Lab1: chụp ảnh RAM

Chuẩn bị:

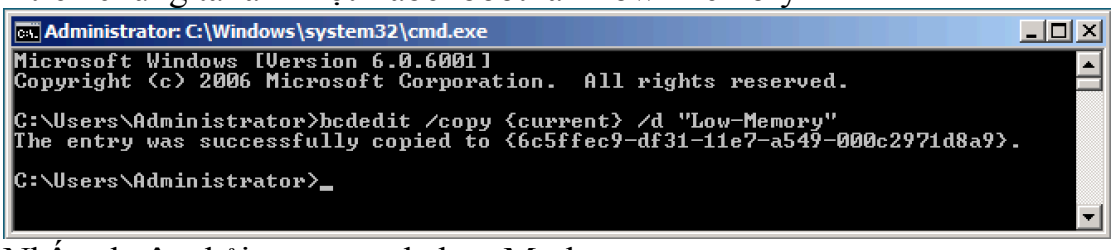
- Một PC Windows Server 2008, và tool Imager_Lite_3.1.1.rar. (nếu không có SV 2008 thì có thể sử dụng windows khác)
- Một máy chạy Kali để phân tích

Mục đích: để lưu lại mọi thông tin trên RAM của máy Windows Server 2008 và sử dụng máy Kali để phân tích.

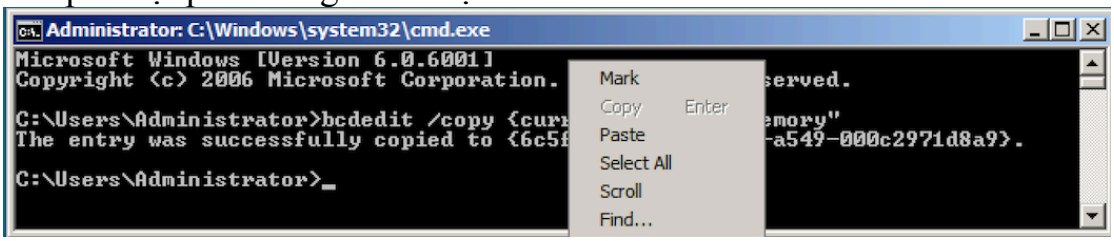
LAB:

1. Giảm sự có sẵn của RAM(**Làm nhanh trong quá trình làm LAB**).
   - Vào **Start ➔ cmd** gõ lệnh:
     bcdedit /copy {current} /d "Low-Memory"

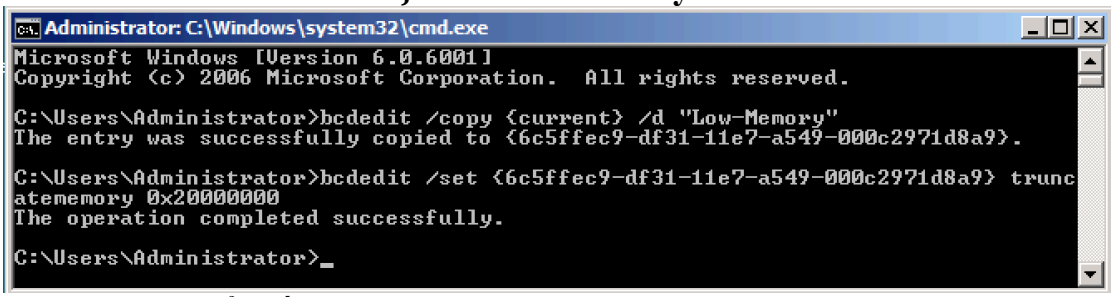
   lệnh trên chúng ta làm một Label boot là "Low-Memory"



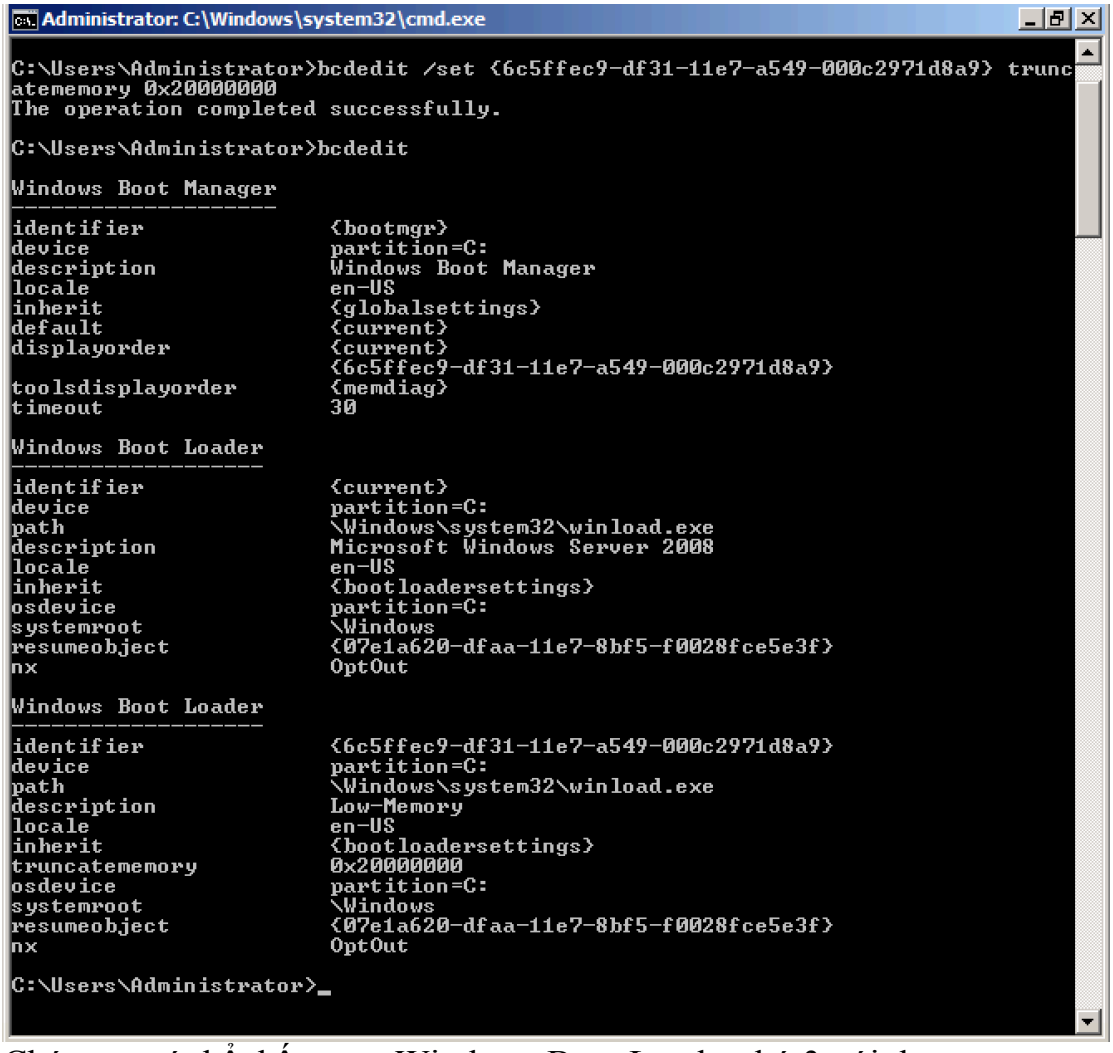
   - Nhấp chuột phải trong cmd chọn Mark



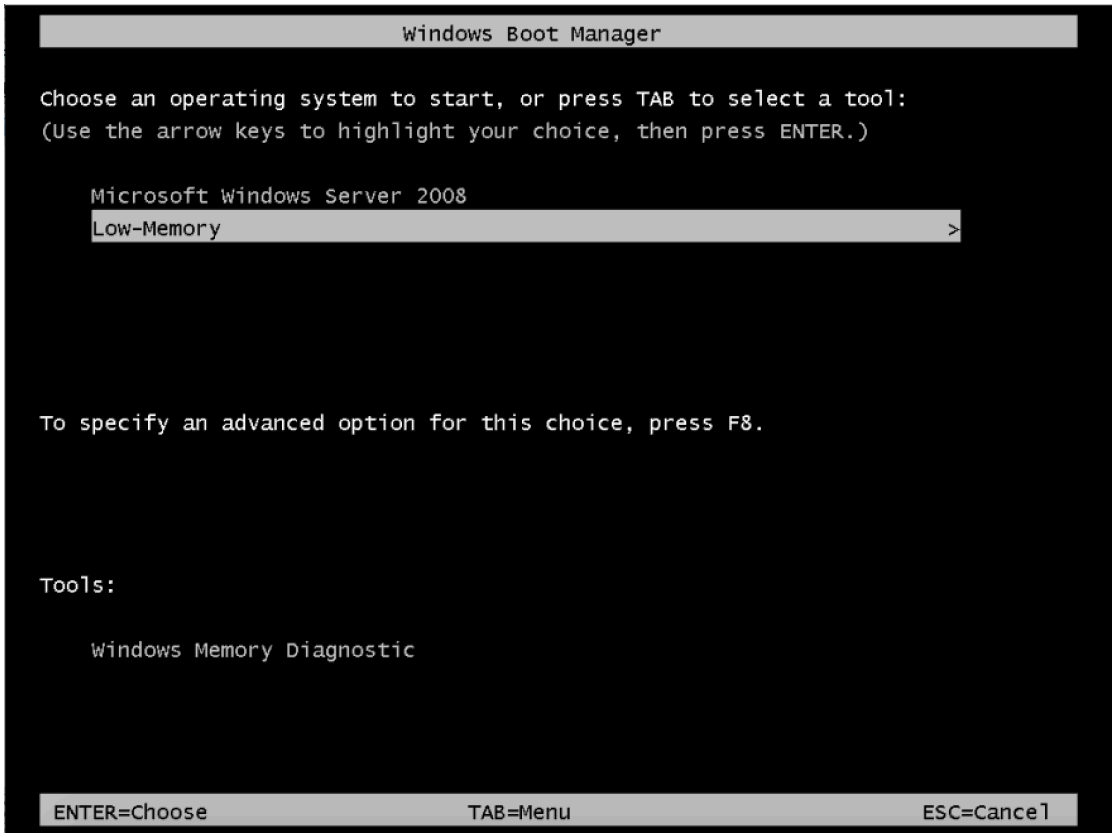
   - Copy: {6c5ffec9-df31-11e7-a549-000c2971d8a9}
   - Trong cmd thực hiện tiếp lệnh:**bcdedit /set {6c5ffec9-df31-11e7-a549-000c2971d8a9} truncatememory 0x20000000**



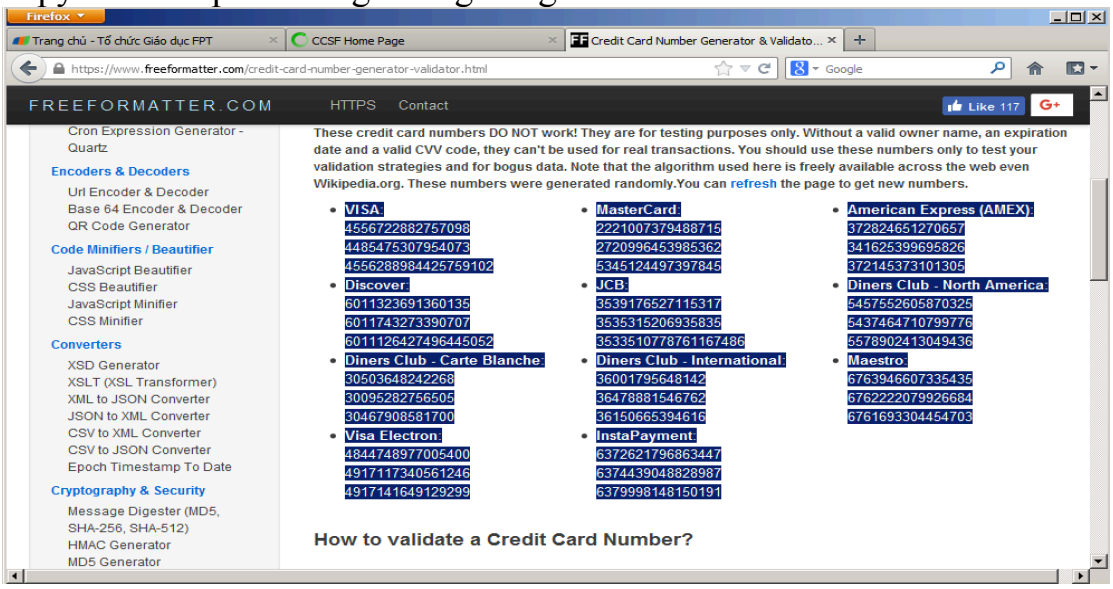
   - Chúng ta có thể thấy dòng "The operation completed successfully."
   - Tiếp theo chạy lệnh bcdedit để kiểm tra.

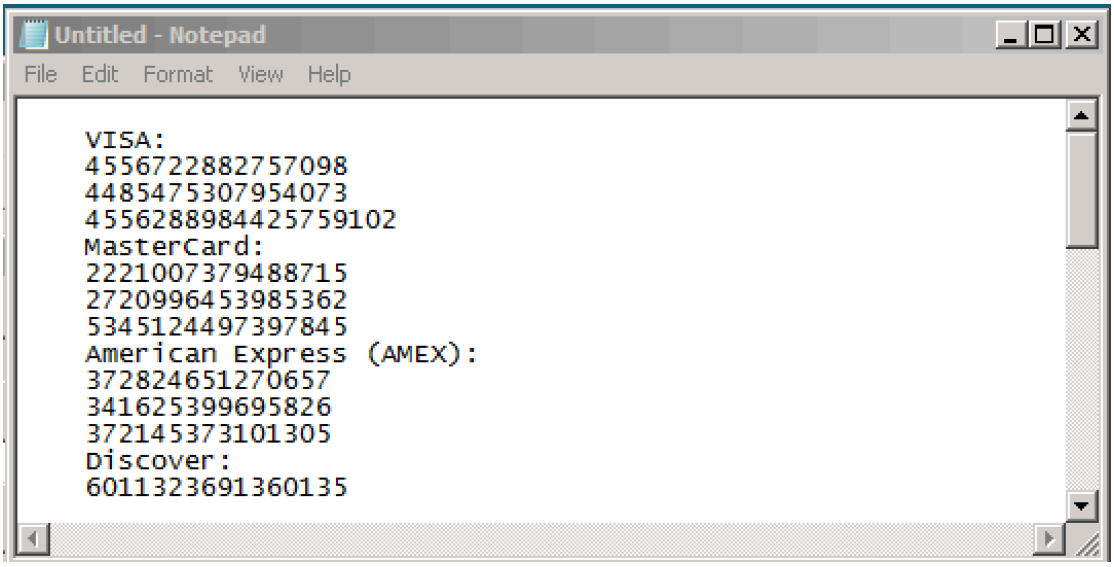


- Chúng ta có thể thấy mục Windows Boot Loader thứ 3 với tham số truncatememory như thiết lập.
- Khởi động lại mấy tính, xuất hiện một menu boot với 2 lựa chọn, chọn “Low-Memory” để boot.

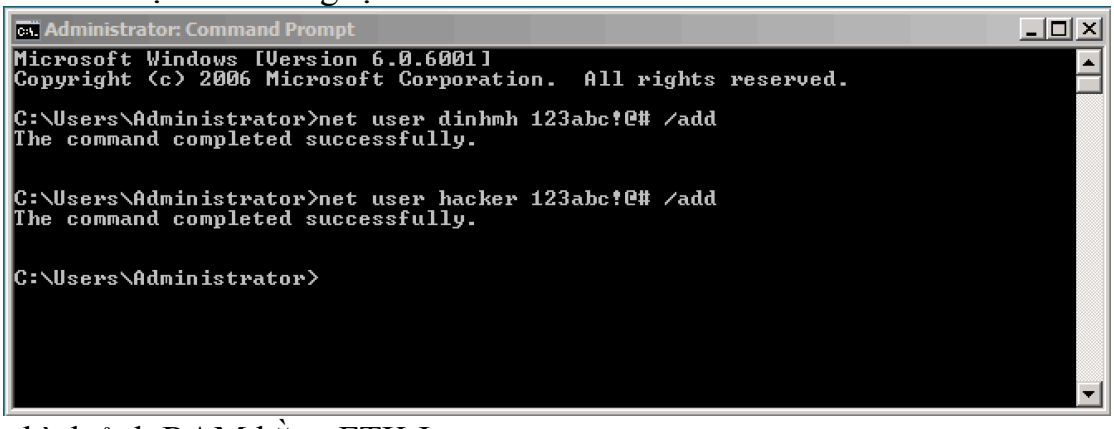


2. Tạo chứng cứ.
   - Truy cập vào các trang:
     - Fpt.edu.vn
     - Ccsf.edu
     - Google.com
   - Trong google.com seach "**fake credit card numbers**" sau đó copy vào notepad nhưng không đóng và save file.

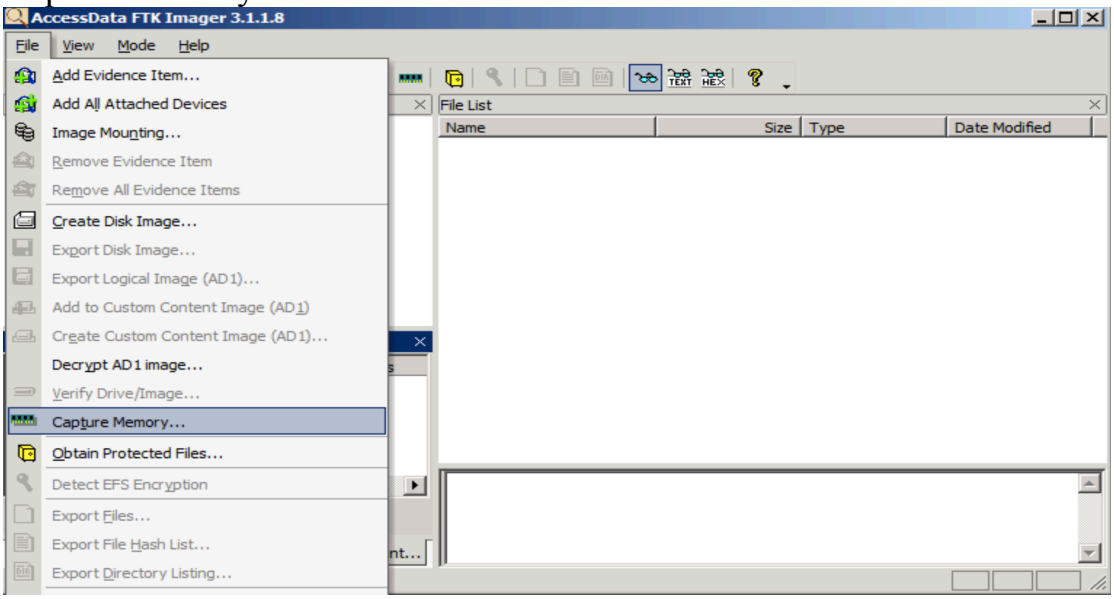




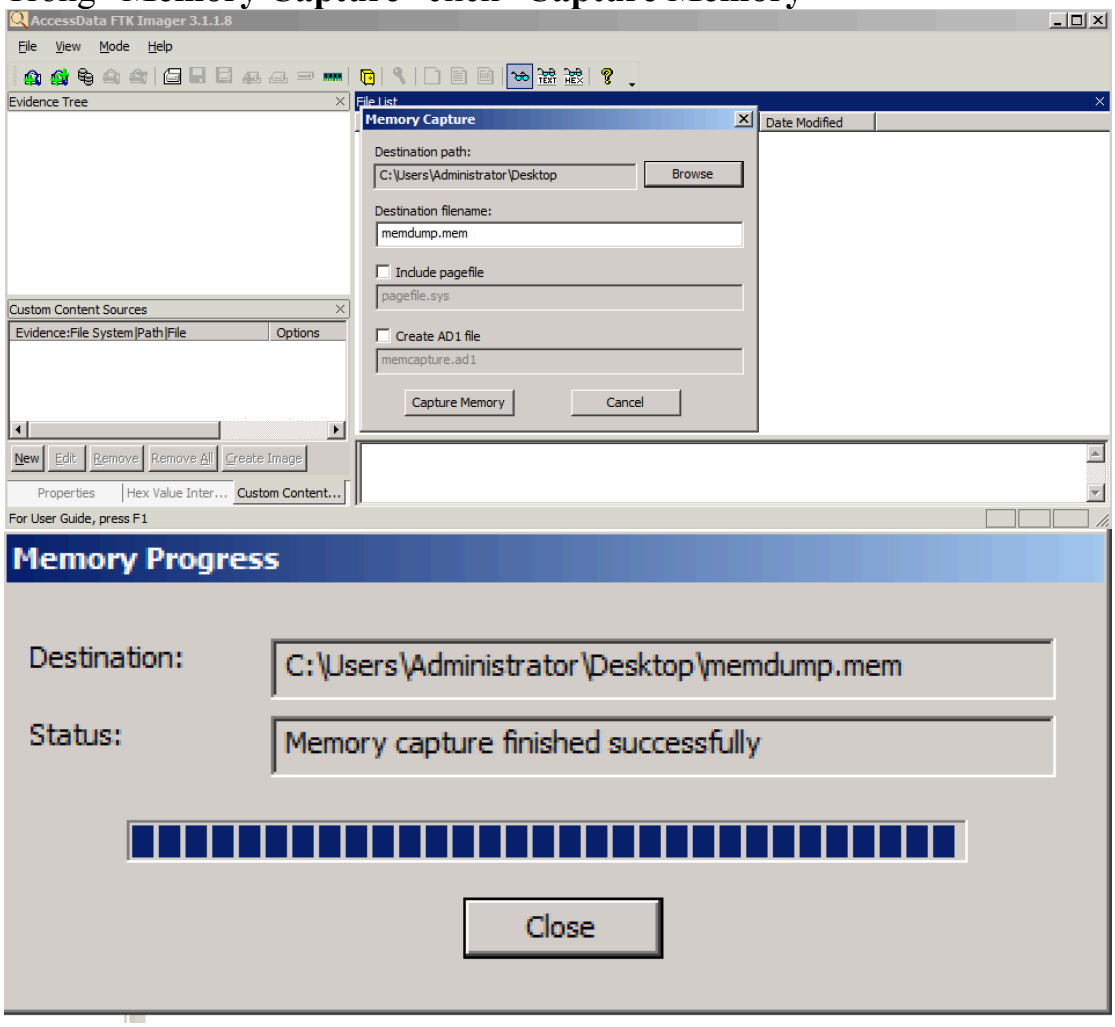
- Mở cmd tạo user bằng lệnh **net user** như hình:



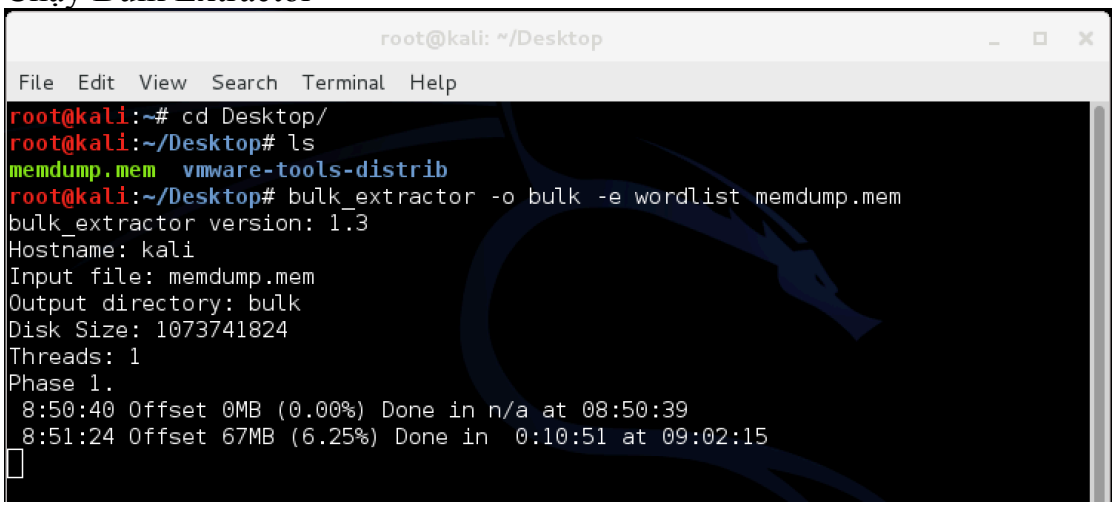
3. Lấy hình ảnh RAM bằng FTK Imager
   - Giải nén **Imager_Lite_3.1.1.rar**
   - Vào **Imager_Lite_3.1.1** và chạy file **FTK Imager.exe**
   - Của sổ AccessData FTK Imager 3.1.1.8 mở ➔chọn File ➔ Capture memory…

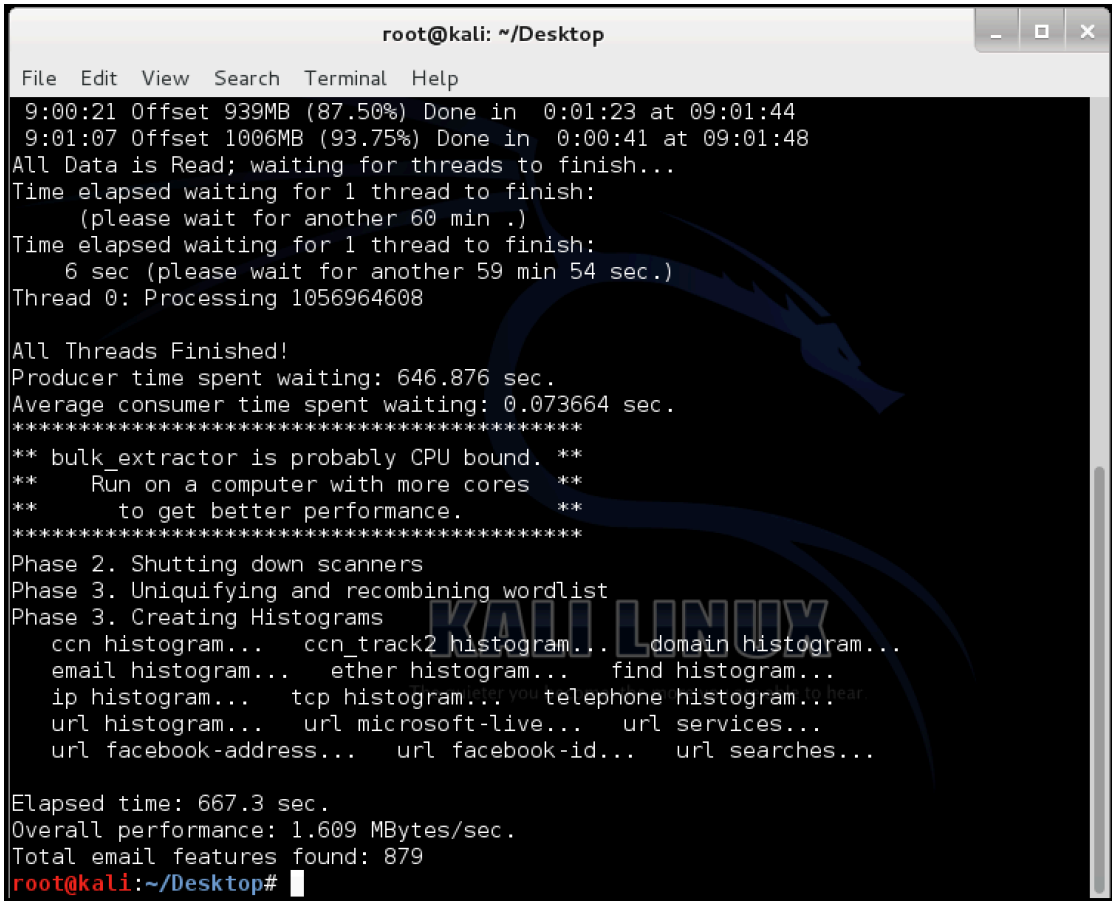


- Trong "**Memory Capture**" click **Browse** ➔ chọn **Desktop** ➔ click OK
- Trong "**Memory Capture**" click "**Capture Memory**"

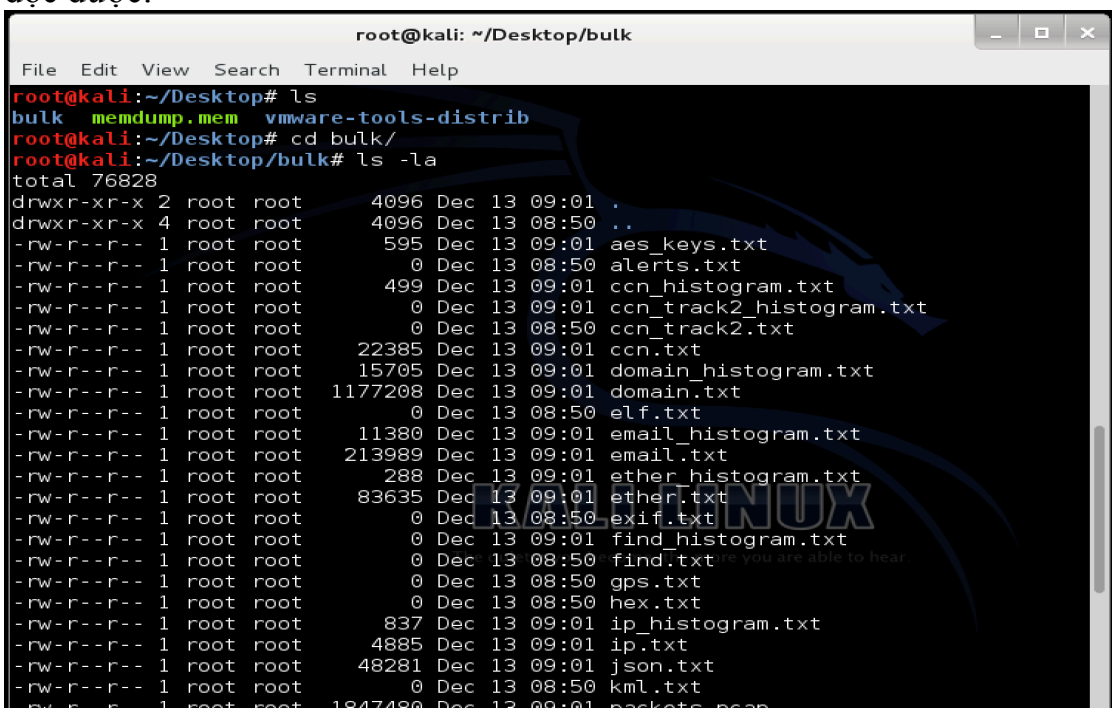


4. Phân tích trên máy Kali.
   Copy file **memdump.mem** từ máy Windows Server 2008 vào máy Kali.
   - Chạy Bulk Extractor



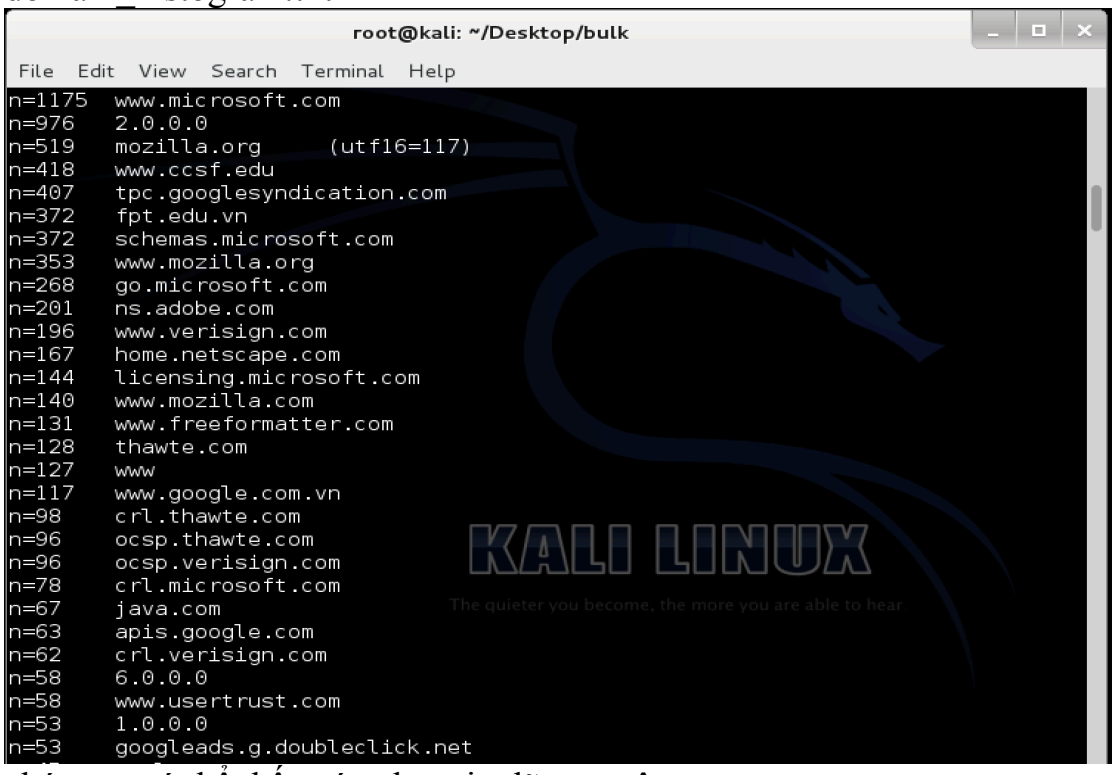


- Bulk Extractor sẽ thu dữ liệu từ tập tin memdump.mem và đưa két quả vào thư mục Bulk và biên dịch tất cả các chuỗi có thể đọc được.



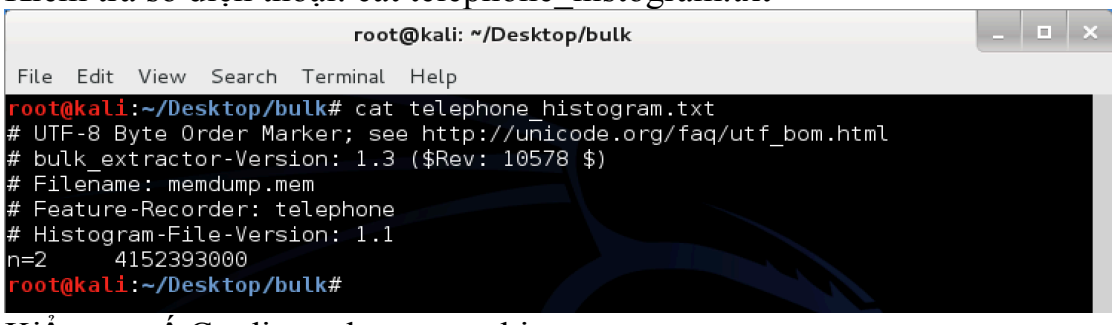
5. Kiểm tra

- kiểm tra Domain Names: trong terminal, thực thi lệnh cat domain_histogram.txt

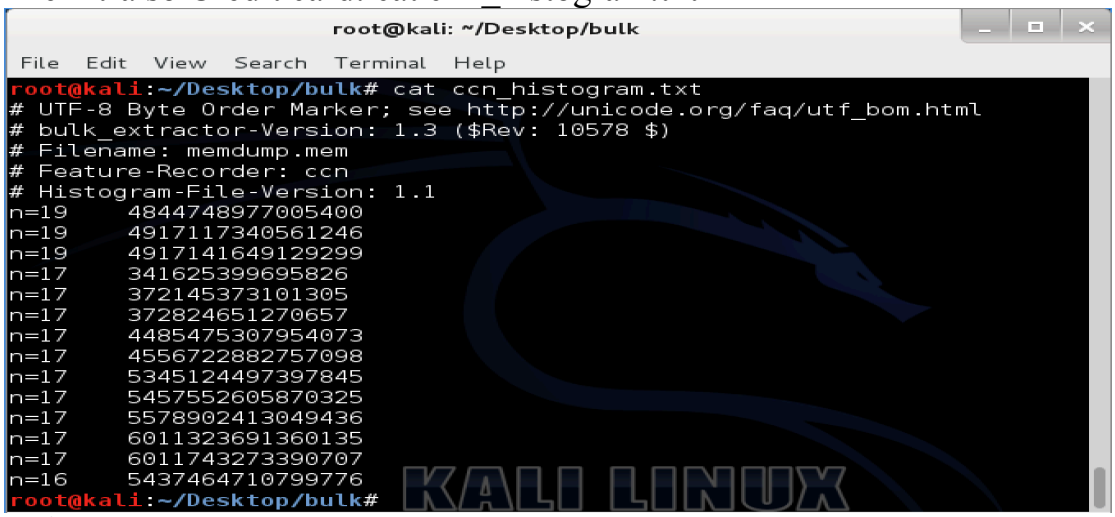


chúng ta có thể thấy các domain đã truy cập.

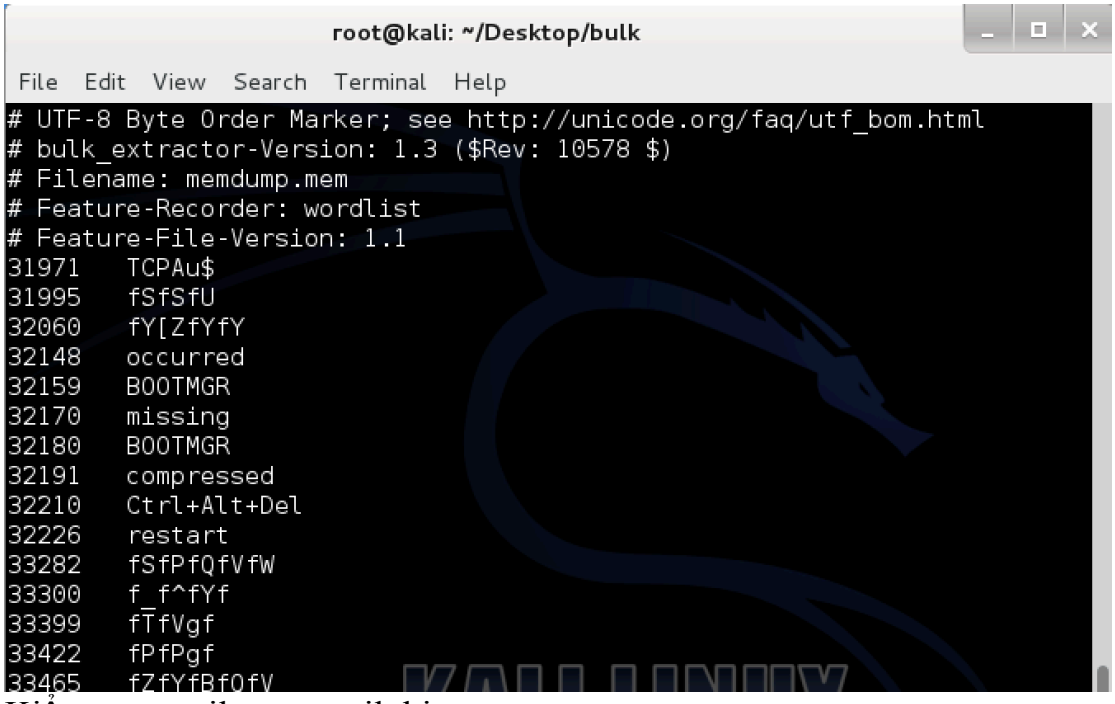
- Kiểm tra số điện thoại: cat telephone_histogram.txt



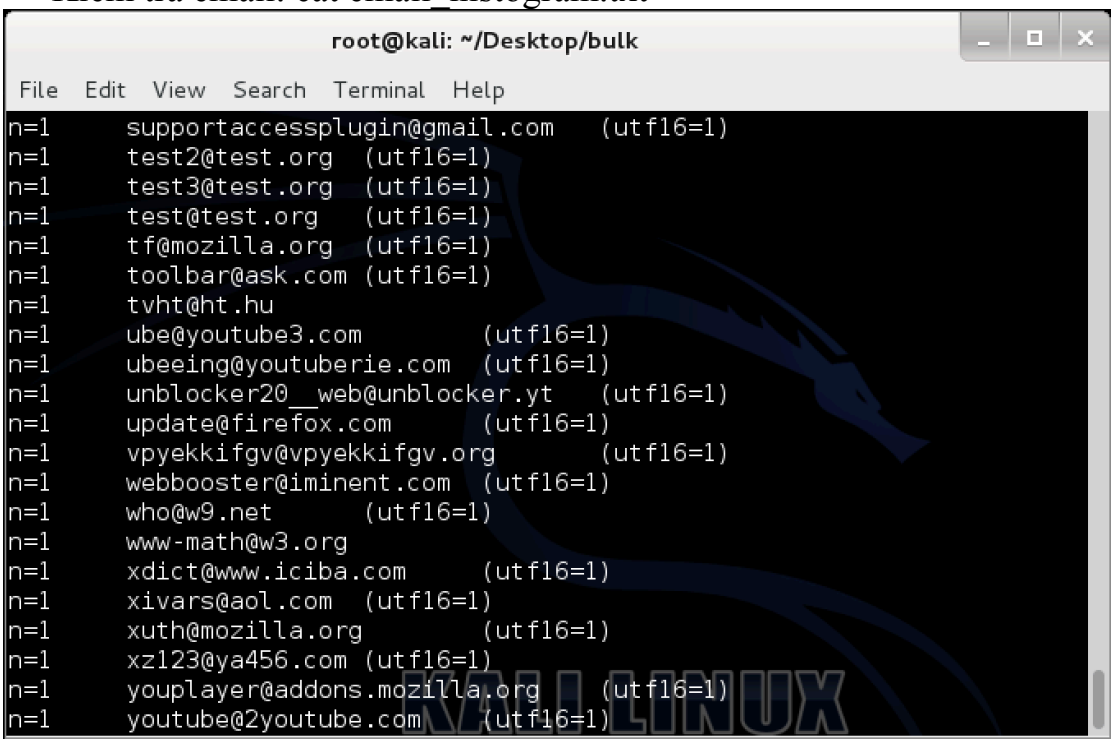
- Kiểm tra số Credit card: cat cnn_histogram.txt



- Kiểm tra Wordlist: cat wordlist.txt



- Kiểm tra email: cat email_histogram.txt



6. Phân tích Image RAM với Volatility.

Trên máy Kali mở terminal và sử dụng lệnh sau:

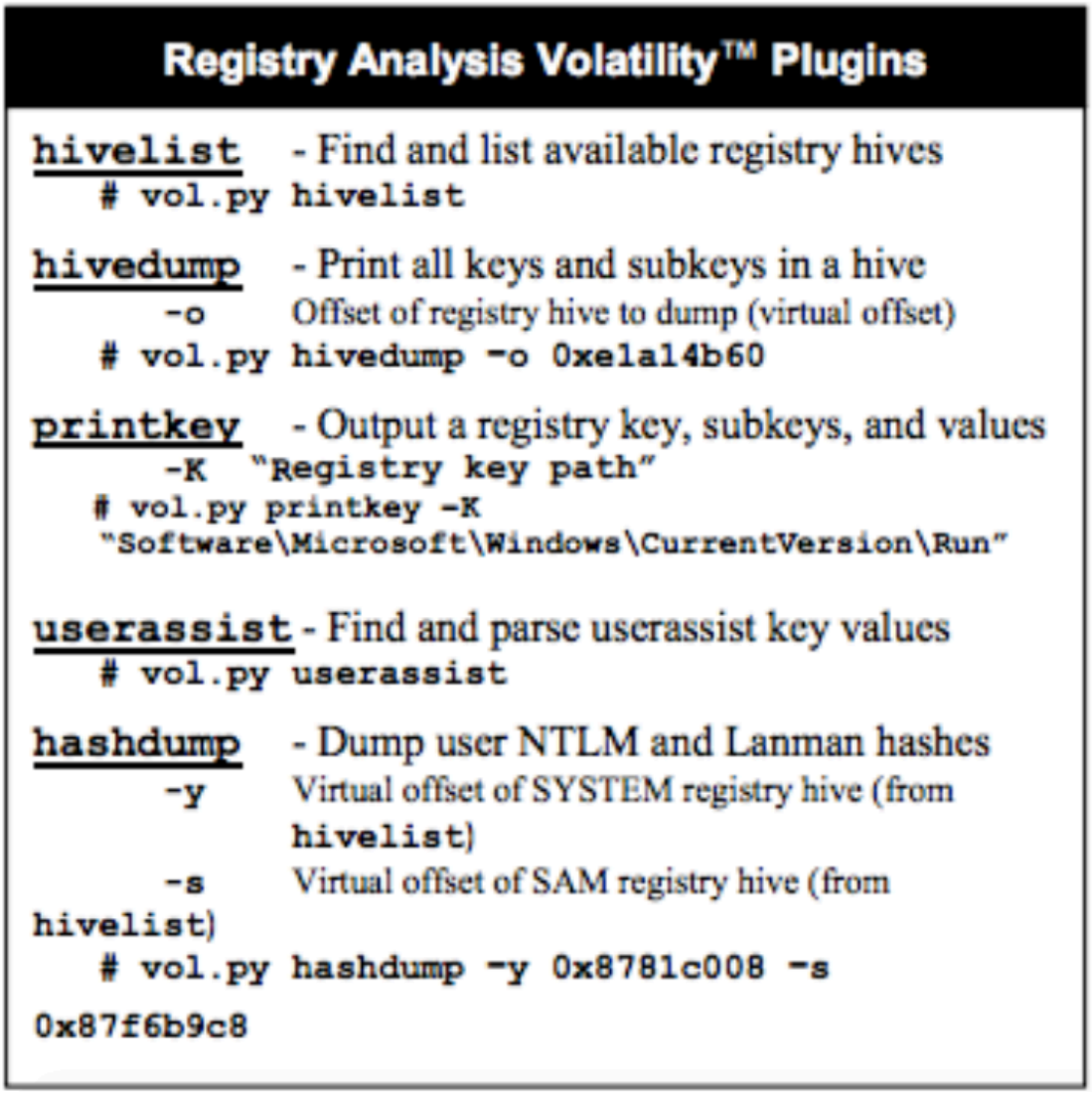
cd /usr/share/volatility

python vol.py –h

```
root@kali:/usr/share/volatility# python vol.py -h
Volatility Foundation Volatility Framework 2.3.1
*** Failed to import volatility.plugins.addrspaces.legacyintel (AttributeError: 'module' object h
as no attribute 'AbstractWritablePagedMemory')
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 timezone for displaying timestamps
  -f FILENAME, --filename=FILENAME
                        Filename to use when opening an image
  --profile=WinXPSP2x86
```

Mô tả của Volatility của SAN



- **Thông tin Image:**

python vol.py imageinfo -f /root/Desktop/memdump.mem

```
root@kali:/usr/share/volatility# python vol.py  imageinfo -f /root/Deskto
p/memdump.mem
Volatility Foundation Volatility Framework 2.3.1
Determining profile based on KDBG search...

          Suggested Profile(s) : VistaSP1x86, Win2008SP1x86, Win2008SP2x8
6, VistaSP2x86
                     AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : FileAddressSpace (/root/Desktop/memdump.
mem)
                      PAE type : PAE
                           DTB : 0x122000L
                          KDBG : 0x8190dc90L
          Number of Processors : 1
     Image Type (Service Pack) : 1
                KPCR for CPU 0 : 0x8190e800L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2017-12-13 14:41:05 UTC+0000
     Image local date and time : 2017-12-13 06:41:05 -0800
root@kali:/usr/share/volatility#
```

Volatility cần biết được hệ điều hành được Image để mô tả bộ nhớ một cách chính xác, ở đây chúng ta đang sử dụng là Win2008sp1x86

- **Các tiến trình đang chạy**:

python vol.py pslist --profile=Win2008SP1x86 -f /root/Desktop/memdump.mem

```
root@kali:/usr/share/volatility# python vol.py  pslist --profile=Win2008SP1x86 -f /root/Desktop/memdump.mem
Volatility Foundation Volatility Framework 2.3.1
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
---------- -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------
0x8a5b55d8 System                    4      0    106      491 ------      0 2017-12-13 14:22:50 UTC+0000
0x8adf55e0 smss.exe                412      4      4       28 ------      0 2017-12-13 14:22:50 UTC+0000
0x8ae5f270 csrss.exe               488    476     11      477      0      0 2017-12-13 14:22:51 UTC+0000
0x8ae8dd90 csrss.exe               536    528      9      267      1      0 2017-12-13 14:22:51 UTC+0000
0x8ae8d348 wininit.exe             544    476      3       98      0      0 2017-12-13 14:22:51 UTC+0000
0x8aea4158 winlogon.exe            576    528      3      114      1      0 2017-12-13 14:22:51 UTC+0000
0x8aeccd90 services.exe            624    544      6      238      0      0 2017-12-13 14:22:52 UTC+0000
0x8aed6198 lsass.exe               636    544     17      612      0      0 2017-12-13 14:22:52 UTC+0000
0x8aed4980 lsm.exe                 644    544     10      163      0      0 2017-12-13 14:22:52 UTC+0000
0x8af641f0 svchost.exe             804    624      7      297      0      0 2017-12-13 14:22:52 UTC+0000
0x8af796b0 vmacthlp.exe            852    624      1       49      0      0 2017-12-13 14:22:52 UTC+0000
0x8af95d90 svchost.exe             884    624      7      277      0      0 2017-12-13 14:22:52 UTC+0000
0x8afba998 svchost.exe             928    624     15      281      0      0 2017-12-13 14:22:52 UTC+0000
0x8afdab98 svchost.exe            1000    624      6      126      0      0 2017-12-13 14:22:52 UTC+0000
0x8afe6578 svchost.exe            1016    624     37      917      0      0 2017-12-13 14:22:52 UTC+0000
0x8afff778 SLsvc.exe              1064    624      4       69      0      0 2017-12-13 14:22:52 UTC+0000
0x8b01dd50 svchost.exe            1108    624     12      480      0      0 2017-12-13 14:22:52 UTC+0000
0x8b02f7d8 svchost.exe            1172    624     20      246      0      0 2017-12-13 14:22:52 UTC+0000
0x8b037478 svchost.exe            1200    624     16      384      0      0 2017-12-13 14:22:52 UTC+0000
0x8b09ed90 svchost.exe            1328    624     29      282      0      0 2017-12-13 14:22:53 UTC+0000
0x8b021870 taskeng.exe            1432   1016      5      132      0      0 2017-12-13 14:23:04 UTC+0000
0x8b082730 spoolsv.exe            1516    624     17      309      0      0 2017-12-13 14:23:08 UTC+0000
0x8b124880 svchost.exe            1580    624      5      125      0      0 2017-12-13 14:23:08 UTC+0000
0x8b135d90 svchost.exe            1600    624      3       73      0      0 2017-12-13 14:23:08 UTC+0000
0x8b1471c0 VGAuthService.e        1640    624      2       81      0      0 2017-12-13 14:23:08 UTC+0000
0x8b187d90 vmtoolsd.exe           1808    624      8      284      0      0 2017-12-13 14:23:08 UTC+0000
```

Offset(v): vị trí trong RAM của tiến trình ở dạng thập lục phân

Name: tên của tiến trình được thể hiện trong Task Manager

PID: ID của tiến trình

PPID: đây là tiến trình cha, Trong hình trên **System** là 4, nó là tiến trình cha của **smss.exe**.

- Các lệnh command:

python vol.py consoles --profile=Win2008SP1x86 -f /root/Desktop/memdump.mem

```
CommandCount: 2 LastAdded: 1 LastDisplayed: 1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x12c
Cmd #0 at 0x6704d80: net user dinhmh 123abc!@# /add
Cmd #1 at 0x6704dc8: net user hacker 123abc!@# /add
----
Screen 0x66f8e48 X:80 Y:300
Dump:
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation.  All rights reserved.

C:\Users\Administrator>net user dinhmh 123abc!@# /add
The command completed successfully.


C:\Users\Administrator>net user hacker 123abc!@# /add
The command completed successfully.


C:\Users\Administrator>
root@kali:/usr/share/volatility#
```

- **Services:**

python vol.py svcscan --profile=Win2008SP1x86 -f /root/Desktop/memdump.mem | more

```
root@kali:/usr/share/volatility# python vol.py  svcscan --profile=Win2008SP1x8
6 -f /root/Desktop/memdump.mem | more
Volatility Foundation Volatility Framework 2.3.1
Offset: 0x90909000
Order: 0
Process ID: -
Service Name: -
Display Name: -
Service Type: SERVICE_INTERACTIVE_PROCESS, SERVICE_WIN32_SHARE_PROCESS
Service State: Unknown choice 3407995
Binary Path: -

Offset: 0x17ef018
Order: 79
Process ID: 1000
Service Name: gpsvc
Display Name: Group Policy Client
Service Type: SERVICE_WIN32_OWN_PROCESS
Service State: SERVICE_RUNNING
Binary Path: C:\Windows\system32\svchost.exe -k GPSvcGroup
```

- Registry Hives:

python vol.py hivelist --profile=Win2008SP1x86 -f /root/Desktop/memdump.mem

```
root@kali:/usr/share/volatility# python vol.py  hivelist --profile=Win2008SP1x
86 -f /root/Desktop/memdump.mem
Volatility Foundation Volatility Framework 2.3.1
Virtual    Physical   Name
---------- ---------- ----
0x90f63008 0x2116e008 \Device\HarddiskVolume1\Windows\System32\config\DEFAULT
0x90f636a8 0x2116e6a8 \Device\HarddiskVolume1\Windows\System32\config\SAM
0x90f76008 0x21c11008 \Device\HarddiskVolume1\Windows\System32\config\SECURITY
0x90f76648 0x21c11648 \Device\HarddiskVolume1\Windows\System32\config\COMPONEN
TS
0x90fd86a8 0x22ebf6a8 \Device\HarddiskVolume1\Boot\BCD
0x99a0ea20 0x25574a20 \Device\HarddiskVolume1\Windows\ServiceProfiles\NetworkS
ervice\NTUSER.DAT
0x99a3d460 0x2555c460 \Device\HarddiskVolume1\Windows\ServiceProfiles\LocalSer
vice\NTUSER.DAT
0x9aea1350 0x10da9350 \Device\HarddiskVolume1\Users\Administrator\NTUSER.DAT
0x9aeada20 0x10c53a20 \Device\HarddiskVolume1\Users\Administrator\AppData\Loca
l\Microsoft\Windows\UsrClass.dat
0x8d611008 0x00ad9008 [no name]
0x8d626008 0x00ae2008 \REGISTRY\MACHINE\SYSTEM
0x8d647008 0x00a45008 \REGISTRY\MACHINE\HARDWARE
0x90f5ba20 0x2119da20 \Device\HarddiskVolume1\Windows\System32\config\SOFTWARE
root@kali:/usr/share/volatility#
```

Chúng ta chú ý 2 địa chỉ được bôi đỏ ở trên, nơi chứa đầy đủ thông tin mật khẩu của

Windows.

- **Password Hashes của Windows**:

python vol.py hashdump --profile=Win2008SP1x86 -f /root/Desktop/memdump.mem -y 0x8d626008 -s 0x90f636a8

```
root@kali:/usr/share/volatility# python vol.py  hashdump --profile=Win2008SP1x86
-f /root/Desktop/memdump.mem -y 0x8d626008 -s 0x90f636a8
Volatility Foundation Volatility Framework 2.3.1
Administrator:500:aad3b435b51404eeaad3b435b51404ee:85d124d30549f4fa5b6d9dc212ff11
e6:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
dinhmh:1000:aad3b435b51404eeaad3b435b51404ee:85d124d30549f4fa5b6d9dc212ff11e6:::
hacker:1001:aad3b435b51404eeaad3b435b51404ee:85d124d30549f4fa5b6d9dc212ff11e6:::
root@kali:/usr/share/volatility#
```

7. Crack Password Hash:
   Vào trang https://crackstation.net và chép đoạn hash vào như hình.