B8 Solid State Drive Technology and Applied Digital Forensics

John J. O'Brien, MA, United States Army, Cyber Counterintelligence Activity, 4553 Llewellyn Avenue, Fort Meade, MD 20755; and Sean P. O'Brien, BS*, Defense Computer Forensic Laboratory, 911 Elkridge Landing Road, Linthicum, MD 21090*

After attending this presentation, attendees will understand some principles of digital forensic methodologies when solid state drives are examined; will understand what the differences are compared to traditional rotating media; and will understand what new concepts may be put into operation and which old ones still work.

Solid state drives are becoming more commonplace. This new "old" technology is finding its way into the notebook computer market as well as enterprise systems, and it is important for forensic practitioners to be ready when they first encounter such a drive. This presentation will impact the forensic science community by preparing practitioners for when the first solid state drive hits a forensic lab.

The purpose of this presentation is to learn about the newest solid state drives and the forensic methodologies that may be applied to these technologies and to specifically answer the question: "What unique issues and challenges do solid state drives present to digital forensics?" A solid-state drive (SSD) is a data storage device that uses solid-state memory to store persistent data. Data on the SSD is interpreted by the installed Operating System (OS) and File System (FS) which presents the data to the user. High Proficiency SATA SSDs are being built in both a 2.5" and 1.8" form factors in capacities from 64-300GB. There are two different types of SSD technologies; the SLC (single level cell), and the MLC (multi-level cell) design. MLC doubles the capacity of flash memory by interpreting four digital states in the signal stored in a single cell – instead of the traditional (binary) two digital states. The forensic techniques for the SSDs may differ from those for traditional rotating media. Areas that will be discussed are: forensic tools for working with SSDs, the Flash File System (FSD), the translation and magic that occurs within the chip sets on the SSD to provide the data to the OS and FS for operations, the Host Protected Area (HBA), residual data, wear leveling rules, data streams, data carving, and recovering deleted file data. **Solid State, Digital Forensics, Computers**

 ** Presenting Author*