

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 엔트리이다.

날짜(H)								날짜(L)							
7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
Y	Y	Y	Y	Y	Y	Y	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

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

000D000A0	E5	F5	C5	D8	BD	BA	7E	31	54	58	54	20	00	34	20	76	åÃÅø~1TXT .4 v
000D000B0	F2	56	F2	56	00	00	21	76	F2	56	00	00	00	00	00	00	òVòV..!vòV.....
000D000C0	24	52	45	43	59	43	4C	45	42	49	4E	16	00	3E	20	76	\$RECYCLEBIN..> v
000D000D0	F2	56	F2	56	00	00	21	76	F2	56	06	00	00	00	00	00	òVòV..!vòV.....
000D000E0	E5	43	50	20	20	20	20	20	54	58	54	20	18	34	20	76	åCP TXT .4 v
000D000F0	F2	56	F2	56	00	00	30	76	F2	56	08	00	07	00	00	00	òVòV..0vòV.....
000D00100	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000D00110	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

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

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

$$0101\ 0 \Rightarrow 10$$

110 111 => 55

1 0010 => 18

마지막 접근 시간 = 10시 55분 18초

```
000D000A0 E5 F5 C5 D8 BD BA 7E 31 54 58 54 20 00 34 20 76 àÃÄÅ~!TXT .4 v
000D000B0 F2 56 F2 56 00 00 21 76 F2 56 00 00 00 00 00 00 òVòV..!vòV.....
000D000C0 24 52 45 43 59 43 4C 45 42 49 4E 16 00 3E 20 76 $RECYCLEBIN..> v
000D000D0 F2 56 F2 56 00 00 21 76 F2 56 06 00 00 00 00 00 òVòV..!vòV.....
000D000E0 E5 43 50 20 20 20 20 20 54 58 54 20 18 34 20 76 àCP      TXT .4 v
000D000F0 F2 56 F2 56 00 00 30 76 F2 56 08 00 07 00 00 00 òVòV..0vòV.....
000D00100 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000D00110 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
```

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 => 49

1 0000 => 16

마지막 수정 시간 = 14시 49분 16초

```
000D000A0 E5 F5 C5 D8 BD BA 7E 31 54 58 54 20 00 34 20 76 åÃÄ~!TXT .4 v
000D000B0 F2 56 F2 56 00 00 21 76 F2 56 00 00 00 00 00 00 òVòV..!vòV.....
000D000C0 24 52 45 43 59 43 4C 45 42 49 4E 16 00 3E 20 76 $RECYCLEBIN..> v
000D000D0 F2 56 F2 56 00 00 21 76 F2 56 06 00 00 00 00 00 00 òVòV..!vòV.....
000D000E0 E5 43 50 20 20 20 20 20 54 58 54 20 18 34 20 76 åCP      TXT .4 v
000D000F0 F2 56 F2 56 00 00 30 76 F2 56 08 00 07 00 00 00 00 òVòV..0vòV.....
000D00100 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000D00110 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
```


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 => 49

$$0 \ 0000 \Rightarrow 0$$

파일 생성 시간 = 14시 49분 0초

```
000D000A0 E5 F5 C5 D8 BD BA 7E 31 54 58 54 20 00 34 20 76 àÃÄÅ~!TXT .4 v
000D000B0 F2 56 F2 56 00 00 21 76 F2 56 00 00 00 00 00 00 òVòV..!vòV.....
000D000C0 24 52 45 43 59 43 4C 45 42 49 4E 16 00 3E 20 76 $RECYCLEBIN..> v
000D000D0 F2 56 F2 56 00 00 21 76 F2 56 06 00 00 00 00 00 òVòV..!vòV.....
000D000E0 E5 43 50 20 20 20 20 20 54 58 54 20 18 34 20 76 àCP      TXT .4 v
000D000F0 F2 56 F2 56 00 00 30 76 F2 56 08 00 07 00 00 00 òVòV..0vòV.....
000D00100 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000D00110 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
```

Q & A