

닉스테크

서울시 성동구 왕십리로 58 포휴빌딩 10 층

전화 02-3497-8900 팩스 02-578-6621



## EDR AGNET 로그 포맷

VERSION	0.0.1
DATE	2018-02-19
WRITER	장욱

---

## DOCUMENT HISTORY (문서정보/수정내역)

수정날짜	수정자	버전	추가/수정항목	내용
2018-02-19	장욱	0.0.1	초안 작성	초안 작성

## 1. 목차

1. 목차.....	3
2. 메시지 바디 포맷.....	4
■ 메타 정보 .....	4
■ 이벤트 아이디 .....	4
■ 예제 .....	5
3. 이벤트 아이디별 로그 포맷 ( event_data ) .....	6
■ Process creation - Event_id 1 .....	6
■ A process changed a file creation time - Event_id 2.....	6
■ Network connection - Event_id 3.....	6
■ Sysmon service state changed - Event_id 4 .....	7
■ Process terminated - Event_id 5.....	7
■ Image loaded - Event_id 7 .....	7
■ Image loaded - Event_id 11.....	8
■ RegistryEvent (Object create and delete) - Event_id 12 .....	8
■ RegistryEvent (Value Set) - Event_id 13 .....	8

## 2. 메시지 바디 포맷

### ■ 메타 정보

필드명	의미	비고
@timestamp	이벤트 발생 시간	UTC 기준 ( +9 해야 함 )
@metadata	에이전트 메타 데이터	사용 안함
process_id	이벤트 아이디	표 2.2 이벤트 아이디 항목 참조
event_data	이벤트 상세 데이터	3. 이벤트 아이디별 로그 포맷 항목 참조
computer_name	PC 호스트 네임	
task	타스크 설명	
기타 나머지 항목	사용하지 않음	

[표 2.1 메타 정보]

### ■ 이벤트 아이디

필드명	의미	비고
1	Process creation	프로세스 생성
2	A process changed a file creation time	파일 접근 시간 변경
3	Network connection	네트워크 접근 ( IP )
4	Sysmon service state changed	사용안함
5	Process terminated	프로세스 종료
6	Driver loaded	사용안함
7	Image loaded	DLL 로드
8	CreateRemoteThread	사용안함
9	RawAccessRead	사용안함
10	ProcessAccess	사용안함
11	FileCreate	파일 생성 (접근)
12	RegistryEvent (Object create and delete)	레지스트리 생성/삭제
13	RegistryEvent (Value Set)	레지스트리 값 설정
14	RegistryEvent (Key-and-Value-Rename)	사용안함
15	FileCreateStreamHash	사용안함
16	없음	사용안함
17	PipeEvent (Pipe-Created)	사용안함
18	PipeEvent (Pipe-Connected)	사용안함
19	WmiEvent (WmiEventFilter-activity-detected)	사용안함
20	WmiEvent (WmiEventConsumer-activity-detected)	사용안함
21	WmiEvent (WmiEventConsumerToFilter-activity-detected)	사용안함
25	Error	사용안함

[표 2.2 이벤트 아이디]

## ■ 예제

### 예제

#### 예제 1. 프로세스 생성

```
{
  "@timestamp": "2018-03-05T07:24:10.194Z",
  "@metadata": {
    "beat": "winlogbeat",
    "type": "doc",
    "version": "6.2.2"
  },
  "message": "Process Create:\nUtcTime: 2018-03-05 07:24:10.147\nProcessGuid: {A376A8F6-F09A-5A9C-0000-00107EE13802}\nProcessId: 5708\nImage: C:\\Program Files\\Mozilla Firefox\\firefox.exe\nFileVersion: 58.0.2\nDescription: Firefox\nProduct: Firefox\nCompany: Mozilla Corporation\nCommandLine: \"C:\\Program Files\\Mozilla Firefox\\firefox.exe\" http://google.co.kr/\nCurrentDirectory: C:\\WINDOWS\\system32\\\nUser: DESKTOP-WJANG\\wook8170\nLogonGuid: {A376A8F6-ECB5-5A9C-0000-00208AB21300}\nLogonId: 0x13B28A\nTerminalSessionId: 1\nIntegrityLevel: Medium\nHashes: MD5=22819EB3C648583352AE83003E4C9A56,SHA256=4B69AE5B7D548EFC56FDBE2E650CE2B519AE0C9C928640023077B956C51A7138\nParentProcessGuid: {A376A8F6-F098-5A9C-0000-00109D6C3702}\nParentProcessId: 24128\nParentImage: C:\\Windows\\System32\\RuntimeBroker.exe\nParentCommandLine: C:\\Windows\\System32\\RuntimeBroker.exe -Embedding",
  "user": {
    "identifier": "S-1-5-18",
    "name": "SYSTEM",
    "domain": "NT AUTHORITY",
    "type": "Well Known Group"
  },
  "task": "Process Create (rule: ProcessCreate)",
  "process_id": 8608,
  "version": 5,
  "level": "정보",
  "record_number": "17",
  "opcode": "정보",
  "thread_id": 19220,
  "type": "wineventlog",
  "log_name": "Microsoft-Windows-Sysmon/Operational",
  "event_id": 1,
  "provider_guid": "{5770385F-C22A-43E0-BF4C-06F5698FFBD9}",
  "source_name": "Microsoft-Windows-Sysmon",
  "event_data": {
    "Hashes": "MD5=22819EB3C648583352AE83003E4C9A56,SHA256=4B69AE5B7D548EFC56FDBE2E650CE2B519AE0C9C928640023077B956C51A7138",
    "FileVersion": "58.0.2",
    "CommandLine": "\"C:\\Program Files\\Mozilla Firefox\\firefox.exe\" http://google.co.kr/",
    "ParentImage": "C:\\Windows\\System32\\RuntimeBroker.exe",
    "ProcessId": "5708",
    "Product": "Firefox",
    "ProcessGuid": "{A376A8F6-F09A-5A9C-0000-00107EE13802}",
    "LogonGuid": "{A376A8F6-ECB5-5A9C-0000-00208AB21300}",
    "ParentCommandLine": "C:\\Windows\\System32\\RuntimeBroker.exe -Embedding",
    "LogonId": "0x13b28a",
    "Image": "C:\\Program Files\\Mozilla Firefox\\firefox.exe",
    "Description": "Firefox",
    "ParentProcessId": "24128",
    "CurrentDirectory": "C:\\WINDOWS\\system32\\",
    "TerminalSessionId": "1",
    "UtcTime": "2018-03-05 07:24:10.147",
    "ParentProcessGuid": "{A376A8F6-F098-5A9C-0000-00109D6C3702}",
    "Company": "Mozilla Corporation",
    "IntegrityLevel": "Medium",
    "User": "DESKTOP-WJANG\\wook8170"
  },
  "beat": {
    "version": "6.2.2",
```

```

    "name": "DESKTOP-WJANG",
    "hostname": "DESKTOP-WJANG",
    "timezone": "+09:00"
  },
  "computer_name": "DESKTOP-WJANG"
}

```

[표 2.3 예제]

### 3. 이벤트 아이디별 로그 포맷 ( EVENT\_DATA )

#### ■ Process creation - Event\_id 1

##### 로그 아이템 기본 포맷

```

{
  "Hashes":
  "MD5=22819EB3C648583352AE83003E4C9A56,SHA256=4B69AE5B7D548EFC56FDBE2E650CE2B519AE0C9C928640023077B956C51A7138",
  "FileVersion": "58.0.2",
  "CommandLine": "\"C:\\Program Files\\Mozilla Firefox\\firefox.exe\" http://google.co.kr/",
  "ParentImage": "C:\\Windows\\System32\\RuntimeBroker.exe",
  "ProcessId": "5708",
  "Product": "Firefox",
  "ProcessGuid": "{A376A8F6-F09A-5A9C-0000-00107EE13802}",
  "LogonGuid": "{A376A8F6-ECB5-5A9C-0000-00208AB21300}",
  "ParentCommandLine": "C:\\Windows\\System32\\RuntimeBroker.exe -Embedding",
  "LogonId": "0x13b28a",
  "Image": "C:\\Program Files\\Mozilla Firefox\\firefox.exe",
  "Description": "Firefox",
  "ParentProcessId": "24128",
  "CurrentDirectory": "C:\\WINDOWS\\system32\\",
  "TerminalSessionId": "1",
  "UtcTime": "2018-03-05 07:24:10.147",
  "ParentProcessGuid": "{A376A8F6-F098-5A9C-0000-00109D6C3702}",
  "Company": "Mozilla Corporation",
  "IntegrityLevel": "Medium",
  "User": "DESKTOP-WJANG\\wook8170"
}

```

#### ■ A process changed a file creation time - Event\_id 2

##### 로그 아이템 기본 포맷

```

{
  "CreationUtcTime": "2017-04-24 03:51:05.300",
  "PreviousCreationUtcTime": "2018-03-05 07:25:49.952",
  "UtcTime": "2018-03-05 07:25:49.971",
  "ProcessGuid": "{A376A8F6-ECC2-5A9C-0000-0010E1111D00}",
  "ProcessId": "17568",
  "Image": "C:\\Program Files\\Mozilla Firefox\\firefox.exe",
  "TargetFilename":
  "C:\\Users\\wook8170\\AppData\\Roaming\\Microsoft\\Windows\\Recent\\CustomDestinations\\JIMMG587JA65SLJ1SYZD.temp"
}

```

#### ■ Network connection - Event\_id 3

#### 로그 아이템 기본 포맷

```
{
  "SourceIsIpv6": "false",
  "DestinationIp": "216.58.200.3",
  "UtcTime": "2018-03-05 07:24:10.536",
  "DestinationPort": "443",
  "ProcessId": "17568",
  "SourceHostname": "DESKTOP-WJANG",
  "SourcePort": "2199",
  "ProcessGuid": "{A376A8F6-ECC2-5A9C-0000-0010E1111D00}",
  "DestinationIsIpv6": "false",
  "DestinationPortName": "https",
  "Protocol": "tcp",
  "SourceIp": "192.168.198.67",
  "Image": "C:\\Program Files\\Mozilla Firefox\\firefox.exe",
  "DestinationHostname": "hkg12s11-in-f3.1e100.net",
  "Initiated": "true",
  "User": "DESKTOP-WJANG\\wook8170"
},
```

### ■ Sysmon service state changed - Event\_id 4

#### 로그 아이템 기본 포맷

```
{
  "Version": "7.01",
  "SchemaVersion": "4.00",
  "UtcTime": "2018-03-05 07:23:14.958",
  "State": "Started"
}
```

### ■ Process terminated - Event\_id 5

#### 로그 아이템 기본 포맷

```
{
  "UtcTime": "2018-03-05 07:24:10.322",
  "ProcessGuid": "{A376A8F6-F09A-5A9C-0000-00107EE13802}",
  "ProcessId": "5708",
  "Image": "C:\\Program Files\\Mozilla Firefox\\firefox.exe"
}
```

### ■ Image loaded - Event\_id 7

#### 로그 아이템 기본 포맷

```
{
  "Signature": "Microsoft Windows",
  "Signed": "true",
  "ProcessId": "17704",
  "UtcTime": "2018-03-05 07:32:36.738",
  "ProcessGuid": "{A376A8F6-F294-5A9C-0000-001052E48503}",
  "FileVersion": "10.0.16299.15 (WinBuild.160101.0800)",
  "Product": "Microsoft® Windows® Operating System",
  "SignatureStatus": "Valid",
  "Image": "C:\\Program Files\\Mozilla Firefox\\firefox.exe",
  "Company": "Microsoft Corporation",
}
```

```

    "Hashes":
    "MD5=222A8E8EA615529B5025DE5782830AF1,SHA256=7C76BB7AEC3C51164A49041E8A710C3C291BA1D30BAE07D126434A52A80D99E1",
    "ImageLoaded": "C:\\Windows\\System32\\kernel32.dll",
    "Description": "Windows NT 기반 API 클라이언트 DLL"
}

```

## ■ Image loaded - Event\_id 11

### 로그 아이템 기본 포맷

```

{
  "ProcessId": "24360",
  "Image": "C:\\WINDOWS\\explorer.exe",
  "TargetFilename": "K:\\cc - 복사본 (2).txt",
  "CreationUtcTime": "2018-03-05 07:27:50.280",
  "UtcTime": "2018-03-05 07:27:50.291",
  "ProcessGuid": "{A376A8F6-EF7D-5A9C-0000-0010537B8601}"
}

```

## ■ RegistryEvent (Object create and delete) - Event\_id 12

### 로그 아이템 기본 포맷

```

{
  "ProcessId": "19128",
  "Image": "C:\\WINDOWS\\regedit.exe",
  "TargetObject": "HKLM\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run\\새 키 #1",
  "EventType": "CreateKey",
  "UtcTime": "2018-03-05 07:43:03.093",
  "ProcessGuid": "{A376A8F6-F4E7-5A9C-0000-001010A5C804}"
},

```

## ■ RegistryEvent (Value Set) - Event\_id 13

### 로그 아이템 기본 포맷

```

{
  "Image": "C:\\WINDOWS\\regedit.exe",
  "TargetObject": "HKLM\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run\\새 값 #1",
  "Details": "(Empty)",
  "EventType": "SetValue",
  "UtcTime": "2018-03-05 07:43:08.639",
  "ProcessGuid": "{A376A8F6-F4E7-5A9C-0000-001010A5C804}",
  "ProcessId": "19128"
},

```