Memory Forensic comparison Volatility and Autopsy

Max Kaeo Soto[1];
[1]University of Hawaii West Oahu

Abstract

The tools being looked at are Autopsy and Volatility. To keep the testing similar all resources will be the same this includes Virtual machine software same amount of CPU cores and Memory dedicated to the Virtual Machine. The Virtual machines that will be used to conduct tests are Kali Linux and Windows 10. Careful consideration was taking into place so that each tool was supported by each operating system. Each test will be using the same memory payload for each tool. Volatility was found not to have that much of a difference between the Kali and Windows 10 VM. Both versions of Volatility performed the same. This includes the Syntax and how you run the program. For Autopsy both versions are vastly different. The Linux version uses a web interface opposed to the Windows version. The Windows version also displays more data and can support more form of forensic evidence. Its best to use the windows version of Autopsy. And for Volatility it comes down to self-preference Kali Linux or Windows.

Research Design & Data Collection

- Qualitative Research method used.
- Programs for memory forensic tested Volatility and Autopsy.
- Virtual machines Kali Linux and Windows 10.
- Memory file used was a Windows XP image.

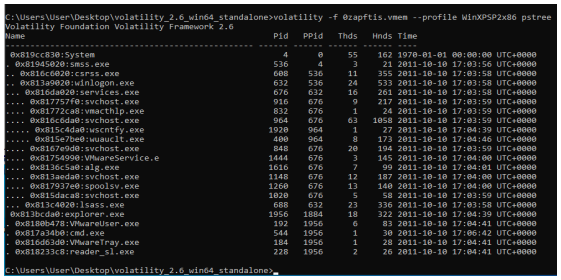


Figure 2. Windows 10 Volatility

Introduction & Research Question

Introduction
This serves to find if there are differences between Memory forensic applications when there ran on different Operating System's. Each application will run the same payload to keep results consistent. From there we can conclude if there is a difference in data and performance.

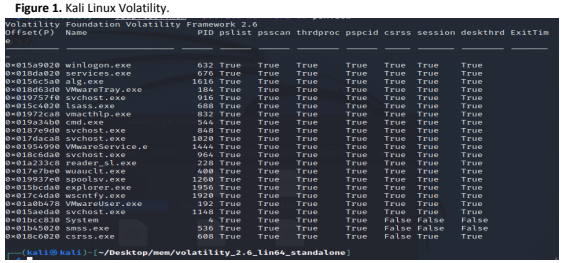
Research Question
Is there a difference between Memory forensic applications when run from different Virtual machines and which performs better.

Hypothesis
Both Memory Forensic Programs have their Pros and Con's. Are there any difference's when on different OS's and when it comes to displaying and finding important information.

Results

Volatility Framework on Kali Linux and Windows 10 operate the same way, and both display the same data. The same syntax was used to operate and install each of the programs. In figure 1 and 2 displays data discovered using Volatility from each of the virtual machines. Both display the same data. It was discovered that there is no difference between each installation. There were some noticeable difference between Kali Linux and Windows 10 version of Autopsy. Some of the Key differences is the This includes memory image support as well as user interface. There was no identifiable data between the two virtual machines.

Figure 1. Kali Linux Volatility.



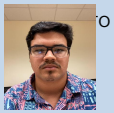
Discussion

Future considerations would be to set up a machine and capture live memory from it. This could be done by implementing additional programs that can capture memory like FTK imager, dd or FTK imager lite.
Also, the testing of more Forensic and memory analysis tools. Also testing Physical hardware with data on it like a Hard drive or Flash drive.

Conclusions

Volatility was tested with a memory sample of Windows XP. Each version of Volatility displayed the same data, and the performance were the same when executing options. Each of the versions of Volatility are command line only and they use the exact same syntax. Kali Linux does come with volatility preinstalled and must install it through the command line. Frequent users of Linux who often install programs via terminal or experience cyber security experts may find the Linux version more suitable. Users of the Windows 10 may find it slightly harder due to the fact that its command line only. After updating Kali Linux version of Autopsy there was some key differences between the windows 10 version. This includes memory image support as well as user interface. There was no identifiable data between the two virtual machines. The Windows 10 installation displayed more useful data and produced results. In terms of performance in the Windows 10 took much longer to parse the data. While in the Kali version you parse data as you navigate through the web interface

Contact



Max Kaeo Soto
University of Hawaii West Oahu
Email: maxsoto@hawaii.edu
Phone: 808 397-0631

References

1. Tien, C. W., Liao, J. W., Chang, S. C., & Kuo, S. Y. (2017, August). Memory forensics using virtual machine introspection for Malware analysis. In *2017 IEEE Conference on Dependable and Secure Computing* (pp. 518-519). IEEE
1. *What does computer memory (RAM) do?* Crucial. (n.d.). Retrieved September 28, 2021, from https://www.crucial.com/articles/about-memory/support-what-does-computer-memory-do
2. Thomas, S., Sherly, K. K., & Dija, S. (2013, April). Extraction of memory forensic artifacts from windows 7 ram image. In *2013 IEEE Conference on Information & Communication Technologies* (pp. 937-942). IEEE.
3. Uroz, D., & Rodríguez, R. J. (2020). On challenges in verifying trusted executable files in memory forensics. *Forensic Science International: Digital Investigation*, *32*, 300917
4. Lewis, N., Case, A., Ali-Gombe, A., & Richard III, G. G. (2018). Memory forensics and the windows subsystem for linux. *Digital Investigation*, *26*, S3-S11.
5. Ruff, N. (2008). Windows memory forensics. *Journal in Computer Virology*, *4*(2), 83-100

6. Kamal, K. M. A., Alfadel, M., & Munia, M. S. (2016, December). Memory forensics tools: Comparing processing time and left artifacts on volatile memory. In *2016 International Workshop on Computational Intelligence (IWCI) (pp. 84-90). IEEE*