Volatility3

Volatility3, a volatile memory extraction utility framework, Is how they say in the official pages. The latest volatility as this paper is written is Volatility3 the successor of its predecessor Volatility2. And this paper will talk mostly about volatility3, an unOfficial Documentation of Volatility3.

The primary goal of Volatility3 is to assist in understanding the state of a computer during the time of its last use. Volatility3 does this by extracting information such as running processes, network connections, open files, and registry keys from memory dumps. This is particularly useful in cybercrime investigations, where attackers often leave traces only in the volatile memory.

One of the key improvements in Volatility3, compared to its predecessor, Volatility2, is its modular design. This makes it more adaptable and scalable for different types of investigations. Moreover, Volatility3 is written in Python, allowing for easier integration with other forensic tools and a more user-friendly experience for investigators who are familiar with Python.

Volatility3 also supports a wide range of plugins that can be used to extract specific types of data from memory dumps. These plugins can be developed by anyone with knowledge of Python, making the tool incredibly flexible and constantly evolving with contributions from the forensic community.

Volatility runs on command line interface, making it hard to learn for a beginner forensic investigator. In order to make volatility easier to use, Meyers et al. developed developed a plugin that can run basic volatility command on a software named Autopsy

How does it work?

Volatility3 works by extracting and analyzing digital artifacts from volatile memory samples. Volatile memory, also known as RAM, is the computer's short-term memory that is lost when the power is turned off. It can store a wealth of information about the system's state, including running processes, network connections, and user activity.

Volatility3 uses a process called memory mapping to create a virtual view of the system's memory. This allows the framework to access and analyze the contents of volatile memory without having to physically access the RAM itself.

Once Volatility3 has a virtual view of the system's memory, it can use a variety of techniques to extract digital artifacts. These techniques include:

- **Process enumeration:** This technique identifies all of the processes that were running on the system at the time the memory sample was taken.
- **Registry parsing:** This technique extracts information from the Windows registry, which is a database that stores configuration settings for the operating system and applications.
- **File carving:** This technique identifies and extracts files from the memory sample, even if they have been deleted or overwritten.

Volatility3 also includes a number of plugins that can be used to perform more specialized tasks, such as analyzing malware infections and investigating data breaches.

Here is an explanation of how Volatility3 works:

1. **Memory acquisition:** The first step is to acquire a memory sample from the system being investigated. This can be done using a variety of methods, such as using a live response tool or by creating a physical image of the RAM.

2. **Memory mapping:** Once a memory sample has been acquired, Volatility3 uses a process called memory mapping to create a virtual view of the system's memory. This allows the framework to access and analyze the contents of volatile memory without having to physically access the RAM itself.

3. **Artifact extraction:** Once Volatility3 has a virtual view of the system's memory, it can use a variety of techniques to extract digital artifacts. These techniques include process enumeration, registry parsing, and file carving.

4. **Analysis:** The final step is to analyze the extracted artifacts. This can be done using a variety of tools, such as Volatility3 itself, other memory forensics tools, or traditional forensic tools.

In conclusion, Volatility3 is a powerful tool that can be used to investigate a wide range of incidents. It is an essential tool any digital forensics investigator should have.