BoB 6기

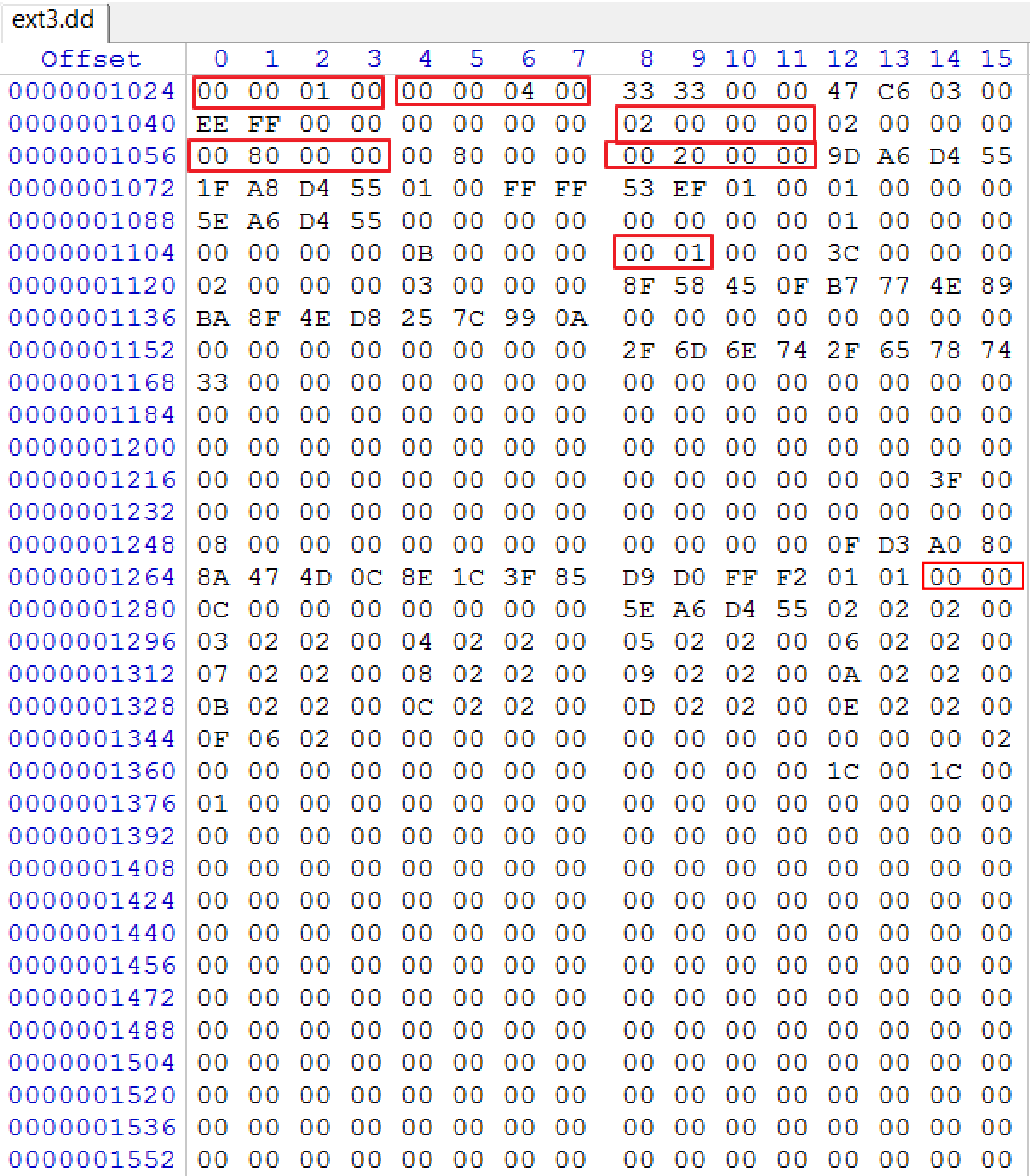
디지털 포렌식

2017.07.30

정경주

Ext3.dd 분석

EXT3.dd



```
    Offset  0  1  2  3  4  5  6  7   8  9 10 11 12 13 14 15
0000001024 00 00 01 00 00 00 04 00  33 33 00 00 47 C6 03 00
0000001040 EE FF 00 00 00 00 00 00  02 00 00 00 02 00 00 00
0000001056 00 80 00 00 00 80 00 00  00 20 00 00 9D A6 D4 55
0000001072 1F A8 D4 55 01 00 FF FF  53 EF 01 00 01 00 00 00
0000001088 5E A6 D4 55 00 00 00 00  00 00 00 00 01 00 00 00
0000001104 00 00 00 00 0B 00 00 00  00 01 00 00 3C 00 00 00
0000001120 02 00 00 00 03 00 00 00  8F 58 45 0F B7 77 4E 89
0000001136 BA 8F 4E D8 25 7C 99 0A  00 00 00 00 00 00 00 00
0000001152 00 00 00 00 00 00 00 00  2F 6D 6E 74 2F 65 78 74
0000001168 33 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000001184 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000001200 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000001216 00 00 00 00 00 00 00 00  00 00 00 00 00 00 3F 00
0000001232 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000001248 08 00 00 00 00 00 00 00  00 00 00 00 0F D3 A0 80
0000001264 8A 47 4D 0C 8E 1C 3F 85  D9 D0 FF F2 01 01 00 00
0000001280 0C 00 00 00 00 00 00 00  5E A6 D4 55 02 02 02 00
0000001296 03 02 02 00 04 02 02 00  05 02 02 00 06 02 02 00
0000001312 07 02 02 00 08 02 02 00  09 02 02 00 0A 02 02 00
0000001328 0B 02 02 00 0C 02 02 00  0D 02 02 00 0E 02 02 00
0000001344 0F 06 02 00 00 00 00 00  00 00 00 00 00 00 00 02
0000001360 00 00 00 00 00 00 00 00  00 00 00 00 1C 00 1C 00
0000001376 01 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000001392 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000001408 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000001424 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000001440 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000001456 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000001472 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000001488 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000001504 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000001520 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000001536 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000001552 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
```

Figure 1 Super block

Inode Count 0x00: 10000

Block Count 0x04: 40000

Log block size 0x18: 4K(4096)

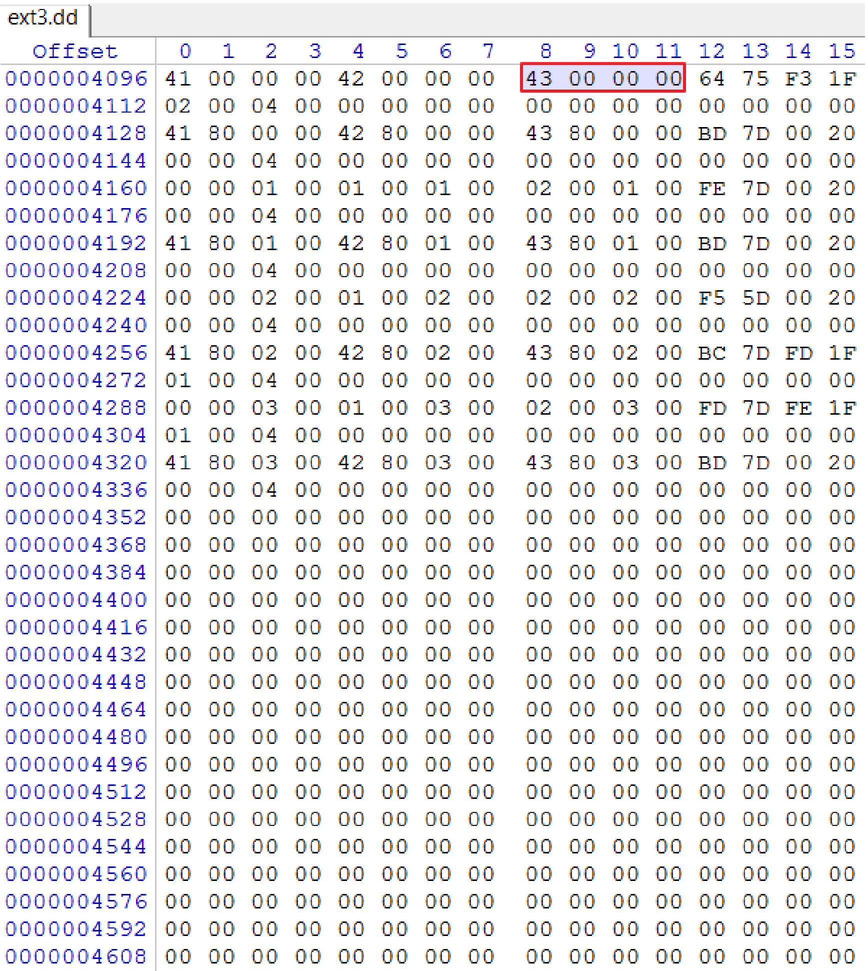
Blocks per group 0x20: 8000

Inodes per group 0x28: 2000

Inode structure size 0x58: 00 01 = 256bytes

Gdt_entry_size 00 -> 32

블록 그룹의 개수 = ceil(total_inodes /inodes_per_group) = 10000 / 2000 = 8



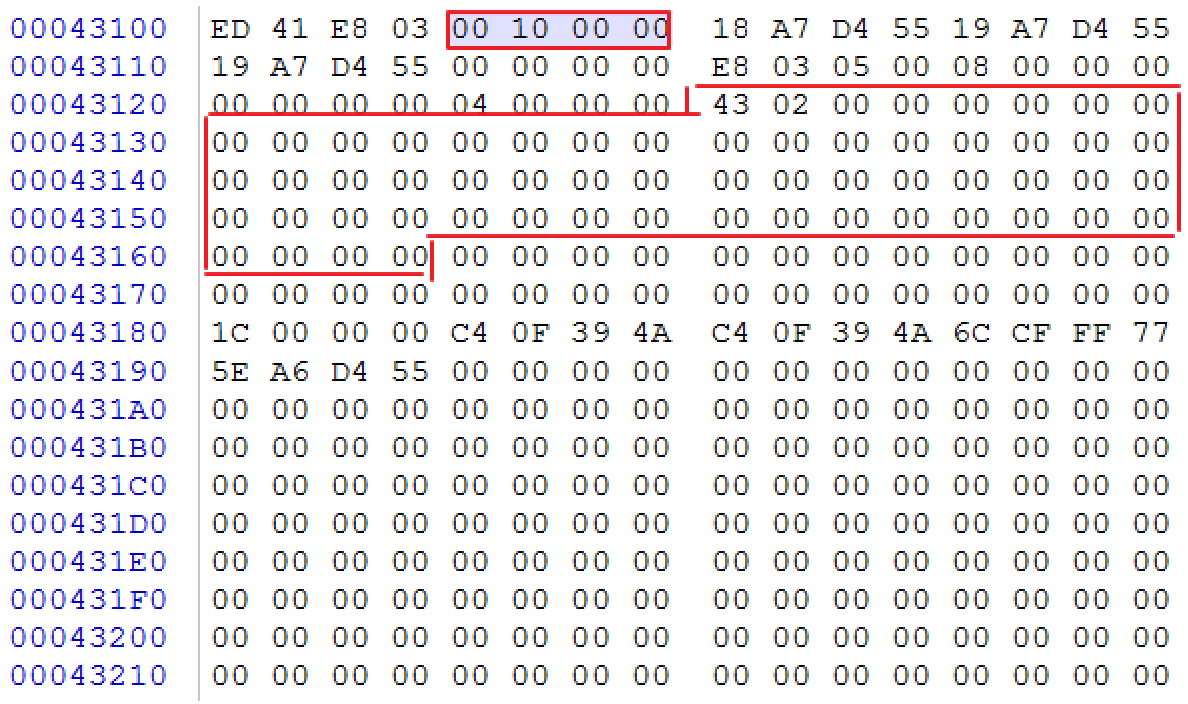
```
  Offset     0  1  2  3  4  5  6  7   8  9 10 11 12 13 14 15
0000004096  41 00 00 00 42 00 00 00  43 00 00 00 64 75 F3 1F
0000004112  02 00 04 00 00 00 00 00  00 00 00 00 00 00 00 00
0000004128  41 80 00 00 42 80 00 00  43 80 00 00 BD 7D 00 20
0000004144  00 00 04 00 00 00 00 00  00 00 00 00 00 00 00 00
0000004160  00 00 01 00 01 00 01 00  02 00 01 00 FE 7D 00 20
0000004176  00 00 04 00 00 00 00 00  00 00 00 00 00 00 00 00
0000004192  41 80 01 00 42 80 01 00  43 80 01 00 BD 7D 00 20
0000004208  00 00 04 00 00 00 00 00  00 00 00 00 00 00 00 00
0000004224  00 00 02 00 01 00 02 00  02 00 02 00 F5 5D 00 20
0000004240  00 00 04 00 00 00 00 00  00 00 00 00 00 00 00 00
0000004256  41 80 02 00 42 80 02 00  43 80 02 00 BC 7D FD 1F
0000004272  01 00 04 00 00 00 00 00  00 00 00 00 00 00 00 00
0000004288  00 00 03 00 01 00 03 00  02 00 03 00 FD 7D FE 1F
0000004304  01 00 04 00 00 00 00 00  00 00 00 00 00 00 00 00
0000004320  41 80 03 00 42 80 03 00  43 80 03 00 BD 7D 00 20
0000004336  00 00 04 00 00 00 00 00  00 00 00 00 00 00 00 00
0000004352  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000004368  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000004384  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000004400  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000004416  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000004432  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000004448  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000004464  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000004480  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000004496  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000004512  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000004528  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000004544  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000004560  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000004576  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000004592  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000004608  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
```

Figure 2 GDT block

Starting block address of inode table 0x8: 43

블록의 크기가 4K이므로 Inode의 정보는 0x43 * 4096 = 0x43000에 있다.

하지만 아이노드 테이블에서 0번째 인덱스는 아무것도 아니므로 ext3의 한블록 크기인 256kb만큼 더 간 0x43100으로 가야한다.



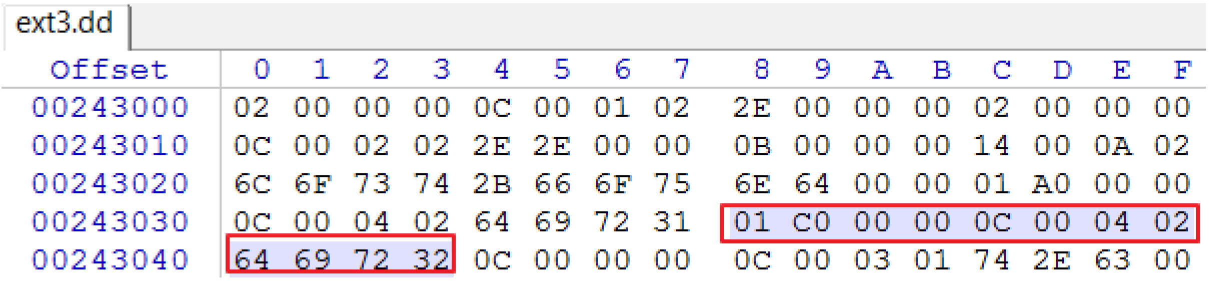
```
00043100  ED 41 E8 03 00 10 00 00  18 A7 D4 55 19 A7 D4 55
00043110  19 A7 D4 55 00 00 00 00  E8 03 05 00 08 00 00 00
00043120  00 00 00 00 04 00 00 00  43 02 00 00 00 00 00 00
00043130  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00043140  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00043150  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00043160  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00043170  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00043180  1C 00 00 00 C4 0F 39 4A  C4 0F 39 4A 6C CF FF 77
00043190  5E A6 D4 55 00 00 00 00  00 00 00 00 00 00 00 00
000431A0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000431B0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000431C0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000431D0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000431E0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000431F0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00043200  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00043210  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
```

Figure 3 Root Inode

File Size 0x4: 1000

Block pointers 0x28: 243

Block pointer의 정보로 가야하니까 블록의 크기인 243kb를 0x243*4096 = 0x243000



```
ext3.dd

  Offset    0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
00243000   02 00 00 00 0C 00 01 02  2E 00 00 00 02 00 00 00
00243010   0C 00 02 02 2E 2E 00 00  0B 00 00 00 14 00 0A 02
00243020   6C 6F 73 74 2B 66 6F 75  6E 64 00 00 01 A0 00 00
00243030   0C 00 04 02 64 69 72 31  01 C0 00 00 0C 00 04 02
00243040   64 69 72 32 0C 00 00 00  0C 00 03 01 74 2E 63 00
```

Figure 4 directory entry

0x243000으로 갔을 때 앞에 부분은 파일이 dir2가 아니기 때문에 해당 정보가 있는 곳으로 가야한다. 그러면 위 그림에 있는 빨간네모안에 있는 정보가 된다. 여기서

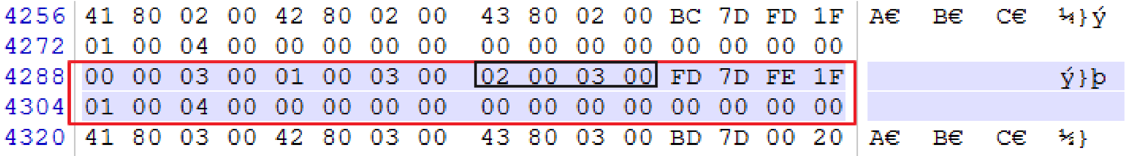
Inode 0x0: C001

Record Length 0x4: c

Name: Dir2

0xC001(49,153) / 2000(8192)(inodes per group) = 6 즉 Group[6]는 7번째다.

따라서 처음 GDT에서 7번째 그룹을 찾아서 정보를 찾으면 된다.

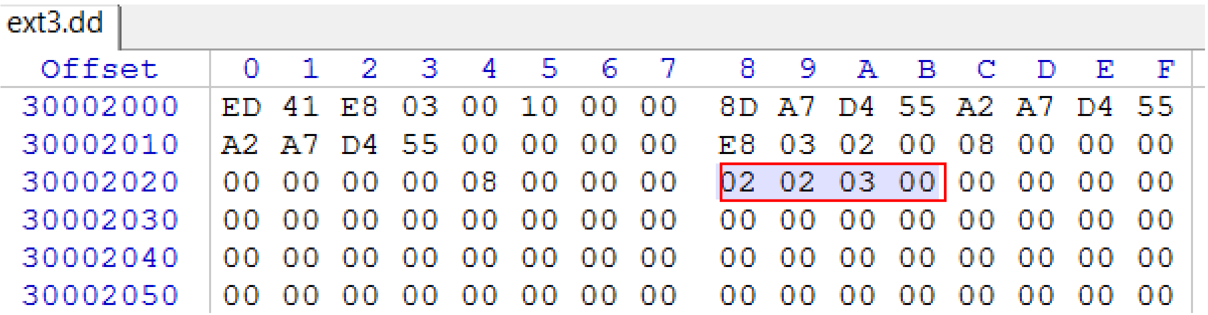


```
4256 41 80 02 00 42 80 02 00  43 80 02 00 BC 7D FD 1F  A€  B€  C€  ¼}ý
4272 01 00 04 00 00 00 00 00  00 00 00 00 00 00 00 00
4288 00 00 03 00 01 00 03 00  02 00 03 00 FD 7D FE 1F              ý}þ
4304 01 00 04 00 00 00 00 00  00 00 00 00 00 00 00 00
4320 41 80 03 00 42 80 03 00  43 80 03 00 BD 7D 00 20  A€  B€  C€  ½}
```

Figure 5 gdt 6번

Starting block address of inode table 0x8: 30002

0x30002 * 4096 = 0x30002000

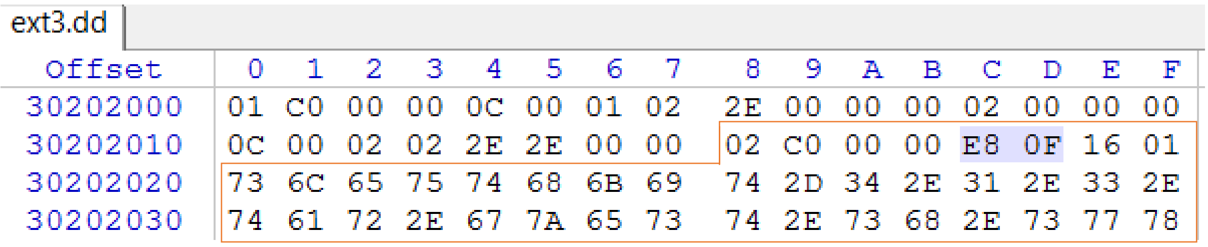


```
ext3.dd
  Offset    0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
 30002000  ED 41 E8 03 00 10 00 00  8D A7 D4 55 A2 A7 D4 55
 30002010  A2 A7 D4 55 00 00 00 00  E8 03 02 00 08 00 00 00
 30002020  00 00 00 00 08 00 00 00  02 02 03 00 00 00 00 00
 30002030  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
 30002040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
 30002050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
```

Figure 6 inode entry

Block pointers 0x28: 30202

Directory entry로 가야하니 0x30202 * 4096 = 0x30202000



```
ext3.dd
  Offset    0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
 30202000  01 C0 00 00 0C 00 01 02  2E 00 00 00 02 00 00 00
 30202010  0C 00 02 02 2E 2E 00 00  02 C0 00 00 E8 0F 16 01
 30202020  73 6C 65 75 74 68 6B 69  74 2D 34 2E 31 2E 33 2E
 30202030  74 61 72 2E 67 7A 65 73  74 2E 73 68 2E 73 77 78
```

Figure 7 directory entry

Inode 0x0: C002

Record Length 0x4: FE8

File length 0x6: 16

File type 0x7: 01

Name 0x8: sleuthkit-4.1.3.tar.gz