



kali@kali: ~/Desktop



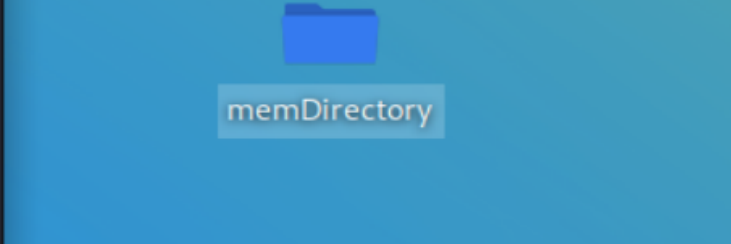
File Actions Edit View Help

```
(kali@kali) - [~/Desktop]  
$ ./Analyzer.sh mem memFile.mem
```

```
File Actions Edit View Help

(kali㉿ kali)-[~/Desktop]
$ ./Analyzer.sh mem memFile.mem
[+] Memory Directory created
[+] Analyzing Memory File
```

---





File Actions Edit View Help

└─\$ ./Analyzer.sh mem memFile.mem

[+] Memory Directory created

[+] Analyzing Memory File

---

Running Volatility imageinfo command

---

Volatility Foundation Volatility Framework 2.6

INFO : volatility.debug : Determining profile based on KDBG search...

memFile Operating System : VistaSP1x86

[+] Running Volatility Ps Scan & Ps Tree Commands

Volatility Foundation Volatility Framework 2.6

Volatility Foundation Volatility Framework 2.6

Volatility Done

Volatility LOG files created inside vol Directory

Data Statistics Saved in memDirectory

Printing Volatility Ps Scan & Ps Tree

Name	Pid	PPid	Thds	Hnds	Time
0x93d94a60:explorer.exe			2708	2672	21 524 2018-0
8-27 23:27:08 UTC+0000					
. 0x8122e508:vmtoolsd.exe			2816	2708	6 204 2018-0
8-27 23:27:09 UTC+0000					
. 0x93d978b8:FTK Imager.exe			3548	2708	8 267 2018-0
8-27 23:28:24 UTC+0000					
. 0x840b5d90:iexplore.exe			3028	2708	12 497 2018-0
8-27 23:27:22 UTC+0000					
. 0x8121dd90:vmx32to64.exe			2800	2708	1 64 2018-0
8-27 23:27:09 UTC+0000					
. 0x8122fd90:jusched.exe			2808	2708	1 49 2018-0
8-27 23:27:09 UTC+0000					
0x83b6bd90:csrss.exe			456	444	10 540 2018-0
8-27 23:26:47 UTC+0000					
0x83f4cd90:wininit.exe			508	444	5 105 2018-0
8-27 23:26:47 UTC+0000					
. 0x84012d90:services.exe			604	508	8 255 2018-0
8-27 23:26:47 UTC+0000					
.. 0x840d7a30:SLsvc.exe			1032	604	4 95 2018-0
8-27 23:26:48 UTC+0000					
.. 0x93d96020:dllhost.exe			2092	604	17 261 2018-0
8-27 23:26:51 UTC+0000					
.. 0x84085020:svchost.exe			780	604	8 307 2018-0
8-27 23:26:47 UTC+0000					
... 0x840dc838:WmiPrvSE.exe			2368	780	13 490 2018-0
8-27 23:26:52 UTC+0000					

## Printing Volatility Ps Scan &amp; Ps Tree

Offset(P)	Name	PID	PPID	PDB	Time created	Time exited
-----------	------	-----	------	-----	--------------	-------------

0x000000000007eb908	dllhost.exe	1764	604	0x0f0db4c0	2018-08-27 23:26:51 UTC+	0000
---------------------	-------------	------	-----	------------	--------------------------	------

0x00000000000a84020	TPAutoConnSvc.e	284	604	0x0f0db480	2018-08-27 23:26:51 UTC+	0000
---------------------	-----------------	-----	-----	------------	--------------------------	------

0x00000000000f1d020	dwm.exe	2684	1168	0x0f0db280	2018-08-27 23:27:08 UTC+	0000
---------------------	---------	------	------	------------	--------------------------	------

0x0000000000014add90	vmx32to64.exe	2800	2708	0x0f0db520	2018-08-27 23:27:09 UTC+	0000
----------------------	---------------	------	------	------------	--------------------------	------

0x000000000001cb0020	TPAutoConnSvc.e	284	604	0x0f0db480	2018-08-27 23:26:51 UTC+	0000
----------------------	-----------------	-----	-----	------------	--------------------------	------

0x000000000002910d90	vmx32to64.exe	2800	2708	0x0f0db520	2018-08-27 23:27:09 UTC+	0000
----------------------	---------------	------	------	------------	--------------------------	------

0x0000000000048af960	TPAutoConnect.e	2420	284	0x0f0db580	2018-08-27 23:26:52 UTC+	0000
----------------------	-----------------	------	-----	------------	--------------------------	------

0x0000000000049a0238	WmiApSrv.exe	2884	604	0x0f0db540	2018-08-27 23:27:11 UTC+	0000
----------------------	--------------	------	-----	------------	--------------------------	------

0x000000000004bc5758	VSSVC.exe	2532	604	0x0f0db5a0	2018-08-27 23:26:53 UTC+	0000
----------------------	-----------	------	-----	------------	--------------------------	------

0x000000000007c9e598	svchost.exe	3084	604	0x0f0db440	2018-08-27 23:27:22 UTC+	0000
----------------------	-------------	------	-----	------------	--------------------------	------

0x000000000009b958b8	FTK Imager.exe	3548	2708	0x0f0db380	2018-08-27 23:28:24 UTC+	0000
----------------------	----------------	------	------	------------	--------------------------	------



File Actions Edit View Help

```

8-27 23:26:50 UTC+0000
... 0x841dd8b8:taskeng.exe          1768  996  11  250 2018-0
8-27 23:26:50 UTC+0000
.. 0x840f79c0:svchost.exe          1168  604  12  240 2018-0
8-27 23:26:48 UTC+0000
... 0x93dc5020:dwm.exe             2684 1168   3   75 2018-0
8-27 23:27:08 UTC+0000
.. 0x841a3020:svchost.exe          1524  604   5  126 2018-0
8-27 23:26:50 UTC+0000
.. 0x93d8c908:dllhost.exe          1764  604  19  232 2018-0
8-27 23:26:51 UTC+0000
. 0x84016d90:lsass.exe             612   508  18  668 2018-0
8-27 23:26:47 UTC+0000
. 0x84018d90:lsm.exe              620   508  10  167 2018-0
8-27 23:26:47 UTC+0000
0x83008790:System                  4     0  102  509 2018-0
8-27 23:26:46 UTC+0000
. 0x83e1d2d0:smss.exe             388    4   4   28 2018-0
8-27 23:26:46 UTC+0000
0x83f56320:winlogon.exe           540   492   4  119 2018-0
8-27 23:26:47 UTC+0000
0x83f4ad90:csrss.exe              500   492   9  230 2018-0
8-27 23:26:47 UTC+0000

```

Strings.txt Created and located in mem Directory










Thank You

File Edit View Go Help

       kali Desktop

memDirectory

## Places

-  Computer
-  kali
-  Desktop
-  Trash
-  Documents
-  Music
-  Pictures
-  Videos
-  Downloads



vol



strings.txt



memFile.mem

