1. Volatility -f name imageinfo
2. volatility -f name pslist --profile=WinXPSP2x86 列举进程：
3. volatility -f name --profile=WinXPSP2x86 volshell
4. dt("\_PEB") 查看进程环境块
5. volatility -f name --profile=WinXPSP2x86 hivelist列举缓存在内存的注册表 ：

**hivedump打印出注册表中的数据 ：**

volatility -f name --profile=WinXPSP2x86 hivedump -o 注册表的 virtual 地址

**显示每个进程的加载dll列表**

Volatility -f name -profile = Win7SP0x86 dlllist> dlllist.txt

**获取SAM表中的用户：**

volatility -f name --profile=WinXPSP2x86 printkey -K "SAM\Domains\Account\Users\Names"

**登陆账户系统**

volatility -f name --profile=WinXPSP2x86 printkey -K "SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon"

**userassist键值包含系统或桌面执行文件的信息，如名称、路径、执行次数、最后一次执行时间等**

volatility -f name --profile=WinXPSP2x86 userassist

**将内存中的某个进程数据以 dmp 的格式保存出来**

volatility -f name --profile=WinXPSP2x86 -p [PID] -D [dump 出的文件保存的目录]

**提取内存中保留的 cmd 命令使用情况**

volatility -f name --profile=WinXPSP2x86 cmdscan

**获取到当时的网络连接情况**

volatility -f name --profile=WinXPSP2x86 netscan

获取 IE 浏览器的使用情况 ：

volatility -f name --profile=WinXPSP2x86 iehistory

**获取内存中的系统密码，可以使用 hashdump 将它提取出来**

1. volatility -f name --profile=WinXPSP2x86 hashdump -y （注册表 system 的 virtual 地址 ）-s （SAM 的 virtual 地址）
2. volatility -f name --profile=WinXPSP2x86 hashdump -y 0xe1035b60 -s 0xe16aab60
3. volatility -f name --profile=WinXPSP2x86 timeliner

**对文件查找及dumo提取某个进程：**

1. volatility -f name --profile=Win7SP1x64 memdump -D . -p 2872
2. strings -e l ./2872.dmp | grep flag
3. volatility -f name --profile=Win7SP1x64 dumpfiles -Q 0x000000007e410890 -n --dump-dir=./

**HASH匹配用户账户名密码：**

Hash, 然后使用john filename --format=NT破解

**安全进程扫描**

volatility -f name --profile=Win7SP1x64 psscan

**Flag字符串扫描：**

strings -e l 2616.dmp | grep flag

**查找图片：**

1. volatility -f name--profile=Win7SP1x64 filescan | grep -E 'jpg|png|jpeg|bmp|gif
2. volatility -f name --profile=Win7SP1x64 netscan

**注册表解析**

1. volatility -f name --profile=Win7SP1x64 hivelist
2. volatility -f name --profile=Win7SP1x64 -o 0xfffff8a000024010 printkey -K "ControlSet001\Control;"

**复制、剪切版：**

1. volatility -f name --profile=Win7SP1x64 clipboard
2. volatility -f name --profile=Win7SP1x64 dlllist -p 3820

**Dump所有进程：**

1. volatility -f name --profile=Win7SP1x64 memdump -n chrome -D .
2. 利用字符串查找download
3. python vol.py -f name --profile=Win7SP1x86 shimcache

**svcscan查看服务**

python vol.py -f name --profile=Win7SP1x86 svcscan

1. modules 查看内核驱动
2. modscan、driverscan 可查看一些隐藏的内核驱动
3. ShimCache来识别应用程序兼容性问题。跟踪文件路径，大小，最后修改时间和最后“执行”时间.