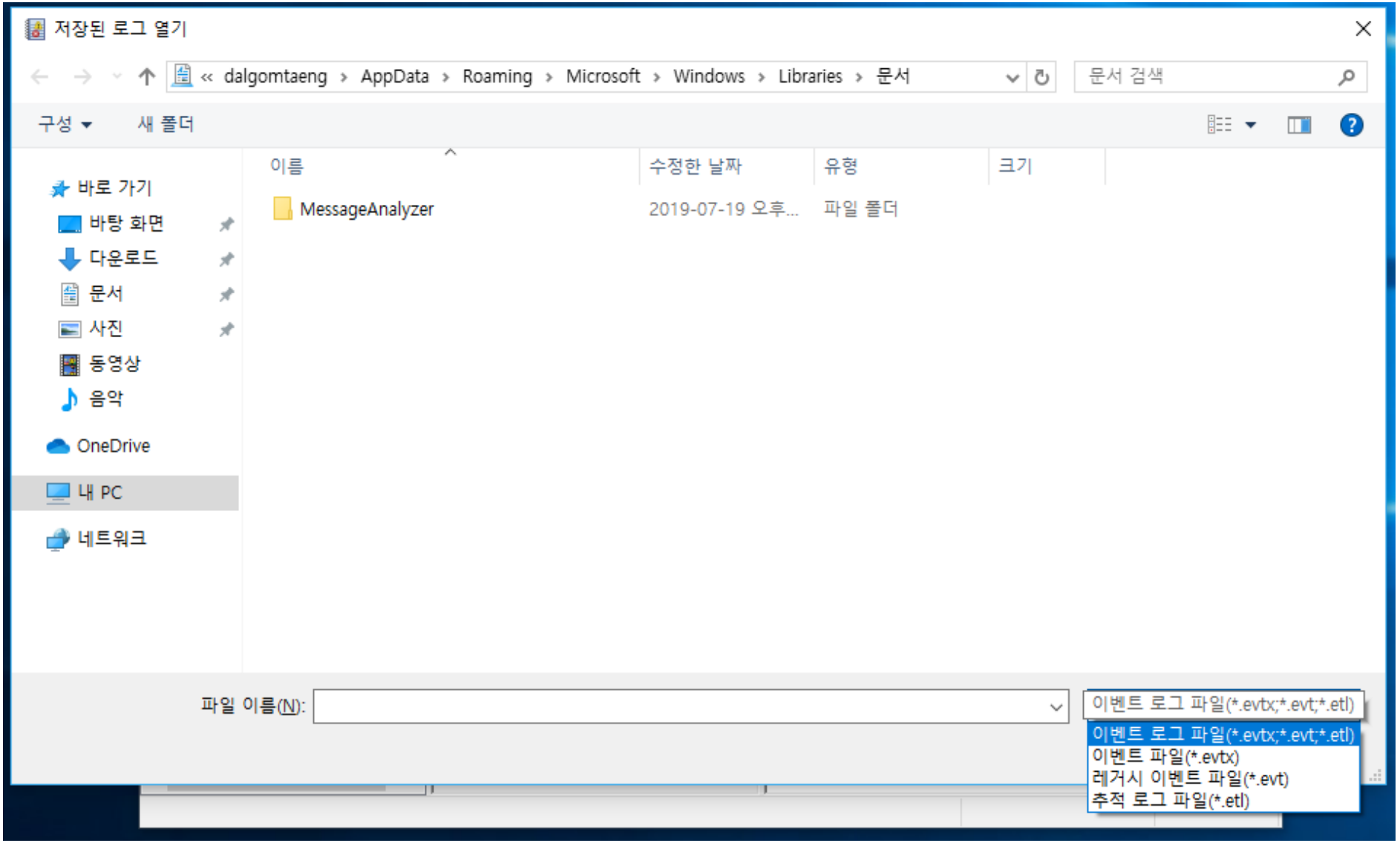
Windows Event Trace Logs

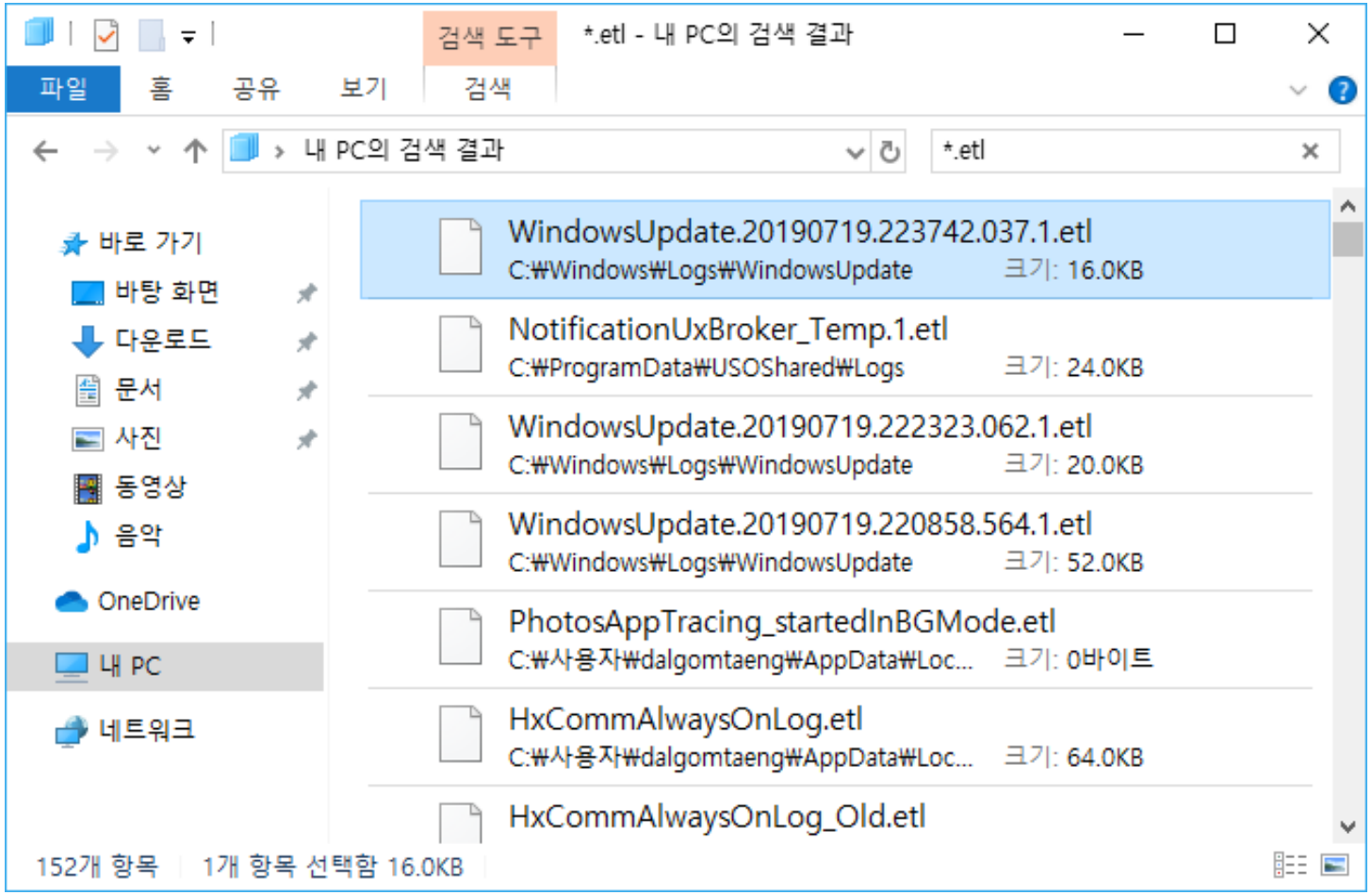
Dalgomtaeng

dalgomtaeng@gmail.com

What?


저장된 로그 열기
« dalgomtaeng › AppData › Roaming › Microsoft › Windows › Libraries › 문서
문서 검색
구성
새 폴더
바로 가기
바탕 화면
다운로드
문서
사진
동영상
음악
OneDrive
내 PC
네트워크
이름
수정한 날짜
유형
크기
MessageAnalyzer
2019-07-19 오후...
파일 폴더
파일 이름(N):
이벤트 로그 파일(*.evtx;*.evt;*.etl)
이벤트 로그 파일(*.evtx;*.evt;*.etl)
이벤트 파일(*.evtx)
레거시 이벤트 파일(*.evt)
추적 로그 파일(*.etl)

What?


검색 도구
*.etl - 내 PC의 검색 결과
파일
홈
공유
보기
검색
내 PC의 검색 결과
*.etl
바로 가기
바탕 화면
다운로드
문서
사진
동영상
음악
OneDrive
내 PC
네트워크
WindowsUpdate.20190719.223742.037.1.etl
C:₩Windows₩Logs₩WindowsUpdate 크기: 16.0KB
NotificationUxBroker_Temp.1.etl
C:₩ProgramData₩USOShared₩Logs 크기: 24.0KB
WindowsUpdate.20190719.222323.062.1.etl
C:₩Windows₩Logs₩WindowsUpdate 크기: 20.0KB
WindowsUpdate.20190719.220858.564.1.etl
C:₩Windows₩Logs₩WindowsUpdate 크기: 52.0KB
PhotosAppTracing_startedInBGMode.etl
C:₩사용자₩dalgomtaeng₩AppData₩Loc... 크기: 0바이트
HxCommAlwaysOnLog.etl
C:₩사용자₩dalgomtaeng₩AppData₩Loc... 크기: 64.0KB
HxCommAlwaysOnLog_Old.etl
152개 항목
1개 항목 선택함 16.0KB

Windows Event Trace Logs

- 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

왜 생기나?

- **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

어떤 정보를 가지고 있나?

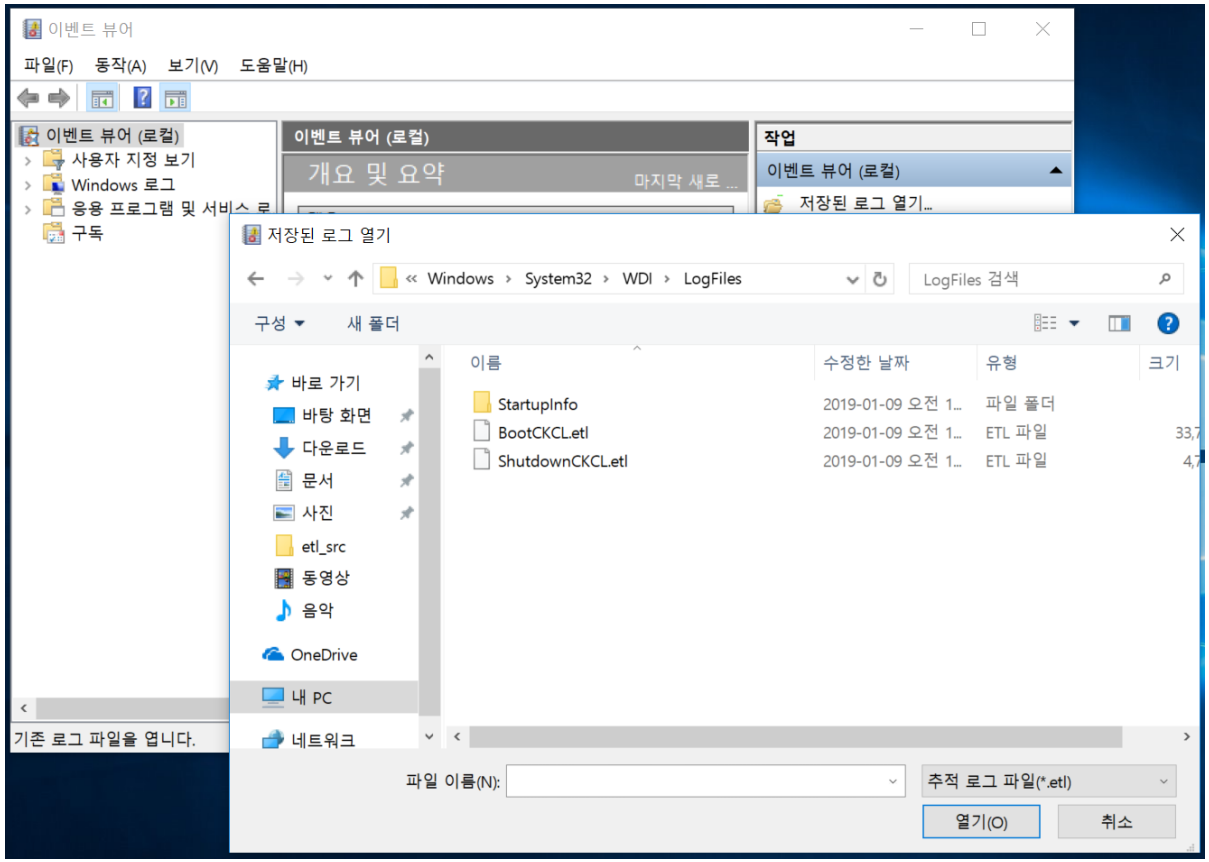
- **코타나 검색부터 WiFi SSID까지 여러 종류의 정보를 가지고 있음**
- **헤더 데이터**
  - 세션 정보
- **이벤트 데이터**
  - 타임스탬프
  - 제공자와 이벤트명
  - 프로세스 및 스레드 ID
  - 등급 및 작업
  - 페이로드

어떻게 내용을 볼 수 있나?

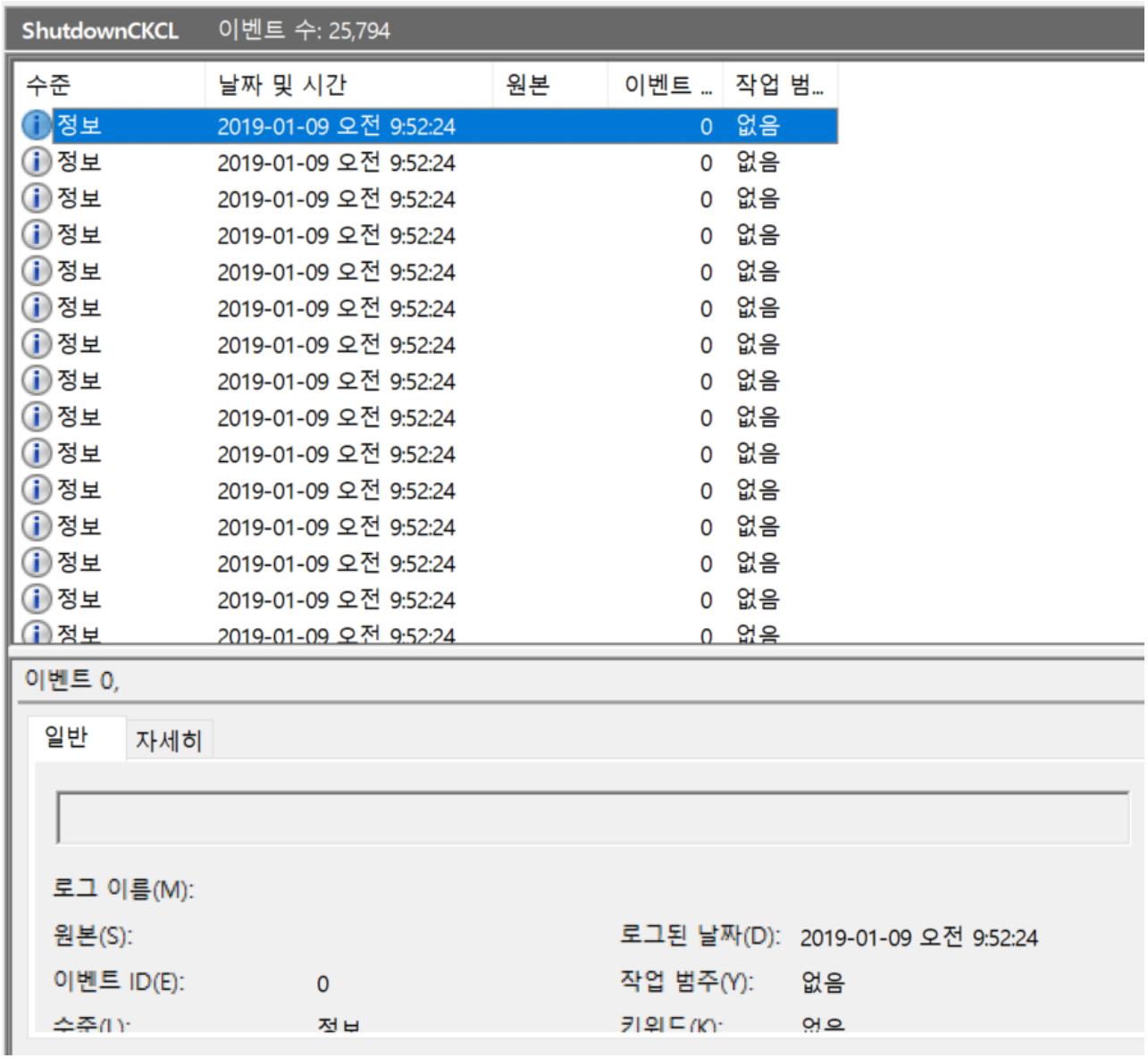
- 윈도우 이벤트 뷰어
- Microsoft Message Analyzer
- 윈도우 SDK 도구들
- ETL Viewer & Parser
- tela
- C#에서 TraceEvent를 Python에서 PyETW 라이브러리 사용 가능
- 모든 도구는 다른 시스템에서 ETL을 복호화하고 파싱하는 것에는 한계가 있음

윈도우 이벤트 뷰어

- **"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



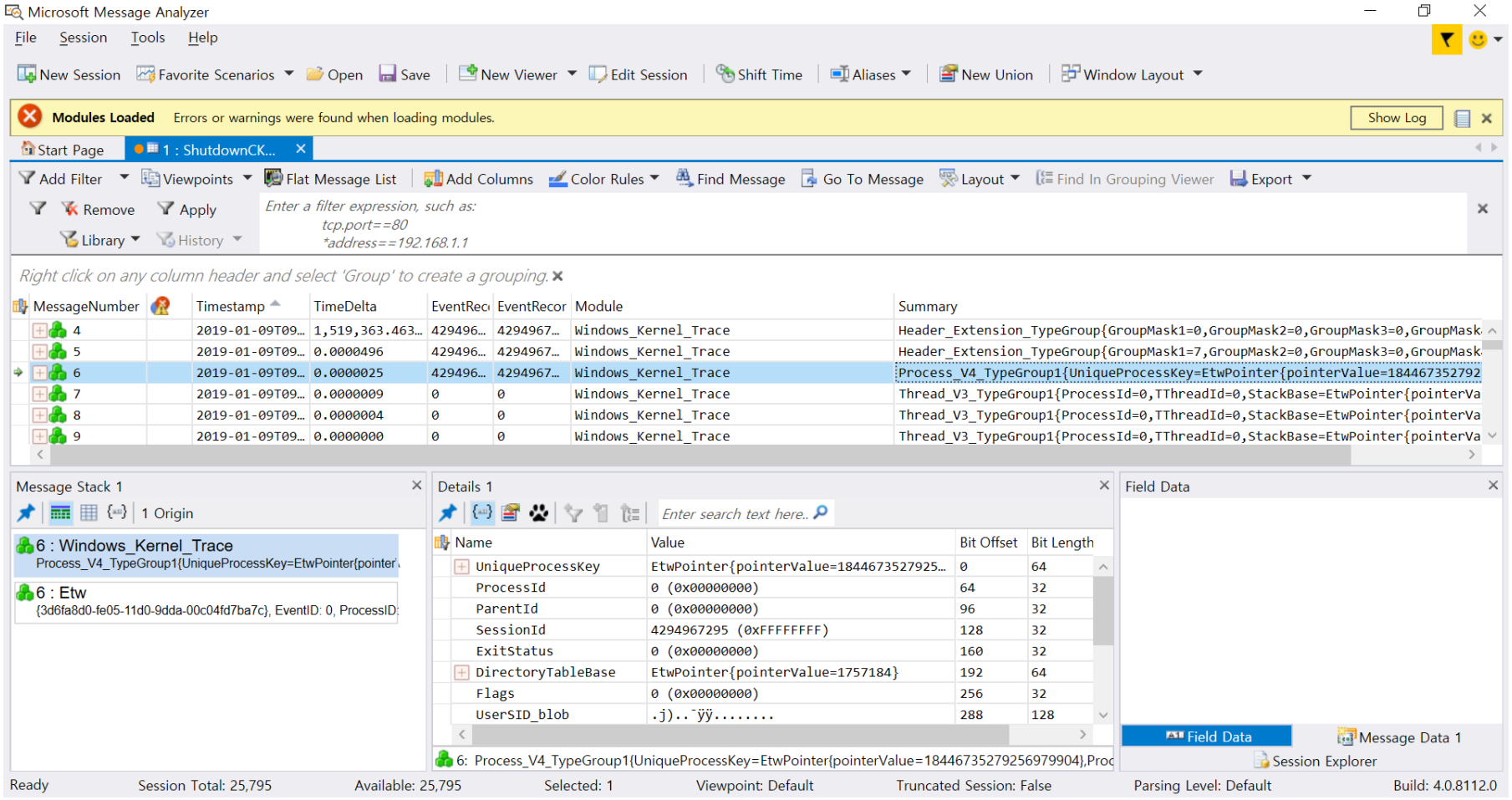
윈도우 이벤트 뷰어


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
이벤트 0,
일반
자세히
로그 이름(M):
원본(S):
로그된 날짜(D): 2019-01-09 오전 9:52:24
이벤트 ID(E): 0
작업 범주(Y): 없음

Microsoft Message Analyzer

- 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

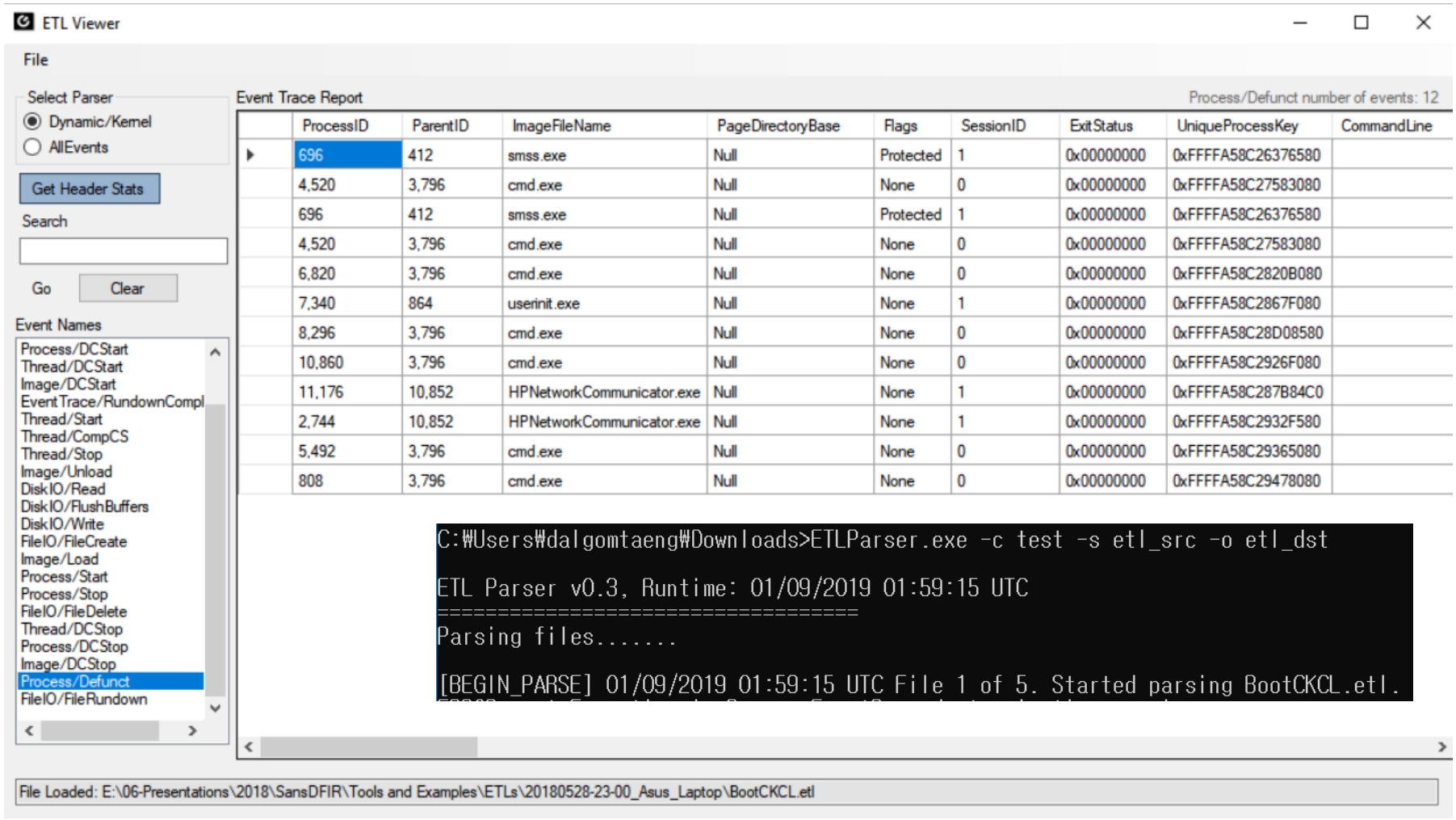
Microsoft Message Analyzer



ETL Viewer & Parser

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

ETL Viewer & Parser



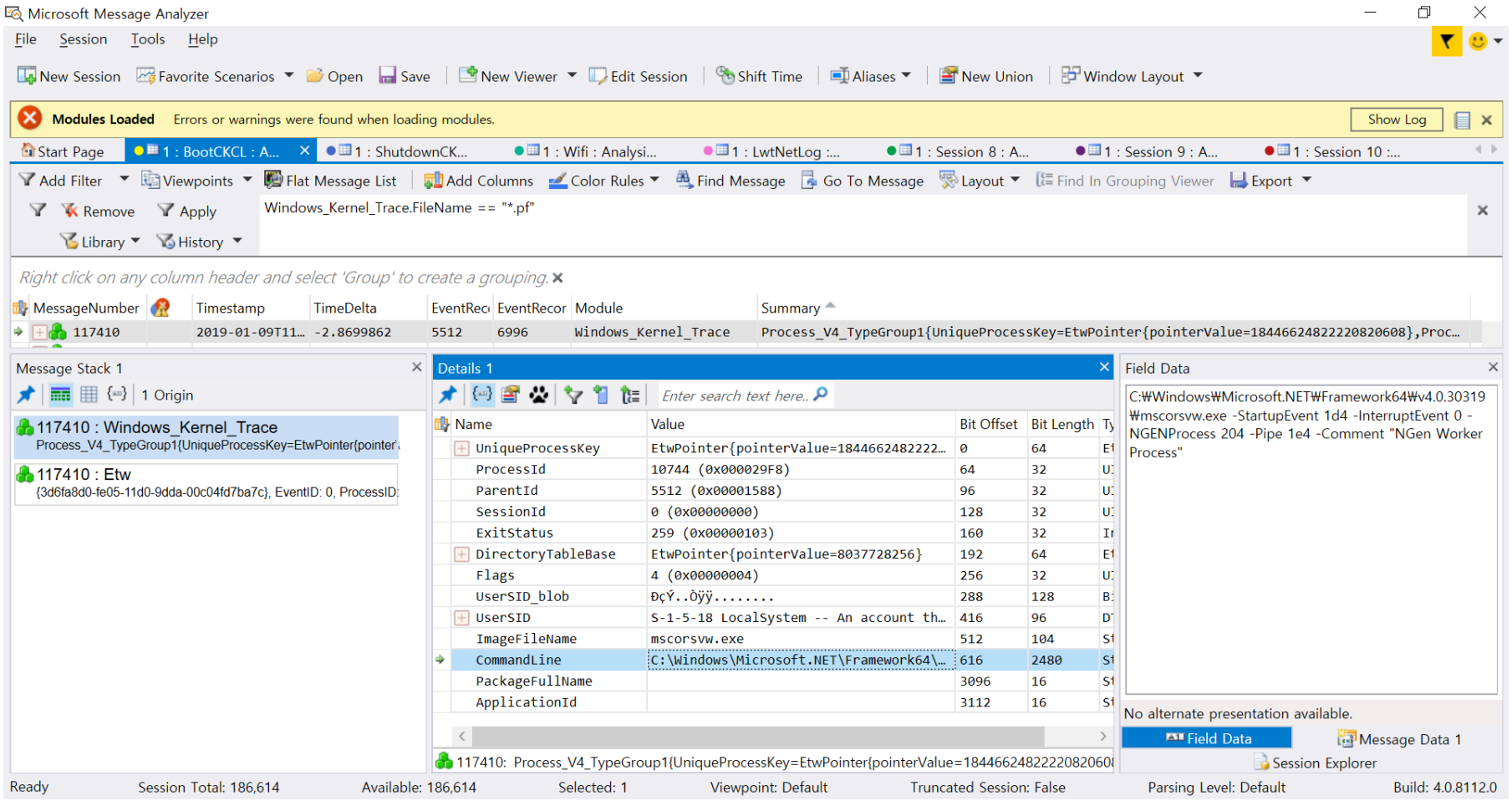
주요 ETL 파일 위치

- **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

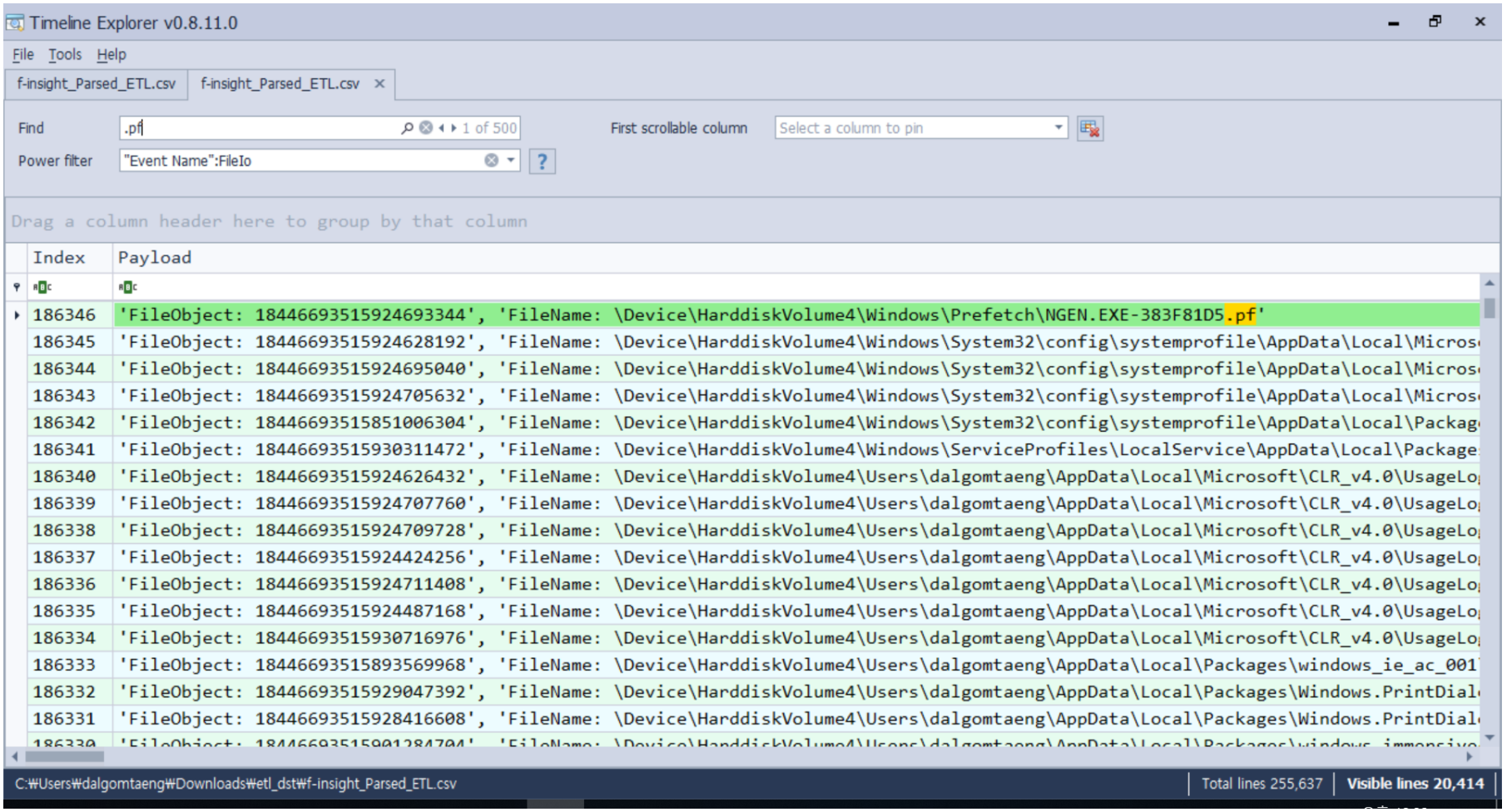
BootCKCL

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

BootCKCL


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 Library History
Windows_Kernel_Trace.FileName == "*.pf"
Right click on any column header and select 'Group' to create a grouping.
MessageNumber Timestamp TimeDelta EventRec EventRecor Module Summary
117410 2019-01-09T11... -2.8699862 5512 6996 Windows_Kernel_Trace Process_V4_TypeGroup1{UniqueProcessKey=EtwPointer{pointerValue=1844662482222082060
Message Stack 1
1 Origin
117410 : Windows_Kernel_Trace
Process_V4_TypeGroup1{UniqueProcessKey=EtwPointer{pointer
117410 : Etw
{3d6fa8d0-fe05-11d0-9dda-00c04fd7ba7c}, EventID: 0, ProcessID:
Details 1
Enter search text here..
Name Value Bit Offset Bit Length
UniqueProcessKey EtwPointer{pointerValue=1844662482222... 0 64
ProcessId 10744 (0x000029F8) 64 32
ParentId 5512 (0x00001588) 96 32
SessionId 0 (0x00000000) 128 32
ExitStatus 259 (0x00000103) 160 32
DirectoryTableBase EtwPointer{pointerValue=8037728256} 192 64
Flags 4 (0x00000004) 256 32
UserSID_blob ÐçÝ..Òÿÿÿ..... 288 128
UserSID S-1-5-18 LocalSystem -- An account th... 416 96
ImageFileName mscorsvw.exe 512 104
CommandLine C:\Windows\Microsoft.NET\Framework64\... 616 2480
PackageFullName 3096 16
ApplicationId 3112 16
117410: Process_V4_TypeGroup1{UniqueProcessKey=EtwPointer{pointerValue=1844662482222082060
Field Data
C:₩Windows₩Microsoft.NET₩Framework64₩v4.0.30319₩mscorsvw.exe -StartupEvent 1d4 -InterruptEvent 0 -NGENProcess 204 -Pipe 1e4 -Comment "NGen Worker Process"
No alternate presentation available.
Field Data Message Data 1
Session Explorer
Ready Session Total: 186,614 Available: 186,614 Selected: 1 Viewpoint: Default Truncated Session: False Parsing Level: Default Build: 4.0.8112.0

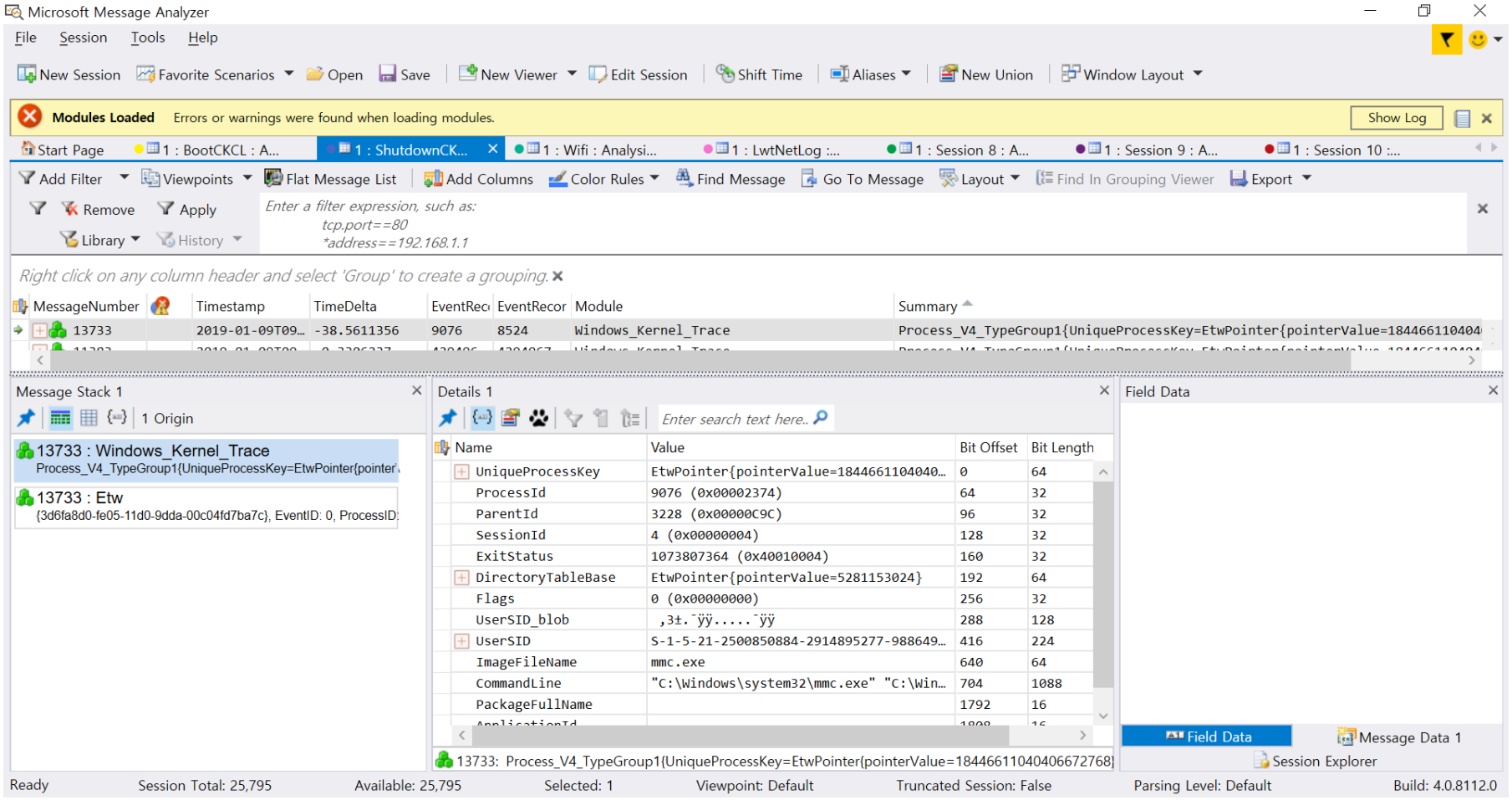
BootCKCL


Timeline Explorer v0.8.11.0
File Tools Help
f-insight_Parsed_ETL.csv
f-insight_Parsed_ETL.csv
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\Micros
186344 'FileObject: 18446693515924695040', 'FileName: \Device\HarddiskVolume4\Windows\System32\config\systemprofile\AppData\Local\Micros
186343 'FileObject: 18446693515924705632', 'FileName: \Device\HarddiskVolume4\Windows\System32\config\systemprofile\AppData\Local\Micros
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
C:\Users\dalgomtaeng\Downloads\etl_dst\f-insight_Parsed_ETL.csv
Total lines 255,637
Visible lines 20,414

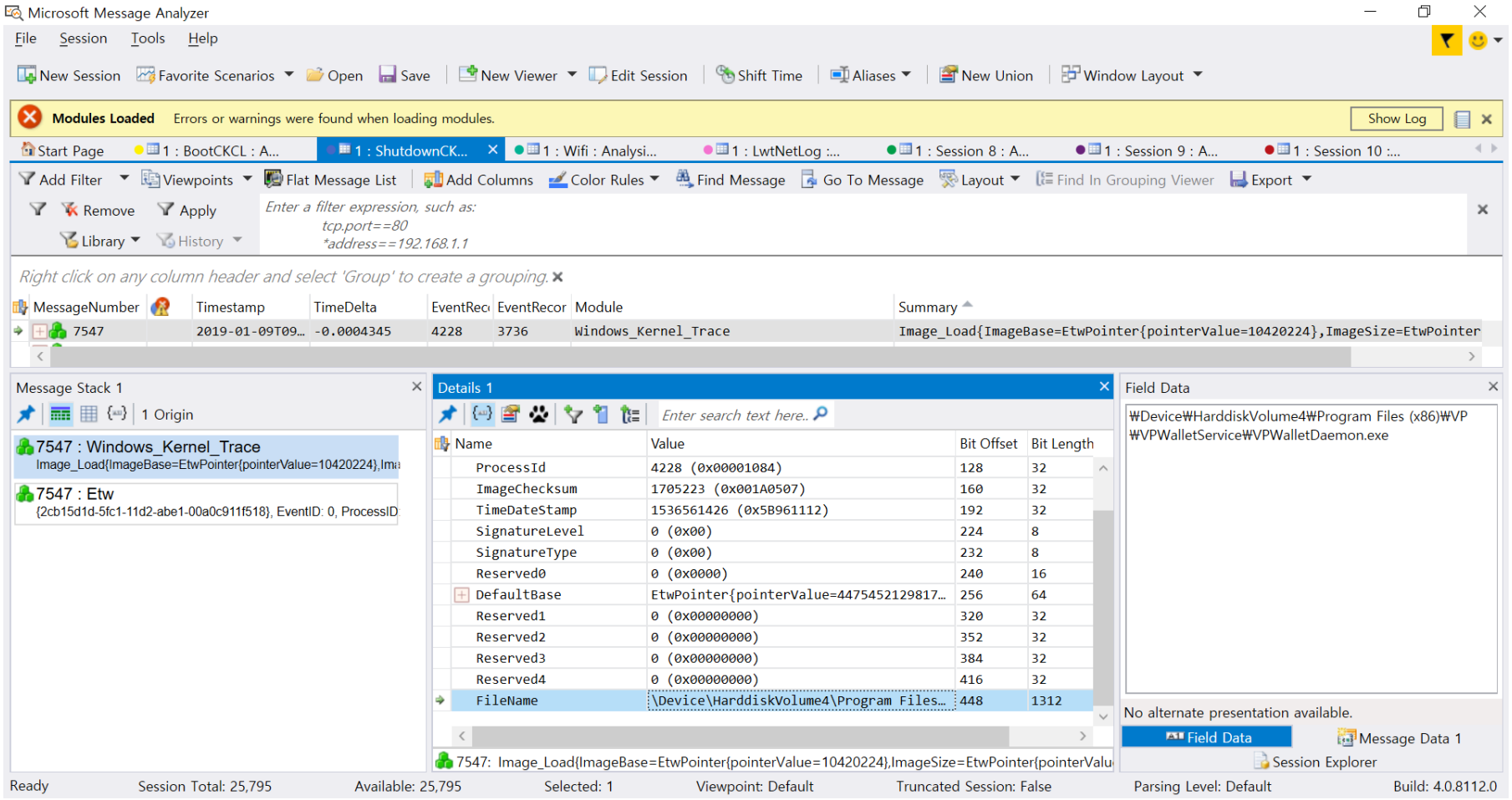
ShutdownCKCL

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

ShutdownCKCL



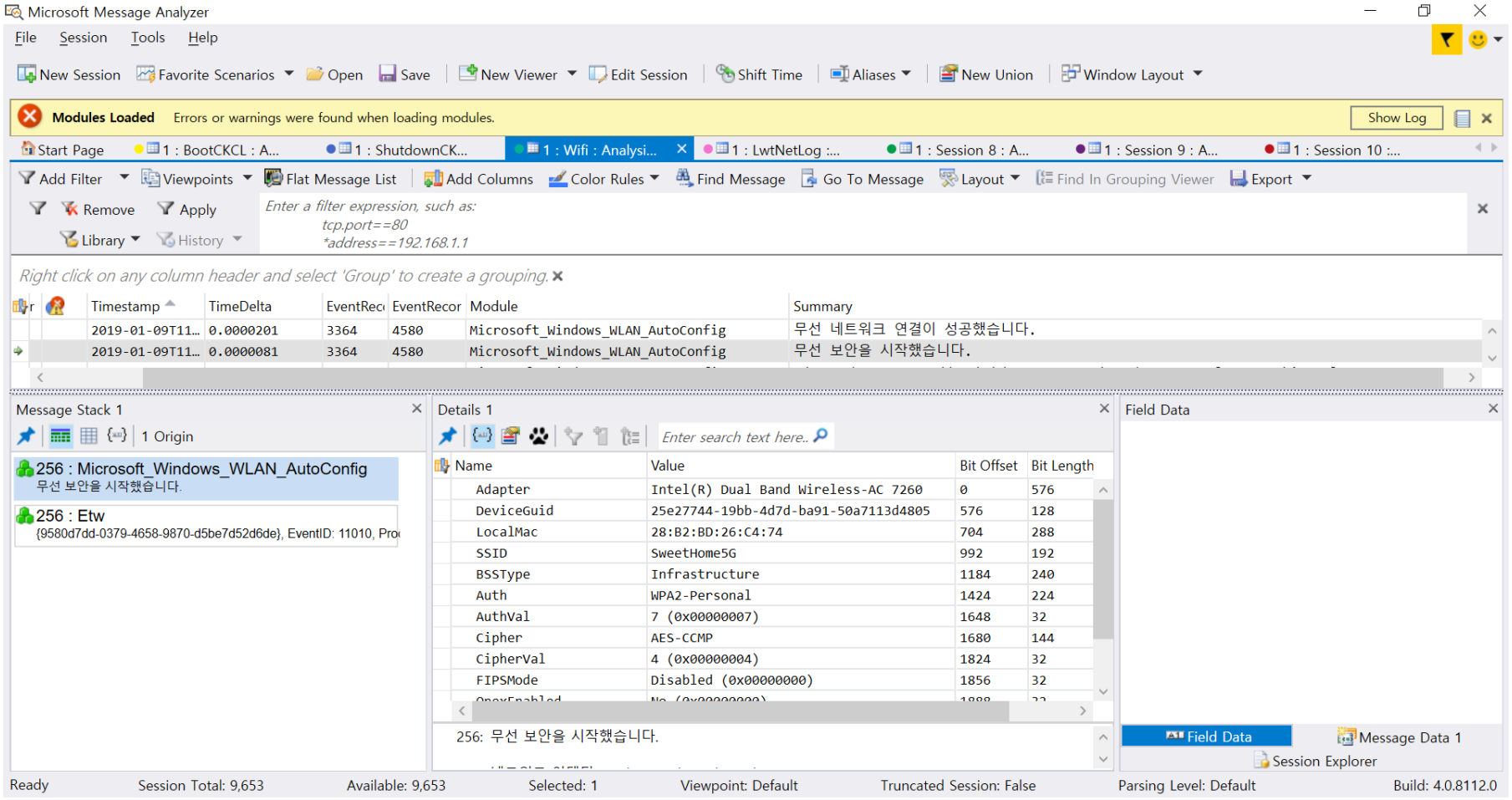
ShutdownCKCL



WIFI Traces

- **C:₩Windows₩System32₩LogFiles₩WMI₩Wifi.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

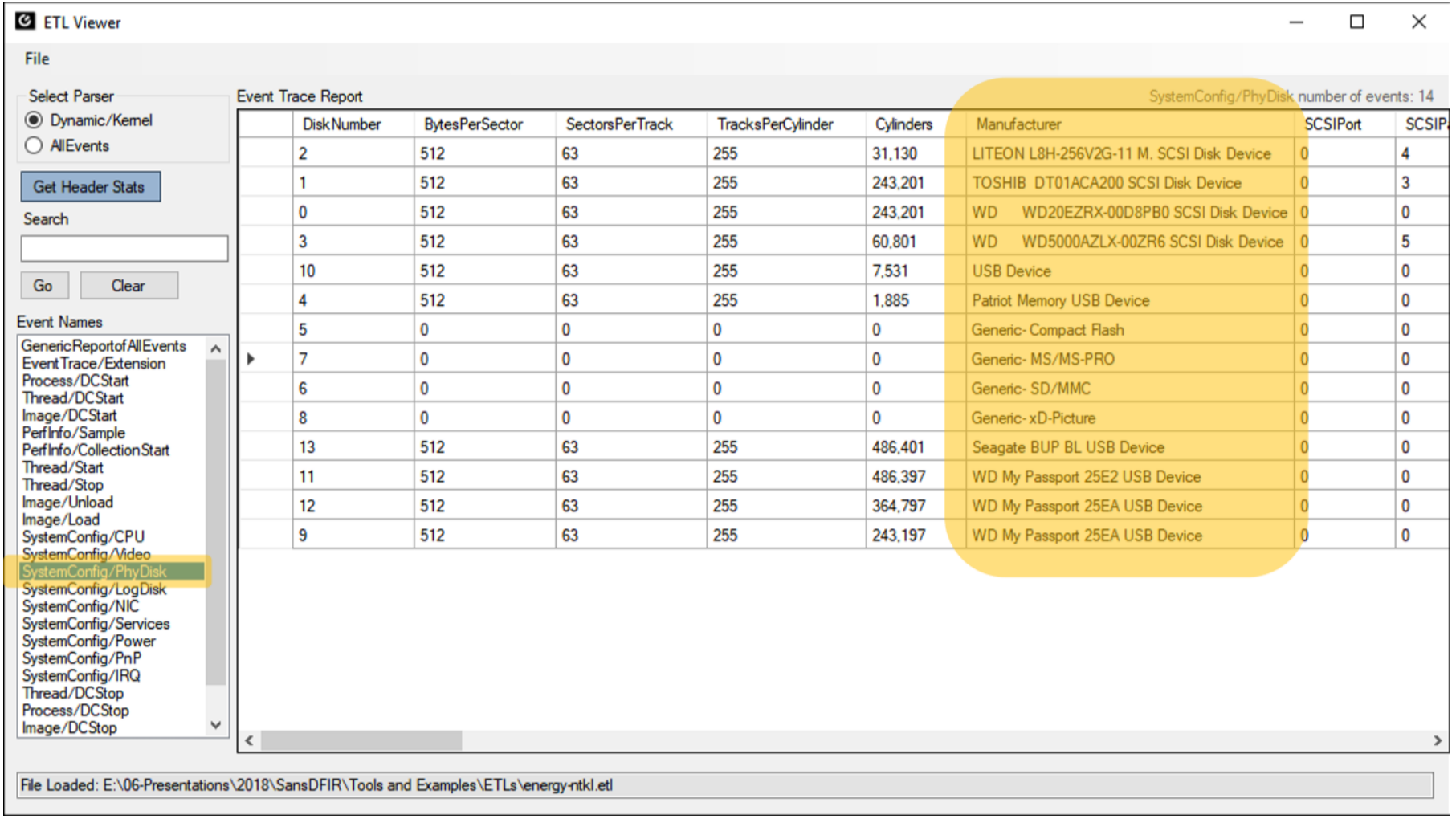
WIFI Traces


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 Library History
Enter a filter expression, such as:
tcp.port==80
*address==192.168.1.1
Right click on any column header and select 'Group' to create a grouping.
Timestamp TimeDelta EventRec EventRecor 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
Enter search text here..
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
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

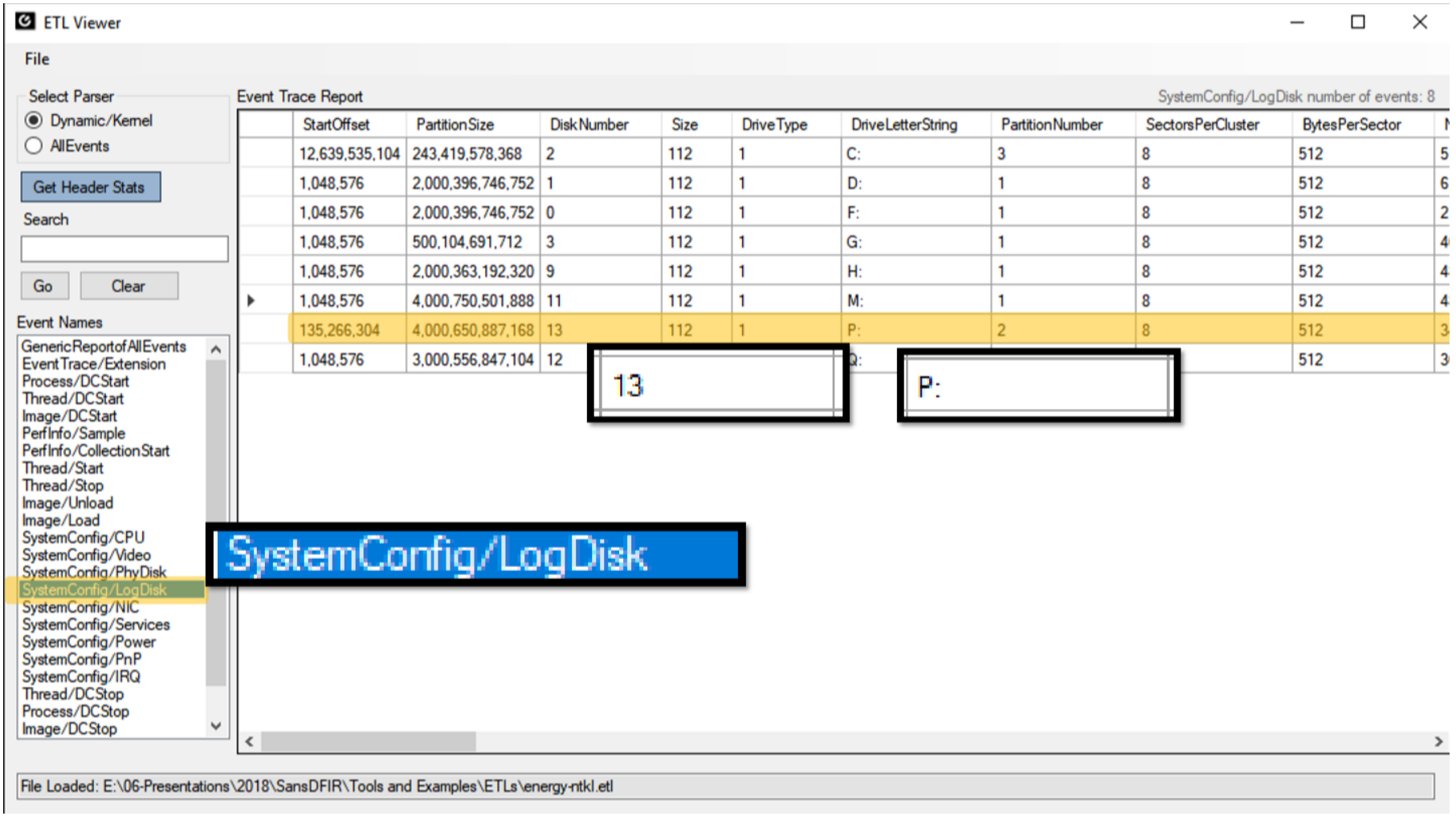
Energy-NTKL Traces

- **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

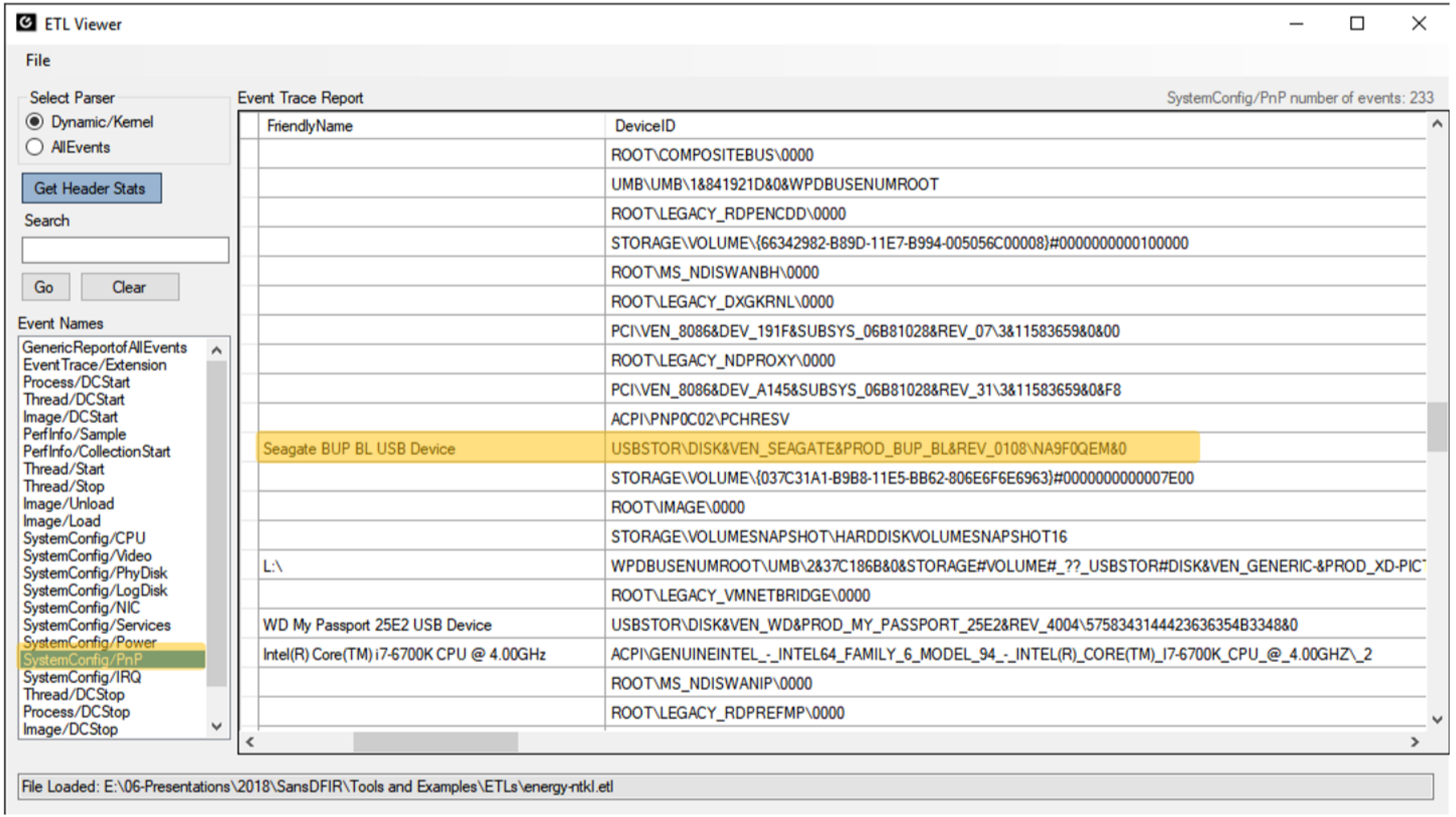
Energy-NTKL Traces



Energy-NTKL Traces



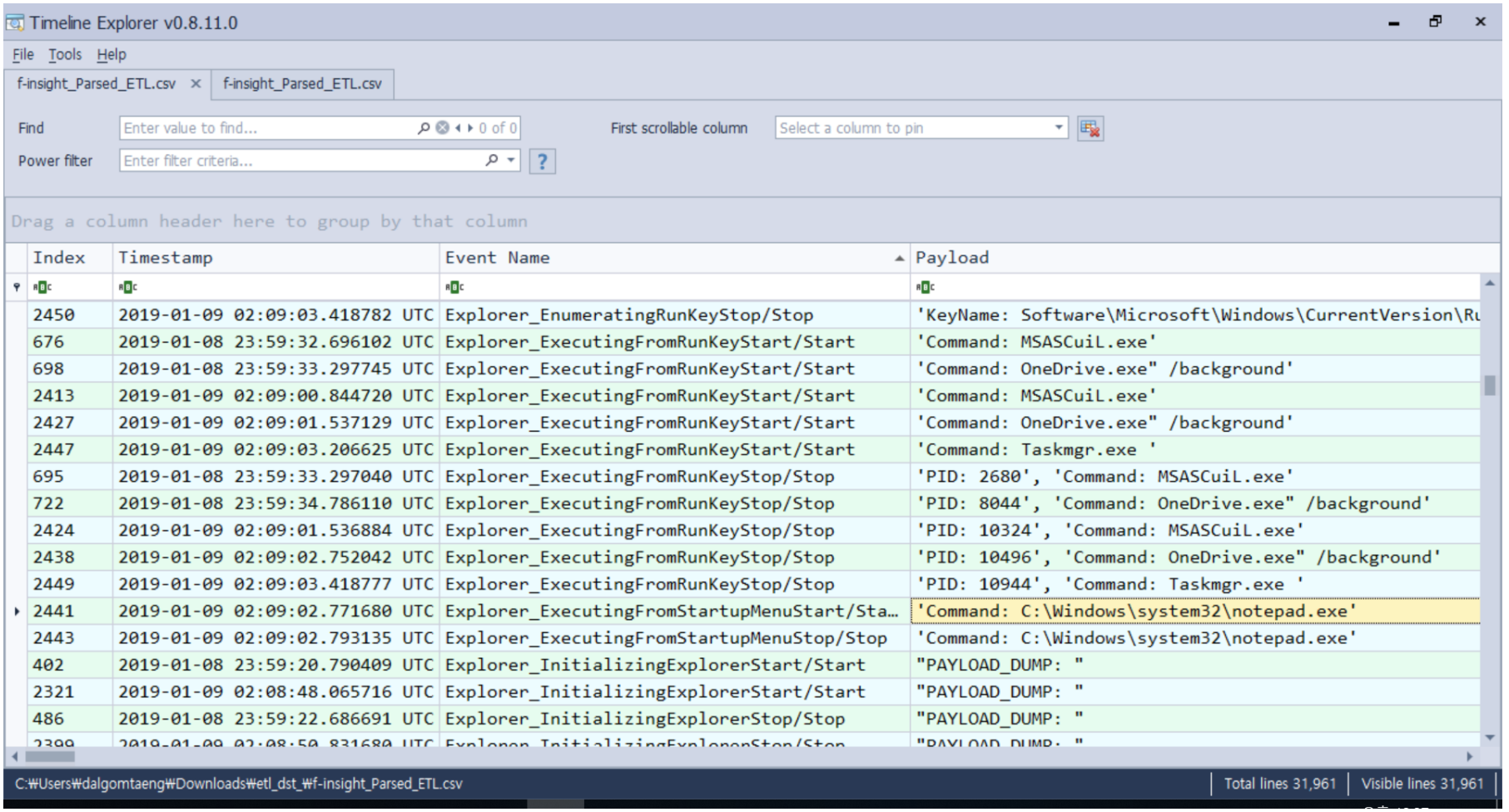
Energy-NTKL Traces



WdiContextLog Traces

- **C:₩Windows₩System32₩WDI ₩LogFiles₩**
  - WdiContextLog.etl.###
- **사용자 로그온과 관련된 정보**
  - Run 키에서 등록된 프로그램 실행
  - Startup 폴더에 등록된 프로그램 실행

WdiContextLog Traces



다른 ETL들

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

주의 사항

- **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

Question and Answer