

## 306 – Event Logs

### Team Information

Team Name : DogeCoin

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

Email Address : dfc-dogecoin@naver.com

### Instructions

**Description** The event logs were collected from the laptop. Analyze the event logs and answer the questions.

Target	Hash (MD5)
EventLogs.7z	2358D1E407DF48C37CB08691F87786D1

### Questions

1. List all files opened with MS Office. (20 points)
2. List all malware diagnosed by Windows Defender. (20 points)
3. What is the ISO format file used by the user? (20 points)
4. What is the product name and IP address of the registered network printer? (20 points)
5. List files printed with "Microsoft Print to PDF". (20 points)
6. Fast Startup that allows the computer start up faster after a shutdown is enabled by default in Windows 10. List all boot dates/times with the Fast Startup. (20 points)
7. Is there any evidence that the user has changed the system time? If so, when and how did the user change the system time? (20 points)
8. List the history of wireless connection via smartphone tethering. (20 points)
  - Connected date/time
  - Disconnected date/time

- SSID
  - Authentication Algorithm
9. List the details of the connected internal storage device (connected to the board). (20 points)
- Manufacturer
  - Model
  - Serial Number
  - Bus Type
  - Capacity
  - Volume Serial Number
10. List the details of the connected external hard disk. (20 points)
- Manufacturer
  - Model
  - Serial Number
  - Bus Type
  - Capacity
  - Volume Serial Number
11. List all connected/disconnected date/time of the "SanDisk Cruzer Blade(4C530001180715107241)" device. (50 points)
12. What is the external storage device where the program "SystemCollector\_x86.exe" was stored? (50 points)
- Manufacturer
  - Model
  - Serial Number

**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:	Message Analyzer	Publisher:	Microsoft
Version:	1.4		
URL:	<a href="https://github.com/riverar/messageanalyzer-archive">https://github.com/riverar/messageanalyzer-archive</a>		

## Step-by-step methodology:

본 보고서의 모든 시각은 UTC+9 (KST) 기준으로 표기하였음

### 1. List all files opened with MS Office. (20 points)

```
EventLog.Channel == "OAlerts"
```

[그림 1] 필터링 구문: MS Office를 통해 열람한 파일에 대한 이벤트

Name	Value	Bit Offset	Bit Length	Type
EventID	300 (0x0000012C)			Int32
Keywords	36028797018963968 (0x0080000000000000)			Int64
Level	4 (0x04)			Byte
LevelDisplayName	Informational			String
Channel	OAlerts			String
Computer	DESKTOP-RIKMTTV			String
Opcode	0 (0x0000)			Int16
OpcodeDisplayName	Info			String
ProcessId	0 (0x00000000)			Int32
EventData	map{0=Microsoft Excel			MapValue
0	Microsoft Excel			String
1	'BrowsingHistory.csv'의 변경 내용을 저장하시겠습니까?			String
2	100216			String
3	16.0.14131.20332			String
4				String
5				String
ProviderName	Microsoft Office 16 Alerts			String
Qualifiers	0 (0x00000000)			Int32
EventRecordID	10 (0x00000000000000A)			Int64
Task	0 (0x00000000)			Int32
TaskDisplayName	None			String
ThreadId	0 (0x00000000)			Int32
TimeCreated	2021-07-28T16:44:56.7040723			DateTime

[그림 2] OAlerts.evtx에 기록된 EventID 300의 상세 내용

Office와 관련해서 알람창이 발생했을 때, 관련 정보를 OAlerts 채널을 통해서 확인할 수 있다. 해당 채널에서 발생하는 이벤트는 문서의 전체 경로가 아닌, 문서의 파일명만 기록된다. 이 사실을 바탕으로 필터링 구문 작성하였다. 해당 필터링 구문을 수행한 결과 중에서 “문서 명”을 식별할 수 있는 것을 정리하면 아래 표와 같다.

타임라인	문서 명	사용 소프트웨어
2021-07-27 00:29:00	문서1	Microsoft Word
2021-07-27 00:38:25	IR300 - Attacker Behavior Analytics.docx	Microsoft Word
2021-07-27 00:40:59	Timeline.xlsx	Microsoft Excel
2021-07-28 02:01:57	Hindsight_output.xlsx	Microsoft Excel
2021-07-28 14:37:37	test.csv	Microsoft Excel
2021-07-28 16:37:55	victim_timeline.xlsx	Microsoft Excel
2021-07-28 16:44:56	BrowsingHistory.csv	Microsoft Excel

[표 1] MS Office를 통해 열람한 파일 목록

## 2. List all malware diagnosed by Windows Defender. (20 points)

```
EventLog.Channel == "Microsoft-Windows-Windows Defender/Operational" and
EventLog.EventID == 1116
```

[그림 3] 필터링 구문: Windows Defender가 검출한 악성코드에 대한 이벤트

Name	Value	Bit Offset	Bit
Keywords	-9223372036854775808 (@x8000000000000000)		
Level	3 (0x03)		
LevelDisplayName	경고		
Channel	Microsoft-Windows-Windows Defender/Operational		
Computer	DESKTOP-RIKMTTV		
Opcode	0 (0x0000)		
OpcodeDisplayName	정보		
ProcessId	4896 (0x00001328)		
EventData	map(Product Name=Microsoft Defender 바이러스 백신, Product Version=4.18.2106.6,0... 11cd958a-c587-4ef3-b5f2-5fd9dfbd2c78 ProviderName Microsoft-Windows-Windows Defender EventRecordID 142 (0x000000000000008E) Task 0 (0x00000000)		
TaskDisplayName			
ThreadId	7508 (0x00001054)		
TimeCreated	2021-07-28T01:49:04.6608427		
Version	0 (0x00)		
Message	Microsoft Defender 바이러스 백신이(가) 멀웨어 또는 기타 사용자 동의 없이 설치된 소...		
UserId	S-1-5-18		

Microsoft Defender 바이러스 백신이(가) 멀웨어 또는 기타 사용자 동의 없이 설치된 소프트웨어를 검색했습니다.  
자세한 내용은 다음을 참조하십시오.  
<https://go.microsoft.com/fwlink/?linkid=37020&name=TrojanDownloader:Win32/Aicat.Alm!&thetrid=2147771506&enterprise=0>  
이름: TrojanDownloader:Win32/Aicat.Alm!  
ID: 2147771506  
심각도: 심각  
범주: Trojan Downloader  
경로: file\_E:\#DFIR\DATA\CASE#2\root\Users\victim2\Downloads\입사지원서\AlkalineJi\_Won\_Seo\_Resume.doc  
작성자: E:\#DFIR\DATA\CASE#2\root\Users\victim2\Downloads\입사지원서\AlkalineJi\_Won\_Seo\_Resume.doc  
사용자: DESKTOP-RIKMTTV\forensicator  
프로세스 이름: E:\www\_forensics203\kwforensics64.exe  
보안 인텔리전스 버전: AV: 1.343.1753.0, AS: 1.343.1753.0, NIS: 1.343.1753.0  
엔진 버전: AM: 1.1.18300.4, NIS: 1.1.18300.4

[그림 4] Windows Defender가 검출한 악성코드에 대한 이벤트 상세 내용

Microsoft-Windows-Windows Defender/Operational 은 Windows Defender 와 어떤 행동을 했을 때 관련 로그들을 기록한다. 특히, 1116 이벤트는 검출한 악성코드에 대한 정보를 포함하며, 검출한 악성코드 목록을 정리하면 아래 표와 같다.

타임라인	경로
2021-07-28 01:49:04	E:\#DFIR\DATA\CASE#2\root\Users\victim2\Downloads\입사지원서\AlkalineJi_Won_Seo_Resume.doc
2021-07-28 01:49:37	E:\#DFIR\DATA\CASE#2\root\Users\victim2\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\hi.exe
2021-07-28 01:49:38	E:\#DFIR\DATA\CASE#2\root\Users\victim2\AppData\Roaming\DtServ32.exe
2021-07-28 01:49:38	E:\#DFIR\DATA\CASE#2\root\Users\victim2\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\hi.exe
2021-07-28 02:03:40	F:\Users\victim\Desktop\a3dc83.exe

[표 2] Windows Defender가 검출한 악성코드 목록

### 3. What is the ISO format file used by the user? (20 points)

```
EventLog.Channel == "Microsoft-Windows-VHDMP-Operational"      and
EventLog.EventID == 25                                         and
EventLog.Message contains ".iso"
```

[그림 5] 필터링 구문: 사용자가 사용한 ISO 파일에 대한 이벤트

Details 1		Field Data	
Name	Value	Bit Offset	Bit Len
EventID	25 (0x00000019)		
Keywords	-9223372036854775807 (0x8000000000000001)		
Level	4 (0x04)		
LevelDisplayName	정보		
Channel	Microsoft-Windows-VHDMP-Operational		
Computer	DESKTOP-RKHMIVV		
Opcode	1 (0x0001)		
OpcodeDisplayName	시작		
ProcessId	5088 (0x000013E0)		
EventData	map{VhdFileName=F:\#IMAGES\2021-07-26T151017_210727_FCase.vhdx,VirtualDisk=184..e2816346-87f4-4f85-95c3-0c79409aa89d}		
ProviderId	e2816346-87f4-4f85-95c3-0c79409aa89d		
ProviderName	Microsoft-Windows-VHDMP		
EventRecordID	10 (0x000000000000000A)		
Task	1205 (0x0000004B5)		
TaskDisplayName	Surface Virtual Disk		
Threadid	6704 (0x00001A30)		
TimeCreated	2021-07-27T00:13:45.5394927		
Version	0 (0x00)		
Message	VHD F:\#IMAGES\2021-07-26T151017_210727_FCase.vhdx 온라인 상태로 전환하기 시작합...		

[그림 6] 사용자가 사용한 ISO 파일에 대한 이벤트 상세 내용

Microsoft-Windows-VHDMP-Operational에는 Windows가 가상 디스크 파일을 마운트했을 때 발생하는 이벤트가 기록되는 채널이다. 25 이벤트는 가상 디스크 파일이 마운트가 완료되어, 볼륨을 할당 받는 것까지 완료했을 때 발생한다. 사용자가 사용한 ISO 파일을 확인하기 위해서, “.iso” 문자열을 포함하는 이벤트만 필터링하였다. [그림 5]의 필터링 구문을 수행한 결과를 정리하면 아래 표와 같다.

타임라인	경로
2021-07-27 00:18:23	E:\PROGRAMS\Adobe CS3 Design Premium (korean)\Adobe CS3 DP Korea.iso

[표 3] 사용자가 사용한 ISO 파일 목록

**4. What is the product name and IP address of the registered network printer?**  
**(20 points)**

EventLog.Channel == "Microsoft-Windows-PrintService/Operational" and  
EventLog.EventID in [300, 307]

[그림 7] 필터링 구문: 프린터 등록 및 인쇄에 대한 이벤트

The screenshot shows the Windows Event Viewer interface. A single event entry is selected in the main pane:

```

Name: Value
EventID: 300 (0x0000012C)
Keywords: 4611686018427389984 (0x40000000000000820)
Level: 4 (0x04)
LevelDisplayName: 정보
Channel: Microsoft-Windows-PrintService/Operational
Computer: DESKTOP-RIKMTTV
Opcode: 11 (0x0008)
OpcodeDisplayName: 스플리 작업 성공
ProcessId: 3804 (0x000000DC)
EventData:
ProviderId: 747ef6fd-e535-4d16-b510-42c90f6873a1
ProviderName: Microsoft-Windows-PrintService
EventRecordID: 11 (0x00000000000000B)
Task: 4 (0x00000004)
TaskDisplayName: 프린터를 추가하는 중
Threadid: 1864 (0x00000048)
TimeCreated: 2021-07-27T23:31:17.8118892
Version: 0 (0x00)
Message: IR C3125 프린터를 만들었습니다. 사용자 작업은 필요하지 않습니다.
UserId: S-1-5-21-2949964769-1086094253-4195774485-1001

```

The message field contains the text: "IR C3125 프린터를 만들었습니다. 사용자 작업은 필요하지 않습니다." (IR C3125 printer was created. No user action required.)

[그림 8] 프린터 등록에 대한 이벤트 상세 내용 (Event ID: 300)

This screenshot shows the same event entry from the Event Viewer, but with more details visible in the right-hand pane:

Field Data pane content:

```

문서 3, 문서 인쇄(소유자: Forensicator, 위치: \\DESKTOP-RIKMTTV\(\)) IR C3125(P_10.10.10.242 포트)에서 인쇄되었습니다. 크기: 1239833바이트, 인쇄된 페이지: 4. 사용자 작업은 필요하지 않습니다.

```

[그림 9] 인쇄에 대한 이벤트 상세 내용 (Event ID: 307)

Microsoft-Windows-PrintService/Operational 채널에는 프린터와 관련된 이벤트가 기록된다. 300 이벤트는 새로운 프린터를 등록했을 때 발생하는 이벤트이며, 프린터 모델명을 포함한다. 또한, 네트워크 프린터라면, 할당 받은 IP 도 기록된다. 307 이벤트는 프린터를 이용해서 인쇄를 했을 때 발생하는 이벤트다. 300 이벤트와 비슷하게 인쇄한 프린터의 모델명 (param 5), 할당 받은 IP (param 6) 등이 기록된다. 이러한 사실을 바탕으로 필터링 구문을 작성하였으며, 필터링 구문 수행을 통해서 나온 목록 중에서 네트워크 프린터와 관련된 이벤트로 정리하면 아래 표와 같다.

인쇄 시작	프린터 모델명	IP 주소
2021-07-27 23:31:17	IR C3125	10.10.10.242

[표 4] 네트워크 프린터 목록

## 5. List files printed with “Microsoft Print to PDF”. (20 points)

```
EventLog.Channel == "Microsoft-Windows-PrintService/Operational" and
EventLog.EventID == 307 and
EventLog.EventData["param5"] == "Microsoft Print to PDF"
```

[그림 10] 필터링 구문: “Microsoft Print to PDF” 흔적 관련 이벤트

The screenshot shows the Windows Event Viewer interface. A search bar at the top contains the filter: "EventLog.Channel == 'Microsoft-Windows-PrintService/Operational' and EventLog.EventID == 307 and EventLog.EventData['param5'] == 'Microsoft Print to PDF'". The main pane displays a list of event details. One event is expanded, showing its properties. The expanded event details are as follows:

Name	Value	Bit Offset	Bit Length	Type
OpcodeDisplayName	스풀러 작업 성공			String
ProcessId	4008 (0x00000fA8)			Int32
EventData	map{param1=2,param2=문서 인쇄,param3=F...}			MapValue
param1	2			String
param2	문서 인쇄			String
param3	Forensicator			String
param4	\\\DESKTOP-RIKMTTV			String
param5	Microsoft Print to PDF			String
param6	C:\Users\Forensicator\Desktop\Functions of AXIOM.pdf			String
param7	1729193			String
param8	22			String
ProviderId	747ef6fd-e535-4d16-b510-42c90f6873a1			Guid
ProviderName	Microsoft-Windows-PrintService			String
EventRecordID	9 (0x0000000000000009)			Int64
Task	26 (0x0000001A)			Int32
TaskDisplayName	문서를 인쇄하는 중			String
Threadid	7936 (0x00001F00)			Int32
TimeCreated	2021-07-27T00:45:09.4322022			DateTime
Version	0 (0x00)			Byte
Message	문서 2, 문서 인쇄(소유자: Forensicator,...)			String
UserId	S-1-5-21-2949964769-1086094253-419577...			String

Right-click context menu options like 'Copy' and 'Paste' are visible above the table.

[그림 11] “Microsoft Print to PDF” 출력에 대한 이벤트 상세 내용 (Event ID: 307)

300 이벤트는 인쇄를 했을 때 발생하며, param 5를 통해서 프린터의 모델명을 알 수 있다고 앞서 언급하였다. “Microsoft Print to PDF”로 문서를 PDF로 출력했을 경우에도, param 5에 “Microsoft Print to PDF”로 기록된다. 이러한 사실을 바탕으로 필터링 구문을 작성하였으며, 해당 필터링 구문을 수행한 결과를 정리하면 아래 표와 같다.

인쇄 시작	경로
2021-07-27 00:45:09	C:\Users\Forensicator\Desktop\Functions of AXIOM.pdf
2021-07-28 15:55:22	C:\Users\Forensicator\Desktop\AXIOM Examine.pdf

[표 5] “Microsoft Print to PDF”로 출력한 목록

**6. Fast Startup that allows the computer start up faster after a shutdown is enabled by default in Windows 10. List all boot dates/times with the Fast Startup. (20 points)**

```
EventLog.ProviderName == "Microsoft-Windows-Power-Troubleshooter" and
EventLog.EventID == 1
```

[그림 12] 필터링 구문: 절전 모드 진입 및 복귀 이벤트

Timestamp	Message	EventData.SleepTime	EventData.WakeTime
2021-07-21T08:39:01.2510801	시스템이 저전원 상태에서 복귀되었습니다.	2021-07-21T06:02:04.5412454	2021-07-21T08:38:59.2372509
2021-07-21T14:28:00.8145225	시스템이 저전원 상태에서 복귀되었습니다.	2021-07-21T08:41:16.1240973	2021-07-21T14:27:59.1885980
2021-07-22T00:38:51.3112517	시스템이 저전원 상태에서 복귀되었습니다.	2021-07-22T00:22:46.9704007	2021-07-22T00:38:49.3011643
2021-07-23T19:04:06.8250737	시스템이 저전원 상태에서 복귀되었습니다.	2021-07-22T00:47:04.2645129	2021-07-23T19:04:05.1947527
2021-07-25T09:02:26.8291619	시스템이 저전원 상태에서 복귀되었습니다.	2021-07-23T19:47:48.8951086	2021-07-25T09:02:25.1818311
2021-07-26T20:39:33.39991882	시스템이 저전원 상태에서 복귀되었습니다.	2021-07-25T15:48:49.8495381	2021-07-26T20:39:31.3903886
2021-07-27T18:26:50.5111830	시스템이 저전원 상태에서 복귀되었습니다.	2021-07-27T01:05:24.8556251	2021-07-27T18:26:48.5517235
2021-07-28T19:03:41.1411959	시스템이 저전원 상태에서 복귀되었습니다.	2021-07-28T17:40:12.3669407	2021-07-28T19:03:39.2484738

[그림 13] 절전 모드 진입 및 복귀 이벤트 목록

Fast Startup(빠른 시작 켜기)은 부팅 속도 향상을 위해서 Windows 10 부터 도입된 기술이다. Fast Startup 은 기능은 기본적으로 활성화된다. PC 종료 버튼을 통해 종료했을 때, 최대 절전모드에 진입한 것과 같이 동작한다<sup>1</sup>. 따라서, 최대 절전모드와 관련된 이벤트에서 Fast Startup 활성화에 따른 부팅 및 종료 시각을 알 수 있다. 이러한 정보를 바탕으로 필터링 구문을 작성하였으며, 부팅 및 종료 시각을 정리하면 아래 표와 같다.

타임라인	행위
2021-07-21 06:02:04	종료
2021-07-21 08:38:59	부팅
2021-07-21 08:41:16	종료
2021-07-21 14:27:59	부팅
2021-07-22 00:22:46	종료
2021-07-22 00:38:49	부팅
2021-07-22 00:47:04	종료
2021-07-23 19:04:05	부팅
2021-07-23 19:47:48	종료
2021-07-25 09:02:25	부팅
2021-07-25 15:48:49	종료
2021-07-26 20:39:31	부팅
2021-07-27 01:05:24	종료
2021-07-27 18:26:48	부팅
2021-07-28 17:40:12	종료

[표 6] 부팅 및 종료 시각 목록

<sup>1</sup> 방수민, 진필근, 김동현, 박정흠, 이상진, 박아란, ... & 정일훈. (2021). Windows 10 내의 hiberfil.sys 파일에 대한 포렌식 활용 방안. 디지털포렌식연구, 15(1), 125-136.

7. Is there any evidence that the user has changed the system time? If so, when and how did the user change the system time? (20 points)

```
(  
    EventLog.ProviderName == "Microsoft-Windows-Kernel-General"    and  
    EventLog.EventID == 1  
) or  
(  
    EventLog.ProviderName == "Microsoft-Windows-Security-Auditing"    and  
    EventLog.EventID == 4616  
)
```

[그림 14] 필터링 구문: 시간 변경 이벤트

Timestamp	EventID	Message	EventData.PreviousTime	EventData.OldTime	EventData.NewTime
2021-03-01T09:10:24...	1	[시스템 시간이 2021-07-26T13:23:48.6814087002에서 2021-03-01T09:10:24.2350000002(으)로]	2021-07-26T22:23:48...	2021-03-01T09:10:24...	2021-03-01T09:10:24...
2021-03-01T09:10:24...	4616	시스템 시간이 변경되었습니다.	2021-07-26T22:23:48...	2021-03-01T09:10:24...	2021-03-01T09:10:24...
2021-03-01T09:10:24...	1	시스템 시간이 2021-03-01T00:10:24.2350000002에서 2021-03-01T00:10:24.2350000002(으)로...	2021-03-01T00:10:24...	2021-03-01T09:10:24...	2021-03-01T09:10:24...
2021-03-01T09:10:24...	4616	시스템 시간이 변경되었습니다.	2021-03-01T09:10:24...	2021-03-01T09:10:24...	2021-03-01T09:10:24...

[그림 15] 시간 변경 이벤트 목록

<table border="1"> <tr><td>Name</td><td>Value</td></tr> <tr><td>EventID</td><td>1 (0x00000001)</td></tr> <tr><td>Keywords</td><td>-9223372036854775792 (0x8000000000000010)</td></tr> <tr><td>Level</td><td>4 (0x04)</td></tr> <tr><td>LevelDisplayName</td><td>정보</td></tr> <tr><td>Channel</td><td>System</td></tr> <tr><td>Computer</td><td>DESKTOP-RIKMTTV</td></tr> <tr><td>Opcode</td><td>0 (0x0000)</td></tr> <tr><td>OpcodeDisplayName</td><td>정보</td></tr> <tr><td>ProcessId</td><td>10604 (0x0000296C)</td></tr> <tr><td>EventData</td><td>map(NewTime=2021-03-01 오전 9:10:24, OldTime=2021-07-26 오후 10:23:48, ProcessId=10604, PreviousTime=2021-03-01T09:10:24.2350000000, NewTime=2021-03-01T09:10:24.2350000000, OldTime=2021-07-26T22:23:48.6814087)</td></tr> <tr><td>NewTime</td><td>2021-03-01T09:10:24.2350000000</td></tr> <tr><td>OldTime</td><td>2021-07-26T22:23:48.6814087</td></tr> <tr><td>Reason</td><td>1 (0x00000001)</td></tr> <tr><td>ProcessName</td><td>\Device\HarddiskVolume4\Windows\System32\SystemSettingsAdminFlows.exe</td></tr> <tr><td>ProcessID</td><td>10604 (0x0000296C)</td></tr> <tr><td>ProviderId</td><td>a68ca8b7-004f-d7b6-a698-07e2de0f1f5d</td></tr> <tr><td>ProviderName</td><td>Microsoft-Windows-Kernel-General</td></tr> <tr><td>EventRecordID</td><td>1067 (0x000000000000042B)</td></tr> <tr><td>Task</td><td>5 (0x00000005)</td></tr> <tr><td>TaskDisplayName</td><td>Security state change</td></tr> <tr><td>Threadid</td><td>9500 (0x0000251C)</td></tr> <tr><td>TimeCreated</td><td>2021-03-01T09:10:24.2355188</td></tr> <tr><td>Version</td><td>2 (0x02)</td></tr> <tr><td>Message</td><td>시스템 시간이 2021-07-26T13:23:48.6814087002에서 2021-03-01T00:10:24.2350000002(으)로...</td></tr> <tr><td>UserId</td><td>5-1-5-21-2949964769-1086094253-4195774485-1001</td></tr> </table>	Name	Value	EventID	1 (0x00000001)	Keywords	-9223372036854775792 (0x8000000000000010)	Level	4 (0x04)	LevelDisplayName	정보	Channel	System	Computer	DESKTOP-RIKMTTV	Opcode	0 (0x0000)	OpcodeDisplayName	정보	ProcessId	10604 (0x0000296C)	EventData	map(NewTime=2021-03-01 오전 9:10:24, OldTime=2021-07-26 오후 10:23:48, ProcessId=10604, PreviousTime=2021-03-01T09:10:24.2350000000, NewTime=2021-03-01T09:10:24.2350000000, OldTime=2021-07-26T22:23:48.6814087)	NewTime	2021-03-01T09:10:24.2350000000	OldTime	2021-07-26T22:23:48.6814087	Reason	1 (0x00000001)	ProcessName	\Device\HarddiskVolume4\Windows\System32\SystemSettingsAdminFlows.exe	ProcessID	10604 (0x0000296C)	ProviderId	a68ca8b7-004f-d7b6-a698-07e2de0f1f5d	ProviderName	Microsoft-Windows-Kernel-General	EventRecordID	1067 (0x000000000000042B)	Task	5 (0x00000005)	TaskDisplayName	Security state change	Threadid	9500 (0x0000251C)	TimeCreated	2021-03-01T09:10:24.2355188	Version	2 (0x02)	Message	시스템 시간이 2021-07-26T13:23:48.6814087002에서 2021-03-01T00:10:24.2350000002(으)로...	UserId	5-1-5-21-2949964769-1086094253-4195774485-1001	<table border="1"> <tr><td>Name</td><td>Value</td></tr> <tr><td>Level</td><td>0 (0x00)</td></tr> <tr><td>LevelDisplayName</td><td>정보</td></tr> <tr><td>Channel</td><td>Security</td></tr> <tr><td>Computer</td><td>DESKTOP-RIKMTTV</td></tr> <tr><td>Opcode</td><td>0 (0x0000)</td></tr> <tr><td>OpcodeDisplayName</td><td>정보</td></tr> <tr><td>ProcessId</td><td>4 (0x00000004)</td></tr> <tr><td>EventData</td><td>map(SubjUserSid=S-1-5-21-2949964769-1086094253-4195774485-1001, SubjUserName=Forensicator, SubjDomainName=DESKTOP-RIKMTTV, SubjLogonId=158181 (0x00000000000269E5))</td></tr> <tr><td>PreviousTime</td><td>2021-07-26T22:23:48.6814087</td></tr> <tr><td>NewTime</td><td>2021-03-01T09:10:24.2350000000</td></tr> <tr><td>ProcessId</td><td>10604 (0x0000000000000296C)</td></tr> <tr><td>ProcessName</td><td>C:\Windows\System32\SystemSettingsAdminFlows.exe</td></tr> <tr><td>ProviderId</td><td>54849625-5478-4994-a5ba-3e3b0328c30d</td></tr> <tr><td>ProviderName</td><td>Microsoft-Windows-Security-Auditing</td></tr> <tr><td>EventRecordID</td><td>4581 (0x000000000000011E9)</td></tr> <tr><td>Task</td><td>12288 (0x00003000)</td></tr> <tr><td>TaskDisplayName</td><td>Security state change</td></tr> <tr><td>Threadid</td><td>7372 (0x00001CC)</td></tr> <tr><td>TimeCreated</td><td>2021-03-01T09:10:24.2356629</td></tr> <tr><td>Version</td><td>1 (0x01)</td></tr> <tr><td>Message</td><td>시스템 시간이 변경되었습니다.</td></tr> </table>	Name	Value	Level	0 (0x00)	LevelDisplayName	정보	Channel	Security	Computer	DESKTOP-RIKMTTV	Opcode	0 (0x0000)	OpcodeDisplayName	정보	ProcessId	4 (0x00000004)	EventData	map(SubjUserSid=S-1-5-21-2949964769-1086094253-4195774485-1001, SubjUserName=Forensicator, SubjDomainName=DESKTOP-RIKMTTV, SubjLogonId=158181 (0x00000000000269E5))	PreviousTime	2021-07-26T22:23:48.6814087	NewTime	2021-03-01T09:10:24.2350000000	ProcessId	10604 (0x0000000000000296C)	ProcessName	C:\Windows\System32\SystemSettingsAdminFlows.exe	ProviderId	54849625-5478-4994-a5ba-3e3b0328c30d	ProviderName	Microsoft-Windows-Security-Auditing	EventRecordID	4581 (0x000000000000011E9)	Task	12288 (0x00003000)	TaskDisplayName	Security state change	Threadid	7372 (0x00001CC)	TimeCreated	2021-03-01T09:10:24.2356629	Version	1 (0x01)	Message	시스템 시간이 변경되었습니다.
Name	Value																																																																																																
EventID	1 (0x00000001)																																																																																																
Keywords	-9223372036854775792 (0x8000000000000010)																																																																																																
Level	4 (0x04)																																																																																																
LevelDisplayName	정보																																																																																																
Channel	System																																																																																																
Computer	DESKTOP-RIKMTTV																																																																																																
Opcode	0 (0x0000)																																																																																																
OpcodeDisplayName	정보																																																																																																
ProcessId	10604 (0x0000296C)																																																																																																
EventData	map(NewTime=2021-03-01 오전 9:10:24, OldTime=2021-07-26 오후 10:23:48, ProcessId=10604, PreviousTime=2021-03-01T09:10:24.2350000000, NewTime=2021-03-01T09:10:24.2350000000, OldTime=2021-07-26T22:23:48.6814087)																																																																																																
NewTime	2021-03-01T09:10:24.2350000000																																																																																																
OldTime	2021-07-26T22:23:48.6814087																																																																																																
Reason	1 (0x00000001)																																																																																																
ProcessName	\Device\HarddiskVolume4\Windows\System32\SystemSettingsAdminFlows.exe																																																																																																
ProcessID	10604 (0x0000296C)																																																																																																
ProviderId	a68ca8b7-004f-d7b6-a698-07e2de0f1f5d																																																																																																
ProviderName	Microsoft-Windows-Kernel-General																																																																																																
EventRecordID	1067 (0x000000000000042B)																																																																																																
Task	5 (0x00000005)																																																																																																
TaskDisplayName	Security state change																																																																																																
Threadid	9500 (0x0000251C)																																																																																																
TimeCreated	2021-03-01T09:10:24.2355188																																																																																																
Version	2 (0x02)																																																																																																
Message	시스템 시간이 2021-07-26T13:23:48.6814087002에서 2021-03-01T00:10:24.2350000002(으)로...																																																																																																
UserId	5-1-5-21-2949964769-1086094253-4195774485-1001																																																																																																
Name	Value																																																																																																
Level	0 (0x00)																																																																																																
LevelDisplayName	정보																																																																																																
Channel	Security																																																																																																
Computer	DESKTOP-RIKMTTV																																																																																																
Opcode	0 (0x0000)																																																																																																
OpcodeDisplayName	정보																																																																																																
ProcessId	4 (0x00000004)																																																																																																
EventData	map(SubjUserSid=S-1-5-21-2949964769-1086094253-4195774485-1001, SubjUserName=Forensicator, SubjDomainName=DESKTOP-RIKMTTV, SubjLogonId=158181 (0x00000000000269E5))																																																																																																
PreviousTime	2021-07-26T22:23:48.6814087																																																																																																
NewTime	2021-03-01T09:10:24.2350000000																																																																																																
ProcessId	10604 (0x0000000000000296C)																																																																																																
ProcessName	C:\Windows\System32\SystemSettingsAdminFlows.exe																																																																																																
ProviderId	54849625-5478-4994-a5ba-3e3b0328c30d																																																																																																
ProviderName	Microsoft-Windows-Security-Auditing																																																																																																
EventRecordID	4581 (0x000000000000011E9)																																																																																																
Task	12288 (0x00003000)																																																																																																
TaskDisplayName	Security state change																																																																																																
Threadid	7372 (0x00001CC)																																																																																																
TimeCreated	2021-03-01T09:10:24.2356629																																																																																																
Version	1 (0x01)																																																																																																
Message	시스템 시간이 변경되었습니다.																																																																																																

[그림 16] 시간 변경 이벤트 상세 정보 (좌 - Event ID 1, 우 - Event ID 4616)

“Microsoft-Windows-Kernel-General” Provider 가 발생하는 1 이벤트와 “Microsoft-Windows-Security-Auditing” Provider 가 발생하는 4616 이벤트를 통해서 시간 변경을 확인할 수 있다. 특히, 시간 변경에 관여한 프로세스가 “SystemSettingsAdminFlows.exe”일 경우, 사용자가 직접 시간 변경한 것이다. 실제로, 4616 이벤트의 SubjectUserName 을 확인하면 “Forensicator”라는 사용자가 변경한 것을 알 수 있다.

시간 변경이 발생하면, 기록되는 이벤트의 시간도 변경된 시각을 기준으로 작성되므로, 이벤트 로그에는 “변경 후 시각”으로 기록된다. 따라서, 이벤트에 기록된 “변경 전 시각”이 시간 변경을 수행한 시간이다. 이를 정리하면 다음과 같다.

시간 변경 시각	변경 전 시각	변경 후 시각
2021-07-26 22:23:48	2021-07-26 22:23:48	2021-03-01 09:10:24

[표 7] 사용자가 시간을 변경한 시점 및 변경 전/후 시각

## 8. List the history of wireless connection via smartphone tethering. (20 points)

```
EventLog.Channel == "Microsoft-Windows-WLAN-AutoConfig/Operational" and
(
    EventLog.EventID == 11000 or
    EventLog.EventID == 11010
)
```

[그림 14] 필터링 구문: 무선 네트워크 연결에 대한 이벤트

Timestamp	EventID	Summary	EventData.SSID	EventData.Auth	EventData.Cipher
EventData.SSID (16): iptime					
EventData.SSID (4): JK's iPhone					
2021-07-26T21:45:12.9709952 11000	11000	무선 네트워크 연결을 시작했습니다.	JK's iPhone	WPA2-Personal	AES-CCMP
2021-07-26T21:45:13.2449184 11010	11010	무선 보안을 시작했습니다.	JK's iPhone	WPA2-Personal	AES-CCMP
2021-07-26T22:17:07.8105100 11000	11000	무선 네트워크 연결을 시작했습니다.	JK's iPhone	WPA2-Personal	AES-CCMP
2021-07-26T22:17:07.9808658 11010	11010	무선 보안을 시작했습니다.	JK's iPhone	WPA2-Personal	AES-CCMP
EventData.SSID (43): KT_Giga_5G_Wave2_6E0B					
EventData.SSID (3): KT_starbucks					
EventData.SSID (14): SSOL 5G					

[그림 15] 무선 네트워크 연결 흔적

Microsoft-Windows-WLAN-AutoConfig/Operational 채널에는 무선 네트워크와 관련된 이벤트가 발생한다. 11000 이벤트는 무선 네트워크 연결을 시작했을 때 발생하며, 11010은 무선 네트워크 연결 이후, 보안이 활성화되었을 때 발생한다.

이러한 이벤트로 무선 네트워크 연결 흔적을 확인할 수 있으며, 이러한 사실을 바탕으로 필터링 구문을 작성하였다. 필터링 구문을 수행하면, 스마트폰 테더링 연결 흔적도 확인할 수 있었다. 스마트폰 테더링 시, SSID는 “XX's smartphone” 형식으로 기본적으로 지정된다. 이러한 특징을 활용하여 스마트폰 테더링 연결 흔적을 식별하였으며, 이를 정리하면 아래 표와 같다.

타임라인	Event ID	SSID	Authentication Method	Cipher Algorithm
2021-07-26 21:45:12	11000 (연결)	JK's iPhone	WPA2-Personal	AES-CCMP
2021-07-26 21:45:13	11010 (해제)	JK's iPhone	WPA2-Personal	AES-CCMP
2021-07-26 22:17:07	11000 (연결)	JK's iPhone	WPA2-Personal	AES-CCMP
2021-07-26 22:17:07	11010 (해제)	JK's iPhone	WPA2-Personal	AES-CCMP

[표 8] 스마트폰 테더링 연결 흔적

**9. List the details of the connected internal storage device (connected to the board). (20 points)**

```
EventLog.Channel == "Microsoft-Windows-Partition/Diagnostic"      and
EventLog.EventID == 1006                                         and
EventLog.EventData["ParentId"] contains "PCI\\\"
```

[그림 16] 필터링 구문: 메인보드에 연결한 Internal storage device에 대한 이벤트

Data.Model	EventData.SerialNumber	EventData.Manufacturer	EventData.BusType	EventData.Capacity	EventData.Location
<b>tdata.SerialNumber (6) :</b> 0100_0000_0000_0000.					
HP SSD EX900 1TB	0100_0000_0000_0000.	NULL	17	1000204886016	PCI Slot 12 : Bus 44 : Device 0 : Function 0 : Adapter 1
HP SSD EX900 1TB	0100_0000_0000_0000.	NULL	17	1000204886016	PCI Slot 12 : Bus 44 : Device 0 : Function 0 : Adapter 1
HP SSD EX900 1TB	0100_0000_0000_0000.	NULL	17	1000204886016	PCI Slot 12 : Bus 44 : Device 0 : Function 0 : Adapter 1
HP SSD EX900 1TB	0100_0000_0000_0000.	NULL	17	1000204886016	PCI Slot 12 : Bus 44 : Device 0 : Function 0 : Adapter 1
HP SSD EX900 1TB	0100_0000_0000_0000.	NULL	17	1000204886016	PCI Slot 12 : Bus 44 : Device 0 : Function 0 : Adapter 1
HP SSD EX900 1TB	0100_0000_0000_0000.	NULL	17	1000204886016	PCI Slot 12 : Bus 44 : Device 0 : Function 0 : Adapter 1
<b>tdata.SerialNumber (6) :</b> NJ02N892910503264 _00000001.					
HFS256GD9TNG-L2A0A	NJ02N892910503264 _00000001.	NULL	17	256060514304	PCI Slot 8 : Bus 43 : Device 0 : Function 0 : Adapter 0
HFS256GD9TNG-L2A0A	NJ02N892910503264 _00000001.	NULL	17	256060514304	PCI Slot 8 : Bus 43 : Device 0 : Function 0 : Adapter 0
HFS256GD9TNG-L2A0A	NJ02N892910503264 _00000001.	NULL	17	256060514304	PCI Slot 8 : Bus 43 : Device 0 : Function 0 : Adapter 0
HFS256GD9TNG-L2A0A	NJ02N892910503264 _00000001.	NULL	17	256060514304	PCI Slot 8 : Bus 43 : Device 0 : Function 0 : Adapter 0
HFS256GD9TNG-L2A0A	NJ02N892910503264 _00000001.	NULL	17	256060514304	PCI Slot 8 : Bus 43 : Device 0 : Function 0 : Adapter 0
HFS256GD9TNG-L2A0A	NJ02N892910503264 _00000001.	NULL	17	256060514304	PCI Slot 8 : Bus 43 : Device 0 : Function 0 : Adapter 0

[그림 17] 메인보드에 연결한 Internal storage device에 대한 이벤트

Microsoft-Windows-Partition/Diagnostic 채널에서 발생하는 1006 이벤트는 저장장치 정보와 연결/해제 정보를 확인할 수 있다. 따라서, Internal storage device 연결 흔적도 식별할 수 있다. Internal storage device 장치를 연결했을 때 특징은 연결한 포트의 ParentId가 “PCI\~~” 형식의 문자열을 가진다.

Volume Serial Number (이하 VSN)은 1006 이벤트에 기록되는 VBR를 통해서 얻을 수 있다. 모든 저장매체에 대하여 VBRI가 기록되지는 않는다. MBR 방식의 저장매체일 경우 VBRI가 기록되고, GPT일 경우 VBR 기록되지 않는다.

이러한 사실을 바탕으로 필터링 구문을 작성하였으며, 수행한 결과를 통해 확인한 결과를 정리하면 아래 표와 같다. 저장매체 “HFS256GD9TNG-L2A0A”는 GPT 방식이어서 이벤트에 VBRI가 기록되지 않으며, VSN을 확인할 수 없었다.

제조사	모델	Serial Number	Bus Type	Capacity	VSN
NULL	HP SSD EX900 1TB	0100_0000_0000_0000.	17	1000204886016	ECA2-28BE
NULL	HFS256GD9TNG-L2A0A	NJ02N892910503264 _00000001.	17	256060514304	-

[표 9] 메인보드에 연결한 Internal storage device의 정보

**10. List the details of the connected external hard disk. (20 points)**

EventLog.Channel == "Microsoft-Windows-Partition/Diagnostic" and	EventLog.EventID == 1006
--	--------------------------

[그림 18] 필터링 구문: 저장장치 연결/해제 이벤트

해당 필터링 구문을 수행한 후, Serial Number로 그룹핑을 수행하였다. PC에 연결된 저장장치를 정리하면 아래 표와 같다. Serial Number가 같지만, 제조사와 모델이 다른 저장장치는 구분하여 정리하였다.

구분	제조사	모델	Serial Number
USB	ADATA	USB Flash Drive	151261308003001C
USB	Generic	USB Flash Disk	
USB	Generic	Flash Disk	1
USB	JetFlash	Transcend 32GB	2947744399
USB	LGE	USB Drive	EB5HGF24000001744
USB	Mass	Storage Device	121220160204
USB	Samsung	Flash Drive	AA000000000000489
USB	SanDisk	Cruzer	200522428309D780EC0E
USB	SanDisk	Ultra USB 3.0	4C530001021012101141
USB	SanDisk	Ultra USB 3.0	4C530001160326114140
USB	SanDisk	Ultra USB 3.0	4C531001460807102273
USB	SanDisk	Cruzer Blade	4C530001180715107241
USB	SanDisk	Extreme Pro	601E87954321
USB	SMI	USB DISK	F4AHAF60000000579
USB	USB	SanDisk 3.2Gen1	0101185d294a3015f473
USB	USB	SanDisk 3.2Gen1	01013d4f471181af754e
USB	USB	Flash Disk	AA000000000000489
USB	WIBU -	CodeMeter-Stick	000002081976
가상장치	StorLib	Virtual Storage	
가상장치	Arsenal	Virtual	{908e92a3-eee3-11eb-9481-58961d61ea8f}
가상장치	Arsenal	Virtual	{908e9deb-eee3-11eb-9481-58961d61ea8f}
가상장치	Arsenal	Virtual	{908ea3cf-eee3-11eb-9481-58961d61ea8f}
가상장치	Arsenal	Virtual	NULL
가상장치	Msft	Virtual Disk	NULL
내부저장장치	NULL	HP SSD EX900 1TB	0100_0000_0000_0000.
내부저장장치	NULL	HFS256GD9TNG-L2A0A	NJ02N892910503264 _00000001.

도킹스테이션	ThinkWay	Core D162	5000000091707102
외장하드	WD	My Passport 259F	WXR1EB501FFJ

[표 10] PC에 연결된 저장장치 구분 및 목록

제조사와 모델명을 인터넷에 검색하는 방법으로 저장장치를 구분하였다. 이벤트 상 External hard disk라고 볼 수 있는 장치는 2개 (초록색 표기)였다. ThinkWay Core D162 장치는 다음 그림과 같이 도킹스테이션으로 확인되었다.

씽크웨이 CORE D162 IRON 2Bay USB3.0  
 최저 32,000원 판매처 2  
 디지털/가전 > 저장장치 > 외장HDD  
 품목 : 도킹스테이션 | HDD종류 : 6.3cm, 8.8cm | HDD방식 : SATA3 |  
 외장하드단자 : USB3.0(USB3.2 Gen1), USB3.1Gen1 | 색상 : 블랙 | 부가기능 : 동작표시LED,  
 리뷰 ★★★★★ 1,562 등록일 2017.11. 찜하기 97 정보 수정요청

[그림 19] Thinkway Core D162 인터넷 검색

일반적으로 도킹스테이션은 저장장치라고 볼 수 없지만, 다음 그림과 같이 1006 이벤트 상으로 해당 장치는 저장장치와 같은 정보(Capacity, Serial Number, VBR 등)가 포함되어 있었다.

EventData.Manufacturer	EventData.Model	EventData.SerialNumber	EventData.PartitionCount	EventData.Capacity	EventData.DiskId
<b>EventData.SerialNumber (4): 5000000091707102</b>					
ThinkWay	Core D162	5000000091707102	4	2000398934016	a9b1a85c-c040-3304-e9ce-a70e8a95ba88
ThinkWay	Core D162	5000000091707102	4	2000398934016	a9b1a85c-c040-3304-e9ce-a70e8a95ba88
ThinkWay	Core D162	5000000091707102	4	2000398934016	a9b1a85c-c040-3304-e9ce-a70e8a95ba88
ThinkWay	Core D162	5000000091707102	0	2000398934016	a9b1a85c-c040-3304-e9ce-a70e8a95ba88

[그림 20] 1006 이벤트에 기록된 ThinkWay Core D162의 정보

따라서, 도킹스테이션에 연결된 하드디스크가 있다고 추정하였다. 도킹스테이션에 연결된 하드디스크 정보는 확인할 수 없었지만, 1006 이벤트에 기록된 정보를 활용하였다. PC에 연결된 external hard disk의 정보를 정리하면 아래 표와 같다. 저장매체 “WD My Passport 259F”는 GPT 방식이어서 이벤트에 VBR이 기록되지 않으며, VSN을 확인할 수 없었다.

제조사	모델	Serial Number	Bus Type	Capacity	VSN
ThinkWay	Core D162	5000000091707102	7	2000398934016	7381-1FE5
WD	My Passport 259F	WXR1EB501FFJ	7	1000170586112	-

[표 11] 연결된 External hard disk 목록

11. List all connected/disconnected date/time of the “SanDisk CruzerBlade (4C530001180715107241)” device. (50 points)

```
EventLog.Channel == "Microsoft-Windows-Partition/Diagnostic" and
EventLog.EventData["SerialNumber"] == "4C530001180715107241"
```

[그림 21] 필터링 구문: SanDisk Cruzer Blade 장치 연결/해제에 대한 이벤트

Timestamp	EventData.Manufacturer	EventData.Model	EventData.SerialNumber	EventData.PartitionCount	EventData.Capacity
2021-07-23T19:05:35...	SanDisk	Cruzer Blade	4C530001180715107241	4	7761035264
2021-07-23T19:47:18...	SanDisk	Cruzer Blade	4C530001180715107241	0	0
2021-07-26T21:31:18...	SanDisk	Cruzer Blade	4C530001180715107241	4	7761035264
2021-07-26T22:07:14...	SanDisk	Cruzer Blade	4C530001180715107241	4	7761035264
2021-07-26T22:11:42...	SanDisk	Cruzer Blade	4C530001180715107241	0	7761035264

[그림 22] 필터링 구문: SanDisk Cruzer Blade 장치 연결/해제에 대한 이벤트

필터링 구문을 수행하여 얻은 이벤트 목록 중 연결/해제 흐름을 분류하면 아래 표와 같다. 저장장치의 연결과 해제는 PartitionCount 와 Capacity 값을 이용해 구분할 수 있다. PartitionCount 와 Capacity 모두 0 보다 큰 값을 가지면 연결이며, 그 외의 경우는 해제다.

연결 또는 해제 시각	PartitionCount	Capacity	행위 (연결/해제)
2021-07-23 19:05:35.8241134	4	7761035264	연결
2021-07-23 19:47:18.5576276	0	0	해제
2021-07-26 21:31:18.2242178	4	7761035264	연결
2021-07-26 22:07:14.0627136	4	7761035264	연결
2021-07-26 22:11:42.5459051	0	7761035264	해제

[표 12] SanDisk Cruzer Blade 장치 연결/해제 행위 목록

상기 표에서 연결 이벤트가 연속으로 발생한 부분([초록색 표기](#))이 있다. 해제 이벤트 발생 없이 연결 이벤트가 연속으로 발생하는 경우는 다음과 같다.

- (1) 연결된 저장장치 포맷 [CASE1]
- (2) 저장장치가 연결된 상태로 PC 종료 후 부팅 [CASE2]

1006 이벤트에서 VBR 값의 변화 여부로 CASE1 을 판별할 수 있다. 포맷을 했다면, VBR 필드 중에서 다음의 필드가 변할 수 있다. 하지만, 연속으로 발생한 연결 이벤트는 서로 같은 VBR 을 가졌다.

- 파일시스템 종류
- 볼륨의 크기
- Volume Serial Number (VSN)

```

(
    EventLog.ProviderName == "Microsoft-Windows-Kernel-General"           and
    EventLog.EventID in [12, 13]
) or
(
    EventLog.ProviderName == "Microsoft-Windows-Power-Troubleshooter"     and
    EventLog.EventID == 1
) or
(
    EventLog.ProviderName == "Microsoft-Windows-Kernel-Power"             and
    EventLog.EventID in [42, 107]
) or
(
    EventLog.Channel == "System" and
    EventLog.EventID in [1074, 6005]
) or
(
    EventLog.Channel == "Microsoft-Windows-Partition/Diagnostic"
)

```

[그림 23] 필터링 구문: 시스템 부팅/종료 이벤트와 저장장치 연결 이벤트

Timestamp	EventID	EventData.Manufacturer	EventData.Model	EventData.SerialNumber	EventData.Capacity	EventData.PartitionCount	Message
2021-07-26T20:41:10...	1006	WIBU -	CodeMeter-Stick	000002081976	41156608	4	내부에서 사용됩니다.
2021-07-26T21:25:22...	1006	WIBU -	CodeMeter-Stick	000002081976	0	0	내부에서 사용됩니다.
2021-07-26T21:31:18...	1006	SanDisk	Cruzer Blade	4C530001180715107241	7761035264	4	내부에서 사용됩니다.
2021-07-26T21:31:49...	1006	SanDisk	Cruzer	2005224283090780EC0E	4004511744	4	내부에서 사용됩니다.
2021-07-26T21:40:29...	1006	SanDisk	Cruzer	2005224283090780EC0E	4004511744	0	내부에서 사용됩니다.
2021-07-26T21:40:36...	1006	USB	Flash Disk	AA00000000000489	4027580416	4	내부에서 사용됩니다.
2021-07-26T22:06:42...	13						운영 체제가 시스템 시간 2021-07-26T13:06:42.8500235002에 종료
2021-07-26T22:07:03...	12						운영 체제가 시스템 시간 2021-07-26T13:07:03.5000000002에 시작
2021-07-26T22:07:04...	1006	NULL	HFS256GD9TN6-L2A0A	NJ02N892910503264...	256060514304	5	내부에서 사용됩니다.
2021-07-26T22:07:04...	1006	NULL	HP SSD EX900 1TB	0100_0000_0000_0000	1000204886016	4	내부에서 사용됩니다.
2021-07-26T22:07:14...	1006	SanDisk	Cruzer Blade	4C530001180715107241	7761035264	4	내부에서 사용됩니다.
2021-07-26T22:07:14...	1006	USB	Flash Disk	AA00000000000489	4027580416	4	내부에서 사용됩니다.
2021-07-26T22:07:14...	6005						이벤트 로그 서비스가 시작되었습니다.

부팅 후 저장장치 연결

[그림 24] 시스템 부팅/종료 이벤트와 저장장치 연결 이벤트

상기 필터링 구문을 통해서 저장장치가 연결 이벤트가 연속적으로 발생한 이유는 확인하였다. 저장장치가 PC 에 연결된 상태에서, PC 가 종료 후 재부팅되어 연결 이벤트가 다시 발생한 것이다. 실제로, SanDisk Cruzer Blade (4C530001180715107241) 뿐만 아니라, 다른 저장장치들이 비슷한 시점에 동시에 연결되었다.

따라서, 2021-07-26 22:07:14 에 발생한 연결 이벤트는 저장장치가 해제된 후 다시 연결되었다고 보기 어려우며, 해당 저장장치는 2021-07-26 21:31:18 이후 계속 PC 에 연결되었다고 볼 수 있다.

12. What is the external storage device where the program “SystemCollector\_x86.exe” was stored? (50 points)

```
EventLog.Channel == "Microsoft-Windows-Application-Experience/Program-Compatibility-Assistant" and  
EventLog.EventData["ExePath"] contains "SystemCollector_x86.exe"
```

[그림 25] 필터링 구문: SystemCollector\_x86.exe의 호환성 이벤트

TimeCreated	EventData.ExePath	EventData.ResolverName
2021-07-28T15:45:45.4545622	F:\#TOOLS\0204vCollector\SystemCollector_x86.exe	DetectorShim_MessageBoxErrorIcon
2021-07-28T15:45:45.4546689	F:\#TOOLS\0204vCollector\SystemCollector_x86.exe	DetectorShim_ShortRunTime

[그림 26] SystemCollector\_x86.exe 경로

Microsoft-Windows-Application-Experience/Program-Compatibility-Assistant 채널에는 응용 프로그램의 호환성 정보를 확인했을 때 이벤트가 기록된다. 해당 이벤트 채널을 통해서 실행한 응용 프로그램에 대한 경로를 확인할 수 있다. 위와 같은 필터링 구문을 통해서 SystemCollector\_x86.exe의 경로와 실행 시각을 확인했다. 다음 과정으로 해당 실행 파일이 실행된 시점에 마운트된 F 볼륨을 식별하였다.

```
(  
    EventLog.Channel == "Microsoft-Windows-Ntfs/Operational"           and  
    EventLog.EventID in [145, 146]  
) or  
(  
    EventLog.Channel == "Microsoft-Windows-Partition/Diagnostic"        and  
    EventLog.EventID == 1006  
) or  
(  
    EventLog.Channel == "Microsoft-Windows-Application-Experience/Program-Compatibility-Assistant" and  
    EventLog.EventData["ExePath"] contains "SystemCollector_x86.exe"  
)
```

[그림 27] 필터링 구문: 해당 실행 파일이 저장된 볼륨 및 저장장치 이벤트

마운트된 F 볼륨을 식별하고 해당 볼륨이 있는 저장장치의 정보를 확인하기 위해서, 마운트된 볼륨 목록과 저장장치의 연결/해제 이력을 나열하였다. 마운트된 볼륨의 정보 (볼륨 문자, 제조사, 제품명 등)는 Microsoft-Windows-Ntfs/Operational에서 발생하는 145, 146 이벤트를 통해 얻었고, 저장장치의 연결/해제 이력은 Microsoft-Windows-Partition/Diagnostic을 통해 얻었다.

또한, 각 이벤트의 연결은 다음과 같은 정보를 통해 수행하였다. DeviceGUID와 DiskId가 같으면, 동일한 장치로 볼 수 있다.

- Microsoft-Windows-Ntfs/Operational → DeviceGUID (NTFS Filesystem Only)
- Microsoft-Windows-Partition/Diagnostic → DiskId

이러한 정보를 바탕으로 필터링 구문을 작성하고, 외부저장장치 정보를 종합하여 정리하면 아래 표와 같다.  
표는 SystemCollector\_x86.exe가 실행된 시점 전후 (2021-07-28 08시 10분 ~ 18시)로 정리했다.

타임라인	행위	제조사	모델	볼륨 레이블	파일시스템	DiskId (Device GUID)
08:10:06	연결	SanDisk	Ultra USB 3.0	J:	NTFS	68c652bc-96c4-3675-4a38-4e4f8558394d
08:45:35	해제	SanDisk	Ultra USB 3.0	J:	NTFS	68c652bc-96c4-3675-4a38-4e4f8558394d
09:21:17	연결	SanDisk	Extreme Pro	-	exFAT	c366371c-3a3b-f59e-4c22-f3c842f9921b
09:30:06	연결	SanDisk	Ultra USB 3.0	G:	NTFS	adfff837-6086-02dd-553c-a0c5afd6bc01
13:58:28	연결	Arsenal	Virtual	H:	NTFS	7d6650d0-7243-b771-72df-10b142be9682
14:41:42	해제	Arsenal	Virtual	H:	NTFS	7d6650d0-7243-b771-72df-10b142be9682
14:51:16	해제	SanDisk	Ultra USB 3.0	G:	NTFS	adfff837-6086-02dd-553c-a0c5afd6bc01
14:51:16	연결	SanDisk	Ultra USB 3.0	G:	NTFS	adfff837-6086-02dd-553c-a0c5afd6bc01
15:38:45	해제	SanDisk	Ultra USB 3.0	G:	NTFS	adfff837-6086-02dd-553c-a0c5afd6bc01
15:38:50	연결	Samsung	Flash Drive	I:	NTFS	e3bd9a-d368-e874-81cb-ec5639ec18e6
15:45:45	실행	F:\#TOOLS\0204vCollector\SystemCollector_x86.exe				
16:45:31	해제	Samsung	Flash Drive	I:	NTFS	e3bd9a-d368-e874-81cb-ec5639ec18e6
16:45:47	연결	Arsenal	Virtual	G:	NTFS	27208f73-a29a-fdc4-c54c-09c944729e62
17:23:11	해제	Arsenal	Virtual	G:	NTFS	27208f73-a29a-fdc4-c54c-09c944729e62
17:23:14	해제	SanDisk	Extreme Pro	-	exFAT	c366371c-3a3b-f59e-4c22-f3c842f9921b
17:23:28	연결	USB	SanDisk 3.2Gen1	F:	NTFS	6bb52482-db8a-0017-64ed-614e3216ff8
17:23:31	연결	Samsung	Flash Drive	I:	NTFS	e3bd9a-d368-e874-81cb-ec5639ec18e6

17:40:11	해제	Samsung	Flash Drive	I:	NTFS	e3bd9a-d368-e874-81cb-ec5639ec18e6
17:40:12	해제	USB	SanDisk 3.2Gen1	F:	NTFS	6bb52482-db8a-0017-64ed-614e32161ff8

[표 13] 저장장치 연결/해제 흔적 및 볼륨 정보

SystemCollector\_x86.exe이 저장된 저장장치로 의심되는 행을 **붉은색**으로 표현하였다. 볼륨의 정보는 NTFS 파일시스템이 아니면, 기록되지 않으므로 SanDisk Extreme Pro가 할당 받은 볼륨을 Event Log 상으로는 확인하기 어렵다. 그러나, 상기 표에 기술된 저장장치의 연결/해제 순서를 따라 추론하면, 합리적으로 SanDisk Extreme Pro의 볼륨은 F 문자를 할당 받은 것을 알 수 있다. 그 근거는 다음과 같다.

(1) SystemCollector\_x86.exe가 실행된 시점에 F 문자를 할당 받은 볼륨은 이벤트 상에서 발견할 수 없다. F 문자를 할당 받은 볼륨은 08시 10분 이전에도 있었지만, 아래 그림과 같이 2021-07-28 02시 즈음에 연결되고 해제되었으므로, 08시 10분부터 17시 23분 28초 (SanDisk 3.2Gen1 연결 시각) 사이에 F 문자는 이벤트 상에서 할당되지 않았다.

TimeCreated	EventID	Event	EventData	EventData.ProductId	EventData	EventData.Model	EventData.Partition	EventData.Capaci	EventData.DiskId	EventData.DeviceGuic
2021-07-28T02:34:50...	1006				USB	SanDisk 3.2Gen1	4	61530439680	6bb52482-db8a...	
2021-07-28T02:35:03...	1006				USB	SanDisk 3.2Gen1	4	61530439680	6bb52482-db8a...	
2021-07-28T02:35:03...	145	F:	USB	SanDisk 3.2Gen1	USB	SanDisk 3.2Gen1	0	61530439680	6bb52482-db8a...	6bb52482-db8a-00...
2021-07-28T03:05:51...	1006									

[그림 28] SystemCollector\_x86.exe 실행 시점 이전 연결된 F 볼륨

(2) Windows의 볼륨 문자 할당 순서는 순차적이다. 상기 표에서 09시 21분에 연결한 SanDisk Extreme Pro와 09시 30분에 연결한 Ultra USB 3.0 (G 문자 할당 받음)은 볼륨 할당 순서에 따라 각각 F와 G를 할당 받은 것을 추론할 수 있다.

(1)과 (2)를 종합하면, SanDisk Extreme Pro 가 연결되기 전까지 볼륨 문자 F는 할당되지 않았고, 해당 저장장치가 연결되었을 때 해당 저장장치의 볼륨에 F 문자를 할당하였다. 따라서, SystemCollector\_x86.exe 가 저장된 저장장치는 아래 표와 같다.

제조사	모델	Serial Number
SanDisk	Extreme Pro	01013d4f471181af754e

[표 14] SystemCollector\_x86.exe가 저장된 외부 저장장치 정보