

205 – Diagnosis

Team Information

Team Name : DogeCoin

Team Member : Dongbin Oh, Donghyun Kim, Donghyun Kim, Yeongwoong Kim

Email Address : dfc-dogecoin@naver.com

Instructions

Description Analyze the given file and answer the question.

Target	Hash (MD5)
Diagnosis.7z	C0656E8347E02E5E050A259C48FF74B7

Questions

1. On which system was the given file collected? (Model name) (10 points)
2. What is the time zone of the operating system installed on the system? (10 points)
3. What search engines did the user visit and what queries did the user entered using the Edge browser? (30 points)
4. List all programs installed on "2021-07-28" (UTC+0). (30 points)
5. List all wireless networks connected to the system. (50 points)
 - SSID
 - Authentication Algorithm
 - AP Manufacturer
 - AP Model Name
6. Identify the information of the external storage device mounted at "J:\". (70 points)
 - Manufacturer
 - Model

- Serial Number
- Volume Serial Number
- Volume Creation Time
- FileSystem
- Connected Date/Time
- Disconnected Date/Time

Teams must:

- Develop and document the step-by-step approach used to solve this problem to allow another examiner to replicate team actions and results.
- Specify all tools used in deriving the conclusion(s).

Tools used:

Name:	Python	Publisher:	Python Foundation
Version:	3.7.0		
URL:	https://www.python.org/		

Name:	pandas	Publisher:	Pandas
Version:	0.23.4		
URL:	https://pandas.pydata.org/		

Name:	SQLite Studio	Publisher:	Pawel Salawa
Version:	3.2.1		
URL:	https://sqlitestudio.pl/		

Name:	SQLite Expert Personal	Publisher:	Coral Creek Software
Version:	5.4.3.528		
URL:	http://www.sqliteexpert.com/download.html		

Step-by-step methodology:

I. 파일이 수집된 시스템 정보 (Model Name)

1. 분석 결과

[표 1] 시스템 정보

제조사	LG Electronics
모델명	17ZD90N-VX7BK
OS	Windows 10.0.19043.1110.amd64fre.vb_release.191206-1406

2. 분석 상세

Model 명이 기록된 파일을 찾기 위해 ProgramData\Microsoft\Diagnosis 경로에서 다음의 명령어를 사용하여 recursive 하게 grep 으로 model 이라는 문자열을 검색하였다.

[표 2] Model 명 탐색

```
ProgramData/Microsoft/Diagnosis$ grep -irn model
```

아래 세개의 파일이 매칭되었다.

- DownloadedSettings/telemetry.ASM-WindowsDefault.json
- EventTranscript/EventTranscript.db
- EventTranscript/EventTranscript.db-wal

이 중 EventTranscript/EventTrascript.db 는 sqlite3 database 파일로서, 크게 ①Browsing history, ②Device connectivity and configuration, ③Inking typing and speech utterance, ④ Product and service performance, ⑤Product and service usage, ⑥Software setup and inventory 등에 대한 진단데이터이다.

EventTranscript db 는 categories, events_persisted, event_categories, event_tags, producers, provider_groups, tag_descriptions 테이블로 구성되어 있다.

The screenshot shows a database interface with a schema tree on the left and a table view on the right. The schema tree includes tables like categories, events_persisted, event_categories, event_tags, producers, provider_groups, and tag_descriptions. The table view shows a table with columns: rowid, sid, timestamp, payload, and full_event_name. The data rows show various system events with timestamps and payloads.

[그림 1] EventTranscript.db events_persisted 테이블 일부

각 테이블의 스키마는 다음과 같다.

[표 3] categories 테이블

```
CREATE TABLE categories (
    category_id            INTEGER PRIMARY KEY AUTOINCREMENT,
    category_id_text       TEXT,
    producer_id            INTEGER,
    CONSTRAINT fk_producer_id
        FOREIGN KEY(producer_id)
        REFERENCES producers(producer_id)
    ON DELETE CASCADE);
```

[표 4] events_persisted 테이블

```
CREATE TABLE events_persisted (
    sid                    TEXT,
    timestamp              INTEGER,
    payload                TEXT,
    full_event_name        TEXT,
    full_event_name_hash   INTEGER,
    event_keywords         INTEGER,
    is_core                INTEGER,
    provider_group_id      INTEGER,
    logging_binary_name    TEXT,
    friendly_logging_binary_name TEXT,
    compressed_payload_size INTEGER,
    producer_id            INTEGER,
    extra1                 TEXT,
    extra2                 TEXT,
    extra3                 TEXT,
    FOREIGN KEY(provider_group_id) REFERENCES provider_groups(group_id),
    CONSTRAINT fk_producer_id
        FOREIGN KEY(producer_id)
        REFERENCES producers(producer_id)
    ON DELETE CASCADE);

CREATE INDEX idx_events_persisted_full_event_name_hash ON events_persisted(full_event_name_hash);

CREATE INDEX idx_events_persisted_logging_binary_name ON events_persisted(logging_binary_name);

CREATE INDEX idx_events_persisted_sid ON events_persisted(sid);

CREATE INDEX idx_events_persisted_timestamp ON events_persisted(timestamp);

CREATE INDEX idx_events_persisted_producer_id ON events_persisted(producer_id);
```

[표 5] event_categories 테이블

```
CREATE TABLE event_categories (
    full_event_name_hash      INTEGER,
    category_id               INTEGER,
    CONSTRAINT fk_category_id
        FOREIGN KEY(category_id)
        REFERENCES categories(category_id)
        ON DELETE CASCADE);

CREATE INDEX idx_event_categories_full_event_name_hash ON event_categories(full_event_name_hash);
```

[표 6] event_tags 테이블

```
CREATE TABLE event_tags (
    full_event_name_hash      INTEGER,
    tag_id                    INTEGER);

CREATE INDEX idx_event_tags_full_event_name_hash ON event_tags(full_event_name_hash);
```

[표 7] producers 테이블

```
CREATE TABLE producers (
    producer_id               INTEGER PRIMARY KEY AUTOINCREMENT,
    producer_id_text          TEXT);
```

[표 8] provider_groups 테이블

```
CREATE TABLE provider_groups (
    group_id                  INTEGER PRIMARY KEY AUTOINCREMENT,
    group_guid                 TEXT);
```

[표 9] tag_descriptions 테이블

```
CREATE TABLE tag_descriptions (
    tag_id                    INTEGER,
    locale_name               TEXT,
    tag_name                  TEXT,
    description                TEXT);
```

실제 진단 데이터는 events_persisted 테이블의 payload 칼럼에 기록되며, payload 칼럼은 json 형식으로 이루어진 데이터이다. 각 레코드는 full_event_name_hash 값을 가지고 있는데 이 값은 event_tags 테이블의 full_event_name_hash 값과 연결되어 있으며 각 full_event_name_hash 값은 tag_id 를 가진다. tag_id 는 tag_descriptions 테이블의 tag_id 와 연결되며 tag_name 값을 가진다. tag_name 은 ①Browsing history, ②Device connectivity and configuration, ③Inking typing and speech utterance, ④ Product and service performance, ⑤Product and service usage, ⑥Software setup and inventory 값 중 1개의 값을 가진다. 이 3 개의 칼럼을 연결함으로써 event_persisted 테이블의 각 레코드가 어떠한 성질의 데이터를 기록한 것인지 알 수 있다.

아래의 표는 events_persisted 테이블에서 row_id 가 1 인 레코드의 payload 를 추출한 것이다. OS 는 windows, 10.0.19043 버전을 사용하고 있으며 모델명은 LG Electronics 의 17ZD90N-VX7BK 임을 알 수 있다.

[표 10] row_id = 1 레코드

```
{
  "data": {
    "wilActivity": {
      "threadId": 1128
    }
  },
  "ext": {
    "app": {
      "asId": 2810,
      "id": "U:windows.immersivecontrolpanel_10.0.2.1000_neutral_neutral_cw5n1h2txyewy!microsoft.windows.immersivecontrolpanel",
      "ver": "10.0.2.1000_neutral_neutral!2009/09/05:02:35:46!1BCAE!systemsettings.exe"
    },
    "device": {
      "deviceClass": "Windows.Desktop",
      "localId": "s:CC7502F9-996D-4855-8CAE-EB0B86CB4E01"
    },
    "loc": {
      "tz": "+09:00"
    },
    "mscv": {
      "cV": "rX9qlaFrRk2jo603.1"
    },
    "os": {
      "bootId": 2,
      "name": "Windows",
      "ver": "10.0.19043.1110.amd64fre.vb_release.191206-1406"
    },
    "protocol": {
      "devMake": "LG Electronics",
      "devModel": "17ZD90N-VX7BK"
    },
    "user": {
      "localId": "w:CCC59980-EE80-654A-649E-0A2579080012"
    },
    "utc": {
      "aId": "B69FC98E-7D12-0002-D2FE-A0B6127DD701",
      "epoch": "303623",
      "eventFlags": 257,
      "flags": 205521456,
      "op": 1,
      "pgName": "WIN",
      "popSample": 2,
      "seq": 77160,
      "shellId": 33786497904279555
    }
  },
  "iKey": "o:0a89d516ae714e01ae89c96d185e9ae3",
  "name": "Microsoft.Windows.ShellExecute.ShellExecuteNormal",
  "time": "2021-07-26T12:40:08.0546621Z",
  "ver": "4.0"
}
```

II. 시스템에 설치된 OS 의 타임존

1. 분석 결과

[표 11] 시스템에 설치된 OS 의 타임존

타임존	UTC+9
-----	-------

2. 분석 상세

아래는 events_persisted 테이블에서 row_id 가 1 인 레코드의 payload 를 추출한 것이다. ext→loc→tz 필드에서 타임존을 기록하는데 해당 시스템의 타임존은 UTC+9 임을 확인할 수 있다. 그러나 데이터 영역에 기록된 타임스탬프들은 UTC 로 기록되는 점을 유의하여야 한다.

[표 12] row_id = 1 레코드

```
{
  "data": {
    "wilActivity": {
      "threadId": 1128
    }
  },
  "ext": {
    "app": {
      "asId": 2810,
      "id":
"U:windows.immersivecontrolpanel_10.0.2.1000_neutral_neutral_cw5n1h2txyewy!microsoft.windows.immersivecontrolpanel",
      "ver": "10.0.2.1000_neutral_neutral!2009/09/05:02:35:46!1BCAE!systemsettings.exe"
    },
    "device": {
      "deviceClass": "Windows.Desktop",
      "localId": "s:CC7502F9-996D-4855-8CAE-EB0B86CB4E01"
    },
    "loc": {
      "tz": "+09:00"
    },
    "mscv": {
      "cV": "rX9qlaFrRk2jo603.1"
    },
    "os": {
      "bootId": 2,
      "name": "Windows",
      "ver": "10.0.19043.1110.amd64fre.vb_release.191206-1406"
    },
    "protocol": {
      "devMake": "LG Electronics",
      "devModel": "17ZD90N-VX7BK"
    },
    "user": {
      "localId": "w:CCC59980-EE80-654A-649E-0A2579080012"
    },
    "utc": {
      "aId": "B69FC98E-7D12-0002-D2FE-A0B6127DD701",
      "epoch": "303623",
      "eventFlags": 257,
      "flags": 205521456,
      "op": 1,
      "pgName": "WIN",
      "popSample": 2,
      "seq": 77160,
      "shellId": 33786497904279555
    }
  },
  "iKey": "o:0a89d516ae714e01ae89c96d185e9ae3",
  "name": "Microsoft.Windows.ShellExecute.ShellExecuteNormal",
  "time": "2021-07-26T12:40:08.0546621Z",
  "ver": "4.0"
}
```

III. 사용자가 방문한 검색 엔진과 사용자가 Edge 브라우저에서 입력한 Query

1. 분석 결과

[표 13] 검색 엔진 및 입력 쿼리

검색엔진	Bing
검색한 쿼리	아이튠즈, itunes

2. 분석 상세

SQLite Studio 로 EventTranscript.db 를 EventTranscript.csv 파일로 Export 하고 Python Pandas 패키지로 CSV 파일을 불러온 후 아래의 분석을 진행하였다.

아래 쿼리를 사용하여 레코드 중 Payload 칼럼에 대소문자 구분 없이 edge.exe 라는 문자열을 포함하고 있는 레코드의 full_event_name 목록을 추출하였다.

[표 14] edge.exe 필터링

`df[df.payload.str.contains('(?!i)edge.exe')].full_event_name.unique()`
쿼리 결과 중 웹 브라우저 History 및 접근한 URL 과 가장 밀접한 관련이 있는 full_event_name 목록을 선별하였다.

```
In [10]: df[df.payload.str.contains('(?!i)edge.exe')].full_event_name.unique()

array(['Microsoft.Windows.TlgAggregateInternal.TlgAggregateSummary',
      'WinHTTP.Function call duration aggregate',
      'Microsoft.Windows.SRUM.Telemetry.AppTimelines',
      'Microsoft.Windows.Shell.DefaultAssoc.CreateAssociatedProcess',
      'Microsoft.Windows.WinRTClassActivation.WinRtClassActivationInfo',
      'Aria.218d658af29e41b6bc37144bd03f018d.Microsoft.WebBrowser.HistoryJournal.HJ_BeforeNavigateExtended',
      'Aria.218d658af29e41b6bc37144bd03f018d.Microsoft.WebBrowser.HistoryJournal.HJ_TabCreated',
      'Microsoft.Windows.Internal.UI.Shell.WindowTabManager.Telemetry.WindowTabAdded',
      'Aria.218d658af29e41b6bc37144bd03f018d.Microsoft.WebBrowser.HistoryJournal.HJ_HistoryAddUrl',
      'Aria.218d658af29e41b6bc37144bd03f018d.Microsoft.WebBrowser.HistoryJournal.HJ_NavigateCompleteExtended',
      'Aria.218d658af29e41b6bc37144bd03f018d.Microsoft.WebBrowser.HistoryJournal.HJ_HistoryAddUrlEx',
      'Aria.218d658af29e41b6bc37144bd03f018d.Microsoft.WebBrowser.HistoryJournal.HJ_PageContentInfo',
      'Microsoft.Windows.Audio.Client.AudioClientInitialize',
      'Microsoft.Windows.Audio.Client.AudioClientStart',
      'Aria.218d658af29e41b6bc37144bd03f018d.Microsoft.WebBrowser.HistoryJournal.HJ_NavigateElementClicked',
      'Microsoft.Windows.Audio.Client.AudioClientStop',
      'Aria.218d658af29e41b6bc37144bd03f018d.Microsoft.WebBrowser.HistoryJournal.HJ_W3cNavTiming',
      'Microsoft.Windows.Graphics.DXGI.SwapChainStatus',
      'Aria.ac270d3405274f1681e7e87dd04f8e71.Microsoft.WebBrowser.Protobuf.UKM.Aggregates'])
```

[그림 2] full_event_name 선별

아래 쿼리를 사용하여 events_persisted 테이블에서 위 full_event_name에 해당되는 레코드를 선별하였다.

[표 15] full_event_name 기반 필터링

```
df[df.full_event_name.str.contains('HistoryJournal.HJ_HistoryAddUrl') |
  df.full_event_name.str.contains('HistoryJournal.HJ_NavigateCompleteExtended') |
  df.full_event_name.str.contains('HistoryJournal.HJ_PageContentInfo') |
  df.full_event_name.str.contains('HistoryJournal.HJ_HistoryAddUrlEx')]
```


아래는 full_event_name 이

Aria.218d658af29e41b6bc37144bd03f018d.Microsoft.WebBrowser.HistoryJournal.HJ_NavigateCompleteExtended 인 레코드를 추출한 것이다.

Status code 와 접속한 URL, 사용한 브라우저를 확인할 수 있다.

[표 16] 웹 브라우저 및 방문 URL 정보

```
{
  "data": {
    "Channel": 4,
    "ConnectionType": "WiFi",
    "CorrelationGuid": "01ba288e-e14e-476f-9798-f10ca3f7f283",
    "EventInfo.Level": 3,
    "FrameId": 4,
    "HttpStatusCode": 200,
    "IsTopLevelUrl": 1,
    "NavigationSource": 6,
    "TabId": 7,
    "Timestamp": "2021-07-26T12:45:23.851Z",
    "client_id": 8704397619262087409,
    "navigationUrl": "https://www.bing.com/search?q=itunes&form=WNSGPH&qs=SW&cvid=0a7eac91c4df4ff68c64e4f42efe7e84&pq=itunes&cc=KR&setlang=ko-KR&nclid=CE795B408ASC29096A162D75A8006CFA&ts=1627303523490&nclids=1627303523&tsms=490&wso=Moderate",
    "navigationUrlRejectCode": 0,
    "payload_id": 8589934594,
    "pop_sample": 100,
    "refererUrl": "",
    "refererUrlRejectCode": 107,
    "utc_flags": 140737488355328
  },
  "ext": {
    "app": {
      "asId": 2154,
      "id": "W:00009ce8fe5883153d4c846d714e00df70c1000ffff!000003ce5e109186552778d6a9b918058f04dde1817e!msedge.exe",
      "name": "msedge",
      "ver": "2021/07/15:20:35:18!322807!msedge.exe"
    },
    "ariaMD": {
      "fields": [
        "n:Channel;t:2",
        "n:EventInfo.Level;t:2",
        "n:FrameId;t:2",
        "n:HttpStatusCode;t:2",
        "n:IsTopLevelUrl;t:1",
        "n:NavigationSource;t:2",
        "n:TabId;t:2",
        "n:client_id;t:2",
        "n:navigationUrlRejectCode;t:2",
        "n:payload_id;t:2",
        "n:pop_sample;t:3",
        "n:refererUrlRejectCode;t:2",
        "n:utc_flags;t:2"
      ]
    },
    "device": {
      "deviceClass": "Windows.Desktop",
      "localId": "s:CC7502F9-996D-4855-8CAE-EB0B86CB4E01"
    },
    "loc": {
      "tz": "+09:00"
    },
    "metadata": {
      "f": {
        "Channel": 4,
        "EventInfo.Level": 4,
        "FrameId": 4,
        "HttpStatusCode": 4,
        "NavigationSource": 4,
        "TabId": 4,
        "client_id": 4,
        "navigationUrlRejectCode": 4,
        "payload_id": 4,
        "pop_sample": 6,

```

```

        "refererRejectCode": 4,
        "utc_flags": 4
    },
    "privTags": 50331650
},
"net": {
    "cost": "Unmetered"
},
"os": {
    "bootId": 2,
    "name": "Windows",
    "ver": "10.0.19043.1110.amd64fre.vb_release.191206-1406"
},
"protocol": {
    "devMake": "LG Electronics",
    "devModel": "17ZD90N-VX7BK"
},
"utc": {
    "epoch": "303623",
    "eventFlags": 524546,
    "flags": 470286896,
    "pgName": "ARIA",
    "seq": 79558,
    "shellId": 33786497904279555
}
},
"iKey": "P-ARIA-218d658af29e41b6bc37144bd03f018d-6bd1d102-d792-414e-a9d8-315e766da244-7471",
"name":
"Aria.218d658af29e41b6bc37144bd03f018d.Microsoft.WebBrowser.HistoryJournal.HJ_NavigateCompleteExtended",
"time": "2021-07-26T12:45:38.6548463Z",
"ver": "4.0"
}

```

아래의 명령어를 사용하여 full_event_name 이

Aria.218d658af29e41b6bc37144bd03f018d.Microsoft.WebBrowser.HistoryJournal.HJ_NavigateCompleteExtended 인 레코드를 CSV 파일로 추출하였다.

[표 17] 레코드 추출 및 CSV 파일 추출

```

df[df.full_event_name.str.contains('HistoryJournal.HJ_NavigateCompleteExtended')]
.to_csv('./HJ_NavigateCompleteExtended.csv')

```

아래 코드를 사용, 추출한 CSV 파일에서 Timestamp 와 접속한 URL, Status Code, 사용한 브라우저명을 추출하여 CSV 파일로 저장하였다.

[표 18] CSV 파일에서 주요 정보 추출 및 재저장 코드

```

import json
import csv

with open("HJ_NavigateCompleteExtended.csv", "r", encoding='utf-8') as f:
    with open("url_extended.csv", "w", newline="") as wf:
        rdr = csv.reader(f)
        for line in rdr:
            data = line[2]
            if data == "payload":
                continue
            payload = json.loads(data)

            try:

```

```

wanted_data = ['Timestamp', 'navigationUrl', 'HttpStatusCode']
data_to_write = []
for d in wanted_data:
    print("{} : {}".format(d, payload['data'][d]))
    data_to_write.append(payload['data'][d])
print("browser : {}".format(payload['ext']['app']['name']))
print("-----")
data_to_write.append(payload['ext']['app']['name'])
csvwriter = csv.writer(wf)
csvwriter.writerow(data_to_write)
except:
    continue

```

아래 표는 추출한 내용이다.

[표 19] 사용자 방문 URL 및 사용 브라우저 정보

TimeStamp (UTC)	NavigatedUrl	Status code	Browser
2021-07-26T12:45:23.851Z	https://www.bing.com/search?q=itunes&form=WNSGPH&q=SW&cvid=0a7eac91c4df4ff68c64e4f42efe7e84&pq=itunes&cc=KR&setlang=ko-KR&nclid=CE795B408A5C29096A162D75A8006CFA&ts=1627303523490&nclids=1627303523&tsms=490&wso=Moderate	200	msedge
2021-07-26T12:45:25.242Z	https://login.microsoftonline.com/common/oauth2/authorize?client_id=9ea1ad79-fdb6-4f9a-8bc3-2b70f96e34c7&response_type=id_token+code&nonce=d1a2f7ad-6a72-4caa-b6a5-b0381518ebba&redirect_uri=https%3a%2f%2fwww.bing.com%2fforgid%2fidtoken%2fconditional&scope=openid&response_mode=form_post&msafed=0&prompt=none&state=%7b%22ig%22%3a%22BA1EBFOE378541D2B2D571F46F5F5DC7%22%7d	200	msedge
2021-07-26T12:45:25.362Z	https://www.bing.com/orgid/idtoken/conditional	200	msedge
2021-07-26T12:45:26.342Z	https://login.live.com/login.srf?wa=wsignin1.0&rpsnv=11&ct=1627303524&rver=6.0.5286.0&wp=MBI_SSL&wreply=https%3a%2f%2fwww.bing.com%2fsecure%2fPassport.aspx%3fpopup%3D1%26ssl%3D1&lc=1042&id=264960&checkda=1	-1	msedge
2021-07-26T12:45:26.356Z	https://www.bing.com/search?q=%ec%95%84%ec%9d%b4%ed%8a%a0%ec%a6%88&filters=dtbk:%22MCFvdmVydmlldyFvdmVydmlldyE2ZWYwMWUzYiO3YzBILWQ4YWItYWI5ZS03MmM2NDZiZjlxYTM%3d%22+sid:%2226ef01e3b-7c0e-d8ab-ab9e-72c646bf21a3%22+tpint:%22f%22&FORM=DEPNAV	200	msedge
2021-07-26T12:45:28.991Z	https://www.bing.com/newtabredir?url=https%3A%2F%2Fwww.apple.com%2Fkr%2Fitunes%2F	200	msedge
2021-07-26T12:45:29.366Z	https://www.apple.com/kr/itunes/	200	msedge
2021-07-26T12:45:33.527Z	https://www.microsoft.com/ko-kr/p/itunes/9pb2mz1zmb1s?cid=appledotcom&rtc=1	200	msedge
2021-07-26T12:45:34.731Z	https://mscom.demdex.net/dest5.html?d_nsld=0#https%3A%2F%2Fwww.microsoft.com	200	msedge
2021-07-26T12:45:37.185Z	https://www.microsoft.com/ko-kr/p/onerf/MeSilentPassport?SilentAuth=1	200	msedge
2021-07-26T12:45:43.139Z	https://fpt.microsoft.com/tags?session_id=8db96c74-7d05-404e-8409-b3b5142a6ec1	200	msedge

2021-07-26T12:45:44.105Z	https://fpt2.microsoft.com/Clear.HTML?ctx=Ls1.0&session_id=8db96c74-7d05-404e-8409-b3b5142a6ec1&id=10c75934-6671-68e0-260c-494e67e26943&w=8D9503347F6781E&tk=H3ihr9e92IdW6yd1ZgQ9SxSk4vLz7GBD1517G7IdE7hDzJaqpSADPXDzBnd%252fVFQ9islnSQAzHyH%252fbfrr7X4iYsQ6PeDE4yI6wssSRUegCeVvyxrzx6mLFzh6dFDpYwJ6L35Ze7EZAf9Pf5vExbXdDNEgtxhttiPo17dlvTrsaNNXXpmb%252fyqksLBbbyceewUnqFEuwMICRlcWP4z586ci5J6MES8uyQwclwXfboHNtfHI3mzRJ%252bZuA%252bZqv3pJTqkfjdCPNJ%252fElXwdR6nMr19JXzCPZFuM5CAe4cxKr7M%253d&CustomerId=02C58649-E822-405B-B6C3-17A7509D2FCC	200	msedge
2021-07-26T12:45:44.548Z	https://fpt2.microsoft.com/Clear.PNG?ctx=Wlcb1.0&session_id=8db96c74-7d05-404e-8409-b3b5142a6ec1&tk=H3ihr9e92IdW6yd1ZgQ9SxSk4vLz7GBD1517G7IdE7hDzJaqpSADPXDzBnd%252fVFQ9islnSQAzHyH%252fbfrr7X4iYsQ6PeDE4yI6wssSRUegCeVvyxrzx6mLFzh6dFDpYwJ6L35Ze7EZAf9Pf5vExbXdDNEgtxhttiPo17dlvTqFDcwvzAB1Jo6MNfmdgL5SOQ9NTVZSRCs8vYFj%2bRuxVrDFLlzdgdHgh%2bgy0aVa4FBjeD3aKngLJedhYEJGhwDBaBelWkFZStwYcx81TGKMhUT2YoqdPU5ZsmBsEanzvw%3d	200	msedge
2021-07-28T06:39:10.957Z	https://support.microsoft.com/ko-kr/topic/windows-%EA%B8%B0%EB%B0%98-%ED%94%84%EB%A1%9C%EA%B7%B8%EB%9E%A8%EC%97%90%EC%84%9C-%EB%8F%84%EC%9B%80%EB%A7%90%EC%9D%84-%EC%97%AC%EB%8A%94-%EC%A4%91-%EC%98%A4%EB%A5%98-%EB%B0%9C%EC%83%9D-%EA%B8%B0%EB%8A%A5-%ED%8F%AC%ED%95%A8-%EC%95%88-%EB%90%A8-%EB%98%90%EB%8A%94-%EB%8F%84%EC%9B%80%EB%A7%90-%EC%A7%80%EC%9B%90-%EC%95%88-%EB%90%A8-3c841463-d67c-6062-0ee7-1a149da3973b	200	msedge
2021-07-28T06:39:11.767Z	https://login.microsoftonline.com/common/oauth2/v2.0/authorize?client_id=ee272b19-4411-433f-8f28-5c13cb6fd407&redirect_uri=https%3A%2F%2Fsupport.microsoft.com%2Fsignin-oidc&response_type=code%20id_token&scope=openid%20profile%20offline_access&response_mode=form_post&nonce=637630511516605649.NTU2YzkWOGitNTEyS00NzE5LWJiYjEtM2RjZjU4NDRhMzhiNjA2MGM1OTAtNmZhMy00NzI1LTk4MjctMWUyMjRiOTZmMDUz&prompt=none&state=CfDJ8GCh8YXpXDvDoVtoijOGOA35xxuOChZjvXpy4tpZGiD6AcfgxzfK8XqJRG07j1MsAXgFPh5u70p7c-LfFsdYhfr4V-k6BTNhP9p-RjeXliVqJ1xgK5SOdn6o0hBSX2VypCQYjyOX-VM-TKzUUIMQ5s62YzYVUgljgJt6X_i58ES-pG0aImb8rW9EJncPbzOJAu2oNg1771J2NT-USD4GmuCWJw1QHAnDMbycb2-wOsz-7V4ft6ImKPDJmpcqdO7yInAczP0bc-jt7hf8SH3PrGpC_AYA-lhnUJHmHRInBaVYAVgMY2qLiFrezw67TznkvMOCLlZaEYJM_pAUXazqH6-3KhME14qSRBs1reivCb&x-client-SKU=ID_NETSTANDARD2_0&x-client-ver=6.7.1.0	200	msedge
2021-07-28T06:39:12.513Z	https://login.live.com/Me.htm?v=3	200	msedge
2021-07-28T06:39:12.677Z	https://support.microsoft.com/ko-kr/silentsigninhandler	200	msedge
2021-07-28T06:39:14.663Z	https://ntp.msn.com/edge/ntp?locale=ko&title=%EC%83%88%20%ED%83%AD&dsp=1&sp=Bing&query=enterprise&prerender=1	200	msedge

노란색으로 표시한 URL 의 구조를 분석해보면 사용자는 Bing 검색엔진을 사용했다. 또한 search?q=다음의 키워드가 입력한 검색어를 의미하므로 사용자가 입력한 검색어는 itunes 와 아이튠즈라는 것을 알 수 있다.

[표 20] 검색 관련 URL

<https://www.bing.com/search?q=itunes&form=WNSGPH&q=SW&cvid=0a7eac91c4df4ff68c64e4f42efe7e84&pg=itunes&cc=KR&setlang=ko-KR&ncld=CE795B408A5C29096A162D75A8006CFA&ts=1627303523490&ncldts=1627303523&tsms=490&wss=Moderate>

<https://www.bing.com/search?q=%ec%95%84%ec%9d%b4%ed%8a%a0%ec%a6%88&filters=dtbk:%22MCFvdmVydmlldyFvdmVydmlldyE2ZWYwMWUzYi03YzB1LWQ4YWItYWl5ZS03MmM2NDZiZjIxYTM%3d%22+sid:%226ef01e3b-7c0e-d8ab-ab9e-72c646bf21a3%22+tpint:%22f%22&FORM=DEPNAV>

Input
<code>=%ec%95%84%ec%9d%b4%ed%8a%a0%ec%a6%88</code>

Output
=아이튠즈

[그림 3] URL 디코딩 결과

IV. 2021-07-28 (UTC+0) 에 설치된 프로그램

1. 분석 결과

[표 21] 2021-07-28 (UTC+0) 에 설치된 프로그램 목록

Name	Version	설치 일자	Root Directory
HashTab	6.0.0.34	2021/07/28	%ProgramFiles%\\hashtab shell extension

2. 분석 상세

프로그램이 설치되면 full_event_name 이 Microsoft.Windows.Inventory.Core.InventoryApplicationAdd 인 레코드가 기록된다. 설치 날짜와 설치 프로그램의 이름, 설치 프로그램의 Root Directory, 설치 방법(ARP, Msi 등)을 포함한 여러 정보가 기록되며 설치 시간은 UTC 로 기록된다.

아래 쿼리를 사용하여 full_event_name 이 Microsoft.Windows.Inventory.Core.InventoryApplicationAdd 인 레코드를 선별하여 csv 파일로 추출하였다.

[표 22] full_event_name 기반 필터

```
df[df.full_event_name ==  
"Microsoft.Windows.Inventory.Core.InventoryApplicationAdd"].to_csv("./InventoryApplicati  
onAdd.csv")
```

아래 코드를 사용하여 2021/07/28 에 설치된 프로그램을 선별하였다.

[표 23] 일자 기반 선별 코드 (2021/07/28)

```
import json  
import csv  
from pprint import pprint  
  
with open("InventoryApplicationAdd.csv", "r", encoding='utf-8') as f:  
    rdr = csv.reader(f)  
    for line in rdr:  
        data = line[2]  
        if data == "payload":  
            continue  
        payload = json.loads(data)  
        try:  
            wanted_data = ['InstallDate', 'RootDirPath', 'Name']  
            for d in wanted_data:  
                if '07/28/2021' in payload['data'][d]:  
                    print("{} : {}".format(d, payload['data'][d]))  
            print("=====")  
        except:  
            continue
```

선별된 프로그램은 HashTab 과 FTK Imager 로, 각각의 정보는 다음과 같다.

[표 24] HashTab

```
{
  "data": {
    "HiddenApp": "false",
    "InstallDate": "07/28/2021 07:01:08",
    "InstallDateArPlastModified": [],
    "InstallDateFromLinkFile": [],
    "InstallDateMsi": [],
    "InventoryVersion": "10019645",
    "Language": 65535,
    "MsiPackageCode": "",
    "MsiProductCode": "",
    "Name": "HashTab 6.0.0.34",
    "OSVersionAtInstallTime": "10.0.0.19043",
    "PackageFullName": "",
    "ProgramInstanceId": "0000cd6179bddfc138a91da14124b64f64ff7cc80bd6",
    "Publisher": "Implbits Software",
    "RootDirPath": "%ProgramFiles%\\hashtab shell extension",
    "Source": "AddRemoveProgram",
    "StoreAppType": "",
    "Type": "Application",
    "Version": "6.0.0.34",
    "baseData": {
      "action": 1,
      "inventoryId": "{BBCC8C4A-6840-C58C-09CD-6C1409FEDA88}",
      "objectInstanceId": "000014f947eb49f9fbd2a869b233226a3aa20000ffff",
      "objectType": "InventoryApplication",
      "syncId": "{b792a6e9-794f-4e3b-9440-82bfcdcfb1342}"
    },
    "baseType": "Ms.Device.DeviceInventoryChange"
  },
  "ext": {
    "app": {
      "asId": 228,
      "id":
        "W:0000f519feec486de87ed73cb92d3cac80240000000!0000010db07461e45b41c886192df6fd425ba8d42d82!svchost.exe",
      "ver": "1972/12/14:16:22:50!1C364!svchost.exe"
    },
    "device": {
      "deviceClass": "Windows.Desktop",
      "localId": "s:CC7502F9-996D-4855-8CAE-EB0B86CB4E01"
    },
    "loc": {
      "tz": "+09:00"
    },
    "metadata": {
      "f": {
        "baseData": {
          "f": {
            "action": 2
          }
        }
      }
    },
    "privTags": 2147485696
  },
  "mscv": {
    "cV": "DjF+h6lX0EiNW9xb.0"
  },
  "os": {
    "bootId": 5,
    "name": "Windows",
    "ver": "10.0.19043.1110.amd64fre.vb_release.191206-1406"
  },
  "protocol": {
    "devMake": "LG Electronics",
    "devModel": "17ZD90N-VX7BK"
  },
  "user": {
    "localId": "w:CCC59980-EE80-654A-649E-0A2579080012"
  }
}
```

```

    },
    "utc": {
      "epoch": "600060",
      "eventFlags": 258,
      "flags": 503317040,
      "pgName": "WINCORE",
      "seq": 73482
    }
  },
  "iKey": "o:0a89d516ae714e01ae89c96d185e9ae3",
  "name": "Microsoft.Windows.Inventory.Core.InventoryApplicationAdd",
  "time": "2021-07-28T07:01:10.6970789Z",
  "ver": "4.0"
}

```

[표 25] FTK Imager

```

{
  "data": {
    "HiddenApp": "false",
    "InstallDate": "07/28/2021 00:00:00",
    "InstallDateArpLastModified": [],
    "InstallDateFromLinkFile": [],
    "InstallDateMsi": [],
    "InventoryVersion": "10019645",
    "Language": 1033,
    "MsiPackageCode": "{3414721F-080F-4E91-B4A1-7873CD1F7624}",
    "MsiProductCode": "{658081EA-E8FE-4E97-AF85-AF5F9E0A7848}",
    "Name": "AccessData_FTK_Imager",
    "OSVersionAtInstallTime": "10.0.0.19043",
    "PackageFullName": "",
    "ProgramInstanceId": "",
    "Publisher": "AccessData",
    "RootDirPath": "%ProgramFiles%\\accessdata\\",
    "Source": "Msi",
    "StoreAppType": "",
    "Type": "Application",
    "Version": "4.5.0.3",
    "baseData": {
      "action": 1,
      "inventoryId": "{BBCC8C4A-6840-C58C-09CD-6C1409FEDA88}",
      "objectInstanceId": "0000c78006b910b77c1883334d869aa6853e00000904",
      "objectType": "InventoryApplication",
      "syncId": "{b792a6e9-794f-4e3b-9440-82bfcdfb1342}"
    },
    "baseType": "Ms.Device.DeviceInventoryChange"
  },
  "ext": {
    "app": {
      "asId": 3630,
      "id":
        "W:0000f519feec486de87ed73cb92d3cac80240000000!0000b4108c1d6832f0d036eedcd3d2f684d43be04996!compattelrunner.exe",
      "ver": "2038/11/30:03:05:59!3244C!compattelrunner.exe"
    },
    "device": {
      "deviceClass": "Windows.Desktop",
      "localId": "s:CC7502F9-996D-4855-8CAE-EB0B86CB4E01"
    },
    "loc": {
      "tz": "+09:00"
    },
    "metadata": {
      "f": {
        "baseData": {
          "f": {
            "action": 2
          }
        }
      }
    }
  }
}

```



```

    },
    "privTags": 2147485696
  },
  "mscv": {
    "cV": "ARcuwCH+xEKX4nZl.0"
  },
  "os": {
    "bootId": 5,
    "name": "Windows",
    "ver": "10.0.19043.1110.amd64fre.vb_release.191206-1406"
  },
  "protocol": {
    "devMake": "LG Electronics",
    "devModel": "17ZD90N-VX7BK"
  },
  "user": {
    "localId": "w:CCC59980-EE80-654A-649E-0A2579080012"
  },
  "utc": {
    "epoch": "600060",
    "eventFlags": 258,
    "flags": 503317040,
    "pgName": "WINCORE",
    "seq": 73633
  }
},
"iKey": "o:0a89d516ae714e01ae89c96d185e9ae3",
"name": "Microsoft.Windows.Inventory.Core.InventoryApplicationAdd",
"time": "2021-07-28T07:02:10.5808169Z",
"ver": "4.0"
}

```

InstallDate 필드가 설치 날짜를 기록하는데, MSDN 에 따르면 폴더 생성 날짜 추론에 따른 가장 가능성이 높은 추측으로 기록된다고 한다.¹

선별된 프로그램에 대하여 추가적인 기록이 있는지 분석하였다. HashTab 은 2021-07-28 이전의 기록이 없었으나 FTK 는 2021-07-27 에 설치 관련 기록이 발견되었다.

[표 26] Microsoft.Windows.Darwin.MsiInstallProduct

```

{
  "data": {
    "Language": "1033",
    "Manufacturer": "AccessData",
    "PackageName": "AccessData_FTK_Imager_(x64).msi",
    "ProductCode": "{658081EA-E8FE-4E97-AF85-AF5F9E0A7848}",
    "ProductName": "AccessData FTK Imager",
    "Status": "0",
    "Version": "4.5.0.3"
  },
  "ext": {
    "app": {
      "asId": 831,
      "id":
"W:0000f519feec486de87ed73cb92d3cac80240000000!00005d6102f5a170e982c7735bfc2b9c1a0a0d435fd1!msiexec.exe",
      "ver": "2042/10/02:20:16:28!18AED!msiexec.exe"
    }
  }
}

```

¹ <https://docs.microsoft.com/ko-kr/windows/privacy/basic-level-windows-diagnostic-events-and-fields-1703>

```

    },
    "device": {
      "deviceClass": "Windows.Desktop",
      "localId": "s:CC7502F9-996D-4855-8CAE-EB0B86CB4E01"
    },
    "loc": {
      "tz": "+09:00"
    },
    "os": {
      "bootId": 5,
      "name": "Windows",
      "ver": "10.0.19043.1110.amd64fre.vb_release.191206-1406"
    },
    "protocol": {
      "devMake": "LG Electronics",
      "devModel": "17ZD90N-VX7BK"
    },
    "user": {
      "localId": "w:CCC59980-EE80-654A-649E-0A2579080012"
    },
    "utc": {
      "epoch": "600060",
      "eventFlags": 257,
      "flags": 205521456,
      "pgName": "WIN",
      "popSample": 2,
      "seq": 23766,
      "shellId": 33786497904279555
    }
  },
  "iKey": "o:0a89d516ae714e01ae89c96d185e9ae3",
  "name": "Microsoft.Windows.Darwin.MsiInstallProduct",
  "time": "2021-07-27T16:23:11.0842348Z",
  "ver": "4.0"
}

```

Microsoft.Windows.Inventory.Core.InventoryApplicationAdd 이벤트에 기록된 설치 방법과 같이 .msi 로 설치된 FTK Imager 의 흔적을 발견할 수 있었다. 해당 기록은 2021-07-27 16:23:11 에 기록되었다. 추측으로 기록되는 Microsoft.Windows.Inventory.Core.InventoryApplicationAdd 이벤트보다 명시적으로 시각이 기록되는 Microsoft.Windows.Darwin.MsiInstallProduct 이벤트에 근거하여 설치 시각을 판단하였다. 따라서 FTK Imager 는 2021-07-27 에 설치되었다. 결론적으로 2021-07-28 에 설치된 프로그램은 HashTab 뿐이다.

V. 시스템에 연결된 무선 네트워크

1. 분석 결과

[표 27] 시스템에 연결된 무선 네트워크 목록

SSID	JK's iPhone
Authentication Algorithm	WPA2-Personal
AP Manufacturer	Apple
AP Model Name	BroadCom Chipset

SSID	SSOL_5G
Authentication Algorithm	WPA2-Personal
AP Manufacturer	ASUSTek Computer Inc.
AP Model Name	RT-AC58U

SSID	KT_GiGA_5G_Wave2_6E0B
Authentication Algorithm	WPA2-Personal
AP Manufacturer	Mercury Co.
AP Model Name	KM08-708H

SSID	iptime
Authentication Algorithm	Open
AP Manufacturer	Realtek Semiconductor Corp.
AP Model Name	RTL8xxx

SSID	iptime
Authentication Algorithm	Open
AP Manufacturer	-
AP Model Name	BroadCom Chipset

2. 분석 상세

무선 네트워크 연결 성공 시 Microsoft.OneCore.NetworkingTriage.GetConnected.WiFiConnectedEvent 레코드가 기록된다. 아래 표는

Microsoft.OneCore.NetworkingTriage.GetConnected.WiFiConnectedEvent 레코드의 예시이다. Ap의 manufacturer와 Model name, Authentication Algorithm, SSID 정보가 기록되는 것을 확인할 수 있다.

[표 28] 무선 네트워크 연결 성공 로그 데이터

```
{
  "data": {
    "apCountOnSSID": 1,
    "apDescription": "00904C",
    "apManufacturer": "Apple",
    "apMaxChannelWidth": 80,
    "apModelName": "BroadCom Chipset",
    "apModelNum": "",
    "apPhyType": "802.11ax",
    "assocDuration": 281,
    "assocRestartCount": 0,
    "associationCount": 1,
    "authAlgo": "WPA2-Personal",
    "authDuration": 0,
    "authRestartCount": 1,
    "bssid": "BE:EE:83:B0:FC:E2",
    "channelFrequency": 5745,
    "channelNumber": 149,
    "cipherAlgo": "AES-CCMP",
    "detailedStatusCode": "0x0 ( DOT11_ASSOC_STATUS_SUCCESS )",
    "eapType": 4294967295,
    "eventSource": "WiFi",
    "eventType": "Manual",
    "firstBSSID": "BE:EE:83:B0:FC:E2",
    "firstDetailedStatusCode": "0x0 ( DOT11_ASSOC_STATUS_SUCCESS )",
    "interfaceDescription": "Intel(R) Wi-Fi 6 AX201 160MHz",
    "interfaceGuid": "7F08A4CA-3246-4F4D-AA02-FE5135F63D24",
    "interfaceType": "WiFi",
    "interferingAPCount": 4,
    "isAUserLoggedIn": true,
    "isHidden": false,
    "isWDI": true,
    "oneXAuthMode": "None",
    "rssi": -50,
    "rxRate": 1500,
    "signalQualityPercentage": 91,
    "ssid": "JK's iPhone",
    "totalVisibleAPCount": 16,
    "txRate": 1500,
    "wlanStatusCode": "0x0 = 작업이 성공했습니다. "
  },
  "ext": {
    "app": {
      "asId": 40,
      "id":
        "W:000f519feec486de87ed73cb92d3cac8024000000!000010db07461e45b41c886192df6fd425ba8d42d82!svchost.exe",
      "ver": "1972/12/14:16:22:50!1C364!svchost.exe"
    },
    "device": {
      "deviceClass": "Windows.Desktop",
      "localId": "s:CC7502F9-996D-4855-8CAE-EB0B86CB4E01"
    },
    "loc": {
      "tz": "+09:00"
    },
    "metadata": {
```

```

        "f": {
            "interfaceGuid": 8,
            "rssi": 2,
            "signalQualityPercentage": 2
        },
        "privTags": 2048
    },
    "os": {
        "bootId": 2,
        "name": "Windows",
        "ver": "10.0.19043.1110.amd64fre.vb_release.191206-1406"
    },
    "protocol": {
        "devMake": "LG Electronics",
        "devModel": "17ZD90N-VX7BK"
    },
    "user": {
        "localId": "w:CCC59980-EE80-654A-649E-0A2579080012"
    },
    "utc": {
        "epoch": "303623",
        "eventFlags": 257,
        "flags": 206045744,
        "pgName": "WIN",
        "popSample": 2,
        "seq": 78808
    }
},
"iKey": "o:0a89d516ae714e01ae89c96d185e9ae3",
"name": "Microsoft.OneCore.NetworkingTriage.GetConnected.WiFiConnectedEvent",
"time": "2021-07-26T12:45:25.0992632Z",
"ver": "4.0"
}

```

아래 쿼리를 사용하여 full_event_name 이

Microsoft.OneCore.NetworkingTriage.GetConnected.WiFiConnectedEvent 인 레코드만 선별하여 csv 파일로 추출하였다.

[표 29] 레코드 선별

```
df[df.full_event_name.str.contains("Microsoft.OneCore.NetworkingTriage.GetConnected.WiFiConnectedEvent")].to_csv("./wifi_connected_event.csv")
```

아래 코드를 사용하여 payload 에서 ssid, interfaceType, authAlgo, apManufacturer, apModelName 정보를 추출하였다.

[표 30] 연결 무선 네트워크 정보 추출 코드

```

import json
import csv

with open("wifi_connected_event.csv", "r", encoding='utf-8') as f:
    rdr = csv.reader(f)
    for line in rdr:
        data = line[2]
        if data == "payload":
            continue
        payload = json.loads(data)
        try:
            wanted_data = ['ssid', 'interfaceType', 'authAlgo', 'apManufacturer', 'apModelName']
            for d in wanted_data:
                print("{} : {}".format(d, payload['data'][d]))
            print("=====")
        except:
            continue

```

VI. J:\에 마운트 된 외부 저장 장치의 정보

1. 분석 결과

[표 31] 외부 저장 장치 정보

Manufacturer	Sandisk
Model	Ultra USB 3.0
Serial Number	4C531001460807102273
Volume Serial Number	1A20-0F4E 1491-7593(포맷 후)
Volume Creation Time (UTC)	2021-05-24 02:04:26 2021-07-27 23:10:18(포맷)
File System	NTFS

[표 32] 연결 시간 기록

시각(UTC)	이벤트
2021-07-26 15:38:57	저장장치 연결(Mount)
2021-07-26 16:04:45	저장장치 제거(연결 해제)
2021-07-27 23:10:06	저장장치 연결(Mount)
2021-07-27 23:10:19	저장장치 포맷 및 Dismount
2021-07-27 23:10:19	저장장치 연결(Mount)
2021-07-27 23:45:35	저장장치 제거(연결 해제)

2. 분석 상세

아래의 쿼리를 사용하여 전체 레코드 중 payload 에 'J:\\'라는 키워드를 포함하고 있는 레코드를 선별하였다.

[표 33] 키워드 기반 선별

```
df[df.payload.str.contains("J:\\\\")]
```

2021-07-26 15:38:56 와 2021-07-27 23:10:07, 2021-07-27 23:10:19 에 J:\\\\ 볼륨이 마운트 된 레코드를 발견하였다. 아래는 각 레코드의 payload 칼럼 데이터이다.

[표 34] 2021-07-26 15:38:56 Microsoft.Windows.Storage.StorageService.SdCardStatus

```
{
```

```

    "data": {
      "BusType": 7,
      "DeviceInstance": 2,
      "STORAGE_APP_PAIRING_DIFFERENT_DEVICE": 0,
      "STORAGE_STATUS_DIRTY": 0,
      "STORAGE_STATUS_DISABLED": 0,
      "STORAGE_STATUS_READ_ONLY": 0,
      "STORAGE_STATUS_UNFORMATTED": 0,
      "StorageId": "1A200F4E-0000-0000-D591-2177B127945E",
      "VolumeName": "\\.\?\Volume{5ef7fa9f-ee12-11eb-947e-58961d61ea8f}",
      "VolumePath": "J:\\",
      "result": 268435456,
      "storageDeviceType": 1
    },
    "ext": {
      "app": {
        "asId": 217,
        "id":
"W:0000f519feec486de87ed73cb92d3cac80240000000!0000010db07461e45b41c886192df6fd425ba8d42d82!svchost.exe",
        "ver": "1972/12/14:16:22:50!1C364!svchost.exe"
      },
      "device": {
        "deviceClass": "Windows.Desktop",
        "localId": "s:CC7502F9-996D-4855-8CAE-EB0B86CB4E01"
      },
      "loc": {
        "tz": "+09:00"
      },
      "metadata": {
        "f": {
          "StorageId": 8,
          "result": 2
        }
      },
      "os": {
        "bootId": 3,
        "name": "Windows",
        "ver": "10.0.19043.1110.amd64fre.vb_release.191206-1406"
      },
      "protocol": {
        "devMake": "LG Electronics",
        "devModel": "17ZD90N-VX7BK"
      },
      "user": {
        "localId": "w:CCC59980-EE80-654A-649E-0A2579080012"
      },
      "utc": {
        "epoch": "400562",
        "eventFlags": 257,
        "flags": 205521456,
        "pgName": "WIN",
        "popSample": 2,
        "seq": 26650
      }
    },
    "iKey": "o:0a89d516ae714e01ae89c96d185e9ae3",
    "name": "Microsoft.Windows.Storage.StorageService.SdCardStatus",
    "time": "2021-07-26T15:38:56.8770592Z",
    "ver": "4.0"
  }
}

```

```
{
  "data": {
    "BusType": 7,
    "DeviceInstance": 0,
    "STORAGE_APP_PAIRING_DIFFERENT_DEVICE": 0,
    "STORAGE_STATUS_DIRTY": 0,
    "STORAGE_STATUS_DISABLED": 0,
    "STORAGE_STATUS_READ_ONLY": 0,
    "STORAGE_STATUS_UNFORMATTED": 0,
    "StorageId": "1A200F4E-0000-0000-D591-2177B127945E",
    "VolumeName": "\\.\?\Volume{5ef7fa9f-ee12-11eb-947e-58961d61ea8f}",
    "VolumePath": "J:\\",
    "result": 268435456,
    "storageDeviceType": 1
  },
  "ext": {
    "app": {
      "asId": 282,
      "id":
"W:0000f519feec486de87ed73cb92d3cac80240000000!0000010db07461e45b41c886192df6fd425ba8d42d82!svchost.exe",
      "ver": "1972/12/14:16:22:50!1C364!svchost.exe"
    },
    "device": {
      "deviceClass": "Windows.Desktop",
      "localId": "s:CC7502F9-996D-4855-8CAE-EB0B86CB4E01"
    },
    "loc": {
      "tz": "+09:00"
    },
    "metadata": {
      "f": {
        "StorageId": 8,
        "result": 2
      }
    },
    "os": {
      "bootId": 5,
      "name": "Windows",
      "ver": "10.0.19043.1110.amd64fre.vb_release.191206-1406"
    },
    "protocol": {
      "devMake": "LG Electronics",
      "devModel": "17ZD90N-VX7BK"
    },
    "user": {
      "localId": "w:CCC59980-EE80-654A-649E-0A2579080012"
    },
    "utc": {
      "aId": "526F7192-82F0-0007-FD80-6F52F082D701",
      "epoch": "600060",
      "eventFlags": 257,
      "flags": 205521456,
      "pgName": "WIN",
      "popSample": 2,
      "seq": 40967
    }
  },
  "iKey": "o:0a89d516ae714e01ae89c96d185e9ae3",
  "name": "Microsoft.Windows.Storage.StorageService.SdCardStatus",
  "time": "2021-07-27T23:10:07.0546849Z",
  "ver": "4.0"
}
```



```
{
  "data": {
    "BusType": 7,
    "DeviceInstance": 0,
    "STORAGE_APP_PAIRING_DIFFERENT_DEVICE": 0,
    "STORAGE_STATUS_DIRTY": 0,
    "STORAGE_STATUS_DISABLED": 0,
    "STORAGE_STATUS_READ_ONLY": 0,
    "STORAGE_STATUS_UNFORMATTED": 0,
    "StorageId": "14917593-0000-0000-E72B-60860C024B95",
    "VolumeName": "\\.\?\Volume{5ef7fa9f-ee12-11eb-947e-58961d61ea8f}\\",
    "VolumePath": "J:\\",
    "result": 268435456,
    "storageDeviceType": 1
  },
  "ext": {
    "app": {
      "asId": 282,
      "id":
"W:0000f519feec486de87ed73cb92d3cac80240000000!0000010db07461e45b41c886192df6fd425ba8d42d82!svchost.exe",
      "ver": "1972/12/14:16:22:50!1C364!svchost.exe"
    },
    "device": {
      "deviceClass": "Windows.Desktop",
      "localId": "s:CC7502F9-996D-4855-8CAE-EB0B86CB4E01"
    },
    "loc": {
      "tz": "+09:00"
    },
    "metadata": {
      "f": {
        "StorageId": 8,
        "result": 2
      }
    },
    "os": {
      "bootId": 5,
      "name": "Windows",
      "ver": "10.0.19043.1110.amd64fre.vb_release.191206-1406"
    },
    "protocol": {
      "devMake": "LG Electronics",
      "devModel": "17ZD90N-VX7BK"
    },
    "user": {
      "localId": "w:CCC59980-EE80-654A-649E-0A2579080012"
    },
    "utc": {
      "epoch": "600060",
      "eventFlags": 257,
      "flags": 205521456,
      "pgName": "WIN",
      "popSample": 2,
      "seq": 41040
    }
  },
  "iKey": "o:0a89d516ae714e01ae89c96d185e9ae3",
  "name": "Microsoft.Windows.Storage.StorageService.SdCardStatus",
  "time": "2021-07-27T23:10:19.9149314Z",
  "ver": "4.0"
}
```

Volume Path 가 J:\이며 volume name 이 동일한 것을 확인할 수 있다.

아래 쿼리를 사용하여 해당 시각에 생성된 레코드를 선별하였다.

[표 37] 시각 기준 레코드 선별

```
df[df.payload.str.contains("2021-07-26T15:38:56")]
df[df.payload.str.contains("2021-07-27T23:10:07")]
df[df.payload.str.contains("2021-07-27T23:10:19")]
```

	payload	full_event_name	logging_binary_name	friendly_logging_binary_name
	AC52AD17-CC01-4F85-8DF5-4DCE433C99B.173_0		UsbHub3.sys	USB3 허브 드라이버
	AC52AD17-CC01-4F85-8DF5-4DCE433C99B.43_2		UsbHub3.sys	USB3 허브 드라이버
	Microsoft.Windows.Storage.Classnp.DeviceGuidGenerated	CLASSPNP.SYS	SCSI Class System Dll	
	Microsoft.Windows.Storage.Classnp.DeviceStarted	CLASSPNP.SYS	SCSI Class System Dll	
	Microsoft.Windows.Storage.Classnp.DeviceDescriptorData	CLASSPNP.SYS	SCSI Class System Dll	
	Microsoft.Windows.Storage.Classnp.DeviceAccessAlignment	CLASSPNP.SYS	SCSI Class System Dll	
	Microsoft.Windows.Storage.Classnp.DeviceSeekPenaltyProperty	CLASSPNP.SYS	SCSI Class System Dll	
	Microsoft.Windows.Storage.VolumeManager.BasicVolumeDeviceCreation	volmgr.sys	볼륨 관리자 드라이버	
	Microsoft.Windows.Storage.Partmgr.DiskDiscovery	partmgr.sys	Partition driver	
	FveVolTraceLogProvKM.BitLocker.Driver.ROPolicy.Mount	fvevol.sys	BitLocker Drive Encryption Driver	
	Microsoft.Windows.Audio.Spatial.Renderer.LockForProcess	audiodg.exe	Windows 오디오 장치 그래픽	
	Microsoft.Windows.Audio.DeviceGraph.DeviceGraphInitialize	audiodg.exe	Windows 오디오 장치 그래픽	
	Microsoft.Windows.Audio.Service.StreamCreate	svchost_?audiosrv.dll?	Windows 오디오 서비스	
	Microsoft.Windows.Audio.Client.AudioClientInitialize	explorer.exe	Windows 탐색기	
	Microsoft.Windows.Audio.Client.AudioClientStart	explorer.exe	Windows 탐색기	
	Microsoft.Windows.FileSystem.NTFS.Mount	Ntfs.sys	NT 파일 시스템 드라이버	
	Microsoft.Windows.FileSystem.NTFS.VolumeInfo	Ntfs.sys	NT 파일 시스템 드라이버	
	Microsoft.Windows.FileSystem.NTFS.VolumeInfoSizes	Ntfs.sys	NT 파일 시스템 드라이버	
	Microsoft.Windows.FileSystem.FltMgr.VolumeAttach	svchost_?FLTMGR.SYS?	Microsoft 파일 시스템 필터 관리자	

[그림 4] 2021-07-26 15:38:56 레코드 선별

NTFS 파일시스템 마운트 이벤트가 발생한 것을 알 수 있었다.

각 시간대에 발생한 Microsoft.Windows.FileSystem.NTFS.Mount 이벤트를 선별하였다.

[표 38] 2021-07-26 15:38:56 Microsoft.Windows.FileSystem.NTFS.Mount 이벤트

```
{
  "data": {
    "MountStageTimes": [
      71137101849,
      71137167884,
      71137191644,
      71137196602,
      71137379062,
      71137419068,
      71138068291,
      71138105788,
      71138105788,
      71138105788
    ],
    "activityId": "00000000-0000-0000-0000-000000000000",
    "busType": 7,
    "diskId": "68C652BC-96C4-3675-4A38-4E4F8558394D",
    "elapsedTimeTicks": 1003939,
    "mountGuid": "5EF7FBB1-EE12-11EB-947E-58961D61EA8F",
    "mountStartTime": "2021-07-26T15:38:57.2657196Z",
  }
}
```



```
{
  "data": {
    "MountStageTimes": [
      318774415912,
      318774480025,
      318774503797,
      318774505188,
      318774665122,
      318774685123,
      318774955070,
      318774994993,
      318774994993,
      318774994993
    ],
    "activityId": "00000000-0000-0000-0000-000000000000",
    "busType": 7,
    "diskId": "68C652BC-96C4-3675-4A38-4E4F8558394D",
    "elapsedTimeTicks": 579081,
    "mountGuid": "908E95D3-EEE3-11EB-9481-58961D61EA8F",
    "mountStartTime": "2021-07-27T23:10:06.9754823Z",
    "originalVolumeId": "00000000-0000-0000-0000-000000000000",
    "productId": "Ultra USB 3.0",
    "status": 0,
    "vcbState": 335548421,
    "vcbState2": 2162724,
    "vendorId": "SanDisk",
    "volumeId": "5EF7FA9F-EE12-11EB-947E-58961D61EA8F",
    "volumeInfoKey": 0
  },
  "ext": {
    "app": {
      "asId": 1,
      "id":
        "W:0000da39a3ee5e6b4b0d3255bfef95601890afd80709!000011000000000000000000000000000000000000000000000000!",
      "ver": "1970/01/01:00:00:00!0!"
    },
    "device": {
      "deviceClass": "Windows.Desktop",
      "localId": "s:CC7502F9-996D-4855-8CAE-EB0B86CB4E01"
    },
    "loc": {
      "tz": "+09:00"
    },
    "metadata": {
      "f": {
        "MountStageTimes": {
          "a": 5
        },
        "activityId": 8,
        "busType": 2,
        "diskId": 8,
        "elapsedTimeTicks": 5,
        "mountGuid": 8,
        "mountStartTime": 9,
        "originalVolumeId": 8,
        "volumeId": 8
      },
      "privTags": 16777216
    },
    "os": {
      "bootId": 5,
      "name": "Windows",
      "ver": "10.0.19043.1110.amd64fre.vb_release.191206-1406"
    },
    "protocol": {
      "devMake": "LG Electronics",
      "devModel": "17ZD90N-VX7BK"
    },
    "user": {
```



```

        "busType": 2,
        "diskId": 8,
        "elapsedTimeTicks": 5,
        "mountGuid": 8,
        "mountStartTime": 9,
        "originalVolumeId": 8,
        "volumeId": 8
    },
    "privTags": 16777216
},
"os": {
    "bootId": 5,
    "name": "Windows",
    "ver": "10.0.19043.1110.amd64fre.vb_release.191206-1406"
},
"protocol": {
    "devMake": "LG Electronics",
    "devModel": "17ZD90N-VX7BK"
},
"user": {
    "localId": "w:CCC59980-EE80-654A-649E-0A2579080012"
},
"utc": {
    "epoch": "600060",
    "eventFlags": 257,
    "flags": 205521456,
    "pgName": "WIN",
    "popSample": 2,
    "seq": 41024
}
},
"iKey": "o:0a89d516ae714e01ae89c96d185e9ae3",
"name": "Microsoft.Windows.FileSystem.NTFS.Mount",
"time": "2021-07-27T23:10:19.3240189Z",
"ver": "4.0"
}

```

Microsoft.Windows.FileSystem.NTFS.VolumeInfo 이벤트를 조회하면 볼륨 생성 시각 등 볼륨 정보를 확인할 수 있다. 같은 시간대에 발생한 Microsoft.Windows.FileSystem.NTFS.VolumeInfo 이벤트를 조회하여 볼륨 정보를 확인하였다.

[표 41] 2021-07-26 15:38:56 Microsoft.Windows.FileSystem.NTFS.Volumeinfo 이벤트

```

{
  "data": {
    "busType": 7,
    "clusterSizeBytes": 4096,
    "corruptionCorruptLogPeakBytesUsed": 0,
    "corruptionFlags": 7681,
    "corruptionState": 0,
    "corruptionVerifyLogPeakBytesUsed": 0,
    "diskId": "68C652BC-96C4-3675-4A38-4E4F8558394D",
    "effectivePhysicalSectorSizeBytes": 512,
    "freeClusters": 10349773,
    "frsSizeBytes": 1024,
    "indexAllocationBufferSizeBytes": 4096,
    "logicalSectorSizeBytes": 512,
    "mountGuid": "5EF7FBB1-EE12-11EB-947E-58961D61EA8F",
    "mountStartTime": "2021-07-26T15:38:57.2657196Z",
    "nextSecurityId": 267,
    "originalVolumeId": "00000000-0000-0000-0000-000000000000",
    "physicalSectorSizeBytes": 512,
    "productId": "Ultra USB 3.0",
    "totalClusters": 15163391,
    "totalReservedClusters": 0,

```

```

    "upcaseTableSizeBytes": 65536,
    "vcbState": 2483032069,
    "vcbState2": 2162756,
    "vendorId": "SanDisk",
    "volumeCreationTime": "2021-05-24T02:04:26.4485958Z",
    "volumeId": "5EF7FA9F-EE12-11EB-947E-58961D61EA8F",
    "volumeInfoKey": 1,
    "volumeStateMisc": 32768
  },
  "ext": {
    "app": {
      "asId": 1,
      "id":
        "W:0000da39a3ee5e6b4b0d3255bfef95601890afd80709!000011000000000000000000000000000000000000000000!",
      "ver": "1970/01/01:00:00:00!0!"
    },
    "device": {
      "deviceClass": "Windows.Desktop",
      "localId": "s:CC7502F9-996D-4855-8CAE-EB0B86CB4E01"
    },
    "loc": {
      "tz": "+09:00"
    },
    "metadata": {
      "f": {
        "busType": 2,
        "diskId": 8,
        "freeClusters": 4,
        "mountGuid": 8,
        "mountStartTime": 9,
        "originalVolumeId": 8,
        "totalClusters": 4,
        "totalReservedClusters": 4,
        "upcaseTableSizeBytes": 4,
        "volumeCreationTime": 9,
        "volumeId": 8
      },
      "privTags": 16777216
    },
    "os": {
      "bootId": 3,
      "name": "Windows",
      "ver": "10.0.19043.1110.amd64fre.vb_release.191206-1406"
    },
    "protocol": {
      "devMake": "LG Electronics",
      "devModel": "17ZD90N-VX7BK"
    },
    "user": {
      "localId": "w:CCC59980-EE80-654A-649E-0A2579080012"
    },
    "utc": {
      "epoch": "400562",
      "eventFlags": 257,
      "flags": 205521456,
      "pgName": "WIN",
      "popSample": 2,
      "seq": 26634
    }
  },
  "iKey": "o:0a89d516ae714e01ae89c96d185e9ae3",
  "name": "Microsoft.Windows.FileSystem.NTFS.VolumeInfo",
  "time": "2021-07-26T15:38:56.8406807Z",
  "ver": "4.0"
}

```

[표 42] 2021-07-27 23:10:07 Microsoft.Windows.FileSystem.NTFS.Volumeinfo 이벤트

```
{
```



```

        "mountGuid": 8,
        "mountStartTime": 9,
        "originalVolumeId": 8,
        "totalClusters": 4,
        "totalReservedClusters": 4,
        "upcaseTableSizeBytes": 4,
        "volumeCreationTime": 9,
        "volumeId": 8
    },
    "privTags": 16777216
},
"os": {
    "bootId": 5,
    "name": "Windows",
    "ver": "10.0.19043.1110.amd64fre.vb_release.191206-1406"
},
"protocol": {
    "devMake": "LG Electronics",
    "devModel": "17ZD90N-VX7BK"
},
"user": {
    "localId": "w:CCC59980-EE80-654A-649E-0A2579080012"
},
"utc": {
    "epoch": "600060",
    "eventFlags": 257,
    "flags": 205521456,
    "pgName": "WIN",
    "popSample": 2,
    "seq": 41026
}
},
"iKey": "o:0a89d516ae714e01ae89c96d185e9ae3",
"name": "Microsoft.Windows.FileSystem.NTFS.VolumeInfo",
"time": "2021-07-27T23:10:19.3243041Z",
"ver": "4.0"
}

```

세 시간대에 연결된 VOLUME 의 정보를 정리하면 다음 표와 같다.

[표 44] 볼륨 정보

구분	2021-07-26 15:38:56 레코드	2021-07-27 23:10:07 레코드	2021-07-27 23:10:19 레코드
mountStartTime	2021-07-26 15:38:57.2657196	2021-07-27 23:10:06.9754823	2021-07-27 23:10:19.2715918Z
Volume Creation Time	2021-05-24T02:04:26.4485958Z	2021-05-24T02:04:26.4485958Z	2021-07-27T23:10:18.4065618Z
DiskID	68C652BC-96C4-3675-4A38-4E4F8558394D	68C652BC-96C4-3675-4A38-4E4F8558394D	68C652BC-96C4-3675-4A38-4E4F8558394D
volumeID	5EF7FA9F-EE12-11EB-947E-58961D61EA8F	5EF7FA9F-EE12-11EB-947E-58961D61EA8F	5EF7FA9F-EE12-11EB-947E-58961D61EA8F
mountGUID	5EF7FBB1-EE12-11EB-947E-58961D61EA8F	908E95D3-EEE3-11EB-9481-58961D61EA8F	908E95DE-EEE3-11EB-9481-58961D61EA8F
vendorID	SanDisk	SanDisk	SanDisk
productID	Ultra USB 3.0	Ultra USB 3.0	Ultra USB 3.0

각각 2021-07-26 15:38:57.2657196, 2021-07-27 23:10:06.9754823, 2021-07-27 23:10:19.2715918 에 마운트가 시작되었으며 Disk ID 가 동일하므로 같은 디스크가 연결되었음을 추정할 수 있다. 연결된 디스크는 Sandisk 제조사의 Ultra USB 3.0 이다.

2021-07-27 23:10:19 레코드의 볼륨 생성 시각이 나머지 두개와 상이한 것을 알 수 있다. 이는 2021-07-27 23:10:06 에 마운트 되었던 볼륨이 마운트 해제(dismount) 되었다가 바로 다시 마운트 되면서 차이가 발생한 것으로 보인다.

mountGuid 가 908E95D3-EEE3-11EB-9481-58961D61EA8F 인 볼륨이 2021-07-27T23:10:19.2653648Z 마운트 해제된 기록을 Microsoft.Windows.FileSystem.NTFS.DismountEnd 이벤트에서 확인할 수 있는데, mountGuid 908E95D3-EEE3-11EB-9481-58961D61EA8F 는 23:10:06 에 마운트 된 볼륨이다.

[표 45] 2021-07-27 23:10:19 Microsoft.Windows.FileSystem.NTFS.DismountEnd 이벤트

<pre>{ "data": { "activityId": "00000000-0000-0000-0000-000000000000", "elapsedTimeTicks": 13807, "mountGuid": "908E95D3-EEE3-11EB-9481-58961D61EA8F", "mountStartTime": "2021-07-27T23:10:06.9754823Z", "status": 0, "volumeId": "5EF7FA9F-EE12-11EB-947E-58961D61EA8F", "volumeInfoKey": 1 }, "ext": { "app": { "asId": 134, "id": "W:0000f519feec486de87ed73cb92d3cac80240000000!0000e8f207634e304790b099454338b819d302024d7b!explorer.exe", "ver": "2093/07/26:17:32:14!4AB6D7!explorer.exe" } } }</pre>
--

```

    },
    "device": {
      "deviceClass": "Windows.Desktop",
      "localId": "s:CC7502F9-996D-4855-8CAE-EB0B86CB4E01"
    },
    "loc": {
      "tz": "+09:00"
    },
    "metadata": {
      "f": {
        "activityId": 8,
        "elapsedTimeTicks": 5,
        "mountGuid": 8,
        "mountStartTime": 9,
        "volumeId": 8
      },
      "privTags": 16777216
    },
    "os": {
      "bootId": 5,
      "name": "Windows",
      "ver": "10.0.19043.1110.amd64fre.vb_release.191206-1406"
    },
    "protocol": {
      "devMake": "LG Electronics",
      "devModel": "17ZD90N-VX7BK"
    },
    "user": {
      "localId": "w:CCC59980-EE80-654A-649E-0A2579080012"
    },
    "utc": {
      "epoch": "600060",
      "eventFlags": 257,
      "flags": 205521456,
      "pgName": "WIN",
      "popSample": 2,
      "seq": 41023,
      "shellId": 33786497904279555
    }
  },
  "iKey": "o:0a89d516ae714e01ae89c96d185e9ae3",
  "name": "Microsoft.Windows.FileSystem.NTFS.DismountEnd",
  "time": "2021-07-27T23:10:19.2653648Z",
  "ver": "4.0"
}

```

제조사가 Sandisk 임에 바탕하여 payload 에 대소문자 관계 없이 sandisk 라는 문자열을 포함하고 있는 레코드 중 해당 시간대에 발생한 이벤트만 선별하였다.

[표 46] 문자열 기반 이벤트 선별

```

df[df.payload.str.contains("(?i)sandisk") & df.payload.str.contains("2021-07-26T15:38:56")]
df[df.payload.str.contains("(?i)sandisk") & df.payload.str.contains("2021-07-27T23:10:07")]

```

아래 표는 선별된 레코드 중 Microsoft.Windows.Storage.StorageService.UsbDiskArrival 이벤트 데이터를 선별한 것이다. 파일시스템, 제조사, ProductId, VID, PID, SerialNumber 정보를 확인할 수 있다.

[표 47] 2021-07-26T15:38:56 Microsoft.Windows.Storage.StorageService.UsbDiskArrival

```

{
  "data": {

```

```

"BusType": 7,
"ContainsRawVolumes": 0,
"DiskNumber": 5,
"FileSystem": "NTFS",
"ParentId": "USB\\VID_0781&PID_5591\\4C531001460807102273",
"PartitionStyle": 0,
"ProductId": "Ultra USB 3.0",
"ProductRevision": "1.00",
"SerialNumber": "4C531001460807102273",
"Size": 62109253632,
"VendorId": "SanDisk",
"VolumeCount": 1
},
"ext": {
  "app": {
    "asId": 217,
    "id":
"W:0000f519feec486de87ed73cb92d3cac80240000000!0000010db07461e45b41c886192df6fd425ba8d42d82!svchost.exe",
    "ver": "1972/12/14:16:22:50!1C364!svchost.exe"
  },
  "device": {
    "deviceClass": "Windows.Desktop",
    "localId": "s:CC7502F9-996D-4855-8CAE-EB0B86CB4E01"
  },
  "loc": {
    "tz": "+09:00"
  },
  "metadata": {
    "f": {
      "BusType": 2,
      "ContainsRawVolumes": 2,
      "DiskNumber": 2,
      "PartitionStyle": 2,
      "Size": 4,
      "VolumeCount": 2
    }
  },
  "os": {
    "bootId": 3,
    "name": "Windows",
    "ver": "10.0.19043.1110.amd64fre.vb_release.191206-1406"
  },
  "protocol": {
    "devMake": "LG Electronics",
    "devModel": "17ZD90N-VX7BK"
  },
  "user": {
    "localId": "w:CCC59980-EE80-654A-649E-0A2579080012"
  },
  "utc": {
    "aId": "20D67CDD-821F-0004-C586-D6201F82D701",
    "epoch": "400562",
    "eventFlags": 257,
    "flags": 205521456,
    "pgName": "WIN",
    "popSample": 2,
    "seq": 26649
  }
},
"iKey": "o:0a89d516ae714e01ae89c96d185e9ae3",
"name": "Microsoft.Windows.Storage.StorageService.UsbDiskArrival",
"time": "2021-07-26T15:38:56.8687881Z",
"ver": "4.0"
}

```

```
{
  "data": {
    "BusType": 7,
    "ContainsRawVolumes": 0,
    "DiskNumber": 2,
    "FileSystem": "NTFS",
    "ParentId": "USB\\VID_0781&PID_5591\\4C531001460807102273",
    "PartitionStyle": 0,
    "ProductId": "Ultra USB 3.0",
    "ProductRevision": "1.00",
    "SerialNumber": "4C531001460807102273",
    "Size": 62109253632,
    "VendorId": "SanDisk",
    "VolumeCount": 1
  },
  "ext": {
    "app": {
      "asId": 282,
      "id":
"W:0000f519feec486de87ed73cb92d3cac80240000000!0000010db07461e45b41c886192df6fd425ba8d42d82!svchost.exe",
      "ver": "1972/12/14:16:22:50!1C364!svchost.exe"
    },
    "device": {
      "deviceClass": "Windows.Desktop",
      "localId": "s:CC7502F9-996D-4855-8CAE-EB0B86CB4E01"
    },
    "loc": {
      "tz": "+09:00"
    },
    "metadata": {
      "f": {
        "BusType": 2,
        "ContainsRawVolumes": 2,
        "DiskNumber": 2,
        "PartitionStyle": 2,
        "Size": 4,
        "VolumeCount": 2
      }
    },
    "os": {
      "bootId": 5,
      "name": "Windows",
      "ver": "10.0.19043.1110.amd64fre.vb_release.191206-1406"
    },
    "protocol": {
      "devMake": "LG Electronics",
      "devModel": "17ZD90N-VX7BK"
    },
    "user": {
      "localId": "w:CCC59980-EE80-654A-649E-0A2579080012"
    },
    "utc": {
      "aId": "526F7192-82F0-0007-FD80-6F52F082D701",
      "epoch": "600060",
      "eventFlags": 257,
      "flags": 205521456,
      "pgName": "WIN",
      "popSample": 2,
      "seq": 40966
    }
  },
  "iKey": "o:0a89d516ae714e01ae89c96d185e9ae3",
  "name": "Microsoft.Windows.Storage.StorageService.UsbDiskArrival",
  "time": "2021-07-27T23:10:07.0530861Z",
  "ver": "4.0"
}
```

아래는 파일시스템, 제조사, ProductId, VID, PID, SerialNumber 정보를 정리한 표이다.

[표 49] 파일시스템 및 주요 정보

파일시스템	NTFS
제조사	Sandisk
VID	0781
PID	5591
productID	Ultra USB 3.0
SerialNumber	4C531001460807102273

전체 레코드 중 disk Id '68C652BC-96C4-3675-4A38-4E4F8558394D' 문자열을 포함한 레코드를 선별했다.

[표 50] 문자열 기반 레코드 선별

```
df[df.payload.str.contains('68C652BC-96C4-3675-4A38-4E4F8558394D')]
```

장치가 연결 해제되었을 때 발생하는 Microsoft.Windows.Storage.Classnpn.DeviceRemoved 이벤트가 근접 시간대에 발생한 것을 확인하였다.

31397	2021-07-27 00:38:56	("ver": "4.0", "name": "Microsoft.Windows.Storage.Partmgr.DiskDiscovery", "time": "2021-07-26T15:38:56.7191627Z", "iKey": "o:0a89d516ae714e01ae89c96d185e9ae3", "ext": {"utc": {"popSan": 000000000000, "firmwareSupportsUpgrade": 0, "firmwareSlotCount": 0, "storageIdCount": 0, "storageIdCodeSet": 0, "storageIdType": 0, "storageIdAssociation": 0, "storageId": "0x", "writeCache": 0}})
31404	2021-07-27 00:38:56	("ver": "4.0", "name": "Microsoft.Windows.FileSystem.NTFS.Mount", "time": "2021-07-26T15:38:56.8406156Z", "iKey": "o:0a89d516ae714e01ae89c96d185e9ae3", "ext": {"utc": {"popSample": 2, "popSamp": 0}})
31405	2021-07-27 00:38:56	("ver": "4.0", "name": "Microsoft.Windows.FileSystem.NTFS.VolumeInfo", "time": "2021-07-26T15:38:56.8406807Z", "iKey": "o:0a89d516ae714e01ae89c96d185e9ae3", "ext": {"utc": {"popSamp": 0}})
33083	2021-07-27 01:04:45	("ver": "4.0", "name": "Microsoft.Windows.Storage.Partmgr.DiskDiscovery", "time": "2021-07-26T16:04:45.8696462Z", "iKey": "o:0a89d516ae714e01ae89c96d185e9ae3", "ext": {"utc": {"popSan": 000000000000, "firmwareSupportsUpgrade": 0, "firmwareSlotCount": 0, "storageIdCount": 0, "storageIdCodeSet": 0, "storageIdType": 0, "storageIdAssociation": 0, "storageId": "0x", "writeCache": 0}})
33084	2021-07-27 01:04:45	("ver": "4.0", "name": "Microsoft.Windows.Storage.Classnpn.DeviceRemoved", "time": "2021-07-26T16:04:45.8697799Z", "iKey": "o:0a89d516ae714e01ae89c96d185e9ae3", "ext": {"utc": {"popSan": 000000000000, "firmwareSupportsUpgrade": 0, "firmwareSlotCount": 0, "storageIdCount": 0, "storageIdCodeSet": 0, "storageIdType": 0, "storageIdAssociation": 0, "storageId": "0x", "writeCache": 0}})
103706	2021-07-28 08:10:06	("ver": "4.0", "name": "Microsoft.Windows.Storage.Classnpn.DeviceGuidGenerated", "time": "2021-07-27T23:10:06.9465870Z", "iKey": "o:0a89d516ae714e01ae89c96d185e9ae3", "ext": {"utc": {"popSample": 2, "popSamp": 0}})
103707	2021-07-28 08:10:06	("ver": "4.0", "name": "Microsoft.Windows.Storage.Classnpn.DeviceStarted", "time": "2021-07-27T23:10:06.9488168Z", "iKey": "o:0a89d516ae714e01ae89c96d185e9ae3", "ext": {"utc": {"popSan": 000000000000, "firmwareSupportsUpgrade": 0, "firmwareSlotCount": 0, "storageIdCount": 0, "storageIdCodeSet": 0, "storageIdType": 0, "storageIdAssociation": 0, "storageId": "0x", "writeCache": 0}})
103708	2021-07-28 08:10:06	("ver": "4.0", "name": "Microsoft.Windows.Storage.Classnpn.DeviceDescriptorData", "time": "2021-07-27T23:10:06.9488193Z", "iKey": "o:0a89d516ae714e01ae89c96d185e9ae3", "ext": {"utc": {"popSample": 2, "popSamp": 0}})
103709	2021-07-28 08:10:06	("ver": "4.0", "name": "Microsoft.Windows.Storage.Classnpn.DeviceAccessAlignment", "time": "2021-07-27T23:10:06.9494903Z", "iKey": "o:0a89d516ae714e01ae89c96d185e9ae3", "ext": {"utc": {"popSample": 2, "popSamp": 0}})
103710	2021-07-28 08:10:06	("ver": "4.0", "name": "Microsoft.Windows.Storage.Classnpn.DeviceSeekPenaltyProperty", "time": "2021-07-27T23:10:06.9494965Z", "iKey": "o:0a89d516ae714e01ae89c96d185e9ae3", "ext": {"utc": {"popSample": 2, "popSamp": 0}})
103711	2021-07-28 08:10:06	("ver": "4.0", "name": "Microsoft.Windows.Storage.VolumeManager.BasicVolumeDeviceCreation", "time": "2021-07-27T23:10:06.9583804Z", "iKey": "o:0a89d516ae714e01ae89c96d185e9ae3", "ext": {"utc": {"popSample": 2, "popSamp": 0}})
103712	2021-07-28 08:10:06	("ver": "4.0", "name": "Microsoft.Windows.Storage.Partmgr.DiskDiscovery", "time": "2021-07-27T23:10:06.9600496Z", "iKey": "o:0a89d516ae714e01ae89c96d185e9ae3", "ext": {"utc": {"popSan": 000000000000, "firmwareSupportsUpgrade": 0, "firmwareSlotCount": 0, "storageIdCount": 0, "storageIdCodeSet": 0, "storageIdType": 0, "storageIdAssociation": 0, "storageId": "0x", "writeCache": 0}})
103717	2021-07-28 08:10:07	("ver": "4.0", "name": "Microsoft.Windows.FileSystem.NTFS.Mount", "time": "2021-07-27T23:10:07.0334876Z", "iKey": "o:0a89d516ae714e01ae89c96d185e9ae3", "ext": {"utc": {"popSample": 2, "popSamp": 0}})
103719	2021-07-28 08:10:07	("ver": "4.0", "name": "Microsoft.Windows.FileSystem.NTFS.VolumeInfo", "time": "2021-07-27T23:10:07.0335623Z", "iKey": "o:0a89d516ae714e01ae89c96d185e9ae3", "ext": {"utc": {"popSample": 2, "popSamp": 0}})
103790	2021-07-28 08:10:19	("ver": "4.0", "name": "Microsoft.Windows.FileSystem.NTFS.Mount", "time": "2021-07-27T23:10:19.3240189Z", "iKey": "o:0a89d516ae714e01ae89c96d185e9ae3", "ext": {"utc": {"popSample": 2, "popSamp": 0}})
103792	2021-07-28 08:10:19	("ver": "4.0", "name": "Microsoft.Windows.FileSystem.NTFS.VolumeInfo", "time": "2021-07-27T23:10:19.3243041Z", "iKey": "o:0a89d516ae714e01ae89c96d185e9ae3", "ext": {"utc": {"popSample": 2, "popSamp": 0}})
104683	2021-07-28 08:45:35	("ver": "4.0", "name": "Microsoft.Windows.Storage.Partmgr.DiskDiscovery", "time": "2021-07-27T23:45:35.5408287Z", "iKey": "o:0a89d516ae714e01ae89c96d185e9ae3", "ext": {"utc": {"popSan": 000000000000, "firmwareSupportsUpgrade": 0, "firmwareSlotCount": 0, "storageIdCount": 0, "storageIdCodeSet": 0, "storageIdType": 0, "storageIdAssociation": 0, "storageId": "0x", "writeCache": 0}})
104684	2021-07-28 08:45:35	("ver": "4.0", "name": "Microsoft.Windows.Storage.Classnpn.DeviceRemoved", "time": "2021-07-27T23:45:35.5410718Z", "iKey": "o:0a89d516ae714e01ae89c96d185e9ae3", "ext": {"utc": {"popSan": 000000000000, "firmwareSupportsUpgrade": 0, "firmwareSlotCount": 0, "storageIdCount": 0, "storageIdCodeSet": 0, "storageIdType": 0, "storageIdAssociation": 0, "storageId": "0x", "writeCache": 0}})

[그림 5] Microsoft.Windows.Storage.Classnpn.DeviceRemoved 이벤트

[표 51] 2021-07-26 16:04:45 Microsoft.Windows.Storage.Classnpn.DeviceRemoved 이벤트

{ "data": { "deviceGuid": "68C652BC-96C4-3675-4A38-4E4F8558394D", "surpriseRemoval": 0 }, }
--


```

    },
    "user": {
      "localId": "w:CCC59980-EE80-654A-649E-0A2579080012"
    },
    "utc": {
      "epoch": "600060",
      "eventFlags": 257,
      "flags": 206045744,
      "pgName": "WIN",
      "popSample": 2,
      "seq": 41918
    }
  },
  "ikey": "o:0a89d516ae714e01ae89c96d185e9ae3",
  "name": "Microsoft.Windows.Storage.Classnp.DeviceRemoved",
  "time": "2021-07-27T23:45:35.5410718Z",
  "ver": "4.0"
}

```

시각을 기준으로 추가 레코드를 확인한 결과 동일한 시각에

Microsoft.Windows.Storage.StorageService.SurpriseRemoval 이벤트가 발생한 것을 확인할 수 있었다.

해당 이벤트는 'usb 안전하게 제거' 기능을 거치지 않고 바로 제거하였을 때 발생한다.

In [26]: `df[df.payload.str.contains("2021-07-26T16:04:45")]`

	timestamp(UTC+9)	
33083	2021-07-27 01:04:45	[{"ver":"4.0","name":"Microsoft.Windows.Storage.Partmgr.DiskDiscovery","time":"2021-07-26T16:04:45.8696462Z","ikey":"o:0a89d516ae714e01ae89c96d185e9ae3","ext":{"utc":{"popSa
33084	2021-07-27 01:04:45	[{"ver":"4.0","name":"Microsoft.Windows.Storage.Classnp.DeviceRemoved","time":"2021-07-26T16:04:45.8697799Z","ikey":"o:0a89d516ae714e01ae89c96d185e9ae3","ext":{"utc":{"popSa
33085	2021-07-27 01:04:45	[{"ver":"4.0","name":"Microsoft.Windows.WinRTClassActivation.WinRTClassActivationInfo","time":"2021-07-26T16:04:45.8955025Z","ikey":"o:0a89d516ae714e01ae89c96d185e9ae3","ex
33086	2021-07-27 01:04:45	[{"ver":"4.0","name":"Microsoft.Windows.Storage.StorageService.SurpriseRemoval","time":"2021-07-26T16:04:45.8955199Z","ikey":"o:0a89d516ae714e01ae89c96d185e9ae3","ext":{"utc
33087	2021-07-27 01:04:45	[{"ver":"4.0","name":"Microsoft.Windows.Desktop.Shell.NotificationArea.DragDropIcon","time":"2021-07-26T16:04:45.8968523Z","ikey":"o:0a89d516ae714e01ae89c96d185e9ae3","ext"
33088	2021-07-27 01:04:45	[{"ver":"4.0","name":"Microsoft.Windows.Desktop.Shell.NotificationArea.LogShowBalloon","time":"2021-07-26T16:04:45.9093741Z","ikey":"o:0a89d516ae714e01ae89c96d185e9ae3","e

In [27]: `df[df.payload.str.contains("2021-07-27T23:45:35")]`

	timestamp(UTC+9)	
104683	2021-07-28 08:45:35	[{"ver":"4.0","name":"Microsoft.Windows.Storage.Partmgr.DiskDiscovery","time":"2021-07-27T23:45:35.5408287Z","ikey":"o:0a89d516ae714e01ae89c96d185e9ae3","ext":{"utc":{"popSa
104684	2021-07-28 08:45:35	[{"ver":"4.0","name":"Microsoft.Windows.Storage.Classnp.DeviceRemoved","time":"2021-07-27T23:45:35.5410718Z","ikey":"o:0a89d516ae714e01ae89c96d185e9ae3","ext":{"utc":{"popSa
104685	2021-07-28 08:45:35	[{"ver":"4.0","name":"Microsoft.Windows.Input.HidClass.StateExit_Dx_NoWake","time":"2021-07-27T23:45:35.5502842Z","ikey":"o:0a89d516ae714e01ae89c96d185e9ae3","ext":{"utc":{"p
104686	2021-07-28 08:45:35	[{"ver":"4.0","name":"Microsoft.Windows.WinRTClassActivation.WinRTClassActivationInfo","time":"2021-07-27T23:45:35.5504556Z","ikey":"o:0a89d516ae714e01ae89c96d185e9ae3","ext
104687	2021-07-28 08:45:35	[{"ver":"4.0","name":"Microsoft.Windows.Storage.StorageService.SurpriseRemoval","time":"2021-07-27T23:45:35.5504766Z","ikey":"o:0a89d516ae714e01ae89c96d185e9ae3","ext":{"utc
104688	2021-07-28 08:45:35	[{"ver":"4.0","name":"Microsoft.Windows.Desktop.Shell.NotificationArea.DragDropIcon","time":"2021-07-27T23:45:35.5686618Z","ikey":"o:0a89d516ae714e01ae89c96d185e9ae3","ext"

[그림 6] Microsoft.Windows.Storage.StorageService.SurpriseRemoval 이벤트

[표 53] 2021-07-26 16:04:45 Microsoft.Windows.Storage.StorageService.SurpriseRemoval 이벤트

```

{
  "data": {
    "busType": 7,
    "dismountReason": 2,
    "storageDeviceType": 1,
    "storageId": "1A200F4E-0000-0000-D591-2177B127945E"
  },
  "ext": {
    "app": {

```

```

        "asId": 217,
        "id":
"W:0000f519feec486de87ed73cb92d3cac80240000000!0000010db07461e45b41c886192df6fd425ba8d42d82!svchost.exe",
        "ver": "1972/12/14:16:22:50!1C364!svchost.exe"
    },
    "device": {
        "deviceClass": "Windows.Desktop",
        "localId": "s:CC7502F9-996D-4855-8CAE-EB0B86CB4E01"
    },
    "loc": {
        "tz": "+09:00"
    },
    "metadata": {
        "f": {
            "storageId": 8
        }
    },
    "os": {
        "bootId": 3,
        "name": "Windows",
        "ver": "10.0.19043.1110.amd64fre.vb_release.191206-1406"
    },
    "protocol": {
        "devMake": "LG Electronics",
        "devModel": "17ZD90N-VX7BK"
    },
    "user": {
        "localId": "w:CCC59980-EE80-654A-649E-0A2579080012"
    },
    "utc": {
        "aId": "20D67CDD-821F-0004-C586-D6201F82D701",
        "epoch": "400562",
        "eventFlags": 257,
        "flags": 205521456,
        "pgName": "WIN",
        "popSample": 2,
        "seq": 28315
    }
},
"iKey": "o:0a89d516ae714e01ae89c96d185e9ae3",
"name": "Microsoft.Windows.Storage.StorageService.SurpriseRemoval",
"time": "2021-07-26T16:04:45.8955199Z",
"ver": "4.0"
}

```

[표 54] 2021-07-27 23:45:35 Microsoft.Windows.Storage.StorageService.SurpriseRemoval 이벤트

```

{
    "data": {
        "busType": 7,
        "dismountReason": 2,
        "storageDeviceType": 1,
        "storageId": "14917593-0000-0000-E72B-60860C024B95"
    },
    "ext": {
        "app": {
            "asId": 282,
            "id":
"W:0000f519feec486de87ed73cb92d3cac80240000000!0000010db07461e45b41c886192df6fd425ba8d42d82!svchost.exe",
            "ver": "1972/12/14:16:22:50!1C364!svchost.exe"
        },
        "device": {
            "deviceClass": "Windows.Desktop",
            "localId": "s:CC7502F9-996D-4855-8CAE-EB0B86CB4E01"
        },
        "loc": {
            "tz": "+09:00"
        },
        "metadata": {
            "f": {
                "storageId": 8
            }
        },
        "os": {
            "bootId": 5,
            "name": "Windows",
            "ver": "10.0.19043.1110.amd64fre.vb_release.191206-1406"
        },
        "protocol": {

```

```

    "devMake": "LG Electronics",
    "devModel": "17ZD90N-VX7BK"
  },
  "user": {
    "localId": "w:CCC59980-EE80-654A-649E-0A2579080012"
  },
  "utc": {
    "aId": "526F7192-82F0-0007-FD80-6F52F082D701",
    "epoch": "600060",
    "eventFlags": 257,
    "flags": 206045744,
    "pgName": "WIN",
    "popSample": 2,
    "seq": 41921
  }
},
"iKey": "o:0a89d516ae714e01ae89c96d185e9ae3",
"name": "Microsoft.Windows.Storage.StorageService.SurpriseRemoval",
"time": "2021-07-27T23:45:35.5504766Z",
"ver": "4.0"
}

```

위 이벤트에서 storageID 라는 값을 확인할 수 있는데, 해당 값은 Microsoft.Windows.Storage.StorageService.SdCardStatus 이벤트의 storageID 값과 동일하며, storageID 값의 앞 8 자리는 Volume Serial Number 를 의미한다.

[표 55] storageID - Volume Serial Number 비교

구분	2021-07-26 15:38:56 레코드	2021-07-27 23:10:07 레코드	2021-07-27 23:10:19 레코드
storageID	1A200F4E-0000-0000-D591-2177B127945E	1A200F4E-0000-0000-D591-2177B127945E	14917593-0000-0000-E72B-60860C024B95

3 번의 마운트 중 마지막 기록의 Volume Serial number 가 상이함을 확인할 수 있는데, 이는 2021-07-27 23:10:19 에 저장장치가 포맷되면서 VSN 이 변경된 것으로 보인다.

Volume serial Number 는 Microsoft.Windows.Storage.Partmgr.DiskDiscovery 이벤트에서 확인할 수 있다. Data 필드의 vbr 필드에서 Volume Boot Record 데이터를 확인할 수 있는데 Volume Serial Number 는 NTFS 파일시스템의 경우 Volume Boot Record 데이터 0x48 오프셋에서 0x4F 오프셋까지 기록되고,

실제로 사용되는 값은 0x48 부터 4 바이트이고 Little Endian 으로 기록된다.

[표 56] 2021-07-26 15:38:56 Microsoft.Windows.Storage.Partmgr.DiskDiscovery

```

{
  "data": {
    "adapterAlignmentMask": 0,
    "adapterId": "00000000-0000-0000-0000-000000000000",
    "adapterMaximumTransferBytes": 65536,
    "adapterMaximumTransferPages": 17,
    "adapterSerialNumber": "",
    "busType": 7,
    "bytesOffsetForSectorAlignment": 0,
    "bytesPerLogicalSector": 512,
    "bytesPerPhysicalSector": 512,
    "bytesPerSector": 512,
    "capacityBytes": 62109253632,

```

```

"characteristics": 262401,
"diskId": "68C652BC-96C4-3675-4A38-4E4F8558394D",
"diskNumber": 5,
"dumpCount": 0,
"faultTolerance": 0,
"firmwareSlotCount": 0,
"firmwareSupportsUpgrade": 0,
"flags": 8208,
"flushCacheSupported": 0,
"hibernationCount": 0,
"hybridCacheBytes": 0,
"hybridSupported": 0,
"idFlags": 0,
"incursSeekPenalty": 0,
"interleaveBytes": 0,
"ioctlSupport": 59681,
"isPowerProtected": 0,
"isSystemCritical": 0,
"isThinProvisioned": 0,
"isTrimSupported": 0,
"location": "Integrated : Bus 0 : Device 0 : Function 3 : Adapter 0 : Port 0",
"manufacturer": "SanDisk",
"mbr":
"0xEB52904E5446532020202000020800000000000000F800003F00FF000000000000000080000000FFFF3A0700000000
0000C000000000002000000000000000F6000000010000004E0F201A21201AC800000000FA33C08ED0BC007CFB68C0071F1E6
86600CB88160E0066813E03004E5446537515B441BBAA55CD13720C81FB55AA7506F7C101007503E9DD001E83EC18681A00B
4488A160E008BF4161FCD139F83C4189E581F72E13B060B0075DBA30F00C12E0F00041E5A33DBB900202BC866FF061100031
60F008EC2FF061600E84B002BC877EFB800BBBCD1A6623C0752D6681FB54435041752481F90201721E166807BB16685211166
8090066536653665516161668B80166610E07CD1A33C0BF0A13B9F60CFCF3AAE9FE01909066601E0666A111006603061C001
E6668000000066500653680100681000B4428A160E00161F8BF4CD1366595B5A665966591F0F82160066FF06110003160F0
08EC2FF0E160075BC071F6661C3A1F601E80900A1FA01E80300F4EBFD8BF0AC3C007409B40EBB0700CD10EBF2C30D0A41206
469736B2072656164206572726F72206F63637572726564000D0A424F4F544D475220697320636F6D70726573736564000D0
A5072657373204374726C2B416C742B44656C20746F20726573746172740D0A000000000000000000000000000000000000
00000008A01A701BF01000055AA",
"model": "Ultra USB 3.0",
"numberOfColumns": 0,
"numberOfLogicalCopies": 0,
"numberOfPhysicalCopies": 0,
"nvCacheEnabled": 0,
"optimalUnmapGranularity": 0,
"pagingCount": 0,
"parentId": "USB\\VID_0781&PID_5591\\4C531001460807102273",
"partitionCount": 1,
"partitionStyle": 0,
"partitionTable":
"0x00000000010000000100000028344793000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000760E00000001000000000000000400010000000000100000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000",
"poolId": "00000000-0000-0000-0000-000000000000",
"portDriver": 5,
"registryId": "5EF7FA9C-EE12-11EB-947E-58961D61EA8F",
"revision": "1.00",
"serial": "4C531001460807102273",
"storageId": "0x",
"storageIdAssociation": 0,
"storageIdCodeSet": 0,
"storageIdCount": 0,
"storageIdType": 0,
"unmapAlignment": 0,
"userRemovalPolicy": 1,
"vbr0":
"0xEB52904E5446532020202000020800000000000000F800003F00FF000000000000000080000000FFFF3A0700000000
0000C000000000002000000000000000F6000000010000004E0F201A21201AC800000000FA33C08ED0BC007CFB68C0071F1E6
86600CB88160E0066813E03004E5446537515B441BBAA55CD13720C81FB55AA7506F7C101007503E9DD001E83EC18681A00B
4488A160E008BF4161FCD139F83C4189E581F72E13B060B0075DBA30F00C12E0F00041E5A33DBB900202BC866FF061100031
60F008EC2FF061600E84B002BC877EFB800BBBCD1A6623C0752D6681FB54435041752481F90201721E166807BB16685211166
8090066536653665516161668B80166610E07CD1A33C0BF0A13B9F60CFCF3AAE9FE01909066601E0666A111006603061C001
E6668000000066500653680100681000B4428A160E00161F8BF4CD1366595B5A665966591F0F82160066FF06110003160F0
08EC2FF0E160075BC071F6661C3A1F601E80900A1FA01E80300F4EBFD8BF0AC3C007409B40EBB0700CD10EBF2C30D0A41206
469736B2072656164206572726F72206F63637572726564000D0A424F4F544D475220697320636F6D70726573736564000D0
A5072657373204374726C2B416C742B44656C20746F20726573746172740D0A000000000000000000000000000000000000

```

```

00000008A01A701BF01000055AA",
  "vbr1": "0x",
  "vbr2": "0x",
  "vbr3": "0x",
  "version": 4,
  "writeCacheChangeable": 0,
  "writeCacheEnabled": 0,
  "writeCacheType": 0,
  "writeThroughSupported": 0
},
"ext": {
  "app": {
    "asId": 1,
    "id":
"W:000da39a3ee5e6b4b0d3255bfef95601890afd80709!000011000000000000000000000000000000000000000000!",
    "ver": "1970/01/01:00:00:00!0!"
  },
  "device": {
    "deviceClass": "Windows.Desktop",
    "localId": "s:CC7502F9-996D-4855-8CAE-EB0B86CB4E01"
  },
  "loc": {
    "tz": "+09:00"
  },
  "metadata": {
    "f": {
      "adapterId": 8,
      "capacityBytes": 5,
      "diskId": 8,
      "hybridCacheBytes": 5,
      "ioctlSupport": 5,
      "optimalUnmapGranularity": 5,
      "poolId": 8,
      "registryId": 8,
      "unmapAlignment": 5
    }
  },
  "os": {
    "bootId": 3,
    "name": "Windows",
    "ver": "10.0.19043.1110.amd64fre.vb_release.191206-1406"
  },
  "protocol": {
    "devMake": "LG Electronics",
    "devModel": "17ZD90N-VX7BK"
  },
  "user": {
    "localId": "w:CCC59980-EE80-654A-649E-0A2579080012"
  },
  "utc": {
    "epoch": "400562",
    "eventFlags": 257,
    "flags": 205521456,
    "pgName": "WIN",
    "popSample": 2,
    "seq": 26626
  }
},
"iKey": "o:0a89d516ae714e01ae89c96d185e9ae3",
"name": "Microsoft.Windows.Storage.Partmgr.DiskDiscovery",
"time": "2021-07-26T15:38:56.7191627Z",
"ver": "4.0"
}

```



```

"user": {
  "localId": "w:CCC59980-EE80-654A-649E-0A2579080012"
},
"utc": {
  "epoch": "600060",
  "eventFlags": 257,
  "flags": 205521456,
  "pgName": "WIN",
  "popSample": 2,
  "seq": 40946
}
},
"iKey": "o:0a89d516ae714e01ae89c96d185e9ae3",
"name": "Microsoft.Windows.Storage.Partmgr.DiskDiscovery",
"time": "2021-07-27T23:10:06.9600496Z",
"ver": "4.0"
}

```

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	EB	52	90	4E	54	46	53	20	20	20	20	00	02	08	00	00	ER.NTFS
00000010	00	00	00	00	00	F8	00	00	3F	00	FF	00	00	00	00	00ø...?.ÿ.....
00000020	00	00	00	00	80	00	00	00	FF	FF	3A	07	00	00	00	00€...ÿÿ:.....
00000030	00	00	0C	00	00	00	00	00	02	00	00	00	00	00	00	00
00000040	F6	00	00	00	01	00	00	00	4E	0F	20	1A	21	20	1A	C8	ö.....N. .! .È
00000050	00	00	00	00	FA	33	C0	8E	D0	BC	00	7C	FB	68	C0	07ú3ÀŽĐ+. úhÀ.
00000060	1F	1E	68	66	00	CB	88	16	0E	00	66	81	3E	03	00	4E	..hf.È^...f.>..N
00000070	54	46	53	75	15	B4	41	BB	AA	55	CD	13	72	0C	81	FB	TFSu.´A»*UÍ.r..û
00000080	55	AA	75	06	F7	C1	01	00	75	03	E9	DD	00	1E	83	EC	U*u.÷Á..u.éÝ..fì
00000090	18	68	1A	00	B4	48	8A	16	0E	00	8B	F4	16	1F	CD	13	.h...´HŠ...<ó..í.
000000A0	9F	83	C4	18	9E	58	1F	72	E1	3B	06	0B	00	75	DB	A3	ŸfÄ.žX.rá;...uŮ&
000000B0	0F	00	C1	2E	0F	00	04	1E	5A	33	DB	B9	00	20	2B	C8	..Á.....Z3Ů+. +È
000000C0	66	FF	06	11	00	03	16	0F	00	8E	C2	FF	06	16	00	E8	fÿ.....ŽÂÿ...è

[그림 8] 2021-07-27 23:10:07 VBR 데이터

0x48 오프셋부터 4E0F201A21201AC8 값이 확인되며, 실제 Volume Serial Number 는 0X48 오프셋부터 4 바이트값인 4e0f201a 의 리틀 엔디안인 1A20-0F4E 이며, storageID 앞 8 자리인 1A200F4E 와 일치하므로, storageID 의 앞 8 자리는 Volume Serial Number 임을 확인할 수 있다. 다른 저장장치 연결기록에서도 해당 데이터는 서로 동일함을 확인했다.

이는 VSN 이 2021-07-27 23:10:19 에 변경된 것을 뒷받침한다. VSN 은 저장장치가 포맷되면서 변경된 것으로 보이는데, 아래의 표와 같이 23:10:19 에 Microsoft.Windows.FileSystem.Chkdsk.Format 이벤트가 발생한 사실이 이를 증명한다.

[표 58] 2021-07-27 23:10:19 Microsoft.Windows.FileSystem.Chkdsk.Format

```

{
  "data": {
    "formatApiCalled": 2,
    "formatClusterSize": 4096,
    "formatDuration": 1547,
    "formatExitStatus": 1,
    "formatFileSystemName": "ntfs",
    "formatFlags": 577,
    "formatLogFileSize": 0,
    "formatPhases": 0,
    "formatSourceTag": 0,
    "formatVersionMajor": 1,
    "formatVersionMinor": 0,
    "formatVolumeId": "5EF7FA9F-EE12-11EB-947E-58961D61EA8F"
  },
  "ext": {

```



```

    "app": {
      "asId": 134,
      "id": "W:0000f519feec486de87ed73cb92d3cac802400000000!0000e8f207634e304790b099454338b819d302024d7b!explorer.exe",
      "ver": "2093/07/26:17:32:14!4AB6D7!explorer.exe"
    },
    "device": {
      "deviceClass": "Windows.Desktop",
      "localId": "s:CC7502F9-996D-4855-8CAE-EB0B86CB4E01"
    },
    "loc": {
      "tz": "+09:00"
    },
    "metadata": {
      "f": {
        "formatDuration": 5,
        "formatVolumeId": 8
      }
    },
    "os": {
      "bootId": 5,
      "name": "Windows",
      "ver": "10.0.19043.1110.amd64fre.vb_release.191206-1406"
    },
    "protocol": {
      "devMake": "LG Electronics",
      "devModel": "17ZD90N-VX7BK"
    },
    "user": {
      "localId": "w:CCC59980-EE80-654A-649E-0A2579080012"
    },
    "utc": {
      "aId": "526F7192-82F0-0005-B62A-7052F082D701",
      "epoch": "600060",
      "eventFlags": 257,
      "flags": 205521456,
      "pgName": "WIN",
      "popSample": 2,
      "seq": 41039,
      "shellId": 33786497904279555
    }
  },
  "iKey": "o:0a89d516ae714e01ae89c96d185e9ae3",
  "name": "Microsoft.Windows.FileSystem.Chkdsk.Format",
  "time": "2021-07-27T23:10:19.9040257Z",
  "ver": "4.0"
}

```

위 기록을 모두 종합하면 2021-07-26 15:38:56 에 연결된 장치는 2021-07-26 16:04:45 에 제거되면서 연결이 해제되었고, 2021-07-27 23:10:06 에 연결된 장치는 2021-07-27 23:10:19 에 포맷되면서 마운트가 해제되었고 포맷 완료 이후 다시 마운트되었다. 이후 2021-07-27 23:45:35 에 장치가 제거되며 연결이 해제되었다.