B5 Random Access Memory Persistence: When Does It Go Away?

Walter T. Hart, MBA, 149 Hamerton Avenue, San Francisco, CA 94131*

After attending this presentation, attendees will understand some basic principles and behaviors related to the persistence of computer random access memory.

This presentation will impact the forensic science community by providing a basic understanding of what forensics artifacts can be found in Random Access Memory (RAM) data captures and what affects its persistence when a computer is shut down, power is removed, or other events occur that can affect RAM.

RAM is known to potentially contain many forensic artifacts related to investigations such as incident response, child exploitation, and almost all other computer forensic cases. These artifacts can include evidence such as images or partial images, malware code or partial malware code, passwords or password hashes, and words used in a variety of computer applications.

There have been a number of articles written over the years about capturing and analyzing RAM. Indeed, there are several groups providing week-long "introductory" classes in RAM capturing and analyzing. There are also articles published now on when RAM may be still available for capture when, for years, assumptions were made that RAM would be cleared, such as when computers are shut down.

This presentation will examine scenarios when RAM appears to persist after shutdown, re-boot, and removal of power. Testing is done where RAM is captured when it is known to be clear after using the computer in a variety of shutdown scenarios including, but not limited to: normal shutdown; pulling the plug; normal shutdown followed by pulling the plug; those scenarios and removing the RAM modules from the computer; etc. These tests are also performed on a laptop computer which adds the element of battery power to the above scenarios.

Possible complicating issues are examined including data that is cached on storage media that can still be analyzed for data from RAM, but also may populate captures from some or all data capture utilities. This cached data is compared to RAM captures. Further tests are done with the cached files eliminated to verify that what is seen in the RAM capture is strictly from volatile data and not cross-populated with non-volatile stored data from memory cache files.

The need for additional research and ideas about future research in this area of forensics will be presented.

RAM, Memory, Random Access Memory

 ** Presenting Author*