1.杂项\_42

压缩包里是很多小的压缩包，解压要密码，但找不到提示线索。binwalk扫描发现zip中夹带一张图片，分离出来，在linux虚拟机中看不出什么(右边)，但放到windows下就可以看到flag了（左边）

2.杂项\_暗中观察

看到dump下意识以为是内存取证，不过binwalk跑完后发现应该流量分析得题。导出http对象列表，发现有一个flag.zip。解压需要密码，追踪tcp流，可以看到登陆数据包，并截获登陆密码为:“eqtbz=ctfshowys168com” 使用登陆密码进行解压缩即可得到flag

3.杂项\_《JOJO的奇妙冒险》

解压需要密码，hint是：标准结局。百度搜了下，可能是最近得热门词“to be continue”,果然密码是“tobecontinue”； 解压得到flag文件，接近300M，查看后发现是16进制字符，转为二进制文件, 使用EmEditor 替换0xa 为 0x0a “ ”为“” 然后替换”0x” 为 “”

得到16进制文本，使用HxD 生成二进制文件

提示密码：JOESTAR进行解压，得到文件virt.qcow2，根据后缀名可以判断是qumu文件使用软件qumu（硬件模拟器）打开，此时缺少uefi，从kali里面复制/usr/share/OVMF/OVMF.fd出来到qemu根目录uefi

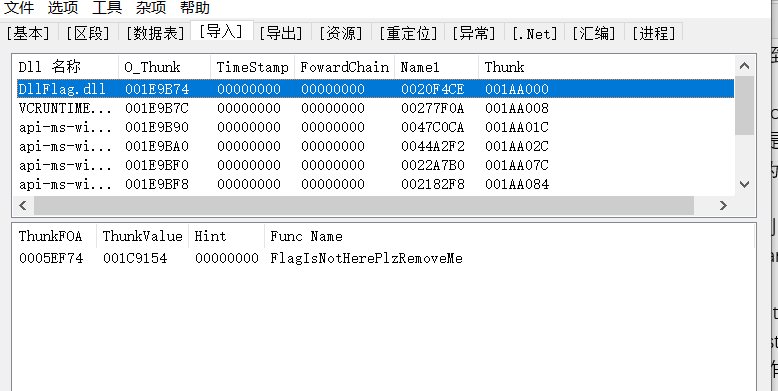
新建批处理文件，配置虚拟机启动参数后启动，使用用户名root，密码tobecontinue登陆

重启虚拟机，加入init参数，mount命令挂载分区到/mnt，修改/mnt/etc/fstab中 / 的uuid，poweroff关闭虚拟机，删除cdrom，最后重启，系统恢复正常，查看操作记录，在/boot/efi中得到flag

4.RunTheEXE

把压缩包里的RunToGetFlag.exe拖进studyPE里

删除DllFlag.dll



修改完后保存，再运行RunToGetFlag.exe即可得到flag

5.签到题

根据提示加群，在群中的资料信息可以找到flag

6.爱拼才会赢

拼图题，23\*13的拼图看着不多，才298块，原题给出了原图和拼图碎片，可以通过比较图片色值的方法“自动拼图”（原图可能需要稍作处理），然后串联文件名得到flag。由于碎片图片文件名是有规律的，感觉这是可行的解题方法，通过js了解验证逻辑和flag计算方法然后自行代码实现“拼图”。但最后并不能得到flag，迷惑了很久。等官方wp出了之后才知道

出题者为了防止根据文件名进行拼图，在使用碎片之前已经随机打散了一次，所以这条路是不通的。