FORENSIC DATA ACQUISITION WITH THE FRED™ USB 3.1 HOTSWAP™ TRAYS

Author: Sara Treleven – Forensic Examiner II, Digital Intelligence, Inc.

Digital Intelligence (aka, "DI") FRED™ forensic workstations are a powerful integration of high-performance hardware and software components purpose built for digital forensics. The new generation of FRED systems includes versatile high-performance USB 3.1 HotSwap™ trays for accessing 3.5" or 2.5" SATA hard drives. These trays can be switched from a general purpose read/write to a write-blocked "forensic mode" for secure, high-speed digital evidence acquisitions.

THE PROBLEM: REDUCING THE FORENSIC IMAGING BACKLOG

As forensic investigators, we all share the pain of time and again lacking enough imaging equipment, especially when it really matters. Remember that time you showed up in the field and realized you were a few duplicators short? How about that one computer with multiple drives and analysis needed to be completed yesterday while your client was impatiently tapping their feet behind you? And of course the times when you're staring at a mountain of drives to image and your coworkers are hogging all of the duplicators.

Between an ever-growing backlog of hard drives to image and a lack of dedicated imaging equipment, FRED is on your side. New for 2019, FRED forensic workstations are built with new USB 3.1 HotSwap trays. These trays can be used as general purpose drive slots for data transfer – or switched to a write-blocked "forensic" mode for evidence acquisition. A standard FRED workstation includes four USB 3.1 HotSwap trays, giving you the capacity to image multiple drives simultaneously. Combining multiple USB 3.1 HotSwap trays with the UltraBay 4 write-blocker gives FRED unmatched forensic imaging performance. Whether you're in the lab on your FRED workstation or out in the field with our microFRED, a simple flip of the HotSwap tray read/write switch and you're set to use the forensic imaging tool of your choice and sail right into your analysis and reporting faster than before.

As part of our normal, rigorous product development process as well as to ensure the compatibility of popular forensic imaging tools with FRED HotSwap trays, we performed testing on a FRED forensic workstation running Windows 10 with 64GB RAM, an Asus Tek X299 motherboard, and an Intel i7 processor with eight physical cores and clock speed of 3.80GHz clock speed.

TESTING METHODS AND TOOLS

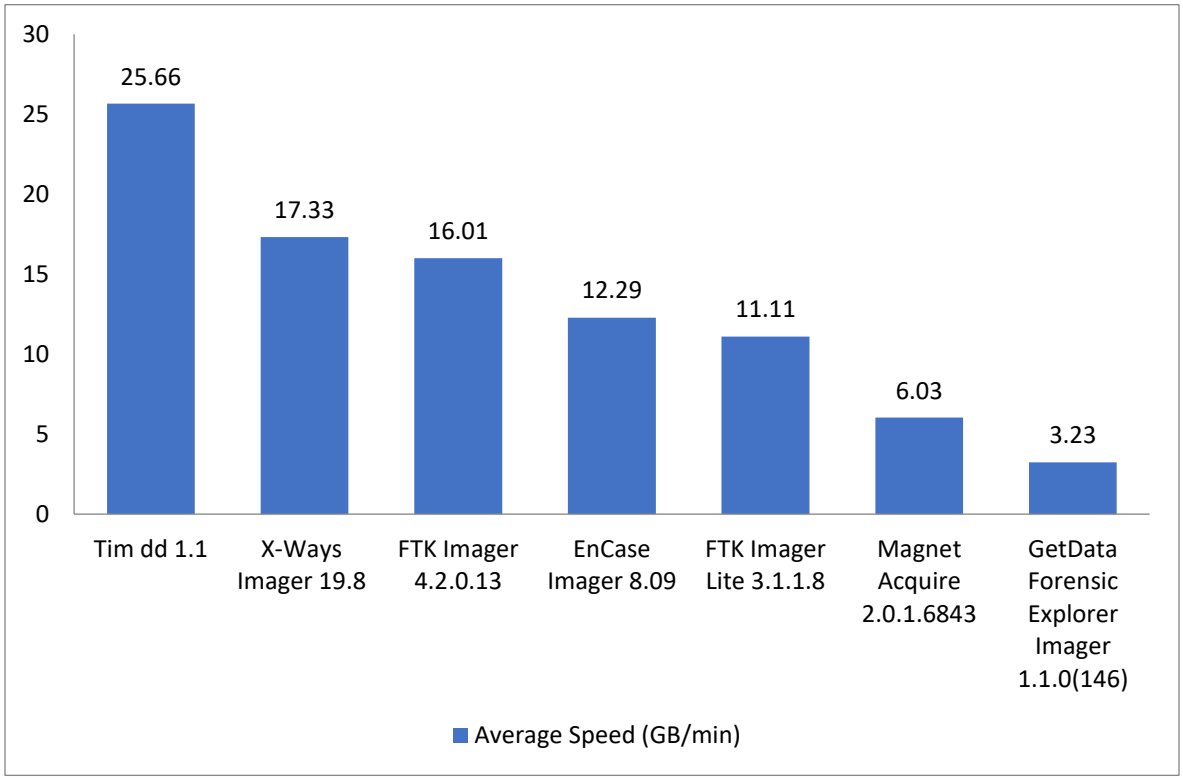
A Samsung 860 Pro solid state drive was filled with medium compressible data and used as the source drive. The source drive was placed in a FRED write-blocked USB 3.1 HotSwap tray. Physical images were created using EnCase Imager, FTK Imager, FTK Imager Lite, GetData Forensic Explorer Imager, Magnet Acquire, Timdd (a command line version of TIM used for forensic product testing), and X-Ways Imager to

another local Samsung 860 Pro solid-state drive in a SATA connected hot swap tray. Uncompressed images were created using both raw and E01 image format.

This testing was primarily focused on compatibility of forensic imaging tools with the write-blocked HotSwap trays, reproducibility of consistent imaging speeds of each tool, and verification of forensic images created. The imaging speed in GBs per minute was calculated from each log file created.

GOAL ACHIEVEMENT AND TEST RESULTS

The following data table shows calculated forensic imaging speeds in GB/min. Test results reflect imaging speeds that are consistent with speeds measured during initial drive tray development using the same forensic imaging software. Additionally, the recent test results yielded rates which exceeded those measured when imaging with the UltraBay 4 and the imaging software products listed below.



SUMMARY

All verified forensic images created have shown consistent imaging speeds relative to the tool being used to assure repeatable and reliable results. Imaging with our write-blocked USB 3.1 HotSwap trays in conjunction with devices on the UltraBay greatly increases the forensic imaging capacity of each FRED system, which in turn frees up more imaging equipment in your lab and provides you with more imaging options while in the field. When combined with the UltraBay 4, write-blocker USB 3.1 HotSwap trays provide a practical, high performance solution to forensic imaging backlogs.

For more information about this topic or any of the testing Digital Intelligence performs on FRED systems, please contact us via our webpage ticketing system.

ABOUT THE AUTHOR

Sara Treleven has been on staff at Digital Intelligence since 2013. She is an EnCE and CFCE certified forensic examiner, mountain biker, car enthusiast, fisherperson, animal lover, and global traveler.

Test Notes:

(1) *At this time, compression ratios, I/O data, and imaging speeds using encryption were not tested.*