南京郵電大學
Nanjing University of Posts and Telecommunications

计算机取证汇报

Windows系统内存数据取证分析

汇报人：邱铭睿　学号：1024041125

南京邮电大学
Nanjing University of Posts and Telecommunications

目录

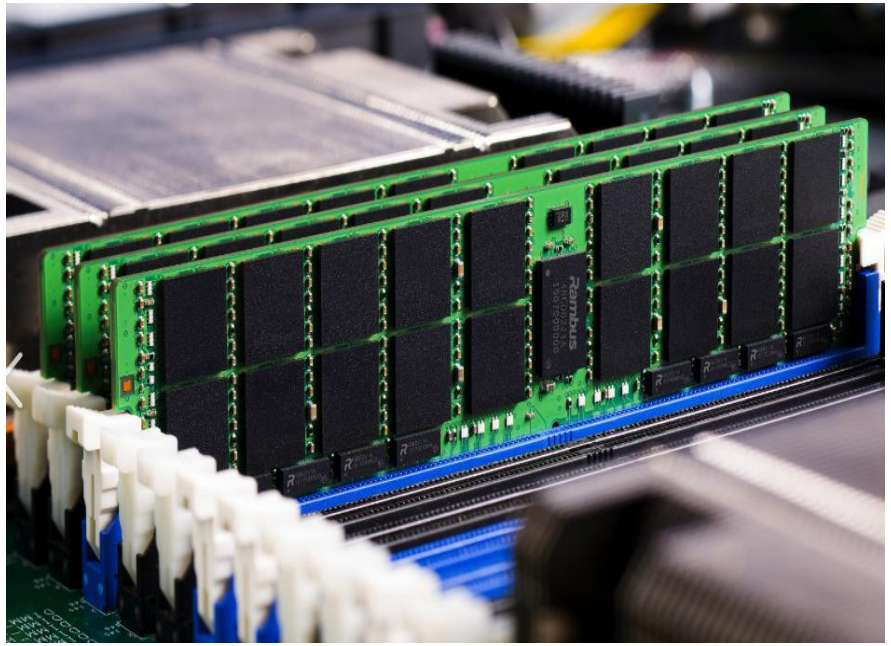
CONTENT

基本概念

基本概念

内存又称主存，是CPU能直接寻址访问的存储空间。在计算机工作的时候，所有的数据都要先经过内存，然后才能交由处理器去处理，内存也被称为，CPU与外存通信的桥梁。它的特点是读写速度快。

内存一般是由半导体器件组成，可分为RAM、ROM、Cache。



基本概念

ROM是一种只读存储器，其中的数据不能被常规方式修改或写入。它包含了固定的数据，例如启动程序、固件等。

ROM:

ROM

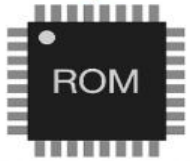
Read Only Memory

只读存储器

ROM：手机或电脑的硬盘
现在的ROM不仅可以读也可以写数据

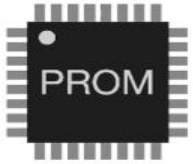
往手机里下载APP，就是往手机ROM中写数据

BIOS



只能读
不能写

最早的ROM只是用来存储程序的地方，比如BIOS（Basic Input Output System），基本输入输出系统，电脑启动时运行的第一个软件。



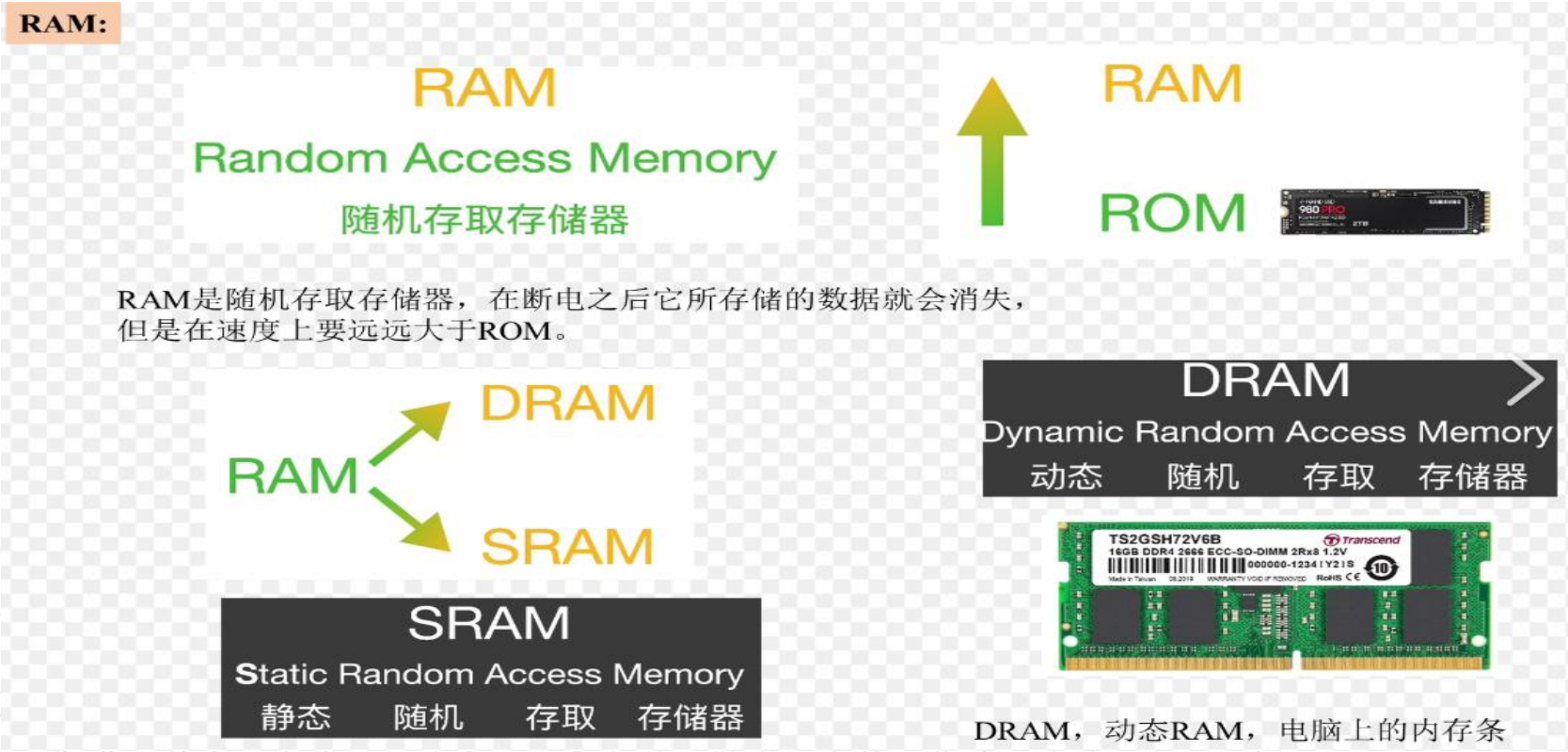
1

熔丝熔断代表0，没有熔断代表1

后来有了PROM,全称是Programmable ROM，可编程只读存储器，写入程序后程序无法更改，利用的是熔丝技术。

基本概念

RAM（随机访问存储器）既可以从中读取数据，也可以从中写入数据，但是断电后数据就会消失。我们现在所使用的内存条，其实就是RAM集成块集中在一起的一块小电路板，它插在计算机的内存插槽上。而RAM又分为两种，DRAM（动态随机存储）和SRAM（静态随机存储）。



基本概念

内存取证，也被称为RAM取证或易失性内存取证，是指在计算机系统运行时，对物理内存（RAM）进行分析的过程。

与硬盘上的数据不同，内存中的数据是易失性的，意味着一旦电源中断，这些数据就会丢失。因此，内存取证需要在系统仍然运行时迅速而准确地进行。

基本概念

内存

运行中的进程

活动进程的状态、线程信息和堆栈数据。

网络连接

开放的端口、连接状态和网络流量信息。

密码和密钥

未加密的凭据、加密密钥和会话信息。

动态加载的模块

例如DLLs和其他动态链接库。

缓冲区和缓存

例如Web浏览器缓存、系统缓存和应用程序缓存。

系统和应用程序状态

包括注册表键值、环境变量和系统日志。

取证目的

取证目的

Windows 系统内存取证的主要目的是在设备仍然运行的状态下获取关键的、易失性的运行数据，以辅助安全分析、事件响应和法律取证。与传统的磁盘取证不同，内存取证可以捕捉到系统当前正在执行的内容，例如正在运行的进程、已加载的模块、活跃的网络连接、登录用户信息、密码凭据、剪贴板数据、命令历史记录以及潜在的恶意软件行为。其特点包括时效性强、数据易失性高、操作需谨慎、分析价值高，能够揭示很多在磁盘中找不到的动态信息，尤其适用于分析高级攻击（如内存驻留型恶意软件）和系统被篡改的情况。因此，在安全事件响应或数字取证过程中，内存取证常被用作首要步骤之一。

取证方法

取证方法

取证步骤：

保持系统运行

保持系统运行状态，避免断电，以确保内存数据的完整性。

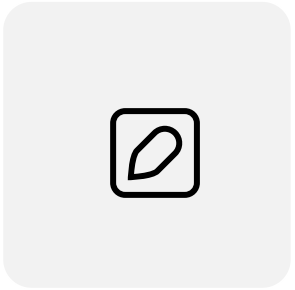
捕获内存镜像

尽快进行内存镜像捕获，使用专业的工具生成内存镜像文件。

校验镜像完整性

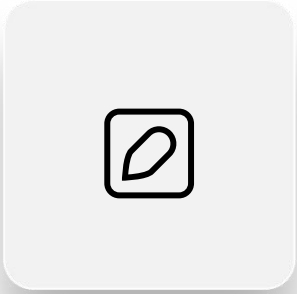
生成内存镜像的哈希值，校验镜像的完整性和真实性。

取证方法



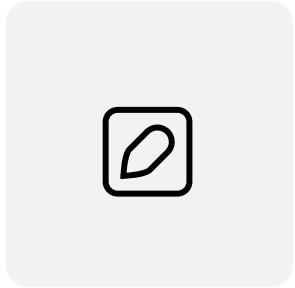
DumpIt

DumpIt是一款轻量化的Windows内存采集工具，一键生成.raw镜像文件，适合快速取证。



FTK Imager

FTK Imager具有可视化界面，可以导出内存及磁盘数据，适合综合取证。



Belkasoft RAM Capturer

Belkasoft RAM Capturer支持32/64位Windows内存采集，功能强大，适合复杂场景。

分析方法

分析方法

分析步骤：

导入内存镜像

将捕获的内存镜像文件导入分析工具，准备进行分析。

执行基本检查

执行基本检查，查看系统信息、进程列表等，了解系统运行状态。

查找可疑行为

查找可疑模块、隐藏进程、内联钩子等，发现潜在的恶意行为。

分析方法

01

Volatility

Volatility 是一款功能强大的内存分析工具，支持Windows、Linux和Mac操作系统，插件丰富。

02

Rekall

Rekall支持交互式分析，兼容Volatility，适合高级用户进行深入分析。

03

Redline

Redline具有友好的GUI界面，适合初学者快速上手，适合教学和入门使用。

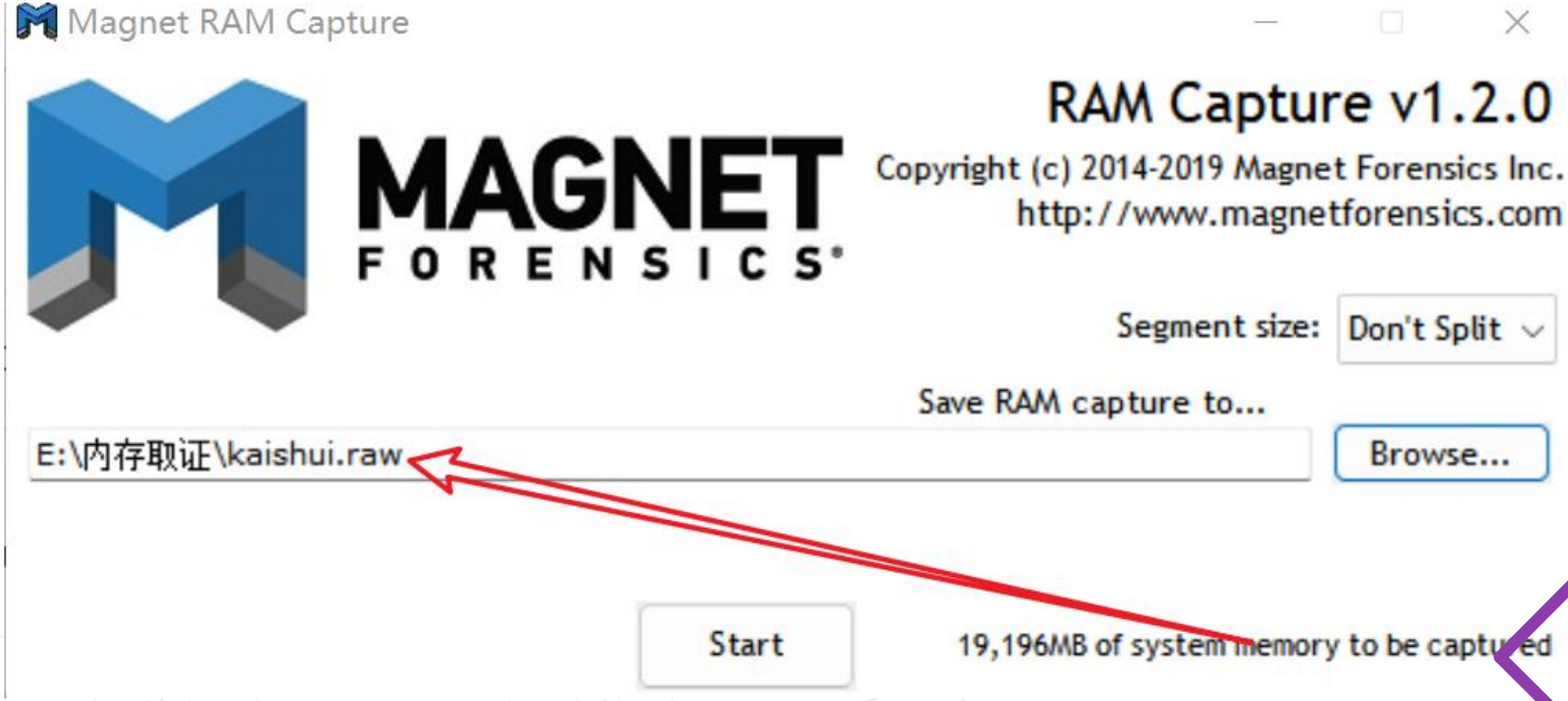
工具应用

工具应用

南京邮电大学 Nanjing University of Posts and Telecommunications

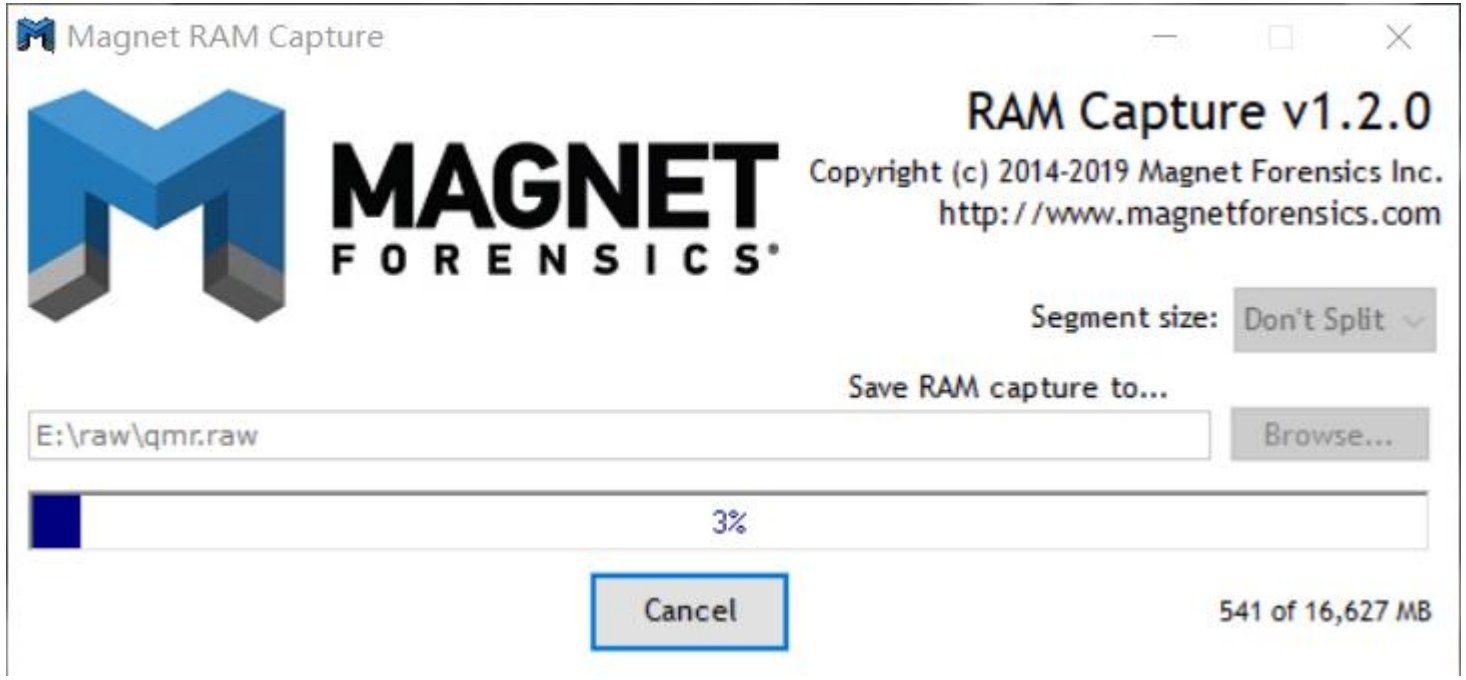
Magnet RAM Capture

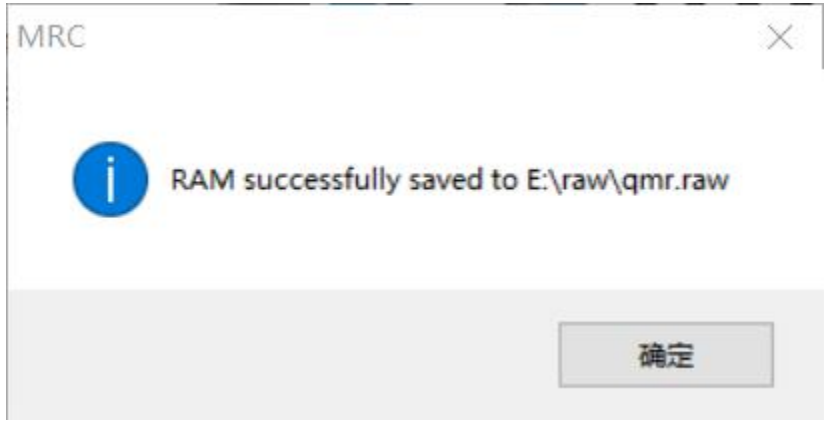
运行软件后可选择分段大小，保存路径，点击start自动获取内存镜像



工具应用

Magnet RAM Capture
用自己的电脑制作一份镜像文件，只需几分钟，十分便捷。

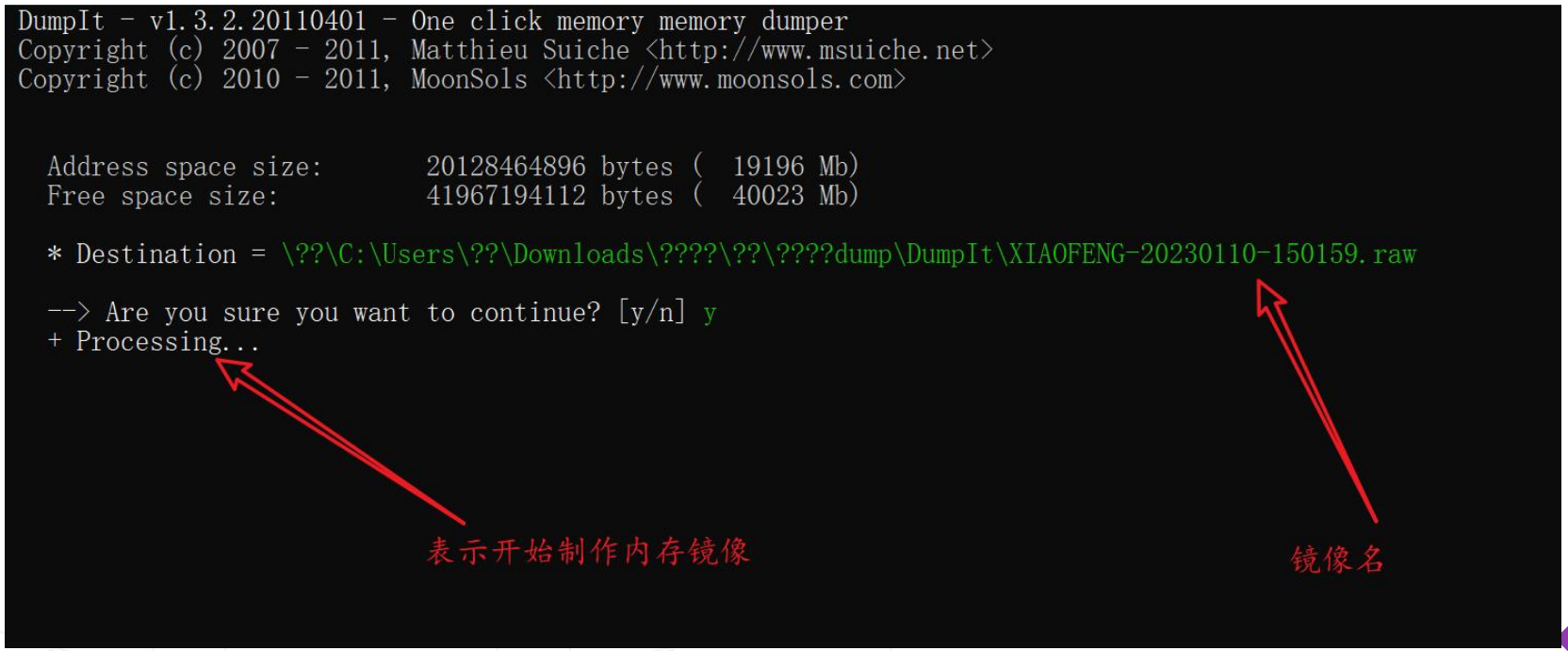




工具应用

DumpIt

双击软件即可运行，输入y即开始制作当前机器内存镜像，默认保存在其所在目录，镜像名称默认为“主机名 + 当前时间”



工具应用

补充知识：

断电情况下，Windows会使用交换文件（Pagefile.sys）来协助内存工作，当内存不满足系统所需的情况下，会释放部分内存数据到Pagefile.sys文件中。因此，当设备断电后，若无法拿到内存镜像，可以通过分析Pagefile.sys文件获取有价值的内存数据。

休眠情况下，系统会在磁盘中生成一个休眠文件（Hiberfil.sys）用于存放内存中的数据，当计算机重新加电时，又将休眠文件中的数据重新写到物理内存中，这个文件也包含有价值的内存数据。

工具应用

Volatility

1.查看基本信息

使用时将这个软件和需要取证的镜像放到一起

打开终端，输入命令

./volatility -f memory.img imageinfo

首先要查出文件概述profile，后面指令都需要指定profile

```
PS D:\Misc\misc tools\volatility内存取证工具> ./volatility -f memory.img imageinfo
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win2003SP0x86, Win2003SP1x86, Win2003SP2x86
                     AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : FileAddressSpace (D:\Misc\misc tools\volatility内存取证工具\memory.img)
                      PAE type : PAE
                           DTB : 0xe02000L
                          KDBG : 0x8088e3e0L
          Number of Processors : 1
     Image Type (Service Pack) : 1
                KPCR for CPU 0 : 0xffdff000L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2019-04-25 08:43:06 UTC+0000
     Image local date and time : 2019-04-25 16:43:06 +0800
PS D:\Misc\misc tools\volatility内存取证工具>
```

工具应用

Volatility

2.查看进程

./volatility -f memory.img --profile=Win2003SP1x86 pslist

```
PS D:\Misc\misc tools\volatility内存取证工具> ./volatility -f memory.img --profile=Win2003SP1x86 pslist
Volatility Foundation Volatility Framework 2.6
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
---------- -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------
0x81f8f020 System                    4      0     56      319 ------      0
0xfe2f8448 smss.exe                380      4      3       18 ------      0 2018-12-07 16:20:54 UTC+0000
0xfe2caa60 csrss.exe               516    380     12      509      0      0 2018-12-07 16:21:00 UTC+0000
0xfe304298 winlogon.exe            580    380     25      504      0      0 2018-12-07 16:21:04 UTC+0000
0xfe2fdd88 services.exe            648    580     16      303      0      0 2018-12-07 16:21:05 UTC+0000
0xfe2e5530 lsass.exe               660    580     38      458      0      0 2018-12-07 16:21:05 UTC+0000
0xfe2f9290 vmacthlp.exe            880    648      1       26      0      0 2018-12-07 16:21:06 UTC+0000
0xfe34d658 svchost.exe             932    648      6       93      0      0 2018-12-07 16:21:07 UTC+0000
0xfde05020 svchost.exe             984    648     10      268      0      0 2018-12-07 16:21:07 UTC+0000
0xfddf4c08 svchost.exe            1040    648     10      138      0      0 2018-12-07 16:21:08 UTC+0000
```

工具应用

Volatility

3.查看浏览器历史记录

./volatility -f memory.img --profile=Win2003SP1x86 iehistory

```
PS D:\Misc\misc tools\volatility内存取证工具> ./volatility -f memory.img --profile=Win2003SP1x86 iehistory
Volatility Foundation Volatility Framework 2.6
**************************************************
Process: 1992 explorer.exe
Cache type "DEST" at 0x167215
Last modified: 2019-04-25 16:43:00 UTC+0000
Last accessed: 2019-04-25 08:43:02 UTC+0000
URL: Administrator@file:///C:/Documents%20and%20Settings/Administrator/Lhb/flag.png
**************************************************
Process: 1992 explorer.exe
Cache type "DEST" at 0x16748d
Last modified: 2019-04-25 16:43:00 UTC+0000
Last accessed: 2019-04-25 08:43:02 UTC+0000
URL: Administrator@file:///C:/Documents%20and%20Settings/Administrator/Lhb/flag.png
PS D:\Misc\misc tools\volatility内存取证工具>
```

工具应用

Volatility3

系统基本信息(windows.info)　vol -f <内存镜像文件路径> windows.info

systentime可以看出镜像制作时间

工具应用

Volatility3

windows.pslist：列出所有进程

C:\Windows\System32\cmd.exe

```
F:\software\volatility3-develop>vol.py -f qmr.raw windows.pslist
Volatility 3 Framework 2.26.2
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime
        File output

4       0       System  0xb78d14cba1c0  254     -       N/A     False   2025-06-09 01:29:03.000000 UTC  N/A     Disabled

148     4       Registry        0xb78d14eed040  4       -       N/A     False   2025-06-09 01:28:57.000000 UTC  N/A
        Disabled
532     4       smss.exe        0xb78d17e95040  2       -       N/A     False   2025-06-09 01:29:03.000000 UTC  N/A
        Disabled
912     616     csrss.exe       0xb78d2242a240  11      -       0       False   2025-06-09 01:29:09.000000 UTC  N/A
        Disabled
948     616     wininit.exe     0xb78d23bd40c0  1       -       0       False   2025-06-09 01:29:12.000000 UTC  N/A
        Disabled
976     936     csrss.exe       0xb78d23897080  15      -       1       False   2025-06-09 01:29:12.000000 UTC  N/A
        Disabled
1040    948     services.exe    0xb78d23cd3240  12      -       0       False   2025-06-09 01:29:12.000000 UTC  N/A
        Disabled
1048    948     lsass.exe       0xb78d23cd7240  8       -       0       False   2025-06-09 01:29:12.000000 UTC  N/A
        Disabled
1124    936     winlogon.exe    0xb78d23d670c0  3       -       1       False   2025-06-09 01:29:12.000000 UTC  N/A
        Disabled
1248    1040    svchost.exe     0xb78d23e0f080  12      -       0       False   2025-06-09 01:29:12.000000 UTC  N/A
        Disabled
1276    948     fontdrvhost.ex  0xb78d23e230c0  5       -       0       False   2025-06-09 01:29:12.000000 UTC  N/A
        Disabled
1280    1124    fontdrvhost.ex  0xb78d23e10080  5       -       1       False   2025-06-09 01:29:12.000000 UTC  N/A
```

工具应用

Volatility3

windows.malfind：检测潜在的内存注入代码。

C:\Windows\System32\cmd.exe - vol.py -f qmr.raw windows.malfind

```
F:\software\volatility3-develop>vol.py -f qmr.raw windows.malfind
Volatility 3 Framework 2.26.2
F:\software\volatility3-develop\volatility3\framework\deprecation.py:28: FutureWarning: This API (volatility3.plugins.wi
ndows.malware.malfind.Malfind.run) will be removed in the first release after 2026-06-07. This plugin has been renamed,
please call volatility3.plugins.windows.malware.malfind.Malfind rather than volatility3.plugins.windows.malfind.Malfind.

  warnings.warn(

PID     Process Start VPN       End VPN Tag     Protection      CommitCharge    PrivateMemory   File output     Notes
        Hexdump Disasm
F:\software\volatility3-develop\volatility3\framework\deprecation.py:105: FutureWarning: This plugin (volatility3.plugin
s.windows.malfind.Malfind) has been renamed and will be removed in the first release after 2026-06-07. Please ensure all
 method calls to this plugin are replaced with calls to volatility3.plugins.windows.malware.malfind.Malfind
  warnings.warn(

1972    svchost.exe     0x1c9619d0000   0x1c9619d2fff   VadS    PAGE_EXECUTE_READWRITE  3       1       Disabled
        N/A
7a 7a 7a 7a 48 81 ec 08 01 00 00 48 c7 44 24 68 zzzzH......H.D$h
00 00 00 00 e8 7b 09 00 00 48 89 84 24 b0 00 00 .....{...H..$...
00 48 8b 84 24 b0 00 00 00 48 89 84 24 d8 00 00 .H..$....H..$...
00 48 8b 84 24 b0 00 00 00 48 25 00 f0 ff ff 48 .H..$....H%....H        7a 7a 7a 7a 48 81 ec 08 01 00 00 48 c7 44 24 68
00 00 00 00 e8 7b 09 00 00 48 89 84 24 b0 00 00 00 48 8b 84 24 b0 00 00 00 48 89 84 24 d8 00 00 00 48 8b 84 24 b0 00 00
00 48 25 00 f0 ff ff 48
1972    svchost.exe     0x7ffdaf370000  0x7ffdaf37ffff  VadS    PAGE_EXECUTE_READWRITE  16      1       Disabled
        N/A
64 74 72 52 00 00 00 00 00 00 00 00 00 00 00 00 dtrR............
00 03 37 af fd 7f 00 00 00 00 00 00 00 00 00 00 ..7.............
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................        64 74 72 52 00 00 00 00 00 00 00 00 00 00 00 00
```

参考文献

参考文献

[1]翟继强,陈攀,徐晓,等.面向Windows 10系统段堆的内存取证研究[J].西北工业大学学报,2021,39(05):1139-1149.
[2]郑文庚,李凌崴,廖广军.Windows系统环境下基于内存分析的木马病毒取证[J].刑事技术,2020,45(06):572-576.DOI:10.16467/j.1008-3650.2020.06.005.
[3]丁兆锟,林思成.主机内存提取分析技术的研究与应用[J].电子技术与软件工程,2020,(23):240-241.DOI:10.20109/j.cnki.etse.2020.23.112.
[4]胡长栋.基于内存取证和行为分析的恶意代码检测方法研究[D].齐鲁工业大学,2024.DOI:10.27278/d.cnki.gsdqc.2024.000936.
[5]韩旭.基于内存取证技术的Windows代码注入攻击检测研究[D].哈尔滨理工大学,2023.DOI:10.27063/d.cnki.ghlgu.2023.001185.
[6]李桂丽.Windows物理内存电子数据取证研究-电子数据质量评测[D].甘肃政法大学,2023.DOI:10.27785/d.cnki.ggszf.2023.000472.
[7]张和禹.面向Windows恶意代码攻击的内存取证分析技术研究[D].战略支援部队信息工程大学,2023.DOI:10.27188/d.cnki.gzjxu.2023.000075.
[8]孙宏泰.Windows 10用户地址空间内存注入攻击取证研究[D].哈尔滨理工大学,2022.DOI:10.27063/d.cnki.ghlgu.2022.000688.

南京郵電大學
Nanjing University of Posts and Telecommunications

感谢聆听