

Pico CTF

Ext Super Magic





문제

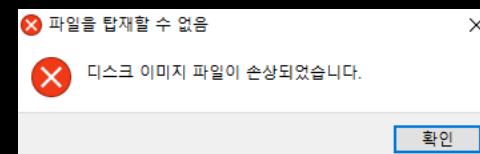
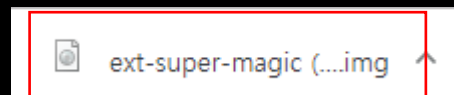
Ext Super Magic - Points: 250 - (Solves: 1317) Forensics - Solved

Solve Hints

We salvaged a ruined Ext SuperMagic II-class mech recently and pulled the filesystem out of the black box. It looks a bit corrupted, but maybe there's something interesting in there. You can also find it in `/problems/ext-super-magic_0_621bc2a94057a3e5a0aa0816da3fe8fb` on the shell server.

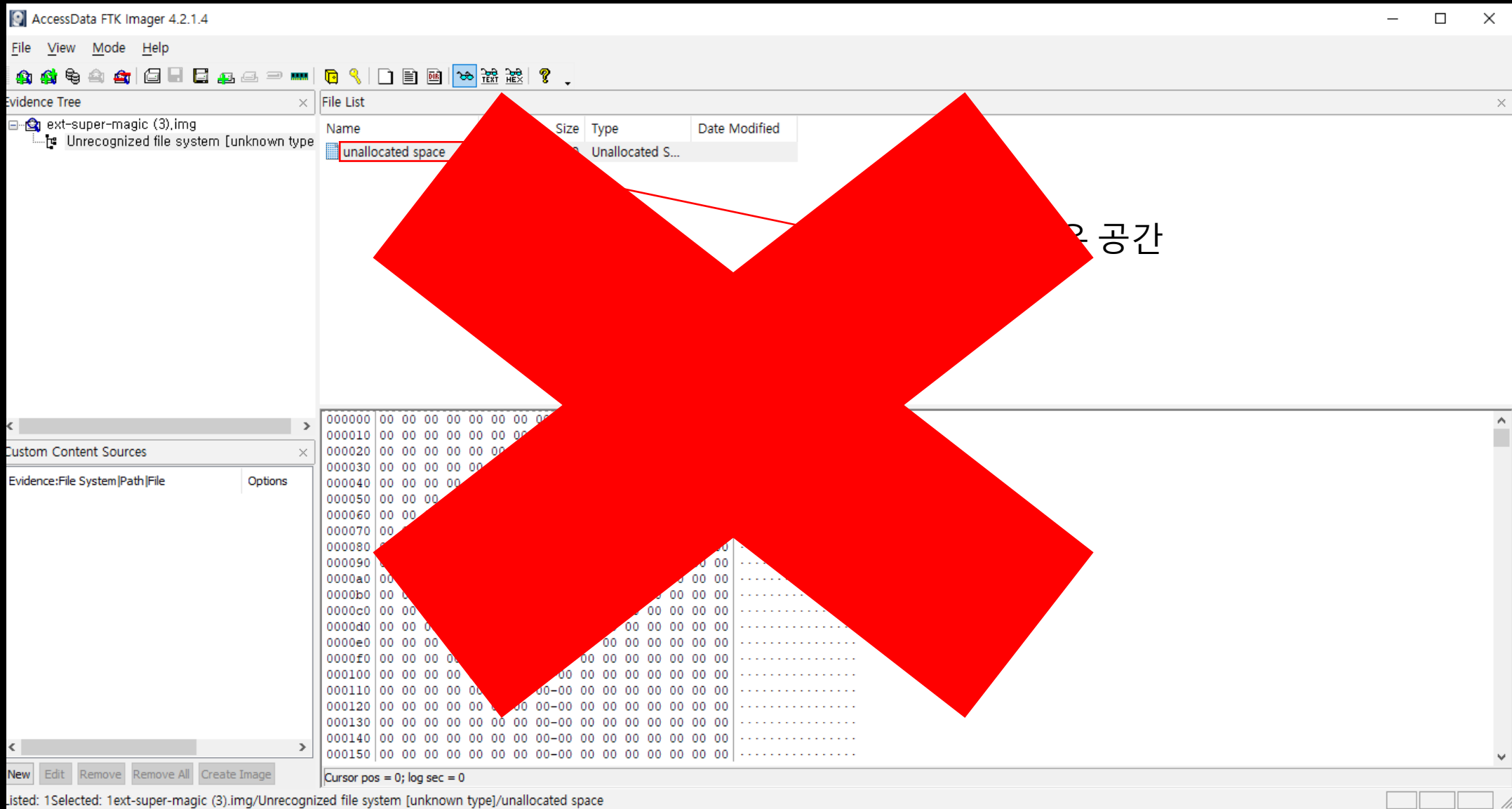
Submit!

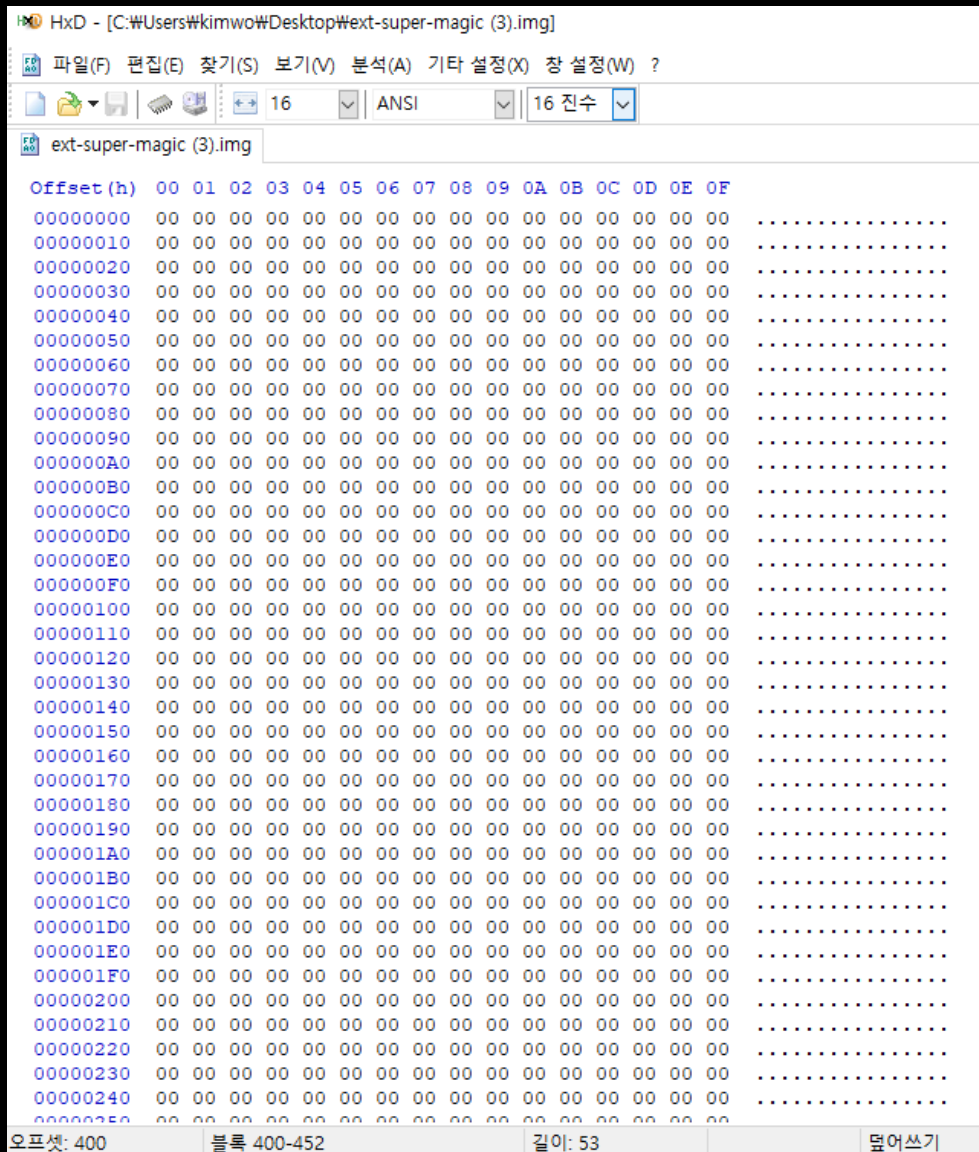
 



```
kwj@kwj-virtual-machine: ~/바탕화면
kwj@kwj-virtual-machine:~$ cd 바탕화면
kwj@kwj-virtual-machine:~/바탕화면$ ;s
dash: syntax error near unexpected token `;'
kwj@kwj-virtual-machine:~/바탕화면$ ls
ext-super-magic (3).img
kwj@kwj-virtual-machine:~/바탕화면$ foremost ext-super-magic\ \ (3\).img
Processing: ext-super-magic (3).img
[*]
kwj@kwj-virtual-machine:~/바탕화면$
```







Ext Super Magic - Points: 250 - (Solves: 1317)

Forensics - Solved

Solve

Hints

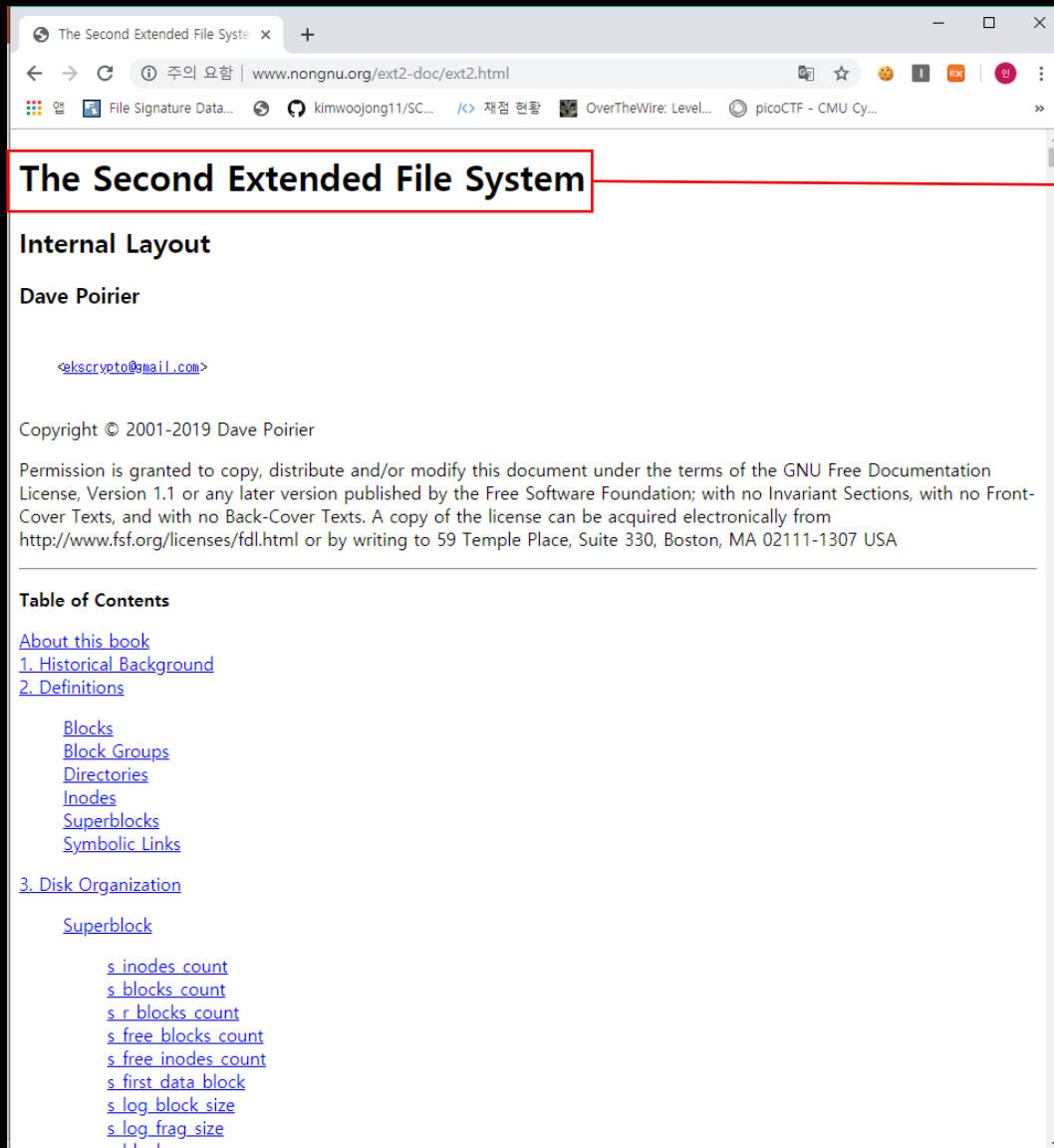
Are there any [tools](#) for diagnosing corrupted filesystems? What do they say if you run them on this one?

How does a linux machine know what [type](#) of file a [file](#) is?

You might find this [doc](#) helpful.

Be careful with [endianness](#) when making edits.

Once you've fixed the corruption, you can use `/sbin/debugfs` to pull the flag file out.



힌트 + 구글링

Ext2 (이차 확장 파일 시스템) : 리눅스 시스템 파일

Ext2 구글링 중 슈퍼블록이라는 것을 알게 됨

Ext2 슈퍼블록

- 슈퍼블록은 Ext2 파일시스템에서 사용되는 주요 설정 정보들이 기록되는 영역으로 블록 그룹의 첫 번째 블록에 위치한다.
- 슈퍼블록은 반드시 블록 그룹의 시작부터 1024Byte 내에 기록되어야 하며, 1024Byte의 크기로 저장되어야 한다.
- 사실상 1024Byte 중 실제 사용되는 영역 보다 사용되지 않은 영역이 더 많다.
- 슈퍼블록에는 파일 시스템의 설정 파일들이 기록되어 있고, 부트 코드가 기록되어 있지 않으며 슈퍼블록의 사본은 모든 블록 그룹들의 첫 번째 블록에 저장된다.
-
- - 슈퍼블록에 저장되는 주요 데이터
 - 1_ 블록의 크기(1KB, 2KB, 4KB)
 - 2_ 총 블록의 개수
 - 3_ 블록 그룹의 개수
 - 4_ Inode의 개수
 - 5_ 그룹 내의 블록/Inode의 개수

슈퍼블록의 시 그니처 값

- 슈퍼블록의 구조 분석을 보던 중 슈퍼블록에는 시그니처 값이 있다는 것을 알게 됨!
- 슈퍼블록의 시그니처 값 = 오프셋 값 56(0x38)에 0xEF53 이라고 함

[illegible]

HxD - [C:\Users\kimwo\Desktop\ext-super-magic (3).img]

파일(F) 편집(E) 찾기(S) 보기(V) 분석(A) 기타 설정(X) 창 설정(W) ?

16 ANSI 16 진수

ext-super-magic (3).img

| Offset (h) | 00 | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 0A | 0B | 0C | 0D | 0E | 0F | |
|------------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|--------------------|
| 00000400 | 00 | 05 | 00 | 00 | 00 | 14 | 00 | 00 | 00 | 01 | 00 | 00 | 57 | 05 | 00 | 00 |W... |
| 00000410 | 00 | 03 | 00 | 00 | 01 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |i (TM\ |
| 00000420 | 00 | 20 | 00 | 00 | 00 | 20 | 00 | 00 | 00 | 05 | 00 | 00 | A1 | 28 | 99 | 5C |i (TM\ |
| 00000430 | A7 | 28 | 99 | 5C | 01 | 00 | FF | FF | 53 | EF | 01 | 00 | 01 | 00 | 00 | 00 | S (TM\..yySi..... |
| 00000440 | A1 | 28 | 99 | 5C | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 01 | 00 | 00 | 00 | i (TM\ |
| 00000450 | 00 | 00 | 00 | 00 | 0B | 00 | 00 | 00 | 80 | 00 | 00 | 00 | 38 | 02 | 00 | 00 |€...8... |
| 00000460 | 02 | 00 | 00 | 00 | 03 | 00 | 00 | 00 | F1 | 00 | 55 | CF | 29 | 2C | 4B | 9C |f.Uİ), Koe |
| 00000470 | 82 | 38 | 14 | 3E | 1F | 85 | BD | D2 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | ,8.Ö. |
| 00000480 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 00000490 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 000004A0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 000004B0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 000004C0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 13 | |
| 000004D0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 000004E0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | FE | D2 | 6C | 09 |p01. |
| 000004F0 | 11 | 3F | 4D | 13 | 86 | 93 | 5C | 3B | 56 | A1 | F0 | 92 | 01 | 00 | 00 | 00 | ..?M.+""\;V;8'.... |
| 00000500 | 0C | 00 | 00 | 00 | 00 | 00 | 00 | 00 | A1 | 28 | 99 | 5C | 00 | 00 | 00 | 00 |i (TM\ |
| 00000510 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 00000520 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 00000530 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 00000540 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 00000550 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 00000560 | 01 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 00000570 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 72 | 0E | 00 | 00 | 00 | 00 | 00 | 00 |F..... |
| 00000580 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 00000590 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 000005A0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 000005B0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 000005C0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 000005D0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 000005E0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 000005F0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 00000600 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 00000610 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 00000620 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 00000630 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 00000640 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 00000650 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |

오프셋: 43A

읽어쓰기

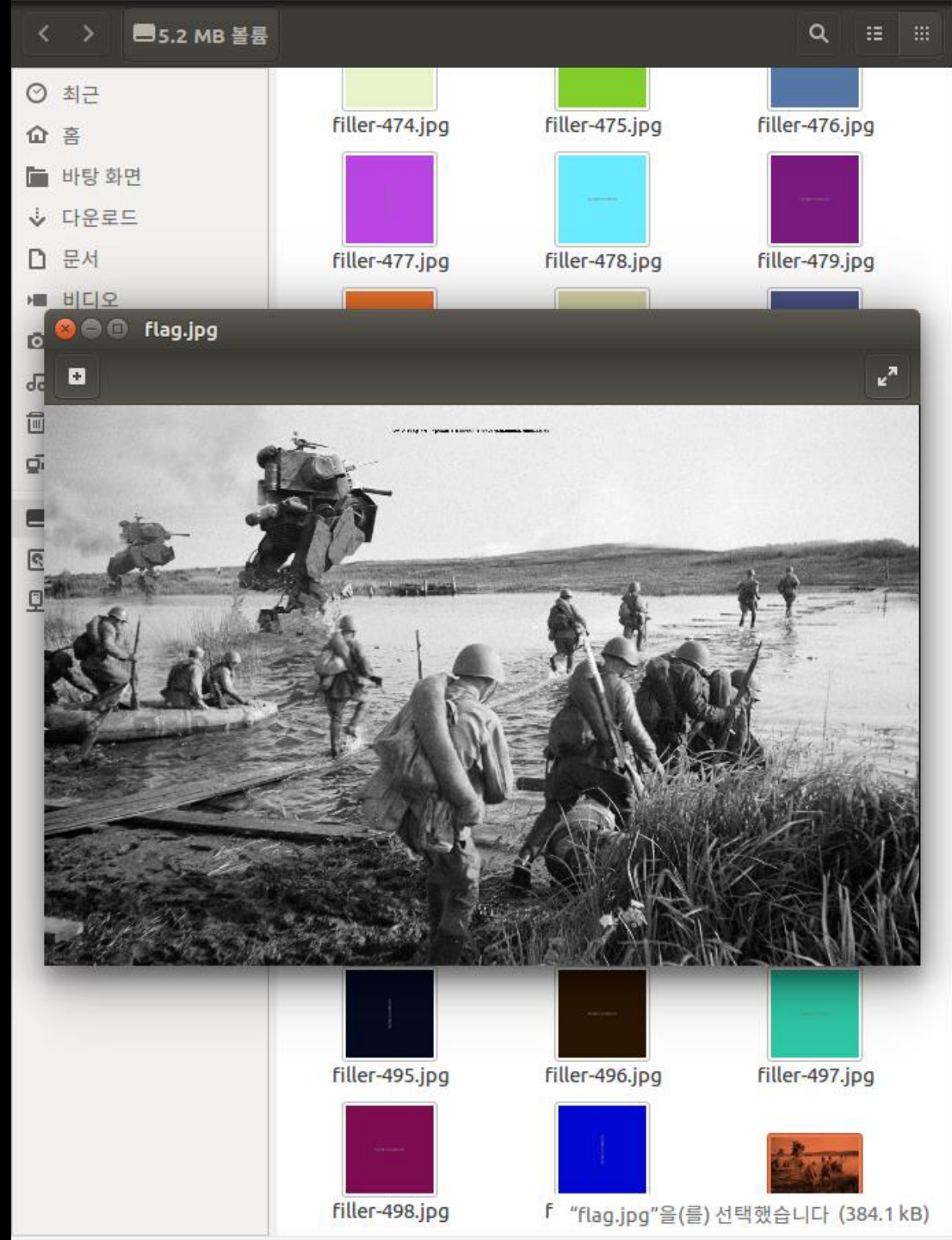
오프셋 값 400부터 입력이 시작되어서 여기를
첫번째 블록이라고 가정하고 400을 0이라 한뒤
오프셋 값 56(0x38)을 봄

0xEF53 이어야 할 값이 0x0000 으로 되어 있음

그래서 바꾸어줌

리눅스 마운트

```
root@kwj-virtual-machine:/home/kwj/바탕화면# mount ext-super-magic\ |(3\).i  
mg dir  
root@kwj-virtual-machine:/home/kwj/바탕화면#
```





Q&A
