WiebeTech
by CRU

USB 3.0 Write Blocking

by James Wiebe

The objective of any write blocking appliance is to provide an investigator with the ability to read evidence from a storage device without modifying the contents of that device. This is important for legal reasons, so that gathered digital evidence may be used in court with verifiable confidence. It is also important for eDiscovery, to provide continuity of procedure in the collection of digital information that is typically used in internal investigations, yet may one day be presented as evidence in court.

Different vendors have taken different technology paths to creating write blocking solutions. The most popular examples of existing write blockers include hardware devices from Guidance Software (the Tableau T8u) and CRU® (the WiebeTech® Forensic UltraDock v5.5).[1] Another strategy is to use operating system or third-party software tools to provide the write blocking. Linux is a straightforward example of a common operating system that will support write blocking at the system level, by user command.

At CRU, we have studied various approaches to write blocking throughout our history. USB write blockers present a unique market opportunity for us, and yet our existing technologies have proved challenging to migrate to provide native USB 3.0 solutions.

In developing a new write blocker for USB 3.0 storage devices and computer hosts, our product goals were simple: provide indisputable write blocking, provide verifiable operation to the user, and most significantly, provide write blocking to a USB 3.0-enabled computer host without affecting transfer performance of the storage device under investigation.

And then we discussed adding a big ‘plus’ to the product being developed: support multiple write blocked streams simultaneously. This would allow the user to acquire and copy from one external

USB 3.0 storage device while doing triage or independent inquiries and investigation into the contents of a second drive.

These goals have been achieved with our newly created CRU WiebeTech USB 3.0 WriteBlocker. It has the following features:

- A single host-side USB 3.0 Type B connection
- A power port (not required if collecting evidence off of low power USB 3 devices, such as thumb drives and many SSD drives)
- Two target-side USB 3.0 Type A ports
- Measured read rate of 400 MB/s
- Support of simultaneous dual channel acquisition and triage at full hard drive speeds
- Conveniently small physical size

Also, our device will not allow anything to mount until the presence of our driver has been validated through our proprietary encrypted communication methodology. Our USB 3.0 WriteBlocker, in the absence of that driver, is a firewall to all USB traffic, blocking communication between the computer host and the storage device(s) in question.

Clearly, this is a novel approach with real benefits to the user. Speed, performance, and system verifiability–all are inherent to the design and manufacture of the device.

INTRODUCING THE WIEBETECH WRITEBLOCKING VALIDATION UTILITY

In conjunction with this new product, we are releasing a new freeware write block testing software tool. Based on the constructs that NIST has defined as part of their public Linux-based testing tool, our software product is capable of testing any write blocker of any manufacturer. We've followed NIST recommendations exactly, and we've also added a testing mode that includes additional commands not covered by NIST's tools so an even more thorough write block test may be performed.

The WWVU software runs on Windows, the operating system most used by criminal and eDiscovery forensics investigators.

SUMMARY

The CRU WiebeTech USB 3.0 WriteBlocker provides a high performance solution for accessing information from USB 3.0 storage devices. It supports multiple attachment streams, all write blocked, so that cost of ownership is reduced, and investigations can be conducted more efficiently. It is physically small and uses a technology designed by CRU that allows transfers at virtually the same speed as the target device in a real world environment.

[1] WiebeTech was founded by the author, James Wiebe. WiebeTech is also a brand of CRU.

For more information,
visit the CRU web site.

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