FAT32 파일 시간 정보

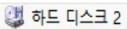
23 고은이

시간 정보

- 포렌식에 있어서 가장 중요한 것은 시간 정보 이다.
- 시간 정보는 디지털 포렌식 분야에서 매우 중요한 역할을 한다. 파일 및 디렉터리의 시간 정보는 디지털 데이터의 생성, 수정, 액세스와 관련된 다양한 중요한 정보를 제공하며, 다양한 분야에서 활용될 수 있다.

- 파일이 생성된 시간, 접근한 시간, 수정된 시간 등 시간 정보로 어떠한 사건의 범행을 입증하는데 중요한 단서를 찾을 수 있을 것이다.
- ▶ FAT32 에서 파일과 디렉터리의 메타데이터를 가지고 있는 구조체는 디렉터리 엔 트리이다.

- 디렉터리 엔트리
- 디렉터리 엔트리는 파일 이름, 파일 유형, 파일 속 성, 파일 크기, 시간 정보, 파일 위치, 권한 정보 등 을 포함 하고 있다.
- . 포렌식 분석이나 파일 시 스템 복구 작업 등에서 디 렉터리 엔트리 정보를 분 석하여 파일의 삭제 여부 를 파악할 수 있다.
- 디렉터리 엔트리에서 얻을 수 있는 정보들은 디지 털 포렌식 분야에서 중요한 역할을 한다.



```
Offset (h)
                         06 07
                              08 09 0A 0B 0C 0D 0E 0F
                                                     Decoded text
000D00000
         BB F5 20 BA BC B7 FD 20 20 20 20
                                                     »õ °ta·ý
                                                     .....vòV.....
000D00010
000D00020
                                                    B .I.n.f.o...rr.
000D00030
                                                     m.a.t.i.o...n...
000D00040
                      73 00 74 00 65 00
                                                     .S.y.s.t.e...rm.
000D00050
         20 00 56 00 6F 00 6C 00 75 00 00 00 6D 00 65 00
                                                      .V.o.l.u...m.e.
                                                              ..Ä.v
                                                     SYSTEM~1
000D00060
                                                    òVòV....VòV.....
000D00070
                                                     åÈÀ .MѤÂ,Ò... .
000D00080
                                                     8».Á..t.x...t...
000D00090
                                                     åőÅØ¾°~1TXT .4 v
000D000A0
                                                     òVòV..!vòV.....
000D000B0
                                                     $RECYCLEBIN..> V
000D000C0
                                                     òVòV..!vòV.....
000D000D0
                                                     åCP
                                                            TXT .4 v
000D000E0
                                                     òVòV.....
         F2 56 F2 56 00 00 30 76 F2
000D000F0
000D00100
         000D00110
```

날짜(H)								날짜(L)							
7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
Υ	Υ	Υ	Υ	Υ	Υ	Υ	M	M	M	M	D	D	D	D	D

	시간(H)							시간(L)							
7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
h	h	h	h	h	m	m	m	m	m	m	S	S	S	S	S

\mathbf{Y}	1980년부터 지난 연도
\mathbf{M}	1월 = 1 12월 = 12
D	1 ~ 31일
h	0 ~ 23시
m	0 ~ 59분
S	2초 단위로 0 ~ 29의 값 저장

```
åõÅØ¾°~1TXT .4 v
000D000A0
                      BD BA 7E 31 54 58 54 20 00 34 20 76
000D000B0
                                                            òVòV..!vòV.....
                                                     00 00
000D000C0
                                                            $RECYCLEBIN..> v
                                                            òVòV...vòV.....
000D000D0
                                                            åCP
000D000E0
                                                                    TXT .4 v
000D000F0
                                                            òVòV.....
                                                     00 00
000D00100
000D00110
```

빨간색 = 파일 생성 날짜 노란색 = 마지막 접근 시간 초록색 = 마지막 수정 시간 분홍색 = 마지막 수정 날짜 하늘색 = 파일 생성 시간

파일 생성 날짜

```
파일이 생성된 날짜 F2 56
리틀 엔디언으로 표기 -> 56 F2
이진수로 나타내기
56 F2 = 0101 0110 1111 0010
0101 011/0 111/1 0010
  녉
         월 /
십진수로 표기
0101\ 011 \Rightarrow 43
0.111 \Rightarrow 7
```

파일 생성 날짜 = 2023.07.18

 $1\,0010 \Rightarrow 18$

마지막 접근 시간

```
마지막 접근 시간 F2 56
리틀 엔디언으로 표기 -> 56 F2
이진수로 나타내기
56 F2 = 0101 0110 1111 0010
0101 0/110 111/1 0010
시 / 분 / 초
십진수로 표기
```

0101 0 => 10

110 111 => 55

 $1\ 0010 \Rightarrow 18$

마지막 접근 시간 = 10시 55분 18초

마지막 수정 시간

```
마지막 수정 시간 30 76
리틀 엔디언으로 표기 -> 76 30
이진수로 나타내기
76 30 = 0111 0110 0011 0000
0111 0/110 001/1 0000
시 / 분 / 초
```

십진수로 표기

 $0111\ 0 \Rightarrow 14$

 $110\ 001 \Rightarrow 49$

 $1\ 0000 \Rightarrow 16$

마지막 수정 시간 = 14시 49분 16초

파일 생성 시간

```
파일 생성 시간 20 76
리틀 엔디언으로 표기 -> 76 20
이진수로 나타내기
76 20 = 0111 0110 0010 0000
0111 0/110 001/0 0000
시 / 분 / 초
```

십진수로 표기

 $0111\ 0 \Rightarrow 14$

 $110\ 001 \Rightarrow 49$

 $0.0000 \Rightarrow 0$

파일 생성 시간 = 14시 49분 0초

Q&A