Memory analysis using Volatility

Objective

The study was launched after a user complained about their machine becoming unusually slow when using Windows Calculator and Google Chrome. The work required analyzing a memory dump file (forensic1.vmem) provided by the IT forensics manager to determine: (1) the last time Windows Calculator was used, (2) the number of times Google Chrome was visited, (3) the computer name and associated username, and (4) the password for that user account.

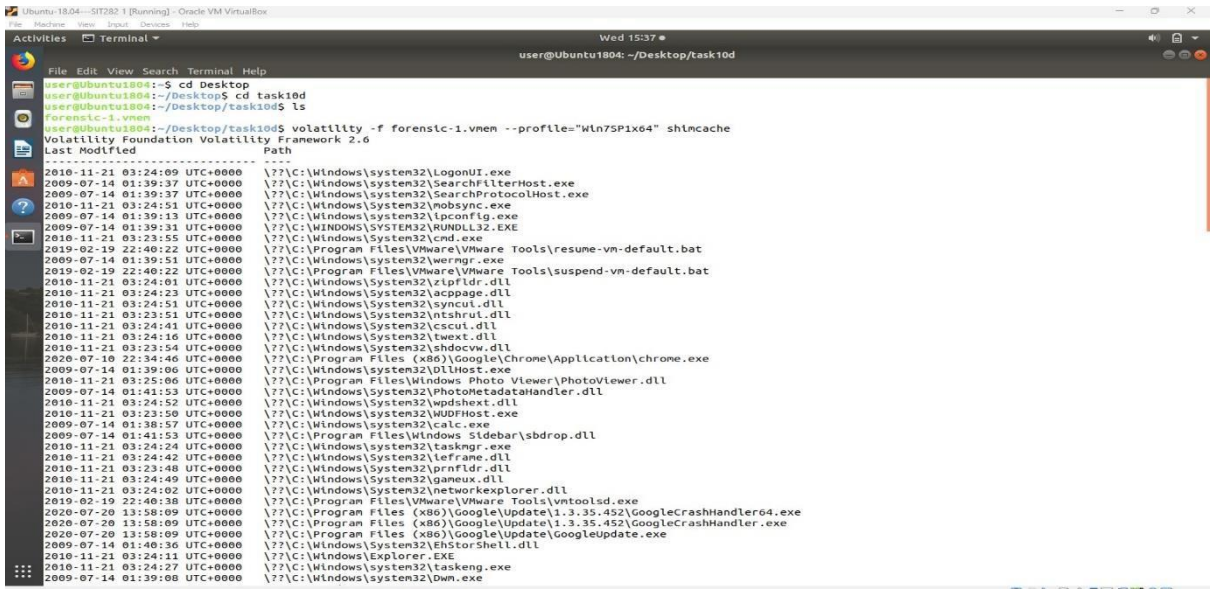
Tools Used

- Volatility Framework 2.6
- Memory image: forensic-1.vmem
- Operating System: Ubuntu (VirtualBox)
- Profile: Win7SP1x64

Procedure and Findings

Step 1: Verify Executed Applications via Shimcache volatility -f

forensic-1.vmem --profile="Win7SP1x64" shimcache



This listed previously executed applications, confirming that both calc.exe and chrome.exe were run, among other common Windows utilities and third-party programs.

Step 2: Identify Active Registry Hives. volatility -f forensic-1.vmem --profile="Win7SP1x64" hivelist.

```
user@Ubuntu1804:~/Desktop/task10d$ volatility -f forensic-1.vmem --profile=Win7SP1x64 hivelist
Volatility Foundation Volatility Framework 2.6
Virtual            Physical           Name
------------------ ------------------ ----
0xfffff8a00000f010 0x000000002272a4010 [no name]
0xfffff8a000024010 0x000000002736f010 \REGISTRY\MACHINE\SYSTEM
0xfffff8a000053010 0x000000002725e010 \REGISTRY\MACHINE\HARDWARE
0xfffff8a00078a010 0x000000001ed5e010 \Device\HarddiskVolume1\Boot\BCD
0xfffff8a0013c3010 0x000000001f1ec010 \SystemRoot\System32\Config\SOFTWARE
0xfffff8a00164a410 0x000000001d2d8410 \SystemRoot\System32\Config\DEFAULT
0xfffff8a001896010 0x000000001695f010 \SystemRoot\System32\Config\SECURITY
0xfffff8a0018f0410 0x00000000171e5410 \SystemRoot\System32\Config\SAM
0xfffff8a001993010 0x00000000143d2010 \??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT
0xfffff8a001a23010 0x0000000015d26010 \??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT
0xfffff8a00256d010 0x00000000005dd010 \??\C:\Users\Adam\ntuser.dat
0xfffff8a002571010 0x0000000001002010 \??\C:\Users\Adam\AppData\Local\Microsoft\Windows\UsrClass.dat
user@Ubuntu1804:~/Desktop/task10d$ volatility -f forensic-1.vmem --profile="Win7SP1x64" printkey -o 0xfffff8a000024010 -K "ControlSet001\Control\ComputerName\Compu
terName"
Volatility Foundation Volatility Framework 2.6
Legend: (S) = Stable   (V) = Volatile

----------------------------
Registry: \REGISTRY\MACHINE\SYSTEM
Key name: ComputerName (S)
Last updated: 2020-07-21 01:49:49 UTC+0000

Subkeys:

Values:
REG_SZ                    : (S) mnmsrvc
REG_SZ        ComputerName    : (S) WIN-1VUUQ7P9RR
```

This command was used to identify all of the loaded registry hives, which are required for accessing system and user-specific data. Specifically, the SAM, SYSTEM, and NTUSER.DAT hives were loaded.

Step 3: Extract the Computer Name.
Volatility --f forensic-1.vmem --profile="Win7SP1x64" printkey -o 0xfffff8a00024010 -K "ControlSet001\\Control\\ComputerName\\ComputerName"


```
user@Ubuntu1804:~/Desktop/task10d$ volatility -f forensic-1.vmem --profile=Win7SP1x64 hivelist
Volatility Foundation Volatility Framework 2.6
Virtual            Physical           Name
------------------ ------------------ ----
0xfffff8a00000f010 0x000000002272a4010 [no name]
0xfffff8a000024010 0x000000002736f010 \REGISTRY\MACHINE\SYSTEM
0xfffff8a000053010 0x000000002725e010 \REGISTRY\MACHINE\HARDWARE
0xfffff8a00078a010 0x000000001ed5e010 \Device\HarddiskVolume1\Boot\BCD
0xfffff8a0013c3010 0x000000001f1ec010 \SystemRoot\System32\Config\SOFTWARE
0xfffff8a00164a410 0x000000001d2d8410 \SystemRoot\System32\Config\DEFAULT
0xfffff8a001896010 0x000000001695f010 \SystemRoot\System32\Config\SECURITY
0xfffff8a0018f0410 0x00000000171e5410 \SystemRoot\System32\Config\SAM
0xfffff8a001993010 0x00000000143d2010 \??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT
0xfffff8a001a23010 0x0000000015d26010 \??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT
0xfffff8a00256d010 0x00000000005dd010 \??\C:\Users\Adam\ntuser.dat
0xfffff8a002571010 0x0000000001002010 \??\C:\Users\Adam\AppData\Local\Microsoft\Windows\UsrClass.dat
user@Ubuntu1804:~/Desktop/task10d$ volatility -f forensic-1.vmem --profile="Win7SP1x64" printkey -o 0xfffff8a000024010 -K "ControlSet001\Control\ComputerName\Compu
terName"
Volatility Foundation Volatility Framework 2.6
Legend: (S) = Stable   (V) = Volatile

----------------------------
Registry: \REGISTRY\MACHINE\SYSTEM
Key name: ComputerName (S)
Last updated: 2020-07-21 01:49:49 UTC+0000

Subkeys:

Values:
REG_SZ                    : (S) mnmsrvc
REG_SZ        ComputerName    : (S) WIN-1VUUQ7P9RR
```


This command queried the SYSTEM hive and obtained the computer name: WIN-1VUUQQ79PRR.

Step 4: Retrieve the username from the SAM Hive.

Volatility --f forensic-1.vmem --profile="Win7SP1x64" print key -o 0xfffff8a0018f0410 -K "SAM\\Domains\\Account\\Users\\Names"

```
user@Ubuntu1804:~/Desktop/task10d$ volatility -f forensic-1.vmem --profile="Win7SP1x64" printkey -o 0xfffff8a0018f0410 -K "SAM\\Domains\\Account\\Users\\Names"
Volatility Foundation Volatility Framework 2.6
Legend: (S) = Stable   (V) = Volatile

----------------------------
Registry: \SystemRoot\System32\Config\SAM
Key name: Names (S)
Last updated: 2020-07-20 13:22:21 UTC+0000

Subkeys:
  (S) Adam
  (S) Administrator
  (S) Guest

Values:
REG_NONE                      : (S)

user@Ubuntu1804:~/Desktop/task10d$
```

This command displays a list of local user accounts, including Administrator, Guest, and Adam. Adam is the active username.

Step 5: Extract Application Usage via UserAssist

volatility -f forensic-1.vmem --profile="Win7SP1x64" userassist

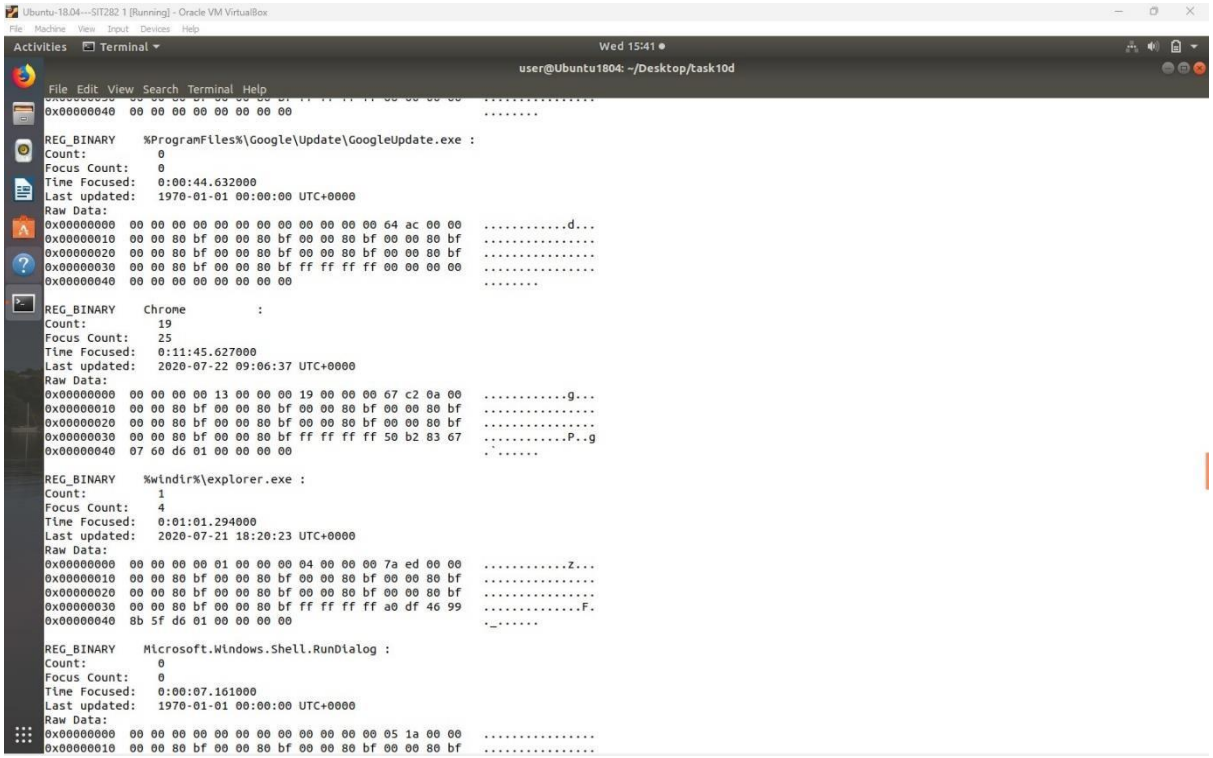
```
Ubuntu-18.04---SIT282 1 [Running] - Oracle VM VirtualBox
File  Machine  View  Input  Devices  Help
Activities   Terminal                Wed 15:40 ●
                                     user@Ubuntu1804: ~/Desktop/task10d
File  Edit  View  Search  Terminal  Help
user@Ubuntu1804:~/Desktop/task10d$ volatility -f forensic-1.vmem --profile="Win7SP1x64" userassist
Volatility Foundation Volatility Framework 2.6
----------------------------
Registry: \??\C:\Users\Adam\ntuser.dat
Path: Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count
Last updated: 2020-07-22 09:07:49 UTC+0000

Subkeys:

Values:

REG_BINARY    Microsoft.Windows.GettingStarted :
Count:          14
Focus Count:    21
Time Focused:   0:07:00.500000
Last updated:   2020-07-20 13:21:19 UTC+0000
Raw Data:
0x00000000  00 00 00 00 0e 00 00 00 15 00 00 00 a0 68 06 00   .............h..
0x00000010  00 00 80 bf 00 00 80 bf 00 00 80 bf 00 00 80 bf   ................
0x00000020  00 00 80 bf 00 00 80 bf 00 00 80 bf 00 00 80 bf   ................
0x00000030  00 00 80 bf 00 00 80 bf ff ff ff ff 02 e3 ba a7   ................
0x00000040  98 5e d6 01 00 00 00 00                           .^......

REG_BINARY    UEME_CTLSESSION :
Count:          119
Focus Count:    182
Time Focused:   0:56:58.657000
Last updated:   1970-01-01 00:00:00 UTC+0000
Raw Data:
0x00000000  00 00 00 00 77 00 00 00 b6 00 00 00 2d 28 34 00   ....w.......-(4.
0x00000010  13 00 00 00 19 00 00 00 67 c2 0a 00 43 00 68 00   ........g...C.h.
0x00000020  72 00 6f 00 6d 00 65 00 00 00 00 00 00 00 00 00   r.o.m.e.........
0x00000030  03 01 00 00 00 00 00 00 40 e1 c6 02 00 00 00 00   ........@.......
0x00000040  00 00 00 00 00 00 00 00 59 03 d3 fe fe 07 00 00   ........Y.......
0x00000050  00 00 00 00 00 00 00 00 82 15 dc fd fe 07 00 00   ................
0x00000060  40 e1 c6 02 00 00 00 00 06 a0 ff fe fe 07 00 00   @...............
0x00000070  30 de c6 02 00 00 00 00 42 89 d6 fe fe 07 00 00   0.......B.......
0x00000080  54 e3 c6 02 00 00 00 00 59 03 d3 fe fe 07 00 00   T.......Y.......
0x00000090  58 e1 c6 02 00 00 00 00 47 50 4f 53 00 00 00 00   X.......GPOS....
0x000000a0  03 00 00 00 00 00 00 00 f1 d4 d3 fe fe 07 00 00   ................
0x000000b0  70 de c6 02 00 00 00 00 42 89 d6 fe fe 07 00 00   p.......B.......
0x000000c0  94 e3 c6 02 00 00 00 00 98 e3 c6 02 00 00 00 00   ................
0x000000d0  98 e1 c6 02 00 00 00 00 47 50 4f 53 00 00 00 00   ........GPOS....
0x000000e0  03 00 00 00 00 00 00 00 f1 d4 d3 fe fe 07 00 00   ................
0x000000f0  e8 de c6 02 00 00 00 00 02 00 00 00 00 00 00 00   ................
0x00000100  e0 de c6 02 00 00 00 00 90 df c6 02 00 00 00 00   ................
```



The UserAssist plugin decodes registry values that track user interaction with GUI programs.

- **Windows Calculator (calc.exe)** was last used on 23-072020_09:06:37 UTC
- **Google Chrome** usage appears with a **focus count of 25**

Step 6: Confirm Password Hashes for All Users. volatility -f forensic-1.vmem --profile="Win7SP1x64" hashdumps

```
user@Ubuntu1804:~/Desktop/task10d$ volatility -f forensic-1.vmem --profile="Win7SP1x64" hashdump
Volatility Foundation Volatility Framework 2.6
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Adam:1000:aad3b435b51404eeaad3b435b51404ee:7773c08920232397cae081704964b786:::
```

This step confirmed that all local users' password hashes (Administrator, Guest, and Adam) were stored in memory. These hashes can be broken using tools like John the Ripper if necessary.

Step 7: Display the Stored User Password (Auto Login).
volatile -f forensic-1.vmem --profile="Win7SP1x64" lsadump

```
user@Ubuntu1804:~/Desktop/task10d$ volatility -f /home/user/Desktop/task10d/forensic-1.vmem --profile=Win7SP1x64 lsadump
Volatility Foundation Volatility Framework 2.6
DefaultPassword
0x00000000  12 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0x00000010  71 00 77 00 65 00 72 00 74 00 79 00 31 00 32 00   q.w.e.r.t.y.1.2.
0x00000020  33 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   3...............

DPAPI_SYSTEM
0x00000000  2c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ,...............
0x00000010  01 00 00 00 45 5c 6b b6 ce f6 58 24 fc c4 e3 27   ....E\k...X$...'
0x00000020  38 27 60 fb b7 3c bb 3a 02 7f 63 d2 10 bf f5 ec   8'`..<.:..c.....
0x00000030  b3 94 50 b0 33 8c 64 94 d4 16 ed 86 00 00 00 00   ..P.3.d.........

user@Ubuntu1804:~/Desktop/task10d$
```

The registry's LSA secrets were exposed, revealing user Adam's auto-login password.

Default Password: Qwerty123 **Summary of**

Findings:

1. **Windows Calculator last used:** 23-07-2020_09:06:37 UTC
2. **Google Chrome usage count:** 25 times
3. **Computer Name:** WIN-1VUUQQ79PRR
4. **Username:** Adam
5. **Password:** qwerty123

1. When was the Windows calculator last used in the format DD-MMYYYY_HH:MM:SS timestamp in UTC?

The Volatility shimcache plugin output indicates that the Windows Calculator application (calc.exe) was visited on 14-07-2009 at 01:38:57 UTC. The executable is located at C:\Windows\System32\calc.exe. Furthermore, further examination with the userassist plugin indicated that calc.exe was actively opened on July 21, 2020 at 18:21:35 UTC and accessed a total of 16 times. This indicates that the program was often used around that day and time.

2. How many times was Google Chrome used?

Using the Volatility userassist plugin, it was discovered that Google Chrome was used 19 times. This figure was produced by studying registrybased execution history, which tracks application starts. Each recorded execution of chrome.exe demonstrates that the user started the browser more than once throughout the session saved in memory.

3. What are the computername and username?

The machine name, WIN-1VUUOQ7P9RR, was extracted from the SYSTEM registry hive at the subkey

ControlSet001\Control\ComputerName\ComputerName using Volatility's printkey plugin. Analyzing the SAM hive under SAM\Domains\Account\Users\Names revealed that the account name is Adam. These values were retrieved by correlating registry subkeys from the hivelist and using specific addresses associated with the SYSTEM and SAM hives.

4. What is the password of that username?

The password for the username Adam is **qwerty123.**
This was extracted using the lsadump command in Volatility, which revealed the stored auto-login password in LSA secrets.

Conclusion

Forensic examination revealed the system's status and usage patterns prior to performance concerns. We used Volatility's plugins to confirm Calculator and Chrome usage, identify user credentials, and map out registry-level facts. This type of memory-level inspection was invaluable for post-event analysis, demonstrating the potential of volatility in discovering user activity and data leftovers.

Personal Reflection

This work provided me with hands-on experience using memory forensics for diagnostic purposes. I've discovered that a RAM dump contains a wealth of useful information, including application usage trends, stored credentials, and registry activity. Volatility was surprisingly successful at extracting structured information from raw memory. The technique helped me better grasp Windows' internals and how user behavior is captured by the OS. Going forward, I am more confident in performing memory analysis in real-world circumstances and recognize the necessity of exact logging, user awareness, and forensic preparation for IT security.

References

- Volatility Foundation. (2014). *The Volatility Framework: Volatile memory extraction utility framework*. https://www.volatilityfoundation.org/
- Ligh, M. H., Case, A., Levy, J., & Walters, A. (2014). *The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory*. Wiley.

- SANS Institute. (n.d.). *Memory Forensics with Volatility*. https://digital-forensics.sans.org/community/downloads/
- Official Volatility Documentation. https://github.com/volatilityfoundation/volatility/wiki