应急响应之取证篇

笔记本： 应急
创建时间： 2022/11/2 9:33

1、简述

在用户遭受到攻击时，除了进行快速响应，可能还会进行取证，主要是对内存、硬盘、入侵流量、浏览器历史等方面内容进行取证。针对vmware虚拟环境，取证相对比较简单，直接拷贝相关目录下虚拟机目录即可，本文主要是对非虚拟环境系统进行取证，分别介绍常见的linux、windows系统。

2、windows系统

2.1 内存取证

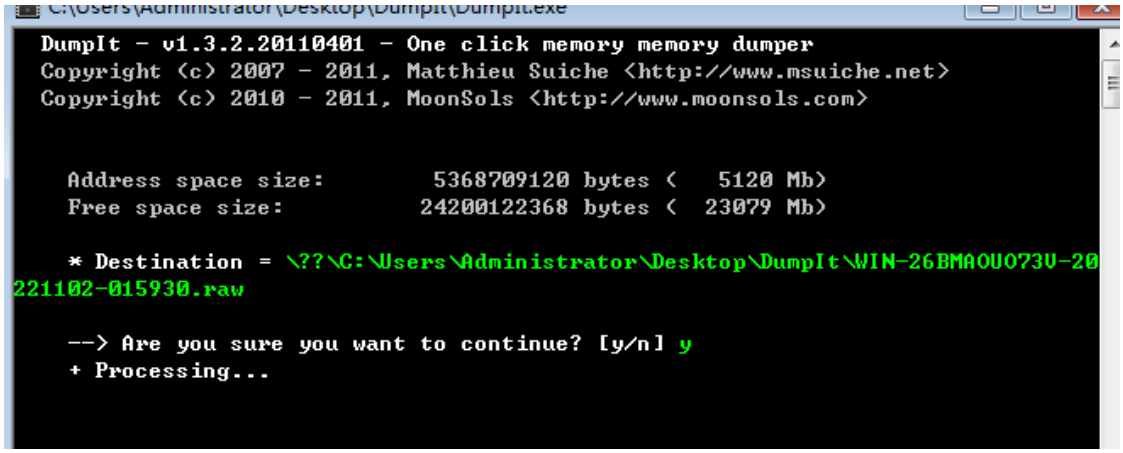
针对虚拟机获取内存，暂停vm并取出.vmem文件即可，很多木在马程序都有较高的隐秘性，可能会修改系统调用的返回值，但是在内存中的数据是真实存在的，所以在应急的时候如果无法从系统中找到痕迹，可看看内存中是否有相关字段，尤其是针对一些仅存于内存中，关机就消失的情况，内存取证是最好的办法。针对内存取证主要介绍两种工具，dumplt 、volatility两种工具。

2.1.1 DumpIt提取内存信息

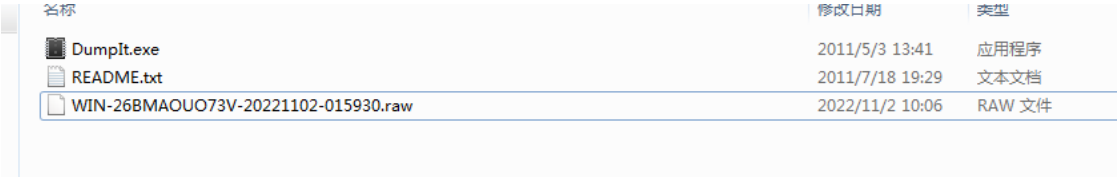
取证过程：
工具下载地址：

```
https://www.toolwar.com/search?q=dumpit
```

该软件大小只有200k，使用也比较简单，直接运行就会将内存存储到raw文件中



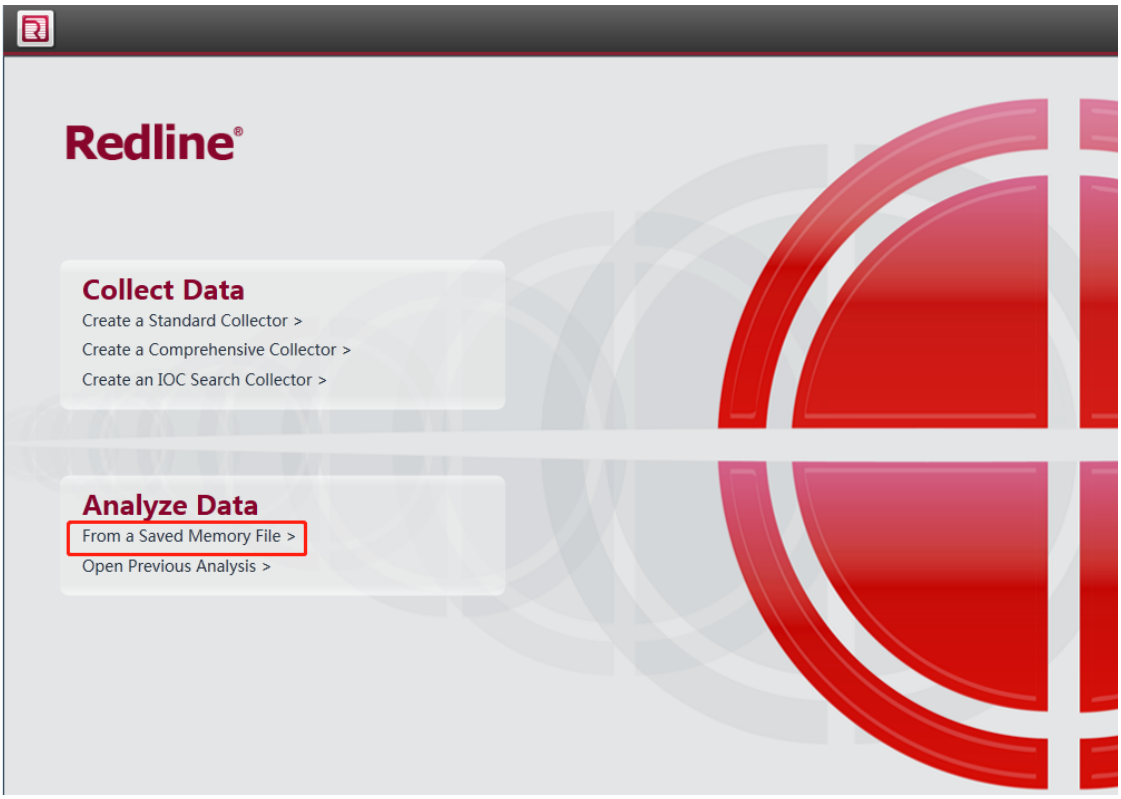
运行完成后在当前目录下生成内存存储文件



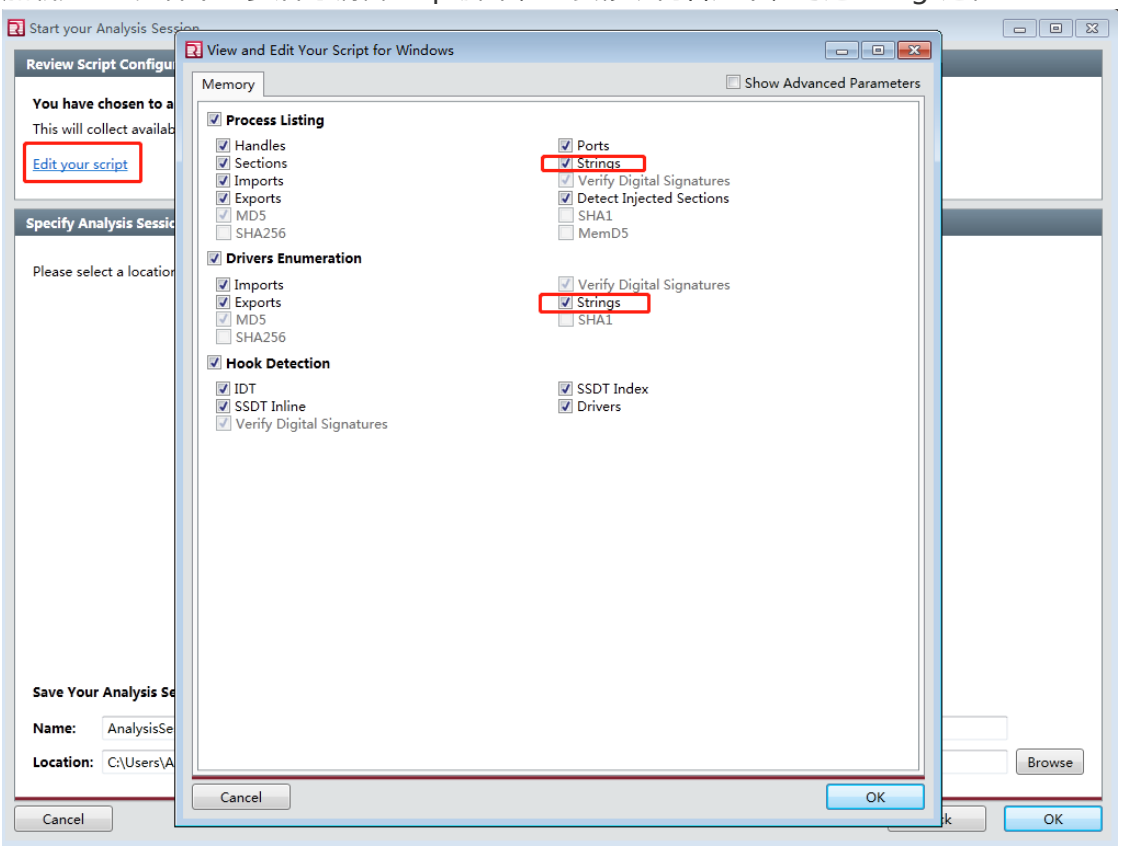
内存分析过程：
redline:
取证结束接下来就是进行内存分析，内存分析采用redline工具
工具下载地址：

```
https://fireeye.market/apps/211364
```

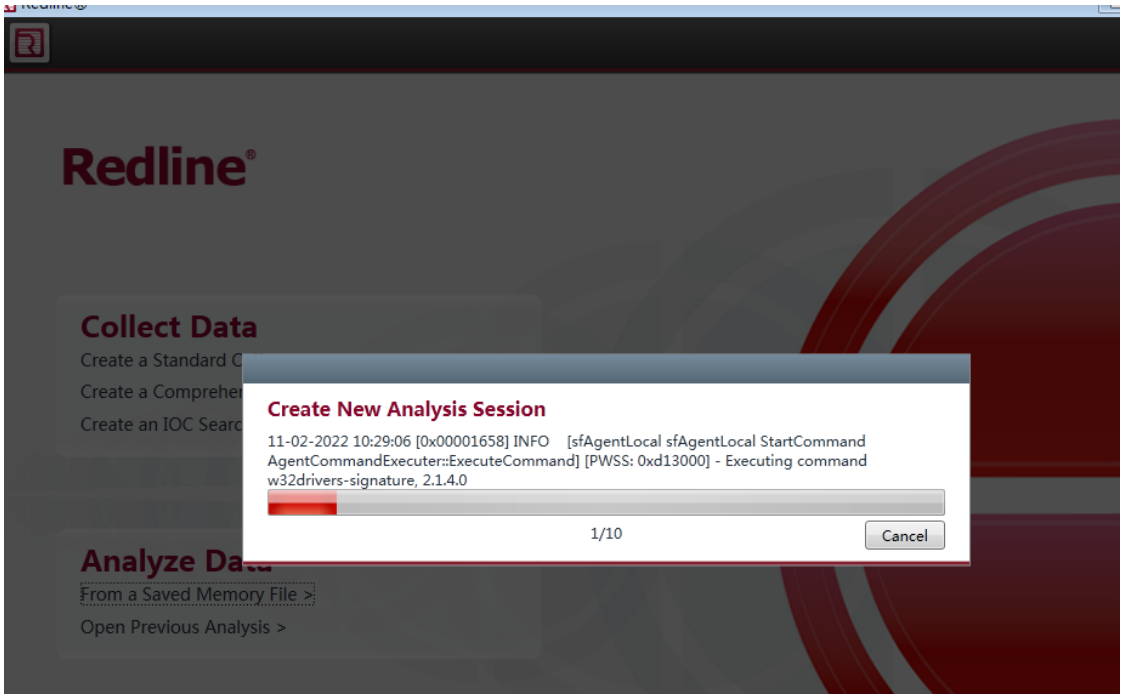
下载之后进行安装即可，安装完成后界面如下，双击已经获取内存镜像，加载之前保存的镜像即可(在进行内存备份时，由于系统使用情况的不同，所以最终备份的大小也不同，有的可能几十个g,所以在备份时建议使用大的硬盘或盘）)



加载完raw文件下一步后可编辑script脚本，主要修改内容如下，勾选strings选框



加载的后的页面如下，由于我保存后的内存大小大约为5G，所以过程可能会慢一些



在打开该软件进行分析时就一直卡在这里，所以还是建议利用Volatility进行分析。

Volatility:

该软件功能还是很强大的，是用python编写，下载地址：

```
https://github.com/volatilityfoundation/volatility
```

上述地址为volatility2.6的版本，所以首先需要python2.7的环境，具体安装过程可参考网上资料：

```
https://www.bnessy.com/archives/%E7%94%B5%E5%AD%90%E6%95%B0%E6%8D%AE%E5%8F%96%E8%
volatility
```

介绍几个常用的功能：

```
vol.py -h
```

查看一些常用的的用法

```
└─# vol.py -h
Volatility Foundation Volatility Framework 2.6.1
Usage: Volatility - A memory forensics analysis platform.

Options:
  -h, --help            list all available options and their default values.
                        Default values may be set in the configuration file
                        (/etc/volatilityrc)
  --conf-file=/root/.volatilityrc
                        User based configuration file
  -d, --debug           Debug volatility
  --plugins=PLUGINS     Additional plugin directories to use (colon separated
)
  --info                Print information about all registered objects
  --cache-directory=/root/.cache/volatility
                        Directory where cache files are stored
  --cache               Use caching
  --tz=TZ               Sets the (Olson) timezone for displaying timestamps
                        using pytz (if installed) or tzset
  -f FILENAME, --filename=FILENAME
                        Filename to use when opening an image
```

vol.py -f win.raw imageinfo 查看备份镜像相关信息

```
└─# vol.py -f win.raw imageinfo
Volatility Foundation Volatility Framework 2.6.1
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win
2008R2SP1x64_24000, Win2008R2SP1x64_23418, Win2008R2SP1x64, Win7SP1x64_24000,
 Win7SP1x64_23418
                     AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
                     AS Layer2 : FileAddressSpace (/root/Desktop/win.raw)
                      PAE type : No PAE
                           DTB : 0x187000L
                          KDBG : 0xf80004a45120L
          Number of Processors : 4
     Image Type (Service Pack) : 1
                KPCR for CPU 0 : 0xfffff80004a47000L
                KPCR for CPU 1 : 0xfffff88004700000L
                KPCR for CPU 2 : 0xfffff8800477e000L
                KPCR for CPU 3 : 0xfffff880009b1000L
             KUSER_SHARED_DATA : 0xfffff78000000000L
           Image date and time : 2022-11-02 02:05:28 UTC+0000
     Image local date and time : 2022-11-02 10:05:28 +0800
```

vol.py -f win.raw --profile=Win7SP1x64 pslist 查看内存中运行的进程信息

```
└─# vol.py -f win.raw --profile=Win7SP1x64 pslist
Volatility Foundation Volatility Framework 2.6.1
Offset(V)          Name                    PID   PPID   Thds     Hnds   Sess
 Wow64 Start                         Exit
---------- -------------------- ------ ------ ------ -------- ------
------ ------------------------------ ------------------------------
0xfffffa8030e58b00 System                    4      0    116      579 ------
     0 2022-11-02 01:29:34 UTC+0000
0xfffffa80318cc920 smss.exe                300      4      2       32 ------
     0 2022-11-02 01:29:34 UTC+0000
0xfffffa803223eb00 csrss.exe               400    392      9      956      0
     0 2022-11-02 01:29:37 UTC+0000
0xfffffa8032087b00 wininit.exe             480    392      3       82      0
     0 2022-11-02 01:29:37 UTC+0000
0xfffffa803208bb00 csrss.exe               492    472     12      492      1
     0 2022-11-02 01:29:37 UTC+0000
0xfffffa80320e94a0 services.exe            540    480      7      249      0
     0 2022-11-02 01:29:37 UTC+0000
0xfffffa80320fdb00 winlogon.exe            564    472      3      121      1
     0 2022-11-02 01:29:37 UTC+0000
0xfffffa8032105060 lsass.exe               572    480      9      779      0
     0 2022-11-02 01:29:37 UTC+0000
0xfffffa803207eb00 lsm.exe                 580    480     10      210      0
     0 2022-11-02 01:29:37 UTC+0000
0xfffffa8032498060 svchost.exe             704    540     10      375      0
     0 2022-11-02 01:29:38 UTC+0000
0xfffffa80324d3540 HipsDaemon.exe          772    540     41      317      0
     1 2022-11-02 01:29:39 UTC+0000
0xfffffa80324f8b00 vmacthlp.exe            804    540      3       61      0
     0 2022-11-02 01:29:40 UTC+0000
0xfffffa803252fb00 svchost.exe             872    540      8      282      0
     0 2022-11-02 01:29:40 UTC+0000
0xfffffa803257bb00 svchost.exe             960    540     19      492      0
     0 2022-11-02 01:29:41 UTC+0000
0xfffffa80325a52a0 svchost.exe            1012    540     19      428      0
     0 2022-11-02 01:29:41 UTC+0000
0xfffffa80325dcb00 svchost.exe             316    540     47     1192      0
     0 2022-11-02 01:29:41 UTC+0000
0xfffffa8032658b00 svchost.exe             892    540      9      535      0
     0 2022-11-02 01:29:41 UTC+0000
0xfffffa803269d170 svchost.exe            1096    540     28      604      0
     0 2022-11-02 01:29:42 UTC+0000
0xfffffa803274fb00 usysdiag.exe           1172    772     11      104      0
```

查看注册表中的用户信息:

```
vol.py -f win.raw --profile=Win7SP1x64 printkey -K
"SAM\Domains\Account\Users\Names"
```

```
└─# vol.py -f win.raw --profile=Win7SP1x64 printkey -K "SAM\Domains\Account\Users\Names"
Volatility Foundation Volatility Framework 2.6.1
Legend: (S) = Stable   (V) = Volatile

----------------------------
Registry: \SystemRoot\System32\Config\SAM
Key name: Names (S)
Last updated: 2019-11-12 09:31:23 UTC+0000

Subkeys:
  (S) 123
  (S) admin
  (S) Administrator
  (S) Guest

Values:
REG_NONE                      : (S)
```

获取系统最后登录的账号

```
vol.py -f win.raw --profile=Win7SP1x64  printkey -K
"SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon"
```

```
└─# vol.py -f win.raw --profile=Win7SP1x64  printkey -K "SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon"
Volatility Foundation Volatility Framework 2.6.1
Legend: (S) = Stable   (V) = Volatile

----------------------------
Registry: \??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT
Key name: Winlogon (S)
Last updated: 2009-07-14 04:45:47 UTC+0000

Subkeys:

Values:
REG_SZ        ExcludeProfileDirs : (S) AppData\Local;AppData\LocalLow;$Recycle.Bin
----------------------------
Registry: \??\C:\Users\Administrator\ntuser.dat
Key name: Winlogon (S)
Last updated: 2017-08-24 09:01:57 UTC+0000

Subkeys:

Values:
REG_SZ        ExcludeProfileDirs : (S) AppData\Local;AppData\LocalLow;$Recycle.Bin
REG_DWORD     BuildNumber        : (S) 7601
REG_DWORD     FirstLogon         : (S) 0
REG_SZ        ParseAutoexec      : (S) 1
----------------------------
Registry: \??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT
Key name: Winlogon (S)
Last updated: 2009-07-14 04:45:48 UTC+0000

Subkeys:

Values:
REG_SZ        ExcludeProfileDirs : (S) AppData\Local;AppData\LocalLow;$Recycle.Bin
```

获取当前用户正在运行的程序

```
vol.py -f win.raw --profile=Win7SP1x64  userassist
```

```
└─# vol.py -f win.raw --profile=Win7SP1x64  userassist
Volatility Foundation Volatility Framework 2.6.1
----------------------------
Registry: \??\C:\Users\Administrator\ntuser.dat
Path: Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count
Last updated: 2022-11-02 02:05:08 UTC+0000

Subkeys:

Values:

REG_BINARY    Microsoft.Windows.GettingStarted :
Count:          0
Focus Count:    0
Time Focused:   0:00:00.500000
Last updated:   2017-08-23 12:59:55 UTC+0000
Raw Data:
0x00000000  02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0x00000010  63 46 65 3d 00 00 00 00 00 00 80 bf 00 00 80 bf   cFe=............
0x00000020  00 00 80 bf 00 00 80 bf 00 00 80 bf 00 00 80 bf   ................
0x00000030  00 00 80 bf 00 00 80 bf 01 00 00 00 0b 30 80 b7   .............0..
0x00000040  0f 1c d3 01 00 00 00 00                            ........

REG_BINARY    UEME_CTLSESSION :
Count:          340
Focus Count:    2667
Time Focused:   1 day, 6:52:33.014000
Last updated:   1970-01-01 00:00:00 UTC+0000
Raw Data:
0x00000000  02 00 00 00 54 01 00 00 6b 0a 00 00 82 0d a0 06   ....T...k.......
0x00000010  2c 00 00 00 db 00 00 00 93 ac 7c 00 7b 00 31 00   ,.........|.{.1.
0x00000020  41 00 43 00 31 00 34 00 45 00 37 00 37 00 2d 00   A.C.1.4.E.7.7.-.
0x00000030  30 00 32 00 45 00 37 00 2d 00 34 00 45 00 35 00   0.2.E.7.-.4.E.5.
0x00000040  44 00 2d 00 42 00 37 00 34 00 34 00 2d 00 32 00   D.-.B.7.4.4.-.2.
0x00000050  45 00 42 00 31 00 41 00 45 00 35 00 31 00 39 00   E.B.1.A.E.5.1.9.
0x00000060  38 00 42 00 37 00 7d 00 5c 00 63 00 6d 00 64 00   8.B.7.}.\.c.m.d.
0x00000070  2e 00 65 00 78 00 65 00 00 00 65 00 00 00 ee ff   ..e.x.e...e.....
0x00000080  f8 1b 0f 03 00 00 00 00 86 00 8a 01 00 00 00 00   ................
0x00000090  1e ff 20 20 00 00 00 00 eb e6 4f 7b 5d ee 00 00   ..........O{]...
0x000000a0  00 00 00 00 00 00 00 00 f8 1b 0f 03 00 00 00 00   ................
0x000000b0  4f 07 01 20 00 00 00 00 20 00 00 00 00 00 00 00   O...............
0x000000c0  f8 1c 0f 03 00 00 00 00 00 00 00 00 00 00 00 00   ................
0x000000d0  00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00   ................
0x000000e0  00 00 00 00 00 00 00 00 0e 2c 84 fe fe 07 00 00   .....,..........
```

显示cmd历史命令

```
vol.py -f win.raw --profile=Win7SP1x64  cmdscan
```

```
└─# vol.py -f win.raw --profile=Win7SP1x64  cmdscan
Volatility Foundation Volatility Framework 2.6.1
**************************************************
CommandProcess: conhost.exe Pid: 5056
CommandHistory: 0x2c69f0 Application: DumpIt.exe Flags: Allocated
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x60
**************************************************
CommandProcess: conhost.exe Pid: 5620
CommandHistory: 0x3f4890 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 3 LastAdded: 2 LastDisplayed: 2
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x60
Cmd #0 @ 0x3f3d70: netstat -ant
Cmd #1 @ 0x3e1f60: tasklist
Cmd #2 @ 0x3e1f80: ipconfig
```

查看网络连接，已经侦听、建立、关闭的连接

```
└─# vol.py -f win.raw --profile=Win7SP1x64  netscan
Volatility Foundation Volatility Framework 2.6.1
Offset(P)          Proto    Local Address                  Foreign Address      State            Pid      Owner          Created
0x1bbe4010         TCPv4    192.168.13.131:1055            69.192.13.224:443    CLOSED           4088     jucheck.exe
0x21792d70         UDPv4    0.0.0.0:58234                  *:*                                   1096     svchost.exe    2022-11-02 02:05:32 UTC+0000
0x21e179a0         TCPv4    0.0.0.0:5082                   0.0.0.0:0            LISTENING        4024     SecurityInput.
0x24d90ad0         TCPv4    0.0.0.0:8834                   0.0.0.0:0            LISTENING        3876     nessusd.exe
0x2df5b550         TCPv4    127.0.0.1:1047                 127.0.0.1:1048       ESTABLISHED      3876     nessusd.exe
0x37a60ef0         TCPv4    127.0.0.1:54530                0.0.0.0:0            LISTENING        4964     ECAgent.exe
0x3cfd8b70         TCPv4    127.0.0.1:1050                 127.0.0.1:54530      ESTABLISHED      2068     SangforPromote
0x527a7010         TCPv4    192.168.13.131:1054            69.192.13.224:443    CLOSED           3516     jusched.exe
0xb1df6010         TCPv4    192.168.13.131:1057            69.192.13.224:443    CLOSED           34996241
0x117aa7620        TCPv4    192.168.192.132:139            0.0.0.0:0            LISTENING        4        System
0x1346d9770        TCPv4    127.0.0.1:54530                127.0.0.1:1050       ESTABLISHED      4964     ECAgent.exe
0x139935950        UDPv4    0.0.0.0:58667                  *:*                                   5532     LoveCloud.exe  2022-11-02 02:04:04 UTC+0000
0x13accf010        UDPv4    0.0.0.0:60318                  *:*                                   1096     svchost.exe    2022-11-02 02:05:56 UTC+0000
0x13b40c900        UDPv4    0.0.0.0:5353                   *:*                                   4316     chrome.exe     2022-11-02 02:03:34 UTC+0000
0x13b6ccd20        UDPv4    0.0.0.0:58381                  *:*                                   1096     svchost.exe    2022-11-02 02:05:59 UTC+0000
0x13b997ec0        UDPv4    0.0.0.0:5353                   *:*                                   4316     chrome.exe     2022-11-02 02:03:34 UTC+0000
0x13b997ec0        UDPv6    :::5353                        *:*                                   4316     chrome.exe     2022-11-02 02:03:34 UTC+0000
0x13ca982f0        UDPv4    127.0.0.1:1900                 *:*                                   4500     svchost.exe    2022-11-02 02:03:12 UTC+0000
0x13cb27900        UDPv4    192.168.192.132:1900           *:*                                   4500     svchost.exe    2022-11-02 02:03:12 UTC+0000
0x13cc1b340        UDPv4    192.168.192.132:137            *:*                                   4        System         2022-11-02 02:03:13 UTC+0000
0x13cc637d0        UDPv4    192.168.192.132:138            *:*                                   4        System         2022-11-02 02:03:13 UTC+0000
0x13ccda010        UDPv6    fe80::4142:f337:fba7:eda3:60477 *:*                                   4500     svchost.exe    2022-11-02 02:03:13 UTC+0000
0x13cd042a0        UDPv4    127.0.0.1:60480                *:*                                   4500     svchost.exe    2022-11-02 02:03:13 UTC+0000
0x13cd1de30        UDPv4    192.168.192.132:60479          *:*                                   4500     svchost.exe    2022-11-02 02:03:13 UTC+0000
0x13cd28010        UDPv4    0.0.0.0:5355                   *:*                                   1096     svchost.exe    2022-11-02 02:03:13 UTC+0000
0x13cd4ec60        UDPv6    ::1:60478                      *:*                                   4500     svchost.exe    2022-11-02 02:03:13 UTC+0000
0x13cd73840        UDPv4    0.0.0.0:5355                   *:*                                   1096     svchost.exe    2022-11-02 02:03:13 UTC+0000
0x13cd73840        UDPv6    :::5355                        *:*                                   1096     svchost.exe    2022-11-02 02:03:13 UTC+0000
0x13cf829b0        UDPv6    ::1:1900                       *:*                                   4500     svchost.exe    2022-11-02 02:03:12 UTC+0000
0x13cf88ec0        UDPv6    fe80::4142:f337:fba7:eda3:1900 *:*                                   4500     svchost.exe    2022-11-02 02:03:12 UTC+0000
0x13ce95da0        TCPv4    127.0.0.1:1241                 0.0.0.0:0            LISTENING        3876     nessusd.exe
0x13cf0cb90        TCPv4    0.0.0.0:8834                   0.0.0.0:0            LISTENING        3876     nessusd.exe
0x13cf0cb90        TCPv6    :::8834                        :::0                 LISTENING        3876     nessusd.exe
0x13d2ad860        TCPv4    0.0.0.0:1043                   0.0.0.0:0            LISTENING        3876     nessusd.exe
```

查看ie浏览记录

```
vol.py -f win.raw --profile=Win7SP1x64  iehistory
```

```
└─# vol.py -f win.raw --profile=Win7SP1x64  iehistory
Volatility Foundation Volatility Framework 2.6.1
**************************************************
Process: 3516 jusched.exe
Cache type "URL " at 0x8f5000
Record length: 0x100
Location: Cookie:administrator@google.co.uk/
Last modified: 2017-12-30 10:19:43 UTC+0000
Last accessed: 2017-12-30 10:19:43 UTC+0000
File Offset: 0x100, Data Offset: 0x8c, Data Length: 0x0
File: administrator@google.co[1].txt
**************************************************
Process: 3516 jusched.exe
Cache type "URL " at 0x8f5100
Record length: 0x100
Location: Cookie:administrator@whoer.net/
Last modified: 2017-12-30 10:31:28 UTC+0000
Last accessed: 2017-12-30 10:31:28 UTC+0000
File Offset: 0x100, Data Offset: 0x88, Data Length: 0x0
File: administrator@whoer[1].txt
**************************************************
Process: 3516 jusched.exe
Cache type "URL " at 0x8f5200
Record length: 0x100
Location: Cookie:administrator@google.com/
Last modified: 2017-12-30 10:14:09 UTC+0000
Last accessed: 2018-01-10 06:56:02 UTC+0000
File Offset: 0x100, Data Offset: 0x8c, Data Length: 0x0
File: administrator@google[1].txt
**************************************************
Process: 3516 jusched.exe
Cache type "URL " at 0x8f5300
Record length: 0x100
Location: Cookie:administrator@refreshyourcache.com/
Last modified: 2017-12-30 10:31:28 UTC+0000
Last accessed: 2017-12-30 10:31:28 UTC+0000
File Offset: 0x100, Data Offset: 0x94, Data Length: 0x0
File: administrator@refreshyourcache[2].txt
**************************************************
Process: 3516 jusched.exe
Cache type "URL " at 0x8f5400
Record length: 0x100
Location: Cookie:administrator@scorecardresearch.com/
Last modified: 2017-12-30 10:14:12 UTC+0000
Last accessed: 2018-01-22 00:52:13 UTC+0000
File Offset: 0x100, Data Offset: 0x94, Data Length: 0x0
File: administrator@scorecardresearch[2].txt
```

时间线:

```
vol.py -f win.raw --profile=Win7SP1x64  timeliner
```

从多个位置收集大量活动信息

```
└─# vol.py -f win.raw --profile=Win7SP1x64  timeliner
Volatility Foundation Volatility Framework 2.6.1
2022-11-02 02:05:28 UTC+0000|[LIVE RESPONSE]| (System time)|
2017-12-30 10:19:43 UTC+0000|[IEHISTORY]| jusched.exe→Cookie:administrator@google.co.uk/| PID: 3516/Cache type "URL " at 0×8f5000 End: 2017-12-30 10:19:43 UTC+0000
2017-12-30 10:31:28 UTC+0000|[IEHISTORY]| jusched.exe→Cookie:administrator@whoer.net/| PID: 3516/Cache type "URL " at 0×8f5100 End: 2017-12-30 10:31:28 UTC+0000
2017-12-30 10:14:09 UTC+0000|[IEHISTORY]| jusched.exe→Cookie:administrator@google.com/| PID: 3516/Cache type "URL " at 0×8f5200 End: 2018-01-10 06:56:02 UTC+0000
2017-12-30 10:31:28 UTC+0000|[IEHISTORY]| jusched.exe→Cookie:administrator@refreshyourcache.com/| PID: 3516/Cache type "URL " at 0×8f5300 End: 2017-12-30 10:31:28 UTC+00
2017-12-30 10:14:12 UTC+0000|[IEHISTORY]| jusched.exe→Cookie:administrator@scorecardresearch.com/| PID: 3516/Cache type "URL " at 0×8f5400 End: 2018-01-22 00:52:13 UTC+0
2018-01-22 01:08:21 UTC+0000|[IEHISTORY]| jusched.exe→Cookie:administrator@www.msn.cn/| PID: 3516/Cache type "URL " at 0×8f5500 End: 2018-01-25 01:48:07 UTC+0000
2019-08-30 03:16:30 UTC+0000|[IEHISTORY]| jusched.exe→Cookie:administrator@bing.com/| PID: 3516/Cache type "URL " at 0×8f5600 End: 2019-09-05 05:23:29 UTC+0000
2018-01-22 01:08:21 UTC+0000|[IEHISTORY]| jusched.exe→Cookie:administrator@linkedin.com/| PID: 3516/Cache type "URL " at 0×8f5700 End: 2018-01-25 01:48:45 UTC+0000
2018-01-10 06:58:14 UTC+0000|[IEHISTORY]| jusched.exe→Cookie:administrator@collect.installeranalytics.com/| PID: 3516/Cache type "URL " at 0×8f5800 End: 2018-01-10 06:58
2018-01-25 01:48:48 UTC+0000|[IEHISTORY]| jusched.exe→Cookie:administrator@adnxs.com/| PID: 3516/Cache type "URL " at 0×8f5900 End: 2018-01-25 01:48:48 UTC+0000
2017-12-30 10:14:35 UTC+0000|[IEHISTORY]| jusched.exe→Cookie:administrator@www.linkedin.com/| PID: 3516/Cache type "URL " at 0×8f5a00 End: 2017-12-30 10:14:35 UTC+0000
2018-01-25 01:48:44 UTC+0000|[IEHISTORY]| jusched.exe→Cookie:administrator@c.bing.com/| PID: 3516/Cache type "URL " at 0×8f5b00 End: 2018-01-25 01:48:44 UTC+0000
2018-01-25 03:15:39 UTC+0000|[IEHISTORY]| jusched.exe→Cookie:administrator@c.msn.cn/| PID: 3516/Cache type "URL " at 0×8f5c00 End: 2018-01-25 03:15:39 UTC+0000
2017-12-30 10:15:05 UTC+0000|[IEHISTORY]| jusched.exe→Cookie:administrator@yandex.ru/| PID: 3516/Cache type "URL " at 0×8f5d00 End: 2017-12-30 10:15:05 UTC+0000
2018-01-21 13:08:40 UTC+0000|[IEHISTORY]| jusched.exe→Cookie:administrator@get.sogou.com/| PID: 3516/Cache type "URL " at 0×8f5e00 End: 2022-11-01 03:13:27 UTC+0000
2018-01-30 07:07:05 UTC+0000|[IEHISTORY]| jusched.exe→Cookie:administrator@ptlogin2.qq.com/| PID: 3516/Cache type "URL " at 0×8f5f00 End: 2018-01-30 07:07:05 UTC+0000
2019-07-11 14:02:43 UTC+0000|[IEHISTORY]| jusched.exe→Cookie:administrator@qq.com/| PID: 3516/Cache type "URL " at 0×8f6000 End: 2022-11-01 08:16:40 UTC+0000
2018-01-22 00:52:14 UTC+0000|[IEHISTORY]| jusched.exe→Cookie:administrator@msn.cn/| PID: 3516/Cache type "URL " at 0×8f6100 End: 2018-01-25 01:48:07 UTC+0000
2022-10-31 03:11:36 UTC+0000|[IEHISTORY]| jusched.exe→Cookie:administrator@soso.com/| PID: 3516/Cache type "URL " at 0×8f6200 End: 2022-11-01 03:13:25 UTC+0000
2018-01-11 01:44:35 UTC+0000|[IEHISTORY]| jusched.exe→Cookie:administrator@hm.baidu.com/| PID: 3516/Cache type "URL " at 0×8f6300 End: 2018-01-30 00:39:40 UTC+0000
2022-10-31 03:11:36 UTC+0000|[IEHISTORY]| jusched.exe→Cookie:administrator@sohu.com/| PID: 3516/Cache type "URL " at 0×8f6400 End: 2022-11-01 03:13:25 UTC+0000
2018-01-21 13:03:50 UTC+0000|[IEHISTORY]| jusched.exe→Cookie:administrator@security.ie.sogou.com/| PID: 3516/Cache type "URL " at 0×8f6500 End: 2018-01-30 07:07:09 UTC+0
2022-11-01 08:51:34 UTC+0000|[IEHISTORY]| jusched.exe→Cookie:administrator@sogou.com/| PID: 3516/Cache type "URL " at 0×8f6600 End: 2022-11-01 08:51:34 UTC+0000
2018-01-25 01:48:47 UTC+0000|[IEHISTORY]| jusched.exe→Cookie:administrator@ads.linkedin.com/| PID: 3516/Cache type "URL " at 0×8f6700 End: 2018-01-25 01:48:47 UTC+0000
2019-07-21 23:57:04 UTC+0000|[IEHISTORY]| jusched.exe→Cookie:administrator@10.28.1.1/| PID: 3516/Cache type "URL " at 0×8f6800 End: 2019-07-21 23:57:06 UTC+0000
2022-11-01 05:53:24 UTC+0000|[IEHISTORY]| jusched.exe→Cookie:administrator@sogou.com/| PID: 3516/Cache type "URL " at 0×8f6900 End: 2022-11-01 08:51:32 UTC+0000
2022-10-31 03:06:43 UTC+0000|[IEHISTORY]| jusched.exe→Cookie:administrator@sogo.com/| PID: 3516/Cache type "URL " at 0×8f6a00 End: 2022-11-01 08:51:32 UTC+0000
2018-01-26 03:34:29 UTC+0000|[IEHISTORY]| jusched.exe→Cookie:administrator@zhuanlan.zhihu.com/| PID: 3516/Cache type "URL " at 0×8f6b00 End: 2018-01-26 03:34:29 UTC+0000
2018-01-26 08:31:58 UTC+0000|[IEHISTORY]| jusched.exe→Cookie:administrator@baidu.com/| PID: 3516/Cache type "URL " at 0×8f6c00 End: 2018-01-30 00:39:40 UTC+0000
2019-08-30 03:16:30 UTC+0000|[IEHISTORY]| jusched.exe→Cookie:administrator@www.bing.com/| PID: 3516/Cache type "URL " at 0×8f6d00 End: 2019-09-05 05:23:30 UTC+0000
2017-10-16 09:03:26 UTC+0000|[IEHISTORY]| jusched.exe→Cookie:administrator@baizhu.cc/| PID: 3516/Cache type "URL " at 0×8f6e00 End: 2017-10-16 09:07:41 UTC+0000
2017-10-16 09:04:59 UTC+0000|[IEHISTORY]| jusched.exe→Cookie:administrator@mmstat.com/| PID: 3516/Cache type "URL " at 0×8f6f00 End: 2017-10-16 09:08:50 UTC+0000
2017-10-16 09:08:19 UTC+0000|[IEHISTORY]| jusched.exe→Cookie:administrator@cdn.baizhu.cc/| PID: 3516/Cache type "URL " at 0×8f7000 End: 2017-10-16 09:08:19 UTC+0000
2017-10-16 09:11:30 UTC+0000|[IEHISTORY]| jusched.exe→Cookie:administrator@ty229.com/| PID: 3516/Cache type "URL " at 0×8f7100 End: 2017-10-16 09:11:30 UTC+0000
2017-10-16 09:08:19 UTC+0000|[IEHISTORY]| jusched.exe→Cookie:administrator@cnzz.com/| PID: 3516/Cache type "URL " at 0×8f7200 End: 2017-11-02 06:32:57 UTC+0000
2017-10-16 09:08:50 UTC+0000|[IEHISTORY]| jusched.exe→Cookie:administrator@csbew.com/| PID: 3516/Cache type "URL " at 0×8f7300 End: 2017-10-16 09:08:50 UTC+0000
2017-10-16 09:08:50 UTC+0000|[IEHISTORY]| jusched.exe→Cookie:administrator@alimama.com/| PID: 3516/Cache type "URL " at 0×8f7400 End: 2017-10-16 09:08:50 UTC+0000
2017-10-16 09:08:52 UTC+0000|[IEHISTORY]| jusched.exe→Cookie:administrator@hot.eastday.com/| PID: 3516/Cache type "URL " at 0×8f7500 End: 2017-10-16 09:08:52 UTC+0000
2017-10-16 09:08:50 UTC+0000|[IEHISTORY]| jusched.exe→Cookie:administrator@eastday.com/| PID: 3516/Cache type "URL " at 0×8f7600 End: 2017-10-16 09:08:50 UTC+0000
2017-10-16 09:08:54 UTC+0000|[IEHISTORY]| jusched.exe→Cookie:administrator@pos.baidu.com/| PID: 3516/Cache type "URL " at 0×8f7700 End: 2017-10-16 09:08:54 UTC+0000
2017-11-15 08:16:41 UTC+0000|[IEHISTORY]| jusched.exe→Cookie:administrator@linkedin.com/| PID: 3516/Cache type "URL " at 0×8f7800 End: 2017-12-30 10:10:41 UTC+0000
2017-10-16 13:21:56 UTC+0000|[IEHISTORY]| jusched.exe→Cookie:administrator@www.maizuo.com/| PID: 3516/Cache type "URL " at 0×8f7900 End: 2017-10-16 13:21:56 UTC+0000
2017-10-16 13:20:36 UTC+0000|[IEHISTORY]| jusched.exe→Cookie:administrator@jiayuan.com/| PID: 3516/Cache type "URL " at 0×8f7a00 End: 2017-10-16 13:20:36 UTC+0000
2017-10-16 13:20:31 UTC+0000|[IEHISTORY]| jusched.exe→Cookie:administrator@keepc.com/| PID: 3516/Cache type "URL " at 0×8f7b00 End: 2017-10-16 13:20:31 UTC+0000
2017-10-16 13:20:57 UTC+0000|[IEHISTORY]| jusched.exe→Cookie:administrator@member.csc86.com/| PID: 3516/Cache type "URL " at 0×8f7c00 End: 2017-10-16 13:20:57 UTC+0000
2017-12-30 09:57:08 UTC+0000|[IEHISTORY]| jusched.exe→Cookie:administrator@sogou.com/| PID: 3516/Cache type "URL " at 0×8f7d00 End: 2017-12-30 09:57:08 UTC+0000
2017-10-16 13:21:42 UTC+0000|[IEHISTORY]| jusched.exe→Cookie:administrator@baixing.com/| PID: 3516/Cache type "URL " at 0×8f7e00 End: 2017-10-16 13:21:42 UTC+0000
2017-10-16 13:22:01 UTC+0000|[IEHISTORY]| jusched.exe→Cookie:administrator@reg.ztgame.com/| PID: 3516/Cache type "URL " at 0×8f7f00 End: 2017-10-16 13:22:01 UTC+0000
```

查看密码：

```
vol.py -f win.raw --profile=Win7SP1x64    hashdump
```

```
┌──(root㉿kali)-[~/Desktop]
└─# vol.py -f win.raw --profile=Win7SP1x64    hashdump
Volatility Foundation Volatility Framework 2.6.1
Administrator:500:aad3b435b51404eeaad3b435b51404ee:62a29ec9300590e70beaa19021e661c1:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
123:1004:aad3b435b51404eeaad3b435b51404ee:5a420e7750b39be09fa29d314fa4b51c:::
admin:1005:aad3b435b51404eeaad3b435b51404ee:e1f3346aeb4f283cb4687ecfaa1122af:::

┌──(root㉿kali)-[~/Desktop]
└─#
```

hash破解网站：

```
https://crackstation.net/
```

内存文件搜索，由于搜索的文件会比较多，可用grep进行过滤，很多时候可能需要分析的数据很多可利用 > aa.txt,这样就可以将文件保存下来，封方便去查看。

```
vol.py -f win.raw --profile=Win7SP1x64    filesacn | grep nessus
```

文件转储：

```
vol.py -f win.raw --profile=Win7SP1x64    dumpfiles -Q 0x00000000523afd80 -D
./
```

进程转存，将看到的可疑进程存储下来

```
└─# vol.py -f win.raw --profile=Win7SP1x64   memdump -p 5532  -D ./
Volatility Foundation Volatility Framework 2.6.1
************************************************************************
Writing LoveCloud.exe [  5532] to 5532.dmp
```

看了很多资料Volatility在ctf中取证题目中这个工具用到的比较多，在应急场景中也是可以用到的，方便进行后续的分析以及证据留存，还有很多其他的命令具体可参考网上前辈整理的一些资料：

```
https://m0re.top/posts/c6e31ef3/
```

2.2 硬盘取证

想来想去，其实硬盘取证就是将硬盘打包成一个镜像，网上类似的工具很多，可使用windows自带的dism命令，还可以采用备份软件，如傲梅备份软件进行数据备份，具体操作过程比较简单，但是在备份时需要准备个大空间的硬盘

3、linux系统

3.1 内存取证

linux内存取证利用LiME 工具，下载地址：

```
https://github.com/504ensicsLabs/LiME
```

使用方法：
在编译的时候可能会报错，但是不影响使用

```
cd src
make
```

```
root@easy-echo-2:~/LiME# ls
doc  LICENSE  README.md  src
root@easy-echo-2:~/LiME# cd src/
root@easy-echo-2:~/LiME/src# ls
deflate.c  disk.c  hash.c  lime.h  main.c  Makefile  Makefile.sample  tcp.c
root@easy-echo-2:~/LiME/src# make
make -C /lib/modules/5.4.0-26-generic/build M="/root/LiME/src" modules
make[1]: Entering directory '/usr/src/linux-headers-5.4.0-26-generic'
  CC [M]  /root/LiME/src/tcp.o
/root/LiME/src/tcp.c: In function ? ⊡ etup_tcp? ⊡
/root/LiME/src/tcp.c:75:5: warning: ISO C90 forbids mixed declarations and code [-Wdeclaration-after-statement]
   75 |     int opt = 1;
      |     ^~~
  CC [M]  /root/LiME/src/disk.o
  CC [M]  /root/LiME/src/main.o
  CC [M]  /root/LiME/src/hash.o
  CC [M]  /root/LiME/src/deflate.o
  LD [M]  /root/LiME/src/lime.o
  Building modules, stage 2.
  MODPOST 1 modules
  CC [M]  /root/LiME/src/lime.mod.o
  LD [M]  /root/LiME/src/lime.ko
make[1]: Leaving directory '/usr/src/linux-headers-5.4.0-26-generic'
strip --strip-unneeded lime.ko
mv lime.ko lime-5.4.0-26-generic.ko
root@easy-echo-2:~/LiME/src# ls
deflate.c  disk.c  hash.c  lime-5.4.0-26-generic.ko  lime.mod    lime.mod.o  main.c  Makefile         modules.order  tcp.c
deflate.o  disk.o  hash.o  lime.h                    lime.mod.c  lime.o      main.o  Makefile.sample  Module.symvers  tcp.o
root@easy-echo-2:~/LiME/src#
```

make结束后会生成lime-5.4.0-26-generic.ko内核模块
加载生成的内核模块来获取系统内存，insmod 命令会帮助加载内核模块；模块一旦被加载，会在你的系统上读取主内存（RAM）并且将内存的内容转储到命令行所提供的 path 目录下的文件中。另一个重要的参数是 format；保持 lime 的格式，如下所示。在插入内核模块之后，使用 lsmod 命令验证它是否真的被加载。

```
insmod ./lime-4.18.0-240.el8.x86_64.ko "path=../RHEL8.3_64bit.mem
format=lime"
```

```
root@easy-echo-2:~/LiME/src# insmod ./lime-5.4.0-26-generic.ko "path=../RHEL8.3_64bit.mem format=lime"
root@easy-echo-2:~/LiME/src# ls
deflate.c  disk.c  hash.c  lime-5.4.0-26-generic.ko  lime.mod    lime.mod.o  main.c  Makefile         modules.order  tcp.c
deflate.o  disk.o  hash.o  lime.h                    lime.mod.c  lime.o      main.o  Makefile.sample  Module.symvers  tcp.o
root@easy-echo-2:~/LiME/src# find / -name RHEL8.3_64bit.mem
/root/LiME/RHEL8.3_64bit.mem
```

在LiME目录下生成.mem文件

```
root@easy-echo-2:~/LiME# ls -lth RHEL8.3_64bit.mem
-r--r--r-- 1 root root 1.1G Nov  3 07:36 RHEL8.3_64bit.mem
```

查看文件信息

```
root@easy-echo-2:~/LiME# hexdump RHEL8.3_64bit.mem  | head
0000000 4d45 4c69 0001 0000 1000 0000 0000 0000
0000010 fbff 0009 0000 0000 0000 0000 0000 0000
0000020 0000 0000 0000 0000 0000 0000 0000 0000
*
000f020 d040 ac9c 92ae ffff b280 bdd9 92ae ffff
000f030 0000 0000 0000 0000 0018 8001 92ae ffff
000f040 0018 8001 92ae ffff 4001 1dc8 0001 0000
000f050 0000 0000 0000 0000 0000 0000 0000 0000
000f060 d740 ac9c 92ae ffff 3340 abf0 92ae ffff
000f070 0000 0000 0000 0000 0058 8001 92ae ffff
root@easy-echo-2:~/LiME#
```

这样就将内存文件dump下来了，然后在利用Volatility工具进行分析。

3.2 硬盘取证

linux有自己的dd命令，在取证之前需要准备新的磁盘空间
复制磁盘：
将/dev/sda完整的复制，dd命令时需要包含if=表示源磁盘，和of=表示目标磁盘

```
dd if=/dev/sda1  of=/dev/sdb
```

```
└─# dd if=/dev/sda1  of=/dev/sdb
dd: writing to '/dev/sdb': No space left on device
1932401+0 records in
1932400+0 records out
989388800 bytes (989 MB, 944 MiB) copied, 8.3998 s, 118 MB/s
```

我在本地进行测试时提示空间不够，所以需要准备足够大的硬盘空间
磁盘镜像：

```
dd if=/dev/sda of=/home/sdadisk.img
```

还原镜像：

```
dd if=sdadisk.img of=/dev/sdb
```

还可以采用异地备份的方式：
通过ssh连接进行备份，如将服务器x.x.x.x的sda文件复制到本地

```
ssh username@x.x.x.x "dd if=/dev/sda | gzip -1 -" | dd of=backup.gz
```

这里只是列举了dd的部分用法，更多的用法可参考前辈总结：

```
https://cloud.tencent.com/developer/article/1720348?from=15425
```

取证方法还是有很多的，这次只是列举了几个操作相对比较简单的方法，方便在工作中使用，在进行取证之前建议准备个大空间的硬盘，不管是内存镜像还是硬盘镜像往往都是需要很大的磁盘空间。