WiebeTech
by CRU

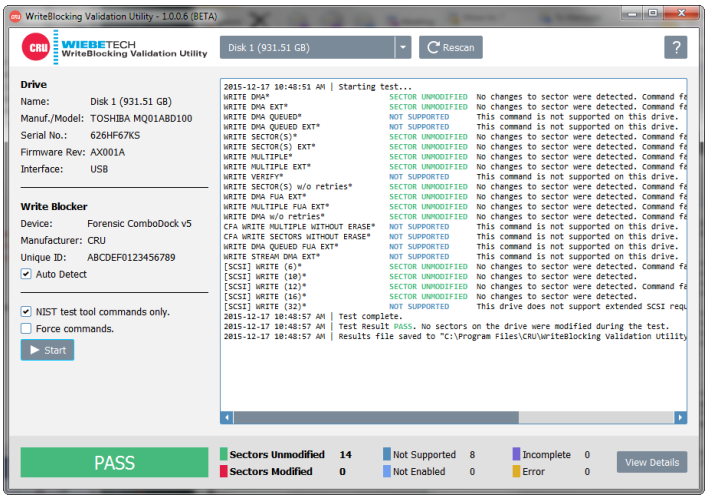
WiebeTech® WriteBlocking Validation Utility

The testing and validation of the tools used to acquire evidence has always been an important responsibility for forensic investigators. This is especially true of tools used in the relatively recent field of digital forensics, since the inner workings of such tools are not immediately obvious. Digital forensic tools (i.e. "write blockers") provide access to data on suspect media such as hard drives, while preventing spoliation of the data by blocking any write commands from a computer's OS that could alter it. Investigators typically adopt a "trust but verify" approach to their equipment, first by selecting tools from reputable manufacturers such as CRU®, and second by testing the tools before use in an investigation. Many organizations require such testing not only prior to first use, but before every new investigation in which the tool will be used. However, the test methods were until recently either unclear, overly time consuming, or inadequate to catch potential product flaws.

One common test method involves accessing a test drive through a write blocker and then writing files to the drive. Depending on the type of write blocking employed by the product, the files may appear to be successfully written. If the write blocker is functioning correctly, the files would disappear after cycling power on the product and remounting the drive, because the files were never actually written. This is a good basic test of the tool's ability to block the most common kinds of write commands, but it would not catch other types of commands that are potentially data-destructive.

A more thorough test would involve sending a wide range of commands to the attached drive, and then reading back the drive's data to see whether any of the commands were successful

in making changes. To that end, the National Institute for Standards in Technology (NIST) is developing a linux-based software utility that automates such a test. The linux utility sends a broad spectrum of data-altering commands to a test drive attached to a write blocker, and then provides a report on the results. This is a much more comprehensive test than is possible with a manual procedure like the one described above. Automation also reduces the chances of human error or inconsistency.



However, NIST's tool is a work in progress and not yet available to the public. Further, some users who could benefit from the tool may be discouraged from adopting it due to its command-line interface and its compatibility with linux only. Many forensic investigators work predominantly with Windows computers and software, and have asked for a Windows-native equivalent to NIST's useful utility.

CRU has responded to these requests by developing the WiebeTech WriteBlocking Validation Utility, a free downloadable software app for Windows. The WriteBlocking Validation Utility was developed specifically for Windows and features a user-friendly graphical user interface that makes it easy to test any write blocking product. A test can be started in seconds–just select the test drive from a drop-down box and then click START. The WriteBlocking Validation Utility sends a variety of commands to the drive, then remounts the drive and checks whether any of the commands were successful in altering data. The utility provides a simple PASS/FAIL overall result, as well as a log containing the individual results of each command type. The log file can also be saved to a text file for inclusion in a case report.

The WriteBlocking Validation Utility fulfils the forensic industry's need for an easy-to-use, Windows-based test app. Designed for maximum usefulness, it is not restricted to certain brands or models of write blockers. It can be used to test any write blocking product quickly and easily. It can be deployed quickly through an organization and adopted with minimal training.

The WiebeTech WriteBlocking Validation Utility is available as a free download from www.cru-inc.com.

For more information,
visit the CRU web site.

cru-inc.com
sales@cru-inc.com