

Lab 12: Capturing a RAM Image

Course Name: Malware Analysis and Reverse Engineering (IAM302)

Student Name: Nguyễn Trần Vinh – SE160258

Instructor Name: Mai Hoàng Đình

Lab Due Date: 25/2/2023

Purpose

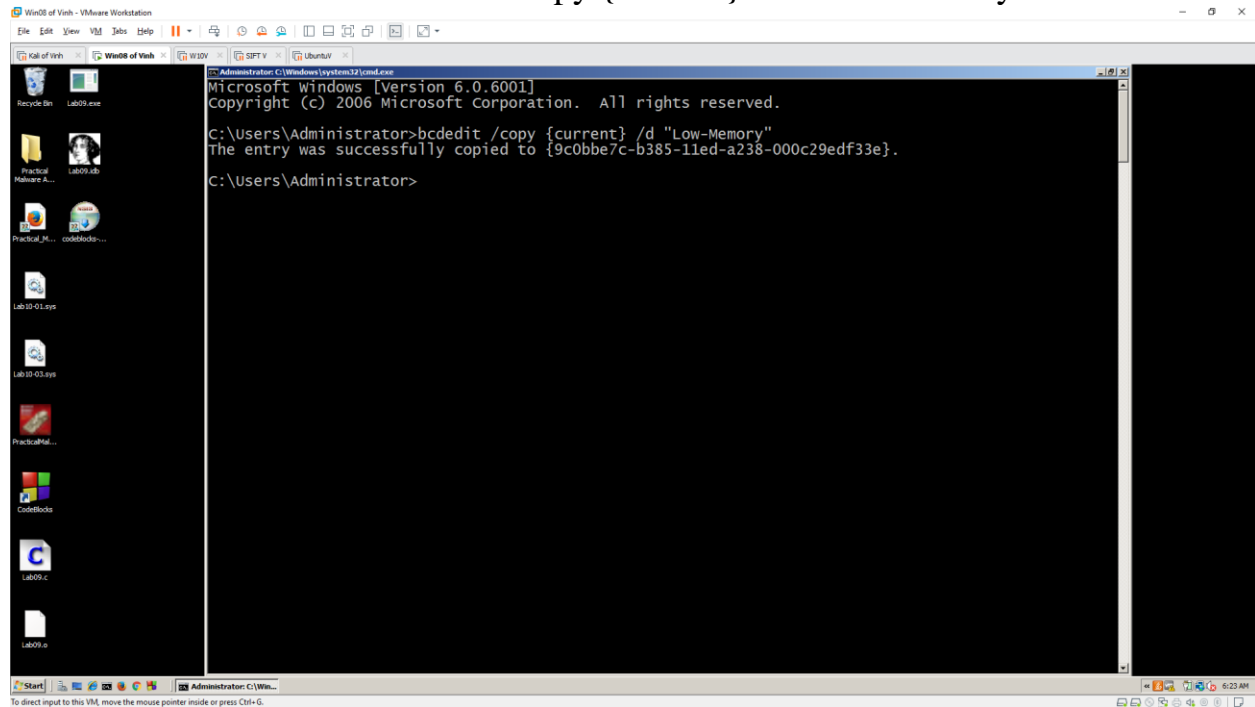
- To save all information on the RAM of the Windows Server 2008 machine and use the Kali machine for analysis.

What we need

- The Windows Server 2008 virtual machine you prepared in the previous project. If you don't have it, you could use any Windows machine, real or virtual.
- Kali machine to analysis

Step by step

- Window + R -> cmd -> bcdedit /copy {current} /d "Low-Memory"



- bcdedit /set {9c0bbe7c-b385-11ed-a238-000c29edf33e} truncatememory 0x20000000

```
Win08 of Vmsh - VMware Workstation
File Edit View VM Tools Help
Kali of Vmsh World of Vmsh WSDV SPTV Ubuntu

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 {9c0bbe7c-b385-11ed-a238-000c29edf33e}.

C:\Users\Administrator>bcdedit /set {9c0bbe7c-b385-11ed-a238-000c29edf33e} truncatememory 0x20000000
The operation completed successfully.

C:\Users\Administrator>
```

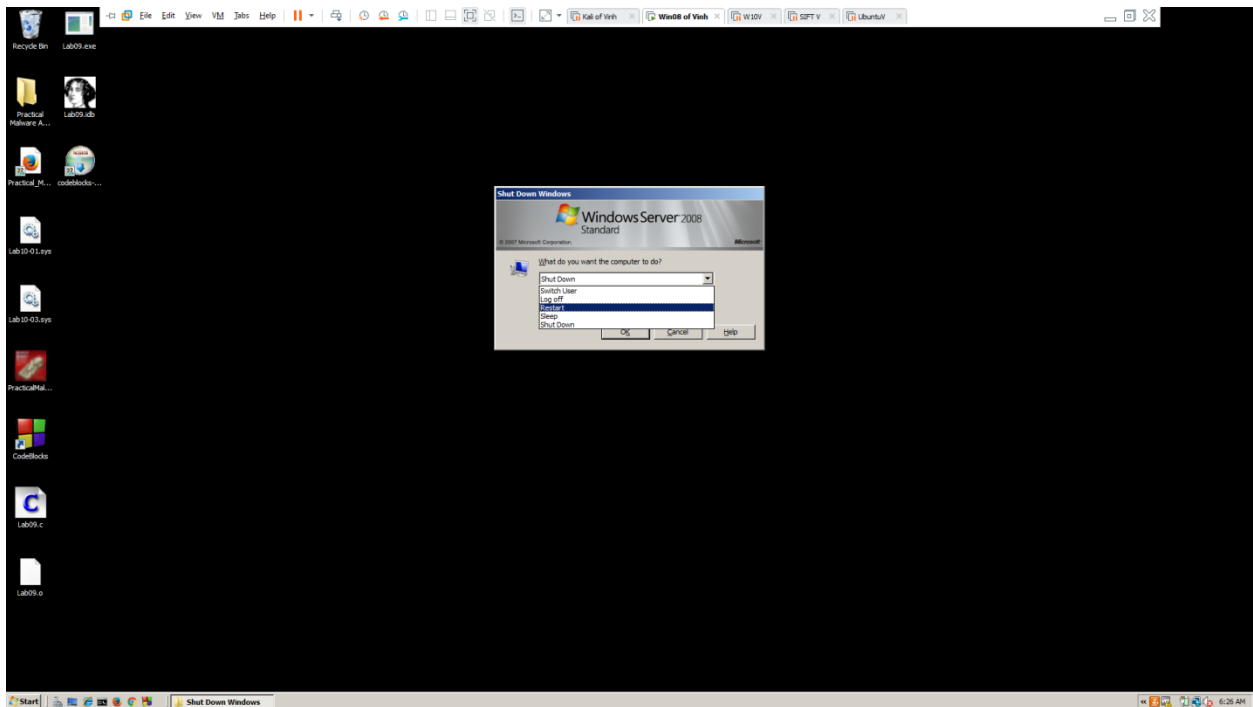
- bcdedit

```
Windows Boot Manager
-----
identifier                {bootmgr}
device                    partition=C:
description                Windows Boot Manager
locale                    en-US
inherit                    {globalsettings}
default                    {current}
displayorder                {current}
toolsdisplayorder          {9c0bbe7c-b385-11ed-a238-000c29edf33e}
timeout                    {memdiag}
timeout                    30

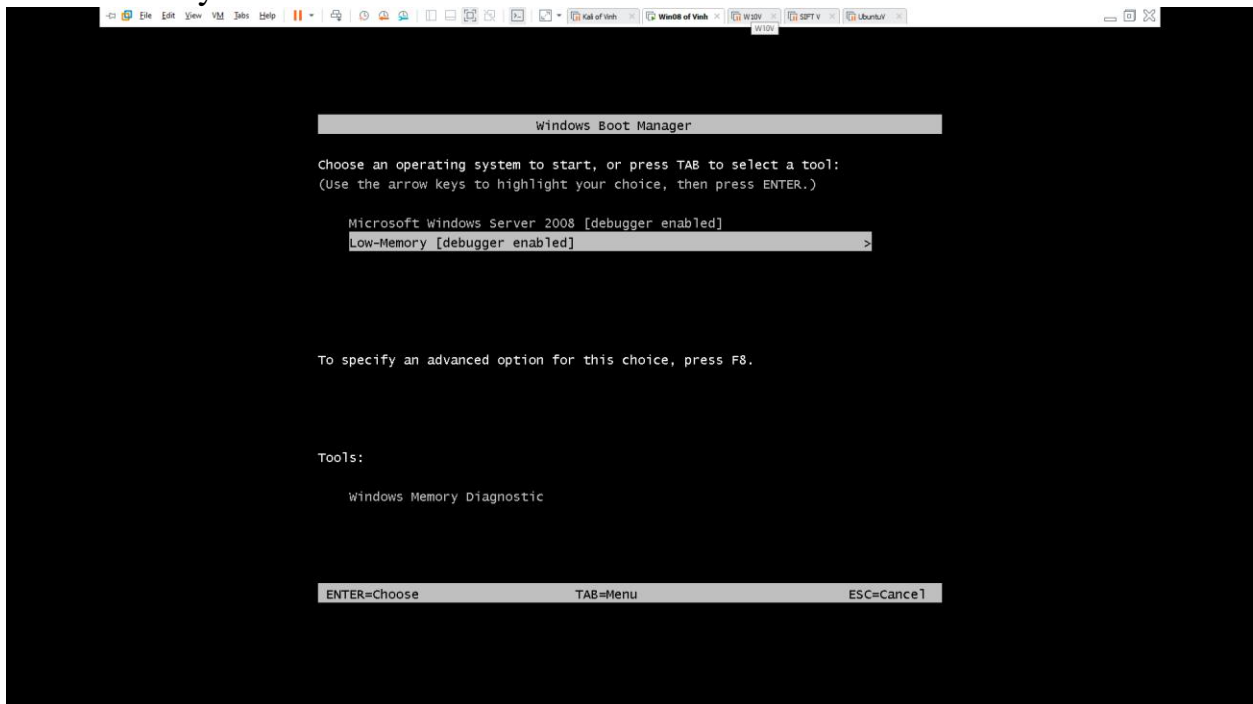
Windows Boot Loader
-----
identifier                {current}
device                    partition=C:
path                        \windows\system32\winload.exe
description                Microsoft Windows Server 2008
locale                    en-US
inherit                    {bootloadersettings}
osdevice                    partition=C:
systemroot                \windows
resumeobject                {65f5eff5-ca68-11e2-b047-d1bf681c9220}
nx                          OptIn
debug                      Yes

Windows Boot Loader
-----
identifier                {9c0bbe7c-b385-11ed-a238-000c29edf33e}
device                    partition=C:
path                        \windows\system32\winload.exe
description                Low-Memory
locale                    en-US
inherit                    {bootloadersettings}
truncatememory              0x20000000
osdevice                    partition=C:
systemroot                \windows
resumeobject                {65f5eff5-ca68-11e2-b047-d1bf681c9220}
nx                          OptIn
debug                      Yes
```

- restart machine

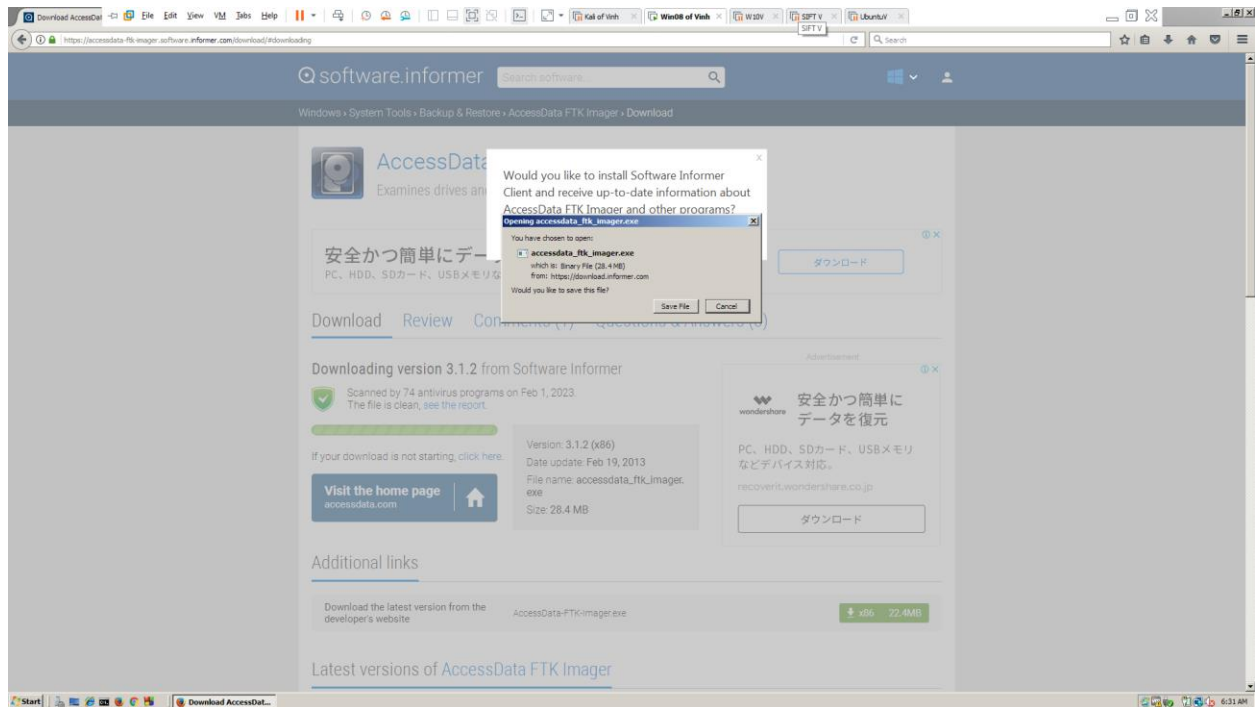


- low-memory

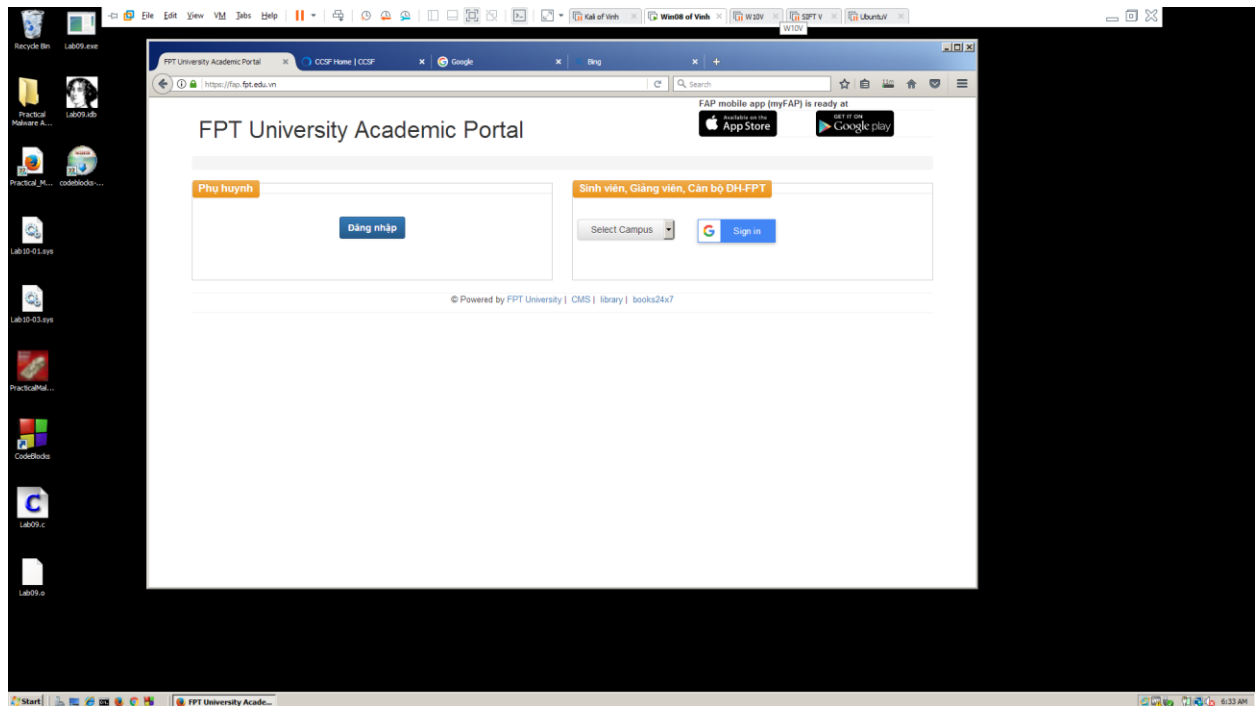


- Creating Evidence

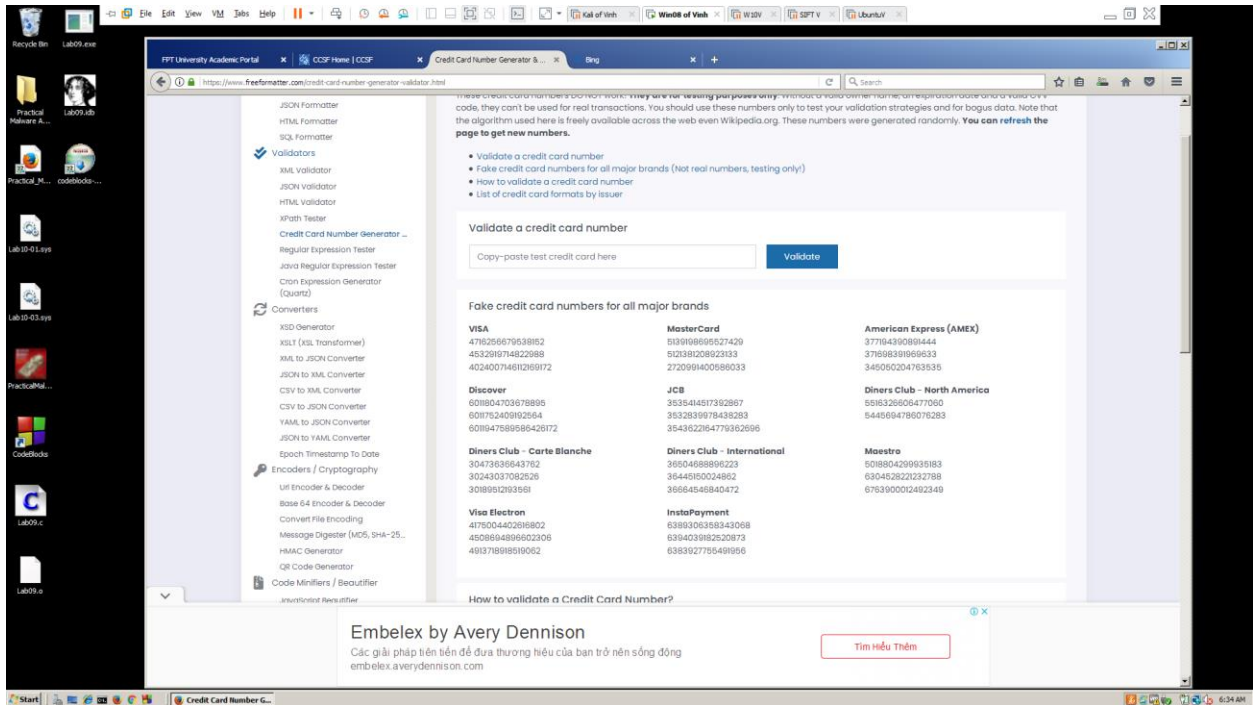
- Download FTK Imager Lite version 3.1.2



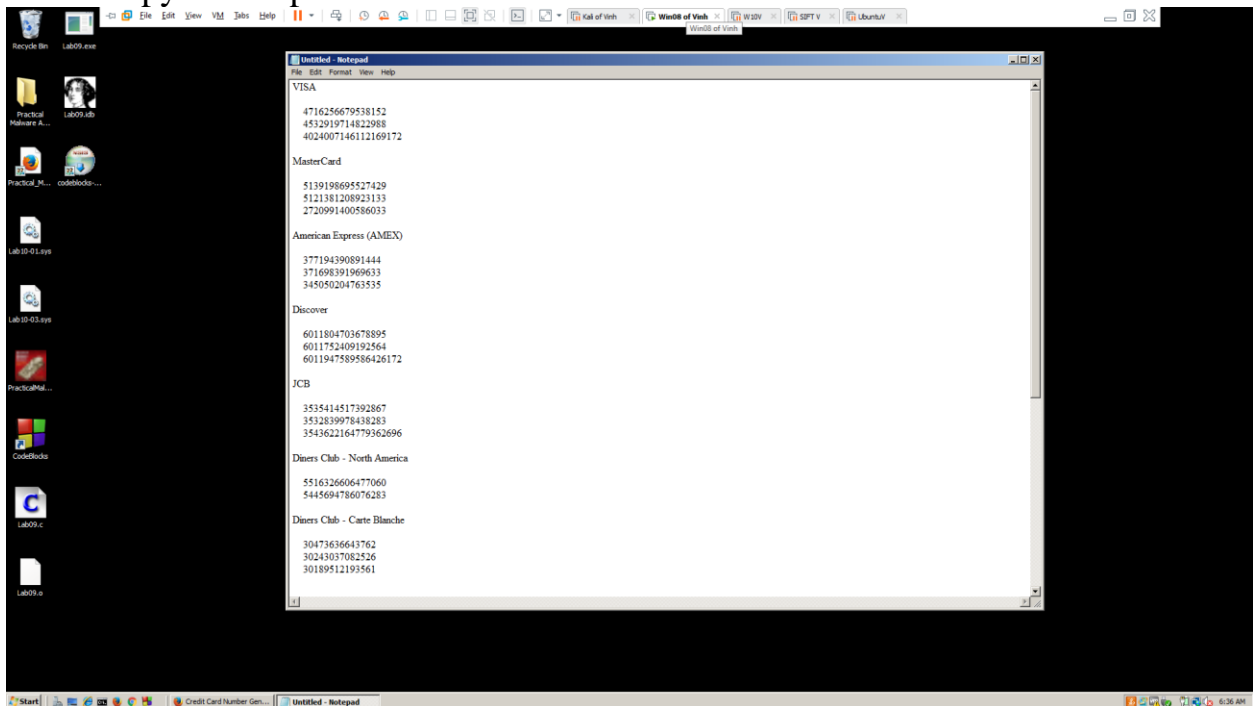
- Visit website:



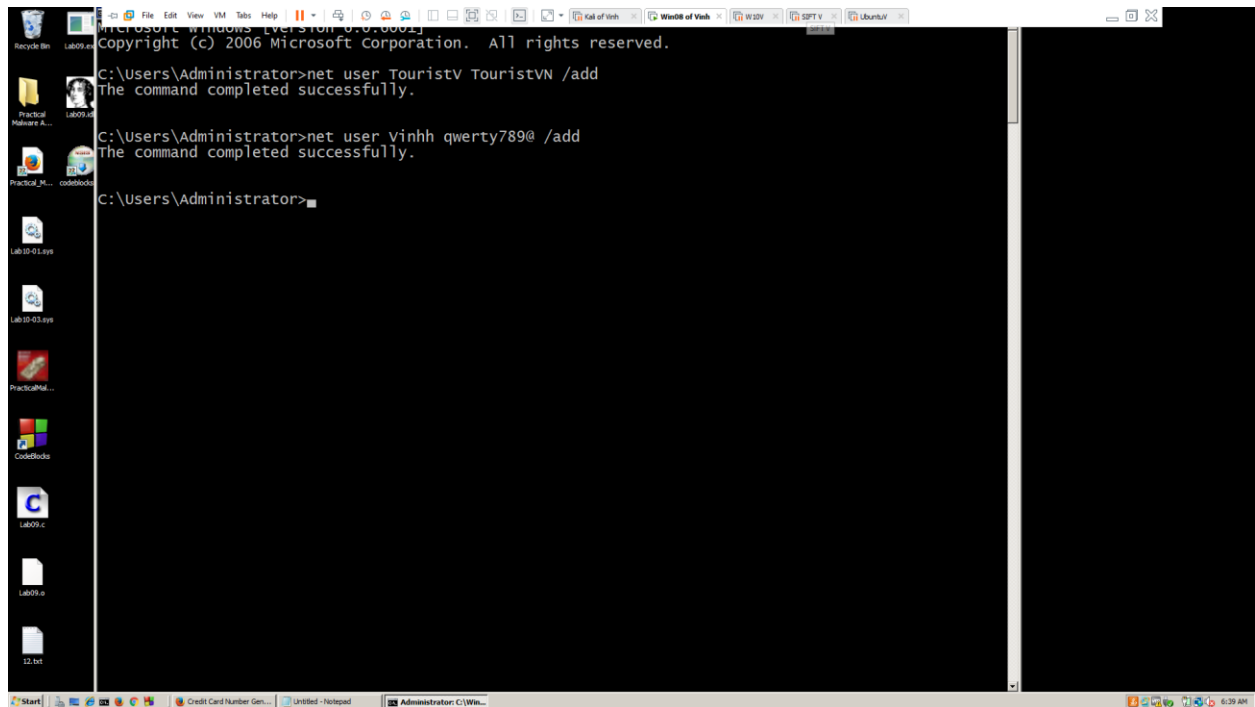
- Search “fake credit card numbers”



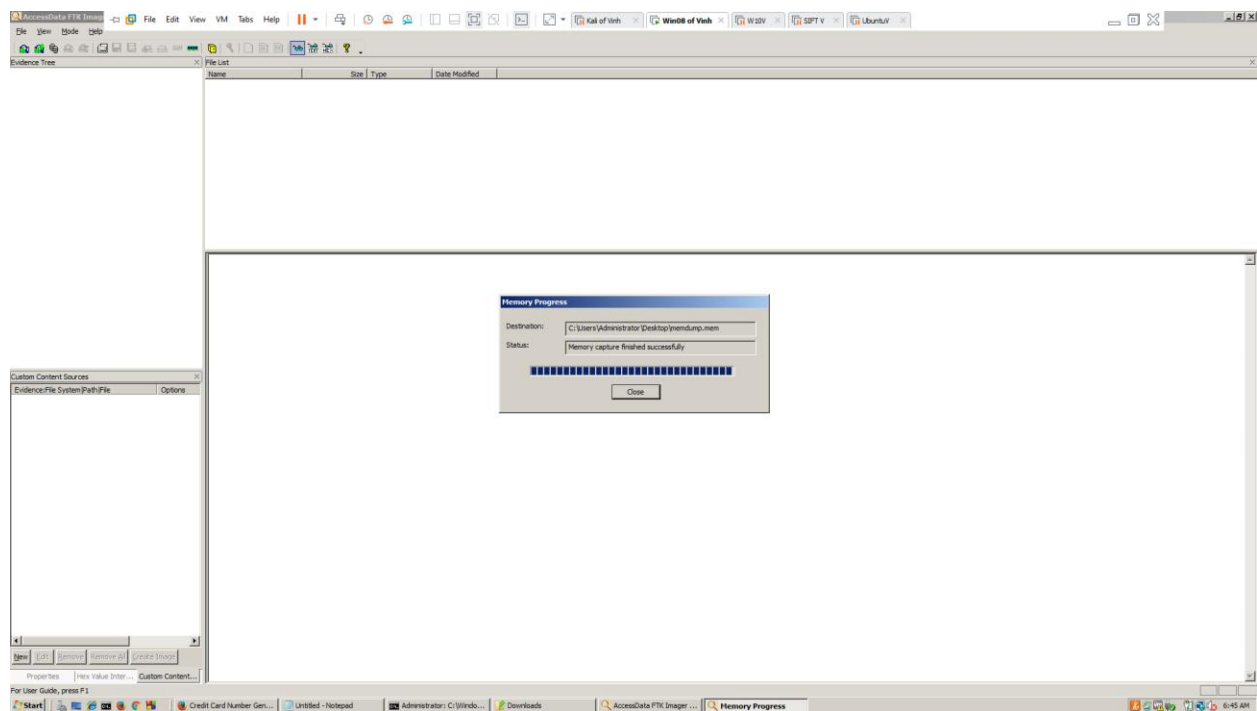
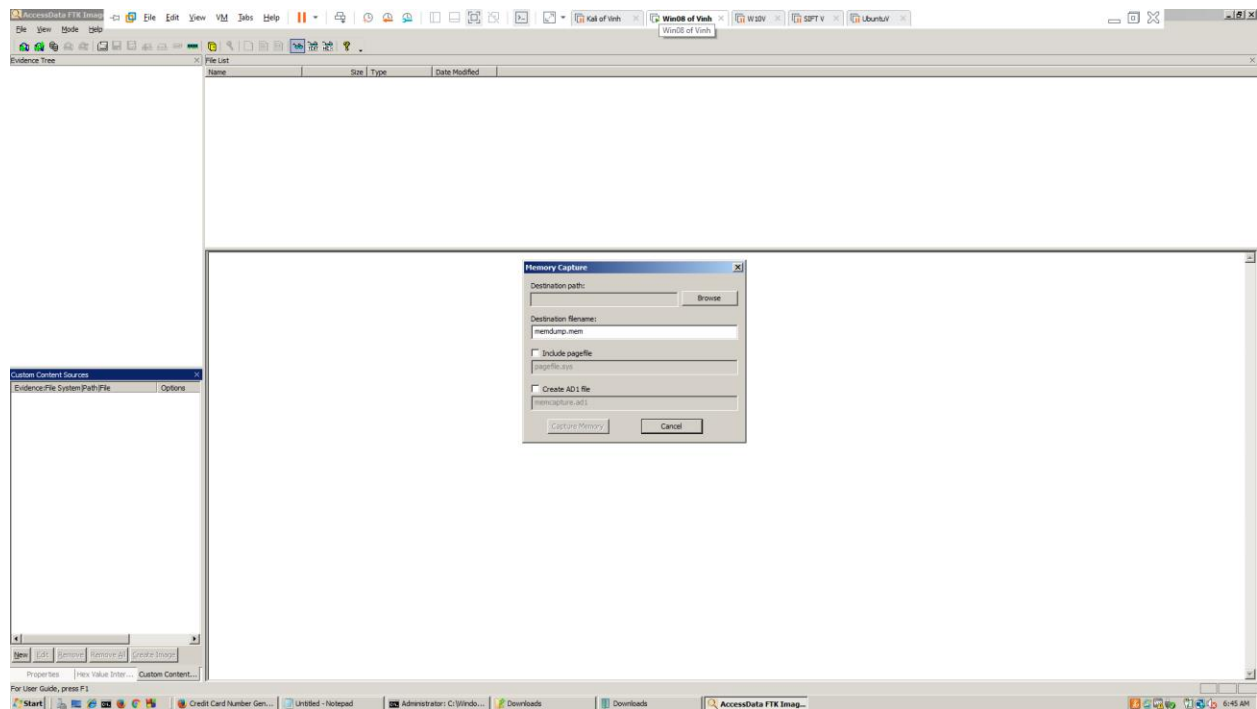
- Copy to notepad



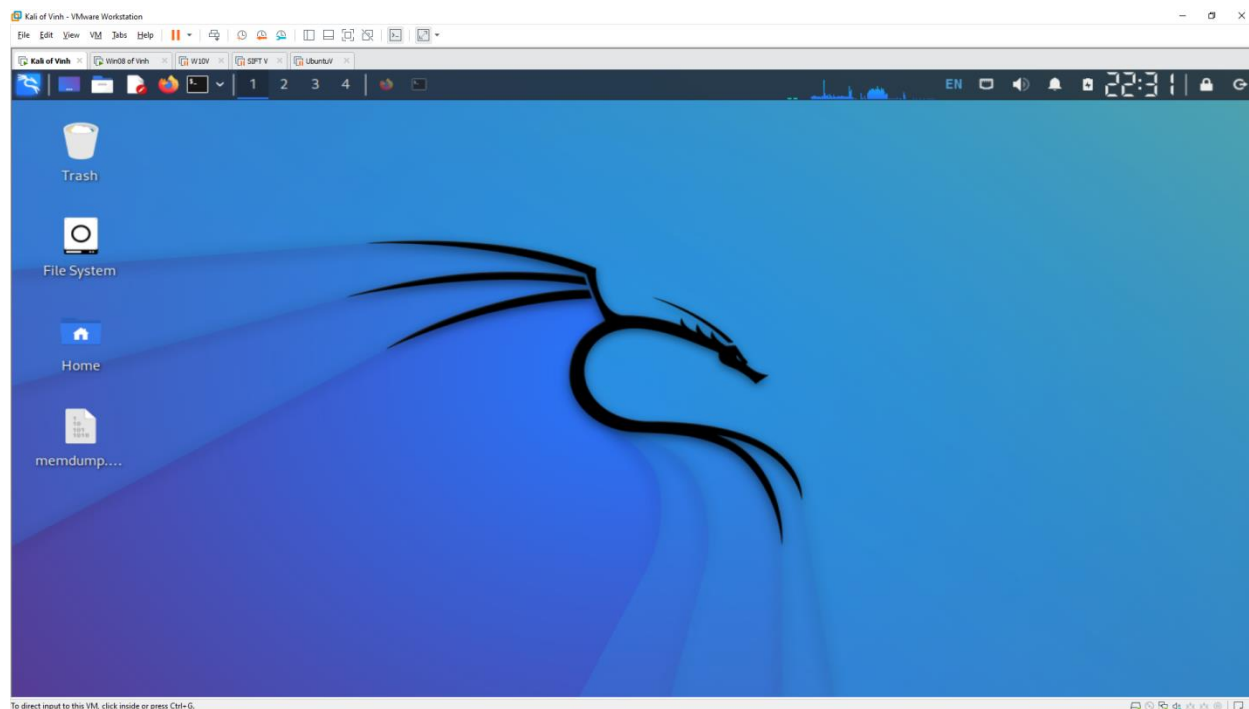
- Create user by net user in cmd



- Acquiring a RAM Image with FTK Imager



- Send file **memdump.mem** to Kali machine



- Bulk Extractor

```
TouristV@kali: ~/Desktop
File Actions Edit View Help
Usage: 100%

(TouristV@kali)~$ cd Desktop
(TouristV@kali)~/Desktop$ bulk_extractor -o bulk -e wordlist memdump.mem
mkdir "bulk"
bulk_extractor version: 2.0.0
Input file: "memdump.mem"
Output directory: "bulk"
Disk Size: 536870912
Scanners: aes base64 elf evtx exif facebook find gzip httplogs json kml_carved mxml net ntfsindx ntfslogfile ntfsmft ntfsusn pdf rar sqlite utmp vcard_carv
ed windirs winlnk winpe winprefetch wordlist zip accts email gps
Threads: 4
going multi-threaded ... ( 4 )
bulk_extractor Thu Feb 23 10:33:45 2023

available_memory: 2776174592
bytes_queued: 0
depth0_bytes_queued: 0
depth0_sbufs_queued: 0
elapsed_time: 0:00:00
estimated_date_completion: 2023-02-23 10:33:44
estimated_time_remaining: n/a
fraction_read: 0.000000 %
max_offset: 0
sbufs_created: 0
sbufs_queued: 0
sbufs_remaining: 0
tasks_queued: 0
thread_count: 4
>.....

bulk_extractor Thu Feb 23 10:33:46 2023
available_memory: 2710212608
bytes_queued: 650117120
```



```
TouristV@kali: ~/Desktop
File Actions Edit View Help
bulk_extractor Thu Feb 23 10:34:23 2023

available_memory: 2664615936
bytes_queued: 33554432
depth0_bytes_queued: 33554432
depth0_sbufs_queued: 2
elapsed_time: 0:00:38
estimated_date_completion: 2023-02-23 10:34:23
estimated_time_remaining: 0:00:00
fraction_read: 100.000000 %
max_offset: 520093696
sbufs_created: 3175687
sbufs_queued: 2
sbufs_remaining: 1
tasks_queued: 0
thread-2: 520093696: accts (16777216 bytes)
thread-3: 520093696: email (16777216 bytes)
thread_count: 4

Phase 2. Shutting down scanners
Computing final histograms and shutting down...
Phase 3. Generating stats and printing final usage information
All Threads Finished!
Elapsed time: 39.64 sec.
Total MB processed: 536
Overall performance: 13.54 MBytes/sec 3.386 (MBytes/sec/thread)
sbufs created: 3175690
sbufs unaccounted: 0
Time producer spent waiting for scanners to process data: 0:00:31 (31.95 seconds)
Time consumer scanners spent waiting for data from producer: 0:00:01 (1.56 seconds)
Average time each consumer spent waiting for data from producer: 0:00:00 (0.00 seconds)
*** More time spent waiting for workers. You need a faster CPU or more cores for improved performance.
Total email features found: 1069

(TouristV@kali)~/Desktop
$
```

```
TouristV@kali: ~/Desktop/bulk
File Actions Edit View Help
Computing final histograms and shutting down...
Phase 3. Generating stats and printing final usage information
All Threads Finished!
Elapsed time: 39.64 sec.
Total MB processed: 536
Overall performance: 13.54 MBytes/sec 3.386 (MBytes/sec/thread)
sbufs created: 3175690
sbufs unaccounted: 0
Time producer spent waiting for scanners to process data: 0:00:31 (31.95 seconds)
Time consumer scanners spent waiting for data from producer: 0:00:01 (1.56 seconds)
Average time each consumer spent waiting for data from producer: 0:00:00 (0.00 seconds)
*** More time spent waiting for workers. You need a faster CPU or more cores for improved performance.
Total email features found: 1069

(TouristV@kali)~/Desktop
$ ls
bulk memdump.mem

(TouristV@kali)~/Desktop
$ cd bulk

(TouristV@kali)~/Desktop/bulk
$ ls
aes_keys.txt          ether_histogram_1.txt ip.txt               packets.pcap         telephone.txt         windirs.txt
alerts.txt            ether_histogram.txt  jpeg_carved.txt     pii_teamviewer.txt  unrar_carved.txt     winlnk.txt
ccn_histogram.txt     ether.txt            json.txt            rar.txt             url_facebook-address.txt winpe_carved.txt
ccn_track2_histogram.txt evtx_carved.txt      kml_carved.txt      report.xml          url_facebook-id.txt  winpe.txt
ccn_track2.txt        evtx_carved.txt      ntfsindx_carved.txt rfc822.txt          url_histogram.txt    winprefetch.txt
ccn.txt              facebook.txt         ntfslogfile_carved.txt sqlite_carved        url_microsoft-live.txt wordlist_dedup_1.txt
domain_histogram.txt find_histogram.txt   ntfsmft_carved.txt  tcp_histogram.txt   url_searches.txt     wordlist.txt
elf.txt              find.txt            ntfsusn_carved.txt  tcp.txt             url_services.txt     zip
email_domain_histogram.txt gps.txt             ntfsusn_carved.txt  telephone_histogram.txt vcard.txt
email_histogram.txt   httplogs.txt        ip_histogram.txt    telephone_histogram.txt vcard.txt
email.txt             ip_histogram.txt    ntfsusn_carved.txt  telephone_histogram.txt vcard.txt

(TouristV@kali)~/Desktop/bulk
$
```

- check domain_histogram.txt

```
TouristV@kali: ~/Desktop/bulk
File Actions Edit View Help

(TouristV@kali)-[~/Desktop/bulk]
$ cat domain_histogram.txt
# BANNER FILE NOT PROVIDED (-b option)
# BULK_EXTRACTOR-Version: 2.0.0
# Feature-Recorder: domain
# Filename: memdump.mem
# Histogram-File-Version: 1.1
n=853 pagead2.googlesyndication.com
n=810 bugzilla.mozilla.org
n=685 www.ccsf.edu
n=416 googleads.g.doubleclick.net
n=413 www.google.com
n=334 www.exterro.com
n=258 mozilla.org (utf16-27)
n=208 www.googletagservices.com
n=173 bugzilla
n=154 www.gstatic.com
n=152 img.informer.com
n=152 www.w3.org
n=147 tpc.googlesyndication.com
n=145 www.freeformatter.com
n=138 fap.fpt.edu.vn
n=134 accessdata-ftk-imager.software.informer.com
n=123 cm.g.doubleclick.net
n=119 cl.adform.net
n=96 ocsp.pki.goog
n=93 www.verisign.com
n=89 www.bing.com
n=88 mozilla.com
n=87 bugzil
n=87 bugzill
n=86 bugzilla.moz
n=86 bugzilla.moz
n=86 bugzilla.mozill
n=86 bugzilla.mozill
n=85 b
n=85 bu
```

- check telephone_histogram.txt

```
TouristV@kali: ~/Desktop/bulk
File Actions Edit View Help

(TouristV@kali)-[~/Desktop/bulk]
$ cat telephone_histogram.txt
$
```

- check cnn_histogram.txt

```
TouristV@kali: ~/Desktop/bulk
File Actions Edit View Help

(TouristV@kali)-[~/Desktop/bulk]
└─$ cat telephone_histogram.txt

(TouristV@kali)-[~/Desktop/bulk]
└─$ cat ccn_histogram.txt
# BANNER FILE NOT PROVIDED (-b option)
# BULK_EXTRACTOR-Version: 2.0.0
# Feature-Recorder: ccn
# Filename: xendump.mem
# Histogram-File-Version: 1.1
n=8 4175004402616802
n=8 6304528221232788
n=7 345050204763535
n=7 4508694896602306
n=7 4716256679538152
n=7 4913718918519062
n=6 5445694786076283
n=5 371698391969633
n=5 377194390891444
n=5 4532919714822988
n=5 5121381208923133
n=5 5139198695527429
n=4 3532839978438283
n=4 3535414517392867
n=4 5516326606477060
n=4 6011752409192564
n=4 6011804703678895
n=2 4539884194397088
n=2 4929259042540320
n=2 4929441085660898
n=2 5460876803621668
n=1 4297967042257224

(TouristV@kali)-[~/Desktop/bulk]
└─$
```

- check wordlist

```
TouristV@kali: ~/Desktop/bulk
File Actions Edit View Help

(TouristV@kali)~/Desktop/bulk
$ cat wordlist.txt
# BANNER FILE NOT PROVIDED (-b option)
# BULK_EXTRACTOR-Version: 2.0.0
# Feature-Recorder: wordlist
# Filename: memdump.mem
# Feature-File-Version: 1.1
31071 TCPAu$
31095 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 fZfYfBfQfV
33503 fYfZfQfVf
34061 fRfQfRf
34191 f^fPfQf3
34412 fPfSfQf
34458 fYf[fX
34657 fSfRf+
34837 fYfYf3
34871 fPfVfXf^f;
34886 fVf@fPfH
34935 fYfYfYfY
34944 fYfYf3
35132 fYfZgf9
35208 fYfZf3
35789 fQfWfRf
35804 fZf_fY
```

```
TouristV@kali: ~/Desktop/bulk
File Actions Edit View Help

522196719-ZIP-2978 aGroup
522196719-ZIP-3206 _contentPrefSvc%
522196719-ZIP-3247 _context
522196719-ZIP-3548 _contentPrefSvc#
522196719-ZIP-3588 _context
522196719-ZIP-3889 _contentPrefSvc
522196719-ZIP-3908 getPrefs
522196719-ZIP-3920 _context
522196719-ZIP-4002 aGroup
522196719-ZIP-4219 _contentPrefSvc
522196719-ZIP-4238 getPrefsByName
522196719-ZIP-4256 _context
522196719-ZIP-4551 _contentPrefSvc
522196719-ZIP-4570 addObserver
522196719-ZIP-4668 aObserver
522196719-ZIP-4882 _contentPrefSvc
522196719-ZIP-4901 removeObserver
522196719-ZIP-5005 aObserver
522196719-ZIP-5054 grouper
522196719-ZIP-5183 _contentPrefSvc
522196719-ZIP-5202 grouper
522196719-ZIP-5261 DBConnection
522196719-ZIP-5395 _contentPrefSvc
522196719-ZIP-5414 DBConnection
522198103-ZIP-4 20180621064021
522198103-ZIP-1132 EXPORTED_SYMBOLS
522198103-ZIP-1152 Components
522198103-ZIP-1166 interfaces
522198103-ZIP-1180 classes
522198103-ZIP-1200 importK
522198103-ZIP-1345 CallbackCaller
522198103-ZIP-1363 prototype
522198103-ZIP-1376 handleResult
522198103-ZIP-1392 handleError!
522198103-ZIP-1407 handleComp

(TouristV@kali)~/Desktop/bulk
```

- check email

```
TouristV@kali: ~/Desktop/bulk
File Actions Edit View Help

(TouristV@kali)~/Desktop/bulk
$ cat email_histogram.txt
# BANNER FILE NOT PROVIDED (-b option)
# BULK_EXTRACTOR-Version: 2.0.0
# Feature-Recorder: email
# Filename: memdump.mem
# Histogram-File-Version: 1.1
n=38 firefox@getpocket.com (utf16=8)
n=33 hotfix-bug-1548973@mozilla.org (utf16=7)
n=32 aushelper@mozilla.org (utf16=6)
n=32 webcompat@mozilla.org (utf16=5)
n=30 e10srollout@mozilla.org (utf16=5)
n=19 mgoodwin@mozilla.com
n=18 wthayer@mozilla.com
n=9 dkeeler@mozilla.com
n=7 cps-requests@verisign.com
n=6 foxsec@mozilla.com
n=5 pki@sk.ee
n=4 anttoolbar@ant.com (utf16=3)
n=4 commonfix@mozillaonline.com
n=4 defaultfavicon@2x.pn (utf16=4)
n=4 eay@cryptsoft.com
n=4 firefox-hotfix@mozilla.org
n=4 flashlight@stephennolan.com.au
n=4 icons@2x.pn (utf16=4)
n=4 premium-server@thawte.com
n=4 proxyselector@mozilla.org
n=4 public.proartex@gmail.com
n=4 searchme@mybrowserbar.com
n=4 stealthyextension@gmail.com
n=4 support@lastpass.com (utf16=1)
n=4 support@todoist.com (utf16=3)
n=4 toolbar-inverted@2x.pn (utf16=4)
n=4 toolbar@2x.pn (utf16=4)
n=4 yslow@yahoo-inc.com (utf16=3)
n=3 12x3q@3244516.com (utf16=3)
n=3 1chtw@facebook.com (utf16=3)
```

- Analyze Image RAM with Volatility

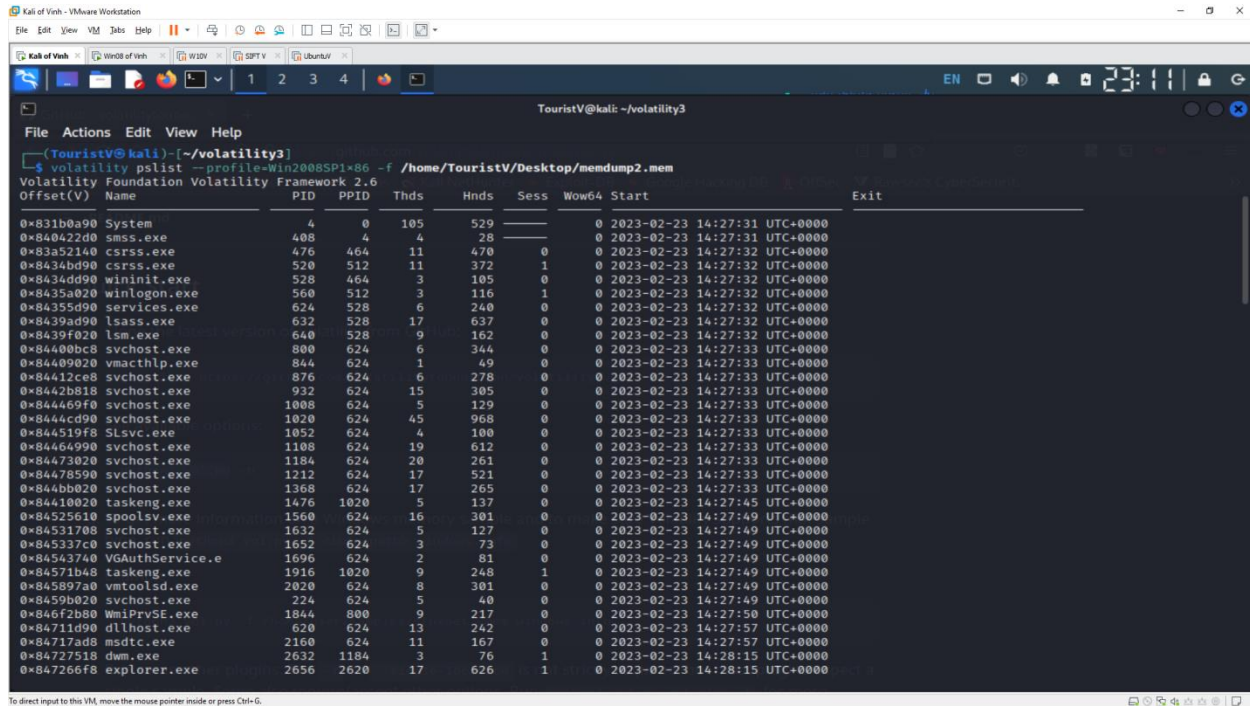
Command: volatility imageinfo -f /home/TouristV/Desktop/memdump2.mem

```
Kali of Vm - VMware Workstation
File Edit View VM Help
Kali of Vm x Win08 of Vm x W10V x SPT V x UbuntuV x
TouristV@kali: ~/volatility3
File Actions Edit View Help
(TouristV@kali)~/volatility3
$ volatility imageinfo -f /home/TouristV/Desktop/memdump2.mem
Volatility Foundation Volatility Framework 2.6
INFO : volatility.debug : Determining profile based on KDBG search...
Suggested Profile(s) : VistaSP1x86, Win2008SP1x86, Win2008SP2x86, VistaSP2x86
AS Layer1 : IA32PagedMemoryPae (kernel AS)
AS Layer2 : FileAddressSpace (/home/TouristV/Desktop/memdump2.mem)
PAE type : PAE
Quick Start
KDBG : 0x81b46c90L
Number of Processors : 1
Image Type (Service Pack) : 1
PCR for CPU 0 : 0x81b47800L
KUSER_SHARED_DATA : 0xffdf0000L
Image date and time : 2023-02-23 15:59:06 UTC+0000
Image local date and time : 2023-02-23 07:59:06 -0800

(TouristV@kali)~/volatility3
$ volatility pslist --profile=Win2008SP1x86 -f /home/TouristV/Desktop/memdump2.mem
Volatility Foundation Volatility Framework 2.6
Offset(V) Name PID PPID Thds Hnds Sess Wow64 Start Exit
0x831b0a90 System 4 0 105 529 0 0 2023-02-23 14:27:31 UTC+0000
0x840422d0 smss.exe 408 4 4 28 0 0 2023-02-23 14:27:31 UTC+0000
0x83a52140 csrss.exe 476 464 11 470 0 0 2023-02-23 14:27:32 UTC+0000
0x8434bd90 csrss.exe 520 512 11 372 1 0 2023-02-23 14:27:32 UTC+0000
0x8434dd90 wininit.exe 528 464 3 185 0 0 2023-02-23 14:27:32 UTC+0000
0x8435a020 winlogon.exe 560 512 3 116 1 0 2023-02-23 14:27:32 UTC+0000
0x8435d90 service2.exe 624 528 6 240 0 0 2023-02-23 14:27:32 UTC+0000
0x8439ad90 lsass.exe 632 528 17 637 0 0 2023-02-23 14:27:32 UTC+0000
0x8439f020 lsm.exe 640 528 9 162 0 0 2023-02-23 14:27:32 UTC+0000
0x84400bc8 svchost.exe 800 624 6 344 0 0 2023-02-23 14:27:33 UTC+0000
0x84409020 vmacthlp.exe 844 624 1 49 0 0 2023-02-23 14:27:33 UTC+0000
0x84412c88 svchost.exe 876 624 6 278 0 0 2023-02-23 14:27:33 UTC+0000
0x8442b018 svchost.exe 932 624 15 385 0 0 2023-02-23 14:27:33 UTC+0000
0x844469f0 svchost.exe 1008 624 5 129 0 0 2023-02-23 14:27:33 UTC+0000
0x8444cd90 svchost.exe 1020 624 45 968 0 0 2023-02-23 14:27:33 UTC+0000
```

- Running processes

Command: volatility pslist --profile=Win2008SP1x86 -f /home/TouristV/Desktop/memdump2.mem



Offset(V)	Name	PID	PPID	Thds	Hnds	Sess	Wow64	Start	Exit
0x831b0a90	System	4	0	105	529		0	2023-02-23 14:27:31 UTC+0000	
0x840422d0	smss.exe	408	4	4	28		0	2023-02-23 14:27:31 UTC+0000	
0x83a52140	csrss.exe	476	464	11	470	0	0	2023-02-23 14:27:32 UTC+0000	
0x8434bd90	csrss.exe	520	512	11	372	1	0	2023-02-23 14:27:32 UTC+0000	
0x8434dd90	wininit.exe	528	464	3	105	0	0	2023-02-23 14:27:32 UTC+0000	
0x8435a020	winlogon.exe	560	512	3	116	1	0	2023-02-23 14:27:32 UTC+0000	
0x84355d90	services.exe	624	528	6	240	0	0	2023-02-23 14:27:32 UTC+0000	
0x8439ad90	lsass.exe	632	528	17	637	0	0	2023-02-23 14:27:32 UTC+0000	
0x8439f020	lsm.exe	640	528	9	162	0	0	2023-02-23 14:27:32 UTC+0000	
0x84400bc8	svchost.exe	800	624	6	344	0	0	2023-02-23 14:27:33 UTC+0000	
0x84409020	vmacthlp.exe	844	624	1	49	0	0	2023-02-23 14:27:33 UTC+0000	
0x84412ce8	svchost.exe	876	624	6	278	0	0	2023-02-23 14:27:33 UTC+0000	
0x8442b818	svchost.exe	932	624	15	305	0	0	2023-02-23 14:27:33 UTC+0000	
0x844469f0	svchost.exe	1008	624	5	129	0	0	2023-02-23 14:27:33 UTC+0000	
0x8444cd90	svchost.exe	1020	624	45	968	0	0	2023-02-23 14:27:33 UTC+0000	
0x844519f8	SLsvc.exe	1052	624	4	100	0	0	2023-02-23 14:27:33 UTC+0000	
0x84464990	svchost.exe	1108	624	19	612	0	0	2023-02-23 14:27:33 UTC+0000	
0x84473020	svchost.exe	1184	624	20	261	0	0	2023-02-23 14:27:33 UTC+0000	
0x84478590	svchost.exe	1212	624	17	521	0	0	2023-02-23 14:27:33 UTC+0000	
0x844bb020	svchost.exe	1368	624	17	265	0	0	2023-02-23 14:27:33 UTC+0000	
0x84410020	taskeng.exe	1476	1020	5	137	0	0	2023-02-23 14:27:45 UTC+0000	
0x84525610	spoolsv.exe	1560	624	16	301	0	0	2023-02-23 14:27:49 UTC+0000	
0x84531708	svchost.exe	1632	624	5	127	0	0	2023-02-23 14:27:49 UTC+0000	
0x845337c0	svchost.exe	1652	624	3	73	0	0	2023-02-23 14:27:49 UTC+0000	
0x84543740	VGAuthService.exe	1696	624	2	81	0	0	2023-02-23 14:27:49 UTC+0000	
0x84571b48	taskeng.exe	1916	1020	9	248	1	0	2023-02-23 14:27:49 UTC+0000	
0x845897a0	vmtoolsd.exe	2020	624	8	381	0	0	2023-02-23 14:27:49 UTC+0000	
0x8459b020	svchost.exe	224	624	5	40	0	0	2023-02-23 14:27:49 UTC+0000	
0x846f2b80	WmiPrvSE.exe	1844	800	9	217	0	0	2023-02-23 14:27:50 UTC+0000	
0x84711d90	dllhost.exe	620	624	13	242	0	0	2023-02-23 14:27:57 UTC+0000	
0x84717ad8	msdtc.exe	2160	624	11	167	0	0	2023-02-23 14:27:57 UTC+0000	
0x84727518	dwm.exe	2632	1184	3	76	1	0	2023-02-23 14:28:15 UTC+0000	
0x847266f8	explorer.exe	2656	2620	17	626	1	0	2023-02-23 14:28:15 UTC+0000	

- Console Command:

Command: volatility consoles --profile=Win2008SP1x86 -f /home/TouristV/Desktop/memdump2.mem

```
0x9ba81388 ntdm.exe 3984 3072 2 98 1 0 2023-02-23 15:55:18 UTC+0000

(TouristV@kali) ~/volatility3
└─$ volatility --profile=Win2008SP1x86 --memory=file:///home/TouristV/Desktop/memdump2.mem ps
Volatility Foundation Volatility Framework 2.6
*****
ConsoleProcess: csrss.exe Pid: 476
Console: 0x1c4944 CommandHistorySize: 50
HistoryBufferCount: 1 HistoryBufferMax: 4
OriginalTitle: taskeng.exe
Title: -
*****
ConsoleProcess: csrss.exe Pid: 476
Console: 0x1c658c CommandHistorySize: 50
HistoryBufferCount: 1 HistoryBufferMax: 4
OriginalTitle: taskeng.exe
Title: -
*****
ConsoleProcess: csrss.exe Pid: 520
Console: 0x2d0da4 CommandHistorySize: 50
HistoryBufferCount: 3 HistoryBufferMax: 4
OriginalTitle: Administrator: C:\Windows\system32\cmd.exe
Title: -
AttachedProcess: cmd.exe Pid: 3072 Handle: 0x394
-----
CommandHistory: 0x2bf6440 Application: net.exe Flags:
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x0
-----
CommandHistory: 0x2bf6310 Application: net.exe Flags:
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x0
-----
CommandHistory: 0x2d37e8 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 5 LastAdded: 4 LastDisplayed: 4
FirstCommand: 0 CommandCountMax: 50

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Kali of Vinh - VMware Workstation
┌─$ volatility --profile=Win2008SP1x86 --memory=file:///home/TouristV/Desktop/memdump2.mem netuser
CommandCount: 5 LastAdded: 4 LastDisplayed: 4
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x394
Cmd #0 at 0x2bf6218: net user TouristV TouristVN /add
Cmd #1 at 0x2bf6558: net user Vinhh qwerty789@ /add
Cmd #2 at 0x2d1470: dir
Cmd #3 at 0x2bf62d8: user
Cmd #4 at 0x2bf62f0: net user

Screen 0x2d1510 X:100 Y:300
Dump:
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>net user TouristV TouristVN /add
The command completed successfully.

C:\Users\Administrator>net user Vinhh qwerty789@ /add
The command completed successfully.

C:\Users\Administrator>dir
Volume in drive C has no label.
Volume Serial Number is C6E7-CFDE

Directory of C:\Users\Administrator
06/27/2017 12:42 PM <DIR> .
06/27/2017 12:42 PM <DIR> ..
02/18/2023 12:04 AM 270 .jasmin
01/07/2023 01:41 AM <DIR> .zenmap
05/31/2013 06:34 PM <DIR> Contacts
02/23/2023 06:45 AM <DIR> Desktop
07/16/2017 11:07 AM <DIR> Documents
02/23/2023 07:14 AM <DIR> Downloads
05/31/2013 06:34 PM <DIR> Favorites
02/11/2023 07:25 AM <DIR> Links
```

- Services:

Command: volatility svcscan --profile=Win2008SP1x86 -f /home/TouristV/Desktop/memdump2.mem

```
TouristV@kali: ~/volatility3
(TouristV@kali)~/volatility3
$ volatility svcscan --profile=Win2008SP1x86 -f /home/TouristV/Desktop/memdump.2.mem
Volatility Foundation Volatility Framework 2.6
Offset: 0x1753640
Order: 190
Start: SERVICE_AUTO_START
Process ID: 1020
Service Name: ProfSvc
Display Name: User Profile Service
Service Type: SERVICE_WIN32_SHARE_PROCESS
Service State: SERVICE_RUNNING
Binary Path: C:\Windows\system32\svchost.exe -k netsvcs

Offset: 0x17535a0
Order: 189
Start: SERVICE_DISABLED
Process ID: -
Service Name: Processor
Display Name: Processor Driver
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x1755310
Order: 188
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: PptpMiniport
Display Name: WAN Miniport (PPTP)
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x1755268
Order: 187
Start: SERVICE_AUTO_START
Process ID: 1632
Service Name: PolicyAgent
```

- Registry Hives:

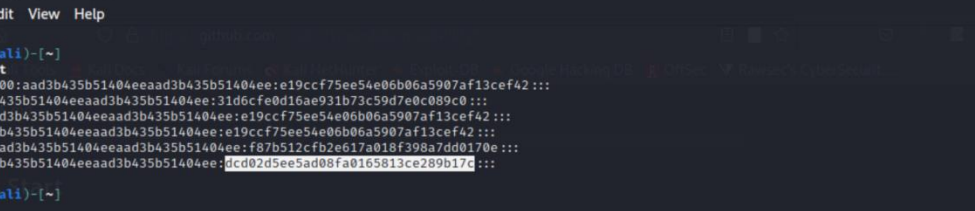
Command: volatility hivelist --profile=Win2008SP1x86 -f /home/TouristV/Desktop/memdump.2.mem

```
TouristV@kali: ~/volatility3
(TouristV@kali)~/volatility3
$ volatility -f /home/TouristV/Desktop/memdump.2.mem --profile=Win2008SP1x86 hivelist
Volatility Foundation Volatility Framework 2.6
Virtual      Physical      Name
-----
0x89c33450 0x1b33f450 \Device\HarddiskVolume1\Windows\System32\config\SAM
0x89c36008 0x1b40b008 \Device\HarddiskVolume1\Windows\System32\config\SECURITY
0x89c47008 0x1b2ec008 \Device\HarddiskVolume1\Windows\System32\config\COMPONENTS
0x89c47a20 0x1b2eca20 \Device\HarddiskVolume1\Windows\System32\config\SOFTWARE
0x89cd1a20 0x19735a20 \Device\HarddiskVolume1\Boot\BCD
0x9465f6a8 0x09ded6a8 \Device\HarddiskVolume1\Users\Administrator\NTUSER.DAT
0x946ae008 0x09fa5008 \Device\HarddiskVolume1\Users\Administrator\AppData\Local\Microsoft\Windows\UsrClass.dat
0x812eb008 0x158b46b0 \Device\HarddiskVolume1\Windows\ServiceProfiles\NetworkService\NTUSER.DAT
0x81321008 0x155be008 \Device\HarddiskVolume1\Windows\ServiceProfiles\LocalService\NTUSER.DAT
0x86211008 0x00aa6008 [no name]
0x86226008 0x00aaf008 \REGISTRY\MACHINE\SYSTEM
0x86248008 0x00a13008 \REGISTRY\MACHINE\HARDWARE
0x89c2f148 0x1b4b1148 \Device\HarddiskVolume1\Windows\System32\config\DEFAULT

(TouristV@kali)~/volatility3
```



```
Command: volatility hashdump --profile=Win2008SP1x86 -f
/home/TouristV/Desktop/memdump.mem -y 0x86226008 -s 0x89c33450 > pass.txt
```



The screenshot shows a Kali Linux terminal window with the prompt `TouristV@kali: ~`. The user has entered `cat pass.txt`, and the terminal displays the contents of the file, which consists of several lines of hex data. The output is as follows:

```

(TouristV@kali)~]$ cat pass.txt
Administrator:500:aad3b435b51404eeaad3b435b51404ee:e19ccf75ee54e06b06a5907af13cef42 :::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
student:1000:aad3b435b51404eeaad3b435b51404ee:e19ccf75ee54e06b06a5907af13cef42 :::
probe:1002:aad3b435b51404eeaad3b435b51404ee:e19ccf75ee54e06b06a5907af13cef42 :::
TouristV:1004:aad3b435b51404eeaad3b435b51404ee:f87b512cfb2e617a018f398a7dd0170e :::
Vinhh:1005:aad3b435b51404eeaad3b435b51404ee:dcd02d5ee5ad08fa0165813ce289b17c :::

```

- Crack password

