FMEM Perl Front-End

Gabe Kahen, Ted Rambert, Tim Lam

Table of Contents

Executive Summary 3

Current Condition Overview 4

Tool Selection 5

Tool Development 6

Conclusion 7

# Executive Summary

FMEM is a kernel module that allows users to read the physical memory on a Linux machine. The major difference between FMEM and other similar kernel modules is that FMEM doesn’t have any limitations. FMEM-PFE is a front end for FMEM written in Perl that provides an alternative means of accessing the /dev/fmem device other than through the terminal.

# Current Condition Overview

The tool is currently in a functional condition. Current features include the ability to choose the destination for the memory image, where the image is saved as the date the memory image was taken. The tool automatically determines the amount of memory installed. For debugging purposes, the terminal output produced by the GUI is displayed in the background.

# Tool Selection

While taking 4050-581 Computer System Forensics at the Rochester Institute of Technology, we learned about the process by which memory can be captured and analyzed off of a machine. One of our assignments required us to find a tool capable of copying the entirety of physical memory off of a machine. For this task, we found FMEM, a part of the Foriana toolkit[[1]](#footnote-1). We felt that the process of copying memory off of the fmem device could be simplified with the addition of a graphical front-end, which is why we decided to create FMEM-PFE.

# Tool Development

First we started with a basic TK window, with a destination and memory field, including an exit and copy button. However, you had to manually type in the destination and the number of blocks of memory to copy. Then we created a window where the user could choose where to save the file. Lastly, we detected the amount of memory in MB and allowed the user to specify the amount of memory to copy. The name of the memory image is as follows: currentdate\_memory.dd .

# Conclusion

The FMEM device is an important tool in procuring memory from a computer. FMEM-PRE is built on top of FMEM in order to make the acquisition of that memory a little less painful for the typical forensic analyst, by providing a hassle-free frontend application.

1. http://hysteria.sk/~niekt0/foriana/ [↑](#footnote-ref-1)