Programming 4: Malware Forensics

Instructor: Guanhua Yan
Due date: Finishing demo by November 18, 2016 (Friday).

The goal of this project assignment is to learn how to find traces of malware infection using memory forensic tools.

Step 1: Create a virtual machine. The choice of OS running inside the VM depends on the type of malware you want to investigate.

Step 2: Run malware inside the virtual machine.
You can find real malware samples from the Internet (e.g., https://github.com/ytisf/theZoo/tree/master/malwares/Binaries and http://contagiodump.blogspot.com/). The recent Mirai source code can be found at: https://github.com/jgamblin/Mirai-Source-Code.
When you run malware, please turn off the network capabilities in case that the malware gets out of the sandbox.

Step 3: Dump the memory of the virtual machine both before the malware runs and during the time when the malware is running.

Step 4: Using the volatility tool (http://www.volatilityfoundation.org/) to analyze the memory dumps.

Step 5: Compare the memory footprints and identify traces of malware execution.

For evaluation of this project, each student needs to do the demo in my office for up to 5 minutes. The evaluation criteria include:

(1) your ability of finding any trace of the malware in the memory (70 points);
(2) your ability of mitigating any security-related risks when analyzing the malware (10 points);
(3) a real malware is analyzed (10 points);
(4) your knowledge about the malware based on your analysis (10 points).