Lab3

Ext2 분석(디지털 포렌식)

과목명 : 운영체제
교수명 : 최종무 교수님
학 과 : 소프트웨어학과
학 번 : 32183698
이 름 : 이현기
제출일 : 2022/05/27

DKU 단국대학교 DANKOOK UNIVERSITY

1. 목표

이번 lab3에선 ext2 file system을 이해하고 직접 파일별 블록 5개를 접근하여 총 10개의 블럭을 찾는 과제이다. ramdisk를 이용하여 파일을 구성하고 학번 끝 세 자리에 해당하는 파일, 여기선 6번 디렉토리 안의 98, 89번 파일에 속한 블록들을 찾아내는 것이 이번 lab3의 목표이다. 여기서 Ext2(Extended file system)은 유닉스 파일시스템을 개선하여 만들어진 파일시스템으로 boot sector와 여러개의 블록들로 구성되있으며, 실린더 그룹으로 구성되있기도 하다. block group은 인접한 track들을 하나의 block group으로 묶어 관리하여 성능 향상에 도움이 된다. 디렉토리와 같이 논리적으로 연관성이 있는 data를 한 블록 그룹에 저장한다. superblock은 파일 시스템의 전반적인 정보를 가지고 있으며 ext2에서 각 블럭 그룹에 복제된 상태로 존재한다. group descriptor table은 각 블록 그룹에 대한 description을 나열한 테이블로 block bitmap, inode bitmap, inode table이 포함되있다. bitmap은 block이나 inode가 할당되었는지 표시하는 것이다. inode table은 블록 그룹들에 할당된 inode들을 나열한 테이블로 12개의 direct pointer와 3개의 indirect pointer로 구성되어있다. 여기서 root directory의 inode 번호는 2번이다. data는 파일 또는 디렉토리가 저장되는 공간이다.

2) 분석 결과 및 캡처

먼저 예시에 나온대로 super block을 분석하기 위해 출력한 결과이다.

```
root@oslab:/home/oslab/2022_DKU_OS/lab3_filesystem# xxd -g 4 -l 0x100 -s 0x400 /dev/ramdisk
00000400: 00800000 00000200 99190000 8ff70100  ................
00000410: f57f0000 00000000 02000000 02000000  ................
00000420: 00800000 00800000 00200000 c2628f62  ......... ...b.b
00000430: c2628f62 0100ffff 53ef0000 01000000  .b.b....S.......
00000440: ad628f62 00000000 00000000 01000000  .b.b............
00000450: 00000000 0b000000 00010000 38000000  ............8...
00000460: 02000000 03000000 d673e562 c86d4e0c  .........s.b.mN.
00000470: af76ae57 ee399e42 00000000 00000000  .v.W.9.B........
00000480: 00000000 00000000 2f686f6d 652f6f73  ......../home/os
00000490: 6c61622f 32303232 5f444b55 5f4f532f  lab/2022_DKU_OS/
000004a0: 6c616233 5f66696c 65737973 74656d2f  lab3_filesystem/
000004b0: 6d6e7400 00000000 00000000 00000000  mnt.............
000004c0: 00000000 00000000 00000000 00001f00  ................
000004d0: 00000000 00000000 00000000 00000000  ................
000004e0: 00000000 00000000 00000000 60114020  ............`.@
000004f0: 331b4563 aefeaf14 40a573db 01000000  3.Ec....@.s.....
root@oslab:/home/oslab/2022_DKU_OS/lab3_filesystem#
```

여기서 알 수 있는 사실로는 inode count:0x8000, block count: 0x20000, log block size: 0x2, blocks per group: 0x8000, inodes per group:0x2000, block group number:0x0임을 알 수 있다.

첫번째 group descriptor table을 분석하기 위해 출력한 결과이다.

```
root@oslab:/home/oslab/2022_DKU_OS/lab3_filesystem# xxd -g 4 -l 0x100 -s 0x1000 /dev/ramdisk
00001000: 21000000 22000000 23000000 d47dc61e  !..."...#....}..
00001010: 05000400 00000000 00000000 00000000  ................
00001020: 21800000 22800000 23800000 db7b361f  !..."...#....{6.
00001030: 02000400 00000000 00000000 00000000  ................
00001040: 00000100 01000100 02000100 5870361f  ............Xp6.
00001050: 02000400 00000000 00000000 00000000  ................
00001060: 21800100 22800100 23800100 da7dd11e  !..."...#....}..
00001070: 03000400 00000000 00000000 00000000  ................
00001080: 00000000 00000000 00000000 00000000  ................
00001090: 00000000 00000000 00000000 00000000  ................
000010a0: 00000000 00000000 00000000 00000000  ................
000010b0: 00000000 00000000 00000000 00000000  ................
000010c0: 00000000 00000000 00000000 00000000  ................
000010d0: 00000000 00000000 00000000 00000000  ................
000010e0: 00000000 00000000 00000000 00000000  ................
000010f0: 00000000 00000000 00000000 00000000  ................
```

여기서 알 수 있는 사실은 group 0의 block bitmap:0x21블록부터 시작하고, inode bitmap:0x22부터 시작하고 inode table:0x23부터 시작한다는 것을 알 수 있다.

inode table 영역을 분석하기 위해 캡처한 것이다.

```
00023100: ed410000 00100000 c2628f62 d3628f62  .A.......b.b.b.b
00023110: d3628f62 00000000 00000d00 08000000  .b.b............
00023120: 00000000 0a000000 23020000 00000000  ........#.......
00023130: 00000000 00000000 00000000 00000000  ................
00023140: 00000000 00000000 00000000 00000000  ................
00023150: 00000000 00000000 00000000 00000000  ................
00023160: 00000000 00000000 00000000 00000000  ................
00023170: 00000000 00000000 00000000 00000000  ................
00023180: 20000000 68e4d4e5 68e4d4e5 fc078d5f   ...h...h......_
00023190: ad628f62 00000000 00000000 00000000  .b.b............
000231a0: 00000000 00000000 00000000 00000000  ................
000231b0: 00000000 00000000 00000000 00000000  ................
000231c0: 00000000 00000000 00000000 00000000  ................
000231d0: 00000000 00000000 00000000 00000000  ................
000231e0: 00000000 00000000 00000000 00000000  ................
000231f0: 00000000 00000000 00000000 00000000  ................
```

여기서 알 수 있는 것은 mode:0x41ed=drwxr-xr-x이며 block pointer 0 : 0x223 block임을 알 수 있다.

data 영역을 분석하기 위해 캡처한 것이다.

```
root@oslab:/home/oslab/2022_DKU_OS/lab3_filesystem# xxd -g 4 -l 0x1000 -s 0x223000 /dev/ramdisk
00223000: 02000000 0c000102 2e000000 02000000  ................
00223010: 0c000202 2e2e0000 0b000000 14000a02  ................
00223020: 6c6f7374 2b666f75 6e640000 01400000  lost+found...@..
00223030: 0c000102 30000000 01200000 0c000102  ....0.... ......
00223040: 31000000 01600000 0c000102 32000000  1....`......2...
00223050: 0c000000 0c000102 33000000 71000000  ........3...q...
00223060: 0c000102 34000000 66200000 0c000102  ....4...f ......
00223070: 35000000 66600000 0c000102 36000000  5...f`......6...
00223080: 66400000 0c000102 37000000 cb600000  f@......7....`..
00223090: 0c000102 38000000 d6000000 680f0102  ....8.......h...
002230a0: 39000000 00000000 00000000 00000000  9...............
```

여기서 우리가 구해야하는 디렉토리는 6번 디렉토리이며 6번 디렉토리의 inode number = 0x6066, file type : 0x2 = directory임을 알 수 있다. 여기서 속한 block group: (0x6066-1)/0x2000 = 3번 block group이고, inode table index: (0x6066 - 1) % 0x2000 = 101임을 알 수 있다. 즉, 6번 디렉토리의 inode는 3번 block group의 inode table에서 101번째에 위치함을 알 수 있다.

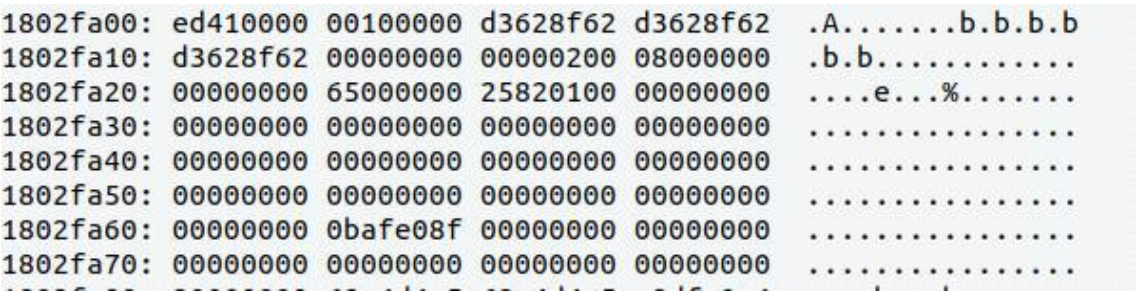
위에서 group descriptor block에서 3번 block group의 inode table이 0x18023으로 시작한다는 것을 알 수 있다. 0x18023을 시작하여 101번째에 위치한 것을 찾은 결과이다.

```
18029500: ed410000 00100000 d3628f62 d3628f62  .A.......b.b.b.b
18029510: d3628f62 00000000 00000200 08000000  .b.b............
18029520: 00000000 65000000 24820100 00000000  ....e...$.......
18029530: 00000000 00000000 00000000 00000000  ................
18029540: 00000000 00000000 00000000 00000000  ................
18029550: 00000000 00000000 00000000 00000000  ................
18029560: 00000000 80a6c572 00000000 00000000  .......r........
18029570: 00000000 00000000 00000000 00000000  ................
```

여기서 mode: 0x41ed = drwxr-xr-x이고, block pointer 0 = 0x18224 block임을 알 수 있다. 그래서 0x18224 block으로 이동한 결과는 다음과 같다.

```
182243e0: 38300000 b8600000 0c000201 38310000  80...`......81..
182243f0: b9600000 0c000201 38320000 ba600000  .`......82...`..
18224400: 0c000201 38330000 bb600000 0c000201  ....83...`......
18224410: 38340000 bc600000 0c000201 38350000  84...`......85..
18224420: bd600000 0c000201 38360000 be600000  .`......86...`..
18224430: 0c000201 38370000 bf600000 0c000201  ....87...`......
18224440: 38380000 c0600000 0c000201 38390000  88...`......89..
18224450: c1600000 0c000201 39300000 c2600000  .`......90...`..
18224460: 0c000201 39310000 c3600000 0c000201  ....91...`......
18224470: 39320000 c4600000 0c000201 39330000  92...`......93..
18224480: c5600000 0c000201 39340000 c6600000  .`......94...`..
18224490: 0c000201 39350000 c7600000 0c000201  ....95...`......
182244a0: 39360000 c8600000 0c000201 39370000  96...`......97..
182244b0: c9600000 0c000201 39380000 ca600000  .`......98...`..
182244c0: 440b0201 39390000 00000000 00000000  D...99..........
```

여기서 우리가 필요한 것은 89와 98이다. 먼저 89를 보면 inode number: 0x60c0, file type = 0x1 : regular file임을 알 수 있고, 98을 보면 inode number: 0x60c9, file type : 0x1 = regular file임을 알 수 있다.
여기서 89에 있던 inode number가 속한 block group : (0x60c0-1)/0x2000 = 3번 block group, inode table index = (0x60c0-1)/0x2000 = 191임을 알 수 있다.
3번 block group의 inode table에서 191번째에 위치한 것을 찾은 결과를 캡처한 것이다.



mode:0x41ed = drwxr-xr-x, block pointer 0: 0x18225임을 알 수 있다. block pointer로 이동하여보면 89번 inode number = 0x6125, file type: 0x01 = regular file임을 알 수 있다. 여기서 0x6125가 속한 block group:(0x6125-1)/0x2000 = 3번 block group, inode table index : (0x6125-1)%0x2000 = 292를 구할 수 있다. 여기서 3번 group의 inode table에 292번째에 위치한 것을 찾지 못하였다.

아까전에 98번 inode number인 0x60c9에서 block group : (0x60c9-1)/0x2000 = 3번 block group, inode table index = (0x60c9-1)%0x2000 = 200임을 알 수 있다. 3번 block group의 inode table에서 200번째에 위치한 것을 찾지 못하였다.

3. 논의

예시과정까지는 pdf에 나와있는대로 따라가면 되서 잘 수행했지만, 그 뒤에 6번 디렉토리의 98번, 89번 파일을 찾아가는 과정이 생각보다 많이 어려웠다. little endian을 big endian으로 바꾸는 것도 익숙치 않아 실습하면서 연산하는데 좀 헷갈렸다. 비록 파일을 끝까지 찾지 못하였지만, 이러한 방식으로 디지털 포렌식을 진행한다는 것이 신기했고, 그 과정이 생각보다도 더 복잡하다는 것을 알게 되었다. 이번 과제를 진행하며 파일이 저장되는 방식에 대해 직접 실습을 통해 더 잘 이해할 수 있었고, 평소 파일을 설치할 때는 클릭 한번이면 되지만, 컴퓨터 안에선 메모리에 inode를 할당하고 block을 만들고 하는 과정이 많이 복잡하게 이루어진다는 것을 잘 알게 되었다. 다음에도 기회가 있다면 이번보다 좀 더 쉽게 실습하여 결과를 얻을 수 있는 것들을 해보고 싶다.