内存取证

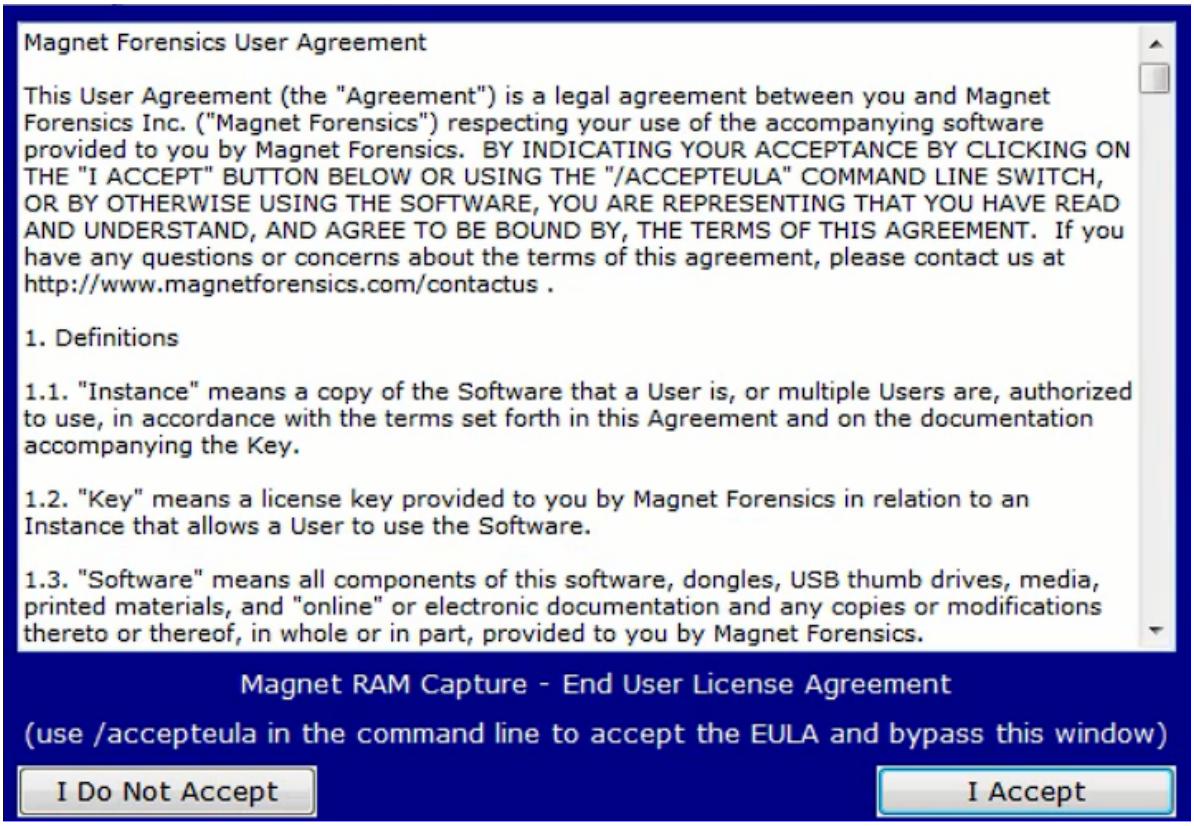
一、获取windows系统内存镜像

1、MAGNET RAM Capture

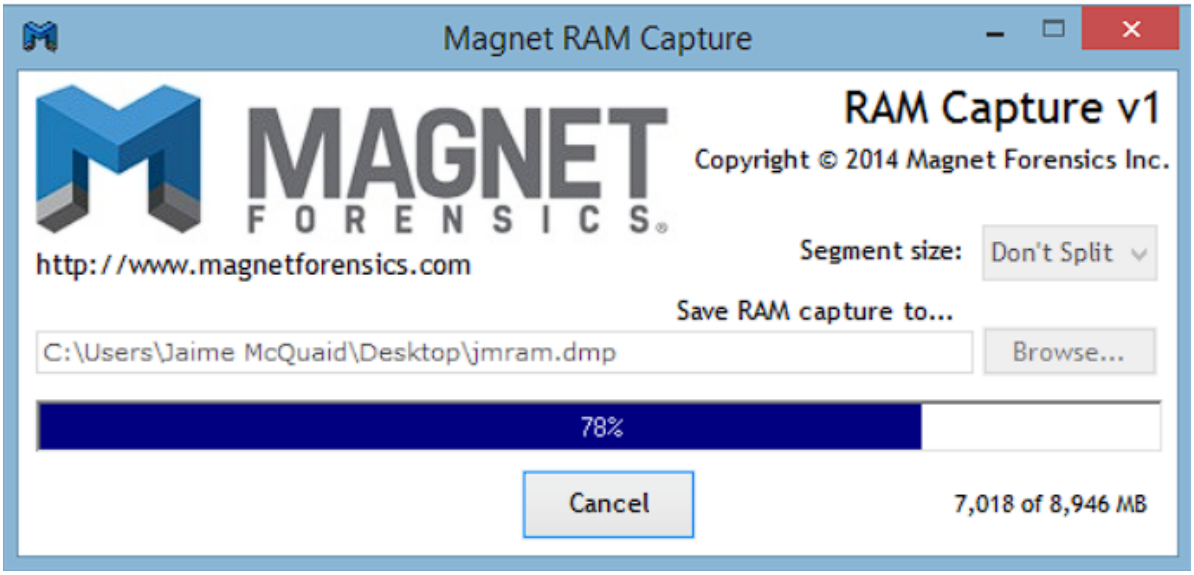
MAGNET RAM Capture是由MAGNET公司开发的一款免费制作内存镜像工具，体积小还可以对内存镜像设置分段。

使用步骤：

① 打开软件，在用户协议界面点击“I Accept”。



② 点击“Browse”，选择制作镜像保存的目录，并自定义文件名，后单击“start”,开始制作镜像。

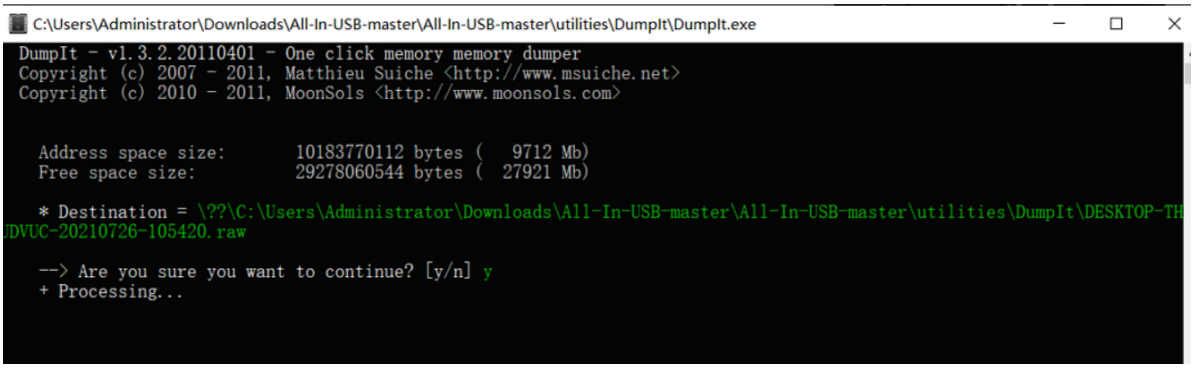


2、DumpIt

DumpIt 是一款绿色免安装的 windows 内存镜像取证工具。利用它我们可以轻松地将一个系统的完整内存镜像下来。

① 直接双击运行 DumpIt.exe 文件

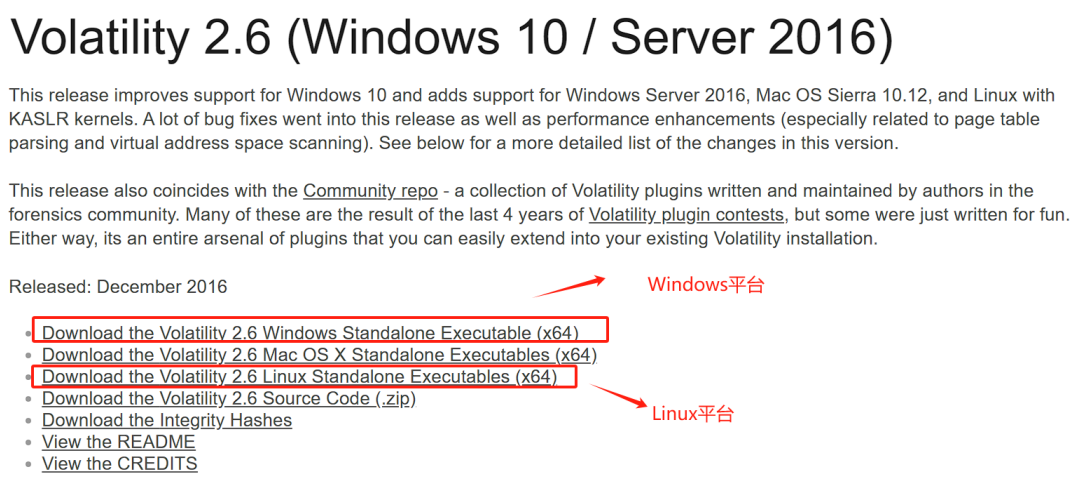
② 输入y并回车，提取的镜像被保存在当前目录下，保存格式为 raw。



二、取证工具——volatility使用方式

Volatility是一款非常强大的内存取证工具,它是由来自全世界的数百位知名安全专家合作开发的一套工具, 可以用于windows,linux,mac osx,android等系统内存取证。Volatility是一款开源内存取证框架，能够对导出的内存镜像进行分析，通过获取内核数据结构，使用插件获取内存的详细情况以及系统的运行状态。

官网下载地址：Volatility 2.6 Release (volatilityfoundation.org)



（一）.使用方法

此处以windows版的程序【volatility_2.6_win64_standalone.exe】距离，若使用源码包进行使用，更改程序名字即可。

1.查看帮助

```
volatility_2.6_win64_standalone.exe --h
```

具体可查看本手册最后【附件10-1】内容

2.查看插件

```
volatility_2.6_win64_standalone.exe --info
```

具体可查看本手册最后【附件10-2】内容

3.分析镜像系统信息

```
# imageinfo
volatility_2.6_win64_standalone.exe -f xxx.raw imageinfo
```

此步骤很重要，后面所有操作都要基于此步骤分析出的系统信息，添加参数操作

4.查看进程

```
# pslist
volatility_2.6_win64_standalone.exe -f xxx.raw --profile=XXX pslist
```

5.进程转储

```
# memdump 导出进程数据
# -p 导出的进程PID值
# -D 导出路径
volatility_2.6_win64_standalone.exe -f xxx.raw --profile=XXX memdump -p 2012
-D ./
```

6.查看用户名

```
# printkey
volatility_2.6_win64_standalone.exe -f xxx.raw --profile=XXX printkey -K
"SAM\Domains\Account\Users\Names"
```

7.查看用户密码

```
# hashdump
volatility_2.6_win64_standalone.exe -f xxx.raw --profile=XXX hashdump
```

8.查看主机名

```
volatility_2.6_win64_standalone.exe -f xxx.raw --profile=XXX printkey -K
"ControlSet001\Control\ComputerName\ComputerName"
```

9.查看cmd进程

```
# cmdscan
volatility_2.6_win64_standalone.exe -f xxx.raw --profile=XXX cmdscan
```

10.扫描文件

```
# filescan
volatility_2.6_win64_standalone.exe -f xxx.raw --profile=XXX filescan
```

11.导出文件

```
# dumplfiles
# -Q 文件的偏移
# -D 保存路径
volatility_2.6_win64_standalone.exe -f xxx.raw --profile=XXX dumplfiles -Q
0x00000123456 -D ./
```

12.查看进程树

```
# pstree
volatility_2.6_win64_standalone.exe -f xxx.raw --profile=XXX pstree
```

13.查看某个进程的DLL

```
# dlllist
# -p 端口号
volatility_2.6_win64_standalone.exe -f xxx.raw --profile=XXX dlllist -p 1234
```

14.查看剪贴板

```
# clipboard
volatility_2.6_win64_standalone.exe -f xxx.raw --profile=XXX clipboard
```

15.查看ie浏览器历史记录

```
# iehistory
volatility_2.6_win64_standalone.exe -f xxx.raw --profile=XXX iehistory
```

16.查看环境变量

```
# envars
volatility_2.6_win64_standalone.exe -f xxx.raw --profile=XXX envars
```

17.查看程序版本信息

```
# verinfo
volatility_2.6_win64_standalone.exe -f xxx.raw --profile=XXX verinfo
```

18.查看开机自启的程序

```
# shimcache
volatility_2.6_win64_standalone.exe -f xxx.raw --profile=XXX shimcache
```

19.查看系统网络连接情况

```
# netscan
volatility_2.6_win64_standalone.exe -f xxx.raw --profile=XXX netscan
```

20.查看注册表配置单元

```
# hivelist
volatility_2.6_win64_standalone.exe -f xxx.raw --profile=XXX hivelist
```

21.查看系统服务

```
# svcscan
volatility_2.6_win64_standalone.exe -f xxx.raw --profile=XXX svcscan
```

22.导出进程的程序

```
# svcscan
volatility_2.6_win64_standalone.exe -f xxx.raw --profile=XXX procdump -p
[PID] -D ./
```

23 导出进程内容

```
# memdump
.\volatility_2.6_win64_standalone.exe -f .\OtterCTF.vmem --profile=Win7SP1x64
memdump -p [PID] -D ./
```

附件10-1

```
Volatility Foundation Volatility Framework 2.6
用法: Volatility - 内存取证分析平台

Options:
  -h, --help            列出所有可用选项及其默认值
                        默认值可以在配置文件中设置
                        (/etc/volatilityrc)
  --conf-file=/home/kali/.volatilityrc
                        基于用户的配置文件
  -d, --debug           调试Volatility
  --plugins=PLUGINS     要使用的其他插件目录（冒号分隔）
  --info                打印所有注册对象的信息
  --cache-directory=/home/kali/.cache/volatility
                        存放缓存文件的目录
  --cache               使用缓存
  --tz=TZ               设置 (Olson) 时区以使用 pytz（如果已安装）或 tzset 显示时
间戳
```

```
  -f FILENAME, --filename=FILENAME
                        打开图像时使用的文件名
  --profile=WinXPSP2x86
                        要加载的配置文件的名称（使用 --info 查看支持的配置文件列表）
  -l LOCATION, --location=LOCATION
                        从中加载地址空间的 URN 位置
  -w, --write           启用写支持
  --dtb=DTB             DTB 地址
  --shift=SHIFT         Mac KASLR 移位地址
  --output=text         以这种格式输出（支持特定于模块，请参阅下面的模块输出选项）
  --output-file=OUTPUT_FILE
                        在此文件中写入输出
  -v, --verbose         详细信息
  -g KDBG, --kdbg=KDBG  指定一个 KDBG 虚拟地址（注意：对于 64 位 Windows 8 及更高版本，这是 KdCopyDataBlock 的地址）
  --force               强制使用可疑配置文件
  -k KPCR, --kpcr=KPCR  指定特定的 KPCR 地址
  --cookie=COOKIE       指定 nt!ObHeaderCookie 的地址（仅适用于 Windows 10）

    支持的插件命令:

        amcache         查看AmCache应用程序痕迹信息
        apihooks        检测内核及进程的内存空间中的API hook
        atoms           列出会话及窗口站atom表
        atomscan        Atom表的池扫描(Pool scanner)
        auditpol        列出注册表HKLMSECURITYPolicyPolAdtEv的审计策略信息
        bigpools        使用BigPagePoolScanner转储大分页池(big page pools)
        bioskbd         从实时模式内存中读取键盘缓冲数据(早期电脑可以读取出BIOS开机密码)
        cachedump       获取内存中缓存的域帐号的密码哈希
        callbacks       打印全系统通知例程
        clipboard       提取Windows剪贴板中的内容
        cmdline         显示进程命令行参数
        cmdscan         提取执行的命令行历史记录（扫描_COMMAND_HISTORY信息）
        connections     打印系统打开的网络连接(仅支持Windows XP 和2003)
        connscan        打印TCP连接信息
        consoles        提取执行的命令行历史记录（扫描_CONSOLE_INFORMATION信息）
        crashinfo       提取崩溃转储信息
        deskscan        tagDESKTOP池扫描(Poolscaner)
        devicetree      显示设备树信息
        dlldump         从进程地址空间转储动态链接库
        dlllist         打印每个进程加载的动态链接库列表
        driverirp       IRP hook驱动检测
        drivermodule    关联驱动对象至内核模块
        driverscan      驱动对象池扫描
        dumpcerts       提取RAS私钥及SSL公钥
        dumpfiles       提取内存中映射或缓存的文件
        dumpregistry    转储内存中注册表信息至磁盘
        editbox         查看Edit编辑控件信息 (Listbox正在实验中)
        envars          显示进程的环境变量
        eventhooks      打印Windows事件hook详细信息
        evtlogs         提取Windows事件日志（仅支持XP/2003)
        filescan        提取文件对象（file objects）池信息
        gahti           转储用户句柄（handle）类型信息
        gditimers       打印已安装的GDI计时器(timers)及回调(callbacks)
```

```
        gdt             显示全局描述符表(Global Deor Table)
        getservicesids  获取注册表中的服务名称并返回SID信息
        getsids         打印每个进程的SID信息
        handles         打印每个进程打开的句柄的列表
        hashdump        转储内存中的Windows帐户密码哈希(LM/NTLM)
        hibinfo         转储休眠文件信息
        hivedump        打印注册表配置单元信息
        hivelist        打印注册表配置单元列表
        hivescan        注册表配置单元池扫描
        hpakextract     从HPAK文件（Fast Dump格式）提取物理内存数据
        hpakinfo        查看HPAK文件属性及相关信息
        idt             显示中断描述符表(Interrupt Deor Table)
        iehistory       重建IE缓存及访问历史记录
        imagecopy       将物理地址空间导出原生DD镜像文件
        imageinfo       查看/识别镜像信息
        impscan         扫描对导入函数的调用
        joblinks        打印进程任务链接信息
        kdbgscan        搜索和转储潜在KDBG值
        kpcrscan        搜索和转储潜在KPCR值
        ldrmodules      检测未链接的动态链接DLL
        lsadump         从注册表中提取LSA密钥信息（已解密）
        machoinfo       转储Mach-O 文件格式信息
        malfind         查找隐藏的和插入的代码
        mbrparser       扫描并解析潜在的主引导记录(MBR)
        memdump         转储进程的可寻址内存
        memmap          打印内存映射
        messagehooks    桌面和窗口消息钩子的线程列表
        mftparser       扫描并解析潜在的MFT条目
        moddump         转储内核驱动程序到可执行文件的示例
        modscan         内核模块池扫描
        modules         打印加载模块的列表
        multiscan       批量扫描各种对象
        mutantscan      对互斥对象池扫描
        notepad         查看记事本当前显示的文本
        objtypescan     扫描窗口对象类型对象
        patcher         基于页面扫描的补丁程序内存
        poolpeek        可配置的池扫描器插件
        printkey        打印注册表项及其子项和值
        privs           显示进程权限
        procdump        进程转储到一个可执行文件示例
        pslist          按照EPROCESS列表打印所有正在运行的进程
        psscan          进程对象池扫描
        pstree          以树型方式打印进程列表
        psxview         查找带有隐藏进程的所有进程列表
        qemuinfo        转储 Qemu 信息
        raw2dmp         将物理内存原生数据转换为windbg崩溃转储格式
        screenshot      基于GDI Windows的虚拟屏幕截图保存
        servicediff     Windows服务列表(ala Plugx)
        sessions        _MM_SESSION_SPACE的详细信息列表(用户登录会话)
        shellbags       打印Shellbags信息
        shimcache       解析应用程序兼容性Shim缓存注册表项
        shutdowntime    从内存中的注册表信息获取机器关机时间
        sockets         打印已打开套接字列表
        sockscan        TCP套接字对象池扫描
        ssdt            显示SSDT条目
```

```
        strings         物理到虚拟地址的偏移匹配(需要一些时间，带详细信息)
        svcscan         Windows服务列表扫描
        symlinkscan     符号链接对象池扫描
        thrdscan        线程对象池扫描
        threads         调查_ETHREAD 和_KTHREADs
        timeliner       创建内存中的各种痕迹信息的时间线
        timers          打印内核计时器及关联模块的DPC
        truecryptmaster Recover      恢复TrueCrypt 7.1a主密钥
        truecryptpassphrase      查找并提取TrueCrypt密码
        truecryptsummary    TrueCrypt摘要信息
        unloadedmodules 打印卸载的模块信息列表
        userassist      打印注册表中UserAssist相关信息
        userhandles     转储用户句柄表
        vaddump         转储VAD数据为文件
        vadinfo         转储VAD信息
        vadtree         以树形方式显示VAD树信息
        vadwalk         显示遍历VAD树
        vboxinfo        转储Virtualbox信息（虚拟机）
        verinfo         打印PE镜像中的版本信息
        vmwareinfo      转储VMware VMSS/VMSN 信息
        volshell        内存镜像中的shell
        windows         打印桌面窗口(详细信息)
        wintree         Z顺序打印桌面窗口树
        wndscan         池扫描窗口站
        yarascan        以Yara签名扫描进程或内核内存
```

附件10-2

```
Volatility Foundation Volatility Framework 2.6

Profiles
--------
VistaSP0x64           - Windows Vista SP0 x64 的配置文件
VistaSP0x86           - Windows Vista SP0 x86 的配置文件
VistaSP1x64           - Windows Vista SP1 x64 的配置文件
VistaSP1x86           - Windows Vista SP1 x86 的配置文件
VistaSP2x64           - Windows Vista SP1 x86 的配置文件
VistaSP2x86           - Windows Vista SP2 x64 的配置文件
Win10x64              - Windows 10 x64 的配置文件
Win10x64_10586        - Windows 10 x64 的配置文件 (10.0.10586.306 / 2016-04-
23)
Win10x64_14393        - Windows 10 x64 的配置文件 (10.0.14393.0 / 2016-07-
16)
Win10x86              - Windows 10 x86 的配置文件
Win10x86_10586        - Windows 10 x86 的配置文件 (10.0.10586.420 / 2016-05-
28)
Win10x86_14393        - Windows 10 x86 的配置文件 (10.0.14393.0 / 2016-07-
16)
Win2003SP0x86         - Windows 2003 SP0 x86 的配置文件
Win2003SP1x64         - Windows 2003 SP0 x86 的配置文件
Win2003SP1x86         - Windows 2003 SP1 x86 的配置文件
Win2003SP2x64         - Windows 2003 SP1 x86 的配置文件
Win2003SP2x86         - Windows 2003 SP2 x86 的配置文件
Win2008R2SP0x64       - Windows 2008 R2 SP0 x64 的配置文件
```

```
Win2008R2SP1x64        - Windows 2008 R2 SP1 x64 的配置文件
Win2008R2SP1x64_23418 - Windows 2008 R2 SP1 x64 的配置文件 (6.1.7601.23418 / 2016-04-09)
Win2008SP1x64          - Windows 2008 SP1 x64 的配置文件
Win2008SP1x86          - Windows 2008 SP1 x86 的配置文件
Win2008SP2x64          - Windows 2008 SP2 x64 的配置文件
Win2008SP2x86          - Windows 2008 SP2 x86 的配置文件
Win2012R2x64           - Windows Server 2012 R2 x64 的配置文件
Win2012R2x64_18340     - Windows Server 2012 R2 x64 的配置文件 (6.3.9600.18340 / 2016-05-13)
Win2012x64             - Windows Server 2012 x64 的配置文件
Win2016x64_14393       - Windows Server 2016 x64 的配置文件 (10.0.14393.0 / 2016-07-16)
Win7SP0x64             - Windows 7 SP0 x64 的配置文件
Win7SP0x86             - Windows 7 SP0 x86 的配置文件
Win7SP1x64             - Windows 7 SP1 x64 的配置文件
Win7SP1x64_23418       - Windows 7 SP1 x64 的配置文件 (6.1.7601.23418 / 2016-04-09)
Win7SP1x86             - Windows 7 SP1 x86 的配置文件
Win7SP1x86_23418       - Windows 7 SP1 x86 的配置文件 (6.1.7601.23418 / 2016-04-09)
Win81U1x64             - Windows 8.1 更新 1 x64 的配置文件
Win81U1x86             - Windows 8.1 更新 1 x86 的配置文件
Win8SP0x64             - Windows 8 x64 的配置文件
Win8SP0x86             - Windows 8 x86 的配置文件
Win8SP1x64             - Windows 8.1 x64 的配置文件
Win8SP1x64_18340       - Windows 8.1 x64 的配置文件 (6.3.9600.18340 / 2016-05-13)
Win8SP1x86             - Windows 8.1 x86 的配置文件
WinXPSP1x64            - Windows XP SP1 x64 的配置文件
WinXPSP2x64            - Windows XP SP2 x64 的配置文件
WinXPSP2x86            - Windows XP SP2 x86 的配置文件
WinXPSP3x86            - Windows XP SP3 x86 的配置文件


Address Spaces
--------------
AMD64PagedMemory              - 标准 AMD 64 位地址空间
ArmAddressSpace               - ARM 处理器的地址空间
FileAddressSpace              - 这是一个直接文件 AS.
HPAKAddressSpace              - 此 AS 支持 HPAK 格式
IA32PagedMemory               - 标准 IA-32 分页地址空间
IA32PagedMemoryPae            - 此类实现 IA-32 PAE 分页地址空间
LimeAddressSpace              - Lime 的地址空间
LinuxAMD64PagedMemory         - Linux 特定的 AMD 64 位地址空间
MachOAddressSpace             - mach-o 文件的地址空间以支持 atc-ny 内存读取器
OSXPmemELF                    - 这个 AS 支持 VirtualBox ELF64 coredump 格式
QemuCoreDumpElf               - 这个 AS 支持 Qemu ELF32 和 ELF64 核心转储格式
VMWareAddressSpace            - 此 AS 支持 VMware 快照 (VMSS) 和保存状态 (VMSS) 文件
VMWareMetaAddressSpace        - 此 AS 支持带有 VMSN/VMSS 元数据的 VMEM 格式
VirtualBoxCoreDumpElf64       - 这个 AS 支持 VirtualBox ELF64 coredump 格式
Win10AMD64PagedMemory         - Windows 10 特定的 AMD 64 位地址空间
WindowsAMD64PagedMemory       - Windows 特定的 AMD 64 位地址空间
WindowsCrashDumpSpace32       - 这个 AS 支持 windows 崩溃转储格式
```

```
WindowsCrashDumpSpace64       - 此 AS 支持 windows Crash Dump 格式
WindowsCrashDumpSpace64BitMap - 此 AS 支持 Windows BitMap Crash Dump 格式
WindowsHiberFileSpace32       - 这是 Windows 休眠文件的休眠地址空间


Plugins
-------
amcache                     - 打印 AmCache 信息
apihooks                    - 检测进程和内核内存中的 API 挂钩
atoms                       - 打印会话和窗口站原子表
atomscan                    - 原子表的池扫描器
auditpol                    - 从 HKLM\SECURITY\Policy\PolAdtEv 打印出审计策略
bigpools                    - 使用 BigPagePoolScanner 转储大页面池
bioskbd                     - 从实模式内存中读取键盘缓冲区
cachedump                   - 从内存中转储缓存的域哈希
callbacks                   - 打印系统范围的通知例程
clipboard                   - 提取 Windows 剪贴板的内容
cmdline                     - 显示进程命令行参数
cmdscan                     - 通过扫描 _COMMAND_HISTORY 来提取命令历史记录
connections                 - 打印打开的连接列表 [仅限 Windows XP 和 2003]
connscan                    - 用于 tcp 连接的池扫描器
consoles                    - 通过扫描 _CONSOLE_INFORMATION 提取命令历史记录
crashinfo                   - 转储崩溃转储信息
deskscan                    - tagDESKTOP（台式机）的 Poolscaner
devicetree                  - 显示设备树
dlldump                     - 从进程地址空间转储 DLL
dlllist                     - 打印每个进程加载的 dll 列表
driverirp                   - 驱动程序 IRP 挂钩检测
drivermodule                - 将驱动程序对象关联到内核模块
driverscan                  - 驱动程序对象的池扫描器
dumpcerts                   - 转储 RSA 私有和公共 SSL 密钥
dumpfiles                   - 提取内存映射和缓存文件
dumpregistry                - 将注册表文件转储到磁盘
editbox                     - 显示有关编辑控件的信息（列表框实验）
envars                      - 显示进程环境变量
eventhooks                  - 在 Windows 事件挂钩上打印详细信息
evtlogs                     - 提取 Windows 事件日志（仅限 XP/2003）
filescan                    - 文件对象的池扫描器
gahti                       - 转储 USER 句柄类型信息
gditimers                   - 打印已安装的 GDI 计时器和回调
gdt                         - 显示全局描述符表
getservicesids              - 获取 Registry 中的服务名称并返回计算的 SID
getsids                     - 打印拥有每个进程的 SID
handles                     - 打印每个进程的打开句柄列表
hashdump                    - 从内存中转储密码哈希 (LM/NTLM)
hibinfo                     - 转储休眠文件信息
hivedump                    - 打印注册表
hivelist                    - 打印注册表配置单元列表
hivescan                    - 注册表配置单元的池扫描程序
hpakextract                 - 从 HPAK 文件中提取物理内存
hpakinfo                    - 有关 HPAK 文件的信息
idt                         - 显示中断描述符表
iehistory                   - 重建 Internet Explorer 缓存/历史
imagecopy                   - 将物理地址空间复制为原始 DD 映像
imageinfo                   - 识别图像的信息
```

```
impscan                  - 扫描对导入函数的调用
joblinks                 - 打印进程作业链接信息
kdbgscan                 - 搜索和转储潜在的 KDBG 值
kpcrscan                 - 搜索和转储潜在的 KPCR 值
ldrmodules               - 检测未链接的 DLL
limeinfo                 - 转储 Lime 文件格式信息
linux_apihooks           - 检查用户态 apihooks
linux_arp                - 打印 ARP 表
linux_aslr_shift         - 自动检测 Linux ASLR shift
linux_banner             - 打印 Linux 横幅信息
linux_bash               - 从 bash 进程内存中恢复 bash 历史记录
linux_bash_env           - 恢复进程的动态环境变量
linux_bash_hash          - 从 bash 进程内存中恢复 bash 哈希表
linux_check_afinfo       - 验证网络协议的操作函数指针
linux_check_creds        - 检查是否有进程共享凭证结构
linux_check_evt_arm      - 检查异常向量表以查找系统调用表挂钩
linux_check_fop          - 检查 rootkit 修改的文件操作结构
linux_check_idt          - 检查 IDT 是否已被更改
linux_check_inline_kernel - 检查内联内核挂钩
linux_check_modules      - 将模块列表与 sysfs 信息进行比较（如果可用）
linux_check_syscall      - 检查系统调用表是否已更改
linux_check_syscall_arm  - 检查系统调用表是否已更改
linux_check_tty          - 检查 tty 设备的钩子
linux_cpuinfo            - 打印每个活动处理器的信息
linux_dentry_cache       - 从 dentry 缓存中收集文件
linux_dmesg              - 收集 dmesg 缓冲区
linux_dump_map           - 将选定的内存映射写入磁盘
linux_dynamic_env        - 恢复进程的动态环境变量
linux_elfs               - 在进程映射中查找 ELF 二进制文件
linux_enumerate_files    - 列出文件系统缓存引用的文件
linux_find_file          - 列出并从内存中恢复文件
linux_getcwd             - 列出每个进程的当前工作目录
linux_hidden_modules     - 雕刻内存以查找隐藏的内核模块
linux_ifconfig           - 收集活动接口
linux_info_regs          - 就像 GDB 中的“信息寄存器”。 它打印出所有
linux_iomem              - 提供类似于 /proc/iomem 的输出
linux_kernel_opened_files - 列出从内核中打开的文件
linux_keyboard_notifiers - 解析键盘通知器调用链
linux_ldrmodules         - 将 proc 映射的输出与 libdl 中的库列表进行比较
linux_library_list       - 列出加载到进程中的库
linux_librarydump        - 将进程内存中的共享库转储到磁盘
linux_list_raw           - 列出具有混杂套接字的应用程序
linux_lsmod              - 收集加载的内核模块
linux_lsof               - 列出文件描述符及其路径
linux_malfind            - 寻找可疑的进程映射
linux_memmap             - 转储 linux 任务的内存映射
linux_moddump            - 提取加载的内核模块
linux_mount              - 收集挂载的 fs/devices
linux_mount_cache        - 从 kmem_cache收集挂载的 fs/devices
linux_netfilter          - 列出 Netfilter 钩子
linux_netscan            - 雕刻网络连接结构
linux_netstat            - 列出打开的套接字
linux_pidhashtable       - 通过 PID 哈希表枚举进程
linux_pkt_queues         - 将每个进程的数据包队列写入磁盘
linux_plthook            - 扫描 ELF 二进制文件的 PLT 以获取非需要图像的挂钩
```

```
linux_proc_maps               - 收集进程内存映射
linux_proc_maps_rb            - 通过映射红黑树为 linux 收集进程映射
linux_procdump                - 将进程的可执行映像转储到磁盘
linux_process_hollow          - 检查进程空心的迹象
linux_psaux                   - 收集进程以及完整的命令行和开始时间
linux_psenv                   - 收集进程及其静态环境变量
linux_pslist                  - 通过遍历 task_struct->task 列表来收集活动任务
linux_pslist_cache            - 从 kmem_cache 收集任务
linux_psscan                  - 扫描进程的物理内存
linux_pstree                  - 显示进程之间的父/子关系
linux_psxview                 - 使用各种进程列表查找隐藏进程
linux_recover_filesystem      - 从内存中恢复整个缓存文件系统
linux_route_cache             - 从内存中恢复路由缓存
linux_sk_buff_cache           - 从 sk_buff kmem_cache 中恢复数据包
linux_slabinfo                - 在运行的机器上模拟 /proc/slabinfo
linux_strings                 - 将物理偏移量与虚拟地址匹配（可能需要一段时间，非常冗
长）
linux_threads                 - 打印进程的线程
linux_tmpfs                   - 从内存中恢复 tmpfs 文件系统
linux_truecrypt_passphrase    - 恢复缓存的 Truecrypt 密码
linux_vma_cache               - 从 vm_area_struct 缓存中收集 VMA
linux_volshell                - 内存映像中的 Shell
linux_yarascan                - Linux 内存映像中的 shell
lsadump                       - 从注册表中转储（解密的）LSA 机密
mac_adium                     - 列出 Adium 消息
mac_apihooks                  - 检查进程中的 API 挂钩
mac_apihooks_kernel           - 检查系统调用和内核函数是否被挂钩
mac_arp                       - 打印 arp 表
mac_bash                      - 从 bash 进程内存中恢复 bash 历史记录
mac_bash_env                  - 恢复 bash 的环境变量
mac_bash_hash                 - 从 bash 进程内存中恢复 bash 哈希表
mac_calendar                  - 从 Calendar.app 获取日历事件
mac_check_fop                 - 验证文件操作指针
mac_check_mig_table           - 列出内核 MIG 表中的整体
mac_check_syscall_shadow      - 查找影子系统调用表
mac_check_syscalls            - 检查系统调用表条目是否被挂钩
mac_check_sysctl              - 检查未知的 sysctl 处理程序
mac_check_trap_table          - 检查 mach 陷阱表条目是否被钩住
mac_compressed_swap           - 打印 Mac OS X VM 压缩器统计数据并转储所有压缩页面
mac_contacts                  - 从 Contacts.app 获取联系人姓名
mac_dead_procs                - 打印终止/取消分配的进程
mac_dead_sockets              - 打印终止/取消分配的网络套接字
mac_dead_vnodes               - 列出释放的 vnode 结构
mac_devfs                     - 列出文件缓存中的文件
mac_dmesg                     - 打印内核调试缓冲区
mac_dump_file                 - 转储指定文件
mac_dump_maps                 - 转储进程的内存范围，可选地包括压缩交换中的页面
mac_dyld_maps                 - 从 dyld 数据结构中获取进程的内存映射
mac_find_aslr_shift           - 查找 10.8+ 图像的 ASLR 移位值
mac_get_profile               - 自动检测 Mac 配置文件
mac_ifconfig                  - 列出所有设备的网络接口信息
mac_interest_handlers         - 列出 IOKit 兴趣处理程序
mac_ip_filters                - 报告任何挂钩的 IP 过滤器
mac_kernel_classes            - 列出内核中加载的 C++ 类
mac_kevents                   - 显示进程的父/子关系
```

```
mac_keychaindump            - 恢复可能的钥匙串密钥。 使用chainbreaker打开相关的keychain文件
mac_ldrmodules              - 将 proc 映射的输出与 libdl 中的库列表进行比较
mac_librarydump             - 转储进程的可执行文件
mac_list_files              - 列出文件缓存中的文件
mac_list_kauth_listeners    - 列出 Kauth Scope 监听器
mac_list_kauth_scopes       - 列出 Kauth 范围及其状态
mac_list_raw                - 列出具有混杂套接字的应用程序
mac_list_sessions           - 枚举会话
mac_list_zones              - 打印活动区域
mac_lsmod                   - 列出加载的内核模块
mac_lsmod_iokit             - 列出通过 IOkit 加载的内核模块
mac_lsmod_kext_map          - 列出加载的内核模块
mac_lsof                    - 列出每个进程打开的文件
mac_machine_info            - 打印有关样本的机器信息
mac_malfind                 - 寻找可疑的进程映射
mac_memdump                 - 将可寻址内存页转储到文件中
mac_moddump                 - 将指定的内核扩展写入磁盘
mac_mount                   - 打印挂载的设备信息
mac_netstat                 - 列出每个进程的活动网络连接
mac_network_conns           - 列出来自内核网络结构的网络连接
mac_notesapp                - 查找 Notes 消息的内容
mac_notifiers               - 检测将钩子添加到 I/O 工具包中的 rootkit（例如 LogKext）
mac_orphan_threads          - 列出不映射回已知模块/进程的线程
mac_pgrp_hash_table         - 遍历进程组哈希表
mac_pid_hash_table          - 遍历 pid 哈希表
mac_print_boot_cmdline      - 打印内核启动参数
mac_proc_maps               - 获取进程的内存映射
mac_procdump                - 转储进程的可执行文件
mac_psaux                   - 在用户区打印带有参数的进程 (**argv)
mac_psenv                   - 在用户空间打印带有环境的进程 (**envp)
mac_pslist                  - 列出正在运行的进程
mac_pstree                  - 显示进程的父/子关系
mac_psxview                 - 使用各种进程列表查找隐藏进程
mac_recover_filesystem      - 恢复缓存的文件系统
mac_route                   - 打印路由表
mac_socket_filters          - 报告套接字过滤器
mac_strings                 - 将物理偏移量与虚拟地址匹配（可能需要一段时间，非常冗长）
mac_tasks                   - 列出活动任务
mac_threads                 - 列出进程线程
mac_threads_simple          - 列出线程及其开始时间和优先级
mac_timers                  - 报告内核驱动程序设置的定时器
mac_trustedbsd              - 列出恶意的trustedbsd 策略
mac_version                 - 打印 Mac 版本
mac_vfsevents               - 列出过滤文件系统事件的进程
mac_volshell                - 内存映像中的外壳
mac_yarascan                - 扫描内存中的 yara 签名
machoinfo                   - 转储 Mach-O 文件格式信息
malfind                     - 查找隐藏和注入的代码
mbrparser                   - 扫描并解析潜在的主引导记录 (MBR)
memdump                     - 转储进程的可寻址内存
memmap                      - 打印内存映射
messagehooks                - 列出桌面和线程窗口消息挂钩
```

```
mftparser                - 扫描并解析潜在的 MFT 条目
moddump                  - 将内核驱动程序转储到可执行文件示例
modscan                  - 内核模块的池扫描器
modules                  - 打印加载模块的列表
multiscan                - 一次扫描各种对象
mutantscan               - 互斥对象的池扫描器
netscan                  - 扫描 Vista（或更高版本）图像的连接和套接字
notepad                  - 列出当前显示的记事本文本
objtypescan              - 扫描 Windows 对象类型对象
patcher                  - 基于页面扫描修补内存
poolpeek                 - 可配置的池扫描器插件
pooltracker              - 显示池标签使用的摘要
printkey                 - 打印注册表项及其子项和值
privs                    - 显示进程权限
procdump                 - 将进程转储到可执行文件示例
pslist                   - 按照 EPROCESS 列表打印所有正在运行的进程
psscan                   - 进程对象的池扫描器
pstree                   - 将进程列表打印为树
psxview                  - 使用各种进程列表查找隐藏进程
qemuinfo                 - 转储 Qemu 信息
raw2dmp                  - 将物理内存样本转换为 windbg 故障转储
screenshot               - 保存基于 GDI 窗口的伪截图
servicediff              - 列出 Windows 服务（ala Plugx）
sessions                 - 列出 _MM_SESSION_SPACE 的详细信息（用户登录会话）
shellbags                - 打印 ShellBags 信息
shimcache                - 解析应用程序兼容性 Shim Cache 注册表项
shutdowntime             - 从注册表打印机器的 ShutdownTime
sockets                  - 打印打开的套接字列表
sockscan                 - tcp 套接字对象的池扫描器
ssdt                     - 显示 SSDT 条目
strings                  - 将物理偏移量与虚拟地址匹配（可能需要一段时间，非常冗
长）
svcscan                  - 扫描 Windows 服务
symlinkscan              - 符号链接对象的池扫描器
thrdscan                 - 线程对象的池扫描器
threads                  - 调查 _ETHREAD 和 _KTHREADs
timeliner                - 从内存中的各种工件创建时间线
timers                   - 打印内核定时器和相关的模块 DPC
truecryptmaster          - 恢复 TrueCrypt 7.1a 主密钥
truecryptpassphrase      - TrueCrypt 缓存密码短语查找器
truecryptsummary         - TrueCrypt 总结
unloadedmodules          - 打印已卸载模块的列表
userassist               - 打印 userassist 注册表项和信息
userhandles              - 转储 USER 句柄表
vaddump                  - 将 vad 部分转储到文件中
vadinfo                  - 转储 VAD 信息
vadtree                  - 遍历 VAD 树并以树格式显示
vadwalk                  - 走 VAD 树
vboxinfo                 - 转储 virtualbox 信息
verinfo                  - 从 PE 图像中打印出版本信息
vmwareinfo               - 转储 VMware VMSS/VMSN 信息
volshell                 - 内存映像中的 Shell
win10cookie              - 查找 Windows 10 的 ObHeaderCookie 值
windows                  - 打印桌面窗口（详细信息）
wintree                  - 打印Z顺序桌面Windows树
```

```
wndscan                    - 用于窗口站的池扫描仪
yarascan                   - 使用 Yara 签名扫描进程或内核内存


Scanner Checks
--------------
CheckPoolSize           - 检查池块大小
CheckPoolType           - 检查池类型
KPCRScannerCheck        - 检查自引用指针以查找KPCR
MultiPrefixFinderCheck - 每页检查多个字符串，在偏移处完成
MultiStringFinderCheck - 每页检查多个字符串
PoolTagCheck            - 此扫描程序检查池标记的出现
```