13Cubed Memory CTF

DATE: Saturday, 26 July, 2025

▼ 📂 Volatility Memory CTF – Day 26 | 13Cubed

Memory Dump: `memdump.mem`

Volatility Version: `Volatility 3 Framework 2.26.2`

Profile: Win10×64

Analyst: Jinay Shah ***(****a.k.a. Jynx****)***

▼ 🔍 Question 1 - Identify Malicious Process

GOAL→ ***Find the running rogue (malicious) process. The flag is the MD5 hash of its PID.***

- **Tool(s):** `pslist`
- **PID Identified:** `360`
- **Suspicious Trait:**

1. **Typo squatting Attack**

   Legitimate: svchost.exe

   Malicious: scvhost.exe (s and v swapped!)

   - **Classic technique**: Slight misspelling to avoid detection

- **Visual deception**: Looks legitimate at quick glance
- **Process hiding**: Blends in with real svchost processes

2. **0 threads**: Impossible for 5+ day runtime.
3. **Wow64: True**: 32-bit process (potentially evasive).
4. **Same parent (4824)**: Spawned by compromised process.
5. **Perfect timing**: Terminated right before memory dump.

- **FLAG** [MD5 HASH - PID]: `e7b24b112a44fdd9ee93bdf998c6ca0e`

```
3016    4824    scvhost.exe.ex  0xc20c6e0bf580  0       -       1       False   2018-08-01 19:52:29.000000 UTC  2018-08-01 19:52:29.000000 UTC  Disabled
336     4824    scvhost.exe.ex  0xc20c6d36c080  0       -       1       False   2018-08-01 19:52:31.000000 UTC  2018-08-01 19:52:31.000000 UTC  Disabled
1404    4824    svchost.exe     0xc20c6d82e080  0       -       1       True    2018-08-01 19:54:55.000000 UTC  2018-08-01 19:56:35.000000 UTC  Disabled
360     4824    scvhost.exe     0xc20c6cdf4580  0       -       1       True    2018-08-01 19:56:45.000000 UTC  2018-08-06 18:12:03.000000 UTC  Disabled
7968    4824    notepad.exe     0xc20c6daf9580  0       -       1       False   2018-08-01 19:57:10.000000 UTC  2018-08-01 19:57:10.000000 UTC  Disabled
8852    4824    svchost.exe     0xc20c6ab70080  0       -       1       True    2018-08-01 19:59:49.000000 UTC  2018-08-01 20:00:08.000000 UTC  Disabled
400     924     OfficeHubTaskH  0xc20c6d482080  10      -       1       False   2018-08-01 20:03:52.000000 UTC  N/A     Disabled
2744    924     RuntimeBroker.  0xc20c6db7c200  9       -       1       False   2018-08-01 20:03:52.000000 UTC  N/A     Disabled
```

Parent process of common suspicious and the actual malware in our findings as well as the multiple svchost.exe:

PPID - `4824`

Process Name - explorer.exe

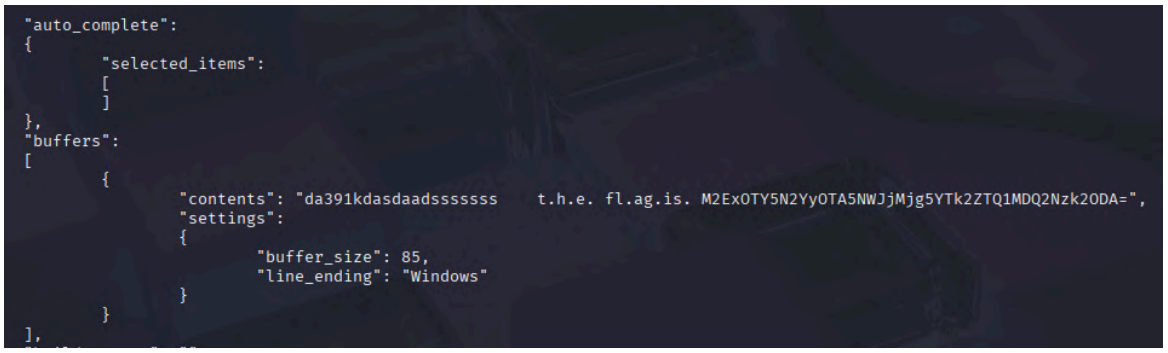
```
┌──(jynx㉿kali)-[~/Desktop/forensics/vol3/Day-26]
└─$ volatility3 -f memdump.mem windows.pslist | grep 4824
4824    4756    explorer.exe    0xc20c69cfe580  125     -       1       False   2018-08-01 19:20:58.000000 UTC  N/A     Disabled
5716    4824    ie4uinit.exe    0xc20c6b588580  0       -       1       False   2018-08-01 19:21:30.000000 UTC  2018-08-01 19:21:31.000000 UTC  Disabled
6268    4824    MSASCuiL.exe    0xc20c6c095580  3       -       1       False   2018-08-01 19:21:56.000000 UTC  N/A     Disabled
3372    4824    vmtoolsd.exe    0xc20c6cfc2580  9       -       1       False   2018-08-01 19:21:56.000000 UTC  N/A     Disabled
2200    4824    OneDrive.exe    0xc20c6cfb1580  18      -       1       True    2018-08-01 19:22:10.000000 UTC  N/A     Disabled
3884    4824    cmd.exe 0xc20c6d86b080  1       -       1       False   2018-08-01 19:37:47.000000 UTC  N/A     Disabled
8868    4824    cmd.exe 0xc20c6e495080  0       -       1       False   2018-08-01 19:40:14.000000 UTC  2018-08-01 19:49:18.000000 UTC  Disabled
10012   4824    svchost.exe     0xc20c6d6fc580  0       -       1       False   2018-08-01 19:49:19.000000 UTC  2018-08-01 19:49:19.000000 UTC  Disabled
7852    4824    svchost.exe     0xc20c6dbc5340  0       -       1       False   2018-08-01 19:49:21.000000 UTC  2018-08-01 19:49:22.000000 UTC  Disabled
6948    4824    Bubbles.scr     0xc20c6d789580  0       -       1       False   2018-08-01 19:50:30.000000 UTC  2018-08-01 19:50:31.000000 UTC  Disabled
10204   4824    Bubbles.scr     0xc20c6d0d2080  0       -       1       False   2018-08-01 19:50:33.000000 UTC  2018-08-01 19:50:38.000000 UTC  Disabled
6532    4824    ByteCodeGenera  0xc20c6ab92580  0       -       1       False   2018-08-01 19:50:42.000000 UTC  2018-08-01 19:50:42.000000 UTC  Disabled
6324    4824    dxdiag.exe      0xc20c6d4d2080  0       -       1       False   2018-08-01 19:51:18.000000 UTC  2018-08-01 19:51:28.000000 UTC  Disabled
252     4824    xwizard.exe     0xc20c6e24f580  0       -       1       False   2018-08-01 19:51:52.000000 UTC  2018-08-01 19:51:55.000000 UTC  Disabled
8140    4824    svchost.exe.ex  0xc20c6d99b580  0       -       1       False   2018-08-01 19:52:16.000000 UTC  2018-08-01 19:52:16.000000 UTC  Disabled
6176    4824    svchost.exe.ex  0xc20c6ab2b580  0       -       1       False   2018-08-01 19:52:19.000000 UTC  2018-08-01 19:52:19.000000 UTC  Disabled
5528    4824    svchost.exe.ex  0xc20c6d5ac340  0       -       1       False   2018-08-01 19:52:20.000000 UTC  2018-08-01 19:52:20.000000 UTC  Disabled
3016    4824    scvhost.exe.ex  0xc20c6e0bf580  0       -       1       False   2018-08-01 19:52:29.000000 UTC  2018-08-01 19:52:29.000000 UTC  Disabled
336     4824    scvhost.exe.ex  0xc20c6d36c080  0       -       1       False   2018-08-01 19:52:31.000000 UTC  2018-08-01 19:52:31.000000 UTC  Disabled
1404    4824    svchost.exe     0xc20c6d82e080  0       -       1       True    2018-08-01 19:54:55.000000 UTC  2018-08-01 19:56:35.000000 UTC  Disabled
360     4824    scvhost.exe     0xc20c6cdf4580  0       -       1       True    2018-08-01 19:56:45.000000 UTC  2018-08-06 18:12:03.000000 UTC  Disabled
7968    4824    notepad.exe     0xc20c6daf9580  0       -       1       False   2018-08-01 19:57:10.000000 UTC  2018-08-01 19:57:10.000000 UTC  Disabled
8852    4824    svchost.exe     0xc20c6ab70080  0       -       1       True    2018-08-01 19:59:49.000000 UTC  2018-08-01 20:00:08.000000 UTC  Disabled
9128    4824    notepad.exe     0xc20c6d732080  0       -       1       False   2018-08-01 20:05:10.000000 UTC  2018-08-01 20:05:12.000000 UTC  Disabled
8800    4824    notepad.exe     0xc20c6e5ca200  0       -       1       False   2018-08-01 20:10:19.000000 UTC  2018-08-01 20:10:21.000000 UTC  Disabled
6372    4824    notepad - Copy  0xc20c6d510080  0       -       1       False   2018-08-01 20:10:32.000000 UTC  2018-08-01 20:10:32.000000 UTC  Disabled
3504    4824    notepad - Copy  0xc20c6d694080  0       -       1       False   2018-08-01 20:10:37.000000 UTC  2018-08-01 20:10:37.000000 UTC  Disabled
8560    4824    svchost.exe     0xc20c6ddad580  10      -       1       False   2018-08-01 20:13:10.000000 UTC  N/A     Disabled
1412    4824    notepad.exe     0xc20c6abeb580  0       -       1       False   2018-08-06 18:12:15.000000 UTC  2018-08-06 18:12:17.000000 UTC  Disabled
```

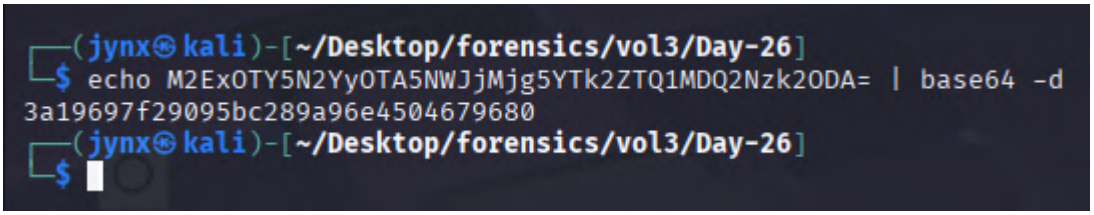
▼ 💾 Question 2 - Dump and Analyze Memory of Rogue Process

GOAL → ***Find the running rogue (malicious) process and dump its memory to disk. You'll find the 32-character flag within that process's memory.***

- **Tool(s):** `memdump` , `strings` , `base64 -d`

- **Base64 Encoded String Found:**
  `M2ExOTY5N2YyOTA5NWJjMjg5YTk2ZTQ1MDQ2Nzk2ODA=`
- **Decoded Flag:** `3a19697f29095bc289a96e4504679680`





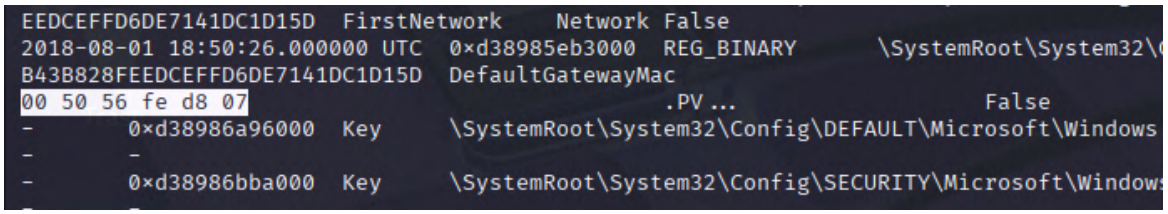
▼ 🌐 Question 3 - MAC Address of Default Gateway

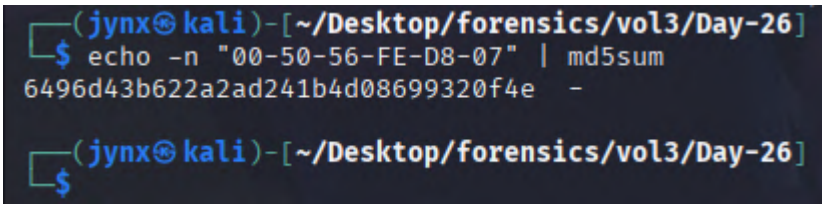
GOAL → ***What is the MAC address of this machine's default gateway? The flag is the MD5 hash of that MAC address in uppercase with dashes (-) as delimiters. Example: 01-00-A4-FB-AF-C2.***

- **Tool(s):** `printkey` , `dumpregistry` , `md5sum`
- **MAC Found:** `00-50-56-FE-D8-07`
- **Flag (MD5):** `6496d43b622a2ad241b4d08699320f4e`

```
# Print the NetworkList signatures to find the specific subkey
volatility3 -f memdump.mem windows.registry.printkey --key
"Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Unmanage
```

```
volatility3 -f memdump.mem windows.registry.printkey --key
"Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Unmanage
000F0000F0080000000F0000F0E3E937A4D0CD0A314266D2986CB7DE
43B828FEEDCEFFD6DE7141DC1D15D"
```



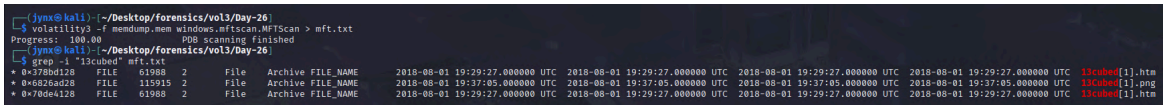


▼ 🗂️ Question 4 - Browser Cache File Path

GOAL → Find the full path of the browser cache created when an analyst visited

"www.13cubed.com." The path will begin with "Users\." Convert the path to uppercase. The flag is the MD5 hash of that string.

- **Tool(s):** -
- **Path (Uppercase):** -
- **Flag (MD5):** -



▼ 📦 Artifacts Collected

▼ 1. Registry Timestamp Discrepancy [10 Seconds]

Artifact	Description	Time Stamp
Registry `0xc20c69d52040`	**Registry should NOT start before System** - this is actually an anomaly.	2018-08-01 19:20:10

Artifact	Description	Time Stamp
	How can a CHILD process initiate before the parent process.	

```
Volatility 3 Framework 2.26.2

PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        File output

4       0       System  0xc20c69c74280  103     -       N/A     False   2018-08-01 19:20:20.000000 UTC  N/A     Disabled
68      4       Registry        0xc20c69d52040  3       -       N/A     False   2018-08-01 19:20:10.000000 UTC  N/A     Disabled
500     4       smss.exe        0xc20c6a212040  2       -       N/A     False   2018-08-01 19:20:20.000000 UTC  N/A     Disabled
612     604     csrss.exe       0xc20c6adac580  10      -       0       False   2018-08-01 19:20:24.000000 UTC  N/A     Disabled
680     672     csrss.exe       0xc20c6b8ed580  14      -       1       False   2018-08-01 19:20:25.000000 UTC  N/A     Disabled
696     604     wininit.exe     0xc20c6b913080  1       -       0       False   2018-08-01 19:20:25.000000 UTC  N/A     Disabled
```

Normally, the **System process (PID 4)** should **always** be the first process and have the earliest timestamp because:

1. **System process** is the kernel itself
2. **Registry process** is created BY the System process
3. **Parent-child relationship**: Registry (PID 68) has PPID 4 (System as parent)

This **10-second discrepancy is suspicious** and warrants further investigation. While it could be explained by technical issues, it's also a potential indicator of:

- **Rootkit activity**
- **Process manipulation**
- **Anti-forensics techniques**
- **System compromise**

▼ 2. svchost.exe suspicious

Artifact	Description	Path/Hash
svchost.exe	- ZERO Threads [Critical] - 5 days later the process terminated but then how was the current memory dump captured while other processes are still running - **PID < PPID**: Child PID lower than parent PID [Unusual]	`0xc20c6bae9580`

```
┌──(jynx㉿kali)-[~/Desktop/forensics/vol3/Day-26]
└─$ volatility3 -f memdump.mem windows.pslist
Volatility 3 Framework 2.26.2
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        File output

4       0       System  0×c20c69c74280  103     -       N/A     False   2018-08-01 19:20:20.000000 UTC  N/A     Disabled
68      4       Registry        0×c20c69d52040  3       -       N/A     False   2018-08-01 19:20:10.000000 UTC  N/A     Disabled
500     4       smss.exe        0×c20c6a212040  2       -       N/A     False   2018-08-01 19:20:20.000000 UTC  N/A     Disabled
612     604     csrss.exe       0×c20c6adac580  10      -       0       False   2018-08-01 19:20:24.000000 UTC  N/A     Disabled
680     672     csrss.exe       0×c20c6b8ed580  14      -       1       False   2018-08-01 19:20:25.000000 UTC  N/A     Disabled
696     604     wininit.exe     0×c20c6b913080  1       -       0       False   2018-08-01 19:20:25.000000 UTC  N/A     Disabled
732     672     winlogon.exe    0×c20c6b910080  6       -       1       False   2018-08-01 19:20:25.000000 UTC  N/A     Disabled
804     696     services.exe    0×c20c6b93e080  16      -       0       False   2018-08-01 19:20:26.000000 UTC  N/A     Disabled
816     696     lsass.exe       0×c20c6b98e080  9       -       0       False   2018-08-01 19:20:26.000000 UTC  N/A     Disabled
904     804     svchost.exe     0×c20c6b8df580  2       -       0       False   2018-08-01 19:20:28.000000 UTC  N/A     Disabled
924     804     svchost.exe     0×c20c6b8dd580  41      -       0       False   2018-08-01 19:20:28.000000 UTC  N/A     Disabled
940     696     fontdrvhost.ex  0×c20c6b8db580  5       -       0       False   2018-08-01 19:20:28.000000 UTC  N/A     Disabled
948     732     fontdrvhost.ex  0×c20c6b8d9580  5       -       1       False   2018-08-01 19:20:28.000000 UTC  N/A     Disabled
1020    804     svchost.exe     0×c20c6ba39580  19      -       0       False   2018-08-01 19:20:28.000000 UTC  N/A     Disabled
628     804     svchost.exe     0×c20c6ba17580  7       -       0       False   2018-08-01 19:20:28.000000 UTC  N/A     Disabled
800     804     svchost.exe     0×c20c6bae9580  0       -       0       False   2018-08-01 19:20:29.000000 UTC  2018-08-06 18:11:48.000000 UTC  Disabled
476     804     svchost.exe     0×c20c6ba9f080  7       -       0       False   2018-08-01 19:20:29.000000 UTC  N/A     Disabled
1040    804     svchost.exe     0×c20c6bae5580  4       -       0       False   2018-08-01 19:20:29.000000 UTC  N/A     Disabled
```

Most Likely Scenarios:

1. **Process Hollowing**
   - Malware created legitimate svchost.exe
   - Replaced its memory with malicious code
   - Left zombie process object
2. **Rootkit Activity**
   - Rootkit manipulating process visibility
   - Hiding active malicious processes
   - Showing terminated processes as decoy
3. **Memory Corruption**
   - Process object partially corrupted
   - Memory dump captured during termination
   - Data structure inconsistencies

▼ 3. Microsoft Edge.

Artifact	Description	Path/Hash
MicrosoftEdge.	- **ZERO Threads** [highly suspicious for a browser] for **3:57 mins**.	0xc20c6debd400

```
10024   804     svchost.exe     0×c20c6ddb1580  3       -       0       False   2018-08-01 19:30:26.000000 UTC  N/A     Disabled
9408    1768    taskhostw.exe   0×c20c6a97b580  6       -       1       False   2018-08-01 19:36:00.000000 UTC  N/A     Disabled
6552    924     MicrosoftEdge.  0×c20c6debd400  0       -       1       False   2018-08-01 19:36:12.000000 UTC  2018-08-01 19:40:09.000000 UTC  Disabled
3884    4824    cmd.exe 0×c20c6d86b080  1       -       1       False   2018-08-01 19:37:47.000000 UTC  N/A     Disabled
9912    3884    conhost.exe     0×c20c6cec3080  4       -       1       False   2018-08-01 19:37:47.000000 UTC  N/A     Disabled
8868    4824    cmd.exe 0×c20c6e495080  0       -       1       False   2018-08-01 19:40:14.000000 UTC  2018-08-01 19:49:18.000000 UTC  Disabled
7136    804     svchost.exe     0×c20c6e0ea580  3       -       0       False   2018-08-01 19:43:01.000000 UTC  N/A     Disabled
6884    924     dllhost.exe     0×c20c6d561080  5       -       1       False   2018-08-01 19:43:12.000000 UTC  N/A     Disabled
3224    804     svchost.exe     0×c20c6b585580  4       -       0       False   2018-08-01 19:43:30.000000 UTC  N/A     Disabled
```

Possible Explanations for 0 Threads

1. Normal Termination Artifact (Possible)

- Edge crashed or was force-killed
  - Memory dump captured during cleanup
  - Thread structures already deallocated
  - Process object not yet removed

2. Process Injection (Suspicious)

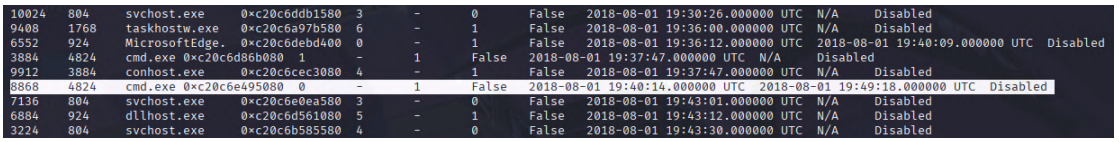
- Malware injected into legitimate Edge process
  - Ran malicious code for 4 minutes
  - Cleaned up threads during exit
  - Left process shell behind

3. Browser Crash (Normal)

- Edge encountered error and crashed
  - Abnormal termination left 0 threads
  - Windows cleanup process ongoing
  - Memory dump timing caught transition

▼ 4. cmd.exe

Artifact	Description	Path/Hash
cmd.exe	- **ZERO Threads** [highly suspicious for a terminal] running for **9:04 mins**.	0xc20c6e495080



10024	804	svchost.exe	0×c20c6ddb1580	3	-	0	False	2018-08-01 19:30:26.000000 UTC	N/A	Disabled	
9408	1768	taskhostw.exe	0×c20c6a97b580	6	-	1	False	2018-08-01 19:36:00.000000 UTC	N/A	Disabled	
6552	924	MicrosoftEdge.	0×c20c6debd400	0	-	1	False	2018-08-01 19:36:12.000000 UTC	2018-08-01 19:40:09.000000 UTC	Disabled	
3884	4824	cmd.exe	0×c20c6d86b080	1	-	1	False	2018-08-01 19:37:47.000000 UTC	N/A	Disabled	
9912	3884	conhost.exe	0×c20c6cec3080	4	-	1	False	2018-08-01 19:37:47.000000 UTC	N/A	Disabled	
8868	4824	cmd.exe	0×c20c6e495080	0	-	1	False	2018-08-01 19:40:14.000000 UTC	2018-08-01 19:49:18.000000 UTC	Disabled	
7136	804	svchost.exe	0×c20c6e0ea580	3	-	0	False	2018-08-01 19:43:01.000000 UTC	N/A	Disabled	
6884	924	dllhost.exe	0×c20c6d561080	5	-	1	False	2018-08-01 19:43:12.000000 UTC	N/A	Disabled	
3224	804	svchost.exe	0×c20c6b585580	4	-	0	False	2018-08-01 19:43:30.000000 UTC	N/A	Disabled	

9-Minute Runtime Impossibility:

Active for 9 minutes: Someone was using it

Zero threads: Process can't function without threads

Still responsive: Had to be processing commands

Clean termination: Got proper exit time

Most Likely Scenarios:

1. Process Hollowing (High Probability)

Malware created legitimate cmd.exe process
- Suspended original cmd.exe threads
- Injected malicious code using different threading
- Ran malware for 9 minutes disguised as cmd.exe
- Cleaned up all original threads during exit

2. Command Injection Attack

Attacker gained cmd.exe access
- Used it to run malicious commands
- Advanced malware manipulated thread visibility
- Anti-forensics technique to hide activity

3. Rootkit Thread Hiding

cmd.exe was actively used by attacker
- Rootkit hid real thread count from system
- Process appeared "inactive" while running malicious commands
- Sophisticated evasion technique

▼ Timeline Correlation

19:49:18 - cmd.exe ends (9-minute session)
19:49:19 - svchost.exe starts (0 seconds runtime)
19:49:21 - svchost.exe starts (1 second runtime)

19:50:30 - Bubbles.scr #(screensaver?)
19:52:16-20 - Multiple svchost.exe.ex processes
19:52:29-31 - MORE scvhost.exe.ex processes
19:56:45 - Main `scvhost.exe` starts #(THE BIG ONE - 5 days!)