A Forensic Tool

19CSE311 Computer Security

CB.EN.U4CSE22424 - **N Sai Kiran Varma**

CB.EN.U4CSE22440 - **Soma Siva Pravallika**

CB.EN.U4CSE22444 - **Suman Panigrahi**

CB.EN.U4CSE22457 - **Sravani Oruganti**

Digital Forensics

Digital forensics is a branch of forensic science focusing on identifying, acquiring, processing, analyzing, and reporting data stored electronically. Electronic evidence is a component of

almost all criminal activities and digital forensics support is crucial for law enforcement investigations.

Volatility in Memory Forensics

The open-source memory forensics framework Volatility examines volatile memory (RAM) from computer systems. This is particularly useful for investigating cyberattacks, malware, and other security incidents.

Key uses:

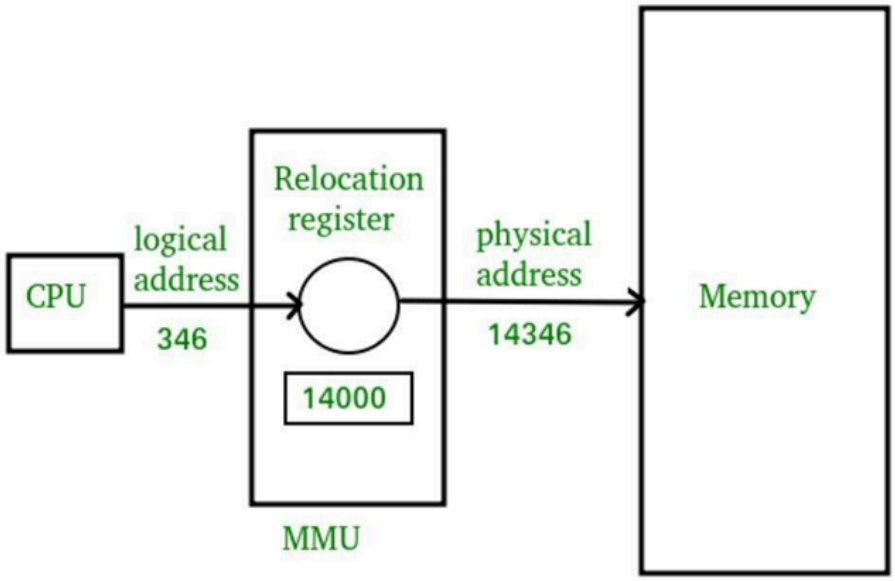
1) Investigating cyberattacks
2) Analyzing malware
3) Examining security incidents
4) Extracting and analyzing the data from a system's memory, including:
    a) Running processes
    b) Open network connections
    c) Registry keys
    d) Other valuable information

Introduction

Volatility is a powerful, open-source tool primarily used in digital forensics to analyze a system's RAM (Random Access Memory) dumps, allowing investigators to extract valuable information like active processes, network connections, registry details, and even potential malware that might only exist in memory, providing crucial insights into a system's state at a specific point in time.

Originally developed by Aaron Walters, Volatility is widely used by cybersecurity experts, forensic analysts, and incident responders to uncover in-memory threats that do not leave traces on disk. It supports multiple operating systems, including Windows, Linux, and macOS.

The primary motivation behind Volatility was to create a robust and extensible tool that could overcome the limitations of traditional disk-based forensics by analyzing the dynamic state of a system captured in memory. This was increasingly important as malware and sophisticated attacks began to operate primarily in memory to evade detection.



Is it open-source?

Volatility is an open-source tool. It is freely available under the GNU General Public License (GPL), allowing researchers and forensic analysts to use, modify, and distribute it.

Why open-source?

- **Transparency:** Security experts can verify and improve its code.
- **Community Contributions:** Developers worldwide enhance its features.
- **Free to use:** No Licensing costs, making it accessible for investigations.

Volatility Compared to Other Memory Forensics Tools

Feature	***Volatility***	***Rekall***	***Redline***	***FTK Imager***
Type	Open Source	Open Source	Free (Limited)	Commercial
OS Support	Windows, Linux, MacOS	Windows, Linux, MacOS	Windows	Windows
Focus Area	RAM Analysis, Malware Detection	RAM Analysis, Incident Response	Memory & Disk Analysis	Disk Imaging & Memory Capture
Command-line or GUI	Command-line	Command-line & Web Interface	GUI	GUI

Feature	***Volatility***	***Rekall***	***Redline***	***FTK Imager***
Malware Detection	✔️Strong	✔️Strong	✔️Moderate	❌No
Live Memory Analysis	✔️Yes	✔️Yes	✔️Limited	❌No
Community Support	✔️Large	✔️Medium	❌Limited	❌Proprietary

Authors of Volatility

The primary author and creator of Volatility is Aaron Walters. He developed the tool to aid in memory forensics, especially for investigating cyberattacks and malware.

Since its creation, many contributors have enhanced Volatility, including experts from various cybersecurity fields. Some notable contributors include:

- **Aaron Walters** pioneered the field of memory forensics by designing a framework that extracts digital artifacts from volatile memory.
- **Michael Hale Ligh** – A leading expert in malware analysis and reverse engineering.
- **Andrew Case** – A core developer of Volatility, Andrew has contributed significantly to digital forensics through his hands-on work in incident response and system analysis, making him a respected voice in the field.
- **Jamie Levy** – One of the earliest contributors to Volatility.

Key Features of Volatility

1. **Malware Analysis:** Volatility is often used to ***detect and analyze malware*** by examining the memory state for suspicious or malicious activity.
2. **Digital Forensics Training:** The tool is widely used in digital forensics training due to its effectiveness in teaching memory analysis techniques.
3. **Automation and Scripting:** It supports automation through scripting, making it ***efficient for processing large datasets*** or repeating tasks.
4. **Forensic Timeline:** Volatility allows users to ***create a timeline of system activity***, aiding in reconstructing events and sequences.

5. **Memory Analysis:** Volatility specializes in ***analyzing the volatile memory (RAM)*** of systems, allowing investigators to extract valuable information from running processes, network connections, and more.
6. **Registry Extraction:** Extracts Windows registry hives from memory.

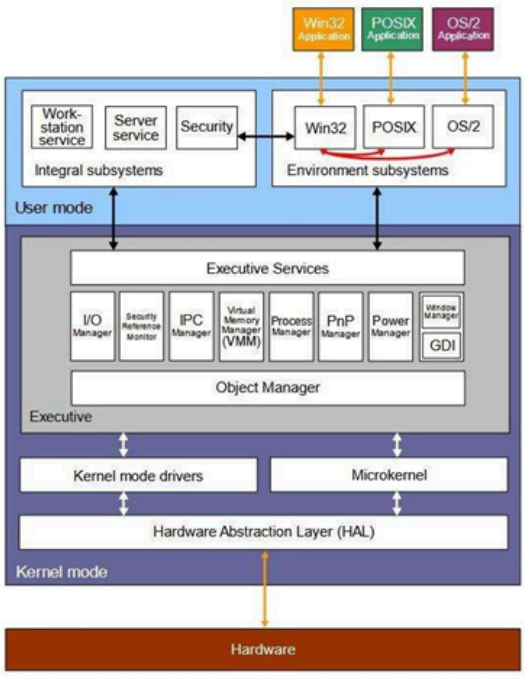


Fig. Windows user mode and kernel mode architecture

A Balanced Look at Its Advantages and Limitations

Pros:

1. **Open Source**: Free to use and highly customizable.
2. **Cross-Platform Support**: Works on Windows, Linux, and macOS, making it versatile for various systems.
3. **Malware Detection**: Effective in detecting fileless malware and hidden in-memory threats.
4. **Extensive Features**: Includes powerful features like process listing, network analysis, and registry extraction.
5. **Active Community**: Supported by a large community of contributors and regular updates.

Cons:

1. **Steep Learning Curve**: Requires command-line expertise, which may be challenging for beginners.
2. **No Built-in GUI**: Primarily command-line based, which may limit usability for non-technical users.
3. **Limited Support for Encrypted Memory**: Can struggle with certain types of encrypted or compressed memory.
4. **Resource Intensive**: This can require significant system resources, especially for large memory dumps.

Commands

1. Process Listing
    a. **Command**: volatility -f memory.dmp pslist
    b. **Description**: Lists running processes in the memory dump.
2. Network Connections
    a. **Command**: volatility -f memory.dmp netscan
    b. **Description**: Scans for active network connections (IP, port).
3. Process Dump
    a. **Command**: volatility -f memory.dmp procdump -p <PID>
    b. **Description**: Dumps memory from a specific process identified by PID.
4. Registry Hives
    a. **Command**: volatility -f memory.dmp hivelist
    b. **Description**: Lists registry hives loaded in memory.
5. Kernel Modules
    a. **Command**: volatility -f memory.dmp modules
    b. **Description**: Lists kernel modules loaded in memory.
6. Malware Detection

a. **Command**: volatility -f memory.dmp malfind

b. **Description**: Scans memory for code injections and malware.

Use Cases of Volatility

1. Malware Analysis

    - **Description**: Volatility is used to ***identify fileless malware*** and other memory-resident threats that don't leave traces on disk. By analyzing live memory dumps, forensic investigators can detect malicious processes, injected code, or abnormal system behavior caused by malware.
    - **Example**: Identifying rootkits or process injection by examining hidden or suspicious processes in memory.

2. Incident Response and Forensics

    - **Description**: Memory forensics is crucial for recovering volatile data during a cyberattack or security breach. Volatility helps incident responders ***extract information*** like user activity, network connections, and file system artifacts, providing critical evidence for forensic investigations.
    - **Example**: Tracing a hacker's activity by reviewing active network connections, recently executed processes, or even identifying stolen credentials in memory.

3. Memory Dump Recovery

    - **Description**: Volatility helps in ***recovering deleted files*** or data from memory dumps, including encryption keys, passwords, and other sensitive data that was lost during system crashes or attacks.
    - **Example**: Extracting ransomware's decryption keys from an infected system's memory dump.

4. System Configuration Analysis

    - **Description**: Volatility allows investigators to analyze system configurations and user activity by ***extracting registry hives*** and other system information from memory. This is useful for understanding how a system was configured or diagnosing abnormal system behavior.
    - **Example**: Identifying unusual registry settings or unauthorized configuration changes that could indicate a compromise.

Demonstration

```
csi@csi-analyst:~/Desktop/memdumps$ vol
volatility        volk-config-info  volk_modtool      volk_profile      volname
csi@csi-analyst:~/Desktop/memdumps$ volatility -f cridex.vmem imageinfo
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with WinXPSP2x86)
                     AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : FileAddressSpace (/home/csi/Desktop/memdumps/cridex.vmem)
                      PAE type : PAE
                           DTB : 0x2fe000L
                          KDBG : 0x80545ae0L
          Number of Processors : 1
     Image Type (Service Pack) : 3
                KPCR for CPU 0 : 0xffdff000L
             KUSER_SHARED_DATA : 0xffdf0000L
```

```
csi@csi-analyst:~/Desktop/memdumps$ volatility -f cridex.vmem --profile=WinXPSP2x86 pslist
Volatility Foundation Volatility Framework 2.6
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start
---------- -------------------- ------ ------ ------ -------- ------ ------ ------------------------------
0x823c89c8 System                    4      0     53      240 ------      0

0x822f1020 smss.exe                368      4      3       19 ------      0 2012-07-22 02:42:31 UTC+0000

0x822a0598 csrss.exe               584    368      9      326      0      0 2012-07-22 02:42:32 UTC+0000

0x82298700 winlogon.exe            608    368     23      519      0      0 2012-07-22 02:42:32 UTC+0000

0x81e2ab28 services.exe            652    608     16      243      0      0 2012-07-22 02:42:32 UTC+0000

0x81e2a3b8 lsass.exe               664    608     24      330      0      0 2012-07-22 02:42:32 UTC+0000

0x82311360 svchost.exe             824    652     20      194      0      0 2012-07-22 02:42:33 UTC+0000

0x81e29ab8 svchost.exe             908    652      9      226      0      0 2012-07-22 02:42:33 UTC+0000

0x823001d0 svchost.exe            1004    652     64     1118      0      0 2012-07-22 02:42:33 UTC+0000

0x821dfda0 svchost.exe            1056    652      5       60      0      0 2012-07-22 02:42:33 UTC+0000
```

```
csi@csi-analyst:~/Desktop/memdumps$ volatility -f cridex.vmem --profile=WinXPSP2x86 pstree
Volatility Foundation Volatility Framework 2.6
Name                                                  Pid   PPid   Thds   Hnds Time
-------------------------------------------------- ------ ------ ------ ------ ----
 0x823c89c8:System                                      4      0     53    240 1970-01-01 00:00:00 UTC+0000
. 0x822f1020:smss.exe                                 368      4      3     19 2012-07-22 02:42:31 UTC+0000
.. 0x82298700:winlogon.exe                            608    368     23    519 2012-07-22 02:42:32 UTC+0000
... 0x81e2ab28:services.exe                           652    608     16    243 2012-07-22 02:42:32 UTC+0000
.... 0x821dfda0:svchost.exe                          1056    652      5     60 2012-07-22 02:42:33 UTC+0000
.... 0x81eb17b8:spoolsv.exe                          1512    652     14    113 2012-07-22 02:42:36 UTC+0000
.... 0x81e29ab8:svchost.exe                           908    652      9    226 2012-07-22 02:42:33 UTC+0000
.... 0x823001d0:svchost.exe                          1004    652     64   1118 2012-07-22 02:42:33 UTC+0000
..... 0x8205bda0:wuauclt.exe                         1588   1004      5    132 2012-07-22 02:44:01 UTC+0000
..... 0x821fcda0:wuauclt.exe                         1136   1004      8    173 2012-07-22 02:43:46 UTC+0000
.... 0x82311360:svchost.exe                           824    652     20    194 2012-07-22 02:42:33 UTC+0000
.... 0x820e8da0:alg.exe                               788    652      7    104 2012-07-22 02:43:01 UTC+0000
.... 0x82295650:svchost.exe                          1220    652     15    197 2012-07-22 02:42:35 UTC+0000
... 0x81e2a3b8:lsass.exe                              664    608     24    330 2012-07-22 02:42:32 UTC+0000
.. 0x822a0598:csrss.exe                               584    368      9    326 2012-07-22 02:42:32 UTC+0000
 0x821dea70:explorer.exe                             1484   1464     17    415 2012-07-22 02:42:36 UTC+0000
. 0x81e7bda0:reader_sl.exe                           1640   1484      5     39 2012-07-22 02:42:36 UTC+0000
```

```
strings 1640.dmp | less
```

```
csi@csi-analyst:~/Desktop/memdumps$ volatility -f cridex.vmem --profile=WinXPSP2x86 connscan
Volatility Foundation Volatility Framework 2.6
Offset(P)  Local Address             Remote Address            Pid
---------- ------------------------- ------------------------- ---
0x02087620 172.16.112.128:1038       41.168.5.140:8080         1484
0x023a8008 172.16.112.128:1037       125.19.103.198:8080       1484
```

```
GetSystemWindowsDirectoryW
D124W
|T %
|` %
|T %
|` %
|p:6
|x:6
ZH:6
Zx:6
ZH:6
B~?y
ZH?6
ReaAdobeReaderSpeedLaunchCmdWnd
A~+wB~
A~kwB~
A~+wB~
Actx
[IY-
SsHd,
[IY-
SsHd,
GsHd(
CeO`
```

```
csi@csi-analyst:~/Desktop/memdumps$ strings 1640.dmp | grep -Fi "KB00207877.exe"
KB00207877.exe
C:\Documents and Settings\Robert\Application Data\KB00207877.exe(,
KB00207877.EXEn
KB00207877.exe
KB00207877.exe
C:\Documents and Settings\Robert\Application Data\KB00207877.exe(,
```

Conclusion

Volatility is an open-source memory forensics framework used to examine a system's runtime memory (RAM) for hidden threats and crucial evidentiary data. It is essential in cybersecurity and incident response, allowing analysts to investigate compromised systems, trace attacker activity, and identify damage. Despite its command-line interface and potential learning curve, Volatility's benefits outweigh the challenges, and its open-source nature ensures continuous development and community support.

References

[1] Volatility Foundation Official Website: Provides comprehensive information about the framework, including downloads and updates.
Site: volatilityfoundation.org

[2] Volatility 3 Documentation: The latest documentation for Volatility 3, detailing its features and usage.
Site: volatility3.readthedocs.io

[3] Volatility Github Repository: https://github.com/volatilityfoundation