Importance of Live Incident Response Forensics

A typical application is a set of instructions which requires to be loaded in memory (RAM) for execution. The application can be referred as a process during execution, for which the system allocates a range of physical memory (RAM) addresses.

Each process running on the system has its own address space which contains the state information of the process. Therefore, the contents of physical memory provide stateful information. Since the kernel state and other information pertaining to the execution of a program is maintained in the RAM, it is only available when the system is powered on.

Among many other reasons driven by changing computing environment, one key requirement that makes collecting the live evidence important is that the sophisticated malwares reside on RAM and do not store any information on the storage media (hard drive). Therefore, the live state is the only way to find more about the malware. The ephemeral content is lost when system is turned off or subjected to major state change, therefore Incident response forensics is very crucial and requires caution.

C program in memory*:

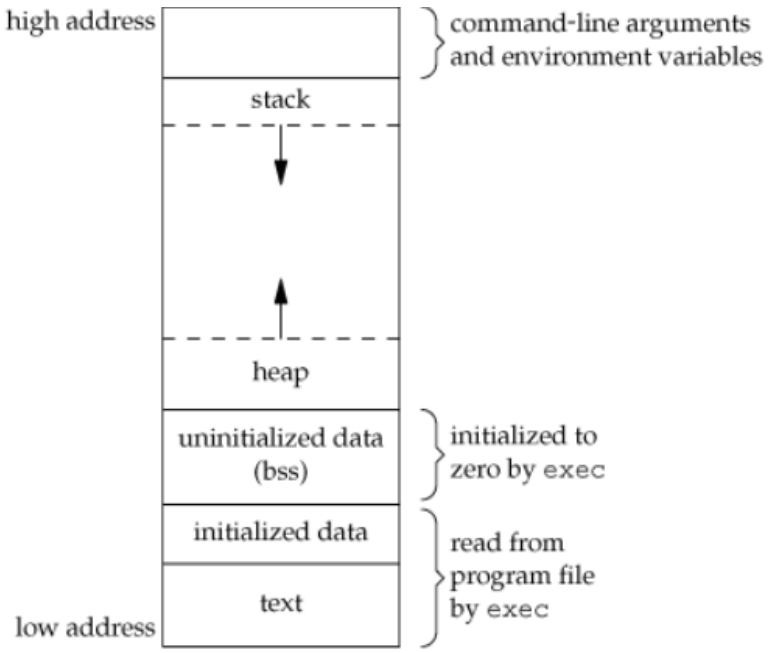

*Image Source: http://www.geeksforgeeks.org/