i春秋网鼎杯网络安全大赛clip题目writeup

原创

iqiqiya 于 2018-08-21 19:51:23 发布 10139 收藏 3
分类专栏： 我的CTF之路 ------2018i春秋网鼎杯 我的CTF进阶之路 文章标签： 网鼎杯网络安全大赛clip题目writeup clip writeup MISC


我的CTF之路 同时被 3 个专栏收录
92 篇文章 5 订阅
订阅专栏


------2018i春秋网鼎杯
6 篇文章 0 订阅
订阅专栏

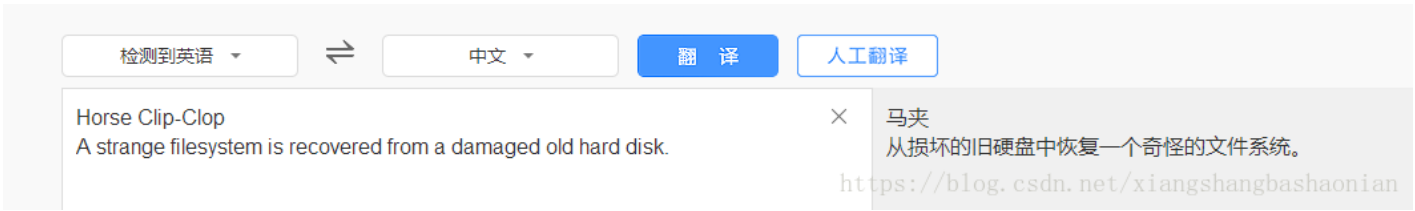
我的CTF进阶之路
108 篇文章 18 订阅
订阅专栏

题目信息：

下载下来是一个压缩包 解压之后可以得到两个文件

下载链接： https://pan.baidu.com/s/1k4UXTq8hYpwGLVzNa9lVEg 密码: 9was

先查看desc.txt的内容并翻译



可以看出damaged.disk是一个磁盘文件

那么里边肯定有东西！

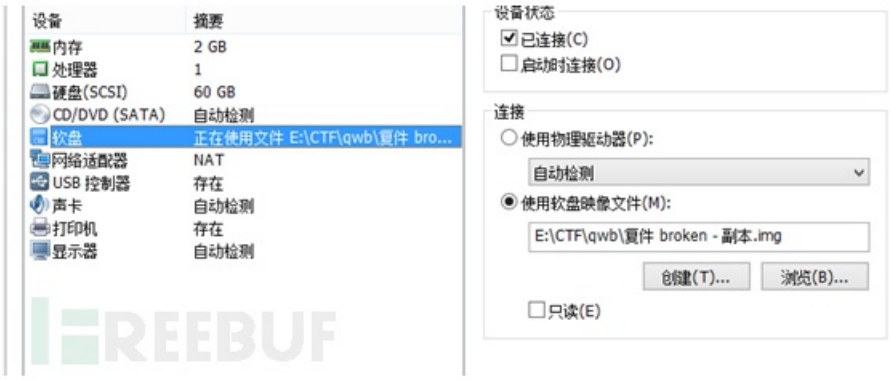
尝试将其放进kali linux用binwalk分析 foremost提取都无果。。。

各种百度damaged Boken

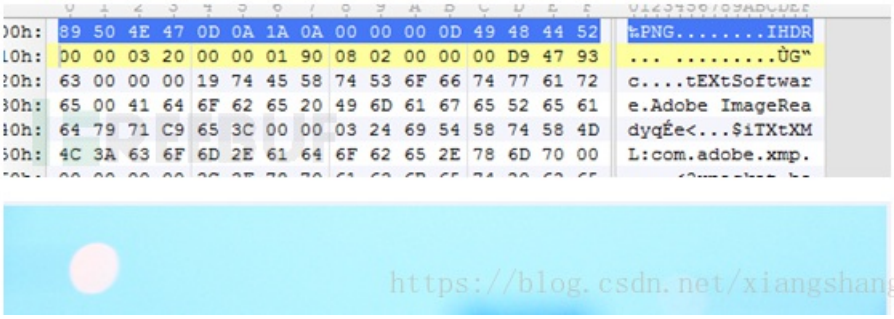
找到一篇类似题目(强网杯的)

Broken

什么都是坏的，找了个正常的引导区直接winhex覆盖头，发现启动不了，通过vmware在windows下挂载软盘镜像或者直接winhex打开，可以找到几个文件：



Flag文件拿下来，补上png的文件头：



开脑洞，调大长度，拿到flag：

那么上winhex分析

根据**PNG文件格式中的数据块格式**

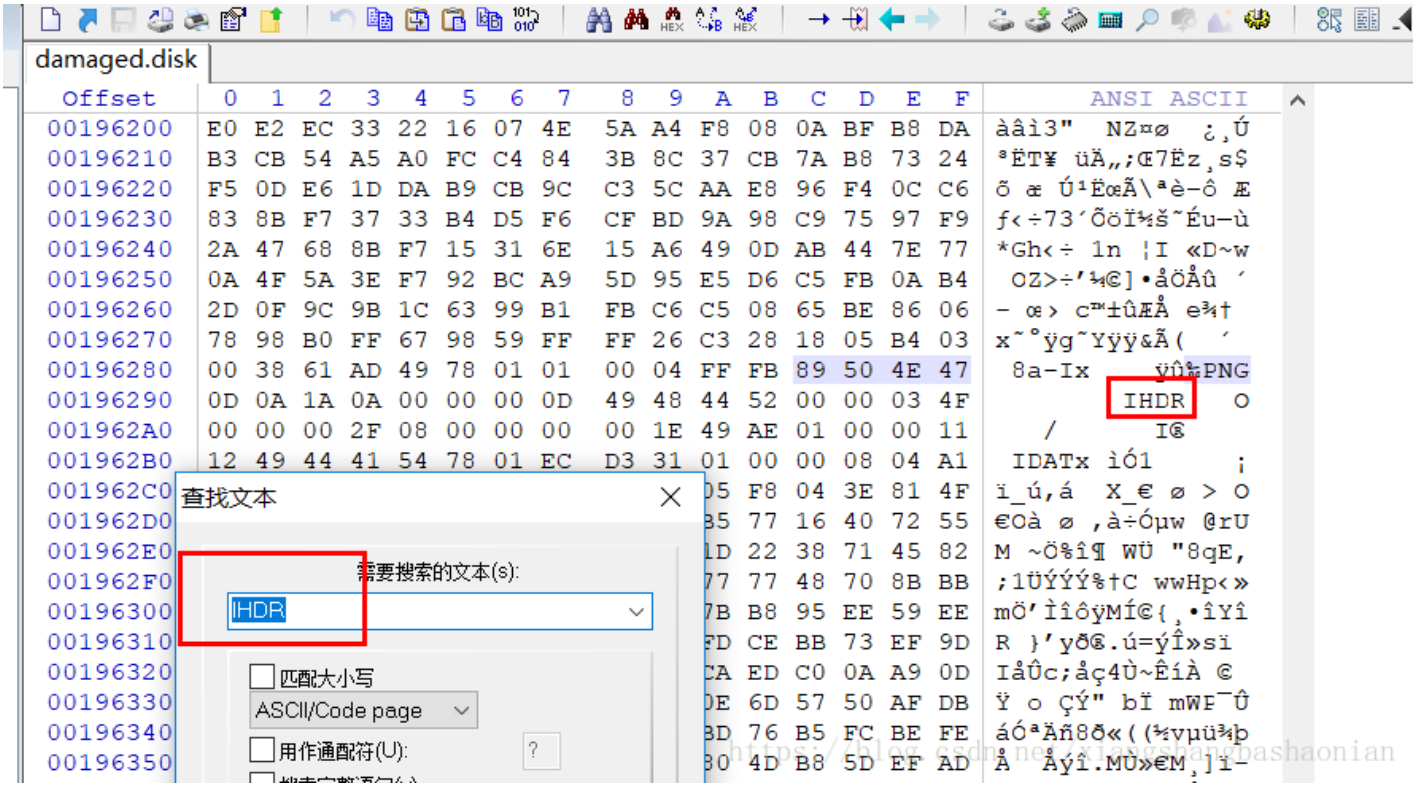
PNG文件格式中的数据块				
数据块符号	数据块名称	多数据块	可选否	位置限制
IHDR	文件头数据块	否	否	第一块

PNG图片文件头和文件尾格式

PNG (png), 文件头：89504E47 文件尾：AE 42 60 82

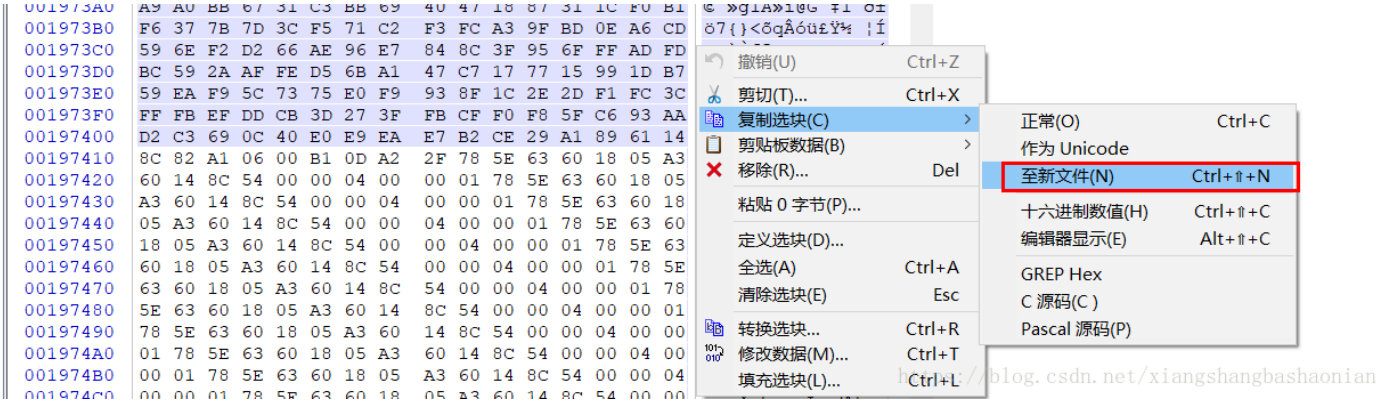
我们直接ctrl+F搜索文本IHDR

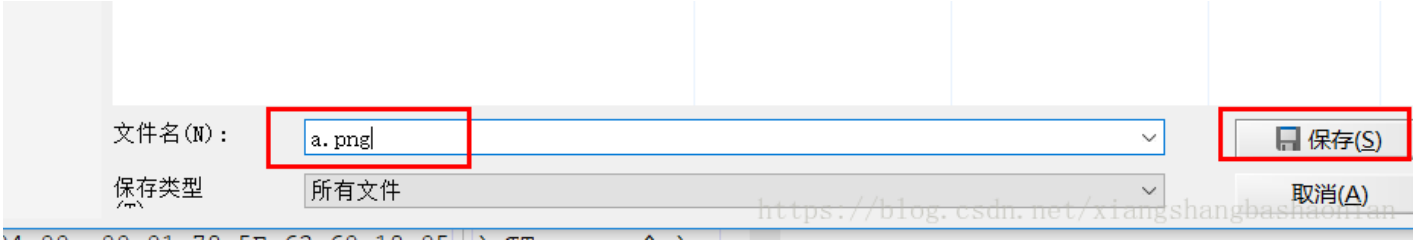
这是第一个图片



这里会出现搜索不到文件尾的情况　直接从89 50 4E 47选中到00197400这一行结尾就好

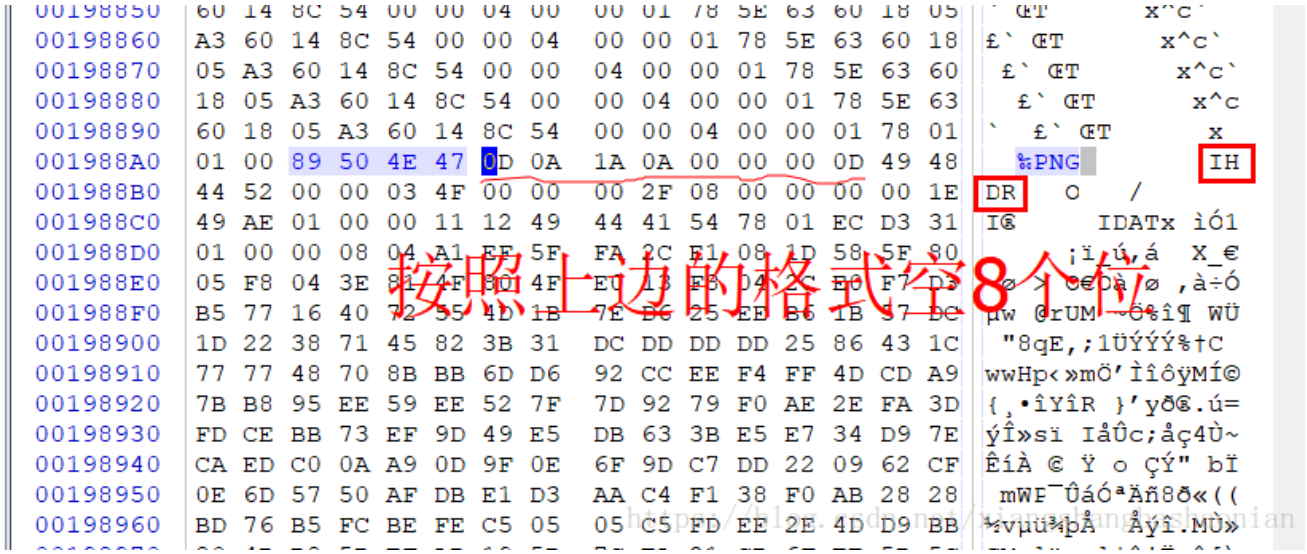
然后右键编辑à复制选块à至新文件à重命名保存

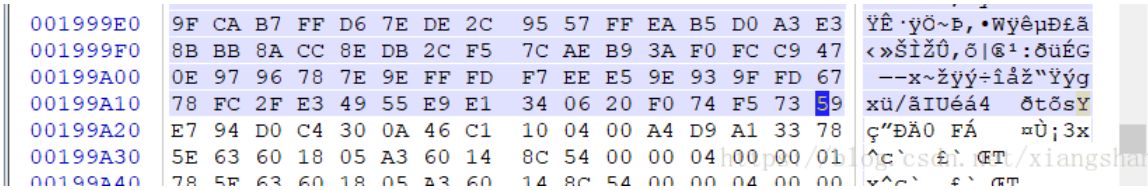




按F3继续向下搜索

找到第二张图片　但是PNG文件头不完整　补齐89 50 4E 47 0D

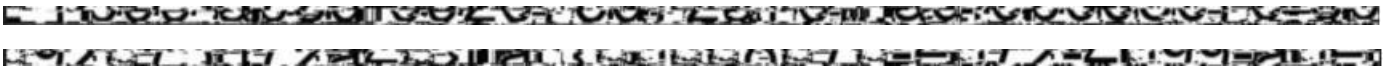




选中到这里结束就好 保存成b.png

接着对比两张图片

然后进行切图 拼图(ps大法好)



最后得到flag