251 - Artifacts Never Lie

Team Information

Team Name : HSPACE

Team Member : Jinung Lee, Beomjun Park, DoHyeon Kim, Soyoung Cho

Email Address : hspacedigitalforensicslab@gmail.com

Teams must:

- Provide a detailed, step-by-step description of their problem-solving approach to ensure reproducibility by another examiner.
- List all tools used to arrive at their conclusions.

Tools used:

Name:	Magnet AXIOM	Publisher:	Magnet Forensics
Version:	9.5.0.45393		
URL:	https://www.magnetforensics.com/		

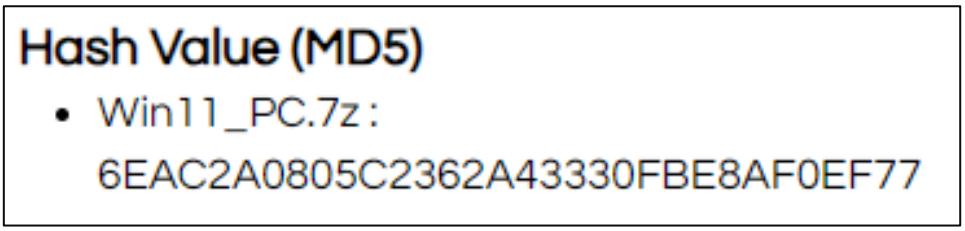
Name:	HashTab	Publisher:	Implbits Software
Version:	6.0.0		
URL:	https://implbits.com/		

Name:	REGA	Publisher:	DFRC
Version:	1.5.3		
URL:	https://dfrc.korea.ac.kr/		

Name:	NTFS Log Tracker	Publisher:	Junghoon Oh(blueangel)
Version:	1.9		
URL:	https://sites.google.com/site/forensicnote/ntfs-log-tracker		

Step-by-step methodology:

문제 풀이에 앞서, dfchallenge.org에 공지된 문제 해시와 다운로드 받은 문제 해시를 비교함으로써 분석 대상이 동일한 파일임을 증명한다.



[그림 1] dfchallenge.org에 공지된 문제 해시(MD5) 값.

[그림 2] HashTab을 통해 확인한 문제 해시(MD5) 값.

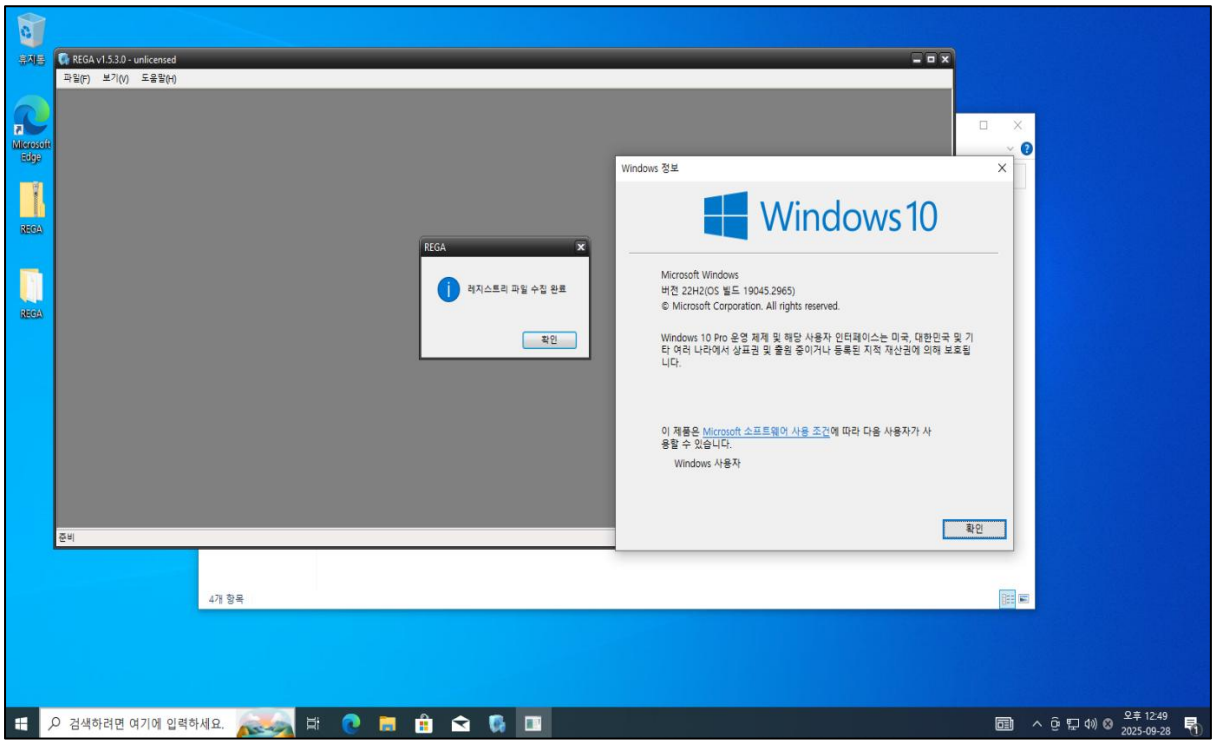
1. 사용자는 윈도우 10에서 윈도우 11로 운영체제를 언제 업그레이드 했나요? (업그레이드 시각)

Windows 10에서 11로 업데이트를 진행할 때, install data가 변경되는 것을 확인했다. 이는, 검증을 통해 알 수 있었으며, 검증 절차는 다음과 같다. 검증에 사용된 Windows 10의 정보는 [표 1]과 같이 정리할 수 있다.

Window 정보	Windows 10 Pro
버전	22H2
OS 빌드	19045.2965

[표 1] 가상환경을 구축을 위해 사용된 window 이미지 파일 정보.

증명을 위한 가상환경 구축을 완료하고, [그림 3]과 같이, Windows 정보를 통하여 위의 정보를 증명하며, 증거 수집으로는 REGA를 이용하였다.



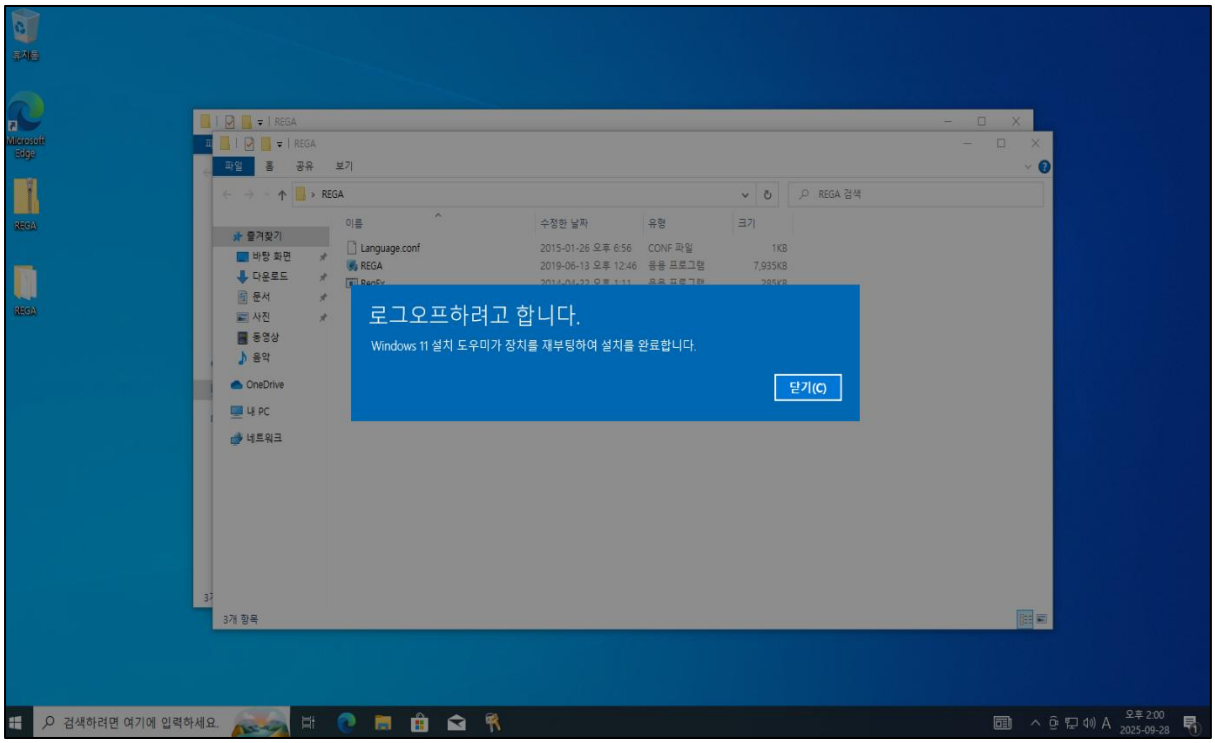
[그림 3] 설치된 Winodws 10의 정보와, REGA를 이용한 증거 수집.

윈도우 설치 정보를 확인한 결과, 설치된 시각은 [그림 4]와 같이, 2025-09-28 03:43:20 (UTC)이라는 것을 알 수 있다.

윈도우 설치 정보	
Product Name	Windows 10 Pro
Owner	Windows 사용자
Organization	
Product ID	00330-80000-00000-AA962
Product Version	Multiprocessor Free 6.3.19041.1.amd64fre.vb_release.191206-1406
Install Date	2025-09-28 03:42:20 Sun (UTC)
System Root	C:₩Windows

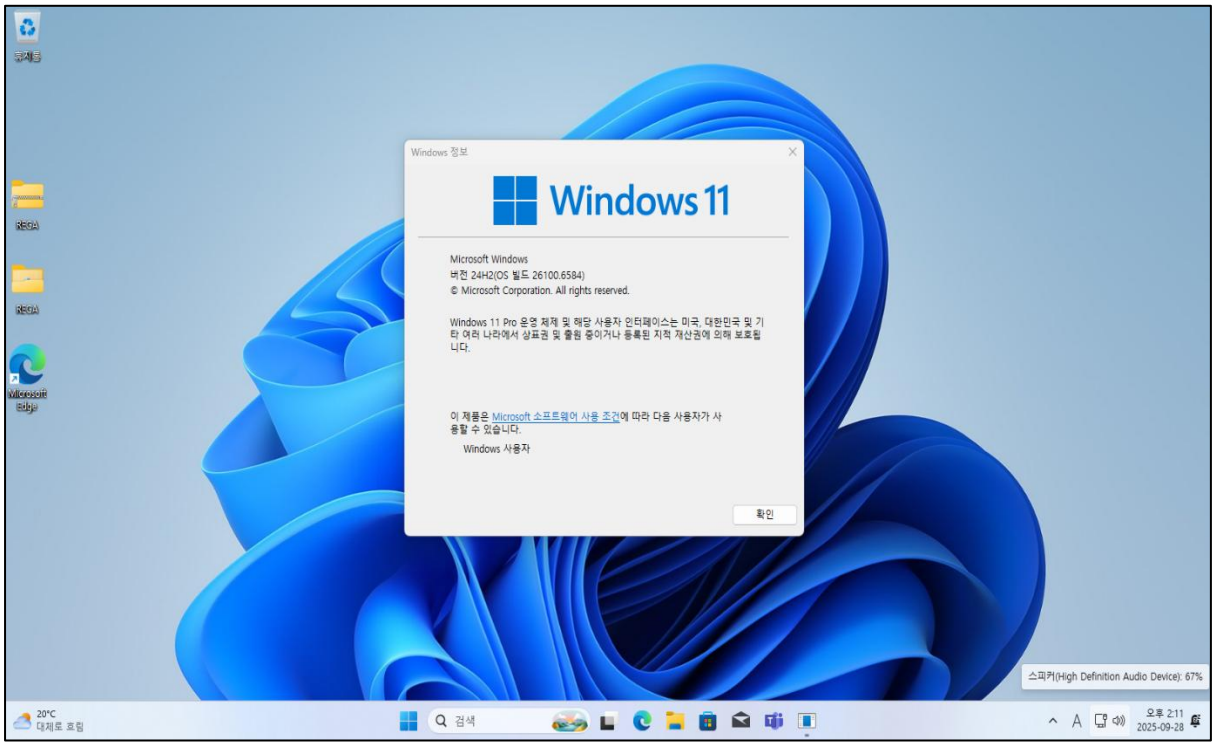
[그림 4] Windows 10의 설치 시각.

REGA를 통하여 Windows 10의 설치 시각을 파악하고 [그림 5]와 같이, Windows 11로 업데이트를 진행했다.



[그림 5] Windows 11로 업데이트를 진행하는 모습.

Windows 11로 업데이트가 완료된 후는 [그림 11]과 같다. 또한 이에 대한 운영체제 정보를 정리하면, [표 2]와 같이 정리할 수 있다.



[그림 6] 가상환경이 Windows 11로 업데이트가 완료된 모습.

Window 정보	Windows 11
버전	25H2
OS 빌드	26100.6584

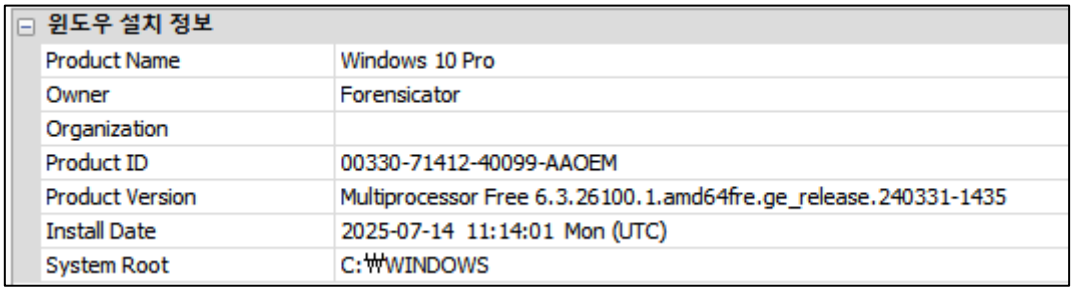
[표 2] Windows 11의 운영체제 정보.

[그림 7]과 같이, 업그레이드를 진행 후 설치된 시각이 변경된 것을 확인할 수 있다.

윈도우 설치 정보	
Product Name	Windows 10 Pro
Owner	Windows 사용자
Organization	
Product ID	00330-80000-00000-AA111
Product Version	Multiprocessor Free 6.3.26100.1.amd64fre.ge_release.240331-1435
Install Date	2025-09-28 05:05:28 Sun (UTC)
System Root	C:₩WINDOWS

[그림 7] Windwos 11로 업그레이드 후 변경된 설치된 시각.

이를 통하여 Windows 11의 업그레이드 시각은 현재 Windows의 설치된 시각이라는 것을 알았으며 이를 통해 해당 문제를 REGA를 통해 분석을 진행했다. 윈도우 설치 정보를 확인한 결과, 답은 2025-07-14 11:14:01 (UTC)라는 것을 알 수 있다.



윈도우 설치 정보	
Product Name	Windows 10 Pro
Owner	Forensicator
Organization	
Product ID	00330-71412-40099-AAOEM
Product Version	Multiprocessor Free 6.3.26100.1.amd64fre.ge_release.240331-1435
Install Date	2025-07-14 11:14:01 Mon (UTC)
System Root	C:₩WINDOWS

[그림 8] 문제파일의 윈도우 설치 정보 확인.

답: 2025-07-14 11:14:01

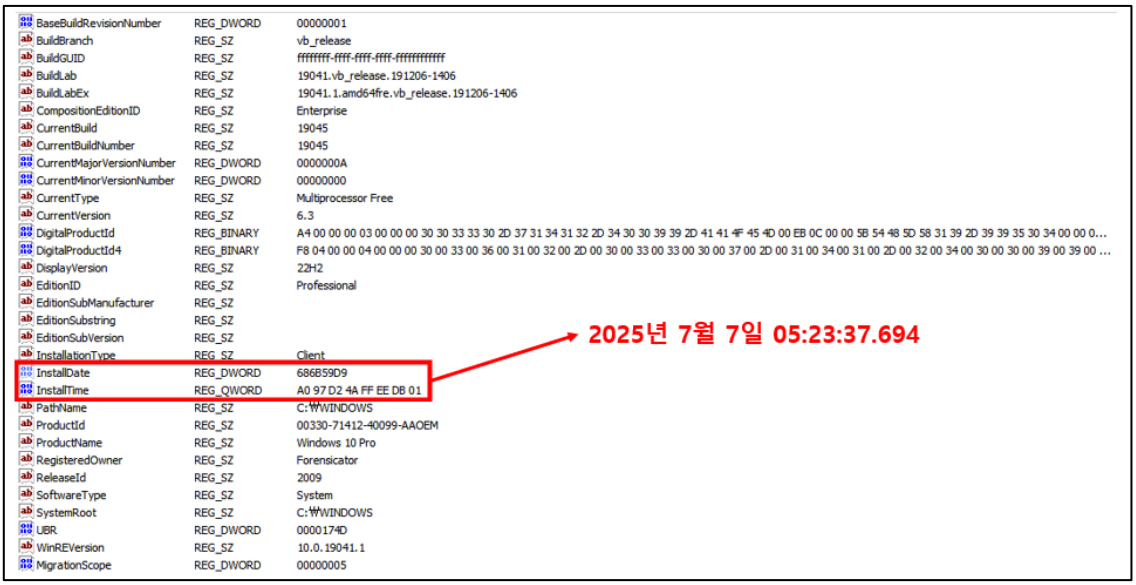
2. 사용자가 사용한 이전 윈도우 10 운영체제는 언제 설치했던 것인가요? (설치 시각)

HKLM₩SYSTEM₩₩SETUP₩Source OS에는 Windows 주요 업그레이드 또는 재설치 전에 생성된 키 정보의 백업 사본이 포함되어 있다. 이를 통하여 확인할 수 있었으며, 문제파일에서는, 2025년 7월 14일에 진행된 업데이트 정보를 확인할 수 있었다.

REGISTRY KEY
HKEY_LOCAL_MACHINE₩SYSTEM₩Setup₩Source OS (Updated on 7/14/2025 17:49:37)

[표 3] 문제 파일에서 발견된 키 정보.

해당 레지스트리 키에는 업그레이드가 진행되기 전의 정보가 들어있다. 이 중 답을 찾기 위한 정보는 [그림 9]와 같이, InstallTime과 InstallDate이다. 이를 해석하면 2025-07-07 05:23.37 (UTC)라는 것을 알 수 있다.

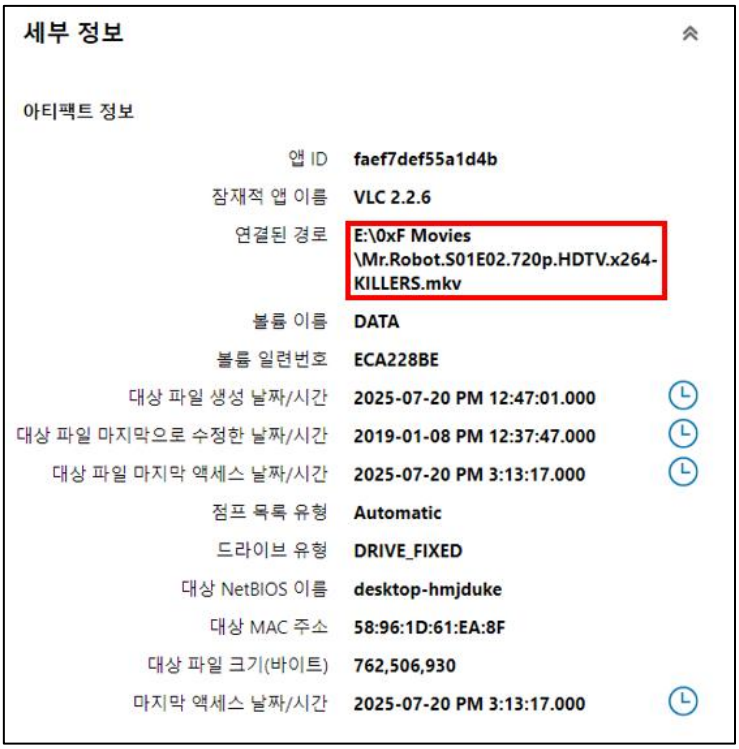


[그림 9] HKEY_LOCAL_MACHINE₩SYSTEM₩Setup₩Source OS에서의 Windows 설치 정보.

답: 2025-07-07 05:23.37

3. 사용자가 VLC Media Player로 재생한 영상을 식별하세요. (영상 전체 경로)

응용 프로그램을 이용하여 문서, 영상 등의 파일을 로드했을 때, 이는 Jumplist에서 확인할 수 있다. 이러한 정보를 바탕으로 Magnet AXIOM으로 Jumplist를 분석한 결과, [그림 10]과 같이, **E:₩0xF Movies₩Mr.Robot.S01E02.720p.HDTV.x264-KILLERS.mkv**를 발견할 수 있었다.

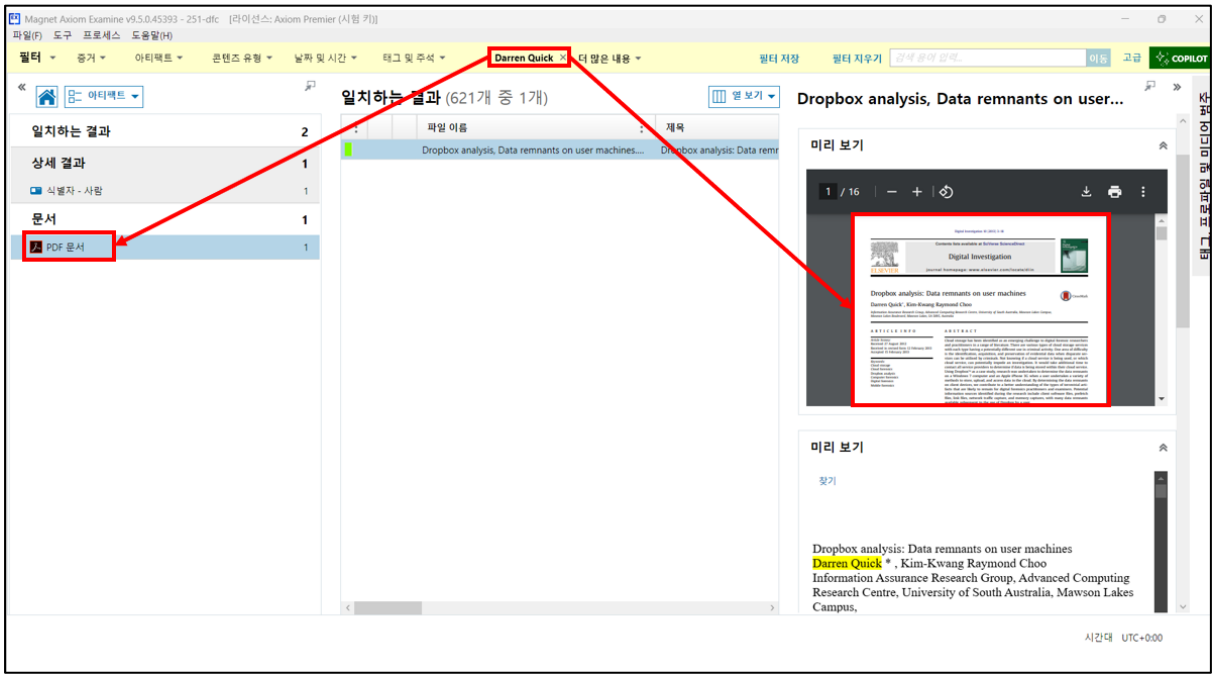


[그림 10] Jumplist에서 발견된 VLC를 이용해 재생된 비디오 정보.

답: E:₩0xF Movies₩Mr.Robot.S01E02.720p.HDTV.x264-KILLERS.mkv

4. 시스템의 문서 파일 중 "Darren Quick"가 작성한 문서는 무엇인가요? (파일명)

Magnet AXIOM 에서는 문서 전처리를 통하여 제목, 작성자를 색인한다. 이러한 정보를 바탕으로 Magnet Axiom 에 Darren Quick 를 검색한 결과, **C:₩Users₩Forensicator₩Documents₩Digital Investigation₩Dropbox analysis, Data remnants on user machines.pdf** 파일을 발견할 수 있었다.



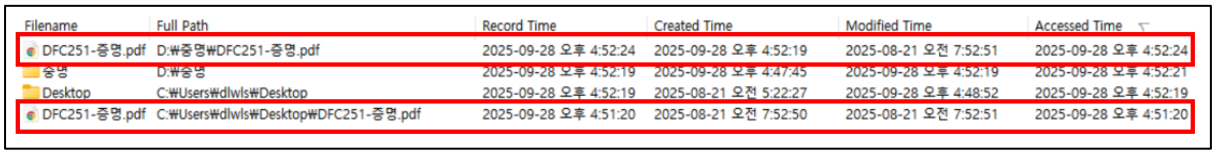
[그림 11] Magnet Axiom을 이용해 Darren Quick를 검색한 결과.

답: Dropbox analysis, Data remnants on user machines.pdf

5. 사용자는 특정 파일을 외장저장장치로 복사했습니다. 어떤 파일을 어떤 외장저장장치에 복사했나요? (복사한 시각, 복사한 파일명, 외장저장장치 제품명/모델명/시리얼번호) (50점)

우선 문제 풀이를 진행하기 전 파일을 외부 저장 장치에 복사하였을 때, 어떻게 기록이 남는지에 대해 검증을 진행해야한다. 하지만 결과적으로 복사한 흔적만으로 찾는 것은 실패했다. 하지만 문제에서 문서를 열람한 기록과 함께, 해당 파일의 생성된 시각, 수정된 시각, 액세스된 시각 3개를 이용한 분석을 통해 해당 기록을 찾을 수 있었다.

증명 과정은 다음과 같다. 파일의 이름은 DFC251-증명.pdf로 변경하고 진행했으며, 바탕화면에서 해당 문서를 열람한 후, 외부저장장치로 복사를 진행하고 다시 문서를 열람했다. 이를 JumpListsView를 통해 분석했으며 이는, [그림 12]와 같다.



Filename	Full Path	Record Time	Created Time	Modified Time	Accessed Time
DFC251-증명.pdf	D:₩증명₩DFC251-증명.pdf	2025-09-28 오후 4:52:24	2025-09-28 오후 4:52:19	2025-08-21 오전 7:52:51	2025-09-28 오후 4:52:24
증명	D:₩증명	2025-09-28 오후 4:52:19	2025-09-28 오후 4:47:45	2025-09-28 오후 4:52:19	2025-09-28 오후 4:52:21
Desktop	C:₩Users₩dlwls₩Desktop	2025-09-28 오후 4:52:19	2025-08-21 오전 5:22:27	2025-09-28 오후 4:48:52	2025-09-28 오후 4:52:19
DFC251-증명.pdf	C:₩Users₩dlwls₩Desktop₩DFC251-증명.pdf	2025-09-28 오후 4:51:20	2025-08-21 오전 7:52:50	2025-08-21 오전 7:52:51	2025-09-28 오후 4:51:20

[그림 12] JumpListsView로 분석한 DFC251-증명.pdf

확인한 결과, 수정한 시간(Modified Time)을 제외한 생성된 시각(Created Time)과 액세스된 시간(Accessed Time)이 최근 시간으로 변경된 것을 확인할 수 있다. 이를 정리하면, [표 4]와 같이 정리할 수 있다. 이를 통해, **외부저장장치로 복사되었을 때, 수정된 시간은 복사전과 동일하지만, 생성된 시각과 액세스 시간은 변경된다는 것을 알 수 있다.**

항목	바탕화면	외부저장장치
Created Time (UTC+9)	2025-08-21 오전 7:52:50	2025-09-28 오후 4:52:19
Modified Time (UTC+9)	2025-08-21 오전 7:52:50	2025-08-21 오전 7:52:51
Accessed Time (UTC+9)	2025-09-28 오후 4:51:20	2025-09-28 오후 4:52:24

[표 4] 검증 파일의 생성, 수정, 액세스 시간 정리.

외장장치에 복사된 파일임을 증명하기 위해서는 다음과 같은 조건에 일치해야한다.

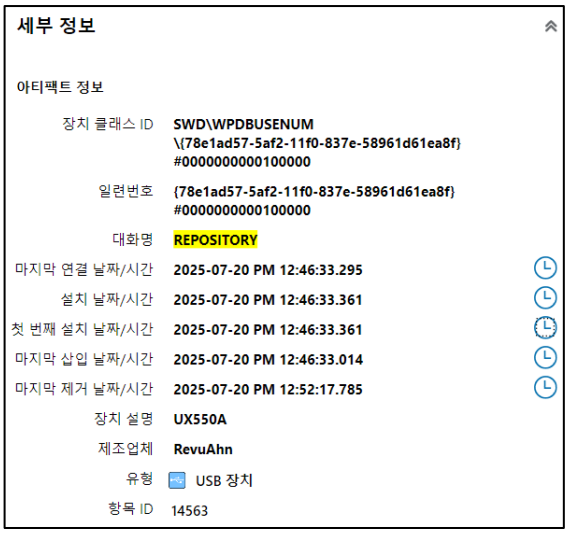
1. 연결된 경로가 C:₩가 아닐 것.
2. 드라이브 유형이 DRIVE_REMOVABLE일 것.
3. 복사대상 파일이 복사된 파일 보다 생성된 시간이 늦을 것. (복사된 파일의 생성된 시각이 최근일 것.)
4. 파일의 시간 순서가 수정된 시간 -> 생성된 시간, 액세스된 시간일 것.
5. 타임스탬프의 시간 순서는 수정된 시간 -> 생성된 시간, 액세스된 시간일 것.

위의 규칙을 통해 3개의 파일을 후보로써 판단할 수 있으며, 이는 [표 5]와 같다.

파일 경로
G:₩#AXWF₩Reference₩XWFQuickStart.pdf
F:₩NAS₩DFC_NAS_01.pdf
F:₩NAS₩DFC_NAS_03.pdf

[표 5] 4개의 조건이 모두 맞은 파일 정리.

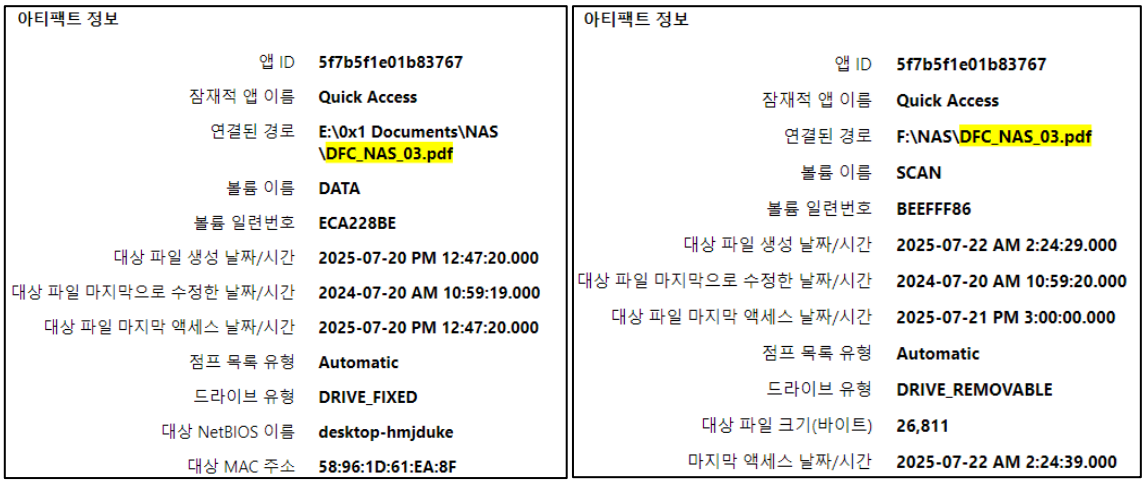
이 중 소거법을 이용하여 정답을 찾을 수 있다. 일단 XWFQuickStart.pdf은 정답이 될 수 없다. [그림 13]은 해당 파일의 Jumplist 아티팩트의 정보이다. 이 중 볼륨 이름은 REPOSITORY인 것을 확인할 수 있다. 이를 확인하면 **해당 파일의 복사된 시점은 2025년 5월 26일로 추정할 수 있다.** 하지만, [그림 14]의 동일한 이름을 가진, USB를 분석하면 **최초 연결 날짜는 2025년 7월 20일**로 확인할 수 있으며, 이는 해당 USB로 복사될 수 없다. **이를 통해 USB 정보를 확인할 수 없음으로, 해당 파일은 문제의 정답이 될 수 없다.**



[그림 13] (좌)XWFQuickStart.pdf의 Jumplist 정보.

[그림 14] (우)REPOSITORY의 대화명을 가진 USB 장치 정보.

NAS₩DFC_NAS_03.pdf 또한 정답이 될 수 없다. 이 또한 jumplist를 통해 증명할 수 있다. 해당 파일의 jumplist를 확인하면, [그림 15]와 같이, E:₩드라이브에서 열람한 내용을 확인할 수 있다. 해당 파일의 수정된 시각이 2024년 7월 20일 10시 59분임을 확인했을 때, 이는 동일한 파일을 복사한 것으로 확인할 수 있다. E: 볼륨이 DRIVE_FIXED지만, 시스템 볼륨(C:)이 아닌, 설치된 볼륨이라는 점으로 이는 정답이 아님을 시사한다.



아티팩트 정보

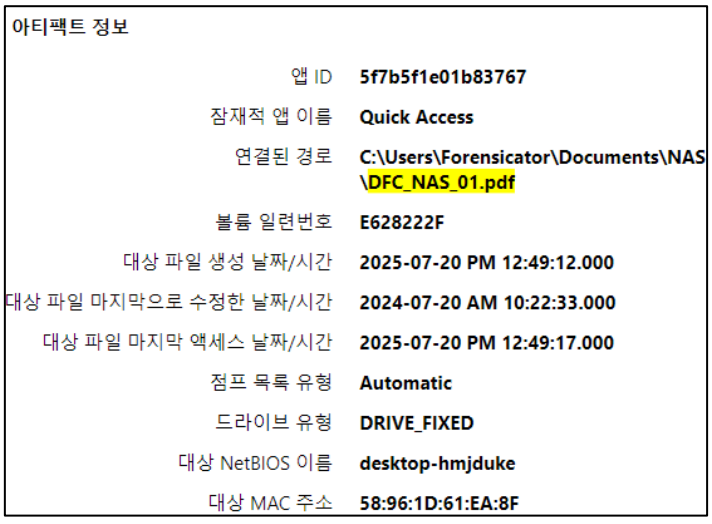
앱 ID	5f7b5f1e01b83767
잠재적 앱 이름	Quick Access
연결된 경로	E:\0x1 Documents\NAS\DFC_NAS_03.pdf
볼륨 이름	DATA
볼륨 일련번호	ECA228BE
대상 파일 생성 날짜/시간	2025-07-20 PM 12:47:20.000
대상 파일 마지막으로 수정한 날짜/시간	2024-07-20 AM 10:59:19.000
대상 파일 마지막 액세스 날짜/시간	2025-07-20 PM 12:47:20.000
점프 목록 유형	Automatic
드라이브 유형	DRIVE_FIXED
대상 NetBIOS 이름	desktop-hmjduke
대상 MAC 주소	58:96:1D:61:EA:8F

아티팩트 정보

앱 ID	5f7b5f1e01b83767
잠재적 앱 이름	Quick Access
연결된 경로	F:\NAS\DFC_NAS_03.pdf
볼륨 이름	SCAN
볼륨 일련번호	BEEFFF86
대상 파일 생성 날짜/시간	2025-07-22 AM 2:24:29.000
대상 파일 마지막으로 수정한 날짜/시간	2024-07-20 AM 10:59:20.000
대상 파일 마지막 액세스 날짜/시간	2025-07-21 PM 3:00:00.000
점프 목록 유형	Automatic
드라이브 유형	DRIVE_REMOVABLE
대상 파일 크기(바이트)	26,811
마지막 액세스 날짜/시간	2025-07-22 AM 2:24:39.000

[그림 15] (좌) DFC_NAS_03.pdf의 복사 대상 파일.
[그림 16] (우) DFC_NAS_03.pdf의 복사된 파일.

NAS₩DFC_NAS_01.pdf의 jumplist를 확인하면, 시스템 드라이브인 C: 볼륨에 위치한 파일임을 알 수 있다. 해당 파일의 수정된 시간은 2024년 7월 20일이다.

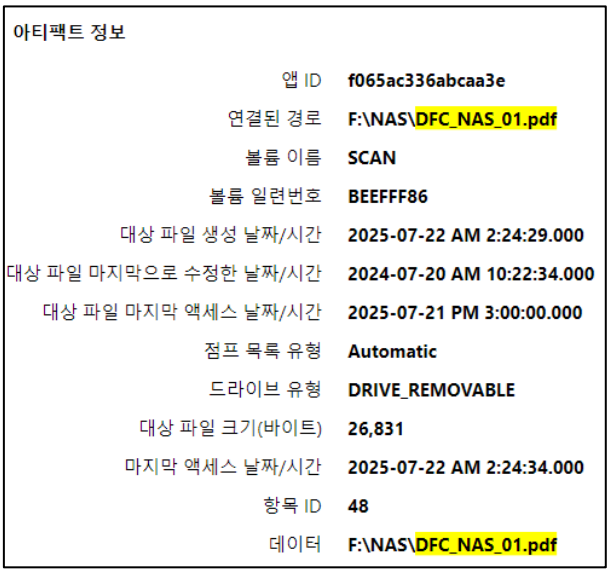


아티팩트 정보

앱 ID	5f7b5f1e01b83767
잠재적 앱 이름	Quick Access
연결된 경로	C:\Users\Forensicator\Documents\NAS\DFC_NAS_01.pdf
볼륨 일련번호	E628222F
대상 파일 생성 날짜/시간	2025-07-20 PM 12:49:12.000
대상 파일 마지막으로 수정한 날짜/시간	2024-07-20 AM 10:22:33.000
대상 파일 마지막 액세스 날짜/시간	2025-07-20 PM 12:49:17.000
점프 목록 유형	Automatic
드라이브 유형	DRIVE_FIXED
대상 NetBIOS 이름	desktop-hmjduke
대상 MAC 주소	58:96:1D:61:EA:8F

[그림 17] 시스템 드라이브의 DFC_NAS_01.pdf jumplist.

이 후 복사된 DFC_NAS_01.pdf를 분석한 결과, 시스템 드라이브의 DFC_NAS_01.pdf와 수정된 시간이 2024년 7월 20일로 동일하다는 것을 근거로 이는 같은 파일임을 알 수 있고, 복사된 파일임을 알 수 있다. 또한 2025년 7월 22일에 생성된 것으로, 이는 2025-07-22 AM 2:24:29(UTC)에 복사됨을 시사한다.



아티팩트 정보

앱 ID	f065ac336abcaa3e
연결된 경로	F:\NAS\DFC_NAS_01.pdf
볼륨 이름	SCAN
볼륨 일련번호	BEEFFF86
대상 파일 생성 날짜/시간	2025-07-22 AM 2:24:29.000
대상 파일 마지막으로 수정한 날짜/시간	2024-07-20 AM 10:22:34.000
대상 파일 마지막 액세스 날짜/시간	2025-07-21 PM 3:00:00.000
점프 목록 유형	Automatic
드라이브 유형	DRIVE_REMOVABLE
대상 파일 크기(바이트)	26,831
마지막 액세스 날짜/시간	2025-07-22 AM 2:24:34.000
항목 ID	48
데이터	F:\NAS\DFC_NAS_01.pdf

[그림 18] F:₩NAS₩DFC_NAS_01.pdf의 jumplist

이러한 파일 메타데이터 정보를 바탕으로 앞서 분석한 USB 장치 연결 이력을 검증한 결과, 파일 복사 직전 sandisk의 USB가 연결되었음을 알 수 있으며 해당 장치를 통해 파일을 복사하였다.

아티팩트 정보

이벤트 ID	1006
생성한 날짜/시간	2025-07-22 AM 2:23:45.124
이벤트 레코드 ID	23
이벤트 설명 요약	Storage Device SanDisk Cruzer Blade Connected.
작업	Connected
총 용량(바이트)	7761035264
제조업체	SanDisk
모델	Cruzer Blade
일련번호	4C530001180715107241
상위 ID	USB\VID_0781&PID_5567\4C530001180715107241
이벤트 데이터	<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event"><System><Provider Name="Microsoft-Windows-Partition" Guid="412bdff2-a8c4-470d-8f33-63fe0d8c20e2" /><EventID>1006</EventID><Version>6</Version><Level>4</Level><Task>0</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated

[그림 19] 복사전에 연결된 SanDisk의 Cruzer Blade 모델 이벤트 로그.

앞서 분석한 내용을 토대로 정답을 정리하면 [표 6]과 같이 정리할 수 있다.

복사된 파일 정보	
복사한 시각 (UTC)	2025-07-22 02:24:29
복사한 파일명	DFC_NAS_01.pdf
외장저장장치 정보	
제품명	SanDisk Cruzer Blade
모델명	Cruzer Blade
시리얼번호	4C530001180715107241

[표 6] 5번 정답 정리.

6. 시스템에 연결한 프린터 모델명과 어떤 문서를 프린터로 출력했는지 식별하세요. (프린터 모델명, 출력시각, 문서의 전체경로) (50점)

이벤트 ID 307을 통해 해당 시스템에서 프린트를 진행한 로그를 발견할 수 있었다. 이는 총 2건으로 2개의 파일을 프린트 했다는 것을 알 수 있다.

이벤...	이벤...	보안 식별자
307		S-1-5-21-908469853-595091727-484439149-10...
307		S-1-5-21-908469853-595091727-484439149-10...

[그림 20] AXIOM의 이벤트 ID 필터링을 통해 확인한 이벤트 ID 307의 수.

307번 이벤트로그에는 [그림 21]과 같이 총 8개의 파라미터가 존재한다. 이는 Eventlog Explorer의 제작사 블로그[1]를 통해 알 수 있다.

```
<Param1>2</Param1>
<Param2>문서 인쇄</Param2>
<Param3>Forensicator</Param3>
<Param4>\\DESKTOP-HMJDUKE</Param4>
<Param5>Canon iR C3125</Param5>
<Param6>WSD-745829f7-0b30-45d4-bf28-47b042cfbfca</
Param6>
<Param7>602580</Param7>
<Param8>2</Param8>
```

[그림 21] 이벤트 ID 307번 이벤트로그의 일부.

[1] https://eventlogxp.com/blog/how-to-track-printer-usage-with-event-logs/

해당 블로그의 내용을 통해 [그림 21]을 해석하면 [표 7]과 같이 정리할 수 있다.

Param	값	설명 및 해석
1	2	인쇄 작업 설명자
2	문서 인쇄	문서 이름(이벤트 로그에 작업 이름 허용" 정책을 활성화하지 않은 경우 문서 이름은 "문서 인쇄"가 된다.)
3	Forensicator	문서의 소유자
4	₩₩DESKTOP-HMJDUKE	문서를 전송한 컴퓨터
5	Canon iR C3125	프린터의 이름
6	WSD-745829f7-0b30-45d4-bf28-47b042cfbfca	인쇄 서버 포트 이름
7	602580	인쇄 서버로 전송된 문서 크기(바이트)
8	2	인쇄 작업으로 인쇄된 총 페이지 수

[표 7] 이벤트 ID 307번의 파라미터 정리.

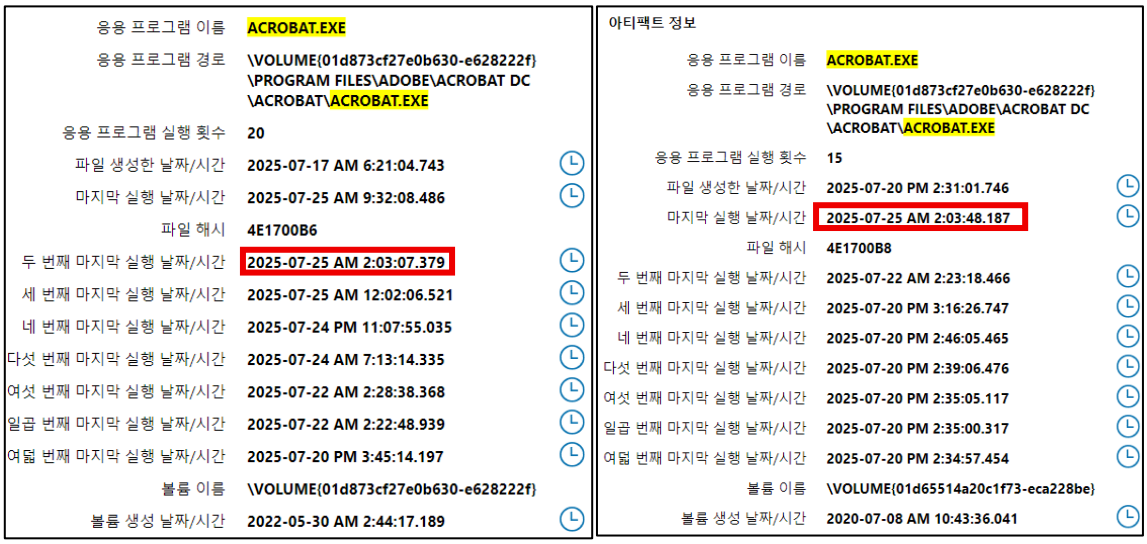
이러한 정보를 바탕으로 2번의 출력을 정리하면 [표 8]과 같이 정리할 수 있다.

이름	첫번째 출력	두번째 출력
이벤트 시간(UTC+0)	2025-07-25 AM 2:03:24.261	2025-07-25 AM 2:04:20.710
인쇄 작업 설명자	2	3
문서의 소유자	Forensicator	Forensicator
프린터 이름	Canon iR C3125	Canon iR C3125
문서의 크기(byte)	3543678	602580
인쇄된 페이지	2	10

[표 8] 프린터된 문서 정리.

이를 통해 총 2건의 문서가 출력되었다는 점이 교차검증 되었고, 프린터는 **Canon iR C3125**를 통해 출력했다는 것을 알 수 있다.

프린트로 출력하기 위한 프로그램의 기록을 찾던 중, Prefetch 분석을 통해 Adobe Acrobat의 실행 시점을 확인할 수 있었다. ACROBAT.EXE (4E1700B6)는 2025-07-25 AM 2:03:07.379에 실행되었고, ACROBAT.EXE(4E1700B8)는 2025-07-25 AM 2:03:48.187에 실행되었다. 이는 프린터 출력 시간과 비슷한 시간의 패턴을 보인다.



응용 프로그램 이름	ACROBAT.EXE
응용 프로그램 경로	\VOLUME{01d873cf27e0b630-e628222f} \PROGRAM FILES\ADOBE\ACROBAT DC \ACROBAT\ACROBAT.EXE
응용 프로그램 실행 횟수	20
파일 생성한 날짜/시간	2025-07-17 AM 6:21:04.743
마지막 실행 날짜/시간	2025-07-25 AM 9:32:08.486
파일 해시	4E1700B6
두 번째 마지막 실행 날짜/시간	2025-07-25 AM 2:03:07.379
세 번째 마지막 실행 날짜/시간	2025-07-25 AM 12:02:06.521
네 번째 마지막 실행 날짜/시간	2025-07-24 PM 11:07:55.035
다섯 번째 마지막 실행 날짜/시간	2025-07-24 AM 7:13:14.335
여섯 번째 마지막 실행 날짜/시간	2025-07-22 AM 2:28:38.368
일곱 번째 마지막 실행 날짜/시간	2025-07-22 AM 2:22:48.939
여덟 번째 마지막 실행 날짜/시간	2025-07-20 PM 3:45:14.197
볼륨 이름	\VOLUME{01d873cf27e0b630-e628222f}
볼륨 생성 날짜/시간	2022-05-30 AM 2:44:17.189

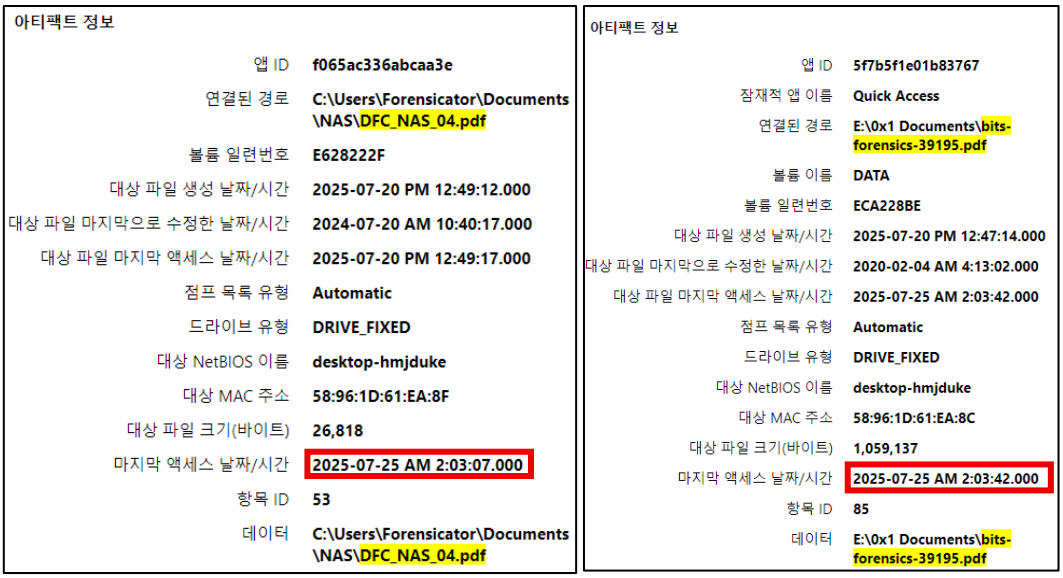
아티팩트 정보

응용 프로그램 이름	ACROBAT.EXE
응용 프로그램 경로	\VOLUME{01d873cf27e0b630-e628222f} \PROGRAM FILES\ADOBE\ACROBAT DC \ACROBAT\ACROBAT.EXE
응용 프로그램 실행 횟수	15
파일 생성한 날짜/시간	2025-07-20 PM 2:31:01.746
마지막 실행 날짜/시간	2025-07-25 AM 2:03:48.187
파일 해시	4E1700B8
두 번째 마지막 실행 날짜/시간	2025-07-22 AM 2:23:18.466
세 번째 마지막 실행 날짜/시간	2025-07-20 PM 3:16:26.747
네 번째 마지막 실행 날짜/시간	2025-07-20 PM 2:46:05.465
다섯 번째 마지막 실행 날짜/시간	2025-07-20 PM 2:39:06.476
여섯 번째 마지막 실행 날짜/시간	2025-07-20 PM 2:35:05.117
일곱 번째 마지막 실행 날짜/시간	2025-07-20 PM 2:35:00.317
여덟 번째 마지막 실행 날짜/시간	2025-07-20 PM 2:34:57.454
볼륨 이름	\VOLUME{01d65514a20c1f73-eca228be}
볼륨 생성 날짜/시간	2020-07-08 AM 10:43:36.041

[그림 22] (좌)프리패치를 통해 확인한 ACROBAT.exe(4E1700B6)

[그림 23] (우)프리패치를 통해 확인한 ACROBAT.exe(4E1700B8)

점프 목록(Jump List) 분석 결과 두 개의 PDF 파일이 프린터 출력 직전에 접근되었음을 확인했다. DFC_NAS_04.pdf는 2025-07-25 AM 2:03:07에 접근되었고, bits-forensics-39195.pdf는 2025-07-25 AM 2:03:42에 접근되었다. 이러한 시간 순서는 **Adobe Acrobat 실행 → 파일 접근 → 프린터 작업 생성**의 논리적 흐름을 보여준다.



아티팩트 정보

앱 ID	f065ac336abcaa3e
연결된 경로	C:\Users\Forensicator\Documents \NAS\DFC_NAS_04.pdf
볼륨 일련번호	E628222F
대상 파일 생성 날짜/시간	2025-07-20 PM 12:49:12.000
대상 파일 마지막으로 수정한 날짜/시간	2024-07-20 AM 10:40:17.000
대상 파일 마지막 액세스 날짜/시간	2025-07-20 PM 12:49:17.000
점프 목록 유형	Automatic
드라이브 유형	DRIVE_FIXED
대상 NetBIOS 이름	desktop-hmjduke
대상 MAC 주소	58:96:1D:61:EA:8F
대상 파일 크기(바이트)	26,818
마지막 액세스 날짜/시간	2025-07-25 AM 2:03:07.000
항목 ID	53
데이터	C:\Users\Forensicator\Documents \NAS\DFC_NAS_04.pdf

아티팩트 정보

앱 ID	5f7b5f1e01b83767
잠재적 앱 이름	Quick Access
연결된 경로	E:\0x1 Documents\bits-forensics-39195.pdf
볼륨 이름	DATA
볼륨 일련번호	ECA228BE
대상 파일 생성 날짜/시간	2025-07-20 PM 12:47:14.000
대상 파일 마지막으로 수정한 날짜/시간	2020-02-04 AM 4:13:02.000
대상 파일 마지막 액세스 날짜/시간	2025-07-25 AM 2:03:42.000
점프 목록 유형	Automatic
드라이브 유형	DRIVE_FIXED
대상 NetBIOS 이름	desktop-hmjduke
대상 MAC 주소	58:96:1D:61:EA:8C
대상 파일 크기(바이트)	1,059,137
마지막 액세스 날짜/시간	2025-07-25 AM 2:03:42.000
항목 ID	85
데이터	E:\0x1 Documents\bits-forensics-39195.pdf

[그림 23] (좌) DFC_NAS_04.pdf의 접근 시간.

[그림 23] (우) bits-forensics-39195.pdf의 접근 시간.

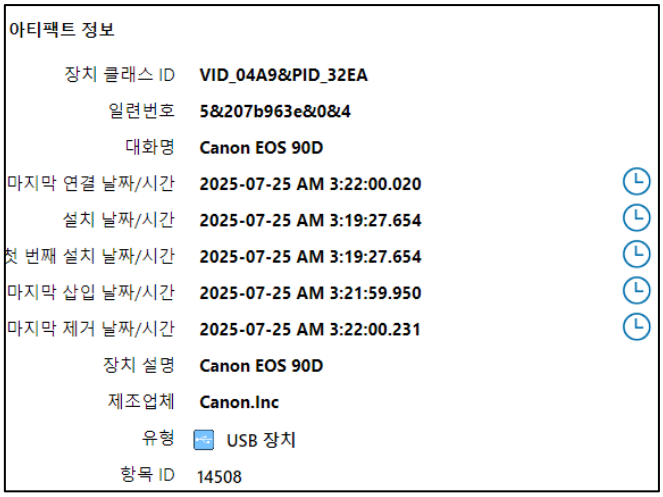
분석 결과를 종합하면 다음과 같이 정리할 수 있다.

구분	첫 번째 출력	두 번째 출력
이벤트 시간(UTC+0)	2025-07-25 AM 2:03:24.261	2025-07-25 AM 2:04:20.710
문서 전체 경로	C:₩Users₩Forensicator₩Documents ₩NAS₩DFC_NAS_04.pdf	E:₩0x1 Documents₩bits-forensics-39195.pdf
문서 크기(byte)	3,543,678	602,580
인쇄된 페이지	2	10
Adobe Acrobat 실행 시간	2025-07-25 AM 2:03:07.379	2025-07-25 AM 2:03:48.187
점프 목록 접근 시간	2025-07-25 AM 2:03:07	2025-07-25 AM 2:03:42

[표 8] 분석 결과 요약 및 6번의 답.

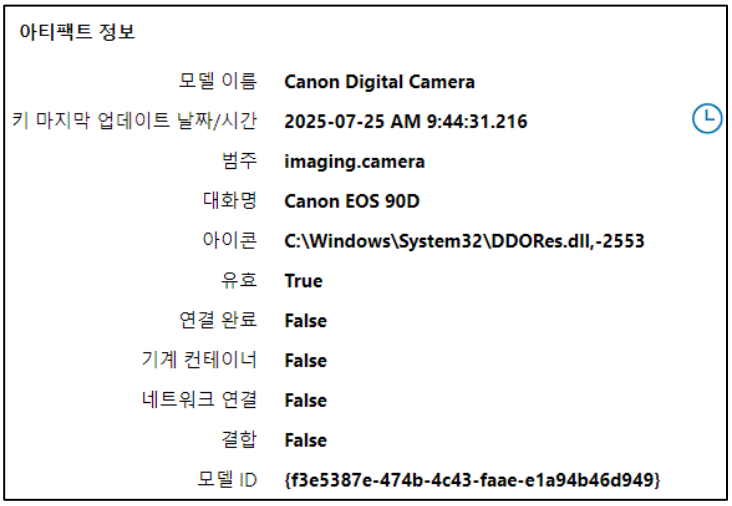
7. 시스템에 연결한 디지털 카메라 모델명과 연결/해제 시작을 식별하세요. (모델명, 연결/해제 시각)

시스템에 연결된 디지털 카메라의 모델명과 연결/해제 시각을 식별하기 위해 USB 장치 레지스트리와 관련 이벤트 로그를 분석했다. Windows는 USB 장치가 연결될 때마다 상세한 로그를 남기기 때문이다. USB 장치 분석 결과 VID_04A9&PID_32EA로 식별되는 Canon EOS 90D가 시스템에 연결되었음을 확인할 수 있었다. VID(Vendor ID) 04A9는 Canon Inc.의 고유식별자이고, PID(Product ID) 32EA는 EOS 90D 모델을 나타낸다.



[그림 24] USB연결 기록에서 확인한 Canon EOS 90D의 로그.

AmCache 장치 컨테이너 분석을 통해 "Canon Digital Camera"로 분류된 장치가 "Canon EOS 90D"로 정확히 식별되었음을 확인했다. 이는 2025-07-25 AM 9:44:31.216에 마지막으로 업데이트 되었다.



[그림 24] AmCache에서 확인한 디지털 카메라 장치 컨테이너 정보.

Windows 이벤트 로그의 애플리케이션 경험 이벤트에서 Canon EOS 90D와 관련된 이벤트들이 2025-07-25 AM 3:19~3:22 시간대에 집중적으로 발생했음을 확인할 수 있었다. 이는 카메라 연결 및 인식 과정에서 발생하는 정상적인 패턴이다. 이를 정리하면, [표 9]와 같다. 이는 [그림 24]의 설치 시간과 연결 해제 시간을 교차검증하는 과정이다.

구분	시각(UTC+0) 2025-07-25	이벤트 ID	설명
장치 인식 시작	03:19:27.146	430	USB 장치 최초 인식 및 드라이버 로딩 시작
장치 연결 완료	03:21:59.737	1010	Canon EOS 90D 연결 완료 및 사용 가능 상태
장치 연결 해제	03:22:00.233	1010	Canon EOS 90D 연결 해제

[표 9] 이벤트 로그에서 확인한 Canon EOS 90D의 연결 및 해제 로그 정리.

답:

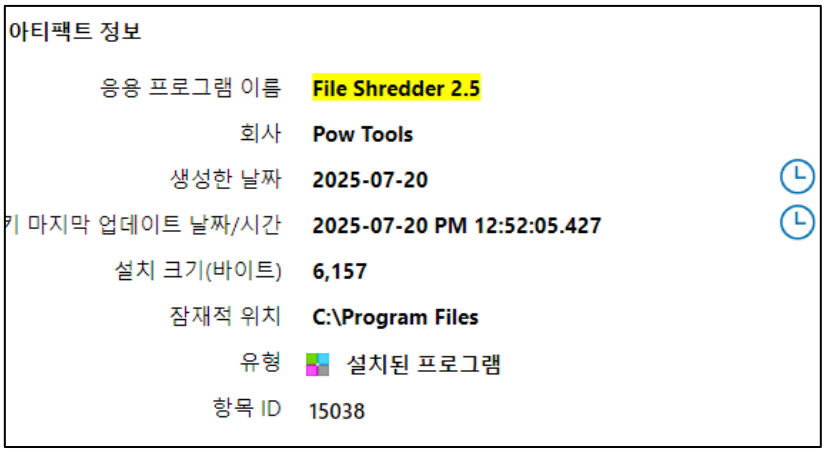
모델명: Canon EOS 90D

연결 시각: 2025-07-25 03:19:27

해제 시각: 2025-07-25 03:22:00

8. 시스템에 설치된 완전삭제 도구는 무엇인가요? (설치시각, 도구명)

설치된 프로그램 목록에서 [그림 24]와 같이, File Shredder 2.5[2]를 발견할 수 있었다. 이는 무료로 배포되고 있는 완전 삭제 도구이다.



[그림 24] 설치된 프로그램에서 발견된 File Shredder 2.5

9. 사용자는 설치된 완전 삭제 도구로 언제, 어떤 파일을 완전삭제했나요 ? (삭제한 시각, 파일명)

NTFS Log Tracker을 사용하여 사용자는 2025-07-25 11:44:50 (UTC+0) 시각에 SHRDDER.exe를 실행시킨 것을 생성된 프리패치(.pf)파일을 를 통해 확인할 수 있다.

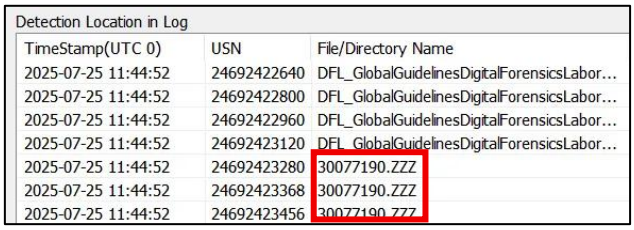
Detection Location in Log

TimeStamp(UTC 0)	USN	File/Directory Name
2025-07-25 11:44:50	24692421248	SMARTSCREEN.EXE-3A39E32D.pf
2025-07-25 11:44:50	24692421368	SMARTSCREEN.EXE-3A39E32D.pf
2025-07-25 11:44:50	24692421488	SHREDDER.EXE-F6B92EA2.pf
2025-07-25 11:44:50	24692421600	SHREDDER.EXE-F6B92EA2.pf
2025-07-25 11:44:50	24692421712	SHREDDER.EXE-F6B92EA2.pf
2025-07-25 11:44:50	24692421824	000072.log
2025-07-25 11:44:50	24692421904	000072.log

[그림 25] SHREDDER.EXE의 프리패치 생성 시각.

[2] https://www.fileshredder.org/index.php

또한 30077190.ZZZ 파일과 함께 DFL_GlobalGuidelinesDigitalForensicsLaboratory.pdf파일을 확인할 수 있다. 이를 통해 해당 파일이 삭제되었음을 시사한다.



Detection Location in Log

TimeStamp(UTC 0)	USN	File/Directory Name
2025-07-25 11:44:52	24692422640	DFL_GlobalGuidelinesDigitalForensicsLabor...
2025-07-25 11:44:52	24692422800	DFL_GlobalGuidelinesDigitalForensicsLabor...
2025-07-25 11:44:52	24692422960	DFL_GlobalGuidelinesDigitalForensicsLabor...
2025-07-25 11:44:52	24692423120	DFL_GlobalGuidelinesDigitalForensicsLabor...
2025-07-25 11:44:52	24692423280	30077190.ZZZ
2025-07-25 11:44:52	24692423368	30077190.ZZZ
2025-07-25 11:44:52	24692423456	30077190.ZZZ

[그림 25] 30077190.ZZZ 파일과 pdf파일.

이 후 [표 10]과 같이, DFL_GlobalGuidelinesDigitalForensicsLaboratory.pdf 파일이 와이핑 되는 것을 다음 과정과 같이 확인할 수 있다. DFL_GlobalGuidelinesDigitalForensicsLaboratory.pdf 이 30077190.ZZZ 로 이름이 바뀌고 삭제되는 것을 확인할 수 있다.

USN	TimeStamp (UTC+0)	Filename	Event
24692396856	2025-07-25 11:44:52	DFL_GlobalGuidelinesDigitalForensicsLaboratory.pdf	File_Created
24692397016	2025-07-25 11:44:52	DFL_GlobalGuidelinesDigitalForensicsLaboratory.pdf	File_Created / Data_Added
24692397176	2025-07-25 11:44:52	DFL_GlobalGuidelinesDigitalForensicsLaboratory.pdf	File_Created / Data_Added / Data_Overwritten
24692397336	2025-07-25 11:44:52	DFL_GlobalGuidelinesDigitalForensicsLaboratory.pdf	File_Created / Data_Added / Data_Overwritten / Named_Stream_Changed
24692397336	2025-07-25 11:44:52	DFL_GlobalGuidelinesDigitalForensicsLaboratory.pdf	File_Created / Data_Added / Data_Overwritten / Named_Data_Stream_Added / Named_Stream_Changed
24692397656	2025-07-25 11:44:52	DFL_GlobalGuidelinesDigitalForensicsLaboratory.pdf	File_Created / Data_Added / Data_Overwritten / Named_Data_Stream_Added / Named_Data_Stream_Overwritten / Named_Stream_Changed
24692397816	2025-07-25 11:44:52	DFL_GlobalGuidelinesDigitalForensicsLaboratory.pdf	File_Created / Basic_Info_Changed / Data_Added / Data_Overwritten / Named_Data_Stream_Added / Named_Data_Stream_Overwritten / Named_Stream_Changed
24692397976	2025-07-25	DFL_GlobalGuidelinesDigitalForensicsLab	File_Created /

	11:44:52	oratory.pdf	Basic_Info_Changed / Data_Added / Data_Overwritten / Named_Data_Stream_Added / Named_Data_Stream_Overwritten / Named_Stream_Changed / File_Closed
24692422640	2025-07-25 11:44:52	DFL_GlobalGuidelinesDigitalForensicsLaboratory.pdf	Data_Overwritten
24692422800	2025-07-25 11:44:52	DFL_GlobalGuidelinesDigitalForensicsLaboratory.pdf	Data_Overwritten / Data_Truncated
24692422960	2025-07-25 11:44:52	DFL_GlobalGuidelinesDigitalForensicsLaboratory.pdf	Data_Overwritten / Data_Truncated / File_Closed
24692423120	2025-07-25 11:44:52	DFL_GlobalGuidelinesDigitalForensicsLaboratory.pdf	File_Renamed_Old
24692423280	2025-07-25 11:44:52	30077190.ZZZ	File_Renamed_New
24692423368	2025-07-25 11:44:52	30077190.ZZZ	File_Renamed_New / File_Closed
24692423456	2025-07-25 11:44:52	30077190.ZZZ	File_Closed / File_Deleted

[표 10] DFL_GlobalGuidelinesDigitalForensicsLaboratory.pdf의 삭제 과정.

답:

삭제한 시각: 2025-07-25 11:44:32

파일명: DFL_GlobalGuidelinesDigitalForensicsLaboratory.pdf