

内存取证分析

一、 计算机物理内存简介

计算机的物理内存一般我们指的就是随机存取存储器(Random AccessMemory, 简称 RAM)。内存是一种易失性存储载体, 它保存处理器主动访问和存储的代码和数据, 是一个临时的数据交换空间。大多数的 PC 的内存属于一种动态是 RAM(DRAM)。它是动态变化的, 因其利用了电容器在充电和放电状态间的差异来存储数据的比特位。为了维持电容器的状态, 动态内存必须周期性刷新- 这也是内存控制器最典型的任务。

由于计算机的内存(DRAM)需要持续供电才能保持数据可持续访问, 因此也称为易失性存储。美国普林斯顿大学曾做过关于计算机冷启动攻击的研究, 计算机在断电后, 在很短的时间内内存的数据就会消失, 然而通过液态氮冷却, 可以将内存中的数据进行冻结, 再通过一些技术方法来解冻并获取原来的内存数据。以下我们先了解一下与内存相关的基本概念。

地址空间(Address Space)

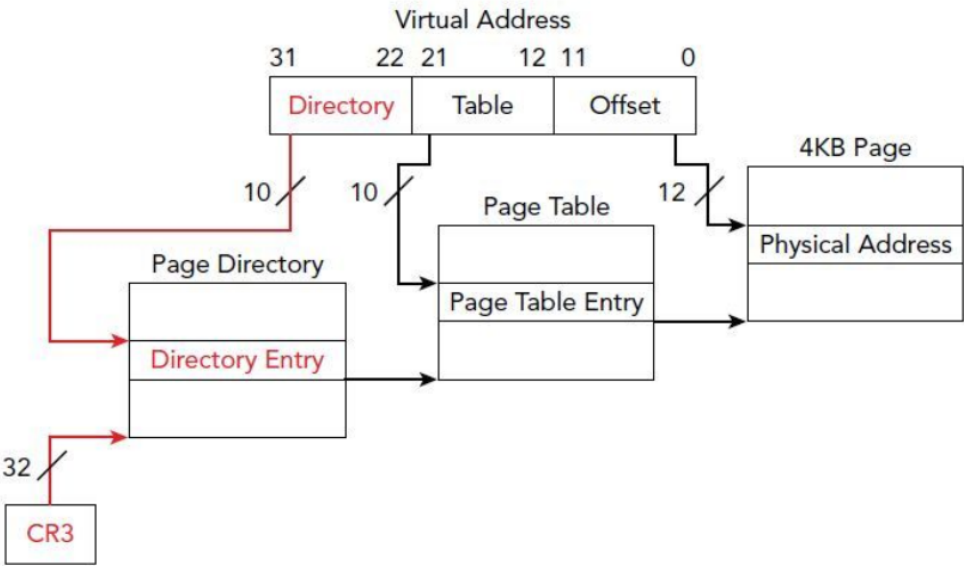
CPU 处理器要在执行指令并访问存储与内存中的数据, 它必须为要访问的数据制定一个唯一性地址。地址空间指的就是一组大量的有效地址, 可用于去识别存储与有限的内存分配空间中的数据。一个正在运行的程序可以访问的单个连续的地址空间一般称为线性地址空间。基于内存模型及采用的分页模式, 我们有时将其称为线性地址, 有时称为虚拟地址。通常我们使用物理地址空间来特指处理器请求访问物理内存的地址。这些地址是通过将线性地址转化为物理地址来获得。

内存分页(Paging)

从抽象意义上来讲页是一个具有固定尺寸的窗口, 从逻辑意义上来讲页是具有固定大小的一组连续线性地址的集合。

分页可以将线性地址空间进行虚拟化。它创建了一个执行环境，大量线性地址空间通过用适量的物理内存和磁盘存储进行模拟。每一个 32 位的线性地址空间被分为固定长度的片段，称为页 (Page)，页可以任何顺序将线性地址空间映射为物理内存。当程序尝试访问线性地址时，这样的映射使用了驻留内存的页目录 (Page Directory) 及页表 (Page Table) 来实现。

一个页的大小可以指定为 4KB (2¹²=4KB) 的任意倍数，这根据不同的体系结构或操作系统的设置而定，而 x86 架构下的 Windows/Linux 均采用 4KB 大小的分页方式，这就说明 32 位线性地址中必定存在一个 12 位的指示页内偏移量的域。



图表为内存分页机制

二、 物理内存中数据的价值

计算机终端及移动终端均使用了 RAM 易失性存储，主要用于数据交换、临时存储等用途。操作系统及各种应用软件均经常需要与物理内存进行数据交互，此外由于内存空间有限，因此计算机系统还可能将内存中的数据缓存到磁盘中，如 pagefile.sys (页交换文件) 及 hiberfil.sys (休眠文件)。

内存中有大量的各类数据，结构化及非结构化数据。通过对物理内存镜像可以提取出有价值的数据。常见有价值的数据，包含以下内容：

- 进程列表(包括恶意程序进程、Rootkit 隐藏进程等)
- 动态链接库（当前系统或程序加载的动态链接库）
- 打开文件列表（当前系统打开的文件列表）
- 网络连接（当前活动的网络连接）
- \$MFT 记录（常驻文件均可以直接提取恢复）
- 注册表（部分注册表信息，包括系统注册表 and 用户注册表文件）
- 加密密钥或密码（如 Windows 账户密码 Hash、BitLocker/SafeBoot/PGP/ TrueCrypt/VeraCrypt 等全盘加密或加密容器的恢复密钥等）
- 聊天记录(如 QQ 聊天记录片段)
- 互联网访问(上网记录 URL 地址、网页缓存及 InPrivate 隐私模式访问数据等)
- 电子邮件（如网页邮件缓存页面）
- 图片及文档等（尚未保存到磁盘中的图片、文档等文件）

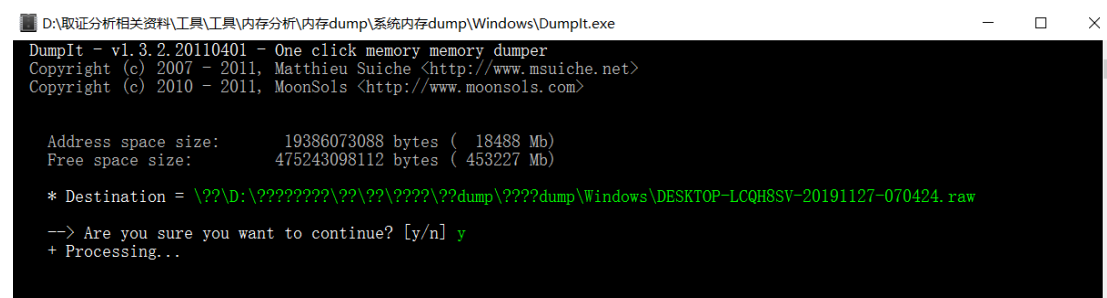
三、 Windows 内存取证方法和分析技术

内存取证(Memory Forensics)通常指对计算机及相关智能设备运行时的物理内存中存储的临时数据进行获取与分析，提取有价值的数据。内存是操作系统及各种软件交换数据的区域，数据易丢失(Volatile)，通常在关机后数据很快就消失。

常见物理内存获取方法：冷启动攻击(Cool Boot Attack)、基于火线(1394)或雷电(ThunderBolt)接口的直接内存访问(DMA)获取及内存获取软件工具。

不同的操作系统需要用到不同的物理内存获取工具。

Windows 操作系统平台下的 DumpIt 是一个简单易用的计算机内存镜像获取工具。通常直接将该工具存放在大容量移动硬盘或优盘中。可直接在正在运行 Windows 系统的平台直接运行，根据提示操作即可。



```
D:\取证分析相关资料\工具\工具\内存分析\内存dump\系统内存dump\Windows\DumpIt.exe
DumpIt - v1.3.2.20110401 - One click memory memory dumper
Copyright (c) 2007 - 2011, Matthieu Suiche <http://www.msuiche.net>
Copyright (c) 2010 - 2011, MoonSols <http://www.moonsols.com>

Address space size:      19386073088 bytes ( 18488 Mb)
Free space size:         475243098112 bytes ( 453227 Mb)

* Destination = \\D:\????????\??\??\????\??dump\????dump\Windows\DESKTOP-LCQH8SV-20191127-070424.raw
-> Are you sure you want to continue? [y/n] y
+ Processing...
```

图表为 DumpIt 内存镜像获取工具

内存分析技术

Windows 操作系统获取出的物理内存镜像需要使用专门的内存分析工具。常见的内存分析工具有 Volatility、Rekall、Forensic Toolkit (FTK)、取证大师及取证神探等，可以解析出常见的基本信息，包括进程信息、网络连接、加载的 DLL 文件及注册表加载信息等。

Volatility

Volatility 是一个完全开放的内存分析工具集，基于 GNU GPL2 许可，以 python 语言进行编写。由于 Volatility 是一款开源免费的工具，无需花任何钱即可进行内存数据的高级分析，此外代码开源的特点，遇到一些无法解决的问题时，还可以对源代码进行修改或扩展功能。

Volatility 支持的操作系统版本

- 64-bit Windows Server 2016
- 64-bit Windows Server 2012 及 2012 R2
- 32- and 64-bit Windows 10

- 32- and 64-bit Windows 8, 8.1, and 8.1 Update 1
- 32- and 64-bit Windows 7 (支持所有 Service Pack)
- 32- and 64-bit Windows Server 2008 (支持所有 Service Pack)
- 64-bit Windows Server 2008 R2 (支持所有 Service Pack)
- 32- and 64-bit Windows Vista (支持所有 Service Pack)
- 32- and 64-bit Windows Server 2003 (支持所有 Service Pack)
- 32- and 64-bit Windows XP (SP2 和 SP3)
- 32- and 64-bit Linux kernels (2.6.11 ~ 4.2.3)
- 32-bit 10.5.x Leopard (64-bit 10.5 Server 尚未支持)
- 32- and 64-bit 10.6.x Snow Leopard
- 32- and 64-bit 10.7.x Lion
- 64-bit 10.8.x Mountain Lion
- 64-bit 10.9.x Mavericks
- 64-bit 10.10.x Yosemite
- 64-bit 10.11.x El Capitan
- 64-bit 10.12.x Sierra

Volatility 支持的内存镜像格式

- 原始物理内存镜像格式
- 火线获取内存格式 (IEEE 1394)
- EWF 格式 (Expert Witness)
- 32- and 64-bit Windows 崩溃转储文件 (Crash Dump)
- 32- and 64-bit Windows 休眠文件 (Windows 7 及早期版本)
- 32- and 64-bit Mach0 文件
- Virtualbox Core Dumps
- VMware 保存状态文件 (.vmss) 及快照文件 (.vmsn)
- HPAK 格式 (FastDump)

- QEMU 内存转储文件

在 Windows 系统平台下，有两种方式可以运行 Volatility 工具。第一种是独立安装 Python 运行环境，再下载 Volatility 源代码执行命令行。第二种为下载 Volatility 独立 Windows 程序（无需另外安装和配置 Python 环境）。最新 Volatility 版本为 v2.6，可以通过官方网站进行下载。

在 Windows 64 位平台，最便捷的方式就是直接使用独立 Windows 程序的 Volatility 版本。进入管理员命令行模式，运行 `volatility_2.6_win64.exe` 程序即可。

Volatility 常用命令行参数

- `-h` 查看相关参数及帮助说明
- `-info` 查看相关模块名称及支持的 Windows 版本
- `-f` 指定要打开的内存镜像文件及路径
- `-d` 开启调试模式
- `-v` 开启显示详细信息模式(verbose)

插件名称	功能
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)
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
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
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
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

查看系统进程列表

```
volatility_2.6_win64>volatility_2.6_win64.exe -f JOHN-PC.raw --  
profile=Win7SP1x86_23418 pslist
```

```
D:\取证分析相关资料\工具\工具\内存分析\内存分析\volatility_2.6_win64>volatility_2.6_win64.exe -f JOHN-PC.  
raw --profile=Win7SP1x86_23418 pslist  
Volatility Foundation Volatility Framework 2.6  
Offset(V)  Name                PID  PPID  Thds    Hnds    Sess  Wow64  Start  
Exit  
-----  
0x8634b958 System                4    0    92     525    ----- 0 2019-05-09 11:18:22 UTC+0000  
0x877edc78 smss.exe             272   4     2      30    ----- 0 2019-05-09 11:18:22 UTC+0000  
0x87f98d40 csrss.exe            372  332    9     479    0 0 2019-05-09 11:18:31 UTC+0000  
0x87d1bd40 wininit.exe          424  332    3      80    0 0 2019-05-09 11:18:32 UTC+0000  
0x88042d40 csrss.exe            432  416   10     235    1 0 2019-05-09 11:18:32 UTC+0000  
0x8726b170 services.exe         496  424    9     212    0 0 2019-05-09 11:18:32 UTC+0000  
0x8872ad40 winlogon.exe       512  416    5     119    1 0 2019-05-09 11:18:32 UTC+0000  
0x87272880 lsass.exe            532  424    8     580    0 0 2019-05-09 11:18:33 UTC+0000  
0x872a3528 lsm.exe              540  424   10     142    0 0 2019-05-09 11:18:33 UTC+0000  
0x88187b50 svchost.exe          656  496   12     402    0 0 2019-05-09 11:18:34 UTC+0000  
0x88195030 vmacthlp.exe         720  496    3      55    0 0 2019-05-09 11:18:35 UTC+0000  
0x881a0030 svchost.exe          764  496    9     284    0 0 2019-05-09 11:18:36 UTC+0000  
0x881c1680 svchost.exe          848  496   22     487    0 0 2019-05-09 11:18:36 UTC+0000  
0x881df778 svchost.exe          896  496   18     437    0 0 2019-05-09 11:18:36 UTC+0000  
0x878f1c88 svchost.exe          940  496   37     964    0 0 2019-05-09 11:18:36 UTC+0000  
0x88208ce8 svchost.exe       1088  496   10     548    0 0 2019-05-09 11:18:38 UTC+0000  
0x88222900 svchost.exe       1180  496   19     490    0 0 2019-05-09 11:18:38 UTC+0000  
0x8828a968 spoolsv.exe       1372  496   12     306    0 0 2019-05-09 11:18:44 UTC+0000  
0x882951a8 svchost.exe       1416  496   18     317    0 0 2019-05-09 11:18:46 UTC+0000  
0x882ca030 svchost.exe       1520  496   16     246    0 0 2019-05-09 11:18:48 UTC+0000  
0x88217210 VMActhService        1560  496    3      87    0 0 2019-05-09 11:18:49 UTC+0000
```

上图为查看系统进程列表

查看网络通讯连接信息

```
volatility_2.6_win64>volatility_2.6_win64.exe -f JOHN-PC.raw --  
profile=Win7SP1x86_23418 netscan
```



```

D:\取证分析相关资料\工具\工具\内存分析\内存分析\volatility_2.6_win64>volatility_2.6_win64.exe -f JOHN-PC.
raw --profile=Win7SP1x86_23418 netscan
Volatility Foundation Volatility Framework 2.6
Offset(P)      Proto  Local Address      Foreign Address      State      Pid
Owner          Created
0x23a274a0     TCPv4   192.168.32.130:49163 201.220.152.101:80  ESTABLISHED 2348
thunkearcon.e
0x3dc28790     UDPv4   127.0.0.1:1900      *:.*                1520
svchost.exe    2019-05-09 13:47:33 UTC+0000
0x3dc403a8     UDPv4   0.0.0.0:68          *:.*                848
svchost.exe    2019-05-09 14:01:26 UTC+0000
0x3dc42bf8     UDPv4   192.168.32.130:137  *:.*                4
System         2019-05-09 13:47:33 UTC+0000
0x3dc902e8     UDPv4   0.0.0.0:3702        *:.*                1520
svchost.exe    2019-05-09 13:49:11 UTC+0000
0x3dc902e8     UDPv6   :::3702             *:.*                1520
svchost.exe    2019-05-09 13:49:11 UTC+0000
0x3dce8bc0     UDPv4   0.0.0.0:3702        *:.*                1520
svchost.exe    2019-05-09 13:49:11 UTC+0000
0x3de1a5f0     UDPv4   192.168.32.130:138  *:.*                4
System         2019-05-09 13:47:33 UTC+0000
0x3de626d0     UDPv4   0.0.0.0:3702        *:.*                1520
svchost.exe    2019-05-09 13:49:11 UTC+0000
0x3de66af8     UDPv4   0.0.0.0:0           *:.*                1180
svchost.exe    2019-05-09 13:47:33 UTC+0000
0x3de66af8     UDPv6   :::0                *:.*                1180
svchost.exe    2019-05-09 13:47:33 UTC+0000

```

上图为查看网络连接通信信息