

## 203 – Find suspicious USB & documents

### Team Information

Team Name : DogeCoin

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

Email Address : [dfc-dogecoin@naver.com](mailto:dfc-dogecoin@naver.com)

### Instructions

**Description** During the search and seizure, the police found traces of suspicious document file (Trade\_list.xlsx) that appeared to be related to the crime. Forensic analysis revealed that the file was on some external storage device. The police asked the suspect if he had an external storage device where the document file was stored, but he said he did not answer. Find out exactly what external storage device the suspicious file is stored on, and find out if there are any additional related files.

Target	Hash (MD5)
system.ad1	7cf1e6a422f8a5b004be3b4afdac450a

### Questions

# Please solve all problems based on UTC+9 time zone.

1. What is the manufacturer, model, and serial number of USB that was most connected to the system? (40 points)
2. What is the manufacturer, model, and serial number of USB where the suspicious file (Trade\_list.xlsx) is stored? (40 points)
3. What is the file system of the USB where the suspicious file (Trade\_list.xlsx) is stored? (40 points)
4. List all connection and disconnection times for USB where the suspicious file (Trade\_list.xlsx) is stored. (UTC+9) (40 points)

5. Among the files on the desktop, identify the files that have been opened while the USB, which has the suspicious file (Trade\_list.xlsx), is connected. And then find the most opened file among them. (40 points)

Teams must:

- Describe step-by-step processes for generating your solution.
- Specify any tools used for this problem.

**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>		

Name:	JumpListsView	Publisher:	NirSoft
Version:	1.16		
URL:	<a href="https://www.nirsoft.net/utils/jump_lists_view.html">https://www.nirsoft.net/utils/jump_lists_view.html</a>		

Name:	RecentFilesView	Publisher:	NirSoft
Version:	1.33		
URL:	<a href="https://www.nirsoft.net/utils/recent_files_view.html">https://www.nirsoft.net/utils/recent_files_view.html</a>		

Name:	WindowsTimeline Parser	Publisher:	Kacos2000
Version:	2.0.81.0		
URL:	<a href="https://github.com/kacos2000/WindowsTimeline">https://github.com/kacos2000/WindowsTimeline</a>		

Name:	BrowsingHistoryView	Publisher:	NirSoft
Version:	2.48		
URL:	<a href="https://www.nirsoft.net/utils/browsing_history_view.html">https://www.nirsoft.net/utils/browsing_history_view.html</a>		

Name:	Registry Explorer	Publisher:	Eric Zimmerman
Version:	1.6.0.0		
URL:	<a href="https://ericzimmerman.github.io/#!index.md">https://ericzimmerman.github.io/#!index.md</a>		

Name:	Shellbags Explorer	Publisher:	Eric Zimmerman
Version:	1.4.0.0		
URL:	<a href="https://ericzimmerman.github.io/#!index.md">https://ericzimmerman.github.io/#!index.md</a>		

Name:	HxD	Publisher:	Maël Hörz
Version:	2.5.0.0		
URL:	<a href="https://mh-nexus.de/en/hxd/">https://mh-nexus.de/en/hxd/</a>		

**Step-by-step methodology:**

1. 가장 많이 연결된 USB의 제조사, 모델, 시리얼 넘버

What is the manufacturer, model, and serial number of USB that was most connected to the system? (40 points)

[그림 1] Q1 지문

Windows 10 기준 Eventlog의 Microsoft-Windows-Partition/Diagnostic 채널에서 1006번 이벤트를 통해 저장장치 연결/해제 흔적을 확인할 수 있다. 해당 이벤트는 연결된 내부저장장치와 외부저장장치 모두 기록하므로, 이벤트 내부에 기록된 값을 활용하여 USB 연결/해제를 구분해야 한다. USB의 연결/해제를 구분할 수 있는 값은 다음과 같다.

- EventData에 기록된 BusType이 7 → USB 나타냄
- EventData의 PartitionCount로 연결/해제를 구분할 수 있음
  - PartitionCount이 0보다 큼 (보통 4) → 연결
  - PartitionCount가 0 → 해제
- **EventData의 PartitionTable에 특정 값이 기록되면 필터링** [\[참조\]](#)

PartitionCount는 연결한 USB에 있는 실제 파티션 수와 상관없이 (1개, 2개, ... 4개 이상) 보통 4로 기록된다. 따라서, 올바르게 USB가 연결되었다면 PartitionCount는 4이다. 또한, 해제할 때는 PartitionCount가 0으로 항상 초기화된다.'

[illegible]

지금까지 알아 낸 내용을 Message Analyzer의 필터 구문으로 바꾸면 [그림 2]와 같다. 그리고, SerialNumber로 그룹핑을 수행하면 연결한 USB의 이력을 [그림 3]과 같이 알 수 있다.

[illegible]

**[그림 2] 연결된 USB 필터링**

Timestamp	EventData.SerialNumber	EventData.Manufacturer	EventData.Model	EventData.Revision	EventData.SerialNumber	EventData.PartitionCount	EventData.BusType
+	EventData.SerialNumber (6): 0101f5aac6f3ff5d4e						
	2021-05-13T13:39:10.8936149	SanDisk	Ultra	1.00	0101f5aac6f3ff5d4e	4	7
	2021-05-14T10:16:23.4628002	SanDisk	Ultra	1.00	0101f5aac6f3ff5d4e	4	7
	2021-05-17T09:52:15.4938181	SanDisk	Ultra	1.00	0101f5aac6f3ff5d4e	4	7
	2021-05-18T11:00:27.9234276	SanDisk	Ultra	1.00	0101f5aac6f3ff5d4e	4	7
	2021-05-19T13:29:05.0973446	SanDisk	Ultra	1.00	0101f5aac6f3ff5d4e	4	7
	2021-05-20T10:51:46.5149529	SanDisk	Ultra	1.00	0101f5aac6f3ff5d4e	4	7
+	EventData.SerialNumber (1): 0123456789ABCDEF						
	2021-05-19T13:32:43.6189528	SanDisk	Firebird	1.07	0123456789ABCDEF	1	7
+	EventData.SerialNumber (5): 1508220917130472481211						
	2021-05-13T13:36:50.3371022	General	UDisk	5.00	1508220917130472481211	4	7
	2021-05-14T10:05:36.9120972	General	UDisk	5.00	1508220917130472481211	4	7
	2021-05-18T10:37:54.9268048	General	UDisk	5.00	1508220917130472481211	4	7
	2021-05-19T13:20:24.6631232	General	UDisk	5.00	1508220917130472481211	4	7
	2021-05-20T10:41:56.4105223	General	UDisk	5.00	1508220917130472481211	4	7
+	EventData.SerialNumber (7): 200517380309E4003426						
	2021-05-13T13:40:06.5481339	Cruzer	Cruzer	1.26	200517380309E4003426	4	7
	2021-05-14T10:20:11.7762041	SanDisk	Cruzer	1.26	200517380309E4003426	4	7
	2021-05-17T10:00:21.1947153	SanDisk	Cruzer	1.26	200517380309E4003426	4	7
	2021-05-18T11:06:09.7003629	SanDisk	Cruzer	1.26	200517380309E4003426	4	7
	2021-05-19T13:33:22.8583433	SanDisk	Cruzer	1.26	200517380309E4003426	4	7
	2021-05-20T10:56:28.1547780	SanDisk	Cruzer	1.26	200517380309E4003426	4	7
+	2021-05-21T15:58:01.3503732	SanDisk	Cruzer	1.26	200517380309E4003426	4	7
+	EventData.SerialNumber (5): 4C530001091028102015						
	2021-05-13T13:38:12.5400761	SanDisk	Ultra USB 3.0	1.00	4C530001091028102015	4	7
	2021-05-14T10:25:03.7855070	SanDisk	Ultra USB 3.0	1.00	4C530001091028102015	4	7
	2021-05-17T09:37:38.4646636	SanDisk	Ultra USB 3.0	1.00	4C530001091028102015	4	7
	2021-05-18T10:53:40.8007282	SanDisk	Ultra USB 3.0	1.00	4C530001091028102015	4	7
	2021-05-20T10:46:05.1774205	SanDisk	Ultra USB 3.0	1.00	4C530001091028102015	4	7
+	EventData.SerialNumber (2): AA000000000000485						
	2021-05-13T13:39:41.2705380	USB	Flash Disk	1100	AA000000000000485	4	7
	2021-05-17T09:56:20.5680338	USB	Flash Disk	1100	AA000000000000485	4	7
+	EventData.SerialNumber (6): AA000000000000489						
	2021-05-13T13:35:41.4898487	Generic	Mass Storage	1100	AA000000000000489	1	7
	2021-05-13T13:36:20.1390827	Generic	Mass Storage	1100	AA000000000000489	1	7
	2021-05-13T13:37:37.0408001	Generic	Mass Storage	1100	AA000000000000489	2	7
	2021-05-14T10:12:07.1521667	Generic	Mass Storage	1100	AA000000000000489	2	7
	2021-05-17T09:42:45.7467243	Generic	Mass Storage	1100	AA000000000000489	2	7
	2021-05-18T10:44:15.9687037	Generic	Mass Storage	1100	AA000000000000489	2	7
+	EventData.SerialNumber (3): D						
	2021-05-13T13:38:41.7097515	Verbatim	STORE N GO	8.07	D	4	7
	2021-05-17T09:47:48.6568130	Verbatim	STORE N GO	8.07	D	4	7
	2021-05-19T13:24:46.5668335	Verbatim	STORE N GO	8.07	D	4	7

**[그림 3] 필터 구문 수행 결과**

따라서, 답은 [표 1]과 같다.

<b>Manufacturer</b>	SanDisk
<b>Model</b>	Cruzer
<b>Serial Number</b>	200517380309E4003426

**[표 1] Q1 답**

## 2. Trade\_list.xlsx이 저장된 USB의 제조사, 모델, 시리얼 넘버

What is the manufacturer, model, and serial number of USB where the suspicious file (trade.xlsx) is stored? (40 points)

### [그림 4] Q2 지문

의심 파일(Trade\_list.xlsx)가 저장된 USB를 식별하려면, 다음과 같은 정보가 필요하다. 각 정보들은 언급한 아티팩트에서 확인하여 종합 분석하면, 의심 파일이 저장되었던 USB를 알 수 있다.

- 각 USB의 연결된 시간 (연결과 해제까지 사이 시간)
  - [Eventlog] Microsoft-Windows-Partition/Diagnostic (1006)
- 할당 받은 드라이브 문자열
  - [Eventlog] Microsoft-Windows-Ntfs/Operational (145): 단, NTFS 파일시스템만 기록됨
    - ◆ 시리얼 번호와 볼륨 GUID를 추가적으로 획득 가능
  - [Registry] VolumeInfoCache
    - ◆ 할당된 드라이브 문자 목록
  - [Registry] Windows Portable Devices
    - ◆ 외부저장장치에 할당된 드라이브 문자 및 외부저장장치 정보
- 특정 USB에 Trade\_list.xlsx가 존재하였다고 아티팩트에 기록된 시간
  - JumpList & Recent (Record Time)
  - Timeline (Open File, In Use & Focus → Start Time)
  - Browser History
  - [Eventlog] OAlerts (300)

각 아티팩트에서 얻은 결과를 표로 정리하면 [표 2]와 같으며 시간 표기 시 소수점을 생략하였다. 다음과 같은 아티팩트로부터 정보를 획득하였다.

- JumpList: Entry가 기록된 시각 (Record Time)

- EventLog: 이벤트 발생 시각
- Timeline: Open File, Focus 행위가 발생한 시각 (Start Time)
- Browser History: 해당 경로의 파일을 열람한 시각 (Visit Time)

시간	이벤트	자세히	출처
2021-05-13 13:35:41	USB 연결	Generic, Mass Storage, AA00000000000489	Eventlog
2021-05-13 13:36:04	USB 해제	Generic, Mass Storage, AA00000000000489	Eventlog
2021-05-13 13:36:20	USB 연결	Generic, Mass Storage, AA00000000000489	Eventlog
2021-05-13 13:36:20	드라이브 할당	E, AA00000000000489	Eventlog
2021-05-13 13:36:39	USB 해제	Generic, Mass Storage, AA00000000000489	Eventlog
2021-05-13 13:36:50	USB 연결	General, UDisk, 1508220917130472481211	Eventlog
2021-05-13 13:36:50	드라이브 할당	E, 1508220917130472481211	Eventlog
2021-05-13 13:37:15	USB 해제	General, UDisk, 1508220917130472481211	Eventlog
2021-05-13 13:37:37	USB 연결	Generic, Mass Storage, AA00000000000489	Eventlog
2021-05-13 13:37:37	드라이브 할당	E, AA00000000000489	Eventlog
2021-05-13 13:37:57	USB 해제	Generic, Mass Storage, AA00000000000489	Eventlog
2021-05-13 13:38:12	USB 연결	SanDisk, Ultra USB 3.0, 4C530001091028102015	Eventlog
2021-05-13 13:38:27	USB 해제	SanDisk, Ultra USB 3.0, 4C530001091028102015	Eventlog
2021-05-13 13:38:41	USB 연결	Verbatim, STORE N GO, D	Eventlog
2021-05-13 13:38:42	드라이브 할당	E, D	Eventlog
2021-05-13 13:39:00	USB 해제	Verbatim, STORE N GO, D	Eventlog
2021-05-13 13:39:10	USB 연결	SanDisk, Ultra, 0101f5aa8cf63ff5d44e	Eventlog
2021-05-13 13:39:11	드라이브 할당	E, 0101f5aa8cf63ff5d44e	Eventlog
2021-05-13 13:39:30	USB 해제	SanDisk, Ultra, 0101f5aa8cf63ff5d44e	Eventlog
2021-05-13 13:39:41	USB 연결	USB, Flash Disk, AA00000000000485	Eventlog
2021-05-13 13:39:55	USB 해제	USB, Flash Disk, AA00000000000485	Eventlog
2021-05-13 13:40:06	USB 연결	SanDisk, Cruzer, 200517380309E4003426	Eventlog
2021-05-13 13:40:52	USB 해제	SanDisk, Cruzer, 200517380309E4003426	Eventlog
2021-05-14 10:05:36	USB 연결	General, UDisk, 1508220917130472481211	Eventlog
2021-05-14 10:05:37	드라이브 할당	E, 1508220917130472481211	Eventlog
2021-05-14 10:11:53	USB 해제	General, UDisk, 1508220917130472481211	Eventlog
2021-05-14 10:12:07	USB 연결	Generic, Mass Storage, AA00000000000489	Eventlog
2021-05-14 10:12:09	드라이브 할당	E, AA00000000000489	Eventlog
2021-05-14 10:15:48	USB 해제	Generic, Mass Storage, AA00000000000489	Eventlog
2021-05-14 10:16:23	USB 연결	SanDisk, Ultra, 0101f5aa8cf63ff5d44e	Eventlog
2021-05-14 10:16:23	드라이브 할당	E, 0101f5aa8cf63ff5d44e	Eventlog
2021-05-14 10:19:45	USB 해제	SanDisk, Ultra, 0101f5aa8cf63ff5d44e	Eventlog

2021-05-14 10:20:11	USB 연결	SanDisk, Cruzer, 200517380309E4003426	Eventlog
2021-05-14 10:23:38	USB 해제	SanDisk, Cruzer, 200517380309E4003426	Eventlog
2021-05-14 10:25:03	USB 연결	SanDisk, Ultra USB 3.0, 4C530001091028102015	Eventlog
2021-05-14 10:25:18	문서 열람 (Open File & Use)	E:\Job\Trade_list.xlsx	Timeline
2021-05-14 10:25:18	문서 열람 (In Focus)	{74033EF5-B3A4-11EB-B6A2-000C295E35EB}\Job\Trade_list.xlsx	Timeline
2021-05-14 10:28:01	USB 해제	SanDisk, Ultra USB 3.0, 4C530001091028102015	Eventlog
2021-05-17 09:37:38	USB 연결	SanDisk, Ultra USB 3.0, 4C530001091028102015	Eventlog
2021-05-17 09:37:51	문서 열람 (In Focus)	{74033EF5-B3A4-11EB-B6A2-000C295E35EB}\Job\Trade_list.xlsx	Timeline
2021-05-17 09:41:34	문서 열람	Trade_list.xlsx	Eventlog
2021-05-17 09:41:48	USB 해제	SanDisk, Ultra USB 3.0, 4C530001091028102015	Eventlog
2021-05-17 09:42:45	USB 연결	Generic, Mass Storage, AA000000000000489	Eventlog
2021-05-17 09:42:45	드라이브 할당	E, AA000000000000489	Eventlog
2021-05-17 09:47:25	USB 해제	Generic, Mass Storage, AA000000000000489	Eventlog
2021-05-17 09:47:48	USB 연결	Verbatim, STORE N GO, D	Eventlog
2021-05-17 09:47:49	드라이브 할당	E, D	Eventlog
2021-05-17 09:51:46	USB 해제	Verbatim, STORE N GO, D	Eventlog
2021-05-17 09:52:15	USB 연결	SanDisk, Ultra, 0101f5aa8cf63ff5d44e	Eventlog
2021-05-17 09:52:15	드라이브 할당	E, 0101f5aa8cf63ff5d44e	Eventlog
2021-05-17 09:55:51	USB 해제	SanDisk, Ultra, 0101f5aa8cf63ff5d44e	Eventlog
2021-05-17 09:56:20	USB 연결	USB, Flash Disk, AA000000000000485	Eventlog
2021-05-17 10:00:02	USB 해제	USB, Flash Disk, AA000000000000485	Eventlog
2021-05-17 10:00:21	USB 연결	SanDisk, Cruzer, 200517380309E4003426	Eventlog
2021-05-17 10:04:21	USB 해제	SanDisk, Cruzer, 200517380309E4003426	Eventlog
2021-05-18 10:37:54	USB 연결	General, UDisk, 1508220917130472481211	Eventlog
2021-05-18 10:37:55	드라이브 할당	E, 1508220917130472481211	Eventlog
2021-05-18 10:43:15	USB 해제	General, UDisk, 1508220917130472481211	Eventlog
2021-05-18 10:44:15	USB 연결	Generic, Mass Storage, AA000000000000489	Eventlog
2021-05-18 10:44:16	드라이브 할당	E, AA000000000000489	Eventlog
2021-05-18 10:49:27	USB 해제	Generic, Mass Storage, AA000000000000489	Eventlog
2021-05-18 10:53:40	USB 연결	SanDisk, Ultra USB 3.0, 4C530001091028102015	Eventlog
2021-05-18 10:53:51	문서 열람	E:\Job\Trade_list.xlsx	JumpList & Recent
2021-05-18 10:53:51	문서 열람	E:\Job\Trade_list.xlsx	Browser History
2021-05-18 10:53:52	문서 열람 (In Focus)	{74033EF5-B3A4-11EB-B6A2-000C295E35EB}\Job\Trade_list.xlsx	Timeline



2021-05-18 10:59:48	USB 해제	SanDisk, Ultra USB 3.0, 4C530001091028102015	Eventlog
2021-05-18 11:00:27	USB 연결	SanDisk, Ultra, 0101f5aa8cf63ff5d44e	Eventlog
2021-05-18 11:00:28	드라이브 할당	E, 0101f5aa8cf63ff5d44e	Eventlog
2021-05-18 11:05:08	USB 해제	SanDisk, Ultra, 0101f5aa8cf63ff5d44e	Eventlog
2021-05-18 11:06:09	USB 연결	SanDisk, Cruzer, 200517380309E4003426	Eventlog
2021-05-18 11:10:31	USB 해제	SanDisk, Cruzer, 200517380309E4003426	Eventlog
2021-05-19 13:20:24	USB 연결	General, UDisk, 1508220917130472481211	Eventlog
2021-05-19 13:20:24	드라이브 할당	E, 1508220917130472481211	Eventlog
2021-05-19 13:24:02	USB 해제	General, UDisk, 1508220917130472481211	Eventlog
2021-05-19 13:24:46	USB 연결	Verbatim, STORE N GO, D	Eventlog
2021-05-19 13:24:47	드라이브 할당	E, D	Eventlog
2021-05-19 13:28:35	USB 해제	Verbatim, STORE N GO, D	Eventlog
2021-05-19 13:29:05	USB 연결	SanDisk, Ultra, 0101f5aa8cf63ff5d44e	Eventlog
2021-05-19 13:29:05	드라이브 할당	E, 0101f5aa8cf63ff5d44e	Eventlog
2021-05-19 13:32:07	USB 해제	SanDisk, Ultra, 0101f5aa8cf63ff5d44e	Eventlog
2021-05-19 13:32:43	USB 연결	SanDisk, Firebird, 0123456789ABCDEF	Eventlog
2021-05-19 13:32:58	USB 해제	SanDisk, Firebird, 0123456789ABCDEF	Eventlog
2021-05-19 13:33:22	USB 연결	SanDisk, Cruzer, 200517380309E4003426	Eventlog
2021-05-19 13:36:47	USB 해제	SanDisk, Cruzer, 200517380309E4003426	Eventlog
2021-05-20 10:41:56	USB 연결	General, UDisk, 1508220917130472481211	Eventlog
2021-05-20 10:41:56	드라이브 할당	E, 1508220917130472481211	Eventlog
2021-05-20 10:45:38	USB 해제	General, UDisk, 1508220917130472481211	Eventlog
2021-05-20 10:46:05	USB 연결	SanDisk, Ultra USB 3.0, 4C530001091028102015	Eventlog
2021-05-20 10:50:05	USB 해제	SanDisk, Ultra USB 3.0, 4C530001091028102015	Eventlog
2021-05-20 10:51:46	USB 연결	SanDisk, Ultra, 0101f5aa8cf63ff5d44e	Eventlog
2021-05-20 10:51:46	드라이브 할당	E, 0101f5aa8cf63ff5d44e	Eventlog
2021-05-20 10:55:26	USB 해제	SanDisk, Ultra, 0101f5aa8cf63ff5d44e	Eventlog
2021-05-20 10:56:28	USB 연결	SanDisk, Cruzer, 200517380309E4003426	Eventlog
2021-05-20 10:59:30	USB 해제	SanDisk, Cruzer, 200517380309E4003426	Eventlog
2021-05-21 15:58:01	USB 연결	SanDisk, Cruzer, 200517380309E4003426	Eventlog
2021-05-21 16:24:30	USB 해제	SanDisk, Cruzer, 200517380309E4003426	Eventlog

[표 2] 의심 파일 및 USB 연결/해제 목록

[표 2]를 통해서 모든 외부저장장치 연결과 해제 시각이 서로 다른 외부저장장치끼리 (1) 중복되는 시간 없이 PC에 연결된 것을 알 수 있다. 또한, 의심 파일이 열람되었을 때와 해당 시점 주위에 연결되었던 USB를 **녹색**과 **주황색**으로 표현하였다. 이를 통해서 (2) SanDisk Ultra USB 3.0이 연결되어 있을 때 (USB 연결, 해제 사이), E 드라이브에 존재하였던 의심 파일이 열람된 것을 확인할 수 있다.

하지만, SanDisk Ultra USB 3.0이 연결될 때, 드라이브 할당 이벤트가 기록되지 않았으므로, 이에 따라서 드라이브 문자를 "E"로 할당받았는지 해당 이벤트로는 알 수 없다. 또한, SanDisk Ultra USB 3.0의 볼륨에 NTFS 파일시스템이 아닌 다른 파일시스템이 설치되었다는 것을 알 수 있다. 할당받은 드라이브 문자를 확인하기 위해 Registry의 VolumeInfoCache와 Windows Portable Devices를 살펴보았다.

VolumeInfoCache를 통해서 컴퓨터에 할당된 드라이브 문자 목록을 확인하였다. [그림 5]와 같이 할당된 드라이브 문자는 C와 E밖에 없었으며, C 드라이브는 시스템이 설치되는 볼륨이므로 (3-1) USB가 연결될 때마다 E 드라이브로 문자가 할당되었다고 추정할 수 있다.

VolumeInfoCache	0	2	2021-05-13 04:35:41
C:	2	0	2020-11-19 07:45:13
E:	2	0	2021-05-17 01:00:21

[그림 5] 할당된 드라이브 문자 확인 (VolumeInfoCache)

Windows Portable Devices를 통해서 외부저장장치가 연결되었을 때 할당받은 드라이브 문자 열 또는 볼륨 레이블을 [그림 6]과 같이 확인하였다. SanDisk Ultra USB 3.0은 2021-05-13 13:38:12에 드라이브 문자 "E"를 할당받았다. 해당 시각은 [표 2]에서 SanDisk Ultra USB 3.0이 최초로 연결된 시각이다. 따라서, (3-2) SanDisk Ultra USB 3.0은 13:38:12 이후로 PC에 연결되면서 항상 드라이브 문자 "E"를 할당받았다.

Timestamp	Device	Serial Number	Friendly Name
2021-05-13 04:37:37			E:W
2021-05-13 04:36:51	DISK&VEN_GENERIC&PROD_UDISK&REV_5.00	1508220917130472481211&0	E:W
2021-05-13 04:36:20	DISK&VEN_GENERIC&PROD_MASS_STORAGE&REV_1100	050619-1070000000112&0	BACKUP-USB2
2021-05-13 04:35:41	DISK&VEN_GENERIC&PROD_MASS_STORAGE&REV_1100	052819-57120&0	BACKUP-USB
2021-05-13 04:40:06	DISK&VEN_SANDISK&PROD_CRUZER&REV_1.26	200517380309E4003426&0	E:W
2021-05-19 04:32:44	DISK&VEN_SANDISK&PROD_FIREBIRD&REV_1.07	0123456789ABCDEF&0	E:W
2021-05-13 04:39:11	DISK&VEN_SANDISK&PROD_ULTRA&REV_1.00	0101F5AA8CF63FF5D44E5DDCDF1B23D15C3D098E29C2376D992E91BC41FEEA7	E:W
2021-05-13 04:38:12	DISK&VEN_SANDISK&PROD_ULTRA_USB_3.0&REV_1.00	4C530001091028102015&0	E:W
2021-05-13 04:39:41	DISK&VEN_USB&PROD_FLASH_DISK&REV_1100	FBH1206120324252&0	USB
2021-05-13 04:38:42	DISK&VEN_VERBATIM&PROD_STORE_N_GO&REV_8.07	DE0A988D&0	E:W

[그림 6] 할당된 드라이브 문자 및 외부저장장치 정보 확인 (Windows Portable Devices)

정리하면, (1), (2), (3-1), (3-2)를 근거로 SanDisk Ultra USB 3.0이 연결되었을 때 항상 E 드라이브로 할당되었고, 해당 USB에 의심 파일이 저장되었다. 따라서 답은 [표 3]과 같다.

<b>Manufacturer</b>	SanDisk
<b>Model</b>	Ultra USB 3.0
<b>Serial Number</b>	4C530001091028102015

[표 3] Q2 답

[추가] *Timeline 아티팩트와 Eventlog의 OAlerts로부터 얻은 Trade\_list.xlsx에 대한 설명*

### #1 Timeline

Timeline에서 문서 열람 행위로 볼 수 있는 기록은 Open File와 In Use/Focus일 때다. [표 2]에서 Timeline의 문서 열람 행위는 경로가 볼륨 GUID로 표현된 것과 E 드라이브로 표현된 것 2가지가 있으며, 다음과 같다.

- E 드라이브로 표현: Open File행위
  - E:\Job\Trade\_list.xlsx
- 볼륨 GUID 표현: In Use & Focus 행위
  - {74033EF5-B3A4-11EB-B6A2-000C295E35EB}\Job\Trade\_list.xlsx

연결된 USB에 해당하는 볼륨 GUID는 Registry의 MountedDevices에서 얻을 수 있으며, SanDisk Ultra USB 3.0에 할당된 볼륨 GUID가 {74033EF5-B3A4-11EB-B6A2-000C295E35EB}인 것을 확인하였다. 해당 볼륨 GUID는 Timeline에 기록된 GUID와 같으므로, SanDisk Ultra USB 3.0이 할당 받은 E 드라이브와 같다. 따라서, In Use/Focus 행위에서 기록된 파일의 경로와 Open File 행위에서 기록된 파일의 경로는 같다.

### #2 Eventlog – OAlerts

해당 이벤트는 Office 문서로 작업을 하는 중에 사용자 행위 또는 PC 상황에 따라서 알람창이 발생했을 때 기록된다. 알람창이 열리는 몇몇 경우는 다음과 같다.

- 변경 내용 발생 후 바로 닫기 버튼을 눌렀을 때 발생하는 저장 여부 선택 창 (CASE 1)
- 잘못된 형식의 파일을 열었을 때 발생하는 확인 창 (CASE 2)
- 등등 (CASE 3~...)

이번 시나리오에 주어진 의심 파일은 [그림 6]을 통해, CASE 1 (저장 여부 선택 창)이 발생하면

서 기록되었다. 해당 이벤트의 발생 시각은 2021-05-17 09:41:34이다. [그림 6]에서 JumpList에 기록된 수정 시각은 2021-05-17 09:41:36이다. (1) 두 아티팩트의 시간 차이는 약 2초이며, OAlerts 이벤트는 E:\JobWTrade\_list.xlsx 파일을 수정한 행위와 관련있다. 또한, JumpList & Recent, Timeline, Browser History에서 (2) Trade\_list.xlsx에 대한 흔적은 "E:\JobWTrade\_list.xlsx"로 유일하며, 이름이 같으면서 경로가 다른 파일을 발견할 수 없었다. 따라서, (1)과 (2)를 근거로 OAlerts 이벤트에 기록된 Trade\_list.xlsx는 "E:\JobWTrade\_list.xlsx"를 나타낸다.

EventID	Timestamp	EventData.1
300	2021-05-12T06:29:36.2881734	Normal의 변경 내용을 저장하시겠습니까?
300	2021-05-14T10:20:39.8109906	'WEO_Data.xls'의 파일 형식 및 확장명이 일치하지 않습니다. 파일이 손상되었거나 안전하지 않을 수 있습니다. 데이터
300	2021-05-17T09:41:34.8839248	'Trade_list.xlsx'의 변경 내용을 저장하시겠습니까?

JumpListsView				
File Edit View Options Help				
Quick Filter				
trade_list				
Find one string Search all columns Show only items match the				
Full Path	Record Time	Created Time	Modified Time	Accessed Time
E:\JobWTrade_list.xlsx	2021-05-18 오전 10:53:51	2021-05-11 오후 5:35:37	2021-05-17 오전 9:41:36	2021-05-17 오전 9:41:36
E:\JobWTrade_list.xlsx	2021-05-18 오전 10:53:51	2021-05-11 오후 5:35:37	2021-05-17 오전 9:41:36	2021-05-17 오전 9:41:36

[그림 7] OAlerts 이벤트와 JumpList에 기록된 의심 파일

### 3. Trade.xlsx이 저장된 USB의 파일시스템

What is the file system of the USB where the suspicious file (Trade\_list.xlsx) is stored?  
(40 points)

#### [그림 8] Q3 지문

외부저장장치의 파티션에 설치된 파일시스템을 파악하려면, 다음과 같은 아티팩트에서 확인할 수 있다.

- [Registry] Shellbags (File entry shell item)
- [Eventlog] Microsoft-Windows-Partition/Diagnostic (1006)
  - 기록된 VBR을 통해서 파일시스템 정보를 파악할 수 있음
- [Eventlog] Microsoft-Windows-Ntfs/Operational: 인식된 파티션이 NTFS 일 경우 기록됨
  - 본 문제의 USB는 NTFS가 아니므로, 해당되지 않음 [\[참조\]](#)

#### 3.1. [Registry] Shellbags

Shellbags에 기록된 폴더는 Job 폴더 한 개밖에 없었으며, Job 폴더의 정보를 기록한 File entry shell item을 통해서 [그림 9]와 같이 파일시스템(exFAT)을 확인하였다.

Value	Icon	Shell Type	MRU Position	Created On	Modified On	Accessed On	First Interacted	Last Interacted	Has Explored	Miscellaneous
Job	No L...	Directory	0	2021-05-12 15:20:00	2021-05-12 15:18:34	2021-05-12 15:19:58	2021-05-13 13:35:48	2021-05-13 13:35:48	<input checked="" type="checkbox"/>	exFAT file system

Summary	Details	Hex
<b>Name: Job</b> Absolute path: Desktop\My Computer\E\Job Key-Value name path: BagMRU\1\1-0 Registry last write time: 2021-05-13 13:35:48.020  <b>Target timestamps</b> Created on: 2021-05-12 15:20:00.000 Modified on: 2021-05-12 15:18:34.000 Last accessed on: 2021-05-12 15:19:58.000  <b>Miscellaneous</b> Shell type: Directory Node slot: 19 MRU position: 0 # of child bags: 0  First interacted with: 2021-05-13 13:35:48.020 Last interacted with: 2021-05-13 13:35:48.020		

[그림 9] Shellbags을 통해 파일시스템 확인

그러나, Shellbags은 경로가 중복되는 폴더가 있다면, 이전 폴더에 대한 정보를 새로운 폴더의 정보로 덮어쓴다. 본 시나리오에서는 다음을 만족하는 경우에 폴더 정보가 덮어쓰워질 수 있다.

- 연결한 USB가 E 드라이브를 할당 받음
- "E:\WJob" 폴더가 존재함
- 사용자가 해당 폴더를 열람함 (Shellbags 갱신 조건)

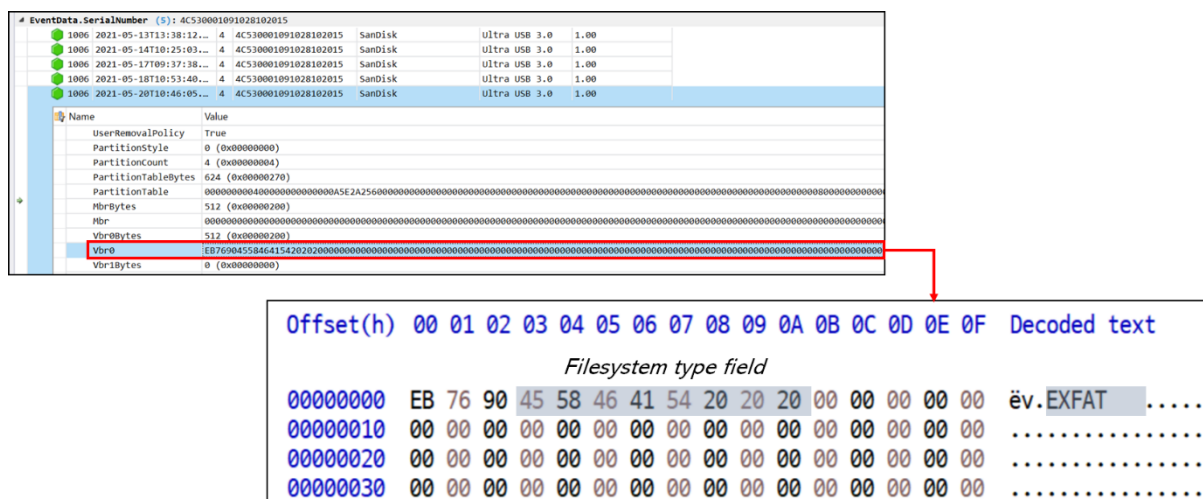
위의 경우를 고려하여, Last write key time를 통해 폴더 정보가 마지막으로 갱신된 시점에 어떤 USB가 연결되어 있었는지 확인해야 한다. [표 4]는 [표 2]의 일부를 발췌하여, "E:\WJob" 갱신 시각을 포함한 것이다. 이를 통해서 Generic Mass Storage의 파일시스템이 exFAT라는 것을 알 수 있다. 즉, Shellbags에 기록된 파일시스템 정보로는 SanDisk Ultra USB 3.0의 파일시스템을 알 수 없었다.

시간	이벤트	자세히	출처
2021-05-13 13:35:41	USB 연결	Generic, Mass Storage, AA00000000000489	Eventlog
2021-05-13 13:35:48	폴더 열람	E:\WJob (파일시스템: exFAT)	Shellbags
2021-05-13 13:36:04	USB 해제	Generic, Mass Storage, AA00000000000489	Eventlog
2021-05-13 13:36:20	USB 연결	Generic, Mass Storage, AA00000000000489	Eventlog
2021-05-13 13:36:20	드라이브 할당	E, AA00000000000489	Eventlog
2021-05-13 13:36:39	USB 해제	Generic, Mass Storage, AA00000000000489	Eventlog
2021-05-13 13:35:41	USB 연결	Generic, Mass Storage, AA00000000000489	Eventlog
2021-05-13 13:36:04	USB 해제	Generic, Mass Storage, AA00000000000489	Eventlog

[표 4] E:\WJob 폴더 갱신 시, 연결된 USB

### 3.2. [Eventlog] Microsoft-Windows-Partition/Diagnostic

해당 이벤트를 통해서 SanDisk Ultra USB 3.0의 VBR을 [그림 10]과 같이 확인하였다. VBR에서 0x03 ~ 0x0A (8 bytes) 영역은 볼륨에 설치된 파일시스템을 나타낸다. SanDisk Ultra USB 3.0에 설치된 파일시스템은 exFAT이다.



Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
<i>Filesystem type field</i>																	
00000000	EB	76	90	45	58	46	41	54	20	20	20	00	00	00	00	00	ëv. EXFAT .....
00000010	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000030	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....

[그림 10] Eventlog를 통해 확인한 SanDisk Ultra USB 3.0의 VBR

Q3 답: exFAT

#### 4. Trade\_list.xlsx이 저장된 USB의 연결/해제 시각 나열

Q2 문제 해결하면서 필요한 지식들은 모두 Q2 에서 설명하였으며, Q2 에서 정리한 [표 2]로부터 관련 USB 의 연결/해제 시각을 [표 5]로 정리하였다.

시간	이벤트	자세히	출처
2021-05-13 13:38:12	USB 연결	SanDisk, Ultra USB 3.0, 4C530001091028102015	Eventlog
2021-05-13 13:38:27	USB 해제	SanDisk, Ultra USB 3.0, 4C530001091028102015	Eventlog
2021-05-14 10:25:03	USB 연결	SanDisk, Ultra USB 3.0, 4C530001091028102015	Eventlog
2021-05-14 10:28:01	USB 해제	SanDisk, Ultra USB 3.0, 4C530001091028102015	Eventlog
2021-05-17 09:37:38	USB 연결	SanDisk, Ultra USB 3.0, 4C530001091028102015	Eventlog
2021-05-17 09:41:48	USB 해제	SanDisk, Ultra USB 3.0, 4C530001091028102015	Eventlog
2021-05-18 10:53:40	USB 연결	SanDisk, Ultra USB 3.0, 4C530001091028102015	Eventlog
2021-05-18 10:59:48	USB 해제	SanDisk, Ultra USB 3.0, 4C530001091028102015	Eventlog
2021-05-20 10:46:05	USB 연결	SanDisk, Ultra USB 3.0, 4C530001091028102015	Eventlog
2021-05-20 10:50:05	USB 해제	SanDisk, Ultra USB 3.0, 4C530001091028102015	Eventlog

[표 5] Q4 답



## 5. Trade\_list.xlsx이 저장된 USB가 연결된 사이에 가장 많이 열람한 파일 (바탕화면 경로를 포함하는) 식별

Among the files on the desktop, identify the files that have been opened while the USB, which has the suspicious file (Trade\_list.xlsx), is connected. And then find the most opened file among them. (40 points)

### [그림 11] Q5 지문

문제에서 의도하는 것처럼 열람한 파일들을 식별하려면 다음의 흔적을 확인하고 종합하여 분석해야 한다.

- 바탕화면 경로 확인
- SandDisk Ultra USB 3.0 연결, 해제 시각: [표 5] 활용
- 바탕화면 경로를 포함하는 문서 열람 흔적 식별
  - 열람 시각이 기록된 아티팩트만이 조사 대상

### 5.1. 바탕화면 경로 확인

바탕화면(Desktop) 폴더는 셸 폴더(Shell folder)이며, 사용자의 설정에 따라 바뀔 수 있다. 바탕화면 셸 폴더에 지정된 경로는 Registry의 Shell Folders에서 확인할 수 있다. 해당 키의 경로는 다음과 같다.

- NTUSER.DAT\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders

Shell Folders의 Key는 사용자 계정마다 각각 기록되는데, 본 시나리오의 PC에서는 사용자 계정은 "Aiden"만 있었다. 사용자 계정 "Aiden"의 바탕화면 경로는 [그림 12]과 같다.

Value Name	Value Type	Data
C:	C:	C:
Favorites	RegSz	C:\Users\Aiden\Favorites
Desktop	RegSz	C:\Users\Aiden\Desktop
Cookies	RegSz	C:\Users\Aiden\AppData\Local\Microsoft\Windows\INetCookies
CD Burning	RegSz	C:\Users\Aiden\AppData\Local\Microsoft\Windows\Burn\Burn

[그림 12] 바탕화면 경로

## 5.2. 바탕화면 경로를 포함하는 열람된 파일 목록

다음과 같은 아티팩트에서 바탕화면 경로(C:\Users\Aiden\Desktop)를 포함하는 파일 열람 흔적을 확인하였다. [표 5]를 포함하여 열람한 파일 목록을 표로 정리한 것이 [표 6]이다.

- JumpList & Recent (Record Time)
- Timeline (Open File → Start Time)
- Browser History
- [Registry] RecentDocs
  - 시간 값이 있는 것만 식별 대상
- [Eventlog] OAlerts (300)
  - 변경 내용 저장 여부를 물어보는 이벤트만 해당

시간	이벤트	자세히	출처
2021-05-13 10:11:01	파일 열람	C:\Users\Aiden\Desktop\Company BWJob1\australias-direction-of-goods-services-trade-financial-years.xlsx	Timeline
2021-05-13 10:11:12	파일 열람	C:\Users\Aiden\Desktop\Company BWJob1\Wd9378590-ab07-306c-bbea-8f80c0abfa84.docx	Timeline
2021-05-13 10:11:21	파일 열람	C:\Users\Aiden\Desktop\Company BWJob1\Final_CETA_Text_e.pdf	JumpList & Recent
2021-05-13 10:11:26	파일 열람	C:\Users\Aiden\Desktop\Company BWJob1\Final_CETA_Text_e.pdf	Timeline
2021-05-13 10:11:41	파일 열람	C:\Users\Aiden\Desktop\Company BWJob2\W5223e.pdf	Timeline
2021-05-13 10:11:46	파일 열람	C:\Users\Aiden\Desktop\Company BWJob3\Wft900.pdf	Timeline
2021-05-13 10:11:47	파일 열람	C:\Users\Aiden\Desktop\Company BWJob3\globaltrade-casestudy-110416.pdf	Timeline
2021-05-13 10:11:50	파일 열람	C:\Users\Aiden\Desktop\Company BWJob3\WP_shortcourse_1504.pptx	Timeline
2021-05-13 10:11:57	파일 열람	C:\Users\Aiden\Desktop\Company BWJob3\Latin-America.pptx	Browser History
2021-05-13 10:11:57	파일 열람	C:\Users\Aiden\Desktop\Company BWJob3\Latin-America.pptx	JumpList & Recent
2021-05-13 10:11:58	파일 열람	C:\Users\Aiden\Desktop\Company BWJob3\Latin-America.pptx	Timeline
2021-05-13 10:11:59	파일 열람	C:\Users\Aiden\Desktop\Company BWJob3\Wm4Merchanting.PPT	Timeline
2021-05-13 10:12:01	파일 열람	C:\Users\Aiden\Desktop\Company BWJob3\WMediterranean Sea Trade.pptx	Timeline
2021-05-13 10:12:07	파일 열람	C:\Users\Aiden\Desktop\Company BWJob3\WSToTAER.pdf	Timeline
2021-05-13 10:12:12	파일 열람	C:\Users\Aiden\Desktop\Company BWJob3\WReducing Trans-Atlantic Barriers to Trade and Investment.pdf	Timeline
2021-05-13 10:18:20	파일 열람	C:\Users\Aiden\Desktop\Company FWJob1\Wwe_14019414USEN.pptx	Timeline
2021-05-13 10:18:22	파일 열람	C:\Users\Aiden\Desktop\Company FWJob1\Wwipo_aripo_smes_hre_07_topic07.ppt	Timeline
2021-05-13 10:18:26	파일 열람	C:\Users\Aiden\Desktop\Company FWJob2\WAgenda-and-Meeting-Objectives-8Jan.doc	Timeline
2021-05-13 10:18:31	파일 열람	C:\Users\Aiden\Desktop\Company FWJob2\Wd13_257109_trade_training_centres_in_schools_program_-_schools_that_have_been_approved_for_funding_in_round_one_phase_two_0.docx	Timeline

2021-05-13 10:18:37	파일 열람	C:\Users\Aiden\Desktop\Company FWJob3\wcms_162297.pdf	Timeline
2021-05-13 13:38:12	USB 연결	SanDisk, Ultra USB 3.0, 4C530001091028102015	Eventlog
2021-05-13 13:38:27	USB 해제	SanDisk, Ultra USB 3.0, 4C530001091028102015	Eventlog
2021-05-13 16:57:29	파일 열람	C:\Users\Aiden\Desktop\Company OWJob3\retail-trade.xlsx	Timeline
2021-05-13 16:57:37	파일 열람	C:\Users\Aiden\Desktop\Company OWJob3\TeamList.xlsx	Timeline
2021-05-13 16:57:43	파일 열람	C:\Users\Aiden\Desktop\Company OWJob3\trade.xlsx	Timeline
2021-05-14 10:06:07	파일 열람	C:\Users\Aiden\Desktop\Company BWJob1\australias-direction-of-goods-services-trade-financial-years.xlsx	JumpList & Recent
2021-05-14 10:06:13	파일 열람	C:\Users\Aiden\Desktop\Company BWJob1\Final_CETA_Text_e.pdf	JumpList & Recent
2021-05-14 10:06:17	파일 열람	C:\Users\Aiden\Desktop\Company BWJob2\i5223e.pdf	JumpList & Recent
2021-05-14 10:06:21	파일 열람	C:\Users\Aiden\Desktop\Company BWJob3\ft900.pdf	JumpList & Recent
2021-05-14 10:06:22	파일 열람	C:\Users\Aiden\Desktop\Company BWJob3\globaltrade-casestudy-110416.pdf	JumpList & Recent
2021-05-14 10:06:23	파일 열람	C:\Users\Aiden\Desktop\Company BWJob3\WP_shortcourse_1504.pptx	Browser History
2021-05-14 10:06:23	파일 열람	C:\Users\Aiden\Desktop\Company BWJob3\WP_shortcourse_1504.pptx	JumpList & Recent
2021-05-14 10:06:25	파일 열람	C:\Users\Aiden\Desktop\Company BWJob3\m4Merchanting.PPT	Browser History
2021-05-14 10:06:25	파일 열람	C:\Users\Aiden\Desktop\Company BWJob3\m4Merchanting.PPT	JumpList & Recent
2021-05-14 10:06:31	파일 열람	C:\Users\Aiden\Desktop\Company BWJob3\Mediterranean Sea Trade.pptx	Browser History
2021-05-14 10:06:31	파일 열람	C:\Users\Aiden\Desktop\Company BWJob3\Mediterranean Sea Trade.pptx	JumpList & Recent
2021-05-14 10:06:33	파일 열람	C:\Users\Aiden\Desktop\Company BWJob3\Reducing Trans-Atlantic Barriers to Trade and Investment.pdf	Browser History
2021-05-14 10:06:33	파일 열람	C:\Users\Aiden\Desktop\Company BWJob3\Reducing Trans-Atlantic Barriers to Trade and Investment.pdf	JumpList & Recent
2021-05-14 10:06:34	파일 열람	C:\Users\Aiden\Desktop\Company BWJob3\SToTAER.pdf	Browser History
2021-05-14 10:06:34	파일 열람	C:\Users\Aiden\Desktop\Company BWJob3\SToTAER.pdf	JumpList & Recent
2021-05-14 10:11:18	파일 열람	C:\Users\Aiden\Desktop\Company BWJob1\wd9378590-ab07-306c-bbea-8f80c0abfa84.docx	JumpList & Recent
2021-05-14 10:12:34	파일 열람	C:\Users\Aiden\Desktop\Company FWJob1\we_14019414USEN.pptx	Browser History
2021-05-14 10:12:34	파일 열람	C:\Users\Aiden\Desktop\Company FWJob1\we_14019414USEN.pptx	JumpList & Recent
2021-05-14 10:12:35	파일 열람	C:\Users\Aiden\Desktop\Company FWJob1\wipo_aripo_smes_hre_07_topic07.ppt	Browser History
2021-05-14 10:12:35	파일 열람	C:\Users\Aiden\Desktop\Company FWJob1\wipo_aripo_smes_hre_07_topic07.ppt	JumpList & Recent
2021-05-14 10:12:42	파일 열람	C:\Users\Aiden\Desktop\Company FWJob3\wcms_162297.pdf	Browser History
2021-05-14 10:12:42	파일 열람	C:\Users\Aiden\Desktop\Company FWJob3\wcms_162297.pdf	JumpList & Recent
2021-05-14 10:15:26	파일 열람	C:\Users\Aiden\Desktop\Company FWJob2\wd13_257109_trade_training_centres_in_schools_program_-_schools_that_have_been_approved_for_funding_in_round_one_phase_two_0.docx	Browser History
2021-05-14 10:15:26	파일 열람	C:\Users\Aiden\Desktop\Company FWJob2\wd13_257109_trade_training_centres_in_schools_program_-_schools_that_have_been_approved_for_funding_in_round_one_phase_two_0.docx	JumpList & Recent
2021-05-14 10:15:27	파일 열람	C:\Users\Aiden\Desktop\Company FWJob2\Agenda-and-Meeting-Objectives-8Jan.doc	Browser History
2021-05-14 10:15:27	파일 열람	C:\Users\Aiden\Desktop\Company FWJob2\Agenda-and-Meeting-Objectives-8Jan.doc	JumpList & Recent
2021-05-14 10:16:53	파일 열람	C:\Users\Aiden\Desktop\Company LWJob1\Ch8.ppt	Browser History
2021-05-14 10:16:53	파일 열람	C:\Users\Aiden\Desktop\Company LWJob1\Ch8.ppt	JumpList & Recent
2021-05-14 10:16:57	파일 열람	C:\Users\Aiden\Desktop\Company LWJob2\Trade Routes_12 June_2019.pdf	Timeline

2021-05-14 10:16:57	파일 열람	C:\Users\Aiden\Desktop\Company L\Job2\Trade Waste Application Form - F10582.pdf	Browser History
2021-05-14 10:16:57	파일 열람	C:\Users\Aiden\Desktop\Company L\Job2\Trade Routes_12 June_2019.pdf	Browser History
2021-05-14 10:16:57	파일 열람	C:\Users\Aiden\Desktop\Company L\Job2\Trade Routes_12 June_2019.pdf	JumpList & Recent
2021-05-14 10:16:57	파일 열람	C:\Users\Aiden\Desktop\Company L\Job2\Trade Waste Application Form - F10582.pdf	JumpList & Recent
2021-05-14 10:16:58	파일 열람	C:\Users\Aiden\Desktop\Company L\Job2\Trade Waste Application Form - F10582.pdf	Timeline
2021-05-14 10:17:02	파일 열람	C:\Users\Aiden\Desktop\Company L\Job3\WA Trade Profiles - October 2020.docx	Timeline
2021-05-14 10:17:02	파일 열람	C:\Users\Aiden\Desktop\Company L\Job3\wipo_ip_dipl_krt_07_3.doc	Timeline
2021-05-14 10:19:26	파일 열람	C:\Users\Aiden\Desktop\Company L\Job3\wipo_ip_dipl_krt_07_3.doc	JumpList & Recent
2021-05-14 10:19:27	파일 열람	C:\Users\Aiden\Desktop\Company L\Job3\wipo_ip_dipl_krt_07_3.doc	Browser History
2021-05-14 10:19:27	파일 열람	C:\Users\Aiden\Desktop\Company L\Job3\WA Trade Profiles - October 2020.docx	Browser History
2021-05-14 10:19:27	파일 열람	C:\Users\Aiden\Desktop\Company L\Job3\WA Trade Profiles - October 2020.docx	JumpList & Recent
2021-05-14 10:20:53	파일 열람	C:\Users\Aiden\Desktop\Company C\Job1\Ch02-World-Trade-An-Overview.pptx	Browser History
2021-05-14 10:20:53	파일 열람	C:\Users\Aiden\Desktop\Company C\Job1\Ch02-World-Trade-An-Overview.pptx	JumpList & Recent
2021-05-14 10:20:54	파일 열람	C:\Users\Aiden\Desktop\Company C\Job1\Ch02-World-Trade-An-Overview.pptx	Timeline
2021-05-14 10:20:54	파일 열람	C:\Users\Aiden\Desktop\Company C\Job1\BEAMA-200102-003.pptx	Browser History
2021-05-14 10:20:54	파일 열람	C:\Users\Aiden\Desktop\Company C\Job1\BEAMA-200102-003.pptx	JumpList & Recent
2021-05-14 10:20:59	파일 열람	C:\Users\Aiden\Desktop\Company C\Job2\TrumpT.pptx	Browser History
2021-05-14 10:20:59	파일 열람	C:\Users\Aiden\Desktop\Company C\Job2\TrumpT.pptx	JumpList & Recent
2021-05-14 10:21:00	파일 열람	C:\Users\Aiden\Desktop\Company C\Job1\BEAMA-200102-003.pptx	Timeline
2021-05-14 10:21:01	파일 열람	C:\Users\Aiden\Desktop\Company C\Job2\TrumpT.pptx	Timeline
2021-05-14 10:21:01	파일 열람	C:\Users\Aiden\Desktop\Company C\Job2\ValentinaMintah.pptx	Browser History
2021-05-14 10:21:01	파일 열람	C:\Users\Aiden\Desktop\Company C\Job2\ValentinaMintah.pptx	JumpList & Recent
2021-05-14 10:21:03	파일 열람	C:\Users\Aiden\Desktop\Company C\Job3\Trade-union-density-rate.xlsx	JumpList & Recent
2021-05-14 10:21:04	파일 열람	C:\Users\Aiden\Desktop\Company C\Job3\VAIAS cancelled closing trades 21.1.2016.xlsx	JumpList & Recent
2021-05-14 10:21:04	파일 열람	C:\Users\Aiden\Desktop\Company C\Job3\wholesale-trade.xlsx	JumpList & Recent
2021-05-14 10:21:06	파일 열람	C:\Users\Aiden\Desktop\Company C\Job3\Trade-union-density-rate.xlsx	Browser History
2021-05-14 10:21:08	파일 열람	C:\Users\Aiden\Desktop\Company C\Job3\VAIAS cancelled closing trades 21.1.2016.xlsx	Browser History
2021-05-14 10:21:10	파일 열람	C:\Users\Aiden\Desktop\Company C\Job3\wholesale-trade.xlsx	Browser History
2021-05-14 10:23:21	파일 열람	C:\Users\Aiden\Desktop\Company C\Job3\Trade-union-density-rate.xlsx	Timeline
2021-05-14 10:23:21	파일 열람	C:\Users\Aiden\Desktop\Company C\Job3\VAIAS cancelled closing trades 21.1.2016.xlsx	Timeline
2021-05-14 10:23:21	파일 열람	C:\Users\Aiden\Desktop\Company C\Job3\wholesale-trade.xlsx	Timeline
2021-05-14 10:23:31	파일 열람	C:\Users\Aiden\Desktop\Company C\Job1\jurje_lavenex_in_handbook_int_pol_economy_of_migration_chapter_12-final.docx	Browser History
2021-05-14 10:23:31	파일 열람	C:\Users\Aiden\Desktop\Company C\Job1\INT-101-17-P040-UNCTAD-GRTAS-JPO-in-Trade-Policy-Geneva.docx	Browser History
2021-05-14 10:23:31	파일 열람	C:\Users\Aiden\Desktop\Company C\Job1\history-of-trade-exhibition-guide.docx	Browser History
2021-05-14 10:23:31	파일 열람	C:\Users\Aiden\Desktop\Company C\Job1\history-of-trade-exhibition-guide.docx	JumpList & Recent
2021-05-14 10:23:31	파일 열람	C:\Users\Aiden\Desktop\Company C\Job1\INT-101-17-P040-UNCTAD-GRTAS-JPO-in-Trade-Policy-Geneva.docx	JumpList & Recent

2021-05-14 10:23:31	파일 열람	C:\Users\Aiden\Desktop\Company C:\Job1\Wjurje_lavenex_in_handbook_int_pol_economy_of_migration_chapter_12-final.docx	JumpList & Recent
2021-05-14 10:25:03	USB 연결	SanDisk, Ultra USB 3.0, 4C530001091028102015	Eventlog
2021-05-14 10:28:01	USB 해제	SanDisk, Ultra USB 3.0, 4C530001091028102015	Eventlog
2021-05-17 09:37:38	USB 연결	SanDisk, Ultra USB 3.0, 4C530001091028102015	Eventlog
2021-05-17 09:41:48	USB 해제	SanDisk, Ultra USB 3.0, 4C530001091028102015	Eventlog
2021-05-17 09:43:09	파일 열람	C:\Users\Aiden\Desktop\Company J\Job1\Graham_-- _IR213_Lecture_4a_Distributing_the_Gains_From_Trade.pptx	Browser History
2021-05-17 09:43:09	파일 열람	C:\Users\Aiden\Desktop\Company J\Job1\Graham_-- _IR213_Lecture_4a_Distributing_the_Gains_From_Trade.pptx	JumpList & Recent
2021-05-17 09:43:10	파일 열람	C:\Users\Aiden\Desktop\Company J\Job1\GTS_Chapter_7_WS.pptx	Browser History
2021-05-17 09:43:10	파일 열람	C:\Users\Aiden\Desktop\Company J\Job1\GTS_Chapter_7_WS.pptx	JumpList & Recent
2021-05-17 09:43:11	파일 열람	C:\Users\Aiden\Desktop\Company J\Job1\Graham_-- _IR213_Lecture_4a_Distributing_the_Gains_From_Trade.pptx	Timeline
2021-05-17 09:43:17	파일 열람	C:\Users\Aiden\Desktop\Company J\Job3\Wtbal-gds-table-2011-1-en.xls	Browser History
2021-05-17 09:43:17	파일 열람	C:\Users\Aiden\Desktop\Company J\Job3\Wtbal-gds-table-2011-1-en.xls	JumpList & Recent
2021-05-17 09:47:15	파일 열람	C:\Users\Aiden\Desktop\Company J\Job2\Wworld-bank.doc	Timeline
2021-05-17 09:47:15	파일 열람	C:\Users\Aiden\Desktop\Company J\Job2\WSC-Excerpt-IPC-Core-Elements-for-Trade- Secret-Protection-Legislation-.doc	Timeline
2021-05-17 09:47:16	파일 열람	C:\Users\Aiden\Desktop\Company J\Job2\WSC-Excerpt-IPC-Core-Elements-for-Trade- Secret-Protection-Legislation-.doc	Browser History
2021-05-17 09:47:16	파일 열람	C:\Users\Aiden\Desktop\Company J\Job2\WSC-Excerpt-IPC-Core-Elements-for-Trade- Secret-Protection-Legislation-.doc	JumpList & Recent
2021-05-17 09:47:18	파일 열람	C:\Users\Aiden\Desktop\Company J\Job2\Wworld-bank.doc	Browser History
2021-05-17 09:47:18	파일 열람	C:\Users\Aiden\Desktop\Company J\Job2\Wworld-bank.doc	JumpList & Recent
2021-05-17 09:48:15	파일 열람	C:\Users\Aiden\Desktop\Company M\Job1\WTrade_Act_Procedures.docx	Timeline
2021-05-17 09:48:17	파일 열람	C:\Users\Aiden\Desktop\Company M\Job2\WAnnual Foreign Trade Statistics, 207475 (201718)_2018-11-30-11-16-30.xlsx	Browser History
2021-05-17 09:48:17	파일 열람	C:\Users\Aiden\Desktop\Company M\Job2\WAnnual Foreign Trade Statistics, 207475 (201718)_2018-11-30-11-16-30.xlsx	JumpList & Recent
2021-05-17 09:48:21	파일 열람	C:\Users\Aiden\Desktop\Company M\Job3\Wtrt_ftacis.pdf	Browser History
2021-05-17 09:48:21	파일 열람	C:\Users\Aiden\Desktop\Company M\Job3\Wtrt_ftacis.pdf	JumpList & Recent
2021-05-17 09:51:33	파일 열람	C:\Users\Aiden\Desktop\Company M\Job3\Wtrt_ftacis.pdf	Timeline
2021-05-17 09:51:41	파일 열람	C:\Users\Aiden\Desktop\Company M\Job1\WTrade_Act_Procedures.docx	Browser History
2021-05-17 09:51:41	파일 열람	C:\Users\Aiden\Desktop\Company M\Job1\WTrade_Act_Procedures.docx	JumpList & Recent
2021-05-17 09:52:40	파일 열람	C:\Users\Aiden\Desktop\Company A\Job1\W05_International_Business_and_Trade.pdf	JumpList & Recent
2021-05-17 09:52:41	파일 열람	C:\Users\Aiden\Desktop\Company A\Job1\W05_International_Business_and_Trade.pdf	Timeline
2021-05-17 09:52:42	파일 열람	C:\Users\Aiden\Desktop\Company A\Job1\WASEAN-Trade-Facilitation-Framework.pdf	Timeline
2021-05-17 09:52:42	파일 열람	C:\Users\Aiden\Desktop\Company A\Job1\WASEAN-Trade-Facilitation-Framework.pdf	JumpList & Recent
2021-05-17 09:52:43	파일 열람	C:\Users\Aiden\Desktop\Company A\Job1\WCommonwealth Trade Review 2015-Full Report.pdf	JumpList & Recent
2021-05-17 09:52:47	파일 열람	C:\Users\Aiden\Desktop\Company A\Job2\W00_Opening.pptx	JumpList & Recent
2021-05-17 09:55:39	파일 열람	C:\Users\Aiden\Desktop\Company A\Job3\WAllowable-water-trade-direction-southern- basin.docx	JumpList & Recent

2021-05-17 09:55:42	파일 열람	C:\Users\Aiden\Desktop\Company A\Job1\Commonwealth Trade Review 2015-Full Report.pdf	Timeline
2021-05-17 09:55:47	파일 열람	C:\Users\Aiden\Desktop\Company A\Job2\00_Opening.pptx	Timeline
2021-05-17 09:56:39	파일 열람	C:\Users\Aiden\Desktop\Company D\Job2\patricia-walter.pptx	Timeline
2021-05-17 09:56:45	파일 열람	C:\Users\Aiden\Desktop\Company D\Job1\Weiler_f03a.doc	Timeline
2021-05-17 09:56:45	파일 열람	C:\Users\Aiden\Desktop\Company D\Job3\morgan bse.doc	Timeline
2021-05-17 09:59:50	파일 열람	C:\Users\Aiden\Desktop\Company D\Job3\morgan bse.doc	Browser History
2021-05-17 09:59:50	파일 열람	C:\Users\Aiden\Desktop\Company D\Job3\morgan bse.doc	JumpList & Recent
2021-05-17 09:59:56	파일 열람	C:\Users\Aiden\Desktop\Company D\Job3\australias-trade-and-economic-indicators-historical.xlsx	Timeline
2021-05-17 10:00:55	파일 열람	C:\Users\Aiden\Desktop\Company R\Job1\gmp-b3-trade-in-feed.xlsx	Browser History
2021-05-17 10:00:55	파일 열람	C:\Users\Aiden\Desktop\Company R\Job1\gmp-b3-trade-in-feed.xlsx	JumpList & Recent
2021-05-17 10:00:58	파일 열람	C:\Users\Aiden\Desktop\Company R\Job2\trade_finance_bis.pdf	Browser History
2021-05-17 10:00:58	파일 열람	C:\Users\Aiden\Desktop\Company R\Job2\trade_finance_bis.pdf	JumpList & Recent
2021-05-17 10:01:02	파일 열람	C:\Users\Aiden\Desktop\Company R\Job3\580804-international-trade-and-the-global-economy.pptx	Browser History
2021-05-17 10:01:02	파일 열람	C:\Users\Aiden\Desktop\Company R\Job3\580804-international-trade-and-the-global-economy.pptx	JumpList & Recent
2021-05-17 10:01:03	파일 열람	C:\Users\Aiden\Desktop\Company R\Job3\580804-international-trade-and-the-global-economy.pptx	Timeline
2021-05-17 10:04:15	파일 열람	C:\Users\Aiden\Desktop\Company R\Job2\trade_finance_bis.pdf	Timeline
2021-05-18 10:38:33	파일 열람	C:\Users\Aiden\Desktop\Company P\Job1\CurveGlobal MiFID II Trade Reporting Template (Oct 2020).xlsx	JumpList & Recent
2021-05-18 10:38:37	파일 열람	C:\Users\Aiden\Desktop\Company P\Job2\Trade-policy-making-in-the-EU.ppt	Browser History
2021-05-18 10:38:37	파일 열람	C:\Users\Aiden\Desktop\Company P\Job2\Trade-policy-making-in-the-EU.ppt	JumpList & Recent
2021-05-18 10:38:45	파일 열람	C:\Users\Aiden\Desktop\Company P\Job2\Trade-policy-making-in-the-EU.ppt	Timeline
2021-05-18 10:38:49	파일 열람	C:\Users\Aiden\Desktop\Company P\Job1\CurveGlobal MiFID II Trade Reporting Template (Oct 2020).xlsx	Timeline
2021-05-18 10:38:50	파일 열람	C:\Users\Aiden\Desktop\Company P\Job1\CurveGlobal MiFID II Trade Reporting Template (Oct 2020).xlsx	Browser History
2021-05-18 10:38:59	파일 열람	C:\Users\Aiden\Desktop\Company P\Job3\UADA-Trade-in_Request_Multiple.docx	Timeline
2021-05-18 10:39:01	파일 열람	C:\Users\Aiden\Desktop\Company P\Job3\updates_to_australian_trade_mark_search.docx	Timeline
2021-05-18 10:43:03	파일 열람	C:\Users\Aiden\Desktop\Company P\Job3\updates_to_australian_trade_mark_search.docx	Browser History
2021-05-18 10:43:03	파일 열람	C:\Users\Aiden\Desktop\Company P\Job3\UADA-Trade-in_Request_Multiple.docx	Browser History
2021-05-18 10:43:03	파일 열람	C:\Users\Aiden\Desktop\Company P\Job3\UADA-Trade-in_Request_Multiple.docx	JumpList & Recent
2021-05-18 10:43:03	파일 열람	C:\Users\Aiden\Desktop\Company P\Job3\updates_to_australian_trade_mark_search.docx	JumpList & Recent
2021-05-18 10:44:52	파일 열람	C:\Users\Aiden\Desktop\Company T\Job1\9.36 Trade-off Report.xlsm	Browser History
2021-05-18 10:44:52	파일 열람	9.36 Trade-off Report.xlsm	RecentDocs
2021-05-18 10:44:52	파일 열람	C:\Users\Aiden\Desktop\Company T\Job1\9.36 Trade-off Report.xlsm	JumpList & Recent
2021-05-18 10:44:54	파일 열람	C:\Users\Aiden\Desktop\Company T\Job1\9.36 Trade-off Report.xlsm	Timeline
2021-05-18 10:45:03	파일 열람	C:\Users\Aiden\Desktop\Company T\Job2\trade-winds-and-manufacturing.pdf	Browser History



2021-05-18 10:45:03	파일 열람	C:\Users\Aiden\Desktop\Company T\Job2\trade-winds-and-manufacturing.pdf	JumpList & Recent
2021-05-18 10:45:10	파일 열람	C:\Users\Aiden\Desktop\Company T\Job3\Trade of CITES listed sharks _ Japan's Practice on NDF_Updated.PPTX	Browser History
2021-05-18 10:45:10	파일 열람	C:\Users\Aiden\Desktop\Company T\Job3\Trade of CITES listed sharks _ Japan's Practice on NDF_Updated.PPTX	JumpList & Recent
2021-05-18 10:45:11	파일 열람	C:\Users\Aiden\Desktop\Company T\Job3\Trade of CITES listed sharks _ Japan's Practice on NDF_Updated.PPTX	Timeline
2021-05-18 10:49:10	파일 열람	9.36 Trade-off Report.xlsm	Eventlog
2021-05-18 10:49:15	파일 열람	C:\Users\Aiden\Desktop\Company T\Job2\trade-winds-and-manufacturing.pdf	Timeline
2021-05-18 10:53:40	USB 연결	SanDisk, Ultra USB 3.0, 4C530001091028102015	Eventlog
2021-05-17 09:41:34	파일 열람	Trade_list.xlsx (= E:\Job\Trade_list.xlsx) <a href="#">[참조]</a>	Eventlog
2021-05-18 10:59:48	USB 해제	SanDisk, Ultra USB 3.0, 4C530001091028102015	Eventlog
2021-05-18 11:01:21	파일 열람	C:\Users\Aiden\Desktop\Company D\Job2\patricia-walter.pptx	Browser History
2021-05-18 11:01:21	파일 열람	patricia-walter.pptx	RecentDocs
2021-05-18 11:01:21	파일 열람	C:\Users\Aiden\Desktop\Company D\Job2\patricia-walter.pptx	JumpList & Recent
2021-05-18 11:01:26	파일 열람	C:\Users\Aiden\Desktop\Company D\Job3\ARK_ARKK_Trades.xls	JumpList & Recent
2021-05-18 11:01:27	파일 열람	C:\Users\Aiden\Desktop\Company D\Job3\ARK_ARKK_Trades.xls	Browser History
2021-05-18 11:01:33	파일 열람	C:\Users\Aiden\Desktop\Company D\Job3\ARK_ARKK_Trades.xls	Timeline
2021-05-18 11:01:41	파일 열람	C:\Users\Aiden\Desktop\Company D\Job3\australias-trade-and-economic-indicators-historical.xlsx	Browser History
2021-05-18 11:01:41	파일 열람	C:\Users\Aiden\Desktop\Company D\Job3\australias-trade-and-economic-indicators-historical.xlsx	JumpList & Recent
2021-05-18 11:04:59	파일 열람	C:\Users\Aiden\Desktop\Company D\Job1\Weiler_f03a.doc	Browser History
2021-05-18 11:04:59	파일 열람	Weiler_f03a.doc	RecentDocs
2021-05-18 11:04:59	파일 열람	C:\Users\Aiden\Desktop\Company D\Job1\Weiler_f03a.doc	JumpList & Recent
2021-05-18 11:06:34	파일 열람	C:\Users\Aiden\Desktop\Company E\Job1\Hog_MonthlyFull.xlsx	Browser History
2021-05-18 11:06:34	파일 열람	C:\Users\Aiden\Desktop\Company E\Job1\Hog_MonthlyFull.xlsx	JumpList & Recent
2021-05-18 11:06:47	파일 열람	C:\Users\Aiden\Desktop\Company E\Job2\wts2020_e.pdf	Browser History
2021-05-18 11:06:47	파일 열람	C:\Users\Aiden\Desktop\Company E\Job2\wts2020_e.pdf	JumpList & Recent
2021-05-18 11:06:49	파일 열람	C:\Users\Aiden\Desktop\Company E\Job2\wts2020_e.pdf	Timeline
2021-05-18 11:06:57	파일 열람	C:\Users\Aiden\Desktop\Company E\Job3\transcript-threat-of-deglobalisation-could-mean-for-trade-outlook-2021.docx	Timeline
2021-05-18 11:10:14	파일 열람	C:\Users\Aiden\Desktop\Company E\Job3\transcript-threat-of-deglobalisation-could-mean-for-trade-outlook-2021.docx	Browser History
2021-05-18 11:10:14	파일 열람	C:\Users\Aiden\Desktop\Company E\Job3\transcript-threat-of-deglobalisation-could-mean-for-trade-outlook-2021.docx	JumpList & Recent
2021-05-18 11:10:15	파일 열람	C:\Users\Aiden\Desktop\Company E\Job1\Hog_MonthlyFull.xlsx	Timeline
2021-05-19 13:28:22	파일 열람	Gislason - Error detection for the statistics of external trade in goods.docx	RecentDocs
2021-05-20 10:42:11	파일 열람	GATT.ppt	RecentDocs
2021-05-20 10:46:05	USB 연결	SanDisk, Ultra USB 3.0, 4C530001091028102015	Eventlog
2021-05-20 10:50:05	USB 해제	SanDisk, Ultra USB 3.0, 4C530001091028102015	Eventlog
2021-05-21 14:05:15	파일 열람	C:\Users\Aiden\Desktop\Company O\Job3\TeamList.xlsx	Browser History
2021-05-21 14:05:15	파일 열람	C:\Users\Aiden\Desktop\Company O\Job3\TeamList.xlsx	JumpList & Recent

2021-05-21 14:05:23	파일 열람	C:\Users\Aiden\Desktop\Company O\Job3\trade.xlsx	Browser History
2021-05-21 14:05:23	파일 열람	C:\Users\Aiden\Desktop\Company O\Job3\trade.xlsx	JumpList & Recent
2021-05-21 15:58:17	파일 열람	quarterly_merch_trade_volume_e.xls	RecentDocs
2021-05-21 15:58:30	파일 열람	Trade_for_all_DG_Trade.pdf	RecentDocs
2021-05-21 17:45:03	파일 열람	C:\Users\Aiden\Desktop\Company O\Job3\retail-trade.xlsx	Browser History
2021-05-21 17:45:03	파일 열람	retail-trade.xlsx	RecentDocs
2021-05-21 17:45:03	파일 열람	C:\Users\Aiden\Desktop\Company O\Job3\retail-trade.xlsx	JumpList & Recent

[표 6] 바탕화면 경로를 포함하는 열람한 파일 목록

[표 6]에서 SanDisk Ultra USB 3.0이 연결된 사이에 바탕화면 경로를 포함하는 파일이 열람된 흔적이 없었다. 실험을 통해서 In Use / Focus는 “파일을 열었음”을 의미한다는 것을 알아냈다. 특정 경로에 있는 파일이 처음 열람될 때 Open File과 In Use / Focus로 동시에 기록되고 다음 번 열람부터는 In Use / Focus로만 기록되는 것을 확인하였다. 그래서, 해당 USB가 연결되었을 때 Timeline 아티팩트에서 In Use / Focus된 파일 목록을 [표 7]과 같이 정리하였다

시간	이벤트	자세히	출처
2021-05-13 10:11:01	파일 열람	C:\Users\Aiden\Desktop\Company B\Job1\australias-direction-of-goods-services-trade-financial-years.xlsx	Timeline (In Use/Focus)
2021-05-13 10:11:10	파일 열람	C:\Users\Aiden\Desktop\Company B\Job1\d9378590-ab07-306c-bbea-8f80c0abfa84.docx	Timeline (In Use/Focus)
2021-05-13 10:11:26	파일 열람	C:\Users\Aiden\Desktop\Company B\Job1\Final_CETA_Text_e.pdf	Timeline (In Use/Focus)
2021-05-13 10:11:41	파일 열람	C:\Users\Aiden\Desktop\Company B\Job2\i5223e.pdf	Timeline (In Use/Focus)
2021-05-13 10:11:46	파일 열람	C:\Users\Aiden\Desktop\Company B\Job3\ft900.pdf	Timeline (In Use/Focus)
2021-05-13 10:11:47	파일 열람	C:\Users\Aiden\Desktop\Company B\Job3\globaltrade-casestudy-110416.pdf	Timeline (In Use/Focus)
2021-05-13 10:11:50	파일 열람	C:\Users\Aiden\Desktop\Company B\Job3\IP_shortcourse_1504.pptx	Timeline (In Use/Focus)
2021-05-13 10:11:58	파일 열람	C:\Users\Aiden\Desktop\Company B\Job3\Latin-America.pptx	Timeline (In Use/Focus)
2021-05-13 10:11:59	파일 열람	C:\Users\Aiden\Desktop\Company B\Job3\m4Merchanting.PPT	Timeline (In Use/Focus)
2021-05-13 10:12:01	파일 열람	C:\Users\Aiden\Desktop\Company B\Job3\Mediterranean Sea Trade.pptx	Timeline (In Use/Focus)
2021-05-13 10:12:07	파일 열람	C:\Users\Aiden\Desktop\Company B\Job3\SToTAER.pdf	Timeline (In Use/Focus)
2021-05-13 10:12:12	파일 열람	C:\Users\Aiden\Desktop\Company B\Job3\ft900.pdf	Timeline (In Use/Focus)
2021-05-13 10:12:12	파일 열람	C:\Users\Aiden\Desktop\Company B\Job3\globaltrade-casestudy-110416.pdf	Timeline (In Use/Focus)



2021-05-13 10:12:12	파일 열람	C:\Users\Aiden\Desktop\Company B\Job3\Reducing Trans-Atlantic Barriers to Trade and Investment.pdf	Timeline (In Use/Focus)
2021-05-13 10:12:20	파일 열람	C:\Users\Aiden\Desktop\Company B\Job1\australias-direction-of-goods-services-trade-financial-years.xlsx	Timeline (In Use/Focus)
2021-05-13 10:13:14	파일 열람	C:\Users\Aiden\Desktop\Company B\Job1\australias-direction-of-goods-services-trade-financial-years.xlsx	Timeline (In Use/Focus)
2021-05-13 10:13:45	파일 열람	C:\Users\Aiden\Desktop\Company B\Job1\australias-direction-of-goods-services-trade-financial-years.xlsx	Timeline (In Use/Focus)
2021-05-13 10:14:10	파일 열람	C:\Users\Aiden\Desktop\Company B\Job1\australias-direction-of-goods-services-trade-financial-years.xlsx	Timeline (In Use/Focus)
2021-05-13 10:15:21	파일 열람	C:\Users\Aiden\Desktop\Company B\Job1\australias-direction-of-goods-services-trade-financial-years.xlsx	Timeline (In Use/Focus)
2021-05-13 10:15:44	파일 열람	C:\Users\Aiden\Desktop\Company B\Job1\australias-direction-of-goods-services-trade-financial-years.xlsx	Timeline (In Use/Focus)
2021-05-13 10:16:08	파일 열람	C:\Users\Aiden\Desktop\Company B\Job1\australias-direction-of-goods-services-trade-financial-years.xlsx	Timeline (In Use/Focus)
2021-05-13 10:16:30	파일 열람	C:\Users\Aiden\Desktop\Company B\Job1\australias-direction-of-goods-services-trade-financial-years.xlsx	Timeline (In Use/Focus)
2021-05-13 10:16:58	파일 열람	C:\Users\Aiden\Desktop\Company B\Job1\australias-direction-of-goods-services-trade-financial-years.xlsx	Timeline (In Use/Focus)
2021-05-13 10:17:22	파일 열람	C:\Users\Aiden\Desktop\Company B\Job1\australias-direction-of-goods-services-trade-financial-years.xlsx	Timeline (In Use/Focus)
2021-05-13 10:17:47	파일 열람	C:\Users\Aiden\Desktop\Company B\Job1\australias-direction-of-goods-services-trade-financial-years.xlsx	Timeline (In Use/Focus)
2021-05-13 10:18:20	파일 열람	C:\Users\Aiden\Desktop\Company F\Job1\we_14019414USEN.pptx	Timeline (In Use/Focus)
2021-05-13 10:18:22	파일 열람	C:\Users\Aiden\Desktop\Company F\Job1\wipo_aripo_smes_hre_07_topic07.ppt	Timeline (In Use/Focus)
2021-05-13 10:18:26	파일 열람	C:\Users\Aiden\Desktop\Company F\Job2\Agenda-and-Meeting-Objectives-8Jan.doc	Timeline (In Use/Focus)
2021-05-13 10:18:30	파일 열람	C:\Users\Aiden\Desktop\Company F\Job2\13_257109_trade_training_centres_in_schools_program_-_schools_that_have_been_approved_for_funding_in_round_one_phase_two_0.docx	Timeline (In Use/Focus)
2021-05-13 10:18:37	파일 열람	C:\Users\Aiden\Desktop\Company F\Job3\wcms_162297.pdf	Timeline (In Use/Focus)
2021-05-13 13:38:12	USB 연결	SanDisk, Ultra USB 3.0, 4C530001091028102015	Eventlog
2021-05-13 13:38:27	USB 해제	SanDisk, Ultra USB 3.0, 4C530001091028102015	Eventlog
2021-05-13 16:57:25	파일 열람	C:\Users\Aiden\Desktop\Company O\Job3\Wretail-trade.xlsx	Timeline (In Use/Focus)
2021-05-13 16:57:34	파일 열람	C:\Users\Aiden\Desktop\Company O\Job3\WTeamList.xlsx	Timeline (In Use/Focus)
2021-05-13 16:57:39	파일 열람	C:\Users\Aiden\Desktop\Company O\Job3\Wtrade.xlsx	Timeline (In Use/Focus)
2021-05-13 16:59:54	파일 열람	C:\Users\Aiden\Desktop\Company O\Job3\Wtrade.xlsx	Timeline (In Use/Focus)
2021-05-14 10:06:10	파일 열람	C:\Users\Aiden\Desktop\Company B\Job1\Wd9378590-ab07-306c-bbea-8f80c0abfa84.docx	Timeline (In Use/Focus)

2021-05-14 10:06:13	파일 열람	C:\Users\Aiden\Desktop\Company BW\Job1\Final_CETA_Text_e.pdf	Timeline (In Use/Focus)
2021-05-14 10:06:18	파일 열람	C:\Users\Aiden\Desktop\Company BW\Job2\Wi5223e.pdf	Timeline (In Use/Focus)
2021-05-14 10:06:21	파일 열람	C:\Users\Aiden\Desktop\Company BW\Job3\Wft900.pdf	Timeline (In Use/Focus)
2021-05-14 10:06:22	파일 열람	C:\Users\Aiden\Desktop\Company BW\Job3\globaltrade-casestudy-110416.pdf	Timeline (In Use/Focus)
2021-05-14 10:06:25	파일 열람	C:\Users\Aiden\Desktop\Company BW\Job3\WP_shortcourse_1504.pptx	Timeline (In Use/Focus)
2021-05-14 10:06:26	파일 열람	C:\Users\Aiden\Desktop\Company BW\Job3\Wm4Merchanting.PPT	Timeline (In Use/Focus)
2021-05-14 10:06:32	파일 열람	C:\Users\Aiden\Desktop\Company BW\Job3\WMediterranean Sea Trade.pptx	Timeline (In Use/Focus)
2021-05-14 10:06:33	파일 열람	C:\Users\Aiden\Desktop\Company BW\Job3\Reducing Trans-Atlantic Barriers to Trade and Investment.pdf	Timeline (In Use/Focus)
2021-05-14 10:06:35	파일 열람	C:\Users\Aiden\Desktop\Company BW\Job3\WSToTAER.pdf	Timeline (In Use/Focus)
2021-05-14 10:11:07	파일 열람	C:\Users\Aiden\Desktop\Company BW\Job1\Waustralias-direction-of-goods-services-trade-financial-years.xlsx	Timeline (In Use/Focus)
2021-05-14 10:11:17	파일 열람	C:\Users\Aiden\Desktop\Company BW\Job3\Reducing Trans-Atlantic Barriers to Trade and Investment.pdf	Timeline (In Use/Focus)
2021-05-14 10:11:17	파일 열람	C:\Users\Aiden\Desktop\Company BW\Job3\globaltrade-casestudy-110416.pdf	Timeline (In Use/Focus)
2021-05-14 10:11:17	파일 열람	C:\Users\Aiden\Desktop\Company BW\Job3\Wft900.pdf	Timeline (In Use/Focus)
2021-05-14 10:11:17	파일 열람	C:\Users\Aiden\Desktop\Company BW\Job2\Wi5223e.pdf	Timeline (In Use/Focus)
2021-05-14 10:11:17	파일 열람	C:\Users\Aiden\Desktop\Company BW\Job1\Final_CETA_Text_e.pdf	Timeline (In Use/Focus)
2021-05-14 10:12:35	파일 열람	C:\Users\Aiden\Desktop\Company FW\Job1\Wwe_14019414USEN.pptx	Timeline (In Use/Focus)
2021-05-14 10:12:39	파일 열람	C:\Users\Aiden\Desktop\Company FW\Job2\WAgenda-and-Meeting-Objectives-8Jan.doc	Timeline (In Use/Focus)
2021-05-14 10:12:39	파일 열람	C:\Users\Aiden\Desktop\Company FW\Job2\Wd13_257109_trade_training_centres_in_schools_program_-_schools_that_have_been_approved_for_funding_in_round_one_phase_two_0.docx	Timeline (In Use/Focus)
2021-05-14 10:12:43	파일 열람	C:\Users\Aiden\Desktop\Company FW\Job3\Wwcms_162297.pdf	Timeline (In Use/Focus)
2021-05-14 10:15:31	파일 열람	C:\Users\Aiden\Desktop\Company FW\Job1\Wwipo_aripo_smes_hre_07_topic07.ppt	Timeline (In Use/Focus)
2021-05-14 10:16:57	파일 열람	C:\Users\Aiden\Desktop\Company LW\Job2\WTrade Routes_12 June_2019.pdf	Timeline (In Use/Focus)
2021-05-14 10:16:58	파일 열람	C:\Users\Aiden\Desktop\Company LW\Job2\WTrade Waste Application Form - F10582.pdf	Timeline (In Use/Focus)
2021-05-14 10:17:02	파일 열람	C:\Users\Aiden\Desktop\Company LW\Job3\WWA Trade Profiles - October 2020.docx	Timeline (In Use/Focus)

2021-05-14 10:17:02	파일 열람	C:\Users\Aiden\Desktop\Company L\Job3\wipo_ip_dipl_krt_07_3.doc	Timeline (In Use/Focus)
2021-05-14 10:19:36	파일 열람	C:\Users\Aiden\Desktop\Company L\Job2\Trade Routes_12 June_2019.pdf	Timeline (In Use/Focus)
2021-05-14 10:20:54	파일 열람	C:\Users\Aiden\Desktop\Company C\Job1\Ch02-World-Trade-An-Overview.pptx	Timeline (In Use/Focus)
2021-05-14 10:20:59	파일 열람	C:\Users\Aiden\Desktop\Company C\Job1\BEAMA-200102-003.pptx	Timeline (In Use/Focus)
2021-05-14 10:21:01	파일 열람	C:\Users\Aiden\Desktop\Company C\Job2\TrumpT.pptx	Timeline (In Use/Focus)
2021-05-14 10:23:21	파일 열람	C:\Users\Aiden\Desktop\Company C\Job3\wholesale-trade.xlsx	Timeline (In Use/Focus)
2021-05-14 10:23:21	파일 열람	C:\Users\Aiden\Desktop\Company C\Job3\VAIAS cancelled closing trades 21.1.2016.xlsx	Timeline (In Use/Focus)
2021-05-14 10:23:21	파일 열람	C:\Users\Aiden\Desktop\Company C\Job3\Trade-union-density-rate.xlsx	Timeline (In Use/Focus)
2021-05-14 10:25:03	USB 연결	SanDisk, Ultra USB 3.0, 4C530001091028102015	Eventlog
2021-05-14 10:28:01	USB 해제	SanDisk, Ultra USB 3.0, 4C530001091028102015	Eventlog
2021-05-17 09:37:38	USB 연결	SanDisk, Ultra USB 3.0, 4C530001091028102015	Eventlog
2021-05-17 09:38:05	파일 열람	C:\Users\Aiden\Desktop\Company O\Job3\retail-trade.xlsx	Timeline (In Use/Focus)
2021-05-17 09:38:12	파일 열람	C:\Users\Aiden\Desktop\Company O\Job3\TeamList.xlsx	Timeline (In Use/Focus)
2021-05-17 09:38:18	파일 열람	C:\Users\Aiden\Desktop\Company O\Job3\trade.xlsx	Timeline (In Use/Focus)
2021-05-17 09:38:28	파일 열람	C:\Users\Aiden\Desktop\Company O\Job3\trade.xlsx	Timeline (In Use/Focus)
2021-05-17 09:41:36	파일 열람	C:\Users\Aiden\Desktop\Company O\Job3\trade.xlsx	Timeline (In Use/Focus)
2021-05-17 09:41:48	USB 해제	SanDisk, Ultra USB 3.0, 4C530001091028102015	Eventlog
2021-05-17 09:43:11	파일 열람	C:\Users\Aiden\Desktop\Company J\Job1\Graham_--_JR213_Lecture_4a_Distributing_the_Gains_From_Trade.pptx	Timeline (In Use/Focus)
2021-05-17 09:47:15	파일 열람	C:\Users\Aiden\Desktop\Company J\Job2\world-bank.doc	Timeline (In Use/Focus)
2021-05-17 09:47:15	파일 열람	C:\Users\Aiden\Desktop\Company J\Job2\WSC-Excerpt-IPC-Core-Elements-for-Trade-Secret-Protection-Legislation-.doc	Timeline (In Use/Focus)
2021-05-17 09:48:15	파일 열람	C:\Users\Aiden\Desktop\Company M\Job1\Trade_Act_Procedures.docx	Timeline (In Use/Focus)
2021-05-17 09:51:33	파일 열람	C:\Users\Aiden\Desktop\Company M\Job3\trt_ftacis.pdf	Timeline (In Use/Focus)
2021-05-17 09:52:41	파일 열람	C:\Users\Aiden\Desktop\Company A\Job1\05_International_Business_and_Trade.pdf	Timeline (In Use/Focus)
2021-05-17 09:52:42	파일 열람	C:\Users\Aiden\Desktop\Company A\Job1\ASEAN-Trade-Facilitation-Framework.pdf	Timeline (In Use/Focus)
2021-05-17 09:55:42	파일 열람	C:\Users\Aiden\Desktop\Company A\Job1\Commonwealth Trade Review 2015-Full Report.pdf	Timeline (In Use/Focus)

2021-05-17 09:55:45	파일 열람	C:\Users\Aiden\Desktop\Company AWJob1\W05_International_Business_and_Trade.pdf	Timeline (In Use/Focus)
2021-05-17 09:55:45	파일 열람	C:\Users\Aiden\Desktop\Company AWJob1\WASEAN-Trade-Facilitation-Framework.pdf	Timeline (In Use/Focus)
2021-05-17 09:55:47	파일 열람	C:\Users\Aiden\Desktop\Company AWJob2\W00_Opening.pptx	Timeline (In Use/Focus)
2021-05-17 09:56:39	파일 열람	C:\Users\Aiden\Desktop\Company DWJob2\Wpatricia-walter.pptx	Timeline (In Use/Focus)
2021-05-17 09:56:45	파일 열람	C:\Users\Aiden\Desktop\Company DWJob1\Wweiler_f03a.doc	Timeline (In Use/Focus)
2021-05-17 09:56:45	파일 열람	C:\Users\Aiden\Desktop\Company DWJob3\Wmorgan bse.doc	Timeline (In Use/Focus)
2021-05-17 09:59:56	파일 열람	C:\Users\Aiden\Desktop\Company DWJob3\Waustralias-trade-and-economic-indicators-historical.xlsx	Timeline (In Use/Focus)
2021-05-17 10:01:03	파일 열람	C:\Users\Aiden\Desktop\Company RWJob3\W580804-international-trade-and-the-global-economy.pptx	Timeline (In Use/Focus)
2021-05-17 10:04:15	파일 열람	C:\Users\Aiden\Desktop\Company RWJob2\Wtrade_finance_bis.pdf	Timeline (In Use/Focus)
2021-05-18 10:38:33	파일 열람	C:\Users\Aiden\Desktop\Company PWJob1\WCurveGlobal MiFID II Trade Reporting Template (Oct 2020).xlsx	Timeline (In Use/Focus)
2021-05-18 10:38:45	파일 열람	C:\Users\Aiden\Desktop\Company PWJob2\WTrade-policy-making-in-the-EU.ppt	Timeline (In Use/Focus)
2021-05-18 10:38:59	파일 열람	C:\Users\Aiden\Desktop\Company PWJob3\WUADA-Trade-in_Request_Multiple.docx	Timeline (In Use/Focus)
2021-05-18 10:39:01	파일 열람	C:\Users\Aiden\Desktop\Company PWJob3\Wupdates_to_australian_trade_mark_search.docx	Timeline (In Use/Focus)
2021-05-18 10:44:52	파일 열람	C:\Users\Aiden\Desktop\Company TWJob1\W9.36 Trade-off Report.xlsm	Timeline (In Use/Focus)
2021-05-18 10:45:11	파일 열람	C:\Users\Aiden\Desktop\Company TWJob3\WTrade of CITES listed sharks _ Japan's Practice on NDF_Updated.PPTX	Timeline (In Use/Focus)
2021-05-18 10:49:15	파일 열람	C:\Users\Aiden\Desktop\Company TWJob2\Wtrade-winds-and-manufacturing.pdf	Timeline (In Use/Focus)
2021-05-18 10:53:40	USB 연결	SanDisk, Ultra USB 3.0, 4C530001091028102015	Eventlog
2021-05-18 10:54:20	파일 열람	C:\Users\Aiden\Desktop\Company OWJob3\Wretail-trade.xlsx	Timeline (In Use/Focus)
2021-05-18 10:57:49	파일 열람	C:\Users\Aiden\Desktop\Company OWJob3\WTeamList.xlsx	Timeline (In Use/Focus)
2021-05-18 10:57:55	파일 열람	C:\Users\Aiden\Desktop\Company OWJob3\Wtrade.xlsx	Timeline (In Use/Focus)
2021-05-18 10:59:48	USB 해제	SanDisk, Ultra USB 3.0, 4C530001091028102015	Eventlog
2021-05-18 11:01:26	파일 열람	C:\Users\Aiden\Desktop\Company DWJob3\WARK_ARKK_Trades.xls	Timeline (In Use/Focus)
2021-05-18 11:01:41	파일 열람	C:\Users\Aiden\Desktop\Company DWJob3\Waustralias-trade-and-economic-indicators-historical.xlsx	Timeline (In Use/Focus)
2021-05-18 11:04:51	파일 열람	C:\Users\Aiden\Desktop\Company DWJob1\Wweiler_f03a.doc	Timeline (In Use/Focus)
2021-05-18 11:04:59	파일 열람	C:\Users\Aiden\Desktop\Company DWJob2\Wpatricia-walter.pptx	Timeline (In Use/Focus)

2021-05-18 11:06:49	파일 열람	C:\Users\Aiden\Desktop\Company E\Job2\wts2020_e.pdf	Timeline (In Use/Focus)
2021-05-18 11:06:57	파일 열람	C:\Users\Aiden\Desktop\Company E\Job3\transcript-threat-of-deglobalisation-could-mean-for-trade-outlook-2021.docx	Timeline (In Use/Focus)
2021-05-18 11:10:15	파일 열람	C:\Users\Aiden\Desktop\Company E\Job1\Hog_MonthlyFull.xlsx	Timeline (In Use/Focus)
2021-05-20 10:46:05	USB 연결	SanDisk, Ultra USB 3.0, 4C530001091028102015	Eventlog
2021-05-20 10:50:05	USB 해제	SanDisk, Ultra USB 3.0, 4C530001091028102015	Eventlog
2021-05-21 14:05:03	파일 열람	C:\Users\Aiden\Desktop\Company O\Job3\retail-trade.xlsx	Timeline (In Use/Focus)
2021-05-21 14:05:15	파일 열람	C:\Users\Aiden\Desktop\Company O\Job3\TeamList.xlsx	Timeline (In Use/Focus)
2021-05-21 14:05:23	파일 열람	C:\Users\Aiden\Desktop\Company O\Job3\trade.xlsx	Timeline (In Use/Focus)
2021-05-21 14:05:34	파일 열람	C:\Users\Aiden\Desktop\Company O\Job3\trade.xlsx	Timeline (In Use/Focus)
2021-05-21 15:58:10	파일 열람	C:\Users\Aiden\Desktop\Company O\Job3\trade.xlsx	Timeline (In Use/Focus)
2021-05-21 15:58:13	파일 열람	C:\Users\Aiden\Desktop\Company O\Job3\trade.xlsx	Timeline (In Use/Focus)
2021-05-21 17:04:12	파일 열람	C:\Users\Aiden\Desktop\Company O\Job3\retail-trade.xlsx	Timeline (In Use/Focus)
2021-05-21 17:04:40	파일 열람	C:\Users\Aiden\Desktop\Company O\Job3\retail-trade.xlsx	Timeline (In Use/Focus)
2021-05-21 17:06:57	파일 열람	C:\Users\Aiden\Desktop\Company O\Job3\retail-trade.xlsx	Timeline (In Use/Focus)
2021-05-21 17:07:31	파일 열람	C:\Users\Aiden\Desktop\Company O\Job3\retail-trade.xlsx	Timeline (In Use/Focus)
2021-05-21 17:07:55	파일 열람	C:\Users\Aiden\Desktop\Company O\Job3\retail-trade.xlsx	Timeline (In Use/Focus)
2021-05-21 17:41:57	파일 열람	C:\Users\Aiden\Desktop\Company O\Job3\retail-trade.xlsx	Timeline (In Use/Focus)
2021-05-21 17:43:37	파일 열람	C:\Users\Aiden\Desktop\Company O\Job3\retail-trade.xlsx	Timeline (In Use/Focus)
2021-05-21 17:45:03	파일 열람	C:\Users\Aiden\Desktop\Company O\Job3\retail-trade.xlsx	Timeline (In Use/Focus)

**[표 7] 바탕화면 경로를 포함하는 열람한 문서 목록 (Timeline – In Use / Focus)**

### 5.3. 바탕화면 경로를 포함하는 열람된 파일 중 가장 많이 열람된 것

Q5 문제의 질문 중 “가장 많이 열람된 것을” 다음과 같이 해석하였다.

- 특정 USB가 연결된 동안 Desktop 경로를 포함하는 열람된 문서 찾기 --- (A)
- A의 결과 중 Focus로 가장 많이 열람된 것

[표 7]에서 SanDisk, Ultra USB 3.0가 연결된 사이에 Focus된 횟수를 정리하면 [표 8]과 같으며, 녹색 행이 Q5에 대한 답이다.

열람된 파일명 (경로 포함)	Focus 로 기록된 시각	Focus 횟수
C:\Users\Aiden\Desktop\Company O\Job3\trade.xlsx	2021-05-17 09:38:18 2021-05-17 09:38:28 2021-05-17 09:41:36 2021-05-17 09:41:36	4
C:\Users\Aiden\Desktop\Company O\Job3\retail-trade.xlsx	2021-05-17 09:38:05 2021-05-18 10:54:20	2
C:\Users\Aiden\Desktop\Company O\Job3\TeamList.xlsx	2021-05-17 09:38:12 2021-05-18 10:57:49	2

[표 8] Q5 답 및 답 근거