[DFC-2023-201] Write-Up

작성자	박혜미
분석 일자	2024.06.01~2024.06.06
작성 일자	2024.06.07
분석 대상	draft_server.001
문서 버전	1.0
작성자 E-mail	parkm0708@naver.com

0. 목차

1. 문제 3
2. 분석 도구 3
3. 환경 3
4. Write-Up 4
5. Flag 11
6. 별도 첨부 12
7. Reference 13

1. 문제

URL	-
문제 내용	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. 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)
문제 파일	(용량이 너무 커 첨부하지 않는다.)
문제 유형	system forensics
난이도	3 / 3

2. 분석 도구

도구명	다운로드 링크	Version
HxD	https://mh-nexus.de/en/hxd/	2.5
ARIN	https://github.com/horensic/ARIN.git	-
DCode	https://www.digital-detective.net/dcode/	5.5

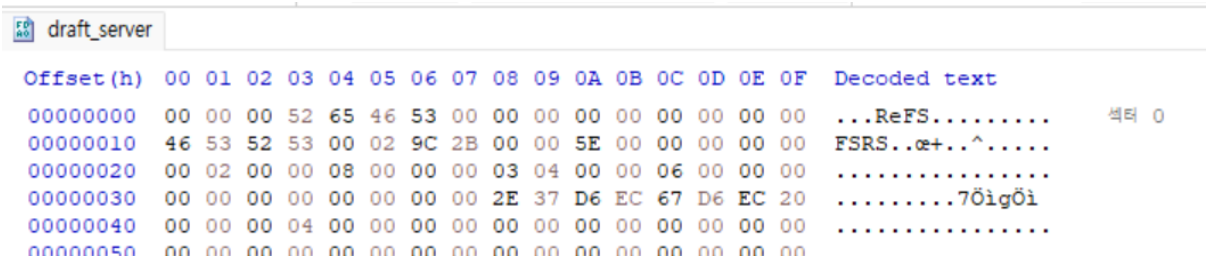
3. 환경

OS
Windows 11 Home

4. Write-Up

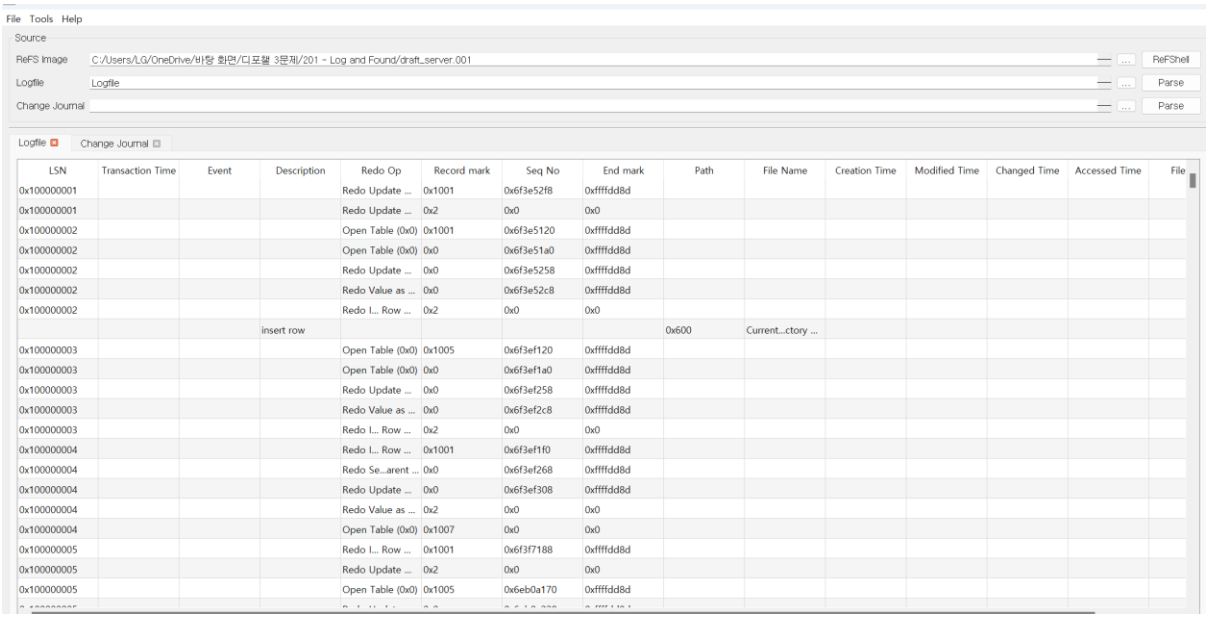
파일명	draft_server.001
용량	2.99GB
SHA256	05846f618c1406372693ee4e9da442740a505f5cac57958d43e07ccdd850c2c5
Timestamp	2023-05-31 22:08:58

1. 이름이 변경된 파일의 원래 파일명과 변경된 파일명을 나열합니다.



[그림 1] HxD draft_server

draft_server 문제 파일을 HxD 를 사용하여 열어보았더니 ReFS 파일 시스템이라는 것을 확인할 수 있다. [7. Reference]에 첨부한 링크를 통해 renaming 의 opcode 패턴을 확인했다. (0x02 -> 0x02 -> 0x01 -> 0x01 -> 0x04)



[그림 2] ARIN을 사용한 ReFS 분석

[WHS-2] .iso

A1 0x100000001

	A	B	C	D	E	F	G	H	I	J	K	L
1	0x100000001				Redo Update Row (0x3)	0x1001	0x6f3e52f8	0xffffdd8d				
2												
3	0x100000001				Redo Update Row (0x3)	0x2	0x0	0x0				
4												
5	0x100000002				Open Table (0x0)	0x1001	0x6f3e5120	0xffffdd8d				
6												
7	0x100000002				Open Table (0x0)	0x0	0x6f3e51a0	0xffffdd8d				
8												
9	0x100000002				Redo Update Data with Root (0	0x0	0x6f3e5258	0xffffdd8d				
10												
11	0x100000002				Redo Value as Key (0x10)	0x0	0x6f3e52c8	0xffffdd8d				
12												
13	0x100000002				Redo Insert Row (0x1)	0x2	0x0	0x0				
14												
15				insert row					0x600	Current Directory Index		
16												
17	0x100000003				Open Table (0x0)	0x1005	0x6f3ef120	0xffffdd8d				

[그림 3] .csv로 저장

검색의 편리성을 위해 .csv 파일 형식으로 저장한다.

찾기(D) 바꾸기(P)

찾을 내용(N): (0x5)

범위(H): 시트
검색(S): 행
찾는 위치(L): 수식

☐ 대/소문자 구분(C)
☐ 전체 셀 내용 일치(O)
☐ 전자/반자 구분(B)

통합 문서	시트	이름	셀	값	수식
2024-06-07 02-34-10-ARIN-Logfile.csv	2024-06-07 02-34-10-ARIN-Logfil		E765	Redo Reparent Table (0x5)	
2024-06-07 02-34-10-ARIN-Logfile.csv	2024-06-07 02-34-10-ARIN-Logfil		E7033	Redo Reparent Table (0x5)	
2024-06-07 02-34-10-ARIN-Logfile.csv	2024-06-07 02-34-10-ARIN-Logfil		E8953	Redo Reparent Table (0x5)	
2024-06-07 02-34-10-ARIN-Logfile.csv	2024-06-07 02-34-10-ARIN-Logfil		E15655	Redo Reparent Table (0x5)	

[그림 4] 검색

총 4 개의 검색 결과가 나온다.

0x10000003d				Redo Delete Row (0x2)	0x1001	0x6eb0a140	0xffffdd8d				
0x10000003d				Redo Reparent Table (0x5)	0x0	0x6eb0a238	0xffffdd8d				
0x10000003d				Redo Insert Row (0x1)	0x2	0x0	0x0				
			update data						0x600	Current Directory Index	
			update data						0x600	1008023_B.jpg	

[그림 5] renaming에 관한 흔적

살펴보니 Redo Delete Row (0x2) -> Redo Reparent Table (0x5) -> Redo Insert Row (0x1)의 순서를 거쳐 0x600 에서 데이터를 업데이트하고 1008023_B.jpg 에 대한 데이터를 업데이트하는 걸 볼 수 있다.

```
1803D000  4D 4C 6F 67 07 75 DB AE 01 00 00 00 00 10 00 00  MLog.uÛ®........   섹터 786,920
1803D010  D4 7C BC D5 69 D2 7D 40 9F E8 58 0B 84 41 AA 0D  Ô|¼Õi}@Ÿ‡X.„Aª.
1803D020  02 00 00 00 00 00 00 00 3D 00 00 00 01 00 00 00  ........=.......
1803D030  3C 00 00 00 01 00 00 00 01 00 00 00 01 00 00 00  <...............
1803D040  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
1803D050  00 00 00 00 78 00 00 00 00 00 00 00 00 00 00 00  ....x...........
1803D060  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
1803D070  00 00 00 00 00 00 00 00 3D 00 00 00 01 00 00 00  ........=.......
1803D080  8A 3F 59 A5 00 00 00 00 00 00 00 00 00 00 00 00  Š?Y¥............
1803D090  3C 00 00 00 01 00 00 00 50 0F 00 00 00 00 00 00  <.......P.......
1803D0A0  38 00 00 00 88 0F 00 00 02 00 00 00 00 00 00 00  8...ˆ...........
1803D0B0  28 02 00 00 08 00 00 00 80 00 00 00 02 00 00 00  (.......€.......
1803D0C0  01 00 00 00 38 00 00 00 01 00 00 00 40 00 00 00  ....8.......@...
1803D0D0  15 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00  ................
1803D0E0  00 00 00 00 01 10 00 00 40 A1 B0 6E 8D DD FF FF  ........@¡°n.Ýÿÿ
1803D0F0  48 00 00 00 1C 00 00 00 68 00 00 00 18 00 00 00  H.......h.......
1803D100  30 E0 00 00 30 01 00 00 00 00 00 00 00 00 00 00  0à..0...........
1803D110  00 00 00 00 00 06 00 00 00 00 00 00 00 00 00 00  ................
1803D120  20 00 00 80 00 00 00 00 1B 00 00 00 00 00 00 00   ..€............
1803D130  00 00 00 00 00 00 00 00 F8 00 00 00 05 00 00 00  ........ø.......
1803D140  02 00 00 00 38 00 00 00 02 00 00 00 48 00 00 00  ....8.......H...
1803D150  15 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00  ................
1803D160  00 00 00 00 00 00 00 00 38 A2 B0 6E 8D DD FF FF  ........8¢°n.Ýÿÿ
1803D170  58 00 00 00 1C 00 00 00 78 00 00 00 2A 00 00 00  X.......x...*...
1803D180  A8 00 00 00 30 00 00 00 D8 00 00 00 1E 00 00 00  ¨...0...Ø.......
1803D190  30 E0 00 00 30 01 00 00 00 00 00 00 00 00 00 00  0à..0...........
1803D1A0  00 00 00 00 00 06 00 00 00 00 00 00 00 00 00 00  ................
1803D1B0  30 01 00 00 80 01 00 00 00 00 00 00 30 00 01 00  0...€.......0...
1803D1C0  31 00 30 00 30 00 38 00 30 00 32 00 32 00 5F 00  1.0.0.8.0.2.2._.
1803D1D0  42 00 2E 00 6A 00 70 00 67 00 00 00 00 00 00 00  B...j.p.g.......
1803D1E0  01 00 00 00 08 00 00 00 10 00 00 00 1C 00 00 00  ................
1803D1F0  30 E0 00 00 30 01 00 00 00 00 00 00 00 00 00 00  0à..0...........
1803D200  00 00 00 00 00 06 00 00 00 00 00 00 00 00 00 00  ................   섹터 786,921
1803D210  30 00 01 00 31 00 30 00 30 00 38 00 30 00 32 00  0...1.0.0.8.0.2.
1803D220  33 00 5F 00 42 00 2E 00 6A 00 70 00 67 00 00 00  3._.B...j.p.g...
```

[그림 6] 0x02 -> 0x05

이러한 흔적을 확인하고 HxD 에서 살펴보면 다음과 같이 적혀 있다.

```
1803D200  00 00 00 00 00 06 00 00 00 00 00 00 00 00 00 00  ................   섹터 786,921
1803D210  30 00 01 00 31 00 30 00 30 00 38 00 30 00 32 00  0...1.0.0.8.0.2.
1803D220  33 00 5F 00 42 00 2E 00 6A 00 70 00 67 00 00 00  3._.B...j.p.g...
1803D230  B0 00 00 00 01 00 00 00 01 00 00 00 38 00 00 00  °...............8...
1803D240  02 00 00 00 40 00 00 00 15 00 00 00 00 00 00 00  ....@...........
1803D250  11 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00  ................
1803D260  00 00 00 00 00 00 00 00 50 00 00 00 1C 00 00 00  ........P.......
1803D270  70 00 00 00 18 00 00 00 88 00 00 00 28 00 00 00  p.......ˆ...(...
1803D280  30 E0 00 00 30 01 00 00 00 00 00 00 00 00 00 00  0à..0...........
1803D290  00 00 00 00 00 06 00 00 00 00 00 00 00 00 00 00  ................
1803D2A0  20 00 00 80 00 00 00 00 1B 00 00 00 00 00 00 00   ..€............
1803D2B0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
1803D2C0  0C 00 1A 00 31 00 30 00 30 00 38 00 30 00 32 00  ....1.0.0.8.0.2.
1803D2D0  33 00 5F 00 42 00 2E 00 6A 00 70 00 67 00 FF FF  3._.B...j.p.g.ÿÿ
```

[그림 7] 0x01

[WHS-2] .iso

```
1803E000  4D 4C 6F 67 07 75 DB AE 01 00 00 00 00 10 00 00  MLog.uÛ®........   섹터 786,928
1803E010  D4 7C BC D5 69 D2 7D 40 9F E8 58 0B 84 41 AA 0D  Ô|¼ÕiÒ}@ŸèX.„Aª.
1803E020  02 00 00 00 00 00 00 00 3E 00 00 00 01 00 00 00  ........>.......
1803E030  3D 00 00 00 01 00 00 00 01 00 00 00 01 00 00 00  =...............
1803E040  00 00 00 00 8D DD FF FF 00 00 00 00 00 00 00 00  .....Ýÿÿ........
1803E050  00 00 00 00 78 00 00 00 05 00 08 00 00 00 00 00  ....x...........
1803E060  68 50 3E 6F 8D DD FF FF 68 50 3E 6F 8D DD FF FF  hP>o.ÝÿÿhP>o.Ýÿÿ
1803E070  FF FF FF 7F 00 00 00 00 3E 00 00 00 01 00 00 00  ÿÿÿ.....>.......
1803E080  25 9E A8 07 00 00 00 00 00 00 00 00 78 00 00 00  %ž¨.........x...
1803E090  3D 00 00 00 01 00 00 00 50 0F 00 00 00 00 00 00  =.......P.......
1803E0A0  38 00 00 00 88 0F 00 00 02 00 00 00 00 00 00 00  8...ˆ...........
1803E0B0  00 01 00 00 08 00 00 00 00 01 00 00 04 00 00 00  ................
1803E0C0  02 00 00 00 38 00 00 00 01 00 00 00 48 00 00 00  ....8.......H...
1803E0D0  15 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00  ................
1803E0E0  00 00 00 00 03 10 00 00 00 00 00 00 00 00 00 00  ................
1803E0F0  50 00 00 00 1C 00 00 00 70 00 00 00 10 00 00 00  P.......p.......
1803E100  80 00 00 00 74 00 00 00 30 E0 00 00 30 01 00 00  €...t...0à..0...
1803E110  00 00 00 00 00 00 00 00 00 00 00 00 00 06 00 00  ................
1803E120  00 00 00 00 00 06 00 00 30 01 00 00 90 01 00 00  ........0.......
1803E130  00 00 00 00 10 00 00 00 41 F2 49 D6 2E 4F D9 01  ........AòIÖ.OÙ.
1803E140  76 A3 9A 61 A3 50 D9 01 76 A3 9A 61 A3 50 D9 01  v£ša£PÙ.v£ša£PÙ.
1803E150  76 A3 9A 61 A3 50 D9 01 00 00 00 00 00 00 00 00  v£ša£PÙ.........
1803E160  AC 74 C5 C1 01 00 00 00 00 00 00 00 00 00 00 00  ¬tÅÁ............
1803E170  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
1803E180  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
1803E190  21 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  !...............
1803E1A0  00 00 00 00 00 00 00 00 01 00 00 00 10 00 00 00  ................
1803E1B0  88 00 00 00 08 00 00 00 18 01 00 00 08 00 00 00  ˆ...............
1803E1C0  18 01 00 00 04 00 00 00 02 00 00 00 38 00 00 00  ............8...
1803E1D0  01 00 00 00 48 00 00 00 15 00 00 00 00 00 00 00  ....H...........
1803E1E0  11 00 00 00 00 00 00 00 00 00 00 00 07 10 00 00  ................
1803E1F0  00 00 00 00 00 00 00 00 50 00 00 00 1C 00 00 00  ........P.......
1803E200  70 00 00 00 2A 00 00 00 A0 00 00 00 74 00 00 00  p...*... ...t...   섹터 786,929
1803E210  30 E0 00 00 30 01 00 00 00 00 00 00 00 00 00 00  0à..0...........
1803E220  00 00 00 00 00 06 00 00 00 00 00 00 00 00 00 00  ................
1803E230  30 01 00 00 80 01 00 00 00 00 00 00 30 00 01 00  0...€.......0...
1803E240  31 00 30 00 30 00 38 00 30 00 32 00 33 00 5F 00  1.0.0.8.0.2.3._.
1803E250  42 00 2E 00 6A 00 70 00 67 00 92 47 A3 50 D9 01  B...j.p.g.'G£PÙ.
1803E260  A3 05 27 3F A3 50 D9 01 00 E2 2B F6 71 0B D7 01  £.'?£PÙ..â+öq.×.
1803E270  76 A3 9A 61 A3 50 D9 01 A3 05 27 3F A3 50 D9 01  v£ša£PÙ.£.'?£PÙ.
```

[그림 8] 0x04 -> 0x04

0x04에서 데이터가 업데이트 되었고, 바뀐 파일명은 1008023_B.jpg이다.

이러한 구조를 따르며 다른 파일을 모두 검색한 결과 1번의 답은 다음과 같다.

- **1008022_B.jpg -> 1008023_B.jpg**
- **1012200_B.jpg -> 1012201_B.jpg**
- **1012377_B.jpg -> 1012378_B.jpg**
- **1014394_B.jpg -> 1014398_B.jpg**

2. 삭제된 파일의 파일명을 나열합니다.

삭제된 파일은 0x0F -> 0x02 -> 0x0F -> 0x02 -> 0x04의 순서를 가지고 있다.

```
185DF000  4D 4C 6F 67 07 75 DB AE 01 00 00 00 00 10 00 00  MLog.uÛ®........     섹터 798,456
185DF010  D4 7C BC D5 69 D2 7D 40 9F E8 58 0B 84 41 AA 0D  Ô|¼ÕiÒ}@ŸèX.„Aª.
185DF020  02 00 00 00 00 00 00 00 DF 05 00 00 01 00 00 00  ........ß.......
185DF030  DE 05 00 00 01 00 00 00 01 00 00 00 01 00 00 00  Þ...............
185DF040  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
185DF050  00 00 00 00 78 00 00 00 00 00 00 00 00 00 00 00  ....x...........
185DF060  4D 00 88 80 00 00 00 00 00 00 00 00 00 00 00 00  M.ˆ€............
185DF070  6C B8 F5 F6 06 82 FF FF DF 05 00 00 01 00 00 00  l¸õö.‚ÿÿß.......
185DF080  A4 E3 3A D3 00 00 00 00 88 20 7D 6F 8D DD FF FF  ¤ã:Ó....ˆ }o.Ýÿÿ
185DF090  DE 05 00 00 01 00 00 00 50 0F 00 00 00 00 00 00  Þ.......P.......
185DF0A0  38 00 00 00 88 0F 00 00 02 00 00 00 00 00 00 00  8...ˆ...........
185DF0B0  50 01 00 00 08 00 00 00 E0 00 00 00 07 00 00 00  P.......à.......
185DF0C0  03 00 00 00 38 00 00 00 02 00 00 00 50 00 00 00  ....8.......P...
185DF0D0  57 00 00 00 00 00 00 00 53 00 00 00 00 00 00 00  W.......S.......
185DF0E0  00 00 00 00 01 10 00 00 A0 21 7D 6F 8D DD FF FF  ........ !}o.Ýÿÿ
185DF0F0  60 00 00 00 1C 00 00 00 80 00 00 00 2A 00 00 00  `.......€...*...
185DF100  B0 00 00 00 12 00 00 00 C8 00 00 00 10 00 00 00  °.......È.......
185DF110  D8 00 00 00 04 00 00 00 30 E0 00 00 30 01 00 00  Ø.......0à..0...
185DF120  00 00 00 00 00 00 00 00 00 00 00 00 00 06 00 00  ................
185DF130  00 00 00 00 00 00 00 00 30 01 00 00 80 01 00 00  ........0...€...
185DF140  00 00 00 00 30 00 01 00 31 00 30 00 31 00 33 00  ....0...1.0.1.3.
185DF150  31 00 39 00 31 00 5F 00 42 00 2E 00 6A 00 70 00  1.9.1._.B...j.p.
185DF160  67 00 70 00 67 00 75 00 80 01 00 00 A0 01 00 00  g.p.g.u.€... ...
185DF170  00 00 00 00 80 00 00 00 00 00 00 00 48 00 00 00  ....€.......H...
185DF180  00 00 00 00 00 00 00 00 45 00 00 00 00 00 00 00  ........E.......
185DF190  00 00 00 00 00 00 00 00 70 00 00 00 04 00 00 00  ........p.......
185DF1A0  00 00 00 00 38 00 00 00 02 00 00 00 38 00 00 00  ....8.......8...
185DF1B0  57 00 00 00 00 00 00 00 53 00 00 00 00 00 00 00  W.......S.......
185DF1C0  00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00  ................
185DF1D0  48 00 00 00 20 00 00 00 68 00 00 00 04 00 00 00  H... ...h.......
185DF1E0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
185DF1F0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

[그림 9] 0x07 -> 0x04

삭제의 경우 Redo Free가 발생함으로 0x07 -> 0x04를 찾을 수 있다. ([7. Reference] 참조)

```
185E0000  4D 4C 6F 67 07 75 DB AE 01 00 00 00 00 10 00 00  MLog.uÛ®........     섹터 798,464
185E0010  D4 7C BC D5 69 D2 7D 40 9F E8 58 0B 84 41 AA 0D  Ô|¼ÕiÒ}@ŸèX.„Aª.
185E0020  02 00 00 00 00 00 00 00 E0 05 00 00 01 00 00 00  ........à.......
185E0030  DF 05 00 00 01 00 00 00 01 00 00 00 01 00 00 00  ß...............
185E0040  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
185E0050  00 00 00 00 78 00 00 00 00 00 00 00 00 00 00 00  ....x...........
185E0060  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
185E0070  00 00 00 00 00 00 00 00 E0 05 00 00 01 00 00 00  ........à.......
185E0080  48 F3 07 B0 00 00 00 00 00 00 00 00 00 00 00 00  Hó.°............
185E0090  DF 05 00 00 01 00 00 00 50 0F 00 00 00 00 00 00  ß.......P.......
185E00A0  38 00 00 00 88 0F 00 00 02 00 00 00 00 00 00 00  8...ˆ...........
185E00B0  58 02 00 00 08 00 00 00 B8 00 00 00 0F 00 00 00  X.......¸.......
185E00C0  03 00 00 00 38 00 00 00 00 00 00 00 50 00 00 00  ....8.......P...
185E00D0  57 00 00 00 00 00 00 00 53 00 00 00 00 00 00 00  W.......S.......
185E00E0  00 00 00 00 01 10 00 00 78 A1 AA 6E 8D DD FF FF  ........x¡ªn.Ýÿÿ
185E00F0  50 00 00 00 1C 00 00 00 70 00 00 00 2A 00 00 00  P.......p...*...
185E0100  A0 00 00 00 12 00 00 00 30 E0 00 00 30 01 00 00   .......0à..0...
185E0110  00 00 00 00 00 00 00 00 00 00 00 00 00 06 00 00  ................
185E0120  00 00 00 00 00 00 00 00 30 01 00 00 80 01 00 00  ........0...€...
185E0130  00 00 00 00 30 00 01 00 31 00 30 00 31 00 33 00  ....0...1.0.1.3.
185E0140  31 00 39 00 31 00 5F 00 42 00 2E 00 6A 00 70 00  1.9.1._.B...j.p.
185E0150  67 00 35 00 31 00 30 00 80 01 00 00 A0 01 00 00  g.5.1.0.€... ...
185E0160  00 00 00 00 80 00 00 00 00 00 00 00 04 00 00 00  ....€...........
185E0170  80 00 00 00 02 00 00 00 01 00 00 00 38 00 00 00  €...........8...
185E0180  01 00 00 00 40 00 00 00 57 00 00 00 00 00 00 00  ....@...W.......
185E0190  53 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  S...............
185E01A0  F8 A1 AA 6E 8D DD FF FF 48 00 00 00 1C 00 00 00  ø¡ªn.ÝÿÿH.......
185E01B0  68 00 00 00 18 00 00 00 30 E0 00 00 30 01 00 00  h.......0à..0...
185E01C0  00 00 00 00 00 00 00 00 00 00 00 00 00 06 00 00  ................
185E01D0  00 00 00 00 00 06 00 00 20 00 00 80 00 00 00 00  ........ ..€....
185E01E0  9C 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00  œ...............
185E01F0  98 00 00 00 0F 00 00 00 02 00 00 00 38 00 00 00  ˜...........8...
```

[그림 10] 0x0F -> 0x02

[WHS-2] .iso

```
185E01F0  98 00 00 00 0F 00 00 00 02 00 00 00 38 00 00 00  ˜...........8...
185E0200  00 00 00 00 48 00 00 00 57 00 00 00 00 00 00 00  ....H...W.......   섹터 798,465
185E0210  53 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  S...............
185E0220  90 A2 AA 6E 8D DD FF FF 48 00 00 00 1C 00 00 00  .c²n.ÝÿÿH.......
185E0230  68 00 00 00 2A 00 00 00 30 E0 00 00 30 01 00 00  h...*...0à..0...
185E0240  00 00 00 00 00 00 00 00 00 00 00 00 00 06 00 00  ................
185E0250  00 00 00 00 30 01 00 00 30 01 00 00 80 01 00 00  ....0...0...€...
185E0260  00 00 00 00 30 00 01 00 31 00 30 00 31 00 33 00  ....0...1.0.1.3.
185E0270  31 00 39 00 31 00 5F 00 42 00 2E 00 6A 00 70 00  1.9.1._.B...j.p.
185E0280  67 00 00 00 38 00 00 00 88 00 00 00 02 00 00 00  g...8...ˆ.......
185E0290  01 00 00 00 38 00 00 00 01 00 00 00 40 00 00 00  ....8.......@...
185E02A0  57 00 00 00 00 00 00 00 53 00 00 00 00 00 00 00  W.......S.......
185E02B0  00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00  ................
185E02C0  48 00 00 00 1C 00 00 00 68 00 00 00 1E 00 00 00  H.......h.......
185E02D0  30 E0 00 00 30 01 00 00 00 00 00 00 00 00 00 00  0à..0...........
185E02E0  00 00 00 00 00 06 00 00 00 00 00 00 30 00 01 00  ............0...
185E02F0  30 00 01 00 31 00 30 00 31 00 33 00 31 00 39 00  0...1.0.1.3.1.9.
185E0300  31 00 5F 00 42 00 2E 00 6A 00 70 00 67 00 00 00  1._.B...j.p.g...
185E0310  00 01 00 00 08 00 00 00 00 01 00 00 04 00 00 00  ................
185E0320  02 00 00 00 38 00 00 00 01 00 00 00 48 00 00 00  ....8.......H...
185E0330  57 00 00 00 00 00 00 00 53 00 00 00 00 00 00 00  W.......S.......
185E0340  00 00 00 00 07 10 00 00 00 00 00 00 00 00 00 00  ................
185E0350  50 00 00 00 1C 00 00 00 70 00 00 00 10 00 00 00  P.......p.......
185E0360  80 00 00 00 74 00 00 00 30 E0 00 00 30 01 00 00  €...t...0à..0...
185E0370  00 00 00 00 00 00 00 00 00 00 00 00 00 06 00 00  ................
185E0380  00 00 00 00 00 00 00 00 30 01 00 00 90 01 00 00  ........0.......
185E0390  00 00 00 00 10 00 00 00 41 F2 49 D6 2E 4F D9 01  ........AòIÖ.OÙ.
185E03A0  E7 E9 67 EC AE 67 D9 01 E7 E9 67 EC AE 67 D9 01  çégì®gÙ.çégì®gÙ.
185E03B0  E7 E9 67 EC AE 67 D9 01 00 00 00 00 00 00 00 00  çégì®gÙ........
185E03C0  AC 74 C5 C1 01 00 00 00 00 00 00 00 00 00 00 00  ¬tÅÁ............
185E03D0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
185E03E0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
185E03F0  16 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

[그림 11] 0x0F -> 0x02

```
185E30A0  38 00 00 00 88 0F 00 00 02 00 00 00 00 00 00 00  8...ˆ...........
185E30B0  00 01 00 00 08 00 00 00 00 01 00 00 04 00 00 00  ................
185E30C0  02 00 00 00 38 00 00 00 01 00 00 00 48 00 00 00  ....8.......H...
185E30D0  59 00 00 00 00 00 00 00 55 00 00 00 00 00 00 00  Y.......U.......
185E30E0  00 00 00 00 03 10 00 00 00 00 00 00 00 00 00 00  ................
185E30F0  50 00 00 00 1C 00 00 00 70 00 00 00 10 00 00 00  P.......p.......
185E3100  80 00 00 00 74 00 00 00 30 E0 00 00 30 01 00 00  €...t...0à..0...
185E3110  00 00 00 00 00 00 00 00 00 00 00 00 00 06 00 00  ................
185E3120  00 00 00 00 00 00 00 00 30 01 00 00 90 01 00 00  ........0.......
185E3130  00 00 00 00 10 00 00 00 41 F2 49 D6 2E 4F D9 01  ........AòIÖ.OÙ.
185E3140  26 E3 39 FC AE 67 D9 01 26 E3 39 FC AE 67 D9 01  &ã9ü®gÙ.&ã9ü®gÙ.
185E3150  26 E3 39 FC AE 67 D9 01 00 00 00 00 00 00 00 00  &ã9ü®gÙ........
185E3160  AC 74 C5 C1 01 00 00 00 00 00 00 00 00 00 00 00  ¬tÅÁ............
185E3170  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
185E3180  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

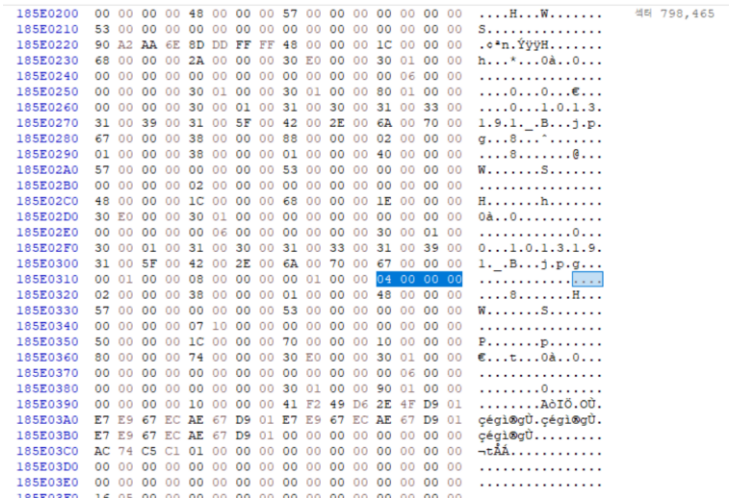
[그림 12] 0x04

위와 같은 방식으로 다른 파일들도 식별한 결과 다음과 같이 정리할 수 있다.

- **1013191_B.jpg**
- **1012353_B.jpg**
- **1008103_B.jpg**
- **1013029_B.jpg**
- **1014381_B.jpg**

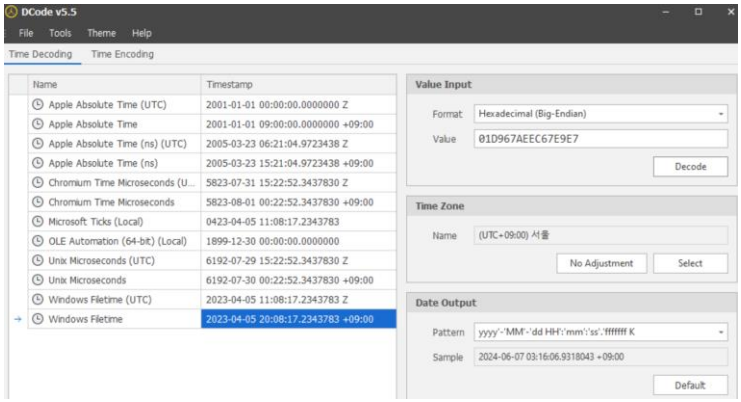
3. 파일별로 삭제된 시간을 제공합니다.

파일이 삭제된 시간은 삭제된 파일의 부모 디렉터리의 수정 시간으로 알 수 있다. 또한, File deletion에 대한 이벤트 시간은 5번째 레코드의 Change Time을 확인하면 된다. ([7. Reference] 참조)



[그림 13] 0x04

위의 정보로 0x04의 레코드에서 Change Time을 확인할 수 있다. (0x01D967AEEC67E9E7) 또한, 4 번째에 기록되어 있는 것을 알 수 있다.



[그림 14] DCode를 사용하여 시간 확인

DCode를 사용하여 삭제된 파일들에 대한 삭제 시간을 알 수 있다.

위와 같은 방법을 사용하여 삭제된 파일의 시간을 알아본 결과는 다음과 같다.

- **1013191_B.jpg : 2023-04-05 20:08:17.2343783 (UTC +09:00)**
- **1012353_B.jpg : 2023-04-05 20:08:43.7762854 (UTC +09:00)**
- **1008103_B.jpg : 2023-04-05 20:09:13.4040759 (UTC +09:00)**
- **1013029_B.jpg : 2023-04-05 20:09:38.4102339 (UTC +09:00)**
- **1014381_B.jpg : 2023-04-05 20:10:06.9314698 (UTC +09:00)**

5. Flag

1. 이름이 변경된 파일의 원래 파일명과 변경된 파일명을 나열합니다.
   A. 1008022_B.jpg -> 1008023_B.jpg
   B. 1012200_B.jpg -> 1012201_B.jpg
   C. 1012377_B.jpg -> 1012378_B.jpg
   D. 1014394_B.jpg -> 1014398_B.jpg

2. 삭제된 파일의 파일명을 나열합니다.
   A. 1013191_B.jpg
   B. 1012353_B.jpg
   C. 1008103_B.jpg
   D. 1013029_B.jpg
   E. 1014381_B.jpg

3. 파일별로 삭제된 시간을 제공합니다.
   A. 1013191_B.jpg : 2023-04-05 20:08:17.2343783 (UTC +09:00)
   B. 1012353_B.jpg : 2023-04-05 20:08:43.7762854 (UTC +09:00)
   C. 1008103_B.jpg : 2023-04-05 20:09:13.4040759 (UTC +09:00)
   D. 1013029_B.jpg : 2023-04-05 20:09:38.4102339 (UTC +09:00)
   E. 1014381_B.jpg : 2023-04-05 20:10:06.9314698 (UTC +09:00)

4. 별도 첨부

- 문제 번역본

케이트는 패션 디자인 회사의 서버 관리자로 최근 서버에 저장된 디자인 파일이 유출되는 사건이 발생하여 회사 내에서 내부 감사를 받았습니다. 회사는 이 문제를 해결하기 위해 서버 볼륨에 대한 디지털 포렌식 분석을 요청했습니다. 각 질문에 대한 분석 결과를 제공해 주시기 바랍니다. 1) 이름이 변경된 파일의 원래 파일명과 변경된 파일명을 나열합니다. (50 점) 2) 삭제된 파일의 파일명을 나열합니다. (50 점) 3) 파일별로 삭제된 시간을 제공합니다. (100 점)

5. Reference

- https://www.dfrws.org/wp-content/uploads/2021/01/2021_APAC_paper-forensic_analysis_of_refs_journaling.pdf