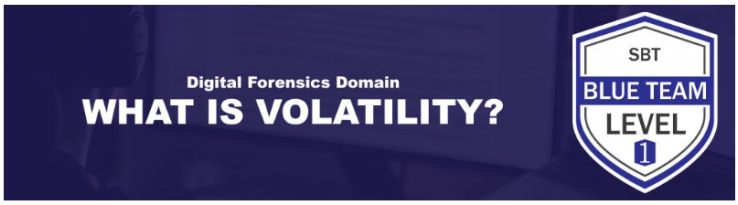
What is Volatility?



Volatility is an open-source memory forensics framework for incident response and malware analysis. It is written in Python and supports Microsoft Windows, Mac OS X, and Linux operating systems. Volatility was originally created by computer scientist Aaron Walters, drawing on academic research he did in memory forensics. This is a very powerful tool, and we can complete lots of interactions with memory dump files, such as:

- List all processes that were running.
- List active and closed network connections.
- View internet history (IE).
- Identify files on the system and retrieve them from the memory dump.
- Read the contents of notepad documents.
- Retrieve commands entered into the Windows Command Prompt (CMD).
- Scan for the presence of malware using YARA rules.
- Retrieve screenshots and clipboard contents.
- Retrieve hashed passwords.
- Retrieve SSL keys and certificates.
- And lots more!

In the next lesson, we will teach you how to perform some basic investigative actions using Volatility, then provide you with two memory dumps which you will analyze and retrieve specific information from, helping you to become more comfortable using this tool for memory forensics. We will also include links to resources where you can download additional memory dumps if you want to sharpen your skills, and even try analyzing some malware infections!

Privacy & Cookies Policy