Windows Event Log

- 김평안 -

Windows Event Log

-- 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 B 폴더 생성	A : 4 B : 0	x	
A 폴더 안 B 폴더 삭제	A : 10 B : 4	x	
B 폴더 열기 (접근)	A : 10 B : 4	x	
	A : 많음 B : 5	?	A 폴더 안 B 텍스트 파일 생성
	A : 많음 B : 약 35	?	A 폴더 안 B 텍스트 파일 수정
	A : 많음 B : 많음	?	A 폴더 안 B 텍스트 파일 삭제
	B : 늘어남	?	B 텍스트 파일 열기 (접근)

WINDOWS EVENT LOG

-감사 설정된 시스템의 모든 기록을 담은 데이터

오류

경고

운영 정보

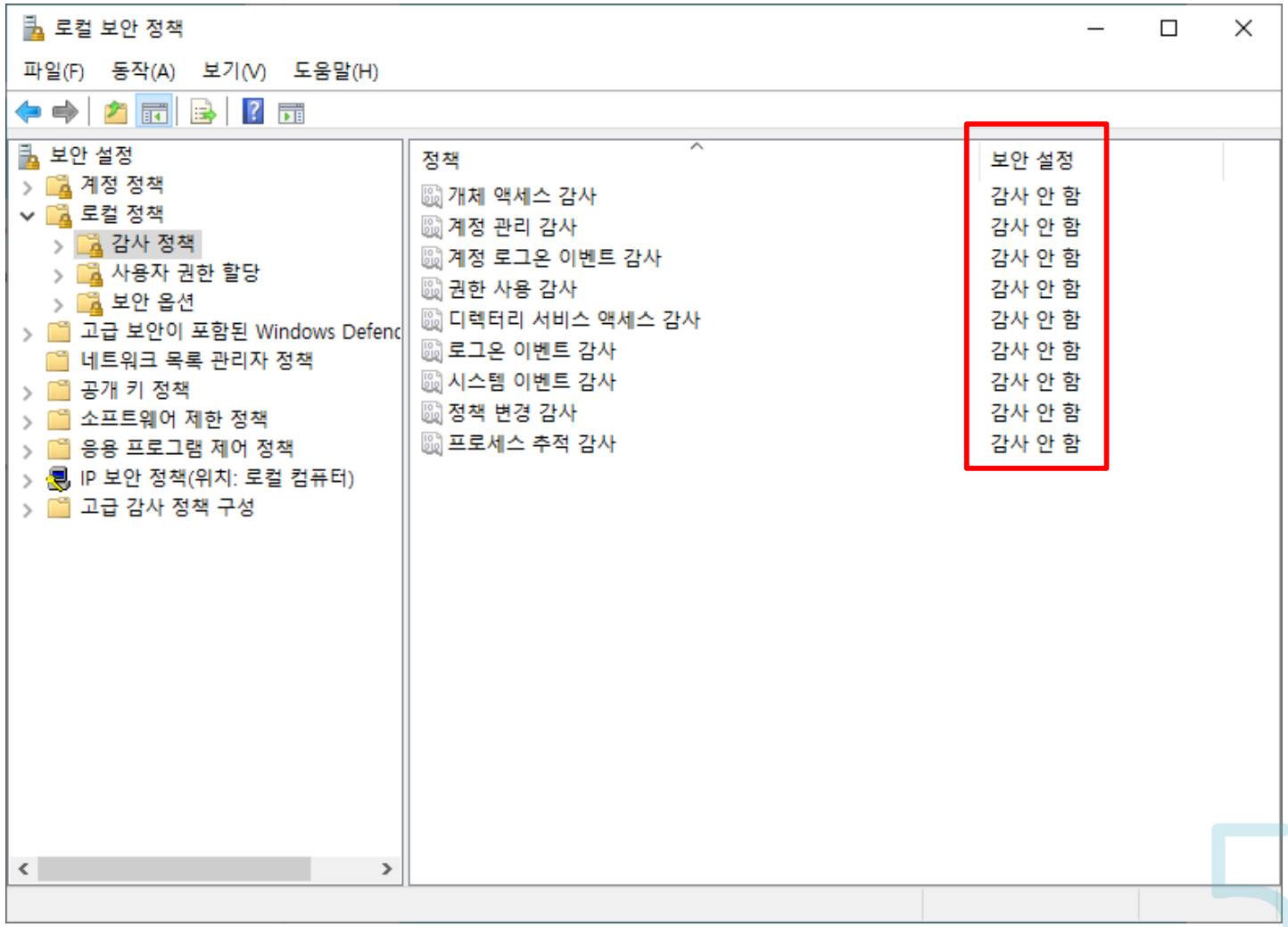
WINDOWS EVENT LOG

- 운영체제에 따른 로그 저장 방식의 차이점

	Win 2000/ XP/ 2003	Win Vista/ 7~
주요 로깅 데이터	응용 프로그램, 보안, 시스템	응용 프로그램, 보안, 시스템
로그 저장 형태	Binary	Binary, XML
저장된 로그 형식	evt	evtx
저장 경로	/windows/system32/config	/windows/system32/winevt/logs

WINDOWS EVENT LOG

- 감사 정책 설정



WINDOWS EVENT LOG

응용 프로그램

어플리케이션의 이벤트

- 앱 실행
- 앱 활동 내역

어떤 프로그램이 오류를 발생시켰는가

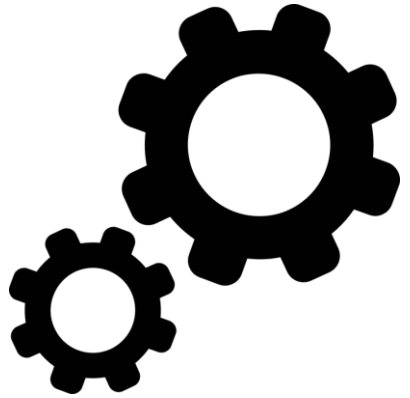
보안

보안 관련 이벤트

- 파일 접근
- 권한 사용

보안 관련 사고 분석

시스템



시스템 구성요소 이벤트

- 드라이버 오류
- 보안 로그 삭제

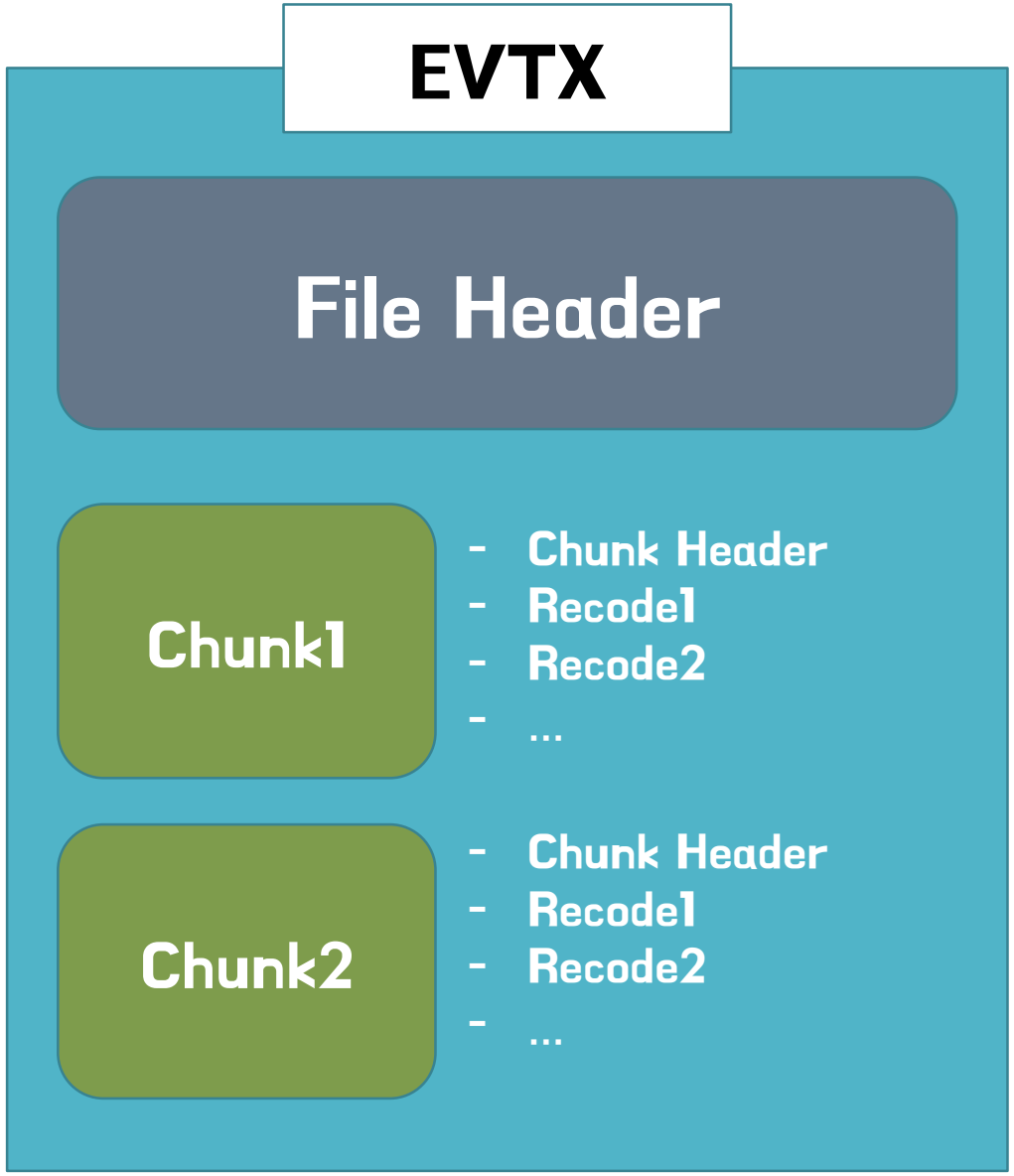
시스템 진단
시스템 시작/종료 시기 분석

WINDOWS EVENT LOG

EVTX 분석

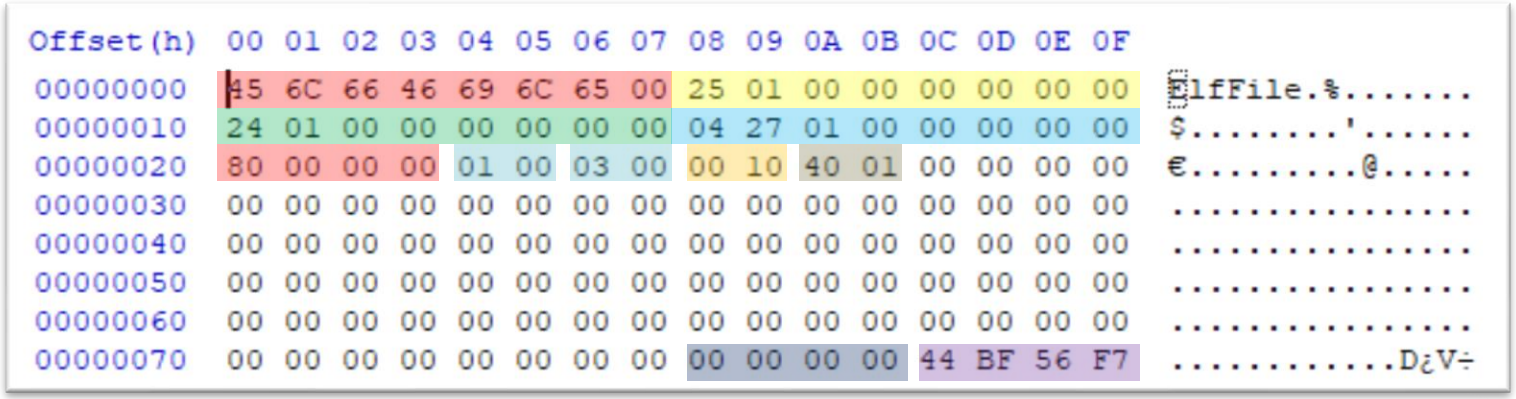
속성	설명
Source	이벤트를 기록한 소프트웨어 (이벤트가 일어난 프로세스)
Event ID	특별한 이벤트 유형을 식별하는 값. 예를 들어 6005는 이벤트로그 서비스가 시작될 때 발생되는 이벤트ID.
Level	이벤트의 심각도를 분류하여 나타낸다. 정보(Information), 경고(Warning), (오류)Error, (심각)Critical, 성공감사(Success Audit), 실패 감사(Failure Audit) 로 구분.
User	이벤트 발생에 대한 사용자의 이름
Operational Code	응용 프로그램에서 이벤트가 발생했을 때 활동이나 시점을 식별하는 숫자 값을 포함.
Log	이벤트가 기록된 로그의 이름입니다.
Task Category	이벤트 게시자의 하위 구성요소 또는 활동을 표현하는데 사용.
Keywords	이벤트를 검색하거나 필터링 하는데 사용할 수 있는 범주 또는 태그의 집합. ex) "네트워크", "보안", "리소스를 찾을 수 없습니다."
Computer	이벤트가 발생한 컴퓨터의 이름.
Date and Time	이벤트가 기록된 날짜 및 시간.
Process ID	이벤트를 생성하는 과정에 대한 식별번호.
Thread ID	이벤트 생성 쓰레드의 식별번호.

WINDOWS EVENT LOG



WINDOWS EVENT LOG

File Header

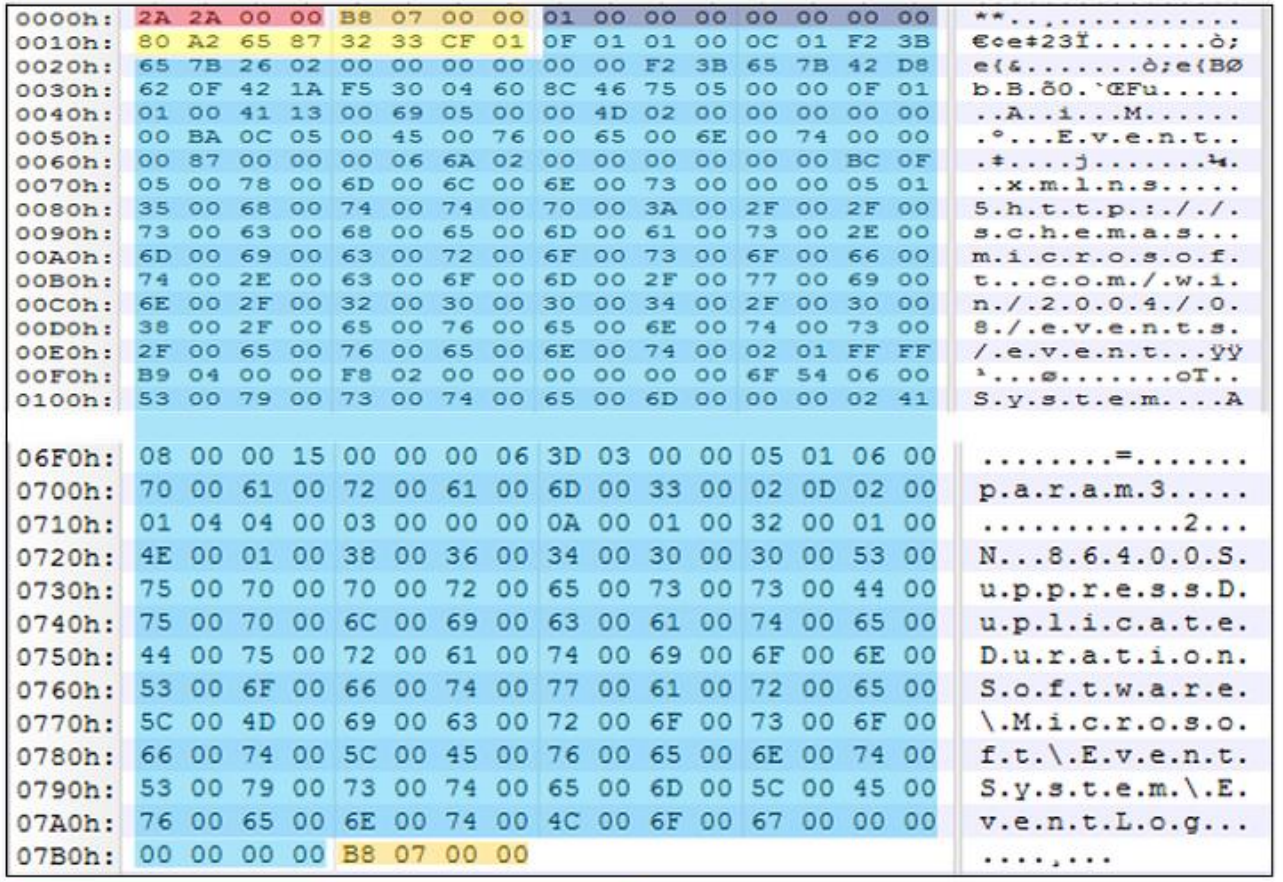


Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
00000000	45	6C	66	46	69	6C	65	00	25	01	00	00	00	00	00	00	ElfFile.%.....
00000010	24	01	00	00	00	00	00	00	04	27	01	00	00	00	00	00	$.....'.....
00000020	80	00	00	00	01	00	03	00	00	10	40	01	00	00	00	00	€.....@.....
00000030	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000040	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000050	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000060	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000070	00	00	00	00	00	00	00	00	00	00	00	00	44	BF	56	F7	............D¿V÷

- 시그니처
  ElfFile0x00
- 첫 번째 청크의 넘버
  293
- 마지막 청크의 넘버
  292
- 다음 레코드의 식별자
  67364
- 파일 플래그
- 체크섬
  0xF756BF44
  4149657412

WINDOWS EVENT LOG

Event record



```
0000h: 2A 2A 00 00 B8 07 00 00 01 00 00 00 00 00 00 00  **..,...........
0010h: 80 A2 65 87 32 33 CF 01 0F 01 01 00 0C 01 F2 3B  €¢e‡23Ï.......ò;
0020h: 65 7B 26 02 00 00 00 00 00 00 F2 3B 65 7B 42 D8  e{&.......ò;e{BØ
0030h: 62 0F 42 1A F5 30 04 60 8C 46 75 05 00 00 0F 01  b.B.õ0.`ŒFu.....
0040h: 01 00 41 13 00 69 05 00 00 4D 02 00 00 00 00 00  ..A..i...M......
0050h: 00 BA 0C 05 00 45 00 76 00 65 00 6E 00 74 00 00  .°...E.v.e.n.t..
0060h: 00 87 00 00 00 06 6A 02 00 00 00 00 00 00 BC 0F  .‡....j.......¼.
0070h: 05 00 78 00 6D 00 6C 00 6E 00 73 00 00 00 05 01  ..x.m.l.n.s.....
0080h: 35 00 68 00 74 00 74 00 70 00 3A 00 2F 00 2F 00  5.h.t.t.p.:././.
0090h: 73 00 63 00 68 00 65 00 6D 00 61 00 73 00 2E 00  s.c.h.e.m.a.s...
00A0h: 6D 00 69 00 63 00 72 00 6F 00 73 00 6F 00 66 00  m.i.c.r.o.s.o.f.
00B0h: 74 00 2E 00 63 00 6F 00 6D 00 2F 00 77 00 69 00  t...c.o.m./.w.i.
00C0h: 6E 00 2F 00 32 00 30 00 30 00 34 00 2F 00 30 00  n./.2.0.0.4./.0.
00D0h: 38 00 2F 00 65 00 76 00 65 00 6E 00 74 00 73 00  8./.e.v.e.n.t.s.
00E0h: 2F 00 65 00 76 00 65 00 6E 00 74 00 02 01 FF FF  /.e.v.e.n.t...ÿÿ
00F0h: B9 04 00 00 F8 02 00 00 00 00 00 00 6F 54 06 00  ¹...ø.......oT..
0100h: 53 00 79 00 73 00 74 00 65 00 6D 00 00 00 02 41  S.y.s.t.e.m....A

06F0h: 08 00 00 15 00 00 00 06 3D 03 00 00 05 01 06 00  ........=.......
0700h: 70 00 61 00 72 00 61 00 6D 00 33 00 02 0D 02 00  p.a.r.a.m.3.....
0710h: 01 04 04 00 03 00 00 00 0A 00 01 00 32 00 01 00  ............2...
0720h: 4E 00 01 00 38 00 36 00 34 00 30 00 30 00 53 00  N...8.6.4.0.0.S.
0730h: 75 00 70 00 70 00 72 00 65 00 73 00 73 00 44 00  u.p.p.r.e.s.s.D.
0740h: 75 00 70 00 6C 00 69 00 63 00 61 00 74 00 65 00  u.p.l.i.c.a.t.e.
0750h: 44 00 75 00 72 00 61 00 74 00 69 00 6F 00 6E 00  D.u.r.a.t.i.o.n.
0760h: 53 00 6F 00 66 00 74 00 77 00 61 00 72 00 65 00  S.o.f.t.w.a.r.e.
0770h: 5C 00 4D 00 69 00 63 00 72 00 6F 00 73 00 6F 00  \.M.i.c.r.o.s.o.
0780h: 66 00 74 00 5C 00 45 00 76 00 65 00 6E 00 74 00  f.t.\.E.v.e.n.t.
0790h: 53 00 79 00 73 00 74 00 65 00 6D 00 5C 00 45 00  S.y.s.t.e.m.\.E.
07A0h: 76 00 65 00 6E 00 74 00 4C 00 6F 00 67 00 00 00  v.e.n.t.L.o.g...
07B0h: 00 00 00 00 B8 07 00 00                          ....¸...
```

시그니처 Size : 4	이벤트 레코드 크기 Size : 4	이벤트 레코드 식별자 Size : 8
이벤트 레코드 작성 날짜와 시간 Size : 8	레코드 정보가 포함된 바이너리 XML Size : ...	

이미지 출처 https://gflow-security.tistory.com/entry/Windows-Artifact6-EventLog?category=262380