

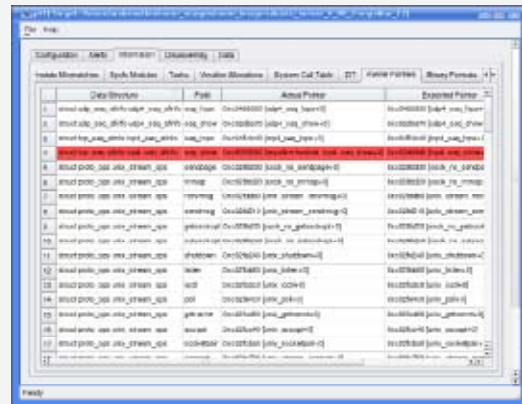


## Volatile Memory Analysis

**Volatile Memory Analysis** – The sophistication of software threats has increased to the point that traditional disk-based forensic analysis is no longer sufficient to detect malicious activities. Instead, volatile memory analysis is now a requirement to truly determine the integrity and trustworthiness of the running Operating System (OS). Through live examination of raw physical memory, malicious kernel modifications, such as those made by rootkits and other advanced malware, can be quickly identified and even removed. The application of volatile memory analysis complements existing forensic technologies, including those that examine persistent data on the hard drive or monitor user and application behavior.

Second Look provides a comprehensive view of the running OS, through the application of volatile memory analysis techniques. Second Look is capable of quickly identifying malicious kernel modifications that have been made to a running system through both existing and unknown methods of kernel alteration. Second Look scans the physical memory of a system looking for discrepancies between data structures and executable kernel code; all portions of the operating system kernel are processed, including: data, kernel code, and executable code belonging to device driver modules. Modifications detected by Second Look can include hidden processes, hidden kernel modules, and altered executable code.

Second Look also examines all of the executable code present in a host's volatile memory and identifies memory regions by classification, such as those regions likely belonging to encryption algorithms or containing encryption keys. Any identified discrepancies are displayed to the user in a graphical fashion with modifications highlighted. The user can then identify links between individual changes, system software, and attack methods.



**Collection Methods** – Second Look provides numerous methods for collecting and analyzing volatile system memory. Memory is collected from a host in real-time using any of the available methods including local, network, and hardware collection methods. Collected memory images can be archived for later analysis, or can be used to provide a current, comprehensive overview of the running operating system and volatile data structures.

**Early Adopters** – Second Look is being developed in conjunction with Johns Hopkins University Applied Physics Laboratory (JHU-APL) under a Small Business Technology Transfer (STTR) contract funded by the Air Force Research Laboratory. Early Adopter releases of Second Look are currently available, and will allow ongoing development of Second Look to be tailored to your usage requirements and operational needs. PA# 88 ABW-09-0098.