

## 201 – Log and Found

### Team Information

**Team Name:** kimbabasaksaksak

**Team Member:** Jaeheon Kim, Donghyun Kim, Soyoung Yoo, Minhee Lee

**Email Address :** uaaoong@gmail.com

### Instructions

**Description** Kate is a server administrator at a fashion design company and recently underwent an internal audit within the company due to an incident where design files stored on the server were leaked. The company has requested a digital forensics analysis of the server's volume to resolve this issue. Please provide the analysis results for each question.

Target	Hash (MD5)
draft_server.001	4e6354ddcf52c2f0e436c60f2c5878ac

### Questions

- 1) List the original and changed file names of the renamed files. (50 points)
- 2) List the file names of the deleted files. (50 points)
- 3) Provide the deleted time for each file. (100 points)

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:	R-STUDIO Technician	Publisher:	R-Tools Technology
Version:	9.2.191153		
URL:	www.r-studio.com		

Name:	Vmware Workstation	Publisher:	Vmware
Version:	16.2.5 build-20904516 Pro		
URL:	www.vmware.com/kr.html		

Name:	Windows Server 2022 ISO	Publisher:	Microsoft
Version:			
URL:	www.microsoft.com/ko-kr/evalcenter/download-windows-server-2022		

Name:	010 Editor	Publisher:	SweetScape Software
Version:	13.0.2		
URL:	www.sweetscape.com		

## Step-by-step methodology:

### ※ Additional information

#### - 참고자료

DFRWS APAC 2021 Author Preprint: Forensic Analysis of ReFS Journaling

#### - 테스트 환경

ReFS 파일시스템에서 파일 생성, 파일 이름 변경, 파일 삭제 이벤트 발생 시 \$Logfile에 기록되는 데이터를 확보하기 위하여, Vmware에 Windows Server 2022를 설치하여 테스트를 진행했다. Windows Server 2022에서 1GB VHD 파일을 생성 후, ReFS 파일시스템으로 포맷하여 VHD 내에서 이벤트를 발생시켰다. 각 이벤트 별로 생성된 \$Logfile 레코드들을 추출하여 본 문제에서 주어진 레코드들과 비교 분석하는데 사용하였다.

**Q1.** List the original and changed file names of the renamed files. (50 points)

ReFS 파일시스템 테스트 환경을 구축하여 파일 생성 및 파일 이름 변경 이벤트를 발생시킨 후, \$Logfile을 분석하였다. 그 결과, 파일 이름이 변경되면, 변경전 파일 이름과 변경후 파일 이름이 하나의 Logfile Entry 내에 기록되는 특징을 발견했다.

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
3:1150h	1F	00	00	00	00	00	00	00	17	00	00	00	00	00	00	00	.....(Rô..€ÿÿ
3:1160h	00	00	00	00	00	00	00	00	28	52	F4	17	0E	80	FF	FF	X.....x...
3:1170h	58	00	00	00	1C	00	00	00	78	00	00	00	20	00	00	00	0a..0.....
3:1180h	98	00	00	00	30	00	00	00	C8	00	00	00	14	00	00	00	변경전 파일 이름
3:1190h	30	E0	00	00	30	01	00	00	00	00	00	00	00	00	00	00	0...Ä.....0...
3:11A0h	00	00	00	00	00	06	00	00	00	00	00	00	00	00	00	00	1.0.0.1...j.p.g.
3:11B0h	30	01	00	00	C0	01	00	00	00	00	00	00	30	00	01	00	0a..0.....
3:11C0h	31	00	30	00	30	00	31	00	2E	00	6A	00	70	00	67	00	0...1.0.0.2...j
3:11D0h	01	00	00	00	08	00	00	00	10	00	00	00	1C	00	00	00	p.g.....
3:11E0h	30	E0	00	00	30	01	00	00	00	00	00	00	00	00	00	00	E.....8...
3:11F0h	00	00	00	00	00	06	00	00	00	00	00	00	00	00	00	00	@.....
3:1200h	30	00	01	00	31	00	30	00	30	00	32	00	2E	00	6A	00	.....(Rô..€ÿÿ
3:1210h	70	00	67	00	00	00	00	00	00	00	00	00	00	00	00	00	0a..0.....
3:1220h	C8	00	00	00	01	00	00	00	01	00	00	00	38	00	00	00	.....€...
3:1230h	04	00	00	00	40	00	00	00	1F	00	00	00	00	00	00	00	0...1.0.0.2...j
3:1240h	17	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	p.g.....
3:1250h	F0	52	F4	17	0E	80	FF	FF	60	00	00	00	1C	00	00	00	.....8.....H...
3:1260h	80	00	00	00	18	00	00	00	98	00	00	00	20	00	00	00	.....
3:1270h	B8	00	00	00	04	00	00	00	C0	00	00	00	04	00	00	00	.....x.....
3:1280h	30	E0	00	00	30	01	00	00	00	00	00	00	00	00	00	00	0a..0.....
3:1290h	00	00	00	00	00	06	00	00	00	00	00	00	00	00	00	00	.....
3:12A0h	20	00	00	80	00	00	00	00	03	00	00	00	00	00	00	00	0...Ä.....0...
3:12B0h	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	1.0.0.2...j
3:12C0h	0C	00	10	00	31	00	30	00	30	00	32	00	2E	00	6A	00	p.g.....
3:12D0h	70	00	67	00	00	00	00	00	00	00	00	00	00	00	00	00	.....8.....
3:12E0h	00	00	00	00	00	00	00	00	B0	00	00	00	04	00	00	00	.....H...
3:12F0h	02	00	00	00	38	00	00	00	02	00	00	00	48	00	00	00	.....
3:1300h	1F	00	00	00	00	00	00	00	17	00	00	00	00	00	00	00	.....x.....
3:1310h	00	00	00	00	02	00	00	00	00	00	00	00	00	00	00	00	.....
3:1320h	58	00	00	00	1C	00	00	00	78	00	00	00	20	00	00	00	0a..0.....
3:1330h	98	00	00	00	02	00	00	00	A0	00	00	00	04	00	00	00	.....
3:1340h	30	E0	00	00	30	01	00	00	00	00	00	00	00	00	00	00	0...Ä.....0...
3:1350h	00	00	00	00	00	06	00	00	00	00	00	00	00	00	00	00	1.0.0.2...j.p.g.
3:1360h	30	01	00	00	C0	01	00	00	00	00	00	00	30	00	01	00	.....p.....
3:1370h	31	00	30	00	30	00	32	00	2E	00	6A	00	70	00	67	00	.....
3:1380h	01	00	00	00	00	00	00	00	70	00	00	00	00	00	00	00	.....
3:1390h	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
3:13A0h	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....

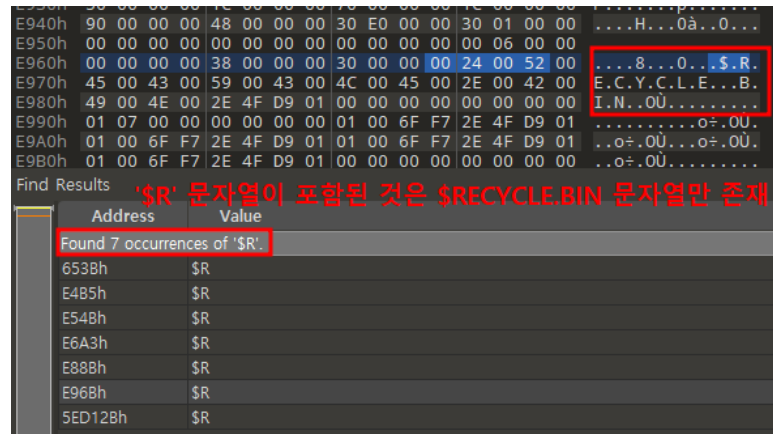
또한, 파일이 생성되고 추가 이벤트가 발생되지 않은 파일보다, 파일 이름 변경 이벤트가 발생한 파일이 \$Logfile에 더 많은 파일 이름이 기록되어 있다는 특징이 있다. R-STUDIO 도구로 문제에서 주어진 이미지 파일에서 \$Logfile 추출하여 분석한 결과, 파일이 생성되고 추가 이벤트가 발생하지 않은 파일은 \$Logfile에 파일 이름이 10번 등장한다는 특징을 발견했다. 또한, 파일 이름 변경 이벤트가 발생한 파일은 \$Logfile에 파일 이름이 11번 등장하는 특징을 발견했다.

앞서 언급한 특징들을 기반으로 \$Logfile을 분석하여 파일 이름 변경 이력을 추적하였다.

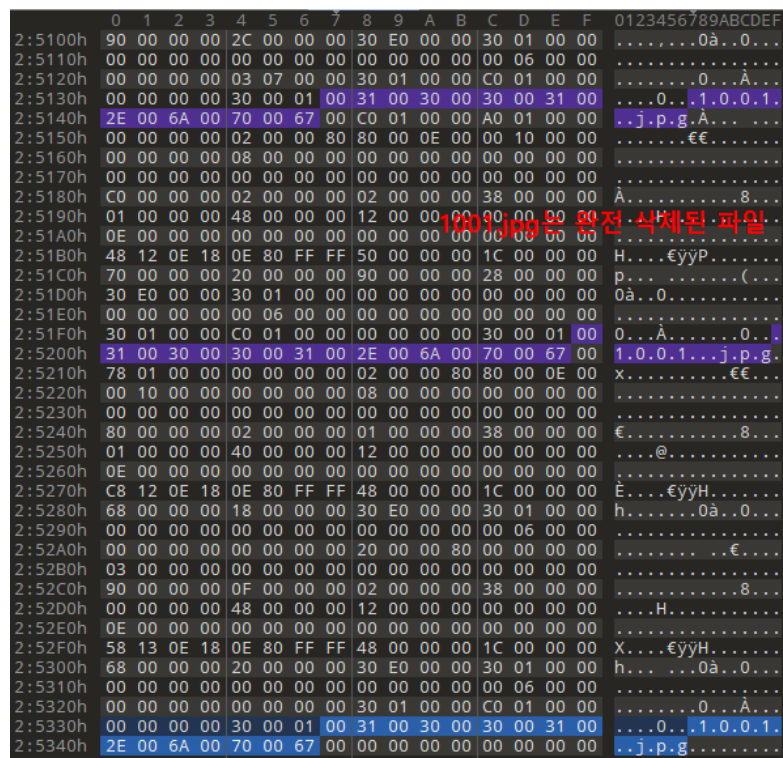
변경전 파일명	변경후 파일명
1008022_B.jpg	1008023_B.jpg
1012200_B.jpg	1012201_B.jpg
1012211_B.jpg	1012210_B.jpg
1012343_B.jpg	1012341_B.jpg
1012377_B.jpg	1012378_B.jpg
1013282_B.jpg	1013283_B.jpg
1014097_B.jpg	1014098_B.jpg
1014179_B.jpg	1014180_B.jpg
1014394_B.jpg	1014398_B.jpg
1015100_B.jpg	1015101_B.jpg

## Q2. List the file names of the deleted files. (50 points)

참고자료(Forensic Analysis of ReFS Journaling)를 확인하면, 파일 삭제는 휴지통으로 이동 후 삭제와 파일 완전 삭제로 구분해야 된다고 한다. 휴지통으로 이동 후 삭제되는 파일은 파일 이름이 \$R로 시작되는 파일 이름으로 변경된다. 하지만, 문제에서 주어진 \$Logfile에는 \$R로 시작되는 파일 이름으로 변경된 기록이 존재하지 않는다. 그러므로 삭제된 모든 파일들은 완전 삭제되었음을 알 수 있다.



테스트 환경에서 파일을 완전 삭제한 후 \$Logfile에 기록되는 패턴을 확인한 결과, 삭제된 파일과 관련된 Logfile Entry 중에서 가장 마지막에 생성된 Logfile Entry에는 파일 이름이 여러 번 기록되는 특징을 발견하였다.



또한, 문제에서 주어진 \$Logfile에서는 파일 완전 삭제 이벤트가 발생한 파일은 파일 이름이 14번 등장하는 특징을 발견했다.

앞서 언급한 특징들을 기반으로 \$Logfile을 분석하여 파일 삭제 이력을 추적하였다.

파일명	파일 삭제 유형
1008103_B.jpg	파일 완전 삭제
1012353_B.jpg	파일 완전 삭제
1013029_B.jpg	파일 완전 삭제
1013191_B.jpg	파일 완전 삭제
1014381_B.jpg	파일 완전 삭제

### Q3. Provide the deleted time for each file. (100 points)

테스트 환경에서 파일을 완전 삭제한 후 \$Logfile에 기록되는 데이터를 분석하여, 파일 삭제 시각이 기록되는 위치를 확인하였다. 파일 삭제 시각은 삭제된 파일 이름이 포함되어 있는 Logfile Entry 중에서 가장 마지막에 생성된 Logfile Entry의 바로 다음 Logfile Entry에 저장되어 있다.

```
3:6FF0h 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
3:7000h 4D 4C 6F 67 06 4F 8C 32 01 00 00 00 00 10 00 00 MLog.0E2.....
3:7010h FD 89 C9 0E 68 AC D2 45 BF 5D BC DB 3C 59 FF D1 y%E.h-0Ez]4U<YyN
3:7020h 02 00 00 00 00 00 00 00 37 00 00 00 01 00 00 00 .....7.....
3:7030h 36 00 00 00 01 00 00 00 01 00 00 00 01 00 00 00 6.....
3:7040h 00 00 00 00 0E 80 FF FF 90 02 00 00 00 00 00 00 .....ëyy.....
3:7050h D0 81 52 18 78 00 00 00 38 02 00 00 00 00 00 00 ð.R.x...8.....
3:7060h 09 00 00 00 00 00 00 00 18 00 00 00 01 00 00 00 .....
3:7070h 11 4A 00 EB 1A 9B D4 11 37 00 00 00 01 00 00 00 ..J.e..0.7.....
3:7080h C6 25 C4 88 00 00 00 00 00 00 00 01 00 00 06 00 Æ%A^.....
3:7090h 36 00 00 00 01 00 00 00 50 0F 00 00 00 00 00 00 6.....P.....
3:70A0h 38 00 00 00 88 0F 00 00 02 00 00 00 00 00 00 00 8.....^.....
3:70B0h 18 03 00 00 08 00 00 00 C8 00 00 00 0F 00 00 00 .....E.....
3:70C0h 03 00 00 00 38 00 00 00 00 00 00 00 50 00 00 00 .....8.....P...
3:70D0h 1C 00 00 00 00 00 00 00 18 00 00 00 00 00 00 00 .....
3:70E0h 00 00 00 00 01 20 00 00 88 51 52 18 0E 80 FF FF ..... ..QR..ëyy
3:70F0h 50 00 00 00 1C 00 00 00 70 00 00 00 20 00 00 00 P.....p.....
3:7100h 90 00 00 00 2C 00 00 00 30 E0 00 00 30 01 00 00 .....0ä..0...
3:7110h 00 00 00 00 00 00 00 00 00 00 00 00 00 06 00 00 .....0...Ä...
3:7120h 00 00 00 00 00 00 00 00 30 01 00 00 C0 01 00 00 .....0...1.0.0.3.
3:7130h 00 00 00 00 30 00 01 00 31 00 30 00 30 00 33 00 .....p.n.g.Ä...
3:7140h 2E 00 70 00 6E 00 67 00 C0 01 00 00 A0 01 00 00 .....ë.....
3:7150h 00 00 00 00 02 00 00 80 80 00 0E 00 00 10 00 00 .....
3:7160h 00 00 00 00 08 00 00 00 00 00 00 00 00 00 00 00 .....
3:7170h 00 00 00 00 08 00 00 00 00 00 00 00 00 00 00 00 .....
3:7180h 00 00 00 00 02 00 00 00 00 00 00 00 38 00 00 00 .....8...
3:7190h 01 00 00 00 48 00 00 00 1C 00 00 00 00 00 00 00 .....H...
3:71A0h 18 03 00 00 0E 80 FF FF 50 00 00 00 1C 00 00 00 .....
3:71B0h 48 52 52 18 0E 80 FF FF 50 00 00 00 1C 00 00 00 HBR ..ëyyP
3:71C0h 1C 00 00 00 30 01 00 00 00 00 00 00 00 00 00 00 p.....0ä..0...
3:71D0h 30 E0 00 00 30 01 00 00 00 00 00 00 00 00 00 00 0ä..0...
3:71E0h 00 00 00 00 00 06 00 00 00 00 00 00 08 00 00 00 .....
3:71F0h 30 01 00 00 C0 01 00 00 00 00 00 00 30 00 01 00 0...Ä.....0...
3:7200h 31 00 30 00 30 00 33 00 2E 00 70 00 6E 00 67 00 1.0.0.3...p.n.g.
3:7210h 78 01 00 00 00 00 00 00 02 00 00 80 80 00 0E 00 x.....ë.....
3:7220h 00 10 00 00 00 00 00 00 08 00 00 00 00 00 00 00 .....
3:7230h 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
```

삭제된 파일 이름이 포함되어 있는 Logfile Entry 중에서 가장 마지막에 생성된 Logfile Entry의 바로 다음 Logfile Entry에 저장되어 있다.

```
3:7FF0h 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
3:8000h 4D 4C 6F 67 06 4F 8C 32 01 00 00 00 00 10 00 00 MLog.0E2.....
3:8010h FD 89 C9 0E 68 AC D2 45 BF 5D BC DB 3C 59 FF D1 y%E.h-0Ez]4U<YyN
3:8020h 02 00 00 00 00 00 00 00 38 00 00 00 01 00 00 00 .....8.....
3:8030h 37 00 00 00 01 00 00 00 01 00 00 00 01 00 00 00 .....7.....
3:8040h 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....h5N0.....
3:8050h 00 00 00 00 78 00 00 00 00 00 00 00 00 00 00 00 .....x.....
3:8060h 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
3:8070h 00 00 00 00 00 00 00 00 38 00 00 00 01 00 00 00 .....8.....
3:8080h 8B 68 72 9D 00 00 00 00 00 00 00 00 00 00 00 00 <hr.....
3:8090h 37 00 00 00 01 00 00 00 50 0F 00 00 00 00 00 00 7.....P.....
3:80A0h 38 00 00 00 88 0F 00 00 02 00 00 00 00 00 00 00 8.....^.....
3:80B0h 00 01 00 00 08 00 00 00 00 01 00 00 04 00 00 00 .....
3:80C0h 02 00 00 00 38 00 00 00 01 00 00 00 48 00 00 00 .....8.....H...
3:80D0h 1C 00 00 00 00 00 00 00 18 00 00 00 00 00 00 00 .....
3:80E0h 00 00 00 00 03 20 00 00 00 00 00 00 00 00 00 00 .....
3:80F0h 50 00 00 00 1C 00 00 00 70 00 00 00 10 00 00 00 P.....p.....
3:8100h 80 00 00 00 74 00 00 00 30 E0 00 00 30 01 00 00 .....t...0ä..0...
3:8110h 00 00 00 00 00 00 00 00 00 00 00 00 00 06 00 00 .....0...ð...
3:8120h 00 00 00 00 00 00 00 00 30 01 00 00 D0 01 00 00 .....f*c|m~Ü.
3:8130h 00 00 00 00 10 00 00 00 66 2A 63 7C 6D 98 D9 01 .....
3:8140h 97 41 ED D3 6F 98 D9 01 97 41 ED D3 6F 98 D9 01 -Ai0o~Ü.-Ai0o~Ü.
3:8150h 97 41 ED D3 6F 98 D9 01 00 00 00 00 00 00 00 00 -Ai0o~Ü.....
3:8160h AC 74 C5 C1 01 00 00 00 00 00 00 00 00 00 00 00 -tAA.....
3:8170h 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
3:8180h 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
3:8190h 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
3:81A0h 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 .....
3:81B0h 48 02 7D 18 0E 80 FF FF 00 00 00 00 00 00 00 00 H.}.ëyy.....
3:81C0h 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
3:81D0h 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
3:81E0h 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
3:81F0h 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
3:8200h 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
3:8210h 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
```

앞서 언급한 내용들을 기반으로 \$Logfile을 분석하여 파일 삭제 시각을 추적하였다.

파일명	파일 삭제 시각 (UTC+0)
1008103_B.jpg	2023-04-05 11:09:13
1012353_B.jpg	2023-04-05 11:08:43
1013029_B.jpg	2023-04-05 11:09:38
1013191_B.jpg	2023-04-05 11:08:17
1014381_B.jpg	2023-04-05 11:10:06