

anti-hack10

这道题和上一题有些类似，但是这道题是从硬盘内容中提取数据。首先进入Ubuntu尝试

```
mount disk.img
```

挂载该镜像，提示错误。于是使用：

```
debugfs disk.img
```

提示其superblock中的magic number出现错误。经过网上的搜索，可以看到magic number是表示文件系统格式的一个2 Bytes的数字。如ext2文件系统的magic number就是EF 53。使用16进制编辑器打开之后发现对应magic number的数据为53 EF。修改顺序后，再次使用debugfs打开，仍然提示错误，但是此时会显示备份块的位置。

使用16进制编辑器将备份的superblock移动到初始位置(1024)，并修改magic number，再次使用debugfs打开，发现仍然提示错误.....

不过这个时候使用file disk.img指令已经可以正常显示其文件系统格式和UUID了，于是我再次使用debugfs指令打开，在其中输入ls，发现它能够显示出文件系统内的目录了。经过一番搜查，终于在usr文件夹内发现了一个名字叫做.flag.swp的文件，看起来像是使用vim的时候没有保存的临时文件。

使用cat .flag.swp命令打开该文件，发现了一串编码，末尾是=符号。考虑base64编码，使用在线解码器进行解码，得到flag。