2022第二届网刃杯网络安全大赛-MISC

原创

夜白君 于 2022-04-25 09:26:04 发布 384 收藏 1

分类专栏： 2022第二届网刃杯网络安全大赛 文章标签： 网络安全 Misc 2022第二届网刃杯 CTF

本文链接：https://blog.csdn.net/qq_43264813/article/details/124397167

2022第二届网刃杯网络安全大赛 专栏收录该内容

4 篇文章 36 订阅

订阅专栏

系列文章目录

前言

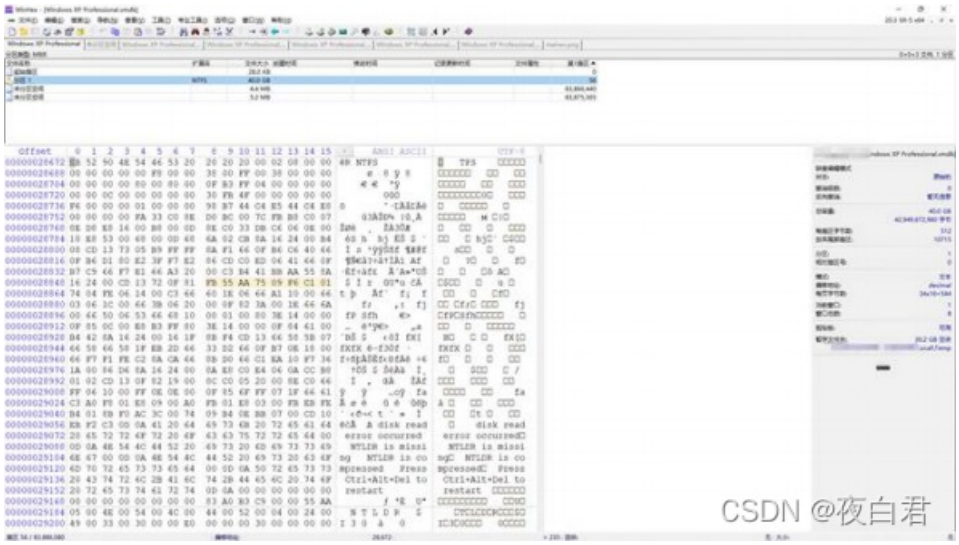
`提示：该内容由夜刃TEOT战队-sn0w师傅原创，禁止抄袭！

一、MISC-玩坏的winxp

难度系数：4.0

题目描述：小敏的电脑Windows XP Professional不小心被玩坏了，里边有重要的东西，你能帮帮她吗？

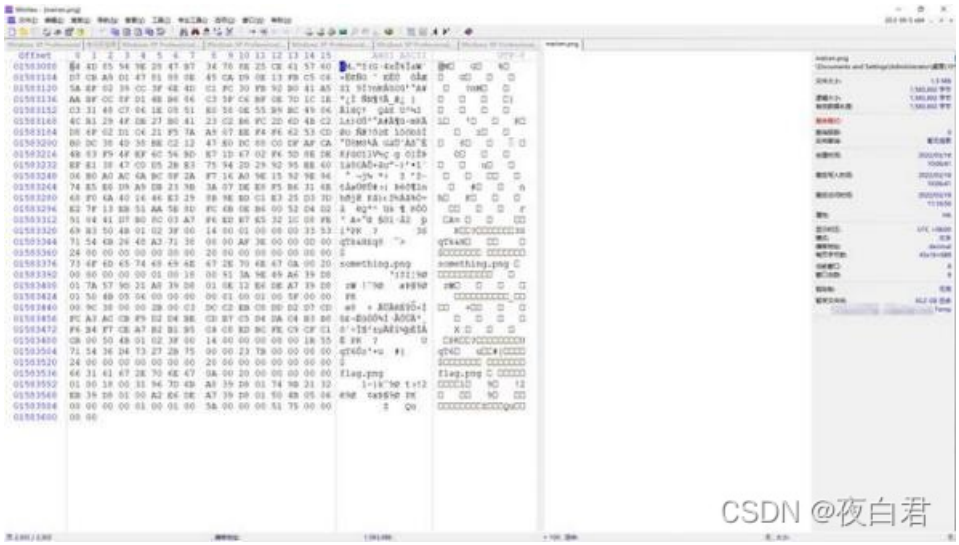
看到vmdk本能的去vm挂载，但是报错打不开，不能挂载，尝试了几次就不想浪费时间了，简单的搜寻之后，winhex也能挂，就挂到winhex下看看



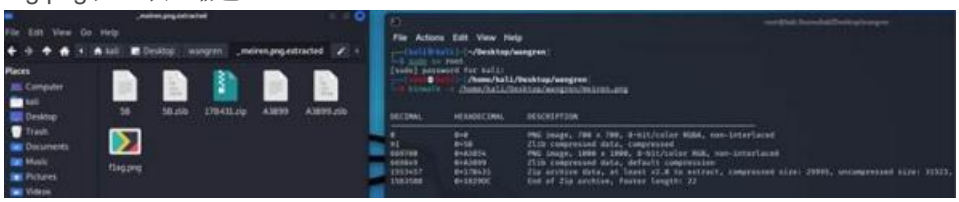
进到分区1里面，先找桌面看有没有有用的信息，看到桌面有个名为“10个t的学习资料”

里面是5个图片，把他们都导出来看看，直接另存为

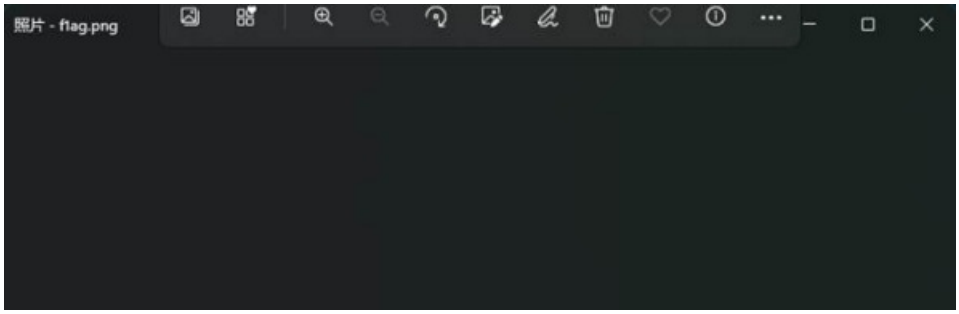
得到了5张图片，每个图直接在winhex里面看看有没有隐藏的文件，看到最后一张图，meiren.png下面有个flag.png，试着用kali分离出来



分离之后看到一个flag.png和一个压缩包

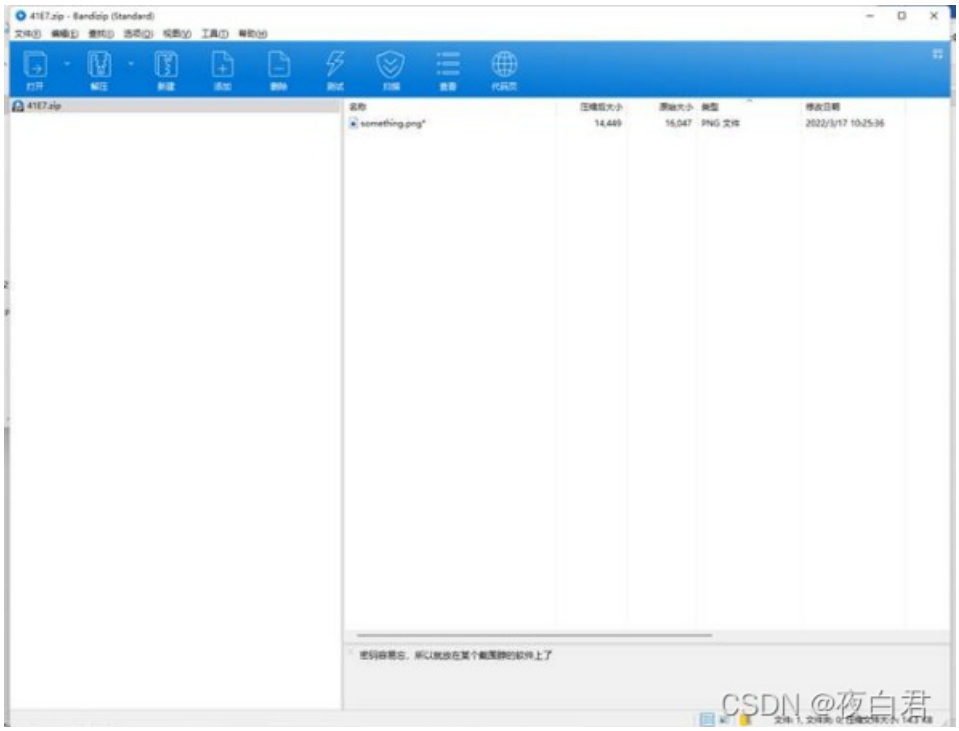


Flag.png什么都没有

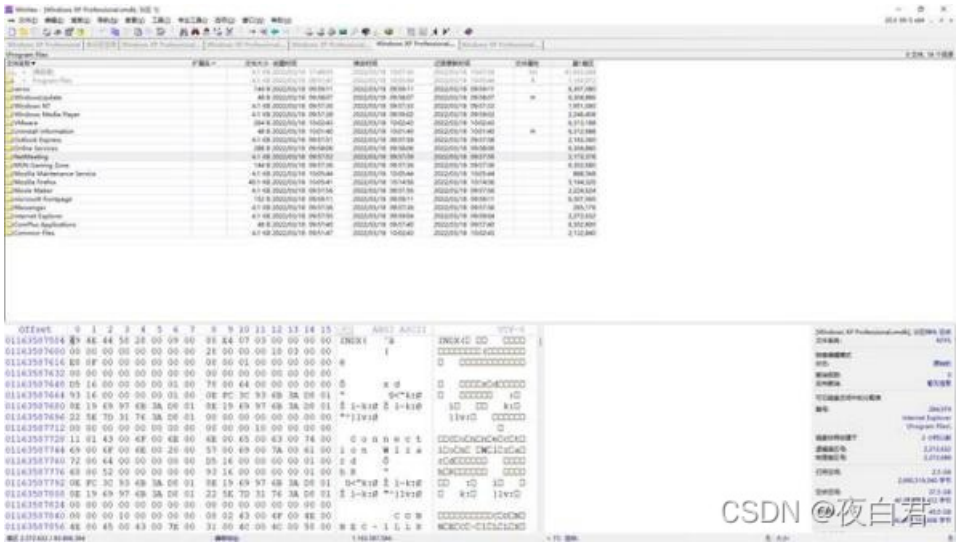


看一下压缩包，里面还有个图，把两个图试着再分离一下

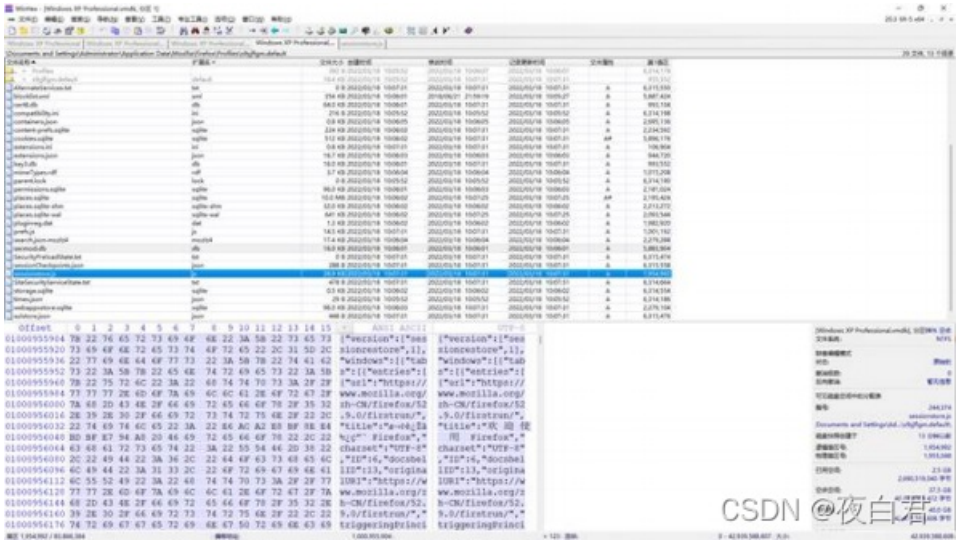
又是一个压缩包和图片，套娃能不能爬阿，打开压缩包，下面有个提示



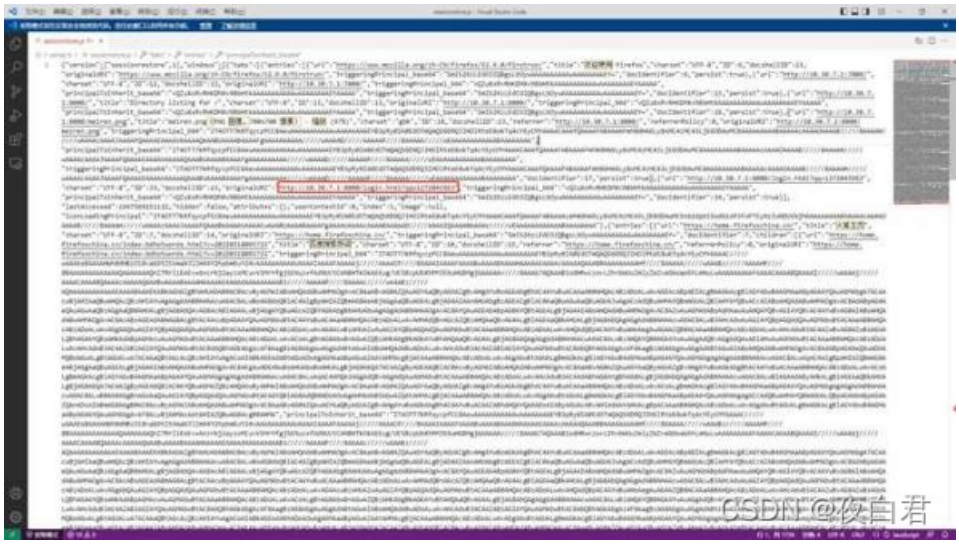
他说密码容易忘，所以就放在某个戴围脖的软件上了，那就回到winhex上继续翻他的软件目录，找有没有这个关键得围脖软件



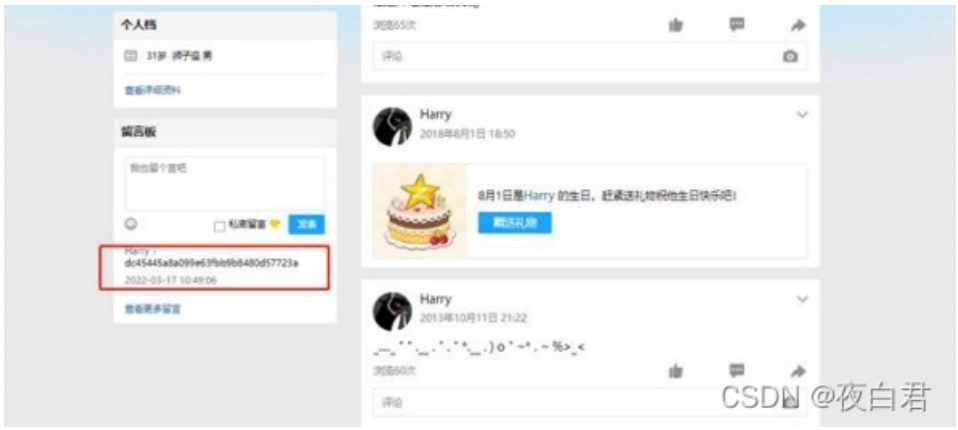
这就是他所有得软件了，看到这些，根据提示和我自己的对比，应该是他这个火狐浏览器了，是浏览器的话，就去看看他的历史浏览记录啥的，看看有没有发现



看到他的界面，恢复出来这个js看看



看到一个qq号，原来带围脖的软件是qq，那搜一下这个qq号，看到空间的动态更加确信了自己的推想，看到留言了一串代码



复制下来直接去md5解密

解密出来是xiaomi520，解开压缩包，得到flag