



LAB 4: OBSESSION

▼ General Info

- **Challenge Name:** Obsession: Shadows of the Deleted
- **Memory Dump File Name:** MemLabs-Lab4.7z
- **Source / URL:** https://github.com/stuxnet999/MemLabs/tree/master/Lab_4
- **Date Started:** Wednesday July 30, 2025
- **Date Completed:** N/A
- **System Profile (from windows.info):** Windows 7 SP1 x64
- **Volatility Version Used:** Volatility 3 Framework - 2.26.0
- **Duration:** N/A
- **Challenge Description:**

"My system was recently compromised. The Hacker stole a lot of information but he also deleted a very important file of mine. I have no idea on how to recover it. The only evidence we have, at this point of time is this memory dump. Please help me."

- **Note:** This challenge is composed of only 1 flag.
- The flag format for this lab is: `inctf{some_133t_Str1ng}`

▼ 🔎 Objective

Clearly describe the goal of the challenge.

Example: “Find a deleted file named Important.txt that contains the flag.”

Lab 4 “Obsession” tests the analyst’s willingness to go beyond default outputs. It’s not about running a plugin — it’s about interpreting memory like a puzzle, obsessing over fragments of deleted data, and pushing every forensic tool to the limit. If you’re not ready to dig deep, you won’t find the truth.

▼ Tools & Setup

Tool	Version/Details
Volatility	Volatility 3 [2.26.0]
OS	Kali Linux
Other Tools	Strings grep exiftool stehide

```
(jynx㉿kali)-[~/Desktop/forensics/July30]
└─$ vol -f MemoryDump_Lab4.raw windows.info
Volatility 3 Framework 2.26.0
Progress: 100.00          PDB scanning finished
Variable      Value

Kernel Base    0xf80002605000
DTB     0x187000
Symbols file:///home/jynx/.local/lib/python3.13/site-packages/volatility3/symbols/windows_ntkrnlmp.pdb/3844DDB920174
967BE7AA4A2C20430FA-2.json.xz
Is64Bit True
IsPAE  False
layer_name    0 WindowsIntel32e
memory_layer   1 FileLayer
KdDebuggerDataBlock 0xf800027f60a0
NTBuildLab    7601.17514.amd64fre.win7sp1_rtm.
CSDBuild      1
KdVersionBlock 0xf800027f6068
Major/Minor    15.7601
MachineType   34404
KeNumberProcessors 1
SystemTime    2019-06-29 07:30:00+00:00
NtSystemRoot  C:\Windows
NTProductType NtProductWinNt
NTMajorVersion 6
NTMinorVersion 1
PE MajorOperatingSystemVersion 6
PE MinorOperatingSystemVersion 1
PE Machine    34404
PE TimeDateStamp Sat Nov 20 09:30:02 2010

(jynx㉿kali)-[~/Desktop/forensics/July30]
└─$ vol
Volatility 3 Framework 2.26.0
usage: vol [-h] [-c CONFIG] [--parallelism [{processes,threads,off}]] [-e EXTEND] [-p PLUGIN_DIRS]
           [-s SYMBOL_DIRS] [-v] [-l LOG] [-o OUTPUT_DIR] [-q] [-r RENDERER] [-f FILE] [--write-config]
           [--save-config SAVE_CONFIG] [--clear-cache] [--cache-path CACHE_PATH] [--offline | -u URL]
           [--filters FILTERS] [--hide-columns [HIDE_COLUMNS ...]] [--single-location SINGLE_LOCATION]
           [--stackers [STACKERS ...]] [--single-swap-locations [SINGLE_SWAP_LOCATIONS ...]]
           PLUGIN ...
vol: error: Please select a plugin to run (see 'vol --help' for options
```

▼ Phase 1: Image Info + Process Mapping

▼ 1. **pslist**

→ The **pslist** plugin is one of the **most fundamental commands in memory forensics** using Volatility.

pslist enumerates **active processes** by scanning the **EPROCESS** structures in the memory dump. It's a way of peeking into the **process list the OS kept in memory when the snapshot was taken**.

Command

```
vol -f MemoryDump_Lab4.raw windows.pslist
```

▼ Findings

▼ 1. High COUNT of Threads on **svchost.exe** [PID - 864]

[jynx@kali] - [~/Desktop/forensics/July30]														
\$ vol -f MemoryDump_Lab4.raw windows.pslist	Volatility 3 Framework 2.26.0													
Progress: 100.00 PDB scanning finished														
PID	PPID	ImageFileName	Offset(V)	Threads	Handles	SessionId	Wow64	CreateTime	ExitTime	File output				
4	0	System	0xfa8000ca0040	79	509	N/A	False	2019-06-29 07:28:07.000000 UTC	N/A	Disabled				
256	4	smss.exe	0xfa80014af950	3	32	N/A	False	2019-06-29 07:28:07.000000 UTC	N/A	Disabled				
328	320	csrss.exe	0xfa8001c57b30	11	385	0	False	2019-06-29 07:28:14.000000 UTC	N/A	Disabled				
376	368	cssrss.exe	0xfa8001c8960	7	200	1	False	2019-06-29 07:28:15.000000 UTC	N/A	Disabled				
384	320	wininit.exe	0xfa8001c6f760	3	75	0	False	2019-06-29 07:28:15.000000 UTC	N/A	Disabled				
412	368	winlogon.exe	0xfa8001c751f0	6	119	1	False	2019-06-29 07:28:15.000000 UTC	N/A	Disabled				
472	384	services.exe	0xfa8001bc1b30	13	193	0	False	2019-06-29 07:28:17.000000 UTC	N/A	Disabled				
480	384	lsass.exe	0xfa8001cb5940	8	582	0	False	2019-06-29 07:28:17.000000 UTC	N/A	Disabled				
488	384	lsm.exe	0xfa8001cc1b30	12	187	0	False	2019-06-29 07:28:17.000000 UTC	N/A	Disabled				
580	472	svchost.exe	0xfa8001d02b30	11	358	0	False	2019-06-29 07:28:21.000000 UTC	N/A	Disabled				
640	472	VBoxService.exe	0xfa8001d30b30	14	137	0	False	2019-06-29 07:28:21.000000 UTC	N/A	Disabled				
708	472	svchost.exe	0xfa8001d43a70	7	260	0	False	2019-06-29 07:28:22.000000 UTC	N/A	Disabled				
804	472	svchost.exe	0xfa8001d4c3b30	19	393	0	False	2019-06-29 07:28:23.000000 UTC	N/A	Disabled				
840	472	svchost.exe	0xfa8001db9b30	21	431	0	False	2019-06-29 07:28:24.000000 UTC	N/A	Disabled				
864	472	svchost.exe	0xfa8001dc6850	37	917	0	False	2019-06-29 07:28:24.000000 UTC	N/A	Disabled				
952	804	audiogd.exe	0xfa8001df1060	7	131	0	False	2019-06-29 07:28:26.000000 UTC	N/A	Disabled				
220	472	svchost.exe	0xfa8001e1b890	16	323	0	False	2019-06-29 07:28:27.000000 UTC	N/A	Disabled				
484	472	svchost.exe	0xfa8001e45630	18	376	0	False	2019-06-29 07:28:29.000000 UTC	N/A	Disabled				
1132	472	spoolsv.exe	0xfa8001eaab30	15	286	0	False	2019-06-29 07:28:32.000000 UTC	N/A	Disabled				
1176	472	svchost.exe	0xfa8001ed7b30	21	307	0	False	2019-06-29 07:28:33.000000 UTC	N/A	Disabled				
1276	472	svchost.exe	0xfa8001f452e0	14	220	0	False	2019-06-29 07:28:34.000000 UTC	N/A	Disabled				
1804	472	taskhost.exe	0xfa8001f81b30	10	161	1	False	2019-06-29 07:28:42.000000 UTC	N/A	Disabled				

- A typical `svchost.exe` instance runs **10–150 threads**, depending on the services it hosts.
- Having **900+ threads** in a single instance is not only unusual but likely points to:
 - **Malware injection**
 - **Process hollowing**
 - **Thread spraying** (evasion tactic)
 - **Rootkit or persistence technique**
 - Possibly a **memory exhaustion DoS vector**

▼ 2. Extremely Low `dwm.exe` handles

[jynx@kali] - [~/Desktop/forensics/July30]														
\$ vol -f MemoryDump_Lab4.raw windows.pslist grep dwm	Volatility 3 Framework 2.26.0													
1908	840	dwm.exe	0xfa80020bbb30	5	77	1	False	2019-06-29 07:28:43.000000 UTC	N/A	Disabled				
3000	840	dwm.exe	0xfa8000e62b30	5	76	2	False	2019-06-29 07:29:36.000000 UTC	N/A	Disabled				

- Normally, `dwm.exe` [Desktop Windows Manager] spawns **once**, and holds **several hundred handles** and dozens of threads.
- We have **two instances, both with only 1 and 2 handles respectively**, and very low thread counts:
 - PID `1908` : 77 threads
 - PID `3000` : 76 threads

This is **highly atypical**, especially since they're spawned under the same parent (PID 840 `svchost.exe`) — even more suspicious because `svchost` is already a candidate for malware injection.

SUSPICIOUS because;

1. **TWO dwm.exe processes** (should only be one!)
2. **Handle counts too low** (76-77 vs expected 200-800+)
3. **Different sessions** (1 and 2)

This Suggests:

- **Process hollowing** (legitimate process replaced with malware)
- **Process impersonation** (malware pretending to be dwm.exe)
- **Possible rootkit activity**

This is **highly atypical**, especially since they're spawned under the same parent (PID 840 `svchost.exe`) — even more suspicious because `svchost` is already a candidate for malware injection.

▼ 2. malfind

→ Volatility plugin that detects signs of code injection and malware in process memory by looking for suspicious memory regions with executable code.

What it finds:

- Injected code in processes
- Shellcode and malware
- Executable memory regions that seem suspicious etc.

Command:

```
vol -f MemoryDump_Lab4.raw windows.malfind
```

▼ Findings:

TEXTBOOK case of **malware injection** and **process hollowing**

1944	explorer.exe	0x3e00000	0x3e0ffff	VadS	PAGE_EXECUTE_READWRITE	16	1	Disabled	N/A
41 ba 80 00 00 00 48 b8 38 a1 93 fe fe 07 00 00 A....H.8.....									
48 ff 20 90 41 ba 81 00 00 00 48 b8 38 a1 93 fe H. .A....H.8...									
fe 07 00 00 48 ff 20 90 41 ba 82 00 00 00 48 b8H. .A....H.									
38 a1 93 fe 07 00 00 48 ff 20 90 41 ba 83 00 8.....H. .A...									
0x3e00000:	mov	r10d, 0x80							
0x3e00006:	movabs	rax, 0x7fefe93a138							
0x3e00010:	jmp	qword ptr [rax]							
0x3e00013:	nop								
0x3e00014:	mov	r10d, 0x81							
0x3e0001a:	movabs	rax, 0x7fefe93a138							
0x3e00024:	jmp	qword ptr [rax]							
0x3e00027:	nop								
0x3e00028:	mov	r10d, 0x82							
0x3e0002e:	movabs	rax, 0x7fefe93a138							
0x3e00038:	jmp	qword ptr [rax]							
0x3e0003b:	nop								

2076	dllhost.exe	0x220000	0x22ffff	VadS	PAGE_EXECUTE_READWRITE	16	1	Disabled	N/A
41 ba 80 00 00 00 48 b8 38 a1 93 fe fe 07 00 00 A....H.8.....									
48 ff 20 90 41 ba 81 00 00 00 48 b8 38 a1 93 fe H. .A....H.8...									
fe 07 00 00 48 ff 20 90 41 ba 82 00 00 00 48 b8H. .A....H.									
38 a1 93 fe 07 00 00 48 ff 20 90 41 ba 83 00 8.....H. .A...									
0x220000:	mov	r10d, 0x80							
0x220006:	movabs	rax, 0x7fefe93a138							
0x220010:	jmp	qword ptr [rax]							
0x220013:	nop								
0x220014:	mov	r10d, 0x81							
0x22001a:	movabs	rax, 0x7fefe93a138							
0x220024:	jmp	qword ptr [rax]							
0x220027:	nop								
0x220028:	mov	r10d, 0x82							
0x22002e:	movabs	rax, 0x7fefe93a138							
0x220038:	jmp	qword ptr [rax]							
0x22003b:	nop								

3012	explorer.exe	0x4000000	0x400ffff	VadS	PAGE_EXECUTE_READWRITE	16	1	Disabled	N/A
41 ba 80 00 00 00 48 b8 38 a1 93 fe fe 07 00 00 A....H.8.....									
48 ff 20 90 41 ba 81 00 00 48 b8 38 a1 93 fe H. .A....H.8...									
fe 07 00 00 48 ff 20 90 41 ba 82 00 00 00 48 b8H. .A....H.									
38 a1 93 fe 07 00 00 48 ff 20 90 41 ba 83 00 8.....H. .A...									
0x400000:	mov	r10d, 0x80							
0x400006:	movabs	rax, 0x7fefe93a138							
0x400010:	jmp	qword ptr [rax]							
0x400013:	nop								
0x400014:	mov	r10d, 0x81							
0x40001a:	movabs	rax, 0x7fefe93a138							
0x400024:	jmp	qword ptr [rax]							
0x400027:	nop								
0x400028:	mov	r10d, 0x82							
0x40002e:	movabs	rax, 0x7fefe93a138							
0x400038:	jmp	qword ptr [rax]							
0x40003b:	nop								

All three processes have the **EXACT SAME** malicious code:
assembly

```
mov r10d, 0x80/0x81/0x82 ← System call numbers
movabs rax, 0x7fefe93a138 ← SAME address in all processes
jmp qword ptr [rax]      ← Jump to malicious code
nop                      ← Padding
```

Classic Injection Indicators:

- **PAGE_EXECUTE_READWRITE** permissions (HUGE red flag!)
- **VadS** (Private memory allocation)
- **Same hex pattern:** 41 ba 80 00 00 00 48 b8 38 a1 93 fe fe 07 00 00

Targeted Processes:

- **explorer.exe** (PID 1944, 3012) - Windows Shell

- `dllhost.exe` (PID 2076) - COM + surrogate

What the attacker probably did:

Step 1: Process Hollowing

- Injected malicious code into **legitimate processes**
- Replaced original code with **shellcode stubs**

Step 2: System Call Hooking

- `mov r10d, 0x80/0x81/0x82` → **System call numbers**
- `0x7fefef93a138` → **Shared malicious handler address**
- **Intercepts system calls** to hide activity

Step 3: Persistence

- Multiple processes → **redundancy**
- If one is killed, others continue

▼ 3. cmdline

Extracts and displays the command line arguments that were used to start each process, and exactly how each program was launched with what parameters and switches.

Command

```
vol -f MemoryDump_Lab4.raw windows.cmdline
```

▼ Findings

```
(jynx㉿kali)-[~/Desktop/forensics/July30]
$ vol -f MemoryDump_Lab4.raw windows.cmdline
Volatility 3 Framework 2.26.0
Progress: 100.00          PDB scanning finished
PID      Process Args
4        System -
256     smss.exe    \SystemRoot\System32\smss.exe
328     csrss.exe   %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,7
DllInitialization,2 ServerDll=sxssrv,4 ProfileControl=Off MaxRequestThreads=16
376     csrss.exe   %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,7
DllInitialization,2 ServerDll=sxssrv,4 ProfileControl=Off MaxRequestThreads=16
384     wininit.exe  wininit.exe
412     winlogon.exe winlogon.exe
472     services.exe C:\Windows\system32\services.exe
480     lsass.exe    C:\Windows\system32\lsass.exe
488     lsm.exe C:\Windows\system32\lsm.exe
580     svchost.exe  C:\Windows\system32\svchost.exe -k DcomLaunch
640     VBoxService.exe C:\Windows\System32\VBoxService.exe
708     svchost.exe  C:\Windows\System32\svchost.exe -k RPCSS
804     svchost.exe  C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted
840     svchost.exe  C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted
864     svchost.exe  C:\Windows\System32\svchost.exe -k netsvcs
952     audiogd.exe  C:\Windows\System32\AUDIODEG.EXE 0x2ac
220     svchost.exe  C:\Windows\System32\svchost.exe -k LocalService
484     svchost.exe  C:\Windows\System32\svchost.exe -k NetworkService
1132    spoolsv.exe C:\Windows\System32\spoolsv.exe
1176    svchost.exe  C:\Windows\System32\svchost.exe -k LocalServiceNoNetwork
1276    svchost.exe  C:\Windows\System32\svchost.exe -k LocalServiceAndNoImpersonation
1804    taskhost.exe "taskhost.exe"
1824    taskeng.exe  taskeng.exe {243F5DED-C140-47D9-B005-B07948B2A976}
1908    dwm.exe "C:\Windows\System32\Dwm.exe"
1944    explorer.exe  C:\Windows\Explorer.EXE
1592    VBoxTray.exe C:\Windows\System32\VBoxTray.exe"
1068    SearchIndexer C:\Windows\System32\SearchIndexer.exe /Embedding
1696    SearchProtocol "C:\Windows\System32\SearchProtocolHost.exe" Global\UsGthrFltPipeMssGthrPipe_S-1-5-
7483646 "Software\Microsoft\Windows Search" Mozilla/4.0 (compatible; MSIE 6.0; Windows NT; MS Search 4.0 R
1688    SearchFilterHo "C:\Windows\System32\SearchFilterHost.exe" 0 516 520 528 65536 524
2076    dllhost.exe  C:\Windows\System32\DllHost.exe /ProcessId:{76D0CB12-7604-4048-B83C-1005C7DDC503}
2272    GoogleCrashHan "C:\Program Files (x86)\Google\Update\1.3.34.11\GoogleCrashHandler.exe"
2284    GoogleCrashHan "C:\Program Files (x86)\Google\Update\1.3.34.11\GoogleCrashHandler64.exe"
2624    DumpIt.exe   "C:\Users\eminem\Desktop\DumpIt\DumpIt.exe"
2636    conhost.exe  \?\C:\Windows\System32\conhost.exe
2700    csrss.exe   %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,7
DllInitialization,2 ServerDll=sxssrv,4 ProfileControl=Off MaxRequestThreads=16
2728    winlogon.exe winlogon.exe
2976    taskhost.exe "taskhost.exe"
3000    dwm.exe "C:\Windows\System32\Dwm.exe"
3012    explorer.exe  C:\Windows\Explorer.EXE
2384    VBoxTray.exe C:\Windows\System32\VBoxTray.exe"
2432    StikyNot.exe C:\Windows\System32\StikyNot.exe"
```

2976 taskhost.exe "taskhost.exe"
1804 taskhost.exe "taskhost.exe"

vs normal taskhost should look like:

taskhost.exe {243F5DED-C140-47D9-B005-B07948B2A976}

→ **taskhost.exe** (PID 1804 and 2976) - Missing the **k** parameter pattern.

- **Real taskhost.exe** manages scheduled tasks with **specific task GUIDs**
- **This one** just has **"taskhost.exe"** in quotes - **no actual task management!**
- It's **masquerading** as a legitimate Windows service

Suspicions:

1. Two taskhost.exe processes (unusual)
2. No task GUIDs or parameters (fake)
3. Simple quoted executable name (lazy impersonation)
4. Different sessions (1 and 2) but same behavior

This suggests:

- Process impersonation - malware pretending to be taskhost.exe
- Lazy coding - attacker didn't bother with realistic parameters
- Multi-session persistence - running in both user sessions

```

1944 explorer.exe  C:\Windows\Explorer.EXE
2076 dllhost.exe   /Processid:{76D0CB12-7604-4048-B83C-10
05C7DDC503}
2728 winlogon.exe  winlogon.exe
2976 taskhost.exe  "taskhost.exe"
3000 dwm.exe       "C:\Windows\system32\Dwm.exe"
3012 explorer.exe  C:\Windows\Explorer.EXE

```

The ".EXE" vs ".exe" Case Anomaly:

Windows is case-insensitive BUT;

- Real processes typically show consistent casing
- Registry entries and system calls preserve original case
- Malware often has different case patterns

```

# Legitimate process creation preserves system casing
CreateProcess("C:\Windows\explorer.exe", ...)

# Malware might use different casing
CreateProcess("C:\Windows\Explorer.EXE", ...) ← Hardcoded by
attacker

```

▼ INSIGHTS:

The attacker got **lazy** or used an **automated tool** that doesn't properly mimic Windows process startup behavior. **Real Windows processes** have **rich command-line parameters**, while **malware processes** just have **basic executable paths**.

- **Real Windows processes** have **complex command-line arguments**
- **Malware** just uses **simple quoted paths** or **bare executable names**
- **No effort** to mimic legitimate process behavior

The attacker created **fake system processes** but didn't research how they **actually start**. They just copied the **executable names** without the **proper command-line arguments**.

This is why the `-k` parameter is like a "digital fingerprint" - it separates **real Windows processes** from **malware impersonation**.

It's a **fundamental Windows internals concept** that many attackers overlook.

▼ 4. **dlllist**

→ Shows all the Dynamic Link Libraries (DLLs) loaded into each process's memory space - reveals what code libraries and functions each program is using.

```
vol -f MemoryDump_Lab4.raw windows.dlllist
```

▼ Findings

PID	Process	Base	Size	Name	Path	LoadTime	File output
256	sms.exe	0x484a0000	0x20000	smss.exe	\SystemRoot\System32\smss.exe	N/A	Disabled
256	sms.exe	0x773f0000	0x1a9000	ntdll.dll	C:\Windows\SYSTEM32\ntdll.dll	N/A	Disabled
328	csrss.exe	0x49700000	0x60000	csrss.exe	C:\Windows\system32\csrss.exe	N/A	Disabled
328	csrss.exe	0x773f0000	0x1a9000	ntdll.dll	C:\Windows\SYSTEM32\ntdll.dll	N/A	Disabled
328	csrss.exe	0x7feffd3c0000	0x13000	CSRSRV.dll	C:\Windows\system32\CSRSRV.dll	2019-06-29 07:28:14.000000 UTC	Disabled
328	csrss.exe	0x7feffd3a0000	0x11000	basesrv.DLL	C:\Windows\system32\basesrv.DLL	2019-06-29 07:28:14.000000 UTC	Disabled
328	csrss.exe	0x7feffd360000	0x38000	winsrv.DLL	C:\Windows\system32\winsrv.DLL	2019-06-29 07:28:14.000000 UTC	Disabled
328	csrss.exe	0x771d0000	0xf4000	USER32.dll	C:\Windows\system32\USER32.dll	2019-06-29 07:28:14.000000 UTC	Disabled
328	csrss.exe	0x7feffe550000	0x67000	GDI32.dll	C:\Windows\system32\GDI32.dll	2019-06-29 07:28:14.000000 UTC	Disabled
328	csrss.exe	0x772d0000	0x11f000	kernel32.dll	C:\Windows\SYSTEM32\kernel32.dll	2019-06-29 07:28:14.000000 UTC	Disabled
328	csrss.exe	0x7feffd6a0000	0x6b000	KERNELBASE.dll	C:\Windows\system32\KERNELBASE.dll	2019-06-29 07:28:14.000000 UTC	Disabled
328	csrss.exe	0x7feffe20000	0xe000	LPK.dll	C:\Windows\system32\LPK.dll	2019-06-29 07:28:14.000000 UTC	Disabled
328	csrss.exe	0x7feffd80000	0xc9000	USP10.dll	C:\Windows\system32\USP10.dll	2019-06-29 07:28:14.000000 UTC	Disabled
328	csrss.exe	0x7feffeed0000	0x9f000	msvcrtd.dll	C:\Windows\system32\msvcrtd.dll	2019-06-29 07:28:14.000000 UTC	Disabled
328	csrss.exe	0x7feffd350000	0xc000	sxssrv.DLL	C:\Windows\system32\sxssrv.DLL	2019-06-29 07:28:15.000000 UTC	Disabled
328	csrss.exe	0x7feffd240000	0x91000	sxs.dll	C:\Windows\system32\sxs.dll	2019-06-29 07:28:17.000000 UTC	Disabled
328	csrss.exe	0x7feffe050000	0x12d000	RPCRT4.dll	C:\Windows\system32\RPCRT4.dll	2019-06-29 07:28:17.000000 UTC	Disabled
328	csrss.exe	0x7feffd230000	0xf000	CRYPTBASE.dll	C:\Windows\system32\CRYPTBASE.dll	2019-06-29 07:28:17.000000 UTC	Disabled
328	csrss.exe	0x7feffe470000	0xd6b000	ADVAPI32.dll	C:\Windows\system32\ADVAPI32.dll	2019-06-29 07:28:23.000000 UTC	Disabled
328	csrss.exe	0x7fefec20000	0x1f000	sechost.dll	C:\Windows\SYSTEM32\sechost.dll	2019-06-29 07:28:23.000000 UTC	Disabled
376	csrss.exe	0x49700000	0x6000	csrss.exe	C:\Windows\system32\csrss.exe	N/A	Disabled

Duplicate Explorer Process

- One is **3012**, and the other explorer.exe was PID **1944**
- **Having multiple explorer.exe processes is highly unusual** and often indicates:
 - Process replacement/hollowing
 - Malware masquerading as explorer.exe
 - System instability or compromise

Suspicious Timing Pattern

- All DLLs load at exactly `2019-06-29 07:29:36.000000 UTC` initially
- This is **8 seconds after the dwm.exe** process we analyzed earlier
- Uniform timestamps across all initial DLLs suggest **batch loading** rather than organic process startup

Missing VirtualBox Components

- **Notable absence:** No `VBoxMRXNP.dll` like in the first explorer.exe (PID 1944)
- This suggests different execution contexts or potential masquerading

Extensive Network/HTTP Components

Additional network components not seen in first explorer:

- `WINHTTP.dll` - HTTP client functionality
- `webio.dll` - Web I/O operations
- Various wireless and network APIs loaded

Delayed Fax Services Loading

- Fax-related DLLs (`fxsst.dll`, `FXSAPI.dll`, `FXSRESM.DLL`) load at `07:29:47`
- **11-second delay** after initial loading - unusual for standard explorer

HIGHLY SUSPICIOUS: Multiple explorer.exe processes running simultaneously is a **major red flag**. This pattern commonly indicates:

1. **Process Hollowing:** Malware replacing legitimate explorer.exe
2. **Persistence Mechanism:** Malware maintaining presence via fake explorer

3. System Compromise: Unauthorized process execution

```
[...]/Desktop/forensics/July20]$ vol -f MemoryDump_Lab4.raw windows.dlllist --pid 3012
Volatility 3 Framework 2.26.0
PID  Process Base  Size Name Path LoadTime File output
3012 explorer.exe 0x2c0000  Explorer.EXE C:\Windows\Explorer.EXE N/A Disabled
3012 explorer.exe 0x1a0000  ntdll.dll C:\Windows\SYSTEM32\ntdll.dll N/A Disabled
3012 explorer.exe 0x100000  kernel32.dll C:\Windows\SYSTEM32\kernel32.dll 2019-06-29 07:29:36.000000 UTC Disabled
3012 explorer.exe 0x080000  KERNELBASE.dll C:\Windows\SYSTEM32\KERNELBASE.dll 2019-06-29 07:29:36.000000 UTC Disabled
3012 explorer.exe 0x7fe7470000  0xb000 ADVAPI32.dll C:\Windows\SYSTEM32\ADVAPI32.dll 2019-06-29 07:29:36.000000 UTC Disabled
3012 explorer.exe 0x7fe7480000  0xb000 cryptbase.dll C:\Windows\SYSTEM32\CRYPTBASE.dll 2019-06-29 07:29:36.000000 UTC Disabled
3012 explorer.exe 0x7fe7c20000  0x1f000 sechost.dll C:\Windows\SYSTEM32\sechost.dll 2019-06-29 07:29:36.000000 UTC Disabled
3012 explorer.exe 0x7fe7e00000  0x12000 RPCRT4.dll C:\Windows\SYSTEM32\RPCRT4.dll 2019-06-29 07:29:36.000000 UTC Disabled
3012 explorer.exe 0x7fe7e10000  0x10000 cryptui.dll C:\Windows\SYSTEM32\CRYPTUI.dll 2019-06-29 07:29:36.000000 UTC Disabled
3012 explorer.exe 0x7fe7e20000  0x1a000 JSE832.dll C:\Windows\SYSTEM32\JSE832.dll 2019-06-29 07:29:36.000000 UTC Disabled
3012 explorer.exe 0x7fe7e30000  0x1e000 cryptsp.dll C:\Windows\SYSTEM32\cryptsp.dll 2019-06-29 07:29:36.000000 UTC Disabled
3012 explorer.exe 0x7fe7e40000  0x1e000 cryptui.dll C:\Windows\SYSTEM32\cryptui.dll 2019-06-29 07:29:36.000000 UTC Disabled
3012 explorer.exe 0x7fe7e50000  0x10000 cryptui.dll C:\Windows\SYSTEM32\cryptui.dll 2019-06-29 07:29:36.000000 UTC Disabled
3012 explorer.exe 0x7fe7e60000  0x10000 SHLWAPI.dll C:\Windows\SYSTEM32\SHLWAPI.dll 2019-06-29 07:29:36.000000 UTC Disabled
3012 explorer.exe 0x7fe7e70000  0x10000 cryptui.dll C:\Windows\SYSTEM32\cryptui.dll 2019-06-29 07:29:36.000000 UTC Disabled
3012 explorer.exe 0x7fe7e80000  0x203000 ole32.dll C:\Windows\SYSTEM32\ole32.dll 2019-06-29 07:29:36.000000 UTC Disabled
3012 explorer.exe 0x7fe7e6d0000  0x17000 OleAut32.dll C:\Windows\SYSTEM32\OLEAUT32.dll 2019-06-29 07:29:36.000000 UTC Disabled
3012 explorer.exe 0x7fe7e6e0000  0x17000 OLEPROXY.dll C:\Windows\SYSTEM32\OLEPROXY.dll 2019-06-29 07:29:36.000000 UTC Disabled
3012 explorer.exe 0x7fe7e750000  0x13000 User.dll C:\Windows\SYSTEM32\User.dll 2019-06-29 07:29:36.000000 UTC Disabled
3012 explorer.exe 0x7fe7e350000  0x2f000 BUIT0.dll C:\Windows\SYSTEM32\BUIT0.dll 2019-06-29 07:29:36.000000 UTC Disabled
3012 explorer.exe 0x7fe7e360000  0x10000 cryptui.dll C:\Windows\SYSTEM32\cryptui.dll 2019-06-29 07:29:36.000000 UTC Disabled
3012 explorer.exe 0x7fe7e770000  0x10000 MSCFT.dll C:\Windows\SYSTEM32\MSCFT.dll 2019-06-29 07:29:36.000000 UTC Disabled
3012 explorer.exe 0x7fe7e560000  0x50000 Extrema.dll C:\Windows\SYSTEM32\Extrema.dll 2019-06-29 07:29:36.000000 UTC Disabled
3012 explorer.exe 0x7fe7e570000  0x10000 Cryptui.dll C:\Windows\SYSTEM32\Cryptui.dll 2019-06-29 07:29:36.000000 UTC Disabled
3012 explorer.exe 0x7fe7e580000  0x1d7000 SETUPAPI.dll C:\Windows\SYSTEM32\SETUPAPI.dll 2019-06-29 07:29:36.000000 UTC Disabled
3012 explorer.exe 0x7fe7e590000  0x10000 cryptui.dll C:\Windows\SYSTEM32\cryptui.dll 2019-06-29 07:29:36.000000 UTC Disabled
3012 explorer.exe 0x7fe7e5d0000  0x1a000 DEVOBJ.dll C:\Windows\SYSTEM32\DEVOBJ.dll 2019-06-29 07:29:36.000000 UTC Disabled
3012 explorer.exe 0x7fe7e5f0000  0x18000 dwmapi.dll C:\Windows\SYSTEM32\dwmapi.dll 2019-06-29 07:29:36.000000 UTC Disabled
3012 explorer.exe 0x7fe7e600000  0x18000 cryptui.dll C:\Windows\SYSTEM32\cryptui.dll 2019-06-29 07:29:36.000000 UTC Disabled
3012 explorer.exe 0x7fe7e610000  0x215000 gdiplus.dll C:\Windows\Win32\andek_microsoft.windows.gdiplus_559584144ccf1df.1.1.7601.17514_none_2b4536c71ed437a\gdiplus.dll 2019-06-29 07:29:36.000000 UTC Disabled
3012 explorer.exe 0x7fe7e620000  0x8000 Secur32.dll C:\Windows\SYSTEM32\Secur32.dll 2019-06-29 07:29:36.000000 UTC Disabled
3012 explorer.exe 0x7fe7e630000  0x10000 cryptui.dll C:\Windows\SYSTEM32\cryptui.dll 2019-06-29 07:29:36.000000 UTC Disabled
3012 explorer.exe 0x7fe7e770000  0x12c000 PROPSYS.dll C:\Windows\SYSTEM32\PROPSYS.dll 2019-06-29 07:29:36.000000 UTC Disabled
3012 explorer.exe 0x7fe7e310000  0x3d000 WINSTA.dll C:\Windows\SYSTEM32\WINSTA.dll 2019-06-29 07:29:36.000000 UTC Disabled
3012 explorer.exe 0x7fe7e320000  0x10000 cryptui.dll C:\Windows\SYSTEM32\cryptui.dll 2019-06-29 07:29:36.000000 UTC Disabled
3012 explorer.exe 0x7fe7eac0000  0x1f4000 comctl32.dll C:\Windows\Win32\andek_microsoft.windows.common-controls_559584144ccf1df.6.0.7601.17514_none_fa396087175a9ac\comctl32.dll 2019-06-29 07:29:36.000000 UTC Disabled
```

▼ 5. getsids

→ Its a plugin used in the Volatility framework for memory analysis, which prints the SIDs (Security Identifiers) owning each process. SIDs are unique values used to identify a trustee, such as a user or group, and are crucial for understanding the privileges and identities of processes in a system's memory.

Command:

```
vol -f MemoryDump_Lab4.raw windows.getsids
```

▼ Findings:

```
(jynx㉿kali)-[~/Desktop/forensics/July30]
└─$ vol -f MemoryDump_Lab4.raw windows.getsids
Volatility 3 Framework 2.26.0
Progress: 100.00          PDB scanning finished
PID      Process SID      Name
4        System  S-1-5-18      Local System
4        System  S-1-5-32-544    Administrators
4        System  S-1-1-0  Everyone
4        System  S-1-5-11      Authenticated Users
4        System  S-1-16-16384   System Mandatory Level
256      smss.exe  S-1-5-18      Local System
256      smss.exe  S-1-5-32-544    Administrators
256      smss.exe  S-1-1-0  Everyone
256      smss.exe  S-1-5-11      Authenticated Users
256      smss.exe  S-1-16-16384   System Mandatory Level
328      csrss.exe  S-1-5-18      Local System
328      csrss.exe  S-1-5-32-544    Administrators
328      csrss.exe  S-1-1-0  Everyone
328      csrss.exe  S-1-5-11      Authenticated Users
328      csrss.exe  S-1-16-16384   System Mandatory Level
376      csrss.exe  S-1-5-18      Local System
376      csrss.exe  S-1-5-32-544    Administrators
376      csrss.exe  S-1-1-0  Everyone
```

User Account Names

- **"eminem" (RID 1000)** - This appears to be a non-standard administrative username, which is unusual for a typical corporate environment
- **"SlimShady" (RID 1001)** - This is clearly suspicious as it references Eminem's alter ego and suggests unauthorized account creation

Privilege Escalation Indicators

- The "eminem" user has **Administrator privileges** (S-1-5-32-544), which may indicate privilege escalation
- Both users are running multiple processes with interactive logon sessions

Unusual Process Execution

- **DumpIt.exe (PID 2624)** running under the "eminem" account with **High Mandatory Level** (S-1-16-12288) - This is a memory dumping tool, which could indicate:
 - Legitimate forensic analysis
 - Malicious memory extraction for credential harvesting

- Anti-forensics attempts

Multiple Active Sessions

- Two separate user sessions are active simultaneously (eminem and SlimShady)
- This could indicate:
 - Session hijacking
 - Unauthorized concurrent access
 - Lateral movement between accounts

Timing Concerns

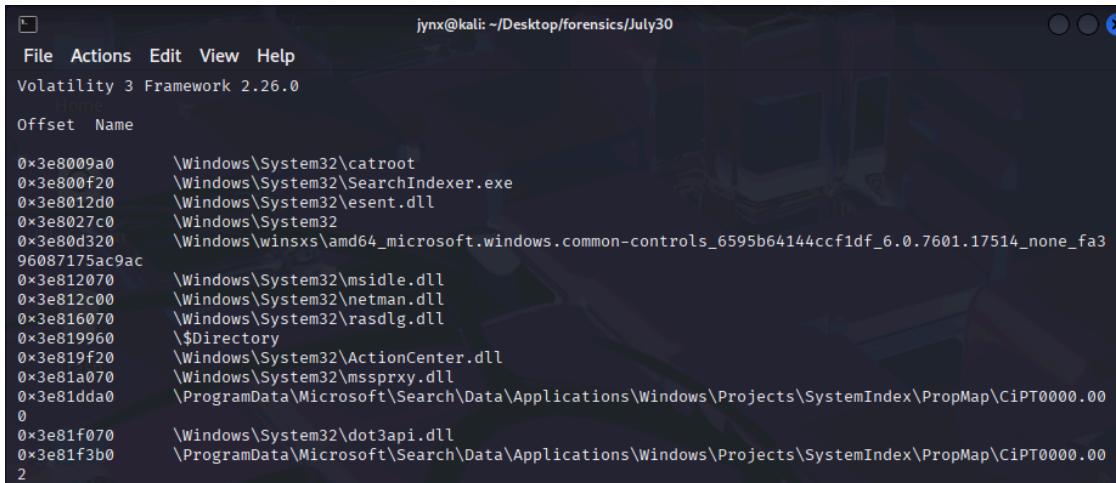
- The presence of GoogleCrashHandler processes suggests recent system activity
- StikyNot.exe (Sticky Notes) running under SlimShady account indicates active user interaction

▼ Phase 2: FLAG FINDING

Command:

```
vol -f MemoryDump_Lab4.raw windows.filescan > filescan.txt
```

▼ Findings:



The screenshot shows the Volatility Framework interface with the following command entered in the terminal window:

```
jynx@kali: ~/Desktop/forensics/July30
File Actions Edit View Help
Volatility 3 Framework 2.26.0
Home
Offset Name
0x3e8009a0 \Windows\System32\catroot
0x3e800f20 \Windows\System32\SearchIndexer.exe
0x3e8012d0 \Windows\System32\esent.dll
0x3e8027c0 \Windows\System32
0x3e80d320 \Windows\winsxs\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_fa3
96087175ac9ac
0x3e812070 \Windows\System32\msidle.dll
0x3e812c00 \Windows\System32\netman.dll
0x3e816070 \Windows\System32\rasdlg.dll
0x3e819960 $\Directory
0x3e819f20 \Windows\System32\ActionCenter.dll
0x3e81a070 \Windows\System32\mssprxy.dll
0x3e81dda0 \ProgramData\Microsoft\Search\Search\Data\Windows\Projects\SystemIndex\PropMap\ciPT0000.00
0
0x3e81f070 \Windows\System32\dot3api.dll
0x3e81f3b0 \ProgramData\Microsoft\Search\Search\Data\Windows\Projects\SystemIndex\PropMap\ciPT0000.00
2
```

The contents of the file `filescan.txt`

```
(jynx㉿kali)-[~/Desktop/forensics/July30]
└─$ less filescan.txt | grep png
0x3e8d19e0      \Users\eminem\Desktop\Screenshot1.png

(jynx㉿kali)-[~/Desktop/forensics/July30]
└─$ less filescan.txt | grep jpg
0x3ebc0690      \Users\eminem\AppData\Roaming\Microsoft\Windows\Themes\TranscodedWallpaper.jpg
0x3fd1bd50      \Users\SlimShady\AppData\Roaming\Microsoft\Windows\Themes\TranscodedWallpaper.jpg

(jynx㉿kali)-[~/Desktop/forensics/July30]
└─$ less filescan.txt | grep jpeg
0x3e8ad250      \Users\eminem\Desktop\galf.jpeg
```

Found a couple of images since the challenge mentions on how a file was deleted and maybe we can find clues on it or plain decoys depending on further look here.

→ I failed to extract the contents of the actual file. Ill see what I can find further on from here.

```
0x3e89b070      \Users\eminem\AppData\Local\GDIPFONTCACHEV1.DAT
0x3e8a4690      \Program Files\Windows Photo Viewer\ImagingEngine.dll
0x3e8a5880      \Windows\Fonts\segoeuiz.ttf
0x3e8a5cd0      \Windows\System32\UIAnimation.dll
0x3e8a6d00      \Windows\Fonts\segoeui.ttf
0x3e8a7a70      \Windows\winsxs\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_fa3
96087175ac9ac
0x3e8a85b0      \Users\eminem\AppData\Roaming\Microsoft\Windows\Recent\Flag_not_here.lnk
0x3e8a9370      \$/Directory
0x3e8a9610      \Users\eminem\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\1b4dd67f29cb1962.au
tomaticDestinations-ms
0x3e8a9a70      \$/Directory
```

sure lol,

```
(jynx㉿kali)-[~/Desktop/forensics/July30]
└─$ grep imp filescan.txt

(jynx㉿kali)-[~/Desktop/forensics/July30]
└─$ grep "imp" filescan.txt

(jynx㉿kali)-[~/Desktop/forensics/July30]
└─$ grep -i "imp" filescan.txt
0xea14f20      \Windows\System32\Tasks\Microsoft\Windows\Customer Experience Improvement Program\Consolidator
0x3ea79750      \Windows\System32\Tasks\Microsoft\Windows\Customer Experience Improvement Program\KernelCeipTask
0x3ed13390      \Windows\System32\Tasks\Microsoft\Windows\Customer Experience Improvement Program\UsbCeip
0x3edee4f0      \Windows\System32\Tasks\Microsoft\Windows\Customer Experience Improvement Program\Uploader
0x3f939720      \Users\SlimShady\AppData\Roaming\Microsoft\Windows\Recent\Important.lnk
0x3fc398d0      \Users\SlimShady\Desktop\Important.txt
```

Lets see if I can retrieve the contents of this Important.txt file or not- I hope I do lol its been hours now 😊

```
(jynx㉿kali)-[~/volatility]
$ python2 vol.py -f MemoryDump_Lab4.raw --profile=Win7SP1x64 filescan | grep -i 'important.txt'
Volatility Foundation Volatility Framework 2.6.1
0x000000003fc398d0      16      0 R--rw- \Device\HarddiskVolume2\Users\SlimShady\Desktop\Important.txt

(jynx㉿kali)-[~/volatility]
$ python2 vol.py -f MemoryDump_Lab4.raw --profile=Win7SP1x64 dumpfiles -Q 0x3fc398d0 -D extracted_files
Volatility Foundation Volatility Framework 2.6.1
*** Failed to import volatility.plugins.registry.shutdown (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.getservicesids (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.timeliner (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.malware.apihooks (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.malware.servicediff (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.userassist (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.getsids (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.shellbags (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.evtlogs (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.shimcache (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.tcaudit (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.dumpregistry (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.lsadump (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.malware.threads (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks_kernel (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.registry.amcache (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.mac.check_syscall_shadow (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.malware.svcsan (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.auditpol (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.ssdt (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.registry.registryapi (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.mac.apihooks (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.envars (ImportError: No module named Crypto.Hash)
DataSectionObject 0x3fc398d0 None \Device\HarddiskVolume2\Users\SlimShady\Desktop\Important.txt
```

Unfortunately, I cannot retrieve nor extract the Important.txt file- my challenge ends here for that matter why? Well try for yourself or watch the creator's solution to know, I'd recommend trying it first but sure you wise enough to make your own decisions.

▼ Creator's Solution Video:

https://www.youtube.com/watch?v=R4ogPvN63Xg&list=PLwHfQPh43gyqJmZxGP2Pbys1g9d0_DHiy