Volatile data – Source of Key Information

About the malicious program:

- The uncompressed machine code of the malicious program.
- Initialized Variables and their values. (Data Segment).
- Dynamically initialized variables and their values (Heap segment).
- Automatic function variables during execution. (Stack segment).

About the system state:

- Network information – IP address, routing table etc.
- Kernel modules – List of Loaded kernel modules and device drivers, their dependencies and binary locations.
- Logged in users.

A C-program in memory*:

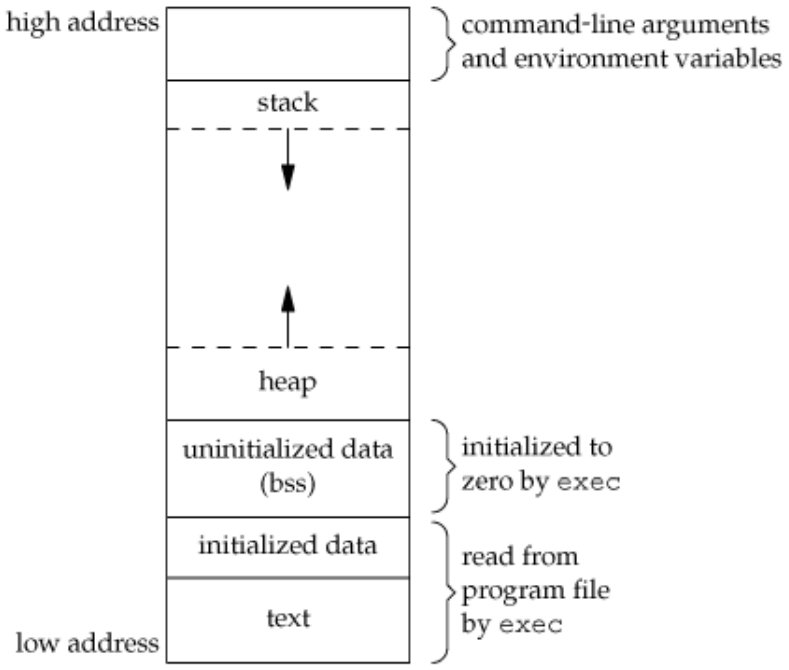

*Image Source: http://www.geeksforgeeks.org/memory-layout-of-c-program/