Blue Team Tools

for SOC Analysts

Table of Contents

03 Procmon

04 Volatility

05 Caldera

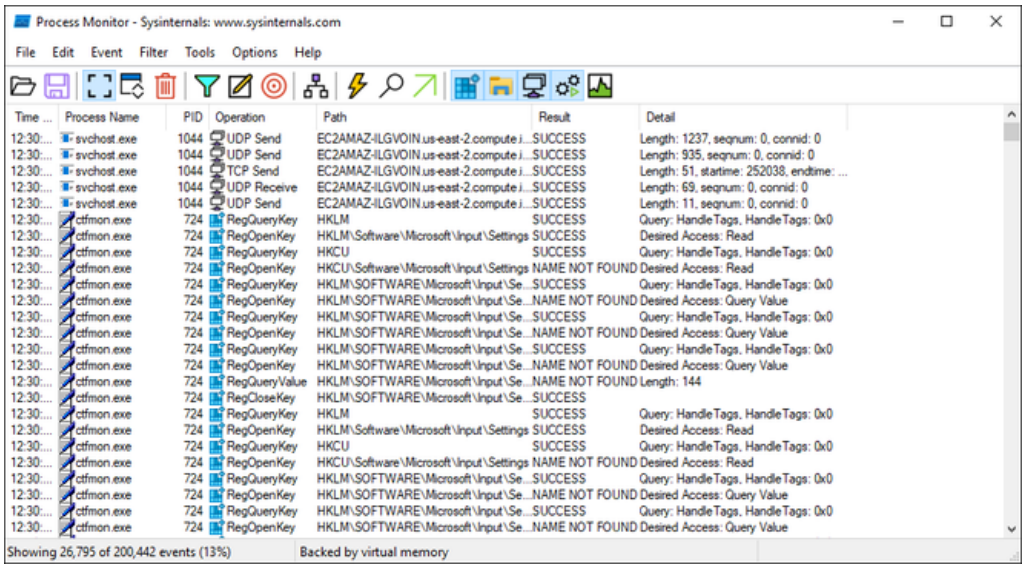
06 Wireshark

07 Immunity Debugger

PROCMON

Procmon(Process Monitor) tool is a useful tool that provides real-time information by monitoring the activities of processes on Windows. With this tool, it is seen what changes a process has made to the system. If the examined process is performing a malicious activity, this activity can be detected with the Procmon tool. For example, the process may be trying to read important files on the system, or it may be trying to maintain persistence on the system by creating a record of its own on the registry. The purpose of the Procmon tool is to analyze the processes running on the machine in real time.

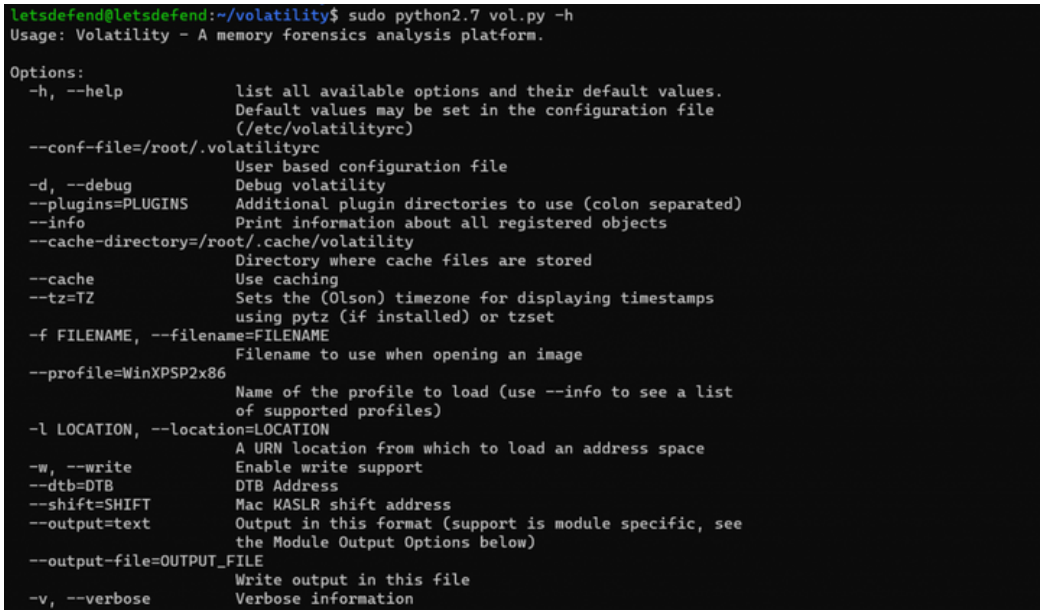
Procmon tool is a tool with a graphical user interface (GUI) included in Sysinternals tools. When the procmon tool is run, a window like the one below appears:



VOLATILITY

Volatility is a tool that enables the analysis of memory dumps taken from a compromised machine during the incident response process. Volatility is one of the memory dump analysis tools that should be used when it is desired to analyze the memory dump instead of performing memory analysis on the live machine. Volatility is written in python and runs on the command line. With this tool, memory dump analysis of both Windows and Linux machines can be done. It is an important tool used to detect malicious process activities on systems. The modules, it contains, enables the carrying out of the analysis process in a target-oriented manner. For example, it provides the analyst with important information such as which processes are running on the system, which subprocesses these processes are connected to, and which process is running which command on the command line.

An example image of the Volatility tool is as follows:

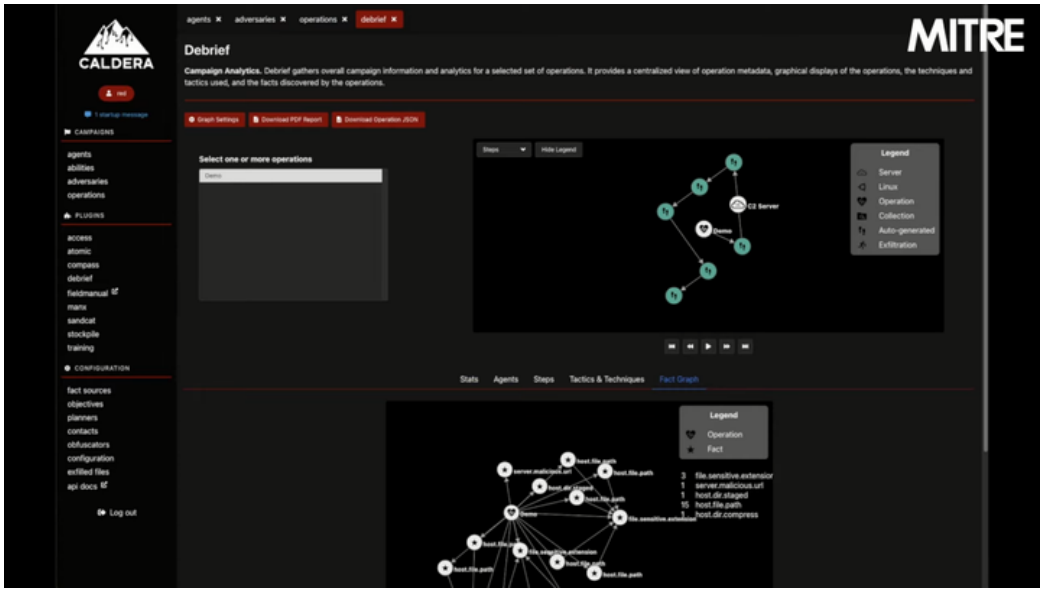


Volatility: https://www.volatilityfoundation.org/
To perform an analysis of a hacked system with Volatility:
https://app.letsdefend.io/training/lessons/memory-forensics

CALDERA

Caldera is a platform where cyber attack methods created by MITRE can be applied. With this tool, various studies can be carried out by applying specific attack methods. For example, the caldera tool can be used for a blue team activity where the necessary attack method is applied and the measures that can be taken against this attack are investigated. With this tool, cyber defense techniques can be developed by performing attack simulations.

An example image of the Caldera tool is as follows:

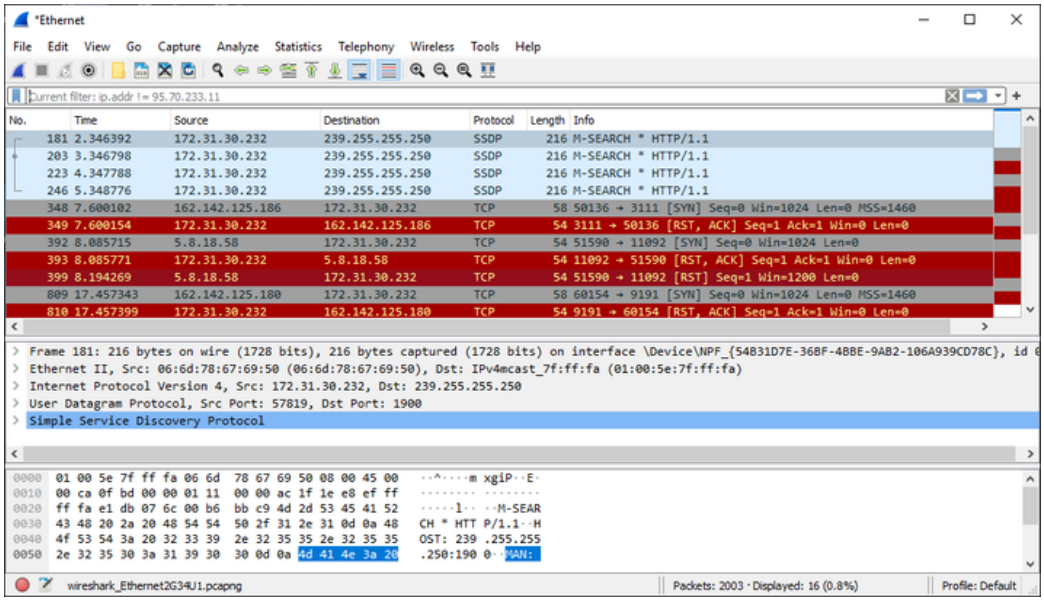


Caldera: https://caldera.mitre.org/

WIRESHARK

Wireshark is a tool that allows capturing, analyzing, and recording network packets passing through network interfaces on the system. The Wireshark tool, which has a long history, can be used for many purposes. For example, it can be used for testing purposes to see if the applications' ability to send data over the network is working. The Wireshark tool provides valuable information when used in cybersecurity-focused studies. For example, it can detect the IP address of the command and control server (C2 Server) with which malware running on the system communicates.

Wireshark tool is a tool with a graphical user interface (GUI). An example image of the Wireshark tool is as follows:

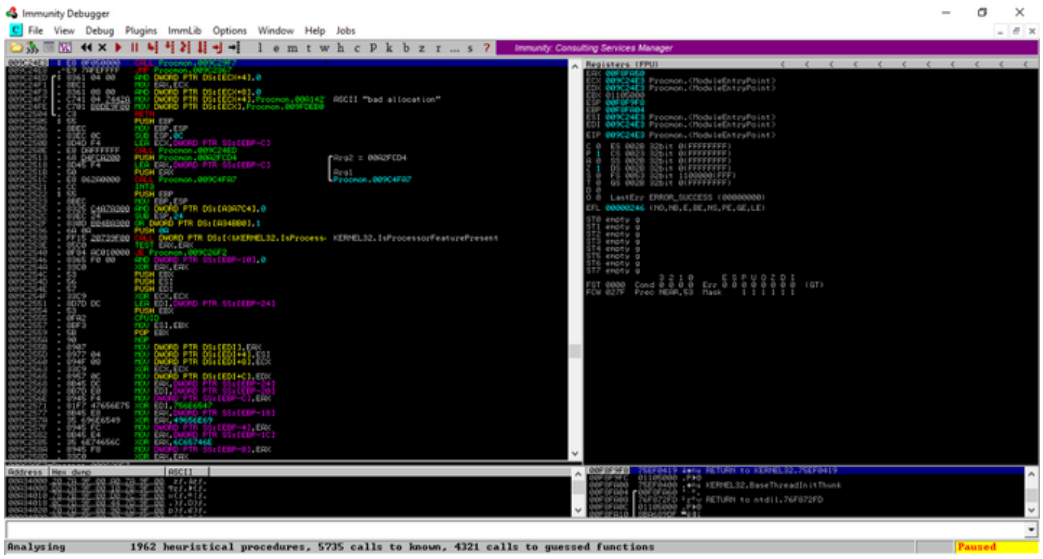


If you want to use Wireshark as a SOC Analyst, you can follow this free hands-on course: https://app.letsdefend.io/training/lessons/malware-traffic-analysis-with-wireshark

IMMUNITY DEBUGGER

Immunity Debugger is a dynamic analysis tool that allows executables to be analyzed at the assembly language level with reverse engineering techniques. In order to use this tool in analysis processes, it is necessary to have technical knowledge about low-level topics such as assembly language, processor working principle, and system architecture. Having this information, the analyst has the opportunity to dynamically analyze the malware at the processor level during operation. In this way, the behavior and malicious activities of the malware can be seen.

The Immunity Debugger tool is a tool with a graphical user interface (GUI). An example image of the Immunity Debugger tool is as follows:



Immunity Debugger: https://www.immunityinc.com/products/debugger/