

# 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

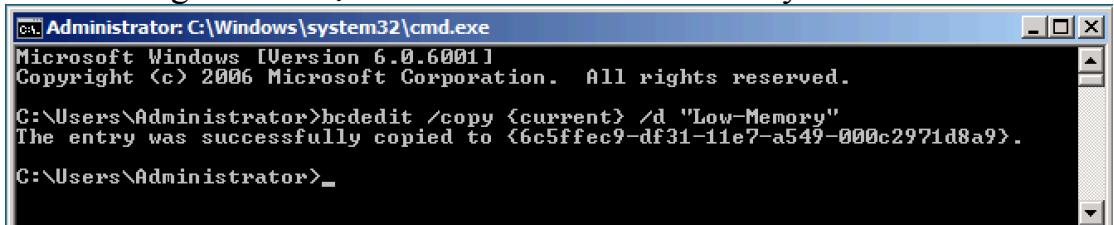
**Mục đích:** để lưu lại mọi thông tin trên RAM của máy Windows Server 2008 và sử dụng máy Kali để phân tích.

## LAB:

1. Giảm sự cố 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”

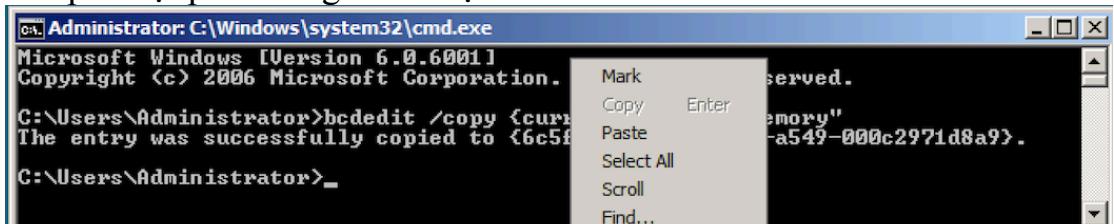


```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.0.6001]
Copyright <c> 2006 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>bcdedit /copy {current} /d "Low-Memory"
The entry was successfully copied to {6c5ffec9-df31-11e7-a549-000c2971d8a9}.

C:\Users\Administrator>_
```

- Nhập chuột phải trong cmd chọn Mark

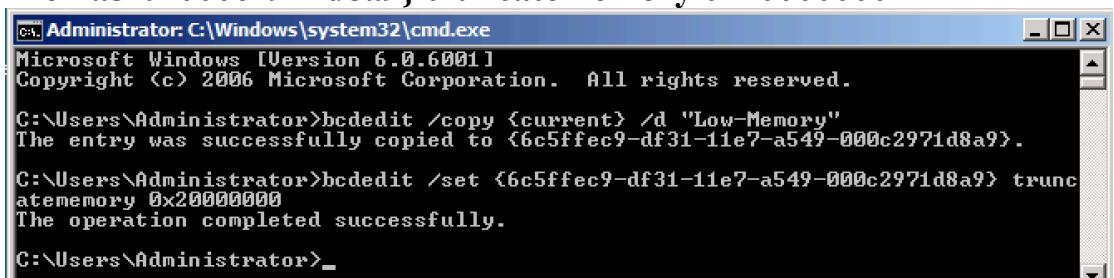


```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.0.6001]
Copyright <c> 2006 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>bcdedit /copy {current} /d "Low-Memory"
The entry was successfully copied to {6c5ffec9-df31-11e7-a549-000c2971d8a9}.

C:\Users\Administrator>_
```

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



```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.0.6001]
Copyright <c> 2006 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>bcdedit /copy {current} /d "Low-Memory"
The entry was successfully copied to {6c5ffec9-df31-11e7-a549-000c2971d8a9}.

C:\Users\Administrator>bcdedit /set {6c5ffec9-df31-11e7-a549-000c2971d8a9} truncatememory 0x20000000
The operation completed successfully.

C:\Users\Administrator>_
```

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

```
Administrator: C:\Windows\system32\cmd.exe
C:\Users\Administrator>bcdedit /set {6c5ffec9-df31-11e7-a549-000c2971d8a9} truncatetomemory 0x20000000
The operation completed successfully.

C:\Users\Administrator>bcdedit

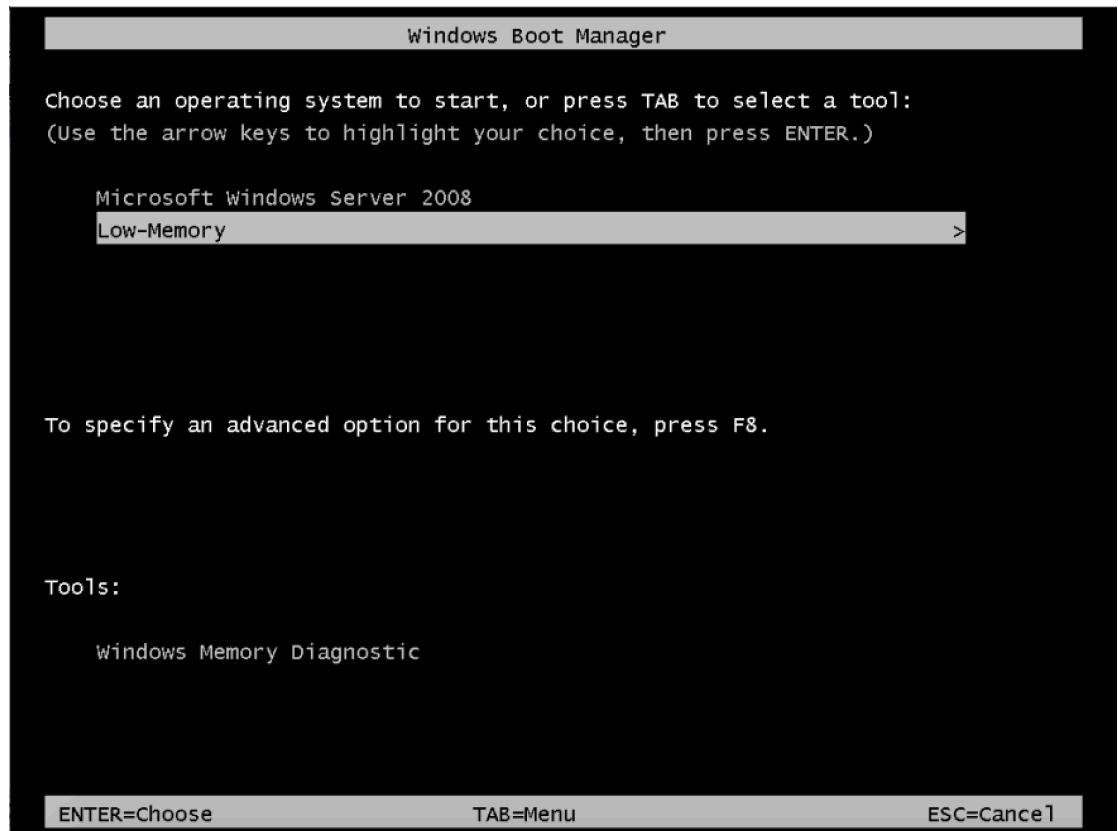
Windows Boot Manager
identifier {bootmgr}
device partition=C:
description Windows Boot Manager
locale en-US
inherit {globalsettings}
default {current}
displayorder {current}
toolsdisplayorder {memdiag}
timeout 30

Windows Boot Loader
identifier {current}
device partition=C:
path \Windows\system32\winload.exe
description Microsoft Windows Server 2008
locale en-US
inherit {bootloadersettings}
osdevice partition=C:
systemroot \Windows
resumeobject {07e1a620-dfaa-11e7-8bf5-f0028fce5e3f}
nx OptOut

Windows Boot Loader
identifier {6c5ffec9-df31-11e7-a549-000c2971d8a9}
device partition=C:
path \Windows\system32\winload.exe
description Low-Memory
locale en-US
inherit {bootloadersettings}
truncatetomemory 0x20000000
osdevice partition=C:
systemroot \Windows
resumeobject {07e1a620-dfaa-11e7-8bf5-f0028fce5e3f}
nx OptOut

C:\Users\Administrator>
```

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



## 2. Tạo chứng cứ.

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

The credit card numbers listed are:

| Card Type                                | Number              |
|--|---------------------|
| VISA                                     | 4556722882757098    |
| VISA                                     | 4485475307954073    |
| VISA                                     | 4556288984425759102 |
| MasterCard                               | 2221007379488715    |
| MasterCard                               | 272096453985362     |
| MasterCard                               | 5345124497397845    |
| American Express (AMEX)                  | 372824651270657     |
| American Express (AMEX)                  | 34162539695826      |
| American Express (AMEX)                  | 372145373101305     |
| JCB                                      | 3539176527115317    |
| JCB                                      | 3535315206935835    |
| JCB                                      | 3633510778761167486 |
| Diners Club - North America              | 5457552605870325    |
| Diners Club - North America              | 5437464710799776    |
| Diners Club - North America              | 5578902413049436    |
| Diners Club - International              | 6763946607335435    |
| Diners Club - International              | 6762222079926684    |
| Maestro                                  | 6761693304454703    |
| Discover                                 | 6011323691360135    |
| Discover                                 | 6011743273390707    |
| Discover                                 | 6011126427496445052 |
| XSD Generator                            | 30503648242268      |
| XSLT (XSL Transformer)                   | 30095282756505      |
| XML to JSON Converter                    | 30467908581700      |
| JSON to XML Converter                    | 36150665394616      |
| CSV to XML Converter                     | 367372621796863447  |
| CSV to JSON Converter                    | 4917117340561246    |
| Epoch Timestamp To Date                  | 4917141649129299    |
| Message Digester (MD5, SHA-256, SHA-512) | 4917141649129299    |
| HMAC Generator                           | 63774439048828987   |
| MD5 Generator                            | 6379998148150191    |

```

VISA:
4556722882757098
4485475307954073
4556288984425759102
MasterCard:
2221007379488715
2720996453985362
5345124497397845
American Express (AMEX):
372824651270657
341625399695826
372145373101305
Discover:
6011323691360135

```

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

```

Administrator: Command Prompt
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.

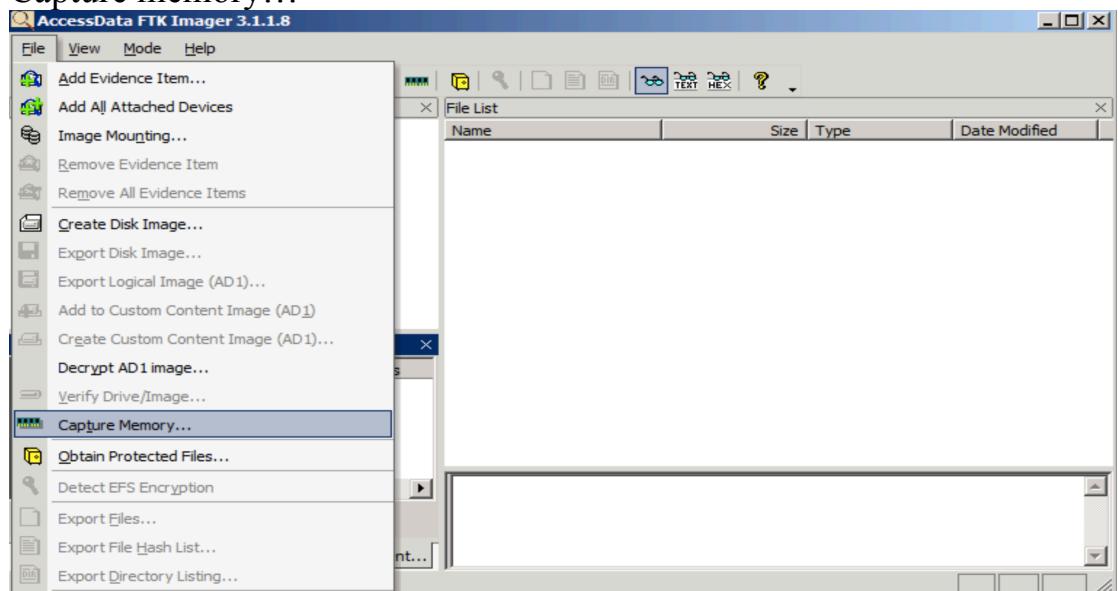
C:\Users\Administrator>net user hacker 123abc!@# /add
The command completed successfully.

C:\Users\Administrator>

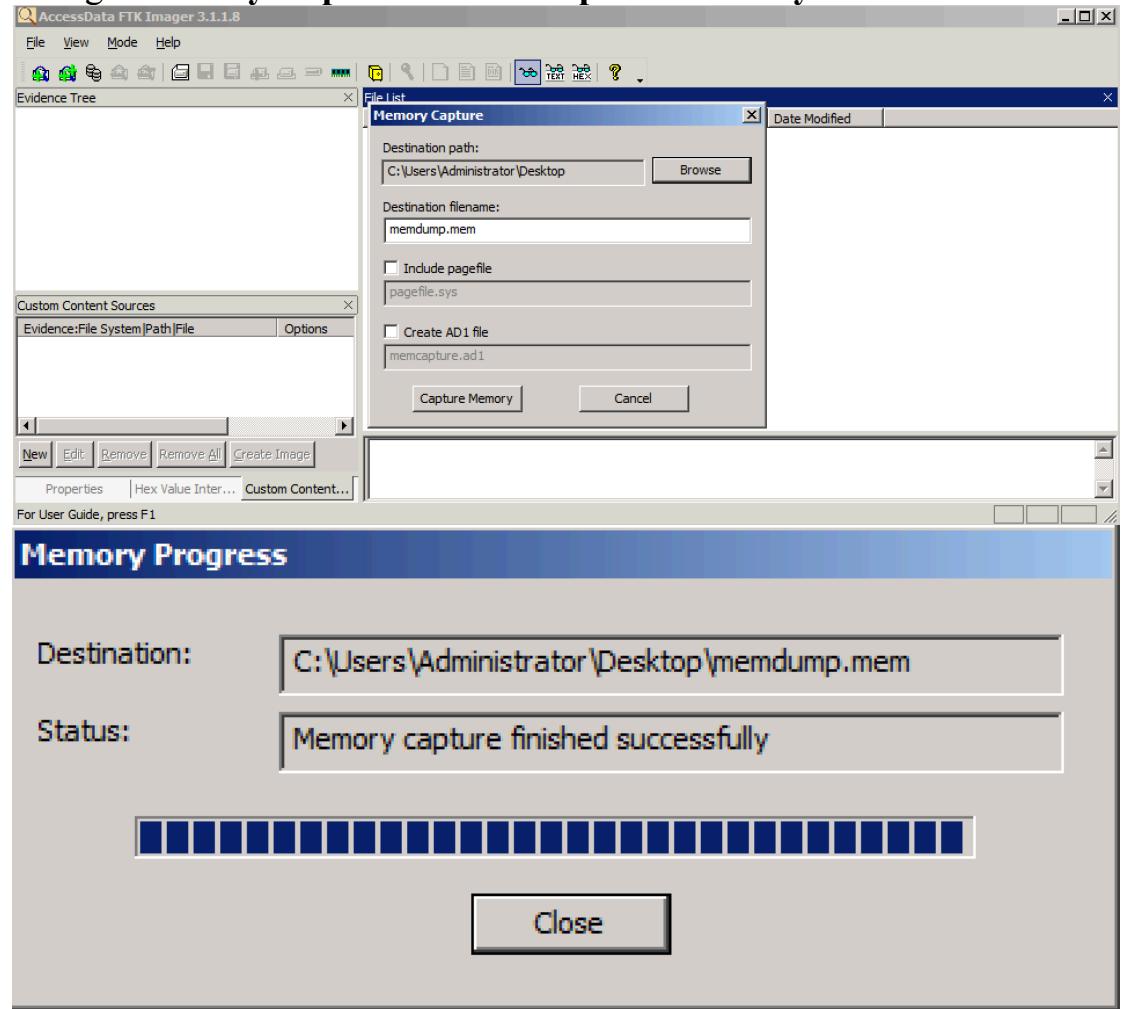
```

### 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**
- Cửa 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

```
root@kali: ~/Desktop
File Edit View Search Terminal Help
root@kali:~# cd Desktop/
root@kali:~/Desktop#
memdump.mem vmmware-tools-distrib
root@kali:~/Desktop# bulk_extractor -o bulk -e wordlist memdump.mem
bulk_extractor version: 1.3
Hostname: kali
Input file: memdump.mem
Output directory: bulk
Disk Size: 1073741824
Threads: 1
Phase 1.
8:50:40 Offset 0MB (0.00%) Done in n/a at 08:50:39
8:51:24 Offset 67MB (6.25%) Done in 0:10:51 at 09:02:15
```

```

root@kali: ~/Desktop
File Edit View Search Terminal Help
9:00:21 Offset 939MB (87.50%) Done in 0:01:23 at 09:01:44
9:01:07 Offset 1006MB (93.75%) Done in 0:00:41 at 09:01:48
All Data is Read; waiting for threads to finish...
Time elapsed waiting for 1 thread to finish:
(please wait for another 60 min .)
Time elapsed waiting for 1 thread to finish:
6 sec (please wait for another 59 min 54 sec.)
Thread 0: Processing 1056964608

All Threads Finished!
Producer time spent waiting: 646.876 sec.
Average consumer time spent waiting: 0.073664 sec.
*****
** bulk_extractor is probably CPU bound. **
** Run on a computer with more cores **
** to get better performance. **
*****
Phase 2. Shutting down scanners
Phase 3. Uniquifying and recombining wordlist
Phase 3. Creating Histograms
    ccn histogram... ccn_track2 histogram... domain histogram...
    email histogram... ether histogram... find histogram...
    ip histogram... tcp histogram... telephone histogram...
    url histogram... url microsoft-live... url services...
    url facebook-address... url facebook-id... url searches...

Elapsed time: 667.3 sec.
Overall performance: 1.609 MBytes/sec.
Total email features found: 879
root@kali:~/Desktop#

```

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

```

root@kali: ~/Desktop/bulk
File Edit View Search Terminal Help
root@kali:~/Desktop# ls
bulk memdump.mem vmware-tools-distrib
root@kali:~/Desktop# cd bulk/
root@kali:~/Desktop/bulk# ls -la
total 76828
drwxr-xr-x 2 root root      4096 Dec 13 09:01 .
drwxr-xr-x 4 root root      4096 Dec 13 08:50 ..
-rw-r--r-- 1 root root      595 Dec 13 09:01 aes_keys.txt
-rw-r--r-- 1 root root      0 Dec 13 08:50 alerts.txt
-rw-r--r-- 1 root root     499 Dec 13 09:01 ccn_histogram.txt
-rw-r--r-- 1 root root      0 Dec 13 09:01 ccn_track2_histogram.txt
-rw-r--r-- 1 root root      0 Dec 13 08:50 ccn_track2.txt
-rw-r--r-- 1 root root    22385 Dec 13 09:01 ccn.txt
-rw-r--r-- 1 root root   15705 Dec 13 09:01 domain_histogram.txt
-rw-r--r-- 1 root root  1177208 Dec 13 09:01 domain.txt
-rw-r--r-- 1 root root      0 Dec 13 08:50 elf.txt
-rw-r--r-- 1 root root   11380 Dec 13 09:01 email_histogram.txt
-rw-r--r-- 1 root root  213989 Dec 13 09:01 email.txt
-rw-r--r-- 1 root root      288 Dec 13 09:01 ether_histogram.txt
-rw-r--r-- 1 root root   83635 Dec 13 09:01 ether.txt
-rw-r--r-- 1 root root      0 Dec 13 08:50 exif.txt
-rw-r--r-- 1 root root      0 Dec 13 09:01 find_histogram.txt
-rw-r--r-- 1 root root      0 Dec 13 08:50 find.txt
-rw-r--r-- 1 root root      0 Dec 13 08:50 gps.txt
-rw-r--r-- 1 root root      0 Dec 13 08:50 hex.txt
-rw-r--r-- 1 root root      837 Dec 13 09:01 ip_histogram.txt
-rw-r--r-- 1 root root   4885 Dec 13 09:01 ip.txt
-rw-r--r-- 1 root root  48281 Dec 13 09:01 json.txt
-rw-r--r-- 1 root root      0 Dec 13 08:50 kml.txt
-rw-r--r-- 1 root root  1847480 Dec 13 09:01 packets_pcap

```

## 5. Kiểm tra

- kiểm tra Domain Names: trong terminal, thực thi lệnh cat domain\_histogram.txt

```
root@kali: ~/Desktop/bulk
File Edit View Search Terminal Help
n=1175 www.microsoft.com
n=976 2.0.0.0
n=519 mozilla.org      (utf16=117)
n=418 www.ccsf.edu
n=407 tpc.googlesyndication.com
n=372 fpt.edu.vn
n=372 schemas.microsoft.com
n=353 www.mozilla.org
n=268 go.microsoft.com
n=201 ns.adobe.com
n=196 www.verisign.com
n=167 home.netscape.com
n=144 licensing.microsoft.com
n=140 www.mozilla.com
n=131 www.freeformatter.com
n=128 thawte.com
n=127 www
n=117 www.google.com.vn
n=98 crl.thawte.com
n=96 ocsp.thawte.com
n=96 ocsp.verisign.com
n=78 crl.microsoft.com
n=67 java.com
n=63 apis.google.com
n=62 crl.verisign.com
n=58 6.0.0.0
n=58 www.usertrust.com
n=53 1.0.0.0
n=53 googleleads.g.doubleclick.net
```

chúng ta có thể thấy các domain đã truy cập.

- Kiểm tra số điện thoại: cat telephone\_histogram.txt

```
root@kali: ~/Desktop/bulk
File Edit View Search Terminal Help
root@kali:~/Desktop/bulk# cat telephone_histogram.txt
# UTF-8 Byte Order Marker; see http://unicode.org/faq/utf_bom.html
# bulk_extractor-Version: 1.3 ($Rev: 10578 $)
# Filename: memdump.mem
# Feature-Recorder: telephone
# Histogram-File-Version: 1.1
n=2 4152393000
root@kali:~/Desktop/bulk#
```

- Kiểm tra số Credit card: cat ccn\_histogram.txt

```
root@kali: ~/Desktop/bulk
File Edit View Search Terminal Help
root@kali:~/Desktop/bulk# cat ccn_histogram.txt
# UTF-8 Byte Order Marker; see http://unicode.org/faq/utf_bom.html
# bulk_extractor-Version: 1.3 ($Rev: 10578 $)
# Filename: memdump.mem
# Feature-Recorder: ccn
# Histogram-File-Version: 1.1
n=19 4844748977005400
n=19 4917117340561246
n=19 4917141649129299
n=17 341625399695826
n=17 372145373101305
n=17 372824651270657
n=17 4485475307954073
n=17 4556722882757098
n=17 5345124497397845
n=17 5457552605870325
n=17 5578902413049436
n=17 6011323691360135
n=17 6011743273390707
n=16 5437464710799776
root@kali:~/Desktop/bulk#
```

- Kiểm tra Wordlist: cat wordlist.txt

```
root@kali: ~/Desktop/bulk
File Edit View Search Terminal Help
# UTF-8 Byte Order Marker; see http://unicode.org/faq/utf_bom.html
# bulk_extractor-Version: 1.3 ($Rev: 10578 $)
# Filename: memdump.mem
# Feature-Recorder: wordlist
# Feature-File-Version: 1.1
31971 TCPAu$
31995 fSfSfU
32060 fY[ZfYfY
32148 occurred
32159 BOOTMGR
32170 missing
32180 BOOTMGR
32191 compressed
32210 Ctrl+Alt+Del
32226 restart
33282 fSfPfQfVfW
33300 f_f^fYf
33399 fTfVgf
33422 fPfPgf
33465 fZfYfBf0fV
```

- Kiểm tra email: cat email\_histogram.txt

```
root@kali: ~/Desktop/bulk
File Edit View Search Terminal Help
n=1 supportaccessplugin@gmail.com (utf16=1)
n=1 test2@test.org (utf16=1)
n=1 test3@test.org (utf16=1)
n=1 test@test.org (utf16=1)
n=1 tf@mozilla.org (utf16=1)
n=1 toolbar@ask.com (utf16=1)
n=1 tvht@ht.hu
n=1 ube@youtube3.com (utf16=1)
n=1 ubeeing@youtuberie.com (utf16=1)
n=1 unblocker20_web@unblocker.yt (utf16=1)
n=1 update@firefox.com (utf16=1)
n=1 vpyekkifgv@vpyekkifgv.org (utf16=1)
n=1 webbooster@iminent.com (utf16=1)
n=1 who@w9.net (utf16=1)
n=1 www-math@w3.org
n=1 xdict@www.iciba.com (utf16=1)
n=1 xivars@aol.com (utf16=1)
n=1 xuth@mozilla.org (utf16=1)
n=1 xz123@ya456.com (utf16=1)
n=1 youplayer@addons.mozilla.org (utf16=1)
n=1 youtube@2youtube.com (utf16=1)
```

## 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.addrspace.legacyintel (AttributeError: 'module' object has 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

## Registry Analysis Volatility™ Plugins

**hivelist** - Find and list available registry hives  
`# vol.py hivelist`

**hivedump** - Print all keys and subkeys in a hive  
`-o` Offset of registry hive to dump (virtual offset)  
`# vol.py hivedump -o 0xelal4b60`

**printkey** - Output a registry key, subkeys, and values  
`-K "Registry key path"`  
`# vol.py printkey -K "Software\Microsoft\Windows\CurrentVersion\Run"`

**userassist** - Find and parse userassist key values  
`# vol.py userassist`

**hashdump** - Dump user NTLM and Lanman hashes  
`-y` Virtual offset of SYSTEM registry hive (from  
`hivelist`)  
`-s` Virtual offset of SAM registry hive (from  
`hivelist`)  
`# vol.py hashdump -y 0x8781c008 -s 0x87f6b9c8`

- Thông tin Image:  
`python vol.py imageinfo -f /root/Desktop/memdump.mem`

```

root@kali:/usr/share/volatility# python vol.py imageinfo -f /root/Desktop/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 : 0xffffdf0000L
        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
```

| Offset(V)  | Name             | PID  | PPID | Thds | Hnds | Sess | Wow64 | Start                          | Exit |
|------------|------------------|------|------|------|------|------|-------|--------------------------------|------|
| 0x8ab55d8  | 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     | 0 2017-12-13 14:22:51 UTC+0000 |      |
| 0x8ae8dd90 | csrss.exe        | 536  | 528  | 9    | 267  | 1    | 0     | 0 2017-12-13 14:22:51 UTC+0000 |      |
| 0x8ae8d348 | wininit.exe      | 544  | 476  | 3    | 98   | 0    | 0     | 0 2017-12-13 14:22:51 UTC+0000 |      |
| 0x8ae4158  | winlogon.exe     | 576  | 528  | 3    | 114  | 1    | 0     | 0 2017-12-13 14:22:51 UTC+0000 |      |
| 0x8aec000  | services.exe     | 624  | 544  | 6    | 238  | 0    | 0     | 0 2017-12-13 14:22:52 UTC+0000 |      |
| 0x8aed6198 | lsass.exe        | 636  | 544  | 17   | 612  | 0    | 0     | 0 2017-12-13 14:22:52 UTC+0000 |      |
| 0x8aed4980 | lsm.exe          | 644  | 544  | 18   | 163  | 0    | 0     | 0 2017-12-13 14:22:52 UTC+0000 |      |
| 0x8af641f0 | svchost.exe      | 804  | 624  | 7    | 297  | 0    | 0     | 0 2017-12-13 14:22:52 UTC+0000 |      |
| 0x8af796b0 | vmacthlp.exe     | 852  | 624  | 1    | 49   | 0    | 0     | 0 2017-12-13 14:22:52 UTC+0000 |      |
| 0x8af95d90 | svchost.exe      | 884  | 624  | 7    | 277  | 0    | 0     | 0 2017-12-13 14:22:52 UTC+0000 |      |
| 0x8afba998 | svchost.exe      | 928  | 624  | 15   | 281  | 0    | 0     | 0 2017-12-13 14:22:52 UTC+0000 |      |
| 0x8afab98  | svchost.exe      | 1000 | 624  | 6    | 126  | 0    | 0     | 0 2017-12-13 14:22:52 UTC+0000 |      |
| 0x8afe6578 | svchost.exe      | 1016 | 624  | 37   | 917  | 0    | 0     | 0 2017-12-13 14:22:52 UTC+0000 |      |
| 0x8afff778 | SLsvc.exe        | 1064 | 624  | 4    | 69   | 0    | 0     | 0 2017-12-13 14:22:52 UTC+0000 |      |
| 0xb01dd50  | svchost.exe      | 1108 | 624  | 12   | 480  | 0    | 0     | 0 2017-12-13 14:22:52 UTC+0000 |      |
| 0xb0f7d8   | svchost.exe      | 1172 | 624  | 20   | 246  | 0    | 0     | 0 2017-12-13 14:22:52 UTC+0000 |      |
| 0xb037478  | svchost.exe      | 1200 | 624  | 16   | 384  | 0    | 0     | 0 2017-12-13 14:22:52 UTC+0000 |      |
| 0xb09ed90  | svchost.exe      | 1328 | 624  | 29   | 282  | 0    | 0     | 0 2017-12-13 14:22:53 UTC+0000 |      |
| 0xb021870  | taskeng.exe      | 1432 | 1016 | 5    | 132  | 0    | 0     | 0 2017-12-13 14:23:04 UTC+0000 |      |
| 0xb0802730 | spoolsv.exe      | 1516 | 624  | 17   | 309  | 0    | 0     | 0 2017-12-13 14:23:08 UTC+0000 |      |
| 0xb124880  | svchost.exe      | 1580 | 624  | 5    | 125  | 0    | 0     | 0 2017-12-13 14:23:08 UTC+0000 |      |
| 0xb135d90  | svchost.exe      | 1600 | 624  | 3    | 73   | 0    | 0     | 0 2017-12-13 14:23:08 UTC+0000 |      |
| 0xb1471c0  | VGAAuthService.e | 1640 | 624  | 2    | 81   | 0    | 0     | 0 2017-12-13 14:23:08 UTC+0000 |      |
| 0xb187d90  | vmtoolsd.exe     | 1808 | 624  | 8    | 284  | 0    | 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#
```

KALI LINUX

### - Services:

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

```
root@kali:/usr/share/volatility# python vol.py svcscan --profile=Win2008SP1x86
-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
```

KALI LINUX

### - Registry Hives:

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

```
root@kali:/usr/share/volatility# python vol.py hivelist --profile=Win2008SP1x86
-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\COMPONENTS
0x90fd86a8 0x22ebf6a8 \Device\HarddiskVolume1\Boot\BCD
0x99a0ea20 0x25574a20 \Device\HarddiskVolume1\Windows\ServiceProfiles\NetworkService\NTUSER.DAT
0x99a3d460 0x2555c460 \Device\HarddiskVolume1\Windows\ServiceProfiles\LocalService\NTUSER.DAT
0x9aea1350 0x10da9350 \Device\HarddiskVolume1\Users\Administrator\NTUSER.DAT
0x9aeada20 0x10c53a20 \Device\HarddiskVolume1\Users\Administrator\AppData\Local\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#
```

KALI LINUX

Chúng ta chú ý 2 địa chỉ được bôi đỏ ở trên, nó 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.

The screenshot shows the CrackStation website interface. At the top, there's a navigation bar with links for 'CrackStation', 'Password Hashing Security', and 'Defuse Security'. Below the navigation, the main title 'Free Password Hash Cracker' is displayed. A text input field is labeled 'Enter up to 20 non-salted hashes, one per line:' followed by a large text area containing the hash '85d124d30549f4fa5b6d9dc212ff11e6'. To the right of the input field is a CAPTCHA challenge with two distorted words ('haart' and 'Cedar') and a 'reCAPTCHA' checkbox. Below the input field, a note says 'Supports: LM, NTLM, md2, md4, md5, md5(md5\_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sh1\_bin)), QubesV3.1BackupDefaults'. A table below shows the cracked result: Hash '85d124d30549f4fa5b6d9dc212ff11e6' is listed under 'Type' as 'NTLM' and the 'Result' is '123abc1#'. A note at the bottom states 'Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.'