MISC常用资料

图片隐写术：

http://bobao.360.cn/learning/detail/243.html

MP3隐写：

MP3stego，需要密码

压缩文件解密：

详见http://www.360zhijia.com/360anquanke/217342.html

密码爆破：

Advanced RAR Password Recovery（公司电脑中有正版）

CRC32爆破：

压缩包内存在小文件时，可以自行生成文件与相应文件的CRC校验码进行比对，可以猜测出小文件中的字符内容

明文攻击：

得到加密压缩包中的某个文件后，便可以利用。使用Advanced RAR Password Recovery，可以将压缩包还原为无密码压缩文件。

伪加密

```
（1）在Mac OS及部分Linux（如Kali）系统中，可以直接打开伪加密的zip压缩包
（2）使用检测伪加密的ZipCenOp.jar，解密后如果能成功打开zip包，则是伪加密，否则说明思路错误
```

（3）使用16进制编辑器改回加密标记位

缺省文件分析：

如缺少文件头，文件需要修复，报文分析等。

游戏分析：

使用相应游戏版本打开存档，寻找与原版不同的地方，被篡改的地方可能就有flag。

流量分析：

https://blog.csdn.net/qq1124794084/article/details/79150285