OtterCTF——Memory Forensics

网址：OtterCTF

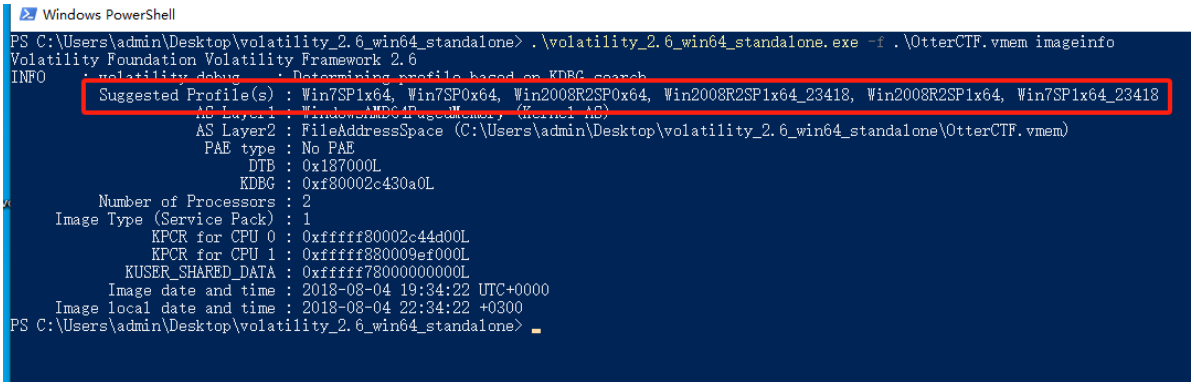
一、What the password?

题目：你得到了rick电脑内存的样本。你能得到他的用户密码吗？格式：CTF{...}

① 当我们获取内存镜像时，需要使用imageinfo命令查看系统信息

```
.\volatility_2.6_win64_standalone.exe -f .\OtterCTF.vmem imageinfo
```

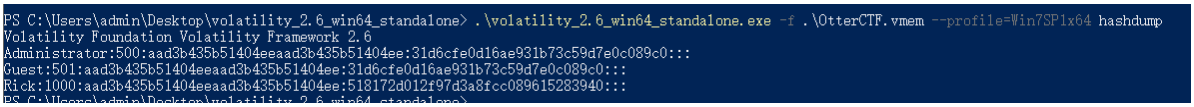
效果如下图所示：



② 使用hashdump命令，获取用户和密码

```
.\volatility_2.6_win64_standalone.exe -f .\OtterCTF.vmem --profile=Win7SP1x64
hashdump
```

效果如下图所示



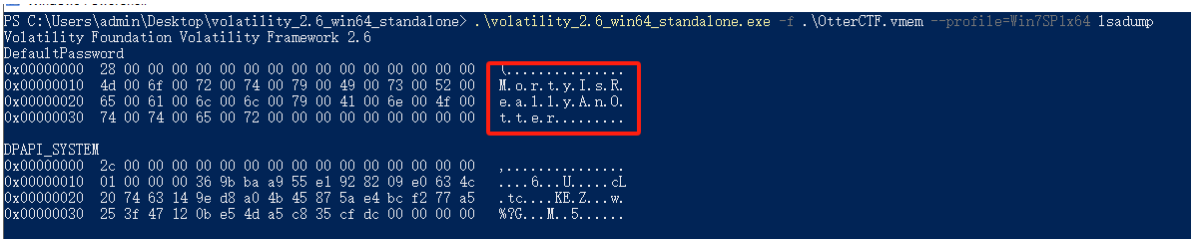
从上图可知，Rick或许是默认的登录账户，猜测存在默认密码。

③ 使用lsadump命令，查看默认账户信息

【lsadump命令的作用是从内存中提取LSA（Local Security Authority）相关的秘密信息，如系统自动登录的缺省密码、远程桌面协议的公钥、Windows数据保护应用程序编程接口使用的授权证书等信息】

```
.\volatility_2.6_win64_standalone.exe -f .\OtterCTF.vmem --profile=Win7SP1x64
lsadump
```

效果如下图所示



此处获取的DefaultPassword很大可能为Rick的密码，尝试将此密码作为flag提交。

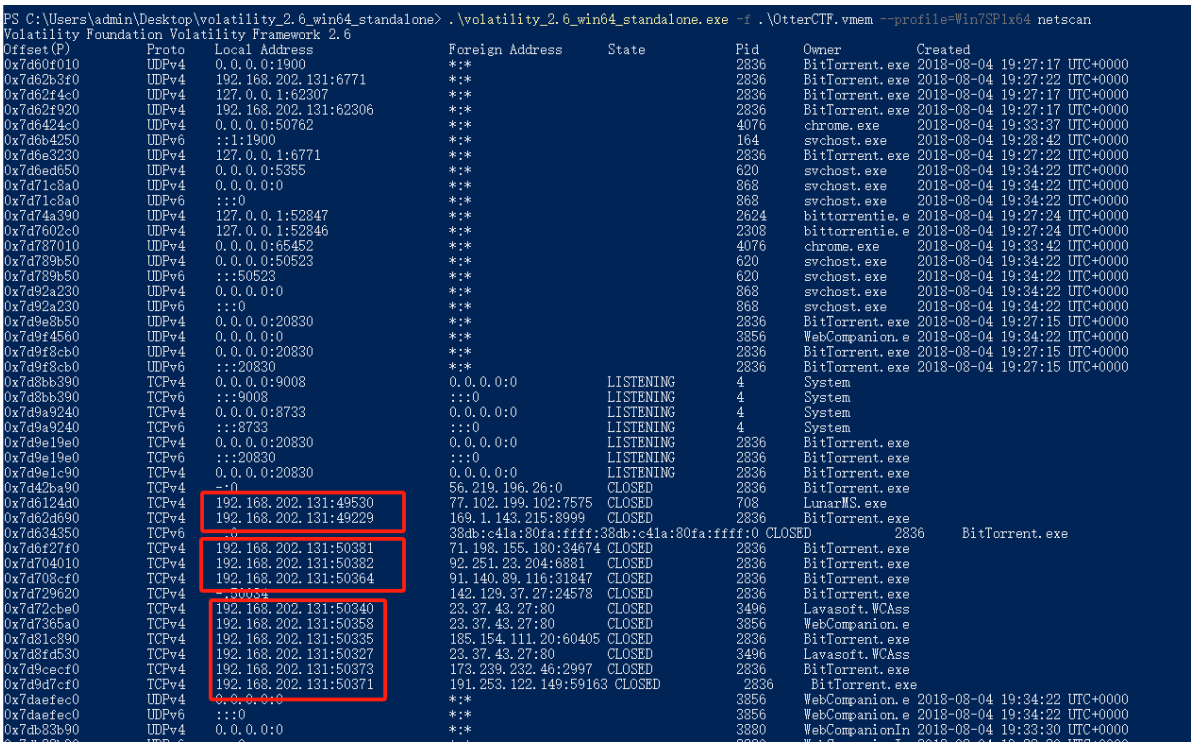
二、General Info

题目：让我们简单地开始吧——电脑的名称和IP地址是什么？格式：CTF{flag}

① 使用netscan命令，查看内存镜像的网络连接信息

```
.\volatility_2.6_win64_standalone.exe -f .\OtterCTF.vmem --profile=Win7SP1x64 netscan
```

效果如下图所示

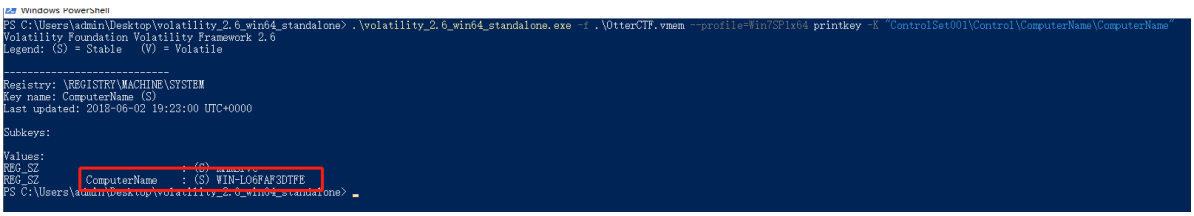


从上图可知本地的ip地址。

② 查看注册表，获取主机名

```
.\volatility_2.6_win64_standalone.exe -f .\OtterCTF.vmem --profile=Win7SP1x64 printkey -K "ControlSet001\Control\ComputerName\ComputerName"
```

效果如下图所示



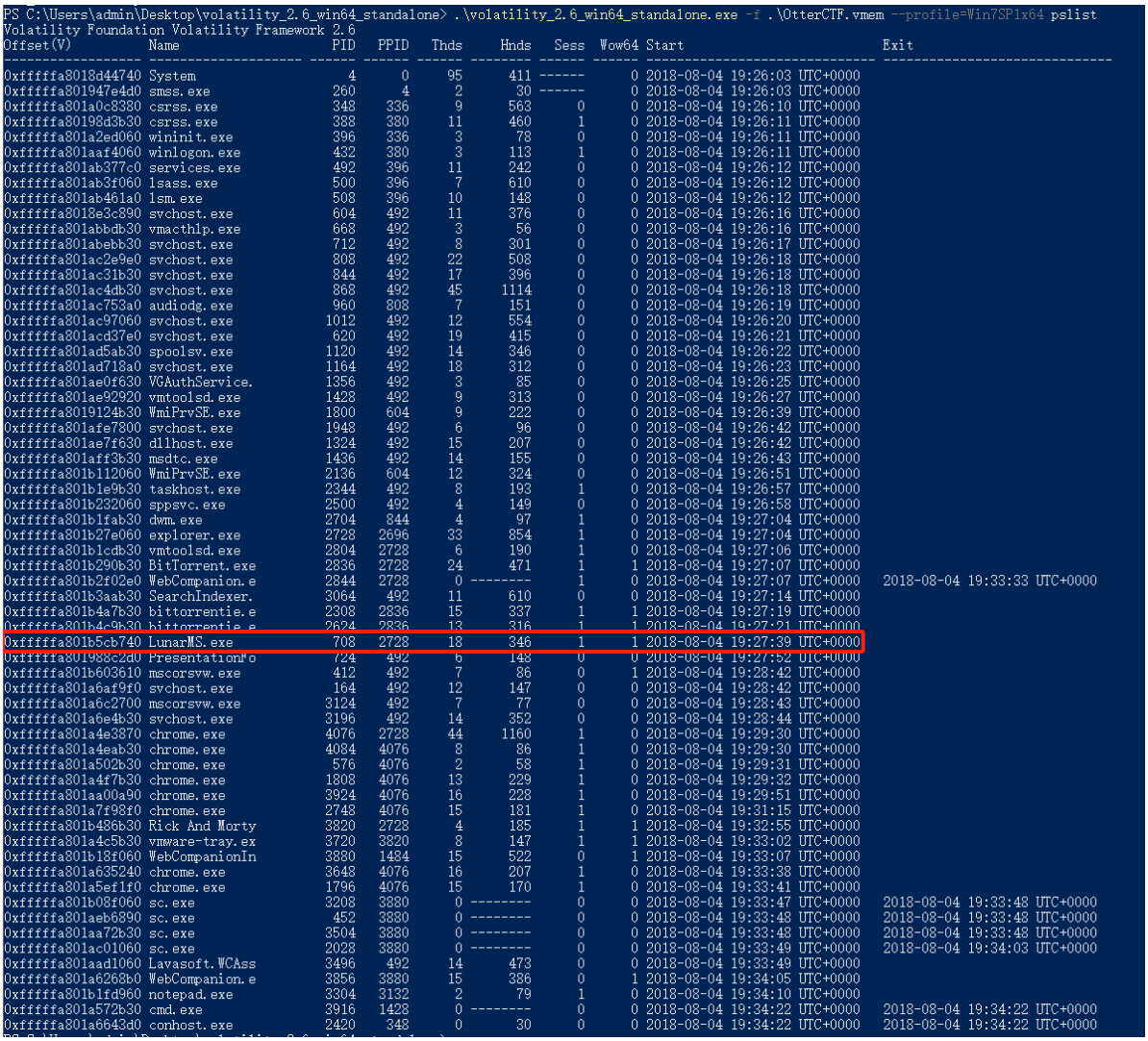
三、Play Time

题目：Rick只是喜欢玩一些好的老式电子游戏。你能说出他在玩什么游戏吗？服务器的IP地址是什么？格式：CTF{flag}

① 使用pslist命令，查看内存镜像的进程信息

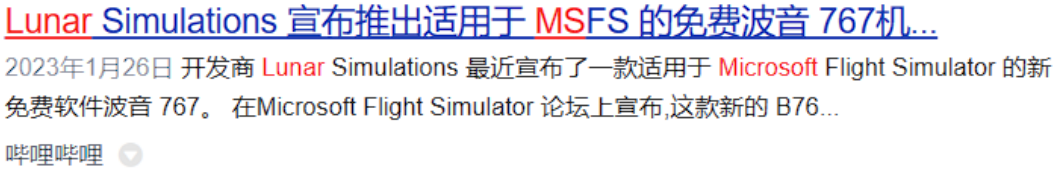
```
.\volatility_2.6_win64_standalone.exe -f .\OtterCTF.vmem --profile=Win7SP1x64 pslist
```

效果如下图所示



```
PS C:\Users\admin\Desktop\volatility_2.6_win64_standalone> .\volatility_2.6_win64_standalone.exe -f .\OtterCTF.vmem --profile=Win7SP1x64 pslist
Volatility Foundation Volatility Framework 2.6
Offset(V)          Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
------------------ -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------------------------
0xfffffa8018d44740 System                    4      0     95      411 ------      0 2018-08-04 19:26:03 UTC+0000
0xfffffa801947e4d0 smss.exe                260      4      2       30 ------      0 2018-08-04 19:26:03 UTC+0000
0xfffffa801a0c8380 csrss.exe               348    336      9      563      0      0 2018-08-04 19:26:10 UTC+0000
0xfffffa80198d3b30 csrss.exe               388    380     11      460      1      0 2018-08-04 19:26:11 UTC+0000
0xfffffa801a2ed060 wininit.exe             396    336      3       78      0      0 2018-08-04 19:26:11 UTC+0000
0xfffffa801aaf4060 winlogon.exe            432    380      3      113      1      0 2018-08-04 19:26:11 UTC+0000
0xfffffa801ab377c0 services.exe            492    396     11      242      0      0 2018-08-04 19:26:12 UTC+0000
0xfffffa801ab3f060 lsass.exe               500    396      7      610      0      0 2018-08-04 19:26:12 UTC+0000
0xfffffa801ab461a0 lsm.exe                 508    396     10      148      0      0 2018-08-04 19:26:12 UTC+0000
0xfffffa8018e3c890 svchost.exe             604    492     11      376      0      0 2018-08-04 19:26:16 UTC+0000
0xfffffa801abbdb30 vmacthlp.exe            668    492      3       56      0      0 2018-08-04 19:26:16 UTC+0000
0xfffffa801abebb30 svchost.exe             712    492      8      301      0      0 2018-08-04 19:26:17 UTC+0000
0xfffffa801ac2e9e0 svchost.exe             808    492     22      508      0      0 2018-08-04 19:26:18 UTC+0000
0xfffffa801ac31b30 svchost.exe             844    492     17      396      0      0 2018-08-04 19:26:18 UTC+0000
0xfffffa801ac4db30 svchost.exe             868    492     45     1114      0      0 2018-08-04 19:26:18 UTC+0000
0xfffffa801ac753a0 audiodg.exe             960    808      7      151      0      0 2018-08-04 19:26:19 UTC+0000
0xfffffa801ac97060 svchost.exe            1012    492     12      554      0      0 2018-08-04 19:26:20 UTC+0000
0xfffffa801acd37e0 svchost.exe             620    492     19      415      0      0 2018-08-04 19:26:21 UTC+0000
0xfffffa801ad5ab30 spoolsv.exe            1120    492     14      346      0      0 2018-08-04 19:26:22 UTC+0000
0xfffffa801ad718a0 svchost.exe            1164    492     18      312      0      0 2018-08-04 19:26:23 UTC+0000
0xfffffa801ae0f630 VGAuthService.         1356    492      3       85      0      0 2018-08-04 19:26:25 UTC+0000
0xfffffa801ae92920 vmtoolsd.exe           1428    492      9      313      0      0 2018-08-04 19:26:27 UTC+0000
0xfffffa8019124b30 WmiPrvSE.exe           1800    604      9      222      0      0 2018-08-04 19:26:39 UTC+0000
0xfffffa801afe7800 svchost.exe            1948    492      6       96      0      0 2018-08-04 19:26:42 UTC+0000
0xfffffa801ae7f630 dllhost.exe            1324    492     15      207      0      0 2018-08-04 19:26:42 UTC+0000
0xfffffa801aff3b30 msdtc.exe              1436    492     14      155      0      0 2018-08-04 19:26:43 UTC+0000
0xfffffa801b112060 WmiPrvSE.exe           2136    604     12      324      0      0 2018-08-04 19:26:51 UTC+0000
0xfffffa801b1e9b30 taskhost.exe           2344    492      8      193      1      0 2018-08-04 19:26:57 UTC+0000
0xfffffa801b232060 sppsvc.exe             2500    492      4      149      0      0 2018-08-04 19:26:58 UTC+0000
0xfffffa801b1fab30 dwm.exe                2704    844      4       97      1      0 2018-08-04 19:27:04 UTC+0000
0xfffffa801b27e060 explorer.exe           2728   2696     33      854      1      0 2018-08-04 19:27:04 UTC+0000
0xfffffa801b1cdb30 vmtoolsd.exe           2804   2728      6      190      1      0 2018-08-04 19:27:06 UTC+0000
0xfffffa801b290b30 BitTorrent.exe         2836   2728     24      471      1      1 2018-08-04 19:27:07 UTC+0000
0xfffffa801b2f02e0 WebCcompanion.e        2844   2728      0 --------      1      0 2018-08-04 19:27:07 UTC+0000   2018-08-04 19:33:33 UTC+0000
0xfffffa801b3aab30 SearchIndexer.         3064    492     11      610      0      0 2018-08-04 19:27:14 UTC+0000
0xfffffa801b4a7b30 bittorrentie.e         2308   2836     15      337      1      1 2018-08-04 19:27:19 UTC+0000
0xfffffa801b4c9b30 bittorrentie.e         2624   2836     13      316      1      1 2018-08-04 19:27:21 UTC+0000
0xfffffa801b5cb740 LunarMS.exe             708   2728     18      346      1      1 2018-08-04 19:27:39 UTC+0000
0xfffffa801988c2d0 PresentationFo          724    492      6      148      0      0 2018-08-04 19:27:52 UTC+0000
0xfffffa801b603610 mscorsvw.exe            412    492      7       86      0      1 2018-08-04 19:28:42 UTC+0000
0xfffffa801a6af9f0 svchost.exe             164    492     12      147      0      0 2018-08-04 19:28:42 UTC+0000
0xfffffa801a6c2700 mscorsvw.exe           3124    492      7       77      0      0 2018-08-04 19:28:43 UTC+0000
0xfffffa801a6e4b30 svchost.exe            3196    492     14      352      0      0 2018-08-04 19:28:44 UTC+0000
0xfffffa801a4e3870 chrome.exe             4076   2728     44     1160      1      0 2018-08-04 19:29:30 UTC+0000
0xfffffa801a4eab30 chrome.exe             4084   4076      8       86      1      0 2018-08-04 19:29:30 UTC+0000
0xfffffa801a502b30 chrome.exe              576   4076      2       58      1      0 2018-08-04 19:29:31 UTC+0000
0xfffffa801a4f7b30 chrome.exe             1808   4076     13      229      1      0 2018-08-04 19:29:32 UTC+0000
0xfffffa801aa00a90 chrome.exe             3924   4076     16      228      1      0 2018-08-04 19:29:51 UTC+0000
0xfffffa801a7f98f0 chrome.exe             2748   4076     15      181      1      0 2018-08-04 19:31:15 UTC+0000
0xfffffa801b486b30 Rick And Morty         3820   2728      4      185      1      1 2018-08-04 19:32:55 UTC+0000
0xfffffa801a4c5b30 vmware-tray.ex         3720   3820      8      147      1      1 2018-08-04 19:33:02 UTC+0000
0xfffffa801b18f060 WebCompanionIn         3880   1484     15      522      0      1 2018-08-04 19:33:07 UTC+0000
0xfffffa801a635240 chrome.exe             3648   4076     16      207      1      0 2018-08-04 19:33:38 UTC+0000
0xfffffa801a5ef1f0 chrome.exe             1796   4076     15      170      1      0 2018-08-04 19:33:41 UTC+0000
0xfffffa801b08f060 sc.exe                 3208   3880      0 --------      0      0 2018-08-04 19:33:47 UTC+0000   2018-08-04 19:33:48 UTC+0000
0xfffffa801aeb6890 sc.exe                  452   3880      0 --------      0      0 2018-08-04 19:33:48 UTC+0000   2018-08-04 19:33:48 UTC+0000
0xfffffa801aa72b30 sc.exe                 3504   3880      0 --------      0      0 2018-08-04 19:33:48 UTC+0000   2018-08-04 19:33:48 UTC+0000
0xfffffa801ac01060 sc.exe                 2028   3880      0 --------      0      0 2018-08-04 19:33:49 UTC+0000   2018-08-04 19:34:03 UTC+0000
0xfffffa801aad1060 Lavasoft.WCAss         3496    492     14      473      0      0 2018-08-04 19:33:49 UTC+0000
0xfffffa801a6268b0 WebCompanion.e         3856   3880     15      386      0      1 2018-08-04 19:34:05 UTC+0000
0xfffffa801b1fd960 notepad.exe            3304   3132      2       79      1      0 2018-08-04 19:34:10 UTC+0000
0xfffffa801a572b30 cmd.exe                3916   1428      0 --------      0      0 2018-08-04 19:34:22 UTC+0000   2018-08-04 19:34:22 UTC+0000
0xfffffa801a6643d0 conhost.exe            2420    348      0       30      0      0 2018-08-04 19:34:22 UTC+0000   2018-08-04 19:34:22 UTC+0000
```

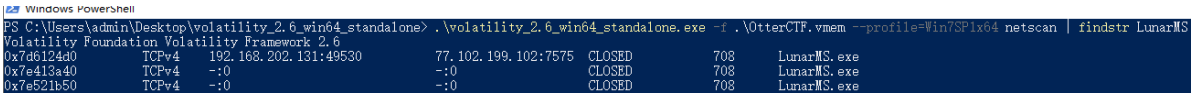
② 将上图的进程名放入百度搜索，发现【LunarMS】是一款游戏名字



③ 使用netscan命令，结合findstr命令，查看lunarMS进程的网络连接信息

```
.\volatility_2.6_win64_standalone.exe -f .\OtterCTF.vmem --profile=Win7SP1x64 netscan | findstr LunarMS
```

效果如下图所示



四、Name Game

题目：我们知道该帐户已登录到一个名为Lunar-3的频道。账户名称是什么？格式：CTF {flag}

① 使用memdump命令，导出LunarMS的进程信息，从【Play Time】题可知，该进程的PID值为708。

【memdump命令可以用于提取内存中的各种信息，如进程、线程、模块、网络连接等，以及与这些信息相关的数据结构。这些数据结构可以包括进程环境块（PEB）、线程环境块（TEB）、系统调用表（KiSystemCallTable）等。】

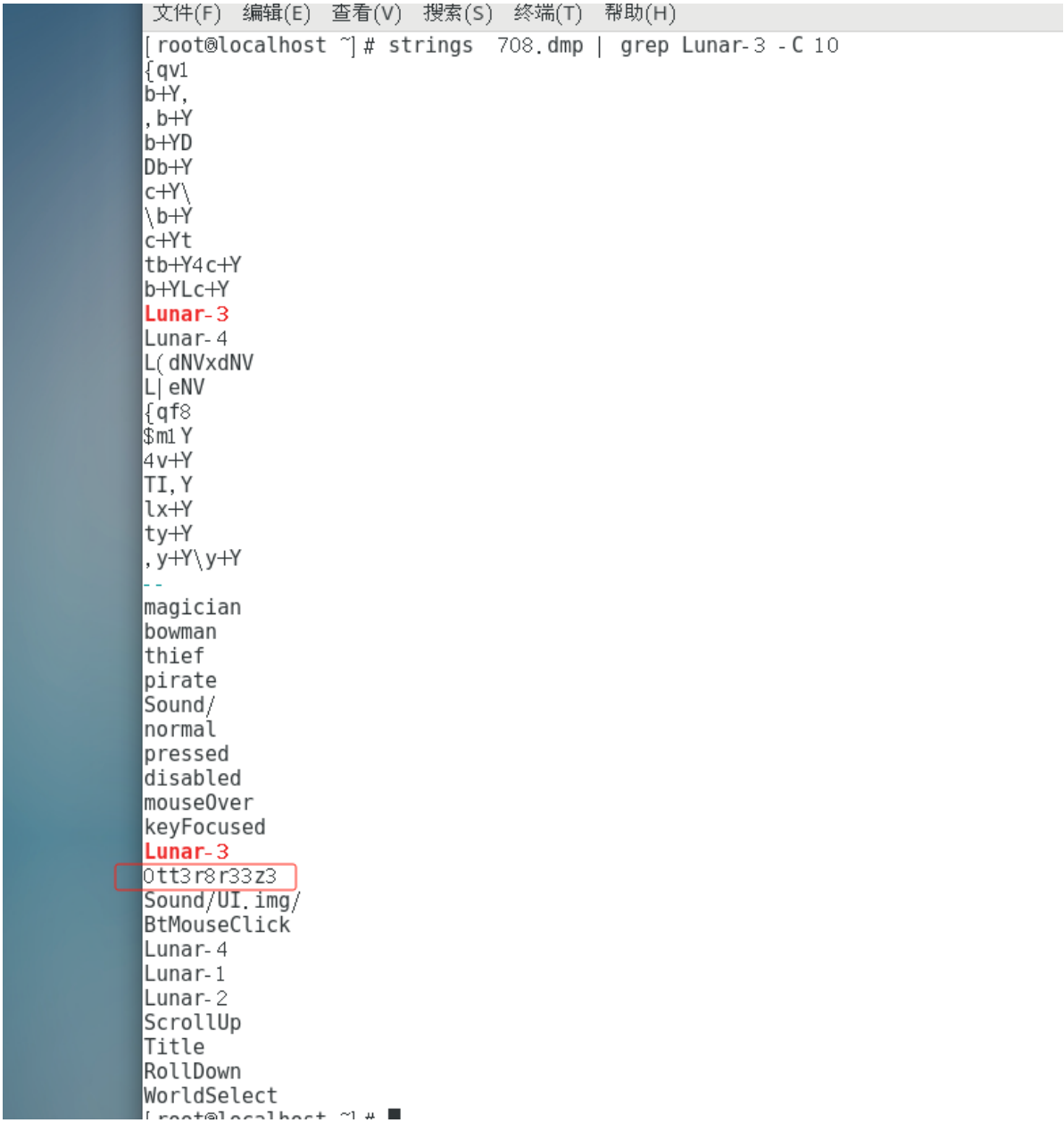
```
.\volatility_2.6_win64_standalone.exe -f .\OtterCTF.vmem --profile=Win7SP1x64 memdump -p 708 -D ./
```

得到708.dmp内存文件。

② 将该文件放进Linux操作系统，使用strings，配合grep指令获取【Lunar-3】前后10行的内容。

```
strings  708.dmp | grep Lunar-3 -C 10
```

效果如下图所示



五、Name Game 2

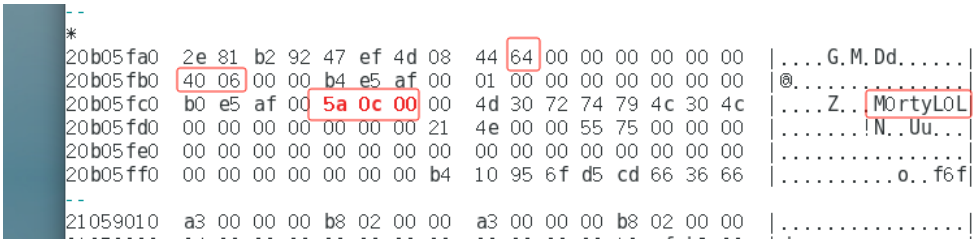
题目：通过一点研究，我们发现登录字符的用户名总是在这个签名之后：0x64 0x？？ {6-8} 0x40 0x06 0x？？{18} 0x5a 0x0c 0x00 {2} rick角色的名字是什么？格式：CTF{...}

① 分析可知，此提示的意思是16进制64后6-8位是16进制40 16进制06，再18位后是十六进制5a 十六进制0c 十六进制00。

② 使用hexdump工具，对708.dmp查找“5a 0c 00”的字符串

```
hexdump -C 708.dmp |grep "5a 0c 00" -A 3 -B 3
```

效果如下图所示



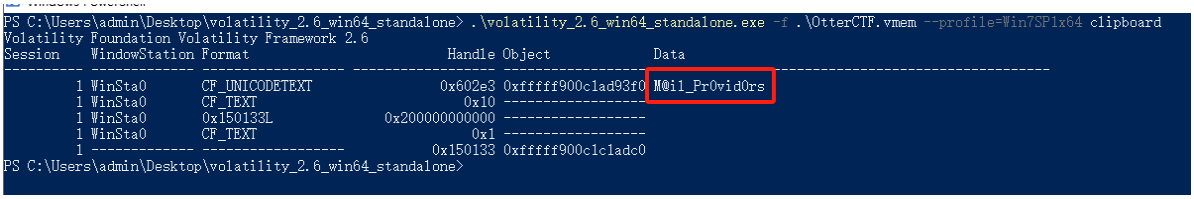
六、Silly Rick

题目：Silly rick总是忘记电子邮件的密码，所以他使用在线存储密码服务来存储密码。他总是复制并粘贴密码，这样他就不会弄错了。rick的电子邮件密码是什么？格式：CTF {flag}

① 使用clipboard命令，查看内存镜像的剪贴板

```
.\volatility_2.6_win64_standalone.exe -f .\OtterCTF.vmem --profile=Win7SP1x64 clipboard
```

效果如下图所示



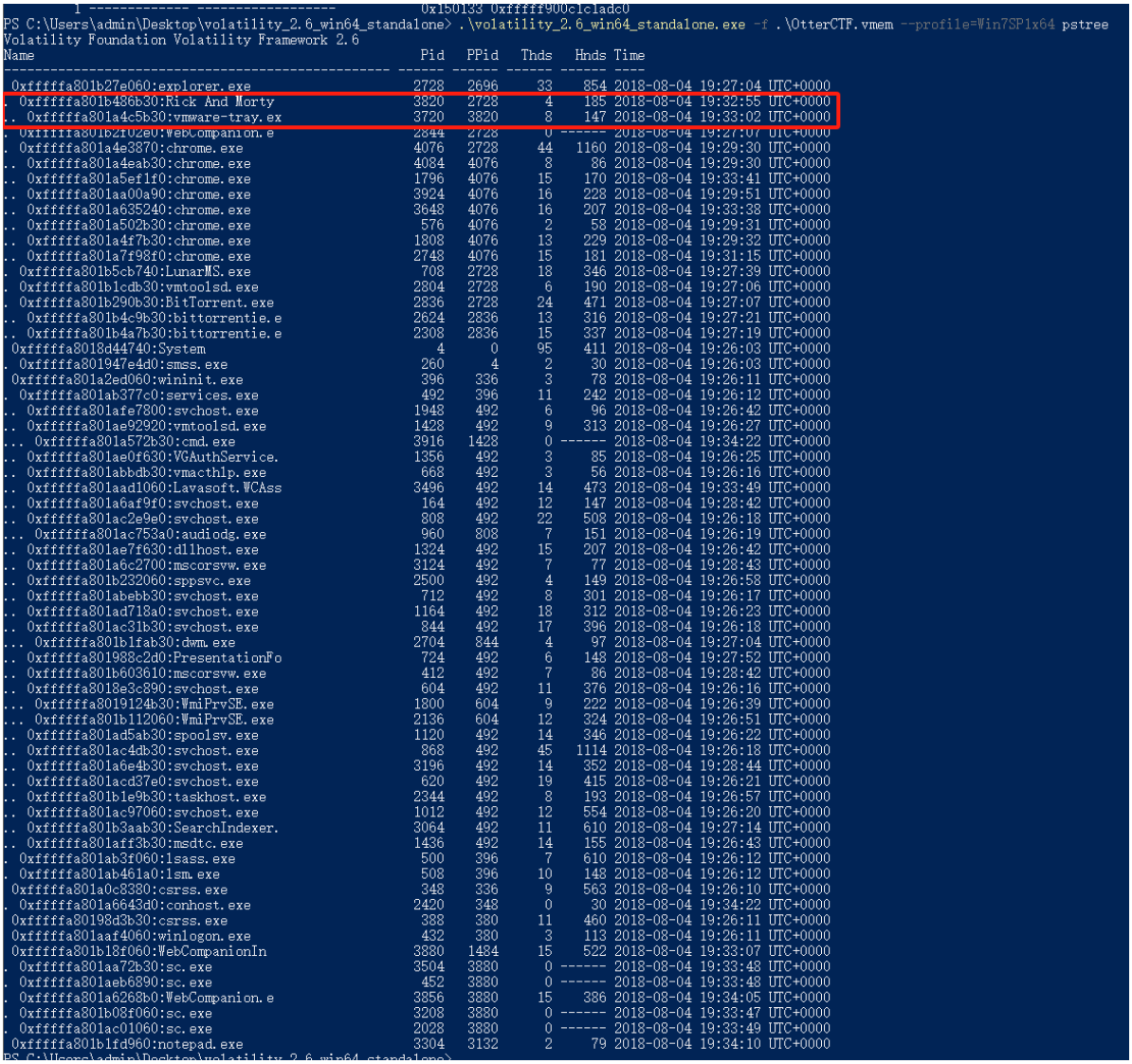
七、Hide And Seek

题目：我们拿走rick电脑内存转储的原因是因为有恶意软件感染。请查找恶意软件进程名称（包括扩展名）注意！只有3次尝试才能获得正确的旗帜！格式：CTF {flag}

① 使用pstree命令查看进程信息（采用pslist也可）

```
.\volatility_2.6_win64_standalone.exe -f .\OtterCTF.vmem --profile=Win7SP1x64 pstree
```

效果如下图所示

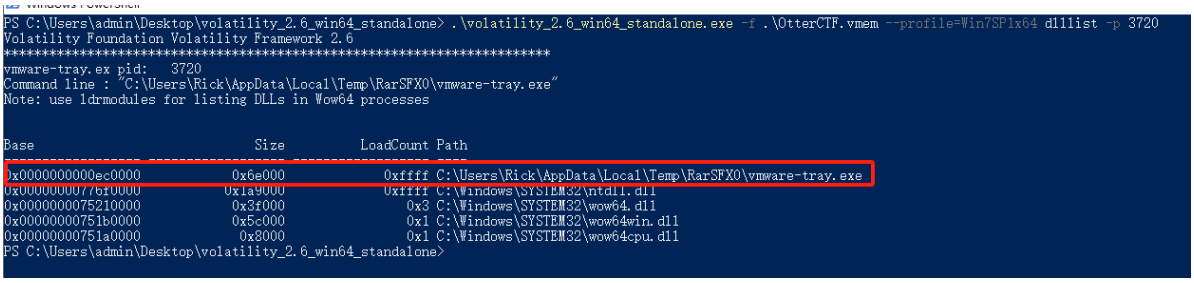


查到【vmware-tray.exe】可疑，因为vmware开头的进程通常是vmware虚拟机软件的程序，而此处显示的PPID的进程名为【Rick And Morty】，显然有问题。

② 查看【vmware-tray.ex】的所使用的dll库

```
.\volatility_2.6_win64_standalone.exe -f .\OtterCTF.vmem --profile=Win7SP1x64 dlllist -p 3720
```

效果如下图所示



此处发现该进程是从【Temp】敏感目录运行，因此可判断该进程为恶意软件。

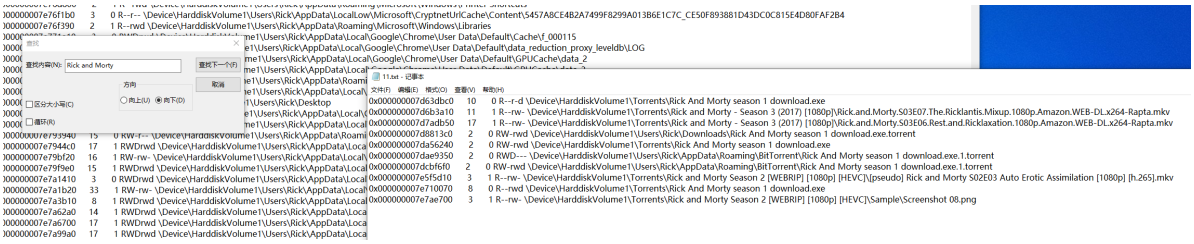
八、Path To Glory

题目：恶意软件是如何进入rick的电脑的？这一定是一种古老的非法习惯。。。 格式：CTF{...}

① 从【Hide And Seek】得知，该恶意软件的父进程程序为【Rick And Morty】，因此搜索跟该进程名有关的文件内容

```
.\volatility_2.6_win64_standalone.exe -f .\OtterCTF.vmem --profile=Win7SP1x64 filescan | findstr "Rick and Morty" > 10.txt
```

② 从10.txt中搜索【Rick and Morty】所在行内容内容，效果如下图所示



一共10条记录，其中包含3个exe文件，3个种子文件，此处怀疑恶意软件是通过种子文件下载而来的。

② 将种子文件进行导出

```
.\volatility_2.6_win64_standalone.exe -f .\OtterCTF.vmem --profile=Win7SP1x64 dumpfiles -Q 0x000000007d8813c0 -D ./

.\volatility_2.6_win64_standalone.exe -f .\OtterCTF.vmem --profile=Win7SP1x64 dumpfiles -Q 0x000000007dae9350 -D ./

.\volatility_2.6_win64_standalone.exe -f .\OtterCTF.vmem --profile=Win7SP1x64 dumpfiles -Q 0x000000007dcbf6f0 -D ./
```

③ 将导出的三个文件，通过Linux的strings命令进行查询

```
strings file*010*
strings file*9e0*
strings file*ccf0*
```

效果如下图所示

真实情况website为下载的URL，此处为模拟情况，因此答案为【M3an_T0rren7_4_R!ck】