

# RAM FORENSICS

June 2024

Version 1

**(Done for Hashemite Univ. students Zinc 2)**

Eng.Ali Bani Bakar

# Inside Memory

- Network connections
- Processes -hidden
- Services – listening
- Malware
- Registry content
- DLL analysis
- Passwords in clear text

# Memory Acquisition



# Volatility

```
C:\Users\admin>volatility --info
Volatility Foundation Volatility Framework 2.6
```

## Profiles

```
-----
VistaSP0x64      - A Profile for Windows Vista SP0 x64
VistaSP0x86      - A Profile for Windows Vista SP0 x86
VistaSP1x64      - A Profile for Windows Vista SP1 x64
VistaSP1x86      - A Profile for Windows Vista SP1 x86
VistaSP2x64      - A Profile for Windows Vista SP2 x64
VistaSP2x86      - A Profile for Windows Vista SP2 x86
Win10x64         - A Profile for Windows 10 x64
Win10x64_10586    - A Profile for Windows 10 x64 (10.0.10586.306 / 2016-04-23)
Win10x64_14393    - A Profile for Windows 10 x64 (10.0.14393.0 / 2016-07-16)
Win10x86         - A Profile for Windows 10 x86
```

## Plugins

-----

amcache	- Print AmCache information
apihooks	- Detect API hooks in process and kernel memory
atoms	- Print session and window station atom tables
atomscan	- Pool scanner for atom tables
auditpol	- Prints out the Audit Policies from HKLM\SECURITY\Policy\PolA
tEv	
bigpools	- Dump the big page pools using BigPagePoolScanner
bioskbd	- Reads the keyboard buffer from Real Mode memory
cachedump	- Dumps cached domain hashes from memory
callbacks	- Print system-wide notification routines
clipboard	- Extract the contents of the windows clipboard
cmdline	- Display process command-line arguments
cmdscan	- Extract command history by scanning for _COMMAND_HISTORY
connections	- Print list of open connections [Windows XP and 2003 Only]
connscan	- Pool scanner for tcp connections
consoles	- Extract command history by scanning for _CONSOLE_INFORMATION
crashinfo	- Dump crash-dump information
deskscan	- Poolscanner for tagDESKTOP (desktops)

```
D:\Case 4>volatility -f ali_hu_ram.mem imageinfo
Volatility Foundation Volatility Framework 2.6
INFO      : volatility.debug      : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64_23418, Win2008R2SP1x64, Win7SP1x64_23418
                                AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
                                AS Layer2 : FileAddressSpace (D:\Case 4\ali_hu_ram.mem)
                                PAE type  : No PAE
                                DTB       : 0x187000L
                                KDBG      : 0xf80002a3d0a0L
          Number of Processors : 1
          Image Type (Service Pack) : 1
          KPCR for CPU 0       : 0xffffffff80002a3ed00L
          KUSER_SHARED_DATA    : 0xffffffff78000000000L
          Image date and time   : 2024-05-31 15:26:21 UTC+0000
          Image local date and time : 2024-05-31 18:26:21 +0300

D:\Case 4>
```

```
D:\Case 4>
D:\Case 4>volatility -f ali_hu_ram.mem --profile=Win7SP1x64 pslist
Volatility Foundation Volatility Framework 2.6
Offset(V)      Name      PID  PPID  Thds  Hnds  Sess  Wow64  Start
-----
0xffffffffa8018dc0040 System      4      0    78   517  -----  0 2024-05-31 14:09:41 UTC+0000
0xffffffffa8019345b30 smss.exe   236     4     2    29  -----  0 2024-05-31 14:09:41 UTC+0000
0xffffffffa8019f774c0 csrss.exe  304   296     9   344     0     0 2024-05-31 14:09:42 UTC+0000
0xffffffffa8018dc5060 wininit.exe 352   296     3    73     0     0 2024-05-31 14:09:42 UTC+0000
0xffffffffa8019f6ab30 csrss.exe  360   344     8   263     1     0 2024-05-31 14:09:42 UTC+0000
0xffffffffa8019f9b060 winlogon.exe 388   344     3   110     1     0 2024-05-31 14:09:42 UTC+0000
0xffffffffa8019f4eb30 services.exe 444   352     6   189     0     0 2024-05-31 14:09:42 UTC+0000
0xffffffffa8019ff4b30 lsass.exe  460   352     7   579     0     0 2024-05-31 14:09:42 UTC+0000
0xffffffffa8019ff3b30 lsm.exe    468   352    10   135     0     0 2024-05-31 14:09:42 UTC+0000
0xffffffffa801a076910 svchost.exe 556   444    10   351     0     0 2024-05-31 14:09:43 UTC+0000
0xffffffffa801a04ab30 svchost.exe 624   444     7   233     0     0 2024-05-31 14:09:43 UTC+0000
0xffffffffa801a106b30 svchost.exe 716   444    18   455     0     0 2024-05-31 14:09:43 UTC+0000
0xffffffffa801a141b30 svchost.exe 764   444    18   459     0     0 2024-05-31 14:09:43 UTC+0000
0xffffffffa801a162b30 svchost.exe 800   444    33   961     0     0 2024-05-31 14:09:43 UTC+0000
0xffffffffa801a200b30 svchost.exe 960   444    11   303     0     0 2024-05-31 14:09:43 UTC+0000
0xffffffffa801a244960 svchost.exe 268   444    12   449     0     0 2024-05-31 14:09:43 UTC+0000
0xffffffffa801a10b060 dwm.exe   1088   764     3     70     1     0 2024-05-31 14:09:44 UTC+0000
0xffffffffa801a12c060 explorer.exe 1112  1076    26   831     1     0 2024-05-31 14:09:44 UTC+0000
0xffffffffa801a19f340 spoolsv.exe 1148   444    12   259     0     0 2024-05-31 14:09:44 UTC+0000
0xffffffffa801a1db060 taskhost.exe 1160   444     7   144     1     0 2024-05-31 14:09:44 UTC+0000
0xffffffffa801a248060 svchost.exe 1208   444    17   303     0     0 2024-05-31 14:09:44 UTC+0000
0xffffffffa801a4b79c0 svchost.exe 1740   444     6     93     0     0 2024-05-31 14:09:45 UTC+0000
0xffffffffa801a4ccb30 svchost.exe 1772   444     5     96     0     0 2024-05-31 14:09:45 UTC+0000
0xffffffffa801a493220 SearchIndexer. 1284  444    13   633     0     0 2024-05-31 14:09:50 UTC+0000
0xffffffffa8018e3f4f0 svchost.exe  656   444     5     69     0     0 2024-05-31 14:11:45 UTC+0000
0xffffffffa8018e72060 sppsvc.exe 1516   444     4   144     0     0 2024-05-31 14:11:45 UTC+0000
0xffffffffa8018e85560 svchost.exe  640   444    12   318     0     0 2024-05-31 14:11:45 UTC+0000
0xffffffffa801a55a060 explorer.exe  648  1112     4   128     1     1 2024-05-31 14:28:02 UTC+0000
0xffffffffa8019615b30 FTK Imager.exe 1216  1112     6   324     1     0 2024-05-31 14:28:15 UTC+0000
0xffffffffa801a86fb30 audiodg.exe 2252   716     4   125     0     0 2024-05-31 15:20:39 UTC+0000
0xffffffffa801a86d150 svchost.exe 2492  1112     4    94     1     1 2024-05-31 15:24:34 UTC+0000
0xffffffffa801a6bf9a0 WUDFHost.exe 2432  764     8   196     0     0 2024-05-31 15:24:58 UTC+0000
0xffffffffa801a669670 FTK Imager.exe 2884  1112    17   359     1     0 2024-05-31 15:25:05 UTC+0000
```



```
D:\Case 4>volatility -f ali_hu_ram.mem --profile=Win7SP1x64 pslist |findstr "svchost.exe"
Volatility Foundation Volatility Framework 2.6
0xffffffffa801a076910 svchost.exe          556      444      10        351        0        0 2024-05-31 14:09:43 UTC+0000
0xffffffffa801a04ab30 svchost.exe          624      444        7        233        0        0 2024-05-31 14:09:43 UTC+0000
0xffffffffa801a106b30 svchost.exe          716      444      18        455        0        0 2024-05-31 14:09:43 UTC+0000
0xffffffffa801a141b30 svchost.exe          764      444      18        459        0        0 2024-05-31 14:09:43 UTC+0000
0xffffffffa801a162b30 svchost.exe          800      444      33        961        0        0 2024-05-31 14:09:43 UTC+0000
0xffffffffa801a200b30 svchost.exe          960      444      11        303        0        0 2024-05-31 14:09:43 UTC+0000
0xffffffffa801a244960 svchost.exe          268      444      12        449        0        0 2024-05-31 14:09:43 UTC+0000
0xffffffffa801a248060 svchost.exe         1208      444      17        303        0        0 2024-05-31 14:09:44 UTC+0000
0xffffffffa801a4b79c0 svchost.exe         1740      444        6         93        0        0 2024-05-31 14:09:45 UTC+0000
0xffffffffa801a4ccb30 svchost.exe         1772      444        5         96        0        0 2024-05-31 14:09:45 UTC+0000
0xffffffffa8018e3f4f0 svchost.exe          656      444        5         69        0        0 2024-05-31 14:11:45 UTC+0000
0xffffffffa8018e85560 svchost.exe          640      444      12        318        0        0 2024-05-31 14:11:45 UTC+0000
0xffffffffa801a86d150 svchost.exe         2492     1112        4         94        1        1 2024-05-31 15:24:34 UTC+0000
```

```
D:\Case 4>volatility -f ali_hu_ram.mem --profile=Win7SP1x64 pslist |findstr 1112
Volatility Foundation Volatility Framework 2.6
0xffffffffa801a12c060 explorer.exe          1112    1076     26      831      1      0 2024-05-31 14:09:44 UTC+0000
0xffffffffa801a55a060 explorer.exe           648    1112      4      128      1      1 2024-05-31 14:28:02 UTC+0000
0xffffffffa8019615b30 FTK Imager.exe       1216    1112      6      324      1      0 2024-05-31 14:28:15 UTC+0000
0xffffffffa801a86d150 svchost.exe          2492    1112      4       94      1      1 2024-05-31 15:24:34 UTC+0000
0xffffffffa801a669670 FTK Imager.exe       2884    1112     17     359      1      0 2024-05-31 15:25:05 UTC+0000
```

D:\Case 4>volatility -f ali\_hu\_ram.mem --profile=Win7SP1x64 pstree

Volatility Foundation Volatility Framework 2.6

Name	Pid	PPid	Thds	Hnds	Time		
-----	-----	-----	-----	-----	----		
0xffffffffa8019f774c0:csrss.exe	304	296	9	344	2024-05-31	14:09:42	UTC+0000
0xffffffffa8018dc5060:wininit.exe	352	296	3	73	2024-05-31	14:09:42	UTC+0000
. 0xffffffffa8019f4eb30:services.exe	444	352	6	189	2024-05-31	14:09:42	UTC+0000
.. 0xffffffffa8018e85560:svchost.exe	640	444	12	318	2024-05-31	14:11:45	UTC+0000
.. 0xffffffffa801a1db060:taskhost.exe	1160	444	7	144	2024-05-31	14:09:44	UTC+0000
.. 0xffffffffa801a4ccb30:svchost.exe	1772	444	5	96	2024-05-31	14:09:45	UTC+0000
.. 0xffffffffa801a244960:svchost.exe	268	444	12	449	2024-05-31	14:09:43	UTC+0000
.. 0xffffffffa8018e3f4f0:svchost.exe	656	444	5	69	2024-05-31	14:11:45	UTC+0000
.. 0xffffffffa801a106b30:svchost.exe	716	444	18	455	2024-05-31	14:09:43	UTC+0000
... 0xffffffffa801a86fb30:audiodg.exe	2252	716	4	125	2024-05-31	15:20:39	UTC+0000
.. 0xffffffffa801a162b30:svchost.exe	800	444	33	961	2024-05-31	14:09:43	UTC+0000
.. 0xffffffffa801a493220:SearchIndexer.	1284	444	13	633	2024-05-31	14:09:50	UTC+0000
.. 0xffffffffa801a076910:svchost.exe	556	444	10	351	2024-05-31	14:09:43	UTC+0000
.. 0xffffffffa801a248060:svchost.exe	1208	444	17	303	2024-05-31	14:09:44	UTC+0000
.. 0xffffffffa801a200b30:svchost.exe	960	444	11	303	2024-05-31	14:09:43	UTC+0000
.. 0xffffffffa801a4b79c0:svchost.exe	1740	444	6	93	2024-05-31	14:09:45	UTC+0000
.. 0xffffffffa8018e72060:sppsvc.exe	1516	444	4	144	2024-05-31	14:11:45	UTC+0000
.. 0xffffffffa801a19f340:spoolsv.exe	1148	444	12	259	2024-05-31	14:09:44	UTC+0000
.. 0xffffffffa801a04ab30:svchost.exe	624	444	7	233	2024-05-31	14:09:43	UTC+0000
.. 0xffffffffa801a141b30:svchost.exe	764	444	18	459	2024-05-31	14:09:43	UTC+0000
... 0xffffffffa801a10b060:dwm.exe	1088	764	3	70	2024-05-31	14:09:44	UTC+0000
... 0xffffffffa801a6bf9a0:WUDFHost.exe	2432	764	8	196	2024-05-31	15:24:58	UTC+0000
. 0xffffffffa8019ff4b30:lsass.exe	460	352	7	579	2024-05-31	14:09:42	UTC+0000
. 0xffffffffa8019ff3b30:lsm.exe	468	352	10	135	2024-05-31	14:09:42	UTC+0000
0xffffffffa8019f9b060:winlogon.exe	388	344	3	110	2024-05-31	14:09:42	UTC+0000
0xffffffffa8019f6ab30:csrss.exe	360	344	8	263	2024-05-31	14:09:42	UTC+0000
0xffffffffa8018dc0040:System	4	0	78	517	2024-05-31	14:09:41	UTC+0000
. 0xffffffffa8019345b30:smss.exe	236	4	2	29	2024-05-31	14:09:41	UTC+0000
0xffffffffa801a12c060:explorer.exe	1112	1076	26	831	2024-05-31	14:09:44	UTC+0000
. 0xffffffffa801a55a060:explorer.exe	648	1112	4	128	2024-05-31	14:28:02	UTC+0000
. 0xffffffffa801a669670:FTK Imager.exe	2884	1112	17	359	2024-05-31	15:25:05	UTC+0000
. 0xffffffffa801a86d150:svchost.exe	2492	1112	4	94	2024-05-31	15:24:34	UTC+0000
. 0xffffffffa8019615b30:FTK Imager.exe	1216	1112	6	324	2024-05-31	14:28:15	UTC+0000

```
D:\Case 4>volatility -f ali_hu_ram.mem --profile=Win7SP1x64 pstree
```

```
Volatility Foundation Volatility Framework 2.6
```

```
Command Prompt
```

```
D:\Case 4>
```

```
D:\Case 4>
```

```
D:\Case 4>volatility -f ali_hu_ram.mem --profile=Win7SP1x64 malfind
```

```
Volatility Foundation Volatility Framework 2.6
```

```
.Process: explorer.exe Pid: 1112 Address: 0x37e0000
```

```
.Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
```

```
.Flags: CommitCharge: 1, MemCommit: 1, PrivateMemory: 1, Protection: 6
```

```
.0x037e0000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
.0x037e0010 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
.0x037e0020 00 00 7e 03 00 00 00 00 00 00 00 00 00 00 00 00 ..~.....
.0x037e0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
.
```

```
.0x037e0000 0000 ADD [EAX], AL
```

```
.0x037e0002 0000 ADD [EAX], AL
```

```
.0x037e0004 0000 ADD [EAX], AL
```

```
.0x037e0006 0000 ADD [EAX], AL
```

```
.0x037e0008 0000 ADD [EAX], AL
```

```
.0x037e000a 0000 ADD [EAX], AL
```

```
.0x037e000c 0000 ADD [EAX], AL
```

```
.0x037e000e 0000 ADD [EAX], AL
```

```
.0x037e0010 0000 ADD [EAX], AL
```

```
.0x037e0012 0000 ADD [EAX], AL
```

```
.0x037e0014 0000 ADD [EAX], AL
```

```
.0x037e0016 0000 ADD [EAX], AL
```

```
.0x037e0018 0000 ADD [EAX], AL
```

```
.0x037e001a 0000 ADD [EAX], AL
```

```
.0x037e001c 0000 ADD [EAX], AL
```

```
.0x037e001e 0000 ADD [EAX], AL
```

```
.0x037e0020 0000 ADD [EAX], AL
```

```
.0x037e0022 7e03 JLE 0x37e0024 BAKAR 0778642376
```

```
.0x037e0024 0000 ADD [EAX], AL
```

Process: svchost.exe. Pid: 2492 Address: 0x20000  
Vad Tag: VadS Protection: PAGE\_EXECUTE\_READWRITE  
Flags: CommitCharge: 1, MemCommit: 1, PrivateMemory: 1, Protection: 6

```
0x00020000 fc e8 8f 00 00 00 60 89 e5 31 d2 64 8b 52 30 8b .....`...1.d.R0.  
0x00020010 52 0c 8b 52 14 8b 72 28 31 ff 0f b7 4a 26 31 c0 R..R..r(1...J&1.  
0x00020020 ac 3c 61 7c 02 2c 20 c1 cf 0d 01 c7 49 75 ef 52 .<a|.,.....Iu.R  
0x00020030 57 8b 52 10 8b 42 3c 01 d0 8b 40 78 85 c0 74 4c W.R..B<...@x..tL
```

```
0x00020000 fc          CLD  
0x00020001 e88f000000    CALL 0x20095  
0x00020006 60          PUSHA  
0x00020007 89e5        MOV EBP, ESP  
0x00020009 31d2        XOR EDX, EDX  
0x0002000b 648b5230    MOV EDX, [FS:EDX+0x30]  
0x0002000f 8b520c      MOV EDX, [EDX+0xc]  
0x00020012 8b5214      MOV EDX, [EDX+0x14]  
0x00020015 8b7228      MOV ESI, [EDX+0x28]  
0x00020018 31ff        XOR EDI, EDI  
0x0002001a 0fb74a26    MOVZX ECX, WORD [EDX+0x26]  
0x0002001e 31c0        XOR EAX, EAX  
0x00020020 ac          LODSB  
0x00020021 3c61        CMP AL, 0x61  
0x00020023 7c02        JL 0x20027  
0x00020025 2c20        SUB AL, 0x20  
0x00020027 c1cf0d      ROR EDI, 0xd  
0x0002002a 01c7        ADD EDI, EAX  
0x0002002c 49          DEC ECX  
0x0002002d 75ef        JNZ 0x2001e  
0x0002002f 52          PUSH EDX  
0x00020030 57          PUSH EDI  
0x00020031 8b5210      MOV EDX, [EDX+0x10]  
0x00020034 8b423c      MOV EAX, [EDX+0x3c]  
0x00020037 01d0        ADD EAX, EDX  
0x00020039 8b4078      MOV EAX, [EAX+0x78]  
0x0002003c 85c0        TEST EAX, EAX  
0x0002003e 744c        JZ 0x2008c
```

```
D:\Case 4>volatility -f ali_hu_ram.mem --profile=Win7SP1x64 -p 2492 procdump -D "d:\case 4"
Volatility Foundation Volatility Framework 2.6
Process(V)          ImageBase          Name          Result
-----
0xffffffffa801a86d150 0x0000000000040000 svchost.exe.   OK: executable.2492.exe
```



```
D:\Case 4>volatility -f ali_hu_ram.mem --profile=Win7SP1x64 -p 2492 dlllist
```

```
Volatility Foundation Volatility Framework 2.6
```

```
*****
```

```
svchost.exe. pid: 2492
```

```
Command line : "C:\Users\admin\Desktop\svchost.exe"
```

```
Note: use ldrmodules for listing DLLs in Wow64 processes
```

Base	Size	LoadCount	Path
0x000000000400000	0x16000	0xffff	C:\Users\admin\Desktop\svchost.exe
0x00000000777a0000	0x1a9000	0xffff	C:\Windows\SYSTEM32\ntdll.dll
0x0000000074910000	0x3f000	0x3	C:\Windows\SYSTEM32\wow64.dll
0x00000000748b0000	0x5c000	0x1	C:\Windows\SYSTEM32\wow64win.dll
0x00000000748a0000	0x8000	0x1	C:\Windows\SYSTEM32\wow64cpu.dll

```
D:\Case 4>volatility -f ali_hu_ram.mem --profile=Win7SP1x64 -p 800 dlllist
```

```
Volatility Foundation Volatility Framework 2.6
```

```
*****
```

```
svchost.exe pid: 800
```

```
Command line : C:\Windows\system32\svchost.exe -k netsvcs
```

```
Service Pack 1
```

Base	Size	LoadCount	Path
0x00000000ffcf0000	0xb000	0xffff	C:\Windows\system32\svchost.exe
0x00000000777a0000	0x1a9000	0xffff	C:\Windows\SYSTEM32\ntdll.dll
0x0000000077680000	0x11f000	0xffff	C:\Windows\system32\kernel32.dll
0x000007fefdd8e0000	0x6b000	0xffff	C:\Windows\system32\KERNELBASE.dll
0x000007fefddd0000	0x9f000	0xffff	C:\Windows\system32\msvcrt.dll
0x000007fefe180000	0x1f000	0xffff	C:\Windows\SYSTEM32\sechost.dll
0x000007feff4b0000	0x12d000	0xffff	C:\Windows\system32\RPCRT4.dll
0x000007feff670000	0x203000	0x61	C:\Windows\system32\ole32.dll
0x000007feffa40000	0x67000	0x1b6	C:\Windows\system32\GDI32.dll
0x0000000077580000	0xfa000	0x1e3	C:\Windows\system32\USER32.dll
0x000007feff5e0000	0xe000	0x62	C:\Windows\system32\LPK.dll
0x000007feff970000	0xc9000	0x62	C:\Windows\system32\USP10.dll
0x000007fefe510000	0x2e000	0x2	C:\Windows\system32\IMM32.DLL
0x000007fefe1a0000	0x109000	0x1	C:\Windows\system32\MSCTF.dll

```
D:\Case 4>volatility -f ali_hu_ram.mem --profile=Win7SP1x64 getsids |findstr "svchost.exe"
Volatility Foundation Volatility Framework 2.6
svchost.exe (556): S-1-5-18 (Local System)
svchost.exe (556): S-1-16-16384 (System Mandatory Level)
svchost.exe (556): S-1-1-0 (Everyone)
svchost.exe (556): S-1-5-32-545 (Users)
svchost.exe (556): S-1-5-6 (Service)
svchost.exe (556): S-1-5-11 (Authenticated Users)
svchost.exe (556): S-1-5-15 (This Organization)
svchost.exe (556): S-1-5-80-1601830629-990752416-3372939810-977361409-3075122917 (DcomLaunch)
svchost.exe (556): S-1-5-80-1981970923-922788642-3535304421-2999920573-318732269 (PlugPlay)
svchost.exe (556): S-1-5-80-2343416411-2961288913-598565901-392633850-2111459193 (Power)
svchost.exe (556): S-1-5-5-0-51113 (Logon Session)
svchost.exe (556): S-1-2-0 (Local (Users with the ability to log in locally))
svchost.exe (556): S-1-5-32-544 (Administrators)
svchost.exe (624): S-1-5-20 (NT Authority)
svchost.exe (624): S-1-16-16384 (System Mandatory Level)
svchost.exe (624): S-1-1-0 (Everyone)
svchost.exe (624): S-1-5-32-545 (Users)
svchost.exe (624): S-1-5-6 (Service)
svchost.exe (624): S-1-5-11 (Authenticated Users)
svchost.exe (624): S-1-5-15 (This Organization)
svchost.exe (624): S-1-5-80-521322694-906040134-3864710659-1525148216-3451224162 (RpcEptMapper)
svchost.exe (624): S-1-5-80-979556362-403687129-3954533659-2335141334-1547273080 (RpcSs)
svchost.exe (624): S-1-5-5-0-70770 (Logon Session)
svchost.exe (624): S-1-2-0 (Local (Users with the ability to log in locally))
svchost.exe (716): S-1-5-19 (NT Authority)
svchost.exe (716): S-1-16-16384 (System Mandatory Level)
svchost.exe (716): S-1-1-0 (Everyone)
```



D:\Case 4>volatility -f ali\_hu\_ram.mem --profile=Win7SP1x64 -p 640 privs

Volatility Foundation Volatility Framework 2.6

Pid	Process	Value	Privilege	Attributes	Description
640	svchost.exe	2	SeCreateTokenPrivilege		Create a token object
640	svchost.exe	3	SeAssignPrimaryTokenPrivilege	Present,Enabled	Replace a process-level token
640	svchost.exe	4	SeLockMemoryPrivilege	Default	Lock pages in memory
640	svchost.exe	5	SeIncreaseQuotaPrivilege	Present,Enabled	Increase quotas
640	svchost.exe	6	SeMachineAccountPrivilege		Add workstations to the domain
640	svchost.exe	7	SeTcbPrivilege	Default	Act as part of the operating system
640	svchost.exe	8	SeSecurityPrivilege	Present,Enabled	Manage auditing and security log
640	svchost.exe	9	SeTakeOwnershipPrivilege		Take ownership of files/objects
640	svchost.exe	10	SeLoadDriverPrivilege		Load and unload device drivers
640	svchost.exe	11	SeSystemProfilePrivilege	Default	Profile system performance
640	svchost.exe	12	SeSystemtimePrivilege		Change the system time
640	svchost.exe	13	SeProfileSingleProcessPrivilege	Default	Profile a single process
640	svchost.exe	14	SeIncreaseBasePriorityPrivilege	Default	Increase scheduling priority
640	svchost.exe	15	SeCreatePagefilePrivilege	Default	Create a pagefile
640	svchost.exe	16	SeCreatePermanentPrivilege	Default	Create permanent shared objects
640	svchost.exe	17	SeBackupPrivilege	Present,Enabled	Backup files and directories
640	svchost.exe	18	SeRestorePrivilege	Present,Enabled	Restore files and directories
640	svchost.exe	19	SeShutdownPrivilege	Present,Enabled	Shut down the system
640	svchost.exe	20	SeDebugPrivilege	Present,Enabled,Default	Debug programs
640	svchost.exe	21	SeAuditPrivilege	Default	Generate security audits
640	svchost.exe	22	SeSystemEnvironmentPrivilege		Edit firmware environment values
640	svchost.exe	23	SeChangeNotifyPrivilege	Present,Enabled,Default	Receive notifications of changes to files or directories
640	svchost.exe	24	SeRemoteShutdownPrivilege		Force shutdown from a remote system
640	svchost.exe	25	SeUndockPrivilege		Remove computer from docking station
640	svchost.exe	26	SeSyncAgentPrivilege		Synch directory service data
640	svchost.exe	27	SeEnableDelegationPrivilege		Enable user accounts to be trusted for delegation
640	svchost.exe	28	SeManageVolumePrivilege		Manage the files on a volume
640	svchost.exe	29	SeImpersonatePrivilege	Present,Enabled,Default	Impersonate a client after authentication
640	svchost.exe	30	SeCreateGlobalPrivilege	Default	Create global objects
640	svchost.exe	31	SeTrustedCredManAccessPrivilege		Access Credential Manager as a trusted caller
640	svchost.exe	32	SeRelabelPrivilege		Modify the mandatory integrity level of an object
640	svchost.exe	33	SeIncreaseWorkingSetPrivilege	Default	Allocate more memory for user applications
640	svchost.exe	34	SeTimeZonePrivilege	Default	Adjust the time zone of the computer's internal clock

D:\Case 4>volatility -f ali\_hu\_ram.mem --profile=Win7SP1x64 -p 2492 privs

Volatility Foundation Volatility Framework 2.6

Pid	Process	Value	Privilege	Attributes	Description
2492	svchost.exe.	2	SeCreateTokenPrivilege		Create a token object
2492	svchost.exe.	3	SeAssignPrimaryTokenPrivilege		Replace a process-level token
2492	svchost.exe.	4	SeLockMemoryPrivilege		Lock pages in memory
2492	svchost.exe.	5	SeIncreaseQuotaPrivilege		Increase quotas
2492	svchost.exe.	6	SeMachineAccountPrivilege		Add workstations to the domain
2492	svchost.exe.	7	SeTcbPrivilege		Act as part of the operating system
2492	svchost.exe.	8	SeSecurityPrivilege		Manage auditing and security log
2492	svchost.exe.	9	SeTakeOwnershipPrivilege		Take ownership of files/objects
2492	svchost.exe.	10	SeLoadDriverPrivilege		Load and unload device drivers
2492	svchost.exe.	11	SeSystemProfilePrivilege		Profile system performance
2492	svchost.exe.	12	SeSystemtimePrivilege		Change the system time
2492	svchost.exe.	13	SeProfileSingleProcessPrivilege		Profile a single process
2492	svchost.exe.	14	SeIncreaseBasePriorityPrivilege		Increase scheduling priority
2492	svchost.exe.	15	SeCreatePagefilePrivilege		Create a pagefile
2492	svchost.exe.	16	SeCreatePermanentPrivilege		Create permanent shared objects
2492	svchost.exe.	17	SeBackupPrivilege		Backup files and directories
2492	svchost.exe.	18	SeRestorePrivilege		Restore files and directories
2492	svchost.exe.	19	SeShutdownPrivilege	Present	Shut down the system
2492	svchost.exe.	20	SeDebugPrivilege		Debug programs
2492	svchost.exe.	21	SeAuditPrivilege		Generate security audits
2492	svchost.exe.	22	SeSystemEnvironmentPrivilege		Edit firmware environment values
2492	svchost.exe.	23	SeChangeNotifyPrivilege	Present,Enabled,Default	Receive notifications of changes to files or directories
2492	svchost.exe.	24	SeRemoteShutdownPrivilege		Force shutdown from a remote system
2492	svchost.exe.	25	SeUndockPrivilege	Present	Remove computer from docking station
2492	svchost.exe.	26	SeSyncAgentPrivilege		Synch directory service data
2492	svchost.exe.	27	SeEnableDelegationPrivilege		Enable user accounts to be trusted for delegation
2492	svchost.exe.	28	SeManageVolumePrivilege		Manage the files on a volume
2492	svchost.exe.	29	SeImpersonatePrivilege		Impersonate a client after authentication
2492	svchost.exe.	30	SeCreateGlobalPrivilege		Create global objects
2492	svchost.exe.	31	SeTrustedCredManAccessPrivilege		Access Credential Manager as a trusted caller
2492	svchost.exe.	32	SeRelabelPrivilege		Modify the mandatory integrity level of an object
2492	svchost.exe.	33	SeIncreaseWorkingSetPrivilege	Present	Allocate more memory for user applications
2492	svchost.exe.	34	SeTimeZonePrivilege	Present	Adjust the time zone of the computer's internal clock
2492	svchost.exe.	35	SeCreateSymbolicLinkPrivilege		Required to create a symbolic link

D:\Case 4>volatility -f ali\_hu\_ram.mem --profile=Win7SP1x64 netscan

# Volatility Foundation Volatility Framework 2.6

Offset(P)	Proto	Local Address	Foreign Address	State	Pid	Owner	Created
0x7e47bec0	UDPv4	0.0.0.0:5355	*:*		268	svchost.exe	2024-05-31 15:23:11 UTC+0000
0x7e47bec0	UDPv6	:::5355	*:*		268	svchost.exe	2024-05-31 15:23:11 UTC+0000
0x7e4b4cb0	UDPv4	0.0.0.0:68	*:*		716	svchost.exe	2024-05-31 15:19:45 UTC+0000
0x7e5e7240	UDPv6	fe80::bcc3:25de:a8fe:a21f:546	*:*		716	svchost.exe	2024-05-31 15:20:08 UTC+0000
0x7e701550	UDPv4	192.168.92.128:138	*:*		4	System	2024-05-31 14:23:15 UTC+0000
0x7e79c420	UDPv4	0.0.0.0:0	*:*		268	svchost.exe	2024-05-31 14:23:15 UTC+0000
0x7e79c420	UDPv6	:::0	*:*		268	svchost.exe	2024-05-31 14:23:15 UTC+0000
0x7e79d530	UDPv4	0.0.0.0:0	*:*		800	svchost.exe	2024-05-31 15:00:18 UTC+0000
0x7e79d530	UDPv6	:::0	*:*		800	svchost.exe	2024-05-31 15:00:18 UTC+0000
0x7e79e350	UDPv4	0.0.0.0:59558	*:*		4	System	2024-05-31 14:14:27 UTC+0000
0x7e804530	UDPv4	0.0.0.0:4500	*:*		800	svchost.exe	2024-05-31 14:09:44 UTC+0000
0x7e804530	UDPv6	:::4500	*:*		800	svchost.exe	2024-05-31 14:09:44 UTC+0000
0x7e982870	UDPv4	0.0.0.0:0	*:*		800	svchost.exe	2024-05-31 14:09:44 UTC+0000
0x7e982870	UDPv6	:::0	*:*		800	svchost.exe	2024-05-31 14:09:44 UTC+0000
0x7e9d5590	UDPv4	0.0.0.0:0	*:*		1772	svchost.exe	2024-05-31 14:09:46 UTC+0000
0x7eac8010	UDPv4	0.0.0.0:500	*:*		800	svchost.exe	2024-05-31 14:09:44 UTC+0000
0x7ead93a0	UDPv4	0.0.0.0:5355	*:*		268	svchost.exe	2024-05-31 15:23:11 UTC+0000
0x7eb0d2b0	UDPv4	0.0.0.0:4500	*:*		800	svchost.exe	2024-05-31 14:09:44 UTC+0000
0x7eb664c0	UDPv4	0.0.0.0:0	*:*		1772	svchost.exe	2024-05-31 14:09:46 UTC+0000
0x7eb664c0	UDPv6	:::0	*:*		1772	svchost.exe	2024-05-31 14:09:46 UTC+0000
0x7ebb0a90	UDPv4	192.168.92.128:137	*:*		4	System	2024-05-31 14:23:15 UTC+0000
0x7ebcb6f0	UDPv4	0.0.0.0:500	*:*		800	svchost.exe	2024-05-31 14:09:44 UTC+0000
0x7ebcb6f0	UDPv6	:::500	*:*		800	svchost.exe	2024-05-31 14:09:44 UTC+0000
0x7ebfc2e0	UDPv4	0.0.0.0:0	*:*		800	svchost.exe	2024-05-31 14:09:44 UTC+0000
0x7e686830	TCPv4	0.0.0.0:445	0.0.0.0:0	LISTENING	4	System	
0x7e686830	TCPv6	:::445	:::0	LISTENING	4	System	
0x7e697cd0	TCPv4	0.0.0.0:49155	0.0.0.0:0	LISTENING	444	services.exe	
0x7e78d2c0	TCPv4	0.0.0.0:49157	0.0.0.0:0	LISTENING	460	lsass.exe	
0x7e799490	TCPv4	192.168.92.128:139	0.0.0.0:0	LISTENING	4	System	
0x7e956ad0	TCPv4	0.0.0.0:49154	0.0.0.0:0	LISTENING	800	svchost.exe	
0x7e956ad0	TCPv6	:::49154	:::0	LISTENING	800	svchost.exe	
0x7eabba30	TCPv4	0.0.0.0:135	0.0.0.0:0	LISTENING	624	svchost.exe	
0x7eabf900	TCPv4	0.0.0.0:135	0.0.0.0:0	LISTENING	624	svchost.exe	
0x7eabf900	TCPv6	:::135	:::0	LISTENING	624	svchost.exe	
0x7eacd940	TCPv4	0.0.0.0:49152	0.0.0.0:0	LISTENING	352	wininit.exe	
0x7eacd940	TCPv6	:::49152	:::0	LISTENING	352	wininit.exe	
0x7eacdef0	TCPv4	0.0.0.0:49152	0.0.0.0:0	LISTENING	352	wininit.exe	
0x7ead6d20	TCPv4	0.0.0.0:49157	0.0.0.0:0	LISTENING	460	lsass.exe	
0x7ead6d20	TCPv6	:::49157	:::0	LISTENING	460	lsass.exe	
0x7eb11c60	TCPv4	0.0.0.0:49156	0.0.0.0:0	LISTENING	1772	svchost.exe	
0x7eb2eef0	TCPv4	0.0.0.0:49153	0.0.0.0:0	LISTENING	716	svchost.exe	
0x7eb3eb10	TCPv4	0.0.0.0:49153	0.0.0.0:0	LISTENING	716	svchost.exe	
0x7eb3eb10	TCPv6	:::49153	:::0	LISTENING	716	svchost.exe	
0x7eb55700	TCPv4	0.0.0.0:49154	0.0.0.0:0	LISTENING	800	svchost.exe	
0x7edbfd90	TCPv4	0.0.0.0:49156	0.0.0.0:0	LISTENING	1772	svchost.exe	
0x7edbfd90	TCPv6	:::49156	:::0	LISTENING	1772	svchost.exe	
0x7e4ac010	TCPv4	192.168.92.128:49163	192.168.92.130:4444	ESTABLISHED	2492	svchost.exe	
0x7e684ba0	TCPv6	-:0	38eb:f419:80fa:ffff:38eb:f419:80fa:ffff:0	CLOSED	2		??\$↓????
0x7eac4cf0	TCPv6	-:0	38ab:41a:80fa:ffff:38ab:41a:80fa:ffff:0	CLOSED	2		??\$↓????
0x7eb3ccf0	TCPv6	-:0	386b:101a:80fa:ffff:98dc:6819:80fa:ffff:0	CLOSED	2		??\$↓????
0x7eb8bcf0	TCPv4	192.168.92.128:49162	192.168.92.130:4444	SYN_SENT	648	explorer.exe	
0x7ed7f010	TCPv4	192.168.92.128:49159	192.168.92.130:4444	ESTABLISHED	648	explorer.exe	
0x7fc48400	UDPv4	0.0.0.0:68	ENG ALI BANI BAKAR 0778642376		716	svchost.exe	2024-05-31 14:59:08 UTC+0000

D:\Case 4>

```
D:\Case 4>volatility -f ali_hu_ram.mem --profile=Win7SP1x64 netscan |findstr 2492
Volatility Foundation Volatility Framework 2.6
0x7e4ac010      TCPv4      192.168.92.128:49163      192.168.92.130:4444  ESTABLISHED      2492      svchost.exe.

D:\Case 4>
```



```
D:\Case 4>volatility -f ali_hu_ram.mem --profile=Win7SP1x64 netscan |findstr TCPv4
```

```
Volatility Foundation Volatility Framework 2.6
```

0x7e67de60	TCPv4	0.0.0.0:49155	0.0.0.0:0	LISTENING	444	services.exe
0x7e686830	TCPv4	0.0.0.0:445	0.0.0.0:0	LISTENING	4	System
0x7e697cd0	TCPv4	0.0.0.0:49155	0.0.0.0:0	LISTENING	444	services.exe
0x7e78d2c0	TCPv4	0.0.0.0:49157	0.0.0.0:0	LISTENING	460	lsass.exe
0x7e799490	TCPv4	192.168.92.128:139	0.0.0.0:0	LISTENING	4	System
0x7e956ad0	TCPv4	0.0.0.0:49154	0.0.0.0:0	LISTENING	800	svchost.exe
0x7eabba30	TCPv4	0.0.0.0:135	0.0.0.0:0	LISTENING	624	svchost.exe
0x7eabf900	TCPv4	0.0.0.0:135	0.0.0.0:0	LISTENING	624	svchost.exe
0x7eacd940	TCPv4	0.0.0.0:49152	0.0.0.0:0	LISTENING	352	wininit.exe
0x7eacdef0	TCPv4	0.0.0.0:49152	0.0.0.0:0	LISTENING	352	wininit.exe
0x7ead6d20	TCPv4	0.0.0.0:49157	0.0.0.0:0	LISTENING	460	lsass.exe
0x7eb11c60	TCPv4	0.0.0.0:49156	0.0.0.0:0	LISTENING	1772	svchost.exe
0x7eb2eef0	TCPv4	0.0.0.0:49153	0.0.0.0:0	LISTENING	716	svchost.exe
0x7eb3eb10	TCPv4	0.0.0.0:49153	0.0.0.0:0	LISTENING	716	svchost.exe
0x7eb55700	TCPv4	0.0.0.0:49154	0.0.0.0:0	LISTENING	800	svchost.exe
0x7edbffd90	TCPv4	0.0.0.0:49156	0.0.0.0:0	LISTENING	1772	svchost.exe
0x7e4ac010	TCPv4	192.168.92.128:49163	192.168.92.130:4444	ESTABLISHED	2492	svchost.exe
0x7eb8bcf0	TCPv4	192.168.92.128:49162	192.168.92.130:4444	SYN_SENT	648	explorer.exe
0x7ed7f010	TCPv4	192.168.92.128:49159	192.168.92.130:4444	ESTABLISHED	648	explorer.exe

```
D:\Case 4>
```

```
D:\Case 4>volatility -f ali_hu_ram.mem --profile=Win7SP1x64 hashdump
Volatility Foundation Volatility Framework 2.6
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
admin:1000:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

D:\Case 4>■
```

```
D:\Case 4>volatility -f ali_hu_ram.mem --profile=Win7SP1x64 cmdscan  
Volatility Foundation Volatility Framework 2.6
```

```
D:\Case 4>■
```

```
D:\Case 4>volatility -f ali_hu_ram.mem --profile=Win7SP1x64 consoles  
Volatility Foundation Volatility Framework 2.6
```

```
D:\Case 4>
```

```
D:\Case 4>volatility -f ali_hu_ram.mem --profile=Win7SP1x64 iehistory
Volatility Foundation Volatility Framework 2.6

D:\Case 4>
```





🔍 URL, IP address, domain or file hash



Sign in

Sign up

We have changed our Privacy Notice and Terms of Use, effective July 18, 2024. You can view the updated [Privacy Notice](#) and [Terms of Use](#).

Accept terms of use



Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.

FILE

URL

SEARCH



Choose file



📁 File/URL

📁 File Collection

🔍 Report Search

📄 YARA Search

📄 String Search

This is a free malware analysis service for the community that detects and analyzes unknown threats using a unique **Hybrid Analysis** technology.



Drag & Drop For Instant Analysis

or

http://www.example.com/suspicious.zip



Analyze

Maximum upload size is 100 MB.

Powered by **CrowdStrike Falcon**® **Sandbox**.

ENG. ALI BANI BAKAR 0778642376

## Releases & Updates

Hybrid Analysis Partners with Bfore.Ai, Integrates AI-Powered URL and Domain Analysis

August 3, 2023

New 'AMSI' Tab at the Process Modal

April 11, 2023

[See More!](#)

## Latest News

HijackLoader Expands Techniques to Improve Defense Evasion

Donato Onofri - Emanuele Calvelli - February 7, 2024

IMPERIAL KITTEN Deploys Novel Malware Families in Middle East-Focused Operations

Counter Adversary Operations - November 9, 2023