

# 윈도우 텔레메트리에 대한 분석과 활용

---

*Jack*

*one01h@korea.ac.kr*





1. 텔레메트리? – Motivation & Introduction

2. 데이터 수집 & 구조 분석 – Data Acquisition & Analysis

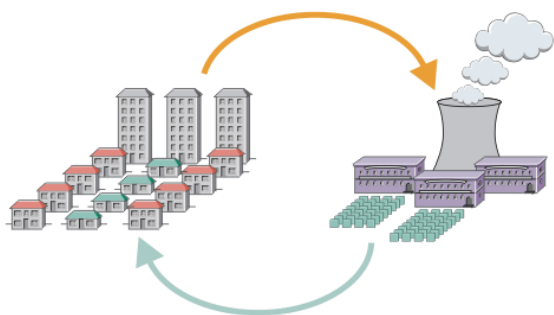
3. 분석결과 활용 – Investigation & Discussion

# 1. 텔레메트리?

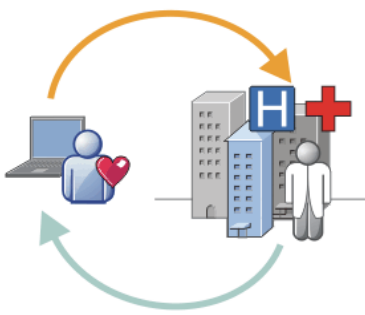
- 간략한 소개
- 윈도우에서 텔레메트리를 어떻게 활용하나?
- 내 컴퓨터는 어떤 상태인가?

## 텔레메트리 (telemetry, 원격 분석)

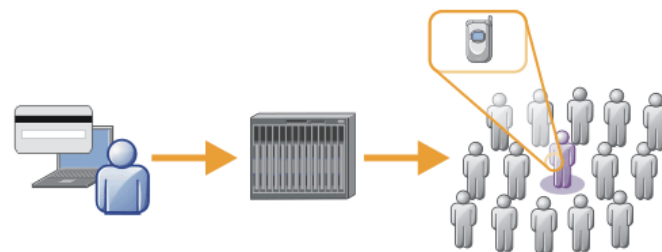
- NMS : SNMP (요청-응답 : 수동적) → SDN : Telemetry & Feedback
  - “최대한 많은 데이터를 가능한 빨리 사용하기 쉽게 어떻게 수집할까?”
- 원격 디바이스에서 얻는 데이터의 자동화된 감지 및 측정
- 디바이스에서 중앙 제어 지점으로의 데이터(디바이스 구성 및 제어 정보) 전송
  - 소프트웨어 산업계 전반에서 사용하는 기술



[ 가정 에너지 모니터링 및 제어 ]



[ 심장병 환자 간호 시스템 ]



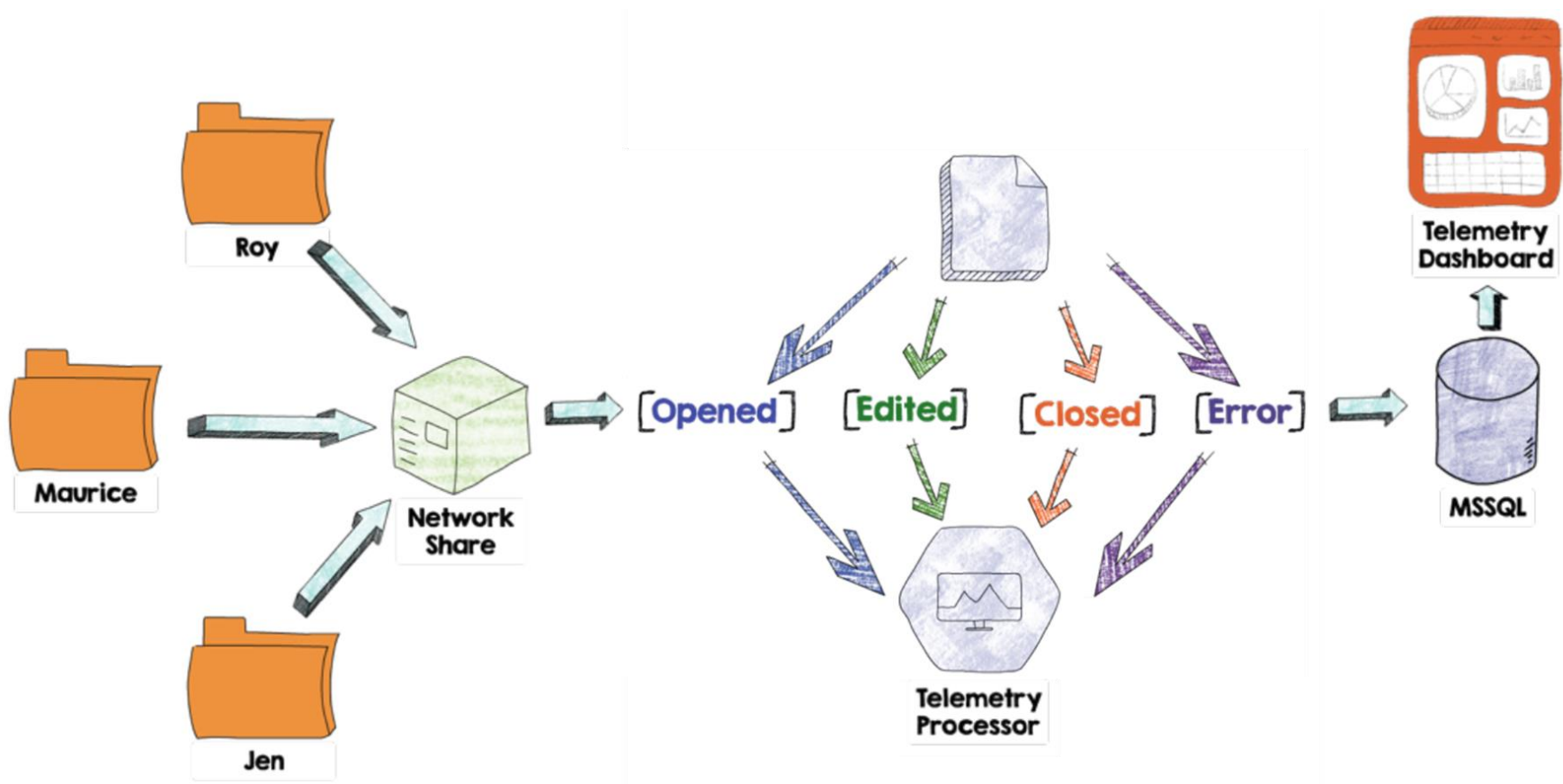
[ 카드 거래에서 개인 식별 ]

[https://www.ibm.com/support/knowledgecenter/ko/SSFKSJ\\_7.1.0/com.ibm.mq.doc/tt10000\\_.htm](https://www.ibm.com/support/knowledgecenter/ko/SSFKSJ_7.1.0/com.ibm.mq.doc/tt10000_.htm)

# 1. 텔레메트리?



- 오피스 텔레메트리 (Office Telemetry)
  - Telemetry to assess office compatibility in Microsoft office



Ref. Samuel Koffman, Microsoft Office Telemetry: Tracking Your Every Move, OSDCon 2018



## Dutch government report says Microsoft Office telemetry collection breaks GDPR

Microsoft pledges to address issues; has already released a "zero exhaust" Office telemetry setting.

By [Catalin Cimpanu](#) for [Zero Day](#) | November 14, 2018 -- 23:00 GMT (07:00 GMT+08:00) | Topic: [Security](#)



## EU to check for GDPR violations in Microsoft's contracts with EU institutions

EU starts investigation of Microsoft's contracts with EU institutions after Dutch government report.

By [Catalin Cimpanu](#) for [Zero Day](#) | April 8, 2019 -- 14:59 GMT (22:59 GMT+08:00) | Topic: [Microsoft](#)



Rijksoverheid

## Data Protection Impact Assessment (DPIA) on Microsoft Office

## Microsoft Office 365 banned in German schools over data privacy

Declaring that Windows 10 and Microsoft Office 365 are not compliant with EU General Data Protection Regulation, schools in Germany have banned its for violating privacy of students and teachers.

Published: 16 Jul 2019, 8:51 PM

Nr	Risk	Possible measure Microsoft	Possible measure per tenant
2	No possibility to influence or end the collection of telemetry data	a. Temporary settings to minimise the collection of telemetry data b. Permanent settings for telemetry levels	Use tool when it becomes available Use temporary minimisation settings Do not use SharePoint/OneDrive Do not use web-only Office 365 Use setting telemetry Off when switch is available
4	Incorrect qualification Microsoft as data processor	a. Minimization of purposes to be able to act as a processor OR New framework agreement b. Only process data from voluntary Connected Services as a data processor OR change default for voluntary Connected Services to 'Off'	Consider deleting some specific users and creating new accounts for them Prohibit user from sending personal data to Microsoft or improve Office software for some functionality (after conducting a separate DPIA)
5	Not enough control over sub-processors and factual processing	More audit rights	Endorse new framework agreement as processor or Prohibit voluntary Connected Services unless Microsoft offers these services as a processor
6	Limitation of purpose	Processing only for strictly necessary purposes for which the tenants have a legal ground	Consider stand-alone deployment without Microsoft account for each user
7	The transfer of data outside the EU	New contractual guarantees to ensure data stays within the EU	- no specific measure, see above
8	The indefinite retention period of diagnostic data	Determine necessary retention periods	- no specific measure, see above



**ZDNet**

VIDEOS EXECUTIVE GUIDES SECURITY CLOUD INNOVATION CXO HARDWARE MORE NEWSLETTERS ALL WRITERS

MUST READ **WINDOWS 10 UPDATES: EXPECT SLIMMED-DOWN, FULL-QUALITY VERSIONS, SAYS MICROSOFT**

## Windows 10 telemetry secrets: Where, when, and why Microsoft collects your data

How does Windows 10 telemetry really work? It's not a state secret. I've gone through the documentation and sorted out the where, when, and why. If you're concerned about private documents accidentally leaving your network, you might want to turn the telemetry setting down.

By Ed Bott for The Ed Bott Report | February 23, 2016 -- 12:24 GMT (20:24 GMT+08:00) | Topic: Windows 10

### Microsoft Says It's Not Sharing Windows 10 Telemetry Data with Anyone

We'll just keep this data for ourselves, the company claims

Nov 26, 2016 15:59 GMT · By Bogdan Popa · Comment · Share:

Microsoft and security company FireEye recently signed a partnership on improving Windows Defender with more advanced capabilities, but according to one report, the deal included more than that.



# 설정 사용자 지정

## 연결 및 오류 보고

열려 있는 추천 핫스팟에 자동으로 연결합니다. 일부 네트워크는 안전하지 않을 수 있습니다.

컴 ☐

내 연락처가 공유하는 네트워크에 자동으로 연결합니다.

컴 ☐

자동으로 핫스팟에 잠시 연결하여 유료 Wi-Fi 서비스를 사용할 수 있는지 확인합니다.

컴 ☐

전체 오류 및 진단 정보를 Microsoft에 보내세요.

컴 ☐



뒤로(B)

다음(N)

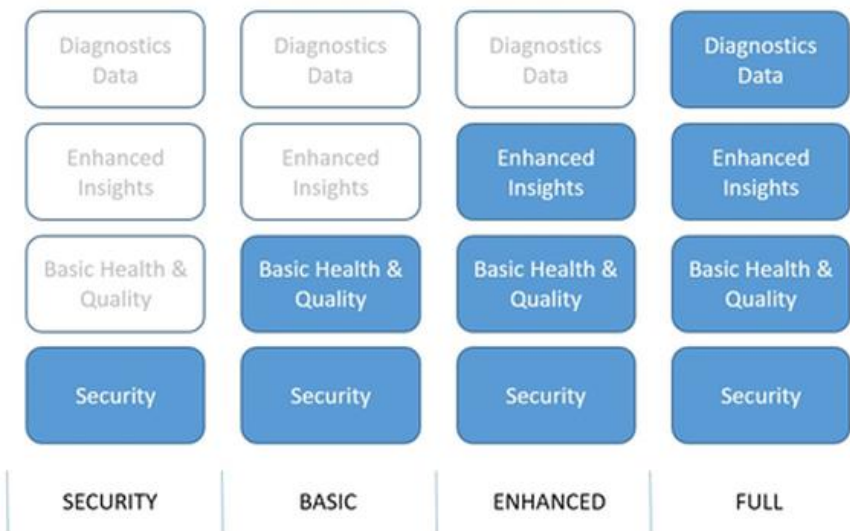


# 1. 텔레메트리?



## 윈도우 텔레메트리

- 사용자 환경의 데이터 수집 및 분석을 통해 더 나은 서비스를 제공하기 위한 목적
  - Microsoft에서 더 나은 서비스를 제공하기 위해 시스템과 사용자 경험 정보를 수집
    - ✓ 수집한 정보를 바탕으로 윈도우 업데이트, 보안 정책 업데이트 등의 서비스를 제공, 개선



[ 원격 분석 데이터의 수준별 분류 ]

데이터 범주	포함하는 정보
Security (보안)	연결된 사용자 환경 및 원격 분석 구성 요소 설정, 악성 소프트웨어 제거 도구 및 Windows Defender에 대한 정보
Basic (기본)	품질 관련 데이터, 앱 호환성, 앱 사용 현황 데이터, <i>보안</i> 수준의 데이터
Enhanced (고급)	앱이 사용된 방식과 수행 방식, 고급 안정성 데이터, <i>기본</i> 수준의 데이터
Full (전체) * 기본설정	문제를 식별하고 쉽게 해결하는 데 필요한 모든 데이터, <i>고급</i> 수준의 데이터

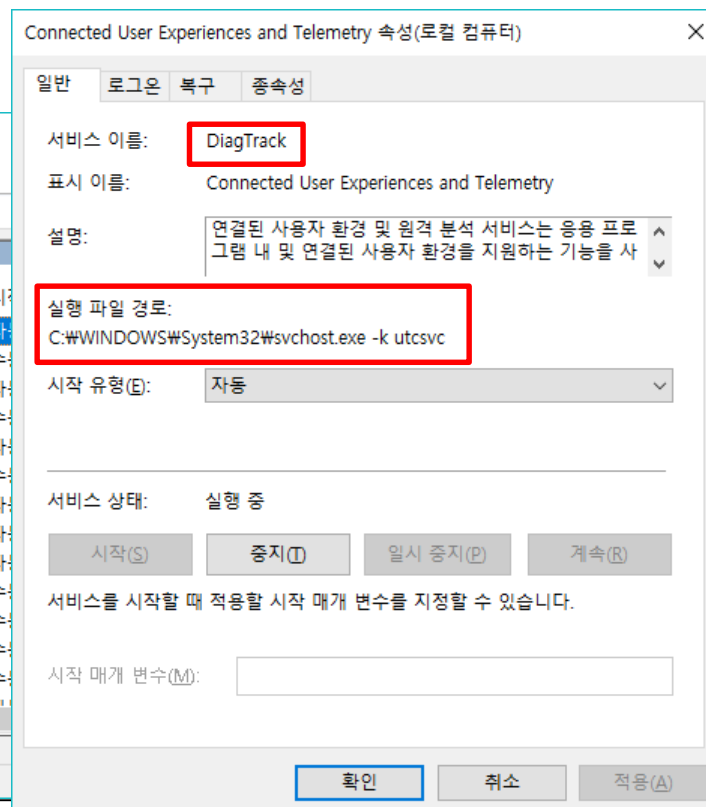
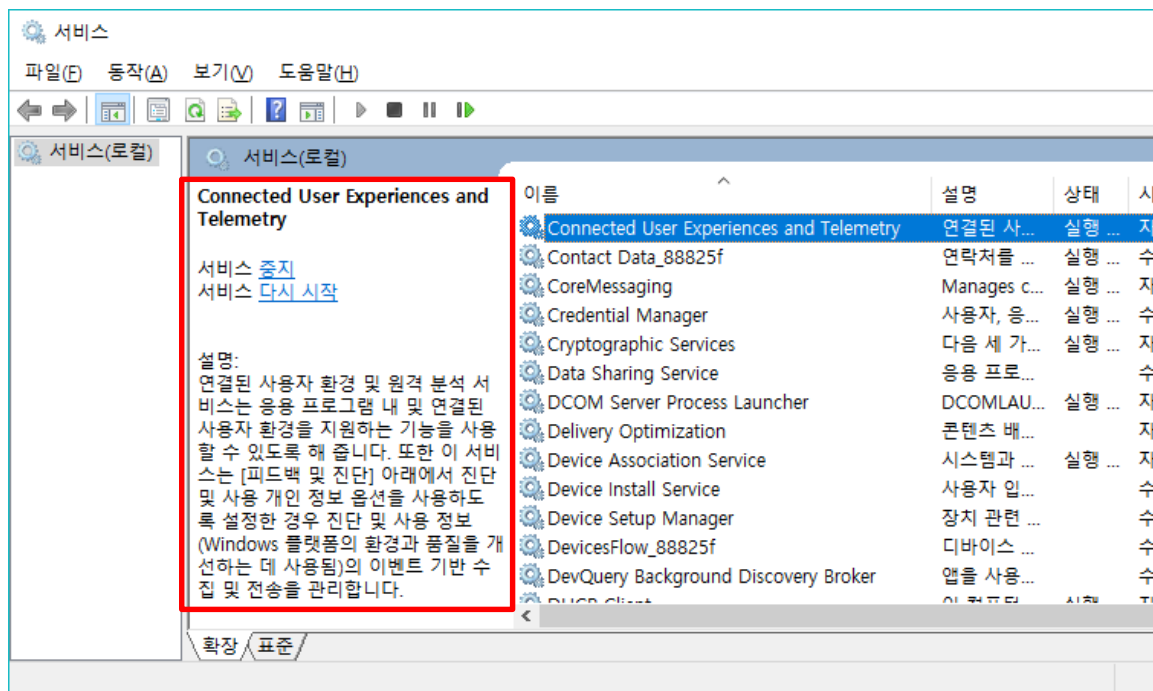
## 서비스 설정

### ■ DiagTrack 서비스에 의해 동작

- 로그파일 내용을 점검하는 동작 수행 (15분 또는 4시간 단위)

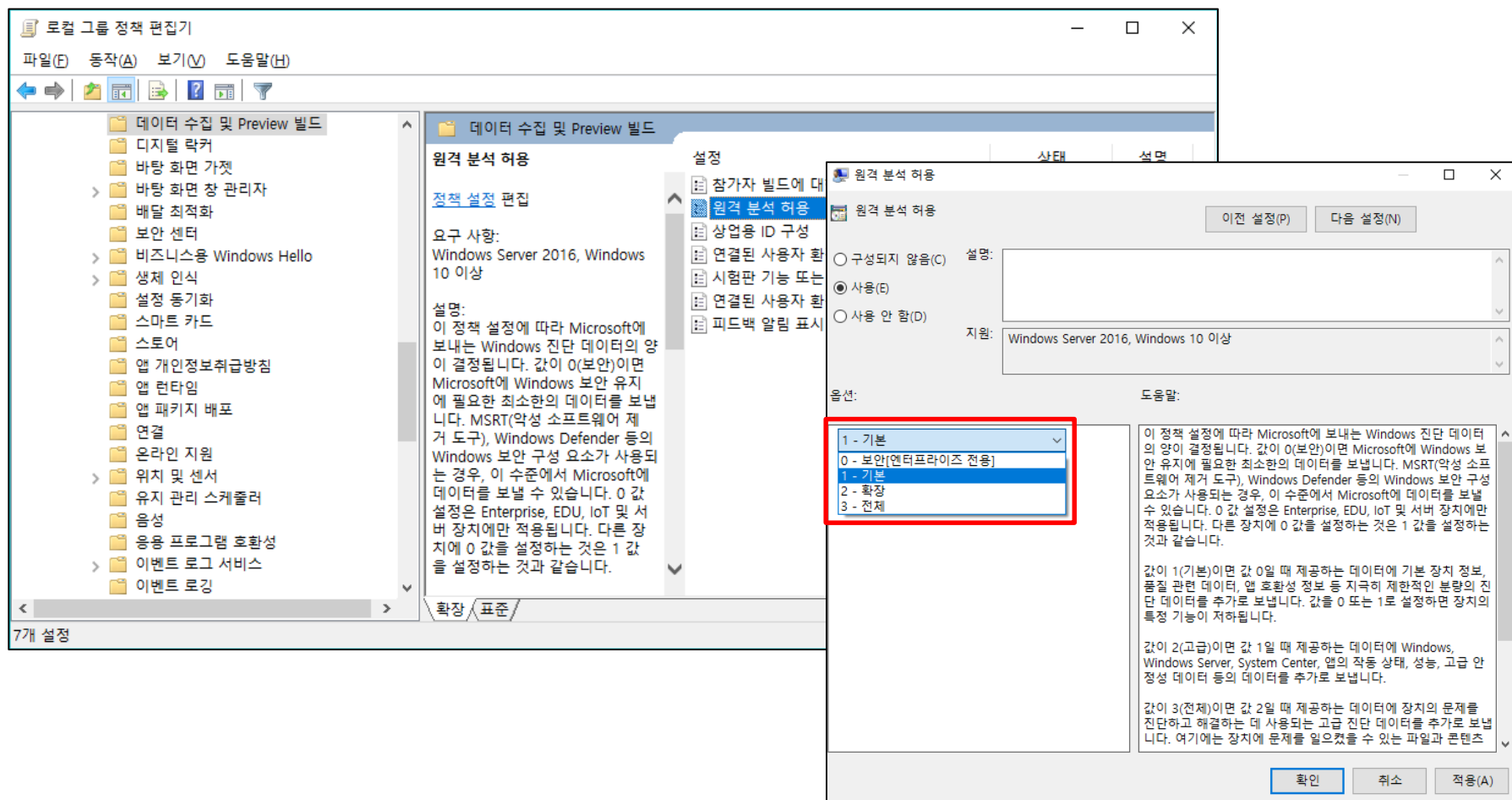
✓ 설정한 특정 이벤트가 발생하였는지를 확인하고 발생한 경우 로그파일을 수정

✓ 이벤트가 발생하지 않은 경우, 기존 로그파일 내용 유지



## 진단 데이터 설정

- 로컬 그룹 정책 편집기 ( gpedit.msc" ) > 컴퓨터 구성 > 관리 템플릿 > Windows 구성요소 > 데이터 수집 및 Preview 빌드 > 원격 분석 허용



The screenshot displays the 'Local Group Policy Editor' window. The left pane shows the tree structure: 'Computer Configuration' > 'Administrative Templates' > 'Windows Components' > 'Data Collection and Preview Builds' > 'Allow Remote Analysis'. The right pane shows the policy settings for '원격 분석 허용' (Allow Remote Analysis). The policy is set to '사용(E)' (Enabled). Below the policy settings, there is a dropdown menu for '옵션' (Options) with the following items: 1 - 기본 (Basic), 0 - 보안[엔터프라이즈 전용] (Security [Enterprise only]), 1 - 기본 (Basic), 2 - 확장 (Extended), and 3 - 전체 (Full). The '1 - 기본' option is selected and highlighted with a red box. The '도움말' (Help) section on the right provides detailed information about the policy settings and their impact on data collection.

**원격 분석 허용**

설정: **원격 분석 허용**

요구 사항: Windows Server 2016, Windows 10 이상

설명: 이 정책 설정에 따라 Microsoft에 보내는 Windows 진단 데이터의 양이 결정됩니다. 값이 0(보안)이면 Microsoft에 Windows 보안 유지에 필요한 최소한의 데이터를 보냅니다. MSRT(악성 소프트웨어 제거 도구), Windows Defender 등의 Windows 보안 구성 요소가 사용되는 경우, 이 수준에서 Microsoft에 데이터를 보낼 수 있습니다. 0 값 설정은 Enterprise, EDU, IoT 및 서버 장치에만 적용됩니다. 다른 장치에 0 값을 설정하는 것은 1 값을 설정하는 것과 같습니다.

옵션:

- 1 - 기본
- 0 - 보안[엔터프라이즈 전용]
- 1 - 기본
- 2 - 확장
- 3 - 전체

도움말:

이 정책 설정에 따라 Microsoft에 보내는 Windows 진단 데이터의 양이 결정됩니다. 값이 0(보안)이면 Microsoft에 Windows 보안 유지에 필요한 최소한의 데이터를 보냅니다. MSRT(악성 소프트웨어 제거 도구), Windows Defender 등의 Windows 보안 구성 요소가 사용되는 경우, 이 수준에서 Microsoft에 데이터를 보낼 수 있습니다. 0 값 설정은 Enterprise, EDU, IoT 및 서버 장치에만 적용됩니다. 다른 장치에 0 값을 설정하는 것은 1 값을 설정하는 것과 같습니다.

값이 1(기본)이면 값 0일 때 제공하는 데이터에 기본 장치 정보, 품질 관련 데이터, 앱 호환성 정보 등 지극히 제한적인 범위의 진단 데이터를 추가로 보냅니다. 값을 0 또는 1로 설정하면 장치의 특정 기능이 저하됩니다.

값이 2(고급)이면 값 1일 때 제공하는 데이터에 Windows, Windows Server, System Center, 앱의 작동 상태, 성능, 고급 안정성 데이터 등의 데이터를 추가로 보냅니다.

값이 3(전체)이면 값 2일 때 제공하는 데이터에 장치의 문제를 진단하고 해결하는 데 사용되는 고급 진단 데이터를 추가합니다. 여기에는 장치가 문제를 일으켰을 수 있는 파일과 콘텐츠



## Motivation

- 윈도우 텔레메트리 로그 파일이 전송하는 정확한 데이터는 무엇?
  - 운영체제가 동작하는 하드웨어 제원, 기동 시간, 설치된 앱, 시스템 이벤트 등 정보를 포함
    - ✓ 개인정보? 사용자 프라이버시? → 민감한 데이터 관리
  - 운영체제에서 원격 분석을 위한 데이터를 외부 서버로 전송 – MS 입장
- 새로운 아티팩트, 조사 과정에서 활용 가능성 파악

```
IP address: 111.221.29.253
ISP: Microsoft Corporation
Organization: Microsoft
City: Hong Kong
Country: Hong Kong (HK) 🇭🇰
Latitude: 22.2833
Longitude: 114.15
```

[ 윈도우 텔레메트리 데이터가 전송되는 주소 정보 ]

## 2. 데이터 수집 & 구조 분석

- 어떤 파일에 데이터가 저장되는가?
- rbs 파일 구조는?
- 담겨진 내용을 어떻게 보아야 할까?



### 데이터 수집

- 로그파일의 저장경로 : %ProgramData%\Microsoft\Diagnosis\\*.rbs
  - 윈도우 10부터 텔레메트리 기술 도입 (윈도우 7/8.1 버전에서 업데이트를 통해 적용 가능)

구 분	파일이름	파일크기(고정)
Windows 7 / 8.1	evnets00.rbs	24,576 KB
	evnets01.rbs	6,226 KB
	evnets10.rbs	492 KB
	evnets11.rbs	1,475 KB
Windows 10 : ~ver. 1511	evnets00.rbs	49,152 KB
	evnets01.rbs	12,452 KB
	evnets10.rbs	984 KB
	evnets11.rbs	2,950 KB
Windows 10 : ver. 1607~	Events_CostDeferred.rbs	6,554 KB
	Events_Normal.rbs	16,384 KB
	Events_NormalCritical.rbs	6,554 KB
	Events_Realtime.rbs	3,277 KB

\* events00 = Events\_Normal, events01 = Events\_NormalCritical, events10 = Events\_Realtime, events11 = Events\_CostDeferred



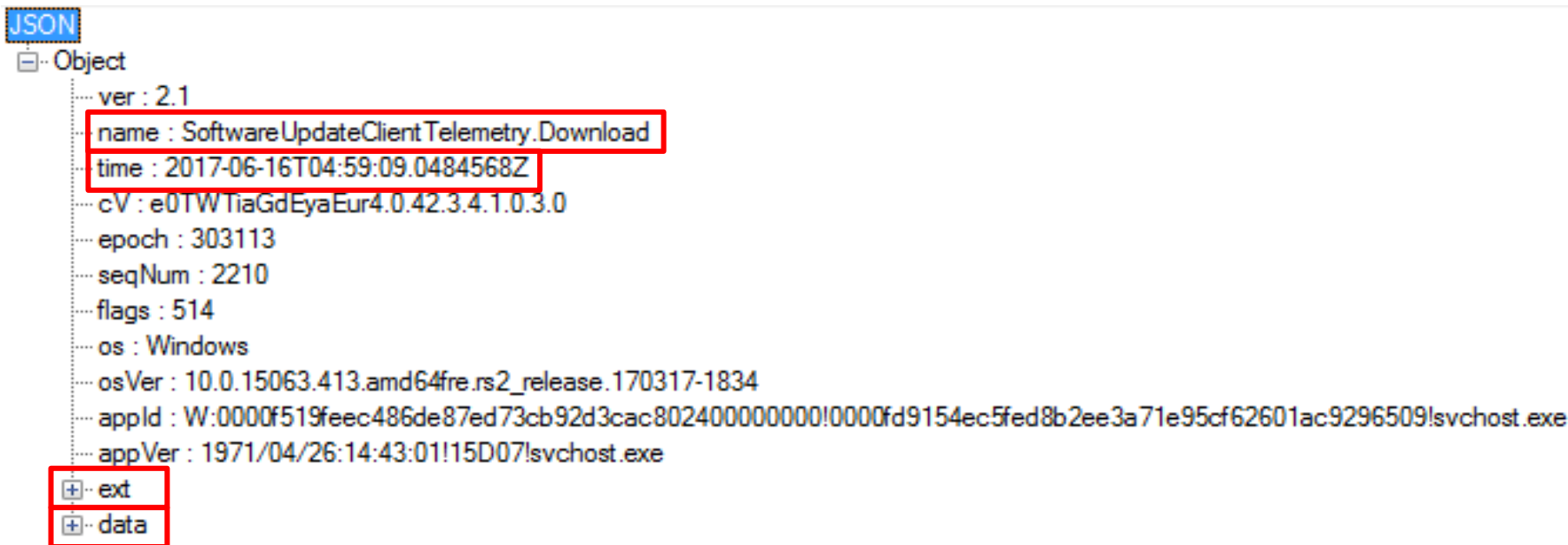
### rbs 파일의 특징

- rbs 파일의 크기는 고정되어 저장되고, 수정사항은 덮어 쓰여지는 방식으로 동작
  - 기록되는 원격 분석 데이터가 적을 경우, 0x00으로 초기화되어 저장
  - 원격 분석 데이터가 파일 크기보다 커질 경우, 파일 헤더 이후 부터 덮어 쓰여짐
    - ✓ 사용자에게 의해 파일을 삭제하기 위해서는 서비스를 종료시켜야 함(서비스 동작 중에는 접근 불가)
- 원격 분석 데이터 전송빈도는 전원 및 인터넷 연결 상태에 따라 다르게 동작
  - 외부 전원 및 유선 인터넷을 사용하는 경우 : 15분 단위로 전송
  - 내장 배터리 전력에 의존하는 노트북 기기의 경우 : 4시간 단위로 전송
  - 인터넷 연결이 제한되는 환경인 경우 : 전송되지 않음



### 텔레메트리 데이터 분석

- JSON 객체 형태의 문자열을 저장, 오브젝트의 태그로 데이터 구분
  - 237개의 "name" 확인 : Normal : 72개 / NormalCritical : 119개 / Realtime : 46개
  - "ext" - "utc", "app", "os", "device", "user" : 사용자 식별자
  - "data" - "name"에 따라 텔레메트리 데이터 저장



[ 데이터 청크의 데이터를 JSON 객체로 변환한 형태 ]



# 3. 분석결과 활용

- “data” 에는 어떤 내용이 있나?
- rbs 파일 분석이 유용할 수 있는 경우?
- 결론 & 향후연구



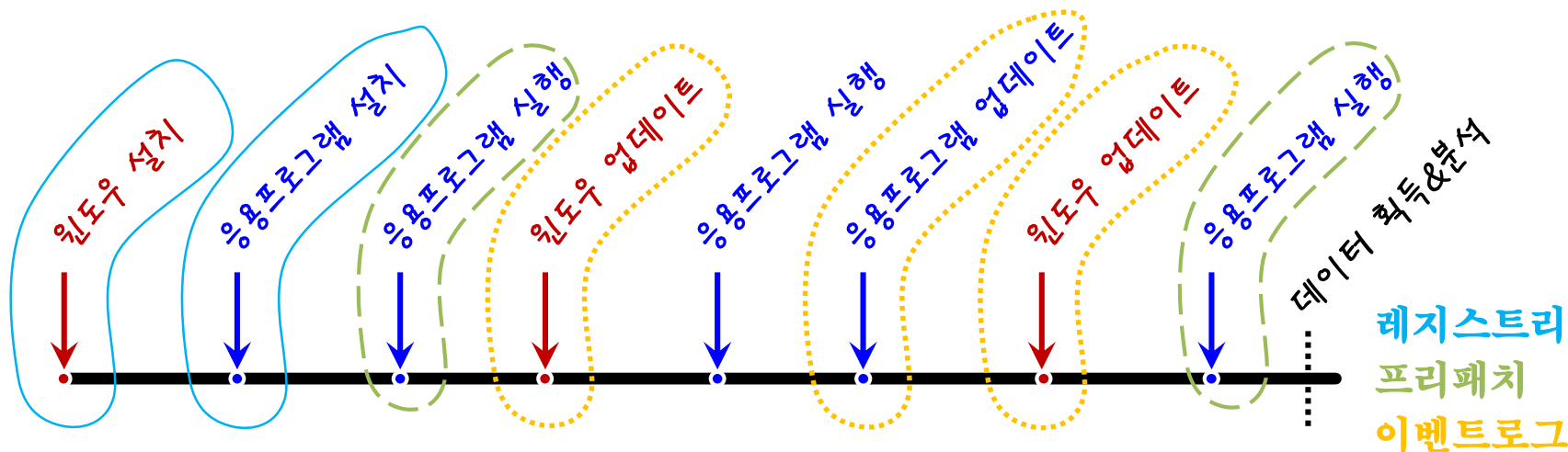
#### 텔레메트리에 포함된 정보

- 설치된 프로그램/업데이트 (~ 약 1년)
  - Windows defender
- 운영체제, 하드웨어 (~ 약 1년)
  - Device Census : 원격 측정 프레임워크
- 실행중인 프로세스/서비스(~ 약 1개월)
- 권한 상승, 사용자, 드라이버, 디스플레이, 오류 이벤트 등

```
{
  "ver": "2.1",
  "name": "Microsoft.Windows.Inventory.Core.InventoryApplicationAdd",
  "time": "2017-04-12T05:12:36.0404206Z",
  "epoch": "1105030",
  "seqNum": 9861,
  "flags": 257,
  "os": "Windows",
  "osVer": "10.0.14393.953.amd64fre.rs1_release.170303-1614",
  "appId": "W:0000f519feec486de87ed73cb92d3cac802400000000!000039e7d1f9",
  "appVer": "2040/03/24:07:52:12!1C0ED!compattelrunner.exe",
  "tags": {
    "BuildFlightId": "{52DCEEAF-E21F-4BAE-84F7-ACD07B725144}.200"
  },
  "ext": {
    "utc": {
      "cat": 140737488355328,
      "flags": 238027268
    },
    "device": {
      "localId": "s:4223EB89-7FD0-4AEF-8556-37BBE0883174",
      "deviceClass": "Windows.Desktop"
    },
    "user": {
      "localId": "w:B04E2543-63EB-D3C6-4722-FBFE64FA31C0"
    }
  },
  "data": {
    "InventoryVersion": "10014979",
    "ProgramInstanceId": "00003cac841794614daa926a5963f496acd61fd296cb",
    "Name": "VMware Workstation",
    "Publisher": "VMware, Inc.",
    "Version": "12.0.1",
    "Language": "1033",
    "Source": "Msi",
    "Type": "Application",
    "StoreAppType": "",
    "MsiProductCode": "{4b855f64-cb51-4fc3-935f-5af7d3372bde}",
    "MsiPackageCode": "{6B9345A5-CE1B-4BA2-849C-90B1B8B89660}",
    "HiddenArp": "",
    "OSVersionAtInstallTime": "10.0.0.14393",
    "PackageFullName": "",
    "RootDirPath": "%commonprogramfiles(x86)%\\thinprint\\tpprintticket.d",
    "InstallDate": "10/17/2014 04:18:34",
  }
}
```

#### 설치된 프로그램 / 업데이트, 운영체제 정보

- 레지스트리, 프리패치, 이벤트로그로부터 확인할 수 있는 데이터
  - 레지스트리 : 윈도우 설치시각, 설치된 응용프로그램 목록  
⇒ 삭제된 응용프로그램, 포터블SW, 윈도우 재설치
  - 프리패치 : 응용프로그램의 최초/마지막 실행시각, 실행횟수  
⇒ 사용시간 추정 가능, 프리패치 파일의 개수 제한, but 실행되었으나 파악되지 않을 가능성
  - 이벤트로그 : 윈도우 업데이트, timezone 변경 ⇒ 구체적인 변경내용 확인 가능
- *이력 확인, 안티-포렌식 행위에 의한 의도적인 데이터 조작의 흔적 확인 가능성*





#### 하드웨어 정보

- 메인보드, CPU, 메모리 - 용량, 스토리지 – 드라이브/파티션 정보 등
  - 분석용 저장장치(또는 이미지 파일)에서 획득할 수 없는 정보
  - WMI Command-Line Utility (wmic.exe) 에서 제공되는 정보
    - ✓ BIOS, SMBIOS(System Management BIOS)
- 시스템의 하드웨어가 교체될 경우,  
하드웨어 변경 이력 추적 가능
  - 저장장치 자체가 변경될 경우?

```
"data":{"ChassisType":3,
"ComputerHardwareID":{"7a5486ea-ebd5-55c3-924a-9fc36f885852"},
"DeviceColor":"#",
"DeviceName":"DESKTOP-GVEB19F",
"OEMDigitalMarkerFileName":"#",
"OEMManufacturerName":"ASUS",
"OEMModelNumber":"All Series",
"OEMModelName":"#",
"OEMModelSKU":"All",
"OEMModelBaseBoard":"Z87-PRO",
"OEMModelBaseBoardVersion":"Rev 1.xx",
"OEMModelSystemFamily":"ASUS MB",
"OEMModelSystemVersion":"System Version",
"OEMOptionalIdentifier":"#",
"OEMSerialNumber":"System Serial Number",
"PhoneManufacturer":"#",
"SoCName":"#",
"DUID":"#",
"InventoryId":{"17EEB331-5BBA-3ED3-E917-C824E999B228"},
"VoiceSupported":"PowerOff",
"PowerPlatformRole":1,
"TPMVersion":0,
"StudyID":0,
"TelemetryLevel":3,
"TelemetrySettingAuthority":2,
"DeviceForm":0,
"DigitizerSupport":0,
"ActiveMicCount":0}}
```

[ Census.Hardware ]



#### 실행중인 프로세스 / 서비스 정보

- 프로세스 이름, 프로세스가 동작하고 있는 상태에서 로그가 수집된 시간을 저장
  - 프로세스 정보를 얻기 위한 전제조건은 활성 시스템
    - ⇒ 분석용 저장장치(또는 이미지 파일)에서도 실행된 프로세스 정보 수집 가능
  
- 파일리스 공격 - 악성코드
  
- 사고 조사 – 침해사고, 감사, 불법도박 프로그램



#### 결론 & 향후연구

- 텔레메트리가 생성되어 있어야 함 (설정 - default)
  - 충분한 기록이 필요, 사용자 설정에 의해 비활성화
  - 활용 사례 부족, 분석기법 미비
  
- 디지털 포렌식 조사에서 활용될 수 있는 가치
  - 기존의 윈도우 아티팩트와 구별되는 정보를 포함 >>> 새로운 윈도우 아티팩트
  - 아티팩트 분석결과 신뢰성 강화, 인코딩 데이터 해석 >>> 향후 연구
  
- 분석도구 개발
  - Microsoft, Diagnostic Data Viewer

