# 一、题目描述

题目链接：[比赛关卡-第五届“强网杯”全国网络安全挑战赛（线上赛） (ichunqiu.com)](https://ctf.ichunqiu.com/2021qwb)

题目来源平台：2021年强网杯

题目名称：CipherMan

题目描述：磁盘内存分析

题目类型：MISC

题目附件：[CipherMan.7z\_免费高速下载|百度网盘-分享无限制 (baidu.com)](https://pan.baidu.com/s/1G2zgTROW7-h7nZ0Cfct-4g)

FLAG：Wow, you have a great ability. How did you solve this? Are you a hacker? Please give me a lesson later.

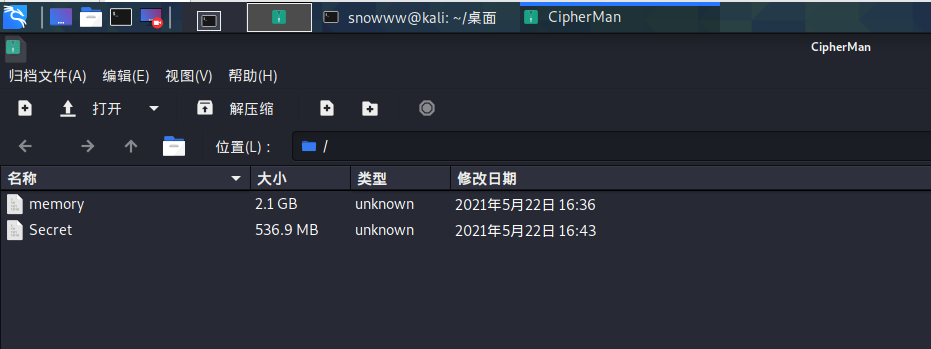
# 二、解题工具

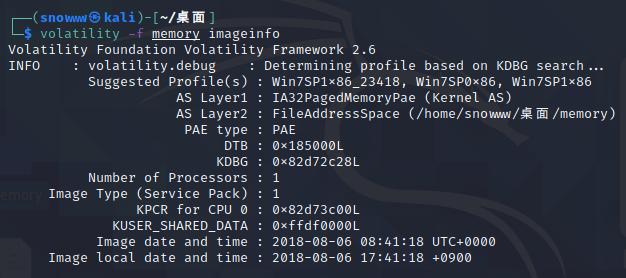
|  |  |  |  |
| --- | --- | --- | --- |
| 工具类型 | 工具名称 | 版本 | 备注 |
| 基础环境 | Linux system |  |  |
|  |  |  |
| 工具 | Volatility | 2.6 |  |
|  |  |  |

# 三、解题过程

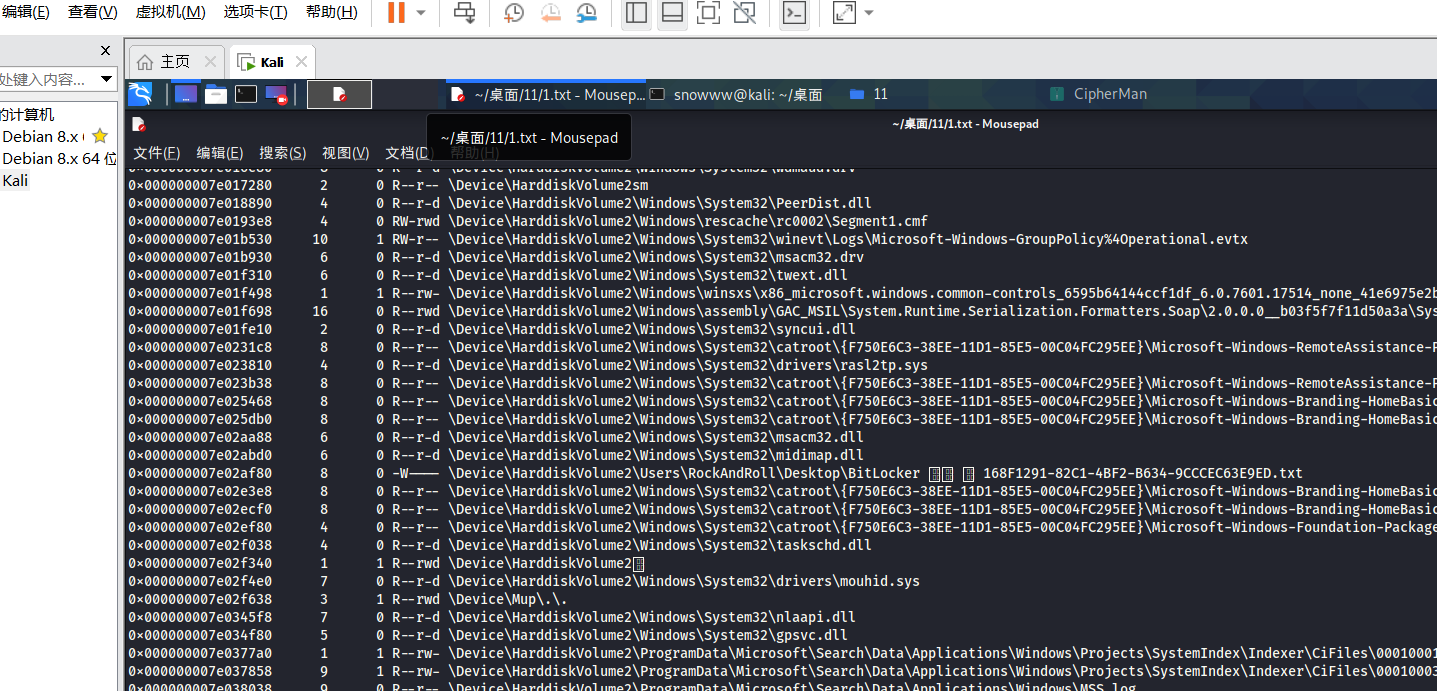
（详细说明CTF赛题的解题过程，分步骤说明）

### 步骤1 把文件拖进kali，发现有一个磁盘镜像和内存镜像

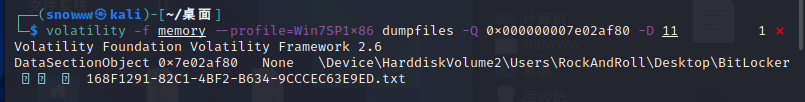


步骤2 使用工具volatility运用指令volatility-f memory imageinfo查看镜像的系统信息，得到了电脑版本为Win7SP1x86

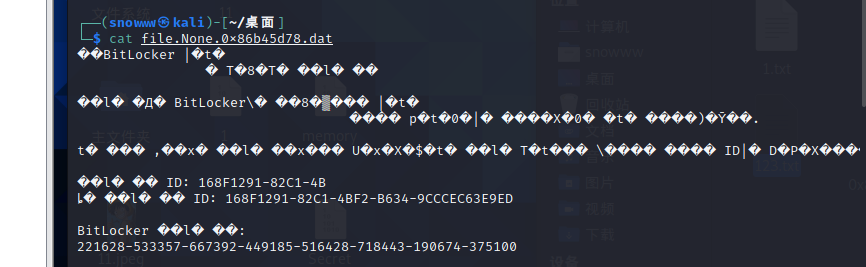
步骤3 在桌面创建文件夹命名为11，使用工具volatility运用指令volatility -f memory --profile=Win7SP1x86 filescan>11/1.txt将结果重导向于文档里，在结果搜索.txt文档，有一串字符不能识别，发现是BitLocker密钥文件



### 步骤4使用指令volatility -f memory --profile=Win7SP1 dumpfiles -Q 0x000000007e02af80 -D 11导出

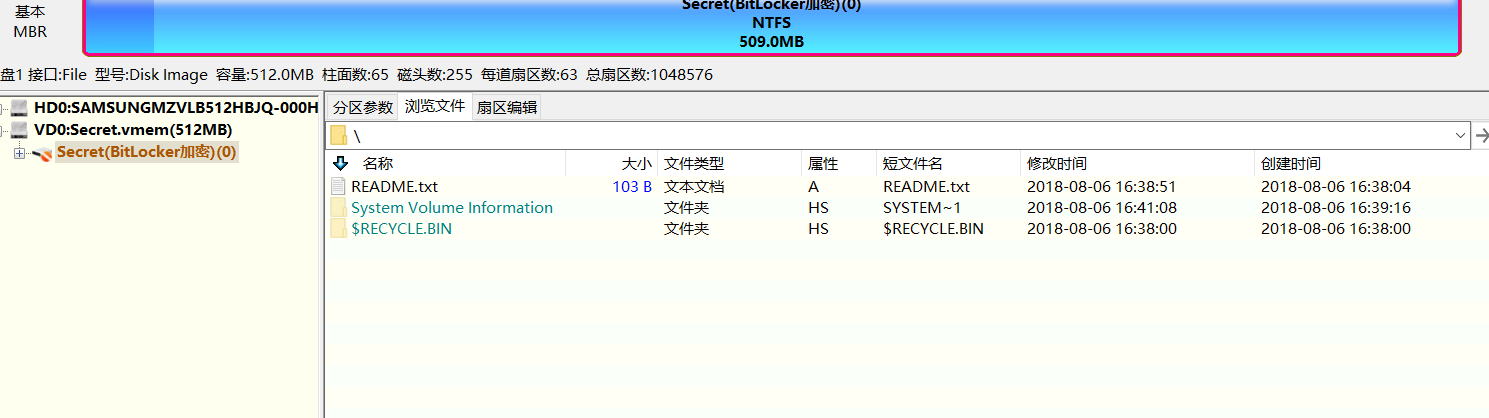


**得到**



**步骤5**

**使用软件DiskGenius打开文件secret，输入恢复密钥**



**打开README.txt,得到flag**

