**题目名称：内存取证**

**类型：Misc**

**介绍：**

内存取证

* 解析 Windows / Linux / Mac OS X 内存结构
* 分析进程，内存数据
* 根据题目提示寻找线索和思路，提取分析指定进程的特定内存数据

本题为Windows下的一次简单内存取证。

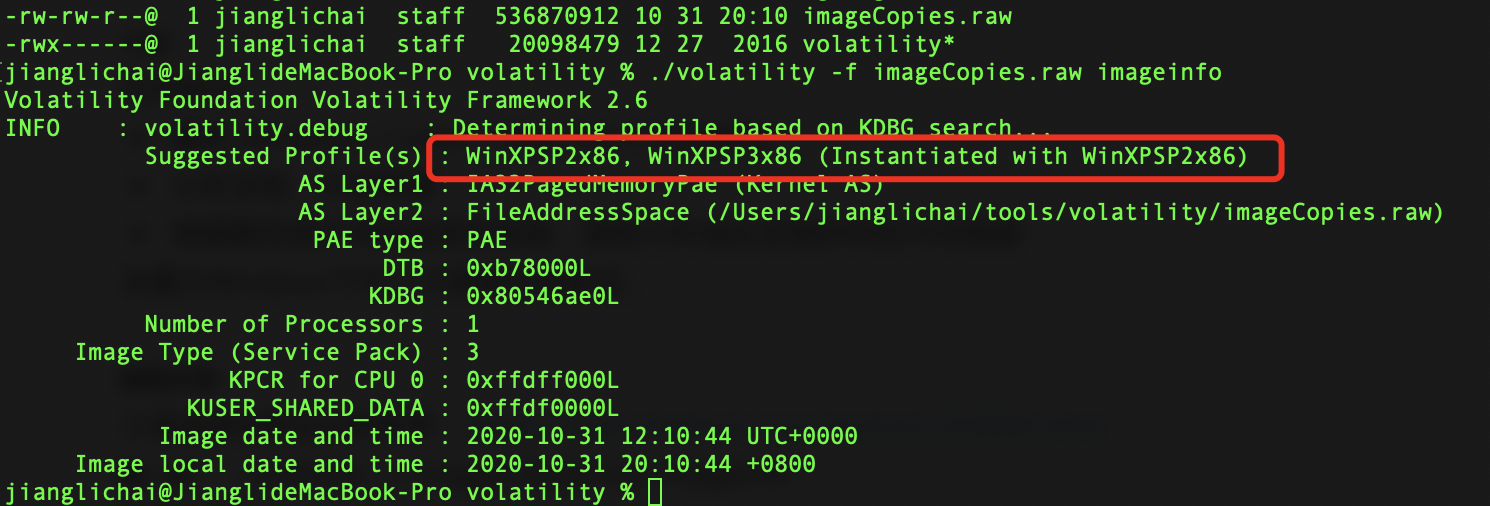
**解题步骤：**

工具安装&取证分析参考：<https://www.freebuf.com/sectool/124690.html>

**第一步：**./volatility -f imageCopies.raw imageinfo

查看镜像信息

主要是为了获取profile

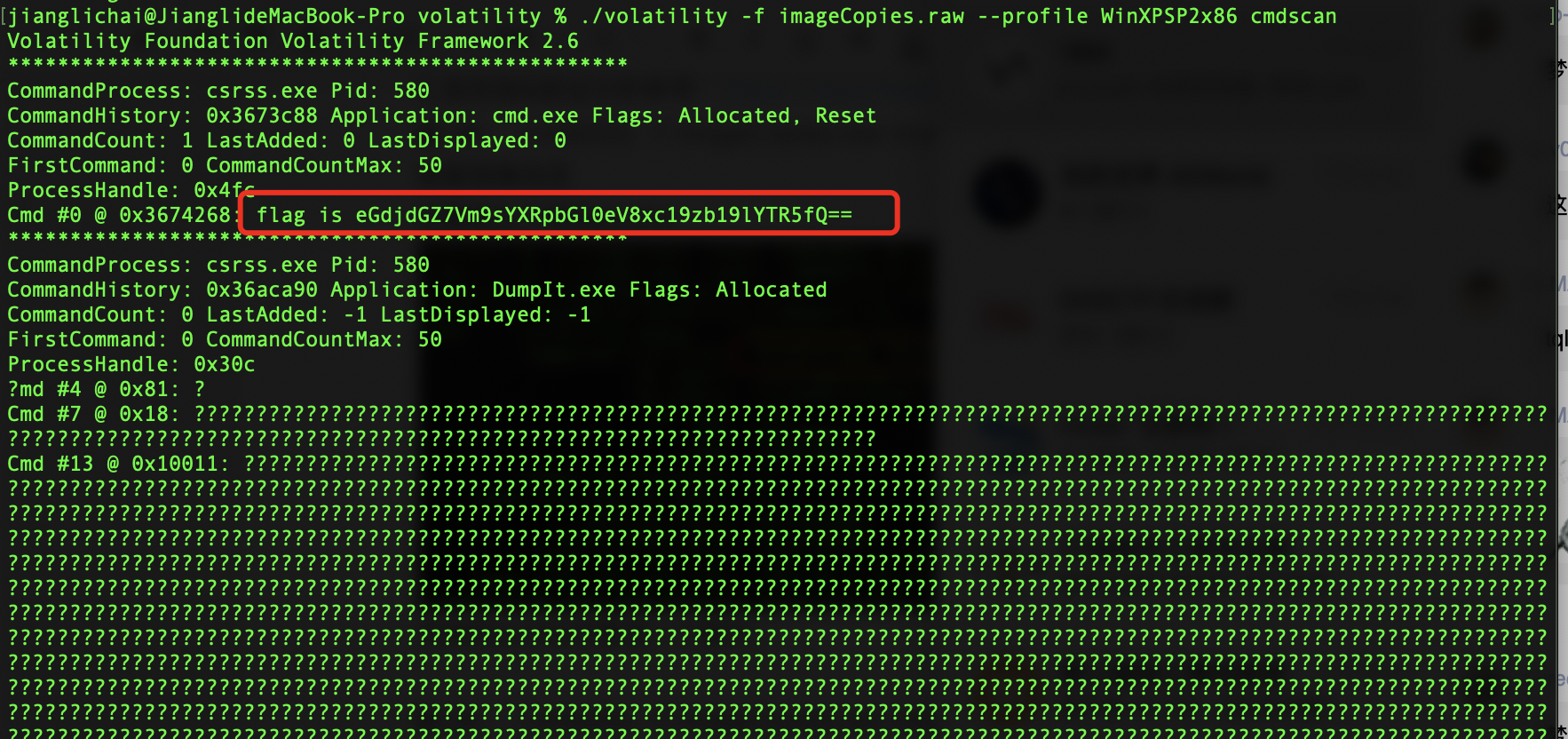


支持的profile任意选一个就行。

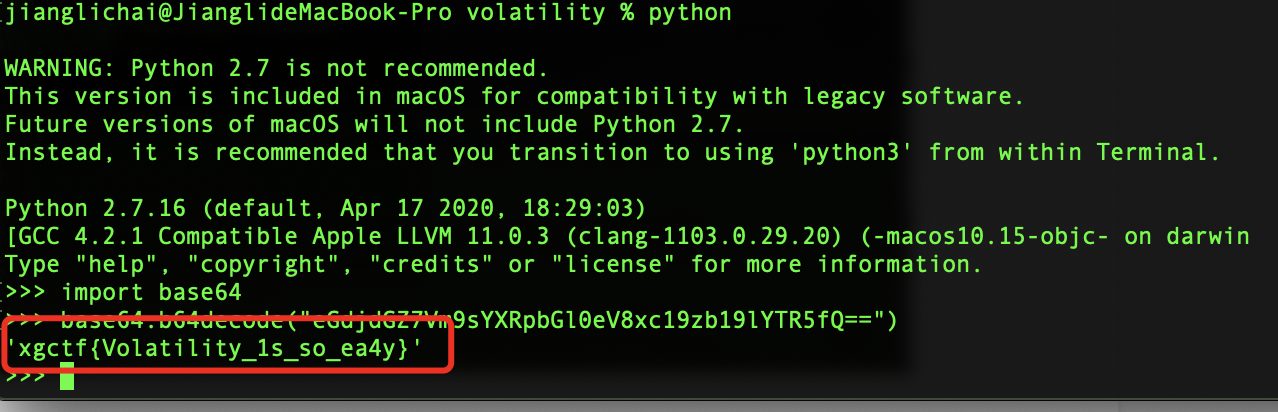
**第二步：** ./volatility -f imageCopies.raw imageinfo --profile WinXPSP2x86 cmdscan

这边使用cmdscan命令也是常规操作。查看cmd执行过那些命令。

因为我知道这边存在flag，所以直接看了。常规的还有看进程内存一类的。



**第三步：** base64解码



**简要总结：**本题旨在初步了解内存取证工具的使用。