B26 Testing Tools to Erase Hard Drives for Reuse

James R. Lyle, PhD, and Craig Russell, MS, National Institute of Standards & Technology, 100 Bureau Drive Stop 8970, Gaithersburg, MD*

After attending this presentation, attendees will be made aware of some of the issues used in testing computer forensic tools used to erase hard drives before reuse of the hard drive.

The presentation will impact the forensic science community by increasing awareness in the community of the tool behaviors and limitations likely to be encountered when using tools to prepare digital media for reuse between cases.

The Computer Forensics Tool Testing (CFTT) project at the National Institute of Standards and Technology develops methodologies for testing computer forensic tools. A methodology for testing tools was developed that erases entire hard drives. Digital media used in the processing and analysis of digital data is often reused between cases. Good practice dictates that the reused media is completely erased between cases so that data from one case does not get mixed in with another case. Test methodologies have been developed to examine the behavior of drive wiping tools. By using this methodology an investigator should have confidence that the tool used to prepare storage disk drives for forensic reuse are in fact wiped of any remnants of earlier investigations.

The core requirement for a tool is the removal of all accessible data on the hard drive. At a minimum all visible sectors should be overwritten with new data that is forensically benign. Some tools may adhere to a policy that ignores hidden sectors (Host Protected Area (HPA) or Device Configuration Overlay (DCO) with the justification that as long as the hidden area is in place it is inaccessible and not likely to cause a problem. Other tools remove hidden areas and then overwrite the formerly hidden data.

An important feature, sometimes overlooked by tools, is the erase instruction built in to recent hard drives. ATA drives that implement the SECURE ERASE instruction can overwrite an entire hard drive with a single command. Our test methodology provides for testing tools that use either multiple WRITE commands or the SECURE ERASE command. There are several advantages to using the SECURE ERASE command; these include faster performance and the erasure of data from failed sectors. Sometimes a hard drive removes a failing sector from normal use and substitutes a new sector from a spare sector pool. The SECURE ERASE command can access the failed sector and remove any data that is present.

There are problems testing two often implemented tool features: multiple overwrites, overwrite verification. To determine if a tool actually completely overwrites a drive multiple times, the overwrite process would need to be intercepted at the end of each pass and the hard drive examined. This would have to be done by guesswork without special purpose equipment such as a bus monitor. For a tool that offers verification of the overwriting, a tester would need to determine that the tool can detect a failure of the overwrite process. This would require detection of the tool finishing the overwrite process and about to begin the verification pass, interruption the execution of the tool, modifying the hard drive being erased and then restarting the tool at the point of interruption. This might be possible by using a virtual machine, but the effort to check the operation of a verification feature may not be the best use of limited resources. The CFTT methodology ignores both features and only considers the basic functionality.

Digital Forensics, Software Testing, Media Erasure

 ** Presenting Author*