarddiskVolume4\Users\dalgomtaeng\AppData\Local\Microsoft\CLR_v4.0\UsageLo
186333	'FileObject: 18446693515893569968', 'FileName: \Device\HarddiskVolume4\Users\dalgomtaeng\AppData\Local\Packages\windows_ie_ac_001
186332	'FileObject: 18446693515929047392', 'FileName: \Device\HarddiskVolume4\Users\dalgomtaeng\AppData\Local\Packages\Windows.PrintDial
186331	'FileObject: 18446693515928416608', 'FileName: \Device\HarddiskVolume4\Users\dalgomtaeng\AppData\Local\Packages\Windows.PrintDial
186330	'FileObject: 18446693515901281704', 'FileName: \Device\HarddiskVolume4\Users\dalgomtaeng\AppData\Local\Packages\Windows.immersive

C:\Users\dalgomtaeng\Downloads\etl_dst\f-insight_Parsed_ETL.csv
Total lines 255,637
Visible lines 20,414



- **C:\Windows\System32\WDI\LogFiles\ShutdownCKCL.etl**
- **시스템이 종료될 때마다 덮어쓰여짐**
- **시스템 종료 과정 동안의 커널 이벤트를 기록함**
 - 실행 중인 프로세스
 - 실행 중인 스레드
 - 로드된 이미지 (DLLs, EXEs, ..)
- **포렌식 관점에서 볼만한 것들**
 - 시스템이 최근에 종료될때 실행 중인 프로세스
 - 악성 도구
 - 특정 프로세스에 의해 로드된 DLL
 - 명령어 실행



Microsoft Message Analyzer

File Session Tools Help

New Session Favorite Scenarios Open Save New Viewer Edit Session Shift Time Aliases New Union Window Layout

Modules Loaded Errors or warnings were found when loading modules. [Show Log](#)

Start Page 1 : BootCKCL : A... 1 : ShutdownCK... 1 : Wifi : Analy... 1 : LwtNetLog ... 1 : Session 8 : A... 1 : Session 9 : A... 1 : Session 10 : ...

Add Filter Viewpoints Flat Message List Add Columns Color Rules Find Message Go To Message Layout Find In Grouping Viewer Export

Remove Apply Enter a filter expression, such as:
tcp.port==80
*address==192.168.1.1

Library History

Right click on any column header and select 'Group' to create a grouping.

MessageNumber	Timestamp	TimeDelta	EventRec	EventReco	Module	Summary
13733	2019-01-09T09...	-38.5611356	9076	8524	Windows_Kernel_Trace	Process_V4_TypeGroup1{UniqueProcessKey=EtwPointer{pointerValue=184466110404...

Message Stack 1

1 Origin

13733 : Windows_Kernel_Trace
Process_V4_TypeGroup1{UniqueProcessKey=EtwPointer{pointerValue=184466110404...

13733 : Etw
{3d6fa8d0-fe05-11d0-9dda-00c04fd7ba7c}, EventID: 0, ProcessID:

Details 1

Enter search text here..

Name	Value	Bit Offset	Bit Length
UniqueProcessKey	EtwPointer{pointerValue=1844661104040...	0	64
ProcessId	9076 (0x00002374)	64	32
ParentId	3228 (0x00000C9C)	96	32
SessionId	4 (0x00000004)	128	32
ExitStatus	1073807364 (0x40010004)	160	32
DirectoryTableBase	EtwPointer{pointerValue=5281153024}	192	64
Flags	0 (0x00000000)	256	32
UserId_blob	,3±. ``ÿÿ..... ``ÿÿ	288	128
UserId	S-1-5-21-2500850884-2914895277-988649...	416	224
ImageFileName	mmc.exe	640	64
CommandLine	"C:\Windows\system32\mmc.exe" "C:\Win...	704	1088
PackageFullName		1792	16
ApplicationId		1808	16

Field Data

Field Data Message Data 1

Session Explorer

Ready Session Total: 25,795 Available: 25,795 Selected: 1 Viewpoint: Default Truncated Session: False Parsing Level: Default Build: 4.0.8112.0



Microsoft Message Analyzer

File Session Tools Help

New Session Favorite Scenarios Open Save New Viewer Edit Session Shift Time Aliases New Union Window Layout

Modules Loaded Errors or warnings were found when loading modules. [Show Log](#)

Start Page 1 : BootCKCL : A... 1 : ShutdownCK... 1 : Wifi : Analy... 1 : LwtNetLog ... 1 : Session 8 : A... 1 : Session 9 : A... 1 : Session 10 ...

Add Filter Viewpoints Flat Message List Add Columns Color Rules Find Message Go To Message Layout Find In Grouping Viewer Export

Remove Apply Enter a filter expression, such as:
tcp.port==80
*address==192.168.1.1

Library History

Right click on any column header and select 'Group' to create a grouping.

MessageNumber	Timestamp	TimeDelta	EventRec	EventReco	Module	Summary
7547	2019-01-09T09...	-0.0004345	4228	3736	Windows_Kernel_Trace	Image_Load{ImageBase=EtwPointer{pointerValue=10420224},ImageSize=EtwPointer

Message Stack 1

1 Origin

7547 : Windows_Kernel_Trace
Image_Load{ImageBase=EtwPointer{pointerValue=10420224},ImageSize=EtwPointer

7547 : Etw
{2cb15d1d-5fc1-11d2-abe1-00a0c911f518}, EventID: 0, ProcessID

Details 1

Enter search text here..

Name	Value	Bit Offset	Bit Length
ProcessId	4228 (0x00001084)	128	32
ImageChecksum	1705223 (0x001A0507)	160	32
TimeDateStamp	1536561426 (0x5B961112)	192	32
SignatureLevel	0 (0x00)	224	8
SignatureType	0 (0x00)	232	8
Reserved0	0 (0x0000)	240	16
DefaultBase	EtwPointer{pointerValue=4475452129817...	256	64
Reserved1	0 (0x00000000)	320	32
Reserved2	0 (0x00000000)	352	32
Reserved3	0 (0x00000000)	384	32
Reserved4	0 (0x00000000)	416	32
FileName	\\Device\\HarddiskVolume4\\Program Files...	448	1312

Field Data

\\Device\\HarddiskVolume4\\Program Files (x86)\\V...
\\VPWalletService\\VPWalletDaemon.exe

No alternate presentation available.

Field Data Message Data 1

Session Explorer

Ready Session Total: 25,795 Available: 25,795 Selected: 1 Viewpoint: Default Truncated Session: False Parsing Level: Default Build: 4.0.8112.0



- **C:\Windows\System32\LogFiles\WMI\Wfi.etl**
- **WiFi 네트워크 관련 이벤트:**
 - WiFi 설정
 - 자동설정 정보
- **포렌식 관점에서 볼만한 것들**
 - 근처 네트워크 SSID
 - WiFi 설정
 - MAC 주소
 - Network 상태 변경
 - 더 많은 데이터가 있음



Microsoft Message Analyzer

File Session Tools Help

New Session Favorite Scenarios Open Save New Viewer Edit Session Shift Time Aliases New Union Window Layout

Modules Loaded Errors or warnings were found when loading modules. Show Log

Start Page 1 : BootCKCL : A... 1 : ShutdownCK... 1 : Wifi : Analy... 1 : LwtNetLog ... 1 : Session 8 : A... 1 : Session 9 : A... 1 : Session 10 : ...

Add Filter Viewpoints Flat Message List Add Columns Color Rules Find Message Go To Message Layout Find In Grouping Viewer Export

Remove Apply Enter a filter expression, such as:
tcp.port==80
*address==192.168.1.1

Library History

Right click on any column header and select 'Group' to create a grouping.

Timestamp	TimeDelta	EventRec	EventReco	Module	Summary
2019-01-09T11...	0.0000201	3364	4580	Microsoft_Windows_WLAN_AutoConfig	무선 네트워크 연결이 성공했습니다.
2019-01-09T11...	0.0000081	3364	4580	Microsoft_Windows_WLAN_AutoConfig	무선 보안을 시작했습니다.

Message Stack 1 1 Origin

256 : Microsoft_Windows_WLAN_AutoConfig
무선 보안을 시작했습니다.

256 : Etw
(9580d7dd-0379-4658-9870-d5be7d52d6de), EventID: 11010, Pro...

Details 1

Name	Value	Bit Offset	Bit Length
Adapter	Intel(R) Dual Band Wireless-AC 7260	0	576
DeviceGuid	25e27744-19bb-4d7d-ba91-50a7113d4805	576	128
LocalMac	28:B2:BD:26:C4:74	704	288
SSID	SweetHome5G	992	192
BSSType	Infrastructure	1184	240
Auth	WPA2-Personal	1424	224
AuthVal	7 (0x00000007)	1648	32
Cipher	AES-CCMP	1680	144
CipherVal	4 (0x00000004)	1824	32
FIPSMODE	Disabled (0x00000000)	1856	32
GroupEnabled	No (0x00000000)	1888	32

256: 무선 보안을 시작했습니다.

Field Data

Field Data Message Data 1

Session Explorer

Ready Session Total: 9,653 Available: 9,653 Selected: 1 Viewpoint: Default Truncated Session: False Parsing Level: Default Build: 4.0.8112.0



- **C:\ProgramData\Microsoft\Windows\Power Efficiency Diagnostics\energy-ntkl.etl**
- **전력 진단**
 - 시스템 설정
 - 논리 드라이브
 - 물리 드라이브
 - NIC
 - 프로세스 및 스레드
 - 서비스
 - 기타 등등
- **포렌식 관점에서 볼만한 것들**
 - 내부 및 외부 드라이브에 대한 상세 정보
 - 실행 중인 서비스
 - 프로세스



ETL Viewer

File

Select Parser

☒ Dynamic/Kernel
 ☐ AllEvents

Get Header Stats

Search

Go

Clear

Event Names

GenericReportofAllEvents
 Event Trace/Extension
 Process/DCStart
 Thread/DCStart
 Image/DCStart
 PerfInfo/Sample
 PerfInfo/CollectionStart
 Thread/Start
 Thread/Stop
 Image/Unload
 Image/Load
 SystemConfig/CPU
 SystemConfig/Video
SystemConfig/PhyDisk
 SystemConfig/LogDisk
 SystemConfig/NIC
 SystemConfig/Services
 SystemConfig/Power
 SystemConfig/PnP
 SystemConfig/IRQ
 Thread/DCStop
 Process/DCStop
 Image/DCStop

Event Trace Report

SystemConfig/PhyDisk number of events: 14

	DiskNumber	BytesPerSector	SectorsPerTrack	TracksPerCylinder	Cylinders	Manufacturer	SCSIPort	SCSIP
	2	512	63	255	31,130	LITEON L8H-256V2G-11 M. SCSI Disk Device	0	4
	1	512	63	255	243,201	TOSHIB DT01ACA200 SCSI Disk Device	0	3
	0	512	63	255	243,201	WD WD20EZR-00D8PB0 SCSI Disk Device	0	0
	3	512	63	255	60,801	WD WD5000AZLX-00ZR6 SCSI Disk Device	0	5
	10	512	63	255	7,531	USB Device	0	0
	4	512	63	255	1,885	Patriot Memory USB Device	0	0
	5	0	0	0	0	Generic- Compact Flash	0	0
	7	0	0	0	0	Generic- MS/MS-PRO	0	0
	6	0	0	0	0	Generic- SD/MMC	0	0
	8	0	0	0	0	Generic- xD-Picture	0	0
	13	512	63	255	486,401	Seagate BUP BL USB Device	0	0
	11	512	63	255	486,397	WD My Passport 25E2 USB Device	0	0
	12	512	63	255	364,797	WD My Passport 25EA USB Device	0	0
	9	512	63	255	243,197	WD My Passport 25EA USB Device	0	0

File Loaded: E:\06-Presentations\2018\SansDFIR\Tools and Examples\ETLs\energy-ntkl.etl



ETL Viewer

File

Select Parser

☒ Dynamic/Kernel
 ☐ AllEvents

Get Header Stats

Search

Go

Clear

Event Names

GenericReportofAllEvents
 EventTrace/Extension
 Process/DCStart
 Thread/DCStart
 Image/DCStart
 PerfInfo/Sample
 PerfInfo/CollectionStart
 Thread/Start
 Thread/Stop
 Image/Unload
 Image/Load
 SystemConfig/CPU
 SystemConfig/Video
 SystemConfig/PhyDisk
SystemConfig/LogDisk
 SystemConfig/NIC
 SystemConfig/Services
 SystemConfig/Power
 SystemConfig/PnP
 SystemConfig/IRQ
 Thread/DCStop
 Process/DCStop
 Image/DCStop

Event Trace Report

SystemConfig/LogDisk number of events: 8

	StartOffset	PartitionSize	Disk Number	Size	Drive Type	DriveLetterString	PartitionNumber	SectorsPerCluster	BytesPerSector	
	12,639,535,104	243,419,578,368	2	112	1	C:	3	8	512	5
	1,048,576	2,000,396,746,752	1	112	1	D:	1	8	512	6
	1,048,576	2,000,396,746,752	0	112	1	F:	1	8	512	2
	1,048,576	500,104,691,712	3	112	1	G:	1	8	512	4
	1,048,576	2,000,363,192,320	9	112	1	H:	1	8	512	4
▶	1,048,576	4,000,750,501,888	11	112	1	M:	1	8	512	4
	135,266,304	4,000,650,887,168	13	112	1	P:	2	8	512	3
	1,048,576	3,000,556,847,104	12			Q:			512	3

13

P:

SystemConfig/LogDisk

File Loaded: E:\06-Presentations\2018\SansDFIR\Tools and Examples\ETLs\energy-ntkl.etl



ETL Viewer

File

Select Parser

☒ Dynamic/Kernel
 ☐ AllEvents

Get Header Stats

Search

Go

Clear

Event Names

GenericReport of AllEvents
 Event Trace/Extension
 Process/DCStart
 Thread/DCStart
 Image/DCStart
 PerfInfo/Sample
 PerfInfo/CollectionStart
 Thread/Start
 Thread/Stop
 Image/Unload
 Image/Load
 SystemConfig/CPU
 SystemConfig/Video
 SystemConfig/PhyDisk
 SystemConfig/LogDisk
 SystemConfig/NIC
 SystemConfig/Services
 SystemConfig/Power
 SystemConfig/PnP
 SystemConfig/IRQ
 Thread/DCStop
 Process/DCStop
 Image/DCStop

Event Trace Report

SystemConfig/PnP number of events: 233

FriendlyName	DeviceID
	ROOT\COMPOSITEBUS\0000
	UMB\UMB\1&841921D&0&WPDBUSENUMROOT
	ROOT\LEGACY_RDPENCDD\0000
	STORAGE\VOLUME\{66342982-B89D-11E7-B994-005056C00008}\#00000000000100000
	ROOT\MS_NDISWANBH\0000
	ROOT\LEGACY_DXGKRNL\0000
	PCI\VEN_8086&DEV_191F&SUBSYS_06B81028&REV_07\3&11583659&0&00
	ROOT\LEGACY_NDPROXY\0000
	PCI\VEN_8086&DEV_A145&SUBSYS_06B81028&REV_31\3&11583659&0&F8
	ACPI\PNP0C02\PCHRESV
Seagate BUP BL USB Device	USBSTOR\DISK&VEN_SEAGATE&PROD_BUP_BL&REV_0108\NA9F0QEM&0
	STORAGE\VOLUME\{037C31A1-B9B8-11E5-BB62-806E6F6E6963}\#00000000000007E00
	ROOT\IMAGE\0000
	STORAGE\VOLUMESNAPSHOT\HARDDISKVOLUMESNAPSHOT16
L:\	WPDBUSENUMROOT\UMB\2&37C186B&0&STORAGE#VOLUME#\??_USBSTOR#DISK&VEN_GENERIC-&PROD_XD-PIC
	ROOT\LEGACY_VMNETBRIDGE\0000
WD My Passport 25E2 USB Device	USBSTOR\DISK&VEN_WD&PROD_MY_PASSPORT_25E2&REV_4004\5758343144423636354B3348&0
Intel(R) Core(TM) i7-6700K CPU @ 4.00GHz	ACPI\GENUINEINTEL_-_INTEL64_FAMILY_6_MODEL_94_-_INTEL(R)_CORE(TM)_I7-6700K_CPU_@_4.00GHZ_2
	ROOT\MS_NDISWANIP\0000
	ROOT\LEGACY_RDPREFMP\0000

File Loaded: E:\06-Presentations\2018\SansDFIR\Tools and Examples\ETLs\energy-ntkl.etl



⑩ C:\Windows\System32\WDI\LogFiles\

⑩ WdiContextLog.etl.###

⑩ 사용자 로그인과 관련된 정보

⑩ Run 키에서 등록된 프로그램 실행

⑩ Startup 폴더에 등록된 프로그램 실행



Timeline Explorer v0.8.11.0

File Tools Help

f-insight_Parsed_ETL.csv x f-insight_Parsed_ETL.csv

Find 0 of 0 First scrollable column

Power filter

Drag a column header here to group by that column

	Index	Timestamp	Event Name	Payload
	2450	2019-01-09 02:09:03.418782 UTC	Explorer_EnumeratingRunKeyStop/Stop	'KeyName: Software\Microsoft\Windows\CurrentVersion\Ru
	676	2019-01-08 23:59:32.696102 UTC	Explorer_ExecutingFromRunKeyStart/Start	'Command: MSASCuiL.exe'
	698	2019-01-08 23:59:33.297745 UTC	Explorer_ExecutingFromRunKeyStart/Start	'Command: OneDrive.exe" /background'
	2413	2019-01-09 02:09:00.844720 UTC	Explorer_ExecutingFromRunKeyStart/Start	'Command: MSASCuiL.exe'
	2427	2019-01-09 02:09:01.537129 UTC	Explorer_ExecutingFromRunKeyStart/Start	'Command: OneDrive.exe" /background'
	2447	2019-01-09 02:09:03.206625 UTC	Explorer_ExecutingFromRunKeyStart/Start	'Command: Taskmgr.exe '
	695	2019-01-08 23:59:33.297040 UTC	Explorer_ExecutingFromRunKeyStop/Stop	'PID: 2680', 'Command: MSASCuiL.exe'
	722	2019-01-08 23:59:34.786110 UTC	Explorer_ExecutingFromRunKeyStop/Stop	'PID: 8044', 'Command: OneDrive.exe" /background'
	2424	2019-01-09 02:09:01.536884 UTC	Explorer_ExecutingFromRunKeyStop/Stop	'PID: 10324', 'Command: MSASCuiL.exe'
	2438	2019-01-09 02:09:02.752042 UTC	Explorer_ExecutingFromRunKeyStop/Stop	'PID: 10496', 'Command: OneDrive.exe" /background'
	2449	2019-01-09 02:09:03.418777 UTC	Explorer_ExecutingFromRunKeyStop/Stop	'PID: 10944', 'Command: Taskmgr.exe '
	2441	2019-01-09 02:09:02.771680 UTC	Explorer_ExecutingFromStartupMenuStart/Sta...	'Command: C:\Windows\system32\notepad.exe'
	2443	2019-01-09 02:09:02.793135 UTC	Explorer_ExecutingFromStartupMenuStop/Stop	'Command: C:\Windows\system32\notepad.exe'
	402	2019-01-08 23:59:20.790409 UTC	Explorer_InitializingExplorerStart/Start	"PAYLOAD_DUMP: "
	2321	2019-01-09 02:08:48.065716 UTC	Explorer_InitializingExplorerStart/Start	"PAYLOAD_DUMP: "
	486	2019-01-08 23:59:22.686691 UTC	Explorer_InitializingExplorerStop/Stop	"PAYLOAD_DUMP: "
	2389	2019-01-09 02:08:50.831680 UTC	Explorer_InitializingExplorerStop/Stop	"PAYLOAD_DUMP: "

C:\Users\#dalgomtaeng#Downloads#etl_dst_#f-insight_Parsed_ETL.csv Total lines 31,961 Visible lines 31,961



- 80여개의 볼만한 다른 ETL 파일이 존재
- 몇몇은 헤더만 존재함
- 많은 종류의 정보를 포함하고 있음



- **로그 덮어쓰기**
 - 순환형
- **이벤트 데이터가 없는 로그**
 - 사이즈가 0인 ETL 파일
 - 카빙이 가능할지도?
- **타임스탬프와 세션**
 - 스냅샷 형태
- **해독 문제**
 - 이전 소프트웨어의 심볼과의 불일치
 - 새로운 소프트웨어 빌드 및 OS 업데이트
 - 제거된 심볼
- **너무 많은 데이터**



- **WINDOWS EVENT TRACE LOGS (SANS DFIR Summit 2018) - Nicole Ibrahim**
 - <https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1528388048.pdf>
- **ETW Event Tracing for Windows and ETL Files - Nicole Ibrahim**
 - <http://www.hecfblog.com/2018/06/etw-event-tracing-for-windows-and-etl.html>
- **Trace Event Log and Analysis (tela)**
 - https://tzworks.net/prototype_page.php?proto_id=40

