

Computer Forensics Tool Testing Handbook



NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

Contact: James Lyle

Computer Forensics Tool Testing Program
Office of Law Enforcement Standards
National Institute of Standards and
Technology

HAVE YOUR COMPUTER FORENSICS TOOLS BEEN TESTED?

NIJ, DHS, and other LE practitioners partnered with NIST to create a testing program for computer forensics tools. It is called the Computer Forensics Tool Testing (CFTT) program. The CFTT tests tools to determine how well they perform core forensics functions such as imaging drives and extracting information from cell phones.

Benefits:

- When you use a tested tool, you can be assured what the tool's capabilities really are.
- If a tool has limitations, you will know what they are so you can take appropriate action (e.g., use another tool, use additional procedures, etc.)
- You have a head start on validating the tool for use in your lab

This booklet contains the results for tests performed under the CFTT program. The tests are organized by functional area tested (e.g., disk imaging tools or cell phone acquisition tools). Within each functional area, the tools are listed alphabetically.

The CFTT continues to test tools. See <http://www.ojp.usdoj.gov/nij/publications/welcome.htm> (select computer forensics tools testing) or www.cftt.nist.gov for the current list. The CFTT site also contains the specification against which the tools are tested and the testing software and complete methodology.

TABLE OF CONTENTS

Disk Imaging

- Logicube Forensic Talon Software Version 2.43
- BlackBag MacQuisition 2.2
- EnCase 6.5
- EnCase LinEn 6.01
- EnCase 5.05f
- FTK Imager 2.5.3.14
- DCCldd (Version 2.0)
- EnCase 4.22a
- EnCase LinEn 5.05f
- IXImager (Version 2.0)
- dd FreeBSD
- EnCase 3.20
- Safeback 2.18
- Safeback (Sydex) 2.0
- dd GNU fileutils 4.0.36

Forensic Media Preparation

- Darik's Boot and Nuke 1.0.7
- Voom HardCopy II (Model XLHCPL-2PD Version 1.11)
- WiebeTech Drive eRazer: DRZR-2-VBND & Drive eRazer PRO Bundle

Write Block (Software)

- ACES Writeblocker Windows 2000 V5.02.00
- ACES Writeblocker Windows XP V6.10.0
- PDBLOCK Version 1.02 (PDB_LITE)
- PDBLOCK Version 2.00
- PDBLOCK Version 2.10
- RCMP HDL V0.4
- RCMP HDL V0.5
- RCMP HDL V0.7
- RCMP HDL V0.8

Write Block (Hardware)

- T4 Forensic SCSI Bridge (FireWire Interface)
- T4 Forensic SCSI Bridge (USB Interface)
- Tableau T8 Forensic USB Bridge (FireWire Interface)
- Tableau T8 Forensic USB Bridge (USB Interface)
- FastBloc FE (USB Interface)
- FastBloc FE (FireWire Interface)
- Tableau T5 Forensic IDE Bridge (USB Interface)
- Tableau T5 Forensic IDE Bridge (FireWire Interface)
- Tableau Forensic SATA Bridge T3u (USB Interface)
- Tableau Forensic SATA Bridge T3u (FireWire Interface)
- Tableau Forensic IDE Pocket Bridge T14 (FireWire Interface)
- WiebeTech Forensic SATADock (FireWire Interface)
- WiebeTech Forensic SATADock (USB Interface)
- WiebeTech Forensic ComboDock (USB Interface)
- WiebeTech Forensic ComboDock (FireWire Interface)
- WiebeTech Bus Powered Forensic ComboDock (USB Interface)
- WiebeTech Bus Powered Forensic ComboDock (FireWire Interface)
- Digital Intelligence UltraBlock SATA (FireWire Interface)
- FastBloc IDE (Firmware Version 16)
- MyKey NoWrite (Firmware Version 1.05)
- ICS ImageMasster DriveLock IDE (Firmware Version 17)
- WiebeTech FireWire DriveDock Combo (FireWire Interface)
- Digital Intelligence Firefly 800 IDE (FireWire Interface)
- Digital Intelligence UltraBlock SATA (USB Interface)

Mobile Devices

- BitPim – 1.0.6 official
- MOBILedit! Forensics 3.2.0.738
- Susteen DataPilot Secure View 1.12.0
- Final Data – Final Mobile Forensics 2.1.0.0313
- Paraben Device Seizure 3.1
- Cellebrite UFED 1.1.05
- Micro Systemation .XRY 3.6
- Guidance Software Neutrino 1.4.14
- Paraben Device Seizure 2.1
- Susteen DataPilot Secure View 1.8.0

TEST REPORT FOR:
**LOGICUBE FORENSIC TALON SOFTWARE VERSION
2.43**

January 2010

The CFTT Project tested the Logicube Forensic Talon Software Version 2.43 against the Digital Data Acquisition Tool Specification available at: http://www.cfft.nist.gov/disk_imaging.htm

Our results are:

Except for one test case, DA-01-PCMCIA, the tested tool acquired all visible and hidden sectors completely and accurately from the test media without anomaly. The following anomaly was observed:

- Data was inaccurately acquired over the PCMCIA interface (DA-01-PCMCIA).

For a complete copy of the report, go to:

<http://www.ojp.usdoj.gov/nij/pubs-sum/228981.htm>

Vendor information:

Logicube

<http://www.logicube.com/>

TEST REPORT FOR: **BLACKBAG MACQUISITION 2.2**

September 2009

**The CFTT Project tested the BlackBag MacQuisition 2.2 against the Digital Data Acquisition Tool Specification available at:
http://www.cfft.nist.gov/disk_imaging.htm**

Our results are:

The tool acquired the source drives accurately except for acquiring a drive with faulty sectors. However, several tool anomalies were observed:

- In one distributed version of MacQuisition 2.2 SHA1 acquisition hashes on the PowerPC architecture are computed incorrectly (DA-06-FW).
- The last hash in a series of block hashes may be omitted (DA-06-SATA28, DA-08-SATA28, DA-08-SATA28-INTEL, DA-09, and DA-09-INTEL).
- Acquisition hashes may be computed incorrectly (DA-06-SATA48, DA-06-SATA48-INTEL, and DA-08-SATA48).
- Block hashes may be computed incorrectly (DA-06-FW, DA-06-FW-INTEL, DA-06-USB, DA-06-USB-INTEL, DA-09, DA-09-INTEL, DA-09-134, and DA-09-134-INTEL).
- The ranges of data over which block hashes are computed are logged inaccurately (DA-06-FW, DA-06-FW-INTEL, DA-06-SATA28, DA-06-USB, DA-06-USB-INTEL, DA-08-DCO, DA-08-SATA28, DA-08-SATA28-INTEL, DA-09, DA-09-INTEL, DA-09-134, and DA-09-134-INTEL).

- Log files are incomplete when acquisitions are written to devices with insufficient space (DA-12).
- The sectors hidden by a device configuration overlay (DCO) or host protected area (HPA) are not acquired (DA-08-DCO, DA-08-SATA28, DA-08-SATA28-INTEL, and DA-08-SATA48).
- Data is not skipped as directed by the skip parameter (DA-07-PART).
- Good sectors in the same block as a faulty sector are not acquired, and other data is written in their place (DA-09, DA-09-INTEL, DA-09-134, and DA-09-134-INTEL).
- When a faulty sector is encountered, a block of sectors equal in size to the imaging block size is omitted from the acquisition image (DA-09, DA-09-TPIPE, and DA-09-134).
- Data for faulty sectors may be replaced in the image file with data from an undetermined source (DA-09, DA-09-INTEL, DA-09-TPIPE, and DA-09-TPIPE-INTEL).
- In the image file, sectors surrounding a faulty sector may contain data that has been previously acquired (DA-09, DA-09-INTEL, DA-09-TPIPE, and DA-09-TPIPE-INTEL).

For a complete copy of the report, go to:

<http://www.ojp.usdoj.gov/nij/pubs-sum/228223.htm>

Vendor information:

BlackBag Technologies, Inc.

<http://www.blackbag.com/>

TEST REPORT FOR: **ENCASE 6.5**

September 2009

The CFTT Project tested the EnCase 6.5 against the Digital Data Acquisition Tool Specification available at: http://www.cftt.nist.gov/disk_imaging.htm

Our results are:

Except for four test cases (DA-07, DA-08, DA-09, and DA-14), the tested tool acquired all visible and hidden sectors completely and accurately from the test media without any anomalies. The following six anomalies were observed:

- If a logical acquisition is made of an NTFS partition, a small number of sectors, seven in the executed test, appear in the image file twice, replacing seven other sectors that fail to be acquired (DA-07-NTFS).
- If a logical acquisition is made of an NTFS partition, the last physical sector of the partition is not acquired (DA-07-NTFS).
- If the tool attempts to acquire a defective sector with an error granularity greater than one sector, some readable sectors near the defective sector are replaced by zeros in the created image file (DA-09-02, DA-09-16, and DA-16-64).
- HPA and DCO hidden sectors can be acquired completely if FastBlock SE is used as a write blocker (DA-08-ATA28) during an acquisition. However, use of some write blockers such as FastBlock FE that do not remove hidden areas prevent the acquisition of sectors hidden in an HPA or DCO (DA-08-ATA48 and DA-08-DCO).

- For some partition types (FAT32 and NTFS) when imaged as a logical (partition) acquisition, if a logical restore is performed there may be a small number of differences in file system metadata between the image file and the restored partition (DA-14-F32, DA-14-F32X and DA-14-NTFS). The differences can be avoided by removing power from the destination drive instead of doing a normal power down sequence (DA-14-F32-ALT, DA-14-F32X-ALT, and DA-14-NTFS-ALT).
- For some removable USB devices (Flash card and thumb drive) that have been physically acquired, there may be a small number of differences in file system metadata between the image file and the restored device (DA-14-CF and DA-14-THUMB).

For a complete copy of the report, go to:

<http://www.ojp.usdoj.gov/nij/pubs-sum/228226.htm>

Vendor information:

Guidance Software, Inc.

<http://www.guidancesoftware.com/>

TEST REPORT FOR: ENCASE LINEN 6.01

October 2008

The CFTT Project tested the EnCase LinEn 6.01 against the Digital Data Acquisition Tool Specification available at:
http://www.cftt.nist.gov/disk_imaging.htm

Our results are:

Except for two test cases (DA-08 and DA-09), the tested tool acquired all visible and hidden sectors completely and accurately from the test media. The two exceptions are the following:

- Up to seven sectors contiguous to a defective sector may be replaced by zeros in the acquisition (DA-09-1 and DA-09-2).
- The sectors hidden by a device configuration overlay (DCO) are not acquired (DA-08-DCO).

For a complete copy of the report, go to:
<http://www.ojp.usdoj.gov/nij/pubs-sum/224147.htm>

Vendor information:
Guidance Software, Inc.
<http://www.guidancesoftware.com/>

TEST REPORT FOR: **ENCASE 5.05F**

June 2008

The CFTT Project tested the EnCase 5.05f against the Digital Data Acquisition Tool Specification available at: http://www.cftt.nist.gov/disk_imaging.htm

Our results are:

Except for three test cases (DA-07, DA-09, and DA-14), the tested tool acquired all visible and hidden sectors completely and accurately from the test media without any anomalies. The following five anomalies were observed:

- If a logical acquisition is made of an NTFS partition, a small number of sectors, seven in the executed test, appear in the image file twice, replacing seven other sectors that fail to be acquired (DA-07-NTFS).
- If a logical acquisition is made of an NTFS partition, the last physical sector of the partition is not acquired (DA-07-NTFS).
- If the tool attempts to acquire a defective sector with an error granularity greater than one sector, some readable sectors near the defective sector are replaced by zeros in the created image file (DA-09-02, DA-09-16, and DA-16-64).
- If the tool attempts to acquire a defective sector from an ATA drive while using FastBloc SE to write block the drive, no notification of faulty sectors is given to the user.

- For some partition types (FAT32 and NTFS) that have been imaged as a logical (partition) acquisition, if a logical restore is performed there may be a small number of differences in file system metadata between the image file and the restored partition (DA-14-F32, DA-14-F32X and DA-14-NTFS). The differences can be avoided by removing power from the destination drive instead of doing a normal power down sequence (DA-14-F32-ALT, DA-14-F32X-ALT and DA-14-NTFS-ALT).

For a complete copy of the report, go to:

<http://www.ojp.usdoj.gov/nij/pubs-sum/223433.htm>

Vendor information:

Guidance Software, Inc.

<http://www.guidancesoftware.com/>

TEST REPORT FOR: **FTK IMAGER 2.5.3.14**

June 2008

The CFTT Project tested the FTK Imager 2.5.3.14 against the Digital Data Acquisition Tool Specification available at: http://www.cftt.nist.gov/disk_imaging.htm

Our results are:

Except for two test cases (DA-07 and DA-08), the tested tool acquired all visible and hidden sectors completely and accurately from the test media without any anomalies. In one test case (DA-25) image file corruption was detected, but the location of the corrupt data was not reported. The following four anomalies were observed in test cases DA-07, DA-08, and DA-25:

- If a logical acquisition is made of an NTFS partition, the last eight sectors of the physical partition are not acquired (DA-07-NTFS).
- The sectors hidden by a *host protected area* (HPA) are not acquired (DA-08- ATA28 and DA-08-ATA48).
- The sectors hidden by a *device configuration overlay* (DCO) are not acquired (DA-08-DCO).
- The location of corrupted data in an image file is not reported (DA-25).

For a complete copy of the report, go to:
<http://www.ojp.usdoj.gov/nij/pubs-sum/222982.htm>

Vendor information:

AccessData

<http://www.accessdata.com>

TEST REPORT FOR:
DCCIDD (VERSION 2.0, JUNE 1, 2007)

January 2008

**The CFTT Project tested the DCCidd (Version 2.0, June 1, 2007) against the Digital Data Acquisition Tool Specification available at:
http://www.cftt.nist.gov/disk_imaging.htm**

Our results are:

Except for two test cases, the tested tool acquired all visible and hidden sectors completely and accurately from the test media. The two exceptions are the following:

- Up to seven sectors contiguous to a faulty sector may be replaced by zeroes in the acquisition.
- The sectors hidden by a *Device Configuration Overlay* (DCO) are not acquired.

For a complete copy of the report, go to:
<http://www.ojp.usdoj.gov/nij/pubs-sum/220223.htm>

Vendor information:
DoD Cyber Crime Institute
<http://www.dc3.mil/>

TEST REPORT FOR: ENCASE 4.22A

January 2008

The CFTT Project tested the EnCase 4.22a against the Digital Data Acquisition Tool Specification available at: http://www.cftt.nist.gov/disk_imaging.htm

Our results are:

Except for three test cases (DA-07, DA-08, and DA-09), the tested tool acquired all visible and hidden sectors completely and accurately from the test media without any anomalies. The following five anomalies were observed:

- If a logical acquisition is made of an NTFS partition, a small number (seven in the executed test) appear in the image file twice, replacing other sectors (DA-07-NTFS).
- If a logical acquisition is made of an NTFS partition, the last physical sector of the partition is not acquired (DA-07-NTFS).
- If the tool attempts to acquire a defective sector, a sixty-four sector block of sectors containing the defective sector is replaced by zeroes in the created image file (DA-09).
- The sectors hidden by a *host protected area* (HPA) are not acquired (DA-08-ATA28 and DA-08-ATA48).
- The sectors hidden by a *device configuration overlay* (DCO) are not acquired (DA-08-DCO).

For a complete copy of the report, go to:

<http://www.ojp.usdoj.gov/nij/pubs-sum/221168.htm>

Vendor information:

Guidance Software, Inc.

<http://www.guidancesoftware.com/>

TEST REPORT FOR:
ENCASE LINEN 5.05F

January 2008

The CFTT Project tested the EnCase LinEn 5.05f against the Digital Data Acquisition Tool Specification available at:
http://www.cfft.nist.gov/disk_imaging.htm

Our results are:

Except for two test cases (DA-08 and DA-09), the tested tool acquired all visible and hidden sectors completely and accurately from the test media. The two exceptions are the following:

- Up to seven sectors contiguous to a defective sector may be replaced by zeroes in the acquisition (DA-09-1 and DA-09-2).
- The sectors hidden by a *device configuration overlay* (DCO) are not acquired (DA-08-DCO).

For a complete copy of the report, go to:
<http://www.ojp.usdoj.gov/nij/pubs-sum/221167.htm>

Vendor information:
Guidance Software, Inc.
<http://www.guidancesoftware.com/>

TEST REPORT FOR:
IXIMAGER (VERSION 2.0, FEB-01, 2006)

April 2007

**The CFTT Project tested the IXimager (Version 2.0, Feb-01, 2006) against the Digital Data Acquisition Tool Specification available at:
http://www.cftt.nist.gov/disk_imaging.htm**

Our results are:

The tested tool acquired all visible and hidden sectors completely and accurately from the test media. In the case of a hard drive with 22 defective sectors, the sectors of the image corresponding to the defective sectors were replaced with forensically benign content.

For a complete copy of the report, go to:
<http://www.ojp.usdoj.gov/nij/pubs-sum/217678.htm>

Vendor information:
U.S. Internal Revenue Service, Criminal Investigation Division,
Electronic Crimes Program
<http://www.ilook-forensics.org/homepage.html>

TEST REPORT FOR: DD FREEBSD

January 2004

The CFTT Project tested the dd FreeBSD against the Digital Data Acquisition Tool Specification available at: http://www.cftt.nist.gov/disk_imaging.htm

Our results are:

The tool shall make a bit-stream duplicate or an image of an original disk or partition. For all 32 test cases that were run, the dd utility produced an accurate bit-stream duplicate or an image on disks or partitions of all disk sectors copied.

The tool shall not alter the original disk. For all the test cases that were run, a SHA-1 hash was created on the source. Another SHA-1 hash was created on the source after the test case was run. In all cases, the hash codes matched (i.e., the source was not altered).

The tool shall be able to verify the integrity of a disk image file. This requirement does not apply to dd.

The tool shall log I/O errors. Assertions requiring read or write errors were not tested. The dd utility did produce a log message that there was no space left on the destination when the source was greater than the destination.

The tool documentation shall be correct. No errors were found in the documentation supplied.

For a complete copy of the report, go to:

<http://www.ojp.usdoj.gov/nij/pubs-sum/203095.htm>

Vendor information:

FreeBSD Foundation

<http://www.freebsd.org>

TEST REPORT FOR: **ENCASE 3.20**

June 2003

The CFTT Project tested the Encase 3.20 against the Digital Data Acquisition Tool Specification available at: http://www.cftt.nist.gov/disk_imaging.htm

Our results are:

The tool shall make a bit-stream duplicate or an image of an original disk or partition. EnCase, with one exception, correctly and completely copied all disk sectors to an image file in the test cases that were run. EnCase, with two other exceptions, correctly and completely restored all disk sectors to a destination drive in the test cases that were run. The three exceptions are the following:

- If the basic input/output system (BIOS) interface is chosen to access integrated drive electronics (IDE) hard drives on an older computer using a legacy BIOS that underreports the number of cylinders on the drive, then there may be a small area of sectors at the end of the drive that is not accessed. The sectors in this area are usually not used by commercial software. If direct access using the advance technology attachment (ATA) interface is chosen instead, EnCase accesses every sector of the hard drive.
- For certain partition types (FAT32 and NTFS), a logical restore of a partition is not an exact duplicate of the original. The vendor documentation states that a logical restore cannot be verified as an exact copy of the source and is not recommended when seeking to create a bit- stream duplicate of the source. For FAT32 partitions, two file system control values (not part of any data file) are adjusted during restoration of an image to a destination. This

adjustment is confined to about 8 bytes of sector 1 and the first sector of the FAT table (and FAT table backup copy) of the partition. For NTFS partitions, other changes were made to about 35 sectors of the partition. In no case was there any effect on sectors used in data files. All sectors of the image file accurately reflect the original sectors. These changes to a restored partition (logical volume) may be a consequence of the Windows shutdown process.

- In the Windows 2000 environment, a hard drive may appear to have fewer sectors than are actually available on the drive. This has two consequences. First, an attempt to restore an entire drive to a drive of an identical size from Windows 2000 does not restore all sectors imaged from the source to the destination. Second, if restoring to a drive larger than the source and the wipe excess sectors option is selected, then not all the excess sectors are wiped. Restoring in a Windows 98 environment did not exhibit this anomaly.

The tool shall not alter the original disk. For all the test cases that were run, EnCase never altered the original hard drive.

The tool shall be able to verify the integrity of a disk image file. For all of the test cases that were run, EnCase always identified image files that had been modified.

The tool shall log I/O errors. For all of the test cases that were run, EnCase always logged I/O errors.

The tool's documentation shall be correct. The tool documentation available was the EnCase Reference Manual, Version 3.0, Revision 3.18. In some cases, the software behavior was not documented or was ambiguous.

For a complete copy of the report, go to:

<http://www.ojp.usdoj.gov/nij/pubs-sum/200031.htm>

Vendor information:

Guidance Software

<http://www.guidancesoftware.com/>

TEST REPORT FOR: **SAFEBACK 2.18**

June 2003

The CFTT Project tested the Safeback 2.18 against the Digital Data Acquisition Tool Specification available at:
http://www.cfft.nist.gov/disk_imaging.htm

Our results are:

The tool shall make a bit-stream duplicate or an image of an original disk or partition. SafeBack, with two exceptions, copied all the disk sectors correctly and completely in the test cases that were run. The exceptions were the following:

- For a certain partition type (FAT32), two file system control values (not part of any data file) are adjusted as a side effect of the copy. This adjustment is confined to 8 bytes of sector 1 of the partition and had no effect on any sectors used in data files.
- If the basic input/output system (BIOS) interface is chosen to access integrated drive electronics (IDE) hard drives on an older computer using a legacy BIOS that underreports the number of cylinders on the drive, then some but not all sectors will be accessed in an area of the disk that is not used by either commercial software or Microsoft operating systems. If direct access using the advanced technology attachment (ATA) interface is chosen instead, SafeBack accesses every sector of the hard drive.

The tool shall not alter the original disk. For all the test cases that were run, SafeBack never altered the original hard drive.

The tool shall be able to verify the integrity of a disk image file. For all of the test cases that were run, SafeBack always identified image files that had been modified.

The tool shall log I/O errors. For all of the test cases that were run, SafeBack always logged I/O errors.

The tool's documentation shall be correct. The tool documentation available was the SafeBack Reference Manual, Version 2.0, Second Edition, October 2001. There was no documentation identified the software behavior was not documented or was ambiguous.

For a complete copy of the report, go to:

<http://www.ojp.usdoj.gov/nij/pubs-sum/200032.htm>

Vendor information:

New Technologies, Inc.

<http://www.forensics-intl.com/>

TEST REPORT FOR:
SAFEBACK (SYDEX) 2.0

April 2003

The CFTT Project tested the Safeback (Sydex) 2.0 against the Digital Data Acquisition Tool Specification available at:
http://www.cfft.nist.gov/disk_imaging.htm

Our results are:

The tool shall not alter the original disk. For all of the test cases that were run, an SHA-1 hash was created on the source, the test case was run, and an SHA-1 hash was created on the source after the run. In all cases the hash codes matched (i.e., the source was not altered).

The tool shall make a bit-stream duplicate or an image of an original disk or partition. For most cases tested, SafeBack produced a complete and accurate bit-stream duplicate or an image on disks or partitions of all disk sectors copied. However, if a legacy BIOS interface that underreports the disk size was used, not all of the sectors on the disk were copied. Also, if a direct disk copy was used on an SCSI disk using an ASPI driver, only a small portion of the sectors was copied.

The tool shall log I/O errors. In whole-disk test cases involving a read error, write error, or corrupt image error, SafeBack flagged the error and generated an error message in the SafeBack log. Test cases involving partitions were not tested sufficiently to report here.

The tool's documentation shall be correct. Documentation available for testing this version of SafeBack was somewhat inconclusive or incomplete, so identification of expected behavior was not always possible.

For a complete copy of the report, go to:

<http://www.ojp.usdoj.gov/nij/pubs-sum/199000.htm>

Vendor information:

New Technologies, Inc.

<http://www.forensics-intl.com/>

TEST REPORT FOR:
DD GNU FILEUTILS 4.0.36

August 2002

The CFTT Project tested the dd GNU fileutils 4.0.36 against the Digital Data Acquisition Tool Specification available at: http://www.cfft.nist.gov/disk_imaging.htm

Our results are:

The tool shall not alter the original disk. For all 32 cases that were run, a SHA-1 hash was created on the source, the test case was run and a SHA-1 hash was created on the source after the run. In all cases the hash codes matched, i.e. the source was not altered.

The tool shall make a bit-stream duplicate or an image of an original disk or partition. In all cases tested, the utility **dd** produced an accurate bit-stream duplicate or an image on disks or partitions of all disk sectors copied. However, for a source (either a disk drive or a partition) with an odd number of sectors, the last sector of the source was omitted. For many file systems and operating environments, the last sector of a hard disk drive or the last sector of a partition is either only accessible by a special purpose software tool or not accessible at all.

The tool shall log I/O errors. Assertions requiring read or write errors were not tested. The utility **dd** did produce a log message that there was no space left on the destination when the source was greater than the destination.

The tool's documentation shall be correct. No errors were found in the documentation supplied.

For a complete copy of the report, go to:

<http://www.ojp.usdoj.gov/nij/pubs-sum/196352.htm>

Vendor information:

Red Hat, Inc.

<http://www.redhat.com/>

TEST REPORT FOR:
DARIK'S BOOT AND NUKE 1.0.7

January 2010

**The CFTT Project tested the Darik's Boot and Nuke 1.0.7 against the Forensic Media Preparation Specification available at:
http://www.cfft.nist.gov/forensic_media.htm**

Our results are:

In all the test cases run against Darik's Boot and Nuke (DBAN) Version 1.0.7, all visible sectors were successfully overwritten. For the test cases that used drives containing an HPA or DCO, the tool behaved as designed by the vendor and did not overwrite hidden sectors.

- HPA remained intact, hidden sectors were not overwritten (FMP-03-HPA & FMP-03-DCO+HPA).
- DCO remained intact, hidden sectors were not overwritten (FMP-03-DCO & FMP-03-DCO+HPA).

For a complete copy of the report, go to:
<http://www.ojp.usdoj.gov/nij/pubs-sum/228983.htm>

Vendor information:
Darik's Boot and Nuke
Vanadac Corporation
<http://www.dban.org>

TEST REPORT FOR:
**VOOM HARDCOPY II (MODEL XLHCPL-2PD VERSION
1.11)**

January 2010

The CFTT Project tested the Voom HardCopy II (Model XLHCPL-2PD Version 1.11) against the Forensic Media Preparation Specification available at: http://www.cfft.nist.gov/forensic_media.htm

Our results are:

In all the test cases run against Voom HardCopy II Version 1-11, all visible sectors were successfully overwritten. For the test cases that used destination drives containing an HPA or DCO, the tool behaved as designed by the vendor. It removed any HPA or DCO and overwrote the sectors with zeros.

For a complete copy of the report, go to:

<http://www.ojp.usdoj.gov/nij/pubs-sum/228980.htm>

Vendor information:

Voom Technologies, Inc.

<http://www.voomtech.com/index.html>

TEST REPORT FOR: **WIEBETECH DRIVE ERAZER: DRZR-2-VBND & DRIVE ERAZER PRO BUNDLE**

September 2009

The CFTT Project tested the WiebeTech Drive eRazer DRZR-2-VBND & Drive eRazer PRO Bundle against the Forensic Media Preparation Specification available at: http://www.cfft.nist.gov/forensic_media.htm

Our results are:

Two versions of the Drive eRazer hardware device were tested: DRZR-2-VBND and Drive eRazer Pro Bundle (03/17/2009). Initially we were testing the DRZR-2-VBND device. During testing, we found that the device failed to recognize certain drives as supporting SECURE ERASE. The eRazer PRO was then included in the testing since the eRazer PRO has revised firmware that fixes the recognition problem but is otherwise the same as the original device. Since the scope of the fix was limited to the recognition problem, it was determined that two test reports were unnecessary if a few test cases were run for both devices. Five test cases, identified in Section 2, were rerun with the eRazer Pro.

The DRZR-2-VBND is referred to as the DRZR-2 and the other device is referred to as the eRazer PRO. A revision letter indicating the firmware version can be found on the back of the product at the end of the number beneath the top bar code. Both devices have a jumper that can be used to select either *single pass* mode (the device uses an ATA WRITE command to overwrite drive content) or *secure erase* mode (the device uses the ATA SECURE ERASE command to overwrite the drive content).

In all the test cases with both the DRZR-2 and the eRazer PRO devices, all visible sectors were successfully overwritten. The test cases that used drives containing an HPA or DCO demonstrated some inconsistent behaviors:

- With the jumper set to single pass mode (device uses a WRITE command to overwrite drive content) an HPA was removed, but content was not changed. This was observed for both the DRZR-2 (case FMP-03-HPA) and the eRazer PRO (cases FMP-03-HPA-ALT and FMP-03-DCO+HPA-3).
- With the jumper set to single pass mode (device uses a WRITE command to overwrite drive content) a DCO was neither removed nor was the content changed. This was observed for both the DRZR-2 (case FMP-03-DCO) and the eRazer PRO (case FMP-03-DCO+HPA-3).
- With the jumper set to secure erase mode (device uses a SECURE ERASE command to overwrite drive content) a DCO was neither removed nor was the content changed. This was observed for both the DRZR-2 (cases FMP-04-DCO and FMP-04-DCO+HPA) and the eRazer PRO (case FMP-03-DCO-ALT).
- With the jumper set to secure erase mode (device uses a SECURE ERASE command to overwrite drive content) an HPA was not removed (cases FMP-04- HPA, FMP-04-DCO-HPA, and FMP-04-HPA-TOS). However, the content of an HPA on a Hitachi HTS722020K9SA00 drive was erased (cases FMP-04-DCO+HPA and FMP-04-HPA), but the content of an HPA on a TOSHIBA MK2049GSY was not changed (case FMP-04-HPA-TOS). All cases were run on the DRZR-2.

For a complete copy of the report, go to:

<http://www.ojp.usdoj.gov/nij/pubs-sum/228228.htm>

Vendor information:

WiebeTech LLC, a brand of CRU-DataPort

<http://www.wiebetech.com/>

TEST REPORT FOR:
ACES WRITEBLOCKER WINDOWS 2000 V5.02.00

January 2008

The CFTT Project tested the ACES Writeblocker Windows 2000 V5.02.00 against the Software Write Block Specification available at: http://www.cfft.nist.gov/software_write_block.htm

Our results are:

The tool shall not allow a protected drive to be changed. The tool failed to block some test commands from the protected categories that were sent to protected drives but no changes to the protected drives were observed.

The tool blocked all SCSI-2 commands from the WRITE category but failed to block most of the SCSI-3 commands in that category. The tool also failed to block four internal IRP functions from the WRITE category. The tool did not block any of the commands from the VENDOR_SPECIFIC and UNDEFINED categories. See Sections 9.3.5, 9.4.5, and 9.5.5 for a complete list of the commands allowed.

The tool shall not prevent obtaining any information from or about any drive. The tool did not alter or block test commands from any nonprotected category that were sent to protected or unprotected drives.

The tool shall not prevent any operations to a drive that is not protected. The tool did not alter or block any test commands sent to unprotected drives.

For a complete copy of the report, go to:
<http://www.ojp.usdoj.gov/nij/pubs-sum/220221.htm>

Vendor information:

Booz, Allen, Hamilton, Inc.

TEST REPORT FOR: **ACES WRITEBLOCKER WINDOWS XP V6.10.0**

January 2008

The CFTT Project tested the ACES Writeblocker Windows XP V6.10.0 against the Software Write Block Specification available at:
http://www.cfft.nist.gov/software_write_block.htm

Our results are:

The tool shall not allow a protected drive to be changed. The tool failed to block some test commands from the protected categories that were sent to protected drives but no changes to the protected drives were observed.

The tool blocked all SCSI-2 commands from the WRITE category but failed to block most of the SCSI-3 commands in that category. The tool also failed to block four internal IRP functions from the WRITE category. The tool did not block any of the commands from the VENDOR_SPECIFIC and UNDEFINED categories. See Sections 9.3.5, 9.4.5, and 9.5.5 for a complete list of the commands allowed.

The tool shall not prevent obtaining any information from or about any drive. The tool did not alter or block test commands from any non-protected category that were sent to protected or unprotected drives.

The tool shall not prevent any operations to a drive that is not protected. The tool did not alter or block any test commands sent to unprotected drives.

For a complete copy of the report, go to:
<http://www.ojp.usdoj.gov/nij/pubs-sum/220222.htm>

Vendor information:

Booz, Allen, Hamilton, Inc.

TEST REPORT FOR: **PDBLOCK VERSION 1.02 (PDB_LITE)**

June 2005

**The CFTT Project tested the PDBLOCK Version 1.02 (PDB_LITE) against the Software Write Block Specification available at:
http://www.cftt.nist.gov/software_write_block.htm**

Our results are:

The tool shall not allow a protected drive to be changed. For all test cases run, the tool always blocked all write commands sent to a protected drive. For some test cases run, the tool did not block all commands that could change protected drives.

The tool blocked all commands from the write category sent to a protected drive. However, the tool did not block some commands from the configuration and miscellaneous categories that are either undefined (invalid) or outmoded and not routinely used by current software. These commands in current BIOS implementations do not write to a hard drive, but in the future they could be defined such that they would change the contents or accessibility of a protected drive. In the test specification, these commands are therefore included in categories that should be blocked.

The tool did not block five commands in the configuration category: Initialize Drive Parameters (0x09), PS/2 ESDI Diagnostic (0x0E), PC/XT Controller Ram Diagnostic (0x12), the controller drive diagnostic command (0x13), and Controller Internal Diagnostic (0x14). These commands are rarely used, if at all. Additionally, two commands in the miscellaneous category were not blocked (command codes 0x1A and 0x22).

Test cases: SWB-04 and SWB-06.

Although PDBLOCK Version 1.02 always protects drives from write commands, it does not report the accessible drives. Therefore it does not meet the SWB-RM-04 requirement from *Software Write Block Tool Specification & Test Plan Version 3.0*: The tool shall report all drives accessible by the covered interfaces.

Test cases: All.

The tool shall not prevent obtaining any information from or about any drive.

For all test cases run, the tool always allowed commands to obtain information from any protected drives.

The tool shall not prevent any operations to a drive that is not protected. For

all test cases run, the tool always allowed any command to access any unprotected drives.

For a complete copy of the report, go to:

<http://www.ojp.usdoj.gov/nij/pubs-sum/209831.htm>

Vendor information:

Digital Intelligence, Inc.

<http://www.digitalintelligence.com>

TEST REPORT FOR: **PDBLOCK VERSION 2.00**

June 2005

**The CFTT Project tested the PDBLOCK Version 2.00 against the Software Write Block Specification available at:
http://www.cfft.nist.gov/software_write_block.htm**

Our results are:

The tool shall not allow a protected drive to be changed. For all test cases run, the tool always blocked all write commands sent to a protected drive. For some test cases run, the tool did not block all commands that could change protected drives.

The tool blocked all commands from the write category sent to a protected drive. However, the tool did not block some commands from the configuration and miscellaneous categories that are either undefined (invalid) or outmoded and not routinely used by current software. These commands in current BIOS implementations do not write to a hard drive, but in the future they could be defined such that they would change the contents or accessibility of a protected drive. In the test specification, these commands are therefore included in categories that should be blocked.

The tool did not block five commands in the configuration category: Initialize Drive Parameters (0x09), PS/2 ESDI Diagnostic (0x0E), PC/XT Controller Ram Diagnostic (0x12), the controller drive diagnostic command (0x13), and Controller Internal Diagnostic (0x14). These commands are rarely used, if at all. The tool only blocked three commands in the miscellaneous category (command codes 0x1A, 0x22, and 0xED). Command code 0xED is always blocked with a return code of *fail* (0x0100), regardless of the setting of the */fail* command line option.

Test cases: SWB-03, SWB-04, SWB-05, SWB-06, SWB-15, SWB-16, SWB-17, and SWB- 18.

Although PDBLOCK Version 2.00 always protects drives from write commands, it does not report the accessible drives. Therefore it does not meet the SWB-RM-04 requirement from *Software Write Block Tool Specification & Test Plan Version 3.0*. The tool shall report all drives accessible by the covered interfaces.

Test cases: All.

The tool shall not prevent obtaining any information from or about any drive.

For all test cases run, the tool always allowed commands to obtain information from any protected drives.

The tool shall not prevent any operations to a drive that is not protected.

For all test cases run, the tool always allowed any command to access any unprotected drives.

For a complete copy of the report, go to:

<http://www.ojp.usdoj.gov/nij/pubs-sum/209832.htm>

Vendor information:

Digital Intelligence, Inc.

<http://www.digitalintelligence.com>

TEST REPORT FOR: **PDBLOCK VERSION 2.10**

June 2005

**The CFTT Project tested the PDBLOCK Version 2.10 against the Software Write Block Specification available at:
http://www.cfft.nist.gov/software_write_block.htm**

Our results are:

The tool shall not allow a protected drive to be changed. For all test cases run, the tool always blocked all write commands sent to a protected drive. For some test cases run, the tool did not block all commands that could change protected drives.

The tool blocked all commands from the write category sent to a protected drive. However, the tool did not block some commands from the miscellaneous category that are either undefined (invalid) or outmoded and not routinely used by current software. These commands in current BIOS implementations do not write to a hard drive, but in the future they could be defined such that they would change the contents or accessibility of a protected drive. In the test specification, these commands are therefore included in categories that should be blocked.

The tool only blocked three commands in the miscellaneous category (command codes 0x1A, 0x22, and 0xED). Command code 0xED is always blocked with a return code of *fail* (0x0100) regardless of the protection status of the drive or the */fail* command line option.

The tool shall not prevent obtaining any information from or about any drive. For all test cases run, the tool always allowed commands to obtain information from any protected drives.

The tool shall not prevent any operations to a drive that is not protected. For all test cases run, the tool always allowed any command to access any unprotected drives. For some test cases run with five drives, the fifth drive was protected even though it was not designated as protected.

For a complete copy of the report, go to:

<http://www.ojp.usdoj.gov/nij/pubs-sum/209833.htm>

Vendor information:

Digital Intelligence, Inc.

<http://www.digitalintelligence.com>

TEST REPORT FOR: **RCMP HDL V0.4**

August 2004

The CFTT Project tested the RCMP HDL V0.4 against the Software Write Block Specification available at:
http://www.cfft.nist.gov/software_write_block.htm

Our results are:

The tool shall not allow a protected drive to be changed.

For all test cases run, the tool did not block some commands that could change protected drives.

The tool blocked all commands from the write category sent to a protected drive. However, the tool did not block some commands from the miscellaneous category that are either undefined (invalid) or outmoded and not routinely used by current software. These commands in current BIOS implementations do not write to a hard drive, but in the future they could be defined such that they would change the contents or accessibility of a protected drive. In the test specification, these commands are therefore included in categories that should be blocked.

The tool only blocked three commands in the miscellaneous category (command codes 0x1A, 0x22, and 0xED). Command code 0xED is always blocked with a return code of *fail* (0x0100) regardless of the protection status of the drive or the */fail* command line option.

The tool shall not prevent obtaining any information from or about any drive.

For all test cases run, the tool always allowed commands to obtain information from any protected drives.

The tool shall not prevent any operations to a drive that is not protected. For all test cases run, the tool always allowed any command to access any unprotected drives.

For a complete copy of the report, go to:

<http://www.ojp.usdoj.gov/nij/pubs-sum/206231.htm>

Vendor information:

Royal Canadian Mounted Police

TEST REPORT FOR: **RCMP HDL V0.5**

August 2004

The CFTT Project tested the RCMP HDL V0.5 against the Software Write Block Specification available at:

http://www.cfft.nist.gov/software_write_block.htm

Our results are:

The tool shall not allow a protected drive to be changed.

For some test cases run, the tool did not block all commands that could change protected drives.

The tool blocked the commands that were listed in the documentation as commands that would be blocked. However, the tool did not block some commands that could change the contents or accessibility of a protected drive. The tool did not block four commands in the configuration category that could change the contents or accessibility of a protected drive. The commands not blocked were the Initialize Drive Parameters (0x09), an EDSI Diagnostic command (0x0E), the Controller RAM Diagnostic command (0x12), and the Controller Internal Diagnostic command (0x14). The tool blocked only two commands in the miscellaneous category.

The tool shall not prevent obtaining any information from or about any drive.

For all test cases run, the tool always allowed commands to obtain information from any protected drives.

The tool shall not prevent any operations to a drive that is not protected.

For all test cases run, the tool always allowed any command to access any unprotected drives.

For a complete copy of the report, go to:

<http://www.ojp.usdoj.gov/nij/pubs-sum/206232.htm>

Vendor information:

Royal Canadian Mounted Police

TEST REPORT FOR: **RCMP HDL V0.7**

August 2004

The CFTT Project tested the RCMP HDL V0.7 against the Software Write Block Specification available at:
http://www.cfft.nist.gov/software_write_block.htm

Our results are:

The tool shall not allow a protected drive to be changed.

For some test cases run, the tool did not block all commands that could change protected drives.

The tool blocked the commands that were listed in the documentation as commands that would be blocked. However, the tool did not block two commands in the configuration category that could change the content or accessibility of a protected drive. The commands not blocked were an EDSI Diagnostic command (0x0E) and the Initialize Drive Parameters command (0x09).

In addition, one command in the control category and one command in the information category that could have been allowed were blocked. The blocked commands were the read drive type (0x15) and the extended seek (0x47) commands.

The tool shall not prevent obtaining any information from or about any drive.

Except for one command in the information category, the tool always allowed commands to obtain information from the protected drives for all test cases run. The read drive type (0x15) command was always blocked on protected drives.

The tool shall not prevent any operations to a drive that is not protected. For all test cases run, the tool always allowed any command to access any unprotected drives.

For a complete copy of the report, go to:

<http://www.ojp.usdoj.gov/nij/pubs-sum/206233.htm>

Vendor information:

Royal Canadian Mounted Police

TEST REPORT FOR: **RCMP HDL V0.8**

February 2004

The CFTT Project tested the RCMP HDL V0.8 against the Software Write Block Specification available at:

http://www.cfft.nist.gov/software_write_block.htm

Our results are:

The tool shall not allow a protected drive to be changed.

For all test cases run, the tool always blocked commands that would have changed any protected drives.

The tool functioned as documented and no anomalies were observed. Two commands in the control category were blocked that could have been allowed: the recalibrate (0x11) and the extended seek (0x47) commands.

The tool shall not prevent obtaining any information from or about any drive.

For all test cases run, the tool always allowed commands to obtain information from any protected drives.

The tool shall not prevent any operations to a drive that is not protected.

For all test cases run, the tool always allowed any command to access any unprotected drives.

For a complete copy of the report, go to:

<http://www.ojp.usdoj.gov/nij/pubs-sum/203196.htm>

Vendor information:

Royal Canadian Mounted Police

TEST REPORT FOR: **T4 FORENSIC SCSI BRIDGE (FIREWIRE INTERFACE)**

September 2009

The CFTT Project tested the T4 Forensic SCSI Bridge (FireWire Interface) against the Hardware Write Block Specification available at:
http://www.cfft.nist.gov/hardware_write_block.htm

Our results are:

An HWB device shall not transmit a command to a protected storage device that modifies the data on the storage device: For all test cases run, the device always blocked any commands that would have changed user or operating system data stored on a protected drive.

An HWB device shall return the data requested by a read operation: For all test cases run, the device always allowed commands to read the protected drive.

An HWB device shall return without modification any access-significant information requested from the drive: For all test cases run, the device always returned access-significant information from the protected drive without modification.

Any error condition reported by the storage device to the HWB device shall be reported to the host: For all test cases run, the device always returned error codes from the protected drive without modification.

For a complete copy of the report, go to:
<http://www.ojp.usdoj.gov/nij/pubs-sum/228225.htm>

Vendor information:

Tableau, LLC

<http://www.tableau.com/>

TEST REPORT FOR: **T4 FORENSIC SCSI BRIDGE (USB INTERFACE)**

September 2009

The CFTT Project tested the T4 Forensic SCSI Bridge (USB Interface) against the Hardware Write Block Specification available at:
http://www.cfft.nist.gov/hardware_write_block.htm

Our results are:

An HWB device shall not transmit a command to a protected storage device that modifies the data on the storage device: For all test cases run, the device always blocked any commands that would have changed user or operating system data stored on a protected drive.

An HWB device shall return the data requested by a read operation: For all test cases run, the device always allowed commands to read the protected drive.

An HWB device shall return without modification any access-significant information requested from the drive: For all test cases run, the device always returned access-significant information from the protected drive without modification.

Any error condition reported by the storage device to the HWB device shall be reported to the host: For all test cases run, the device always returned error codes from the protected drive without modification.

For a complete copy of the report, go to:
<http://www.ojp.usdoj.gov/nij/pubs-sum/228224.htm>

Vendor information:

Tableau, LLC

<http://www.tableau.com/>

TEST REPORT FOR:
**TABLEAU T8 FORENSIC USB BRIDGE (FIREWIRE
INTERFACE)**

August 2008

The CFTT Project tested the Tableau T8 Forensic USB Bridge (FireWire Interface) against the Hardware Write Block Specification available at: http://www.cfft.nist.gov/hardware_write_block.htm

Our results are:

An HWB device shall not transmit a command to a protected storage device that modifies the data on the storage device: For all test cases run, the device always blocked any commands that would have changed user or operating system data stored on a protected drive.

An HWB device shall return the data requested by a read operation: For all test cases run, the device always allowed commands to read the protected drive.

An HWB device shall return without modification any access-significant information requested from the drive: For all test cases run, the device always returned access-significant information from the protected drive without modification.

Any error condition reported by the storage device to the HWB device shall be reported to the host: For all test cases run, the device always returned error codes from the protected drive without modification.

For a complete copy of the report, go to:
<http://www.ojp.usdoj.gov/nij/pubs-sum/223431.htm>

Vendor information:

Tableau, LLC

<http://www.tableau.com/>

TEST REPORT FOR:
TABLEAU T8 FORENSIC USB BRIDGE (USB INTERFACE)

August 2008

The CFTT Project tested the Tableau T8 Forensic USB Bridge (USB Interface) against the Hardware Write Block Specification available at:
http://www.cfft.nist.gov/hardware_write_block.htm

Our results are:

An HWB device shall not transmit a command to a protected storage device that modifies the data on the storage device: For all test cases run, the device always blocked any commands that would have changed user or operating system data stored on a protected drive.

An HWB device shall return the data requested by a read operation: For all test cases run, the device always allowed commands to read the protected drive.

An HWB device shall return without modification any access-significant information requested from the drive: For all test cases run, the device always returned access-significant information from the protected drive without modification.

Any error condition reported by the storage device to the HWB device shall be reported to the host: For all test cases run, the device always returned error codes from the protected drive without modification.

For a complete copy of the report, go to:
<http://www.ojp.usdoj.gov/nij/pubs-sum/223432.htm>

Vendor information:

Tableau, LLC

<http://www.tableau.com/>

TEST REPORT FOR: **FASTBLOC FE (USB INTERFACE)**

June 2007

The CFTT Project tested the FastBloc FE (USB Interface) against the Hardware Write Block Specification available at:
http://www.cfft.nist.gov/hardware_write_block.htm

Our results are:

An HWB device shall not transmit a command to a protected storage device that modifies the data on the storage device: For all test cases run, the device always blocked any commands that would have changed user or operating system data stored on a protected drive.

An HWB device shall return the data requested by a read operation: For all test cases run, the device always allowed commands to read the protected drive.

An HWB device shall return without modification any access-significant information requested from the drive: For all test cases run, the device always returned access-significant information from the protected drive without modification.

Any error condition reported by the storage device to the HWB device shall be reported to the host: For all test cases run, the device always returned error codes from the protected drive without modification.

For a complete copy of the report, go to:
<http://www.ojp.usdoj.gov/nij/pubs-sum/218378.htm>

Vendor information:

Guidance Software, Inc.

TEST REPORT FOR:
FASTBLOC FE (FIREWIRE INTERFACE)

June 2007

The CFTT Project tested the FastBloc FE (FireWire Interface) against the Hardware Write Block Specification available at:
http://www.cfft.nist.gov/hardware_write_block.htm

Our results are:

An HWB device shall not transmit a command to a protected storage device that modifies the data on the storage device: For all test cases run, the device always blocked any commands that would have changed user or operating system data stored on a protected drive.

An HWB device shall return the data requested by a read operation: For all test cases run, the device always allowed commands to read the protected drive.

An HWB device shall return without modification any access-significant information requested from the drive: For all test cases run, the device always returned access-significant information from the protected drive without modification.

Any error condition reported by the storage device to the HWB device shall be reported to the host: For all test cases run, the device always returned error codes from the protected drive without modification.

For a complete copy of the report, go to:
<http://www.ojp.usdoj.gov/nij/pubs-sum/218379.htm>

Vendor information:

Guidance Software, Inc.

TEST REPORT FOR:
TABLEAU T5 FORENSIC IDE BRIDGE (USB INTERFACE)

June 2007

The CFTT Project tested the Tableau T5 Forensic IDE Bridge (USB Interface) against the Hardware Write Block Specification available at:
http://www.cfft.nist.gov/hardware_write_block.htm

Our results are:

An HWB device shall not transmit a command to a protected storage device that modifies the data on the storage device: For all test cases run, the device always blocked any commands that would have changed user or operating system data stored on a protected drive.

An HWB device shall return the data requested by a read operation: For all test cases run, the device always allowed commands to read the protected drive.

An HWB device shall return without modification any access-significant information requested from the drive: For all test cases run, the device always returned access-significant information from the protected drive without modification.

Any error condition reported by the storage device to the HWB device shall be reported to the host: For all test cases run, the device always returned error codes from the protected drive without modification.

For a complete copy of the report, go to:
<http://www.ojp.usdoj.gov/nij/pubs-sum/218380.htm>

Vendor information:

Tableau, LLC

<http://www.tableau.com/>

TEST REPORT FOR:
**TABLEAU T5 FORENSIC IDE BRIDGE (FIREWIRE
INTERFACE)**

June 2007

The CFTT Project tested the Tableau T5 Forensic IDE Bridge (FireWire Interface) against the Hardware Write Block Specification available at: http://www.cfft.nist.gov/hardware_write_block.htm

Our results are:

An HWB device shall not transmit a command to a protected storage device that modifies the data on the storage device: For all test cases run, the device always blocked any commands that would have changed user or operating system data stored on a protected drive.

An HWB device shall return the data requested by a read operation: For all test cases run, the device always allowed commands to read the protected drive.

An HWB device shall return without modification any access-significant information requested from the drive: For all test cases run, the device always returned access-significant information from the protected drive without modification.

Any error condition reported by the storage device to the HWB device shall be reported to the host: For all test cases run, the device always returned error codes from the protected drive without modification.

For a complete copy of the report, go to:
<http://www.ojp.usdoj.gov/nij/pubs-sum/218381.htm>

Vendor information:

Tableau, LLC

<http://www.tableau.com/>

TEST REPORT FOR:
**TABLEAU FORENSIC SATA BRIDGE T3U (USB
INTERFACE)**

January 2007

The CFTT Project tested the Tableau Forensic SATA Bridge T3u (USB Interface) against the Hardware Write Block Specification available at: http://www.cfft.nist.gov/hardware_write_block.htm

Our results are:

An HWB device shall not transmit a command to a protected storage device that modifies the data on the storage device: For all test cases run, the HWB device always blocked any commands that would have changed user or operating system data stored on a protected drive.

An HWB device shall return the data requested by a read operation: For all test cases run, the HWB device always allowed commands to read the protected drive.

An HWB device shall return without modification any access-significant information requested from the drive: For all test cases run, the HWB device always returned access significant information from the protected drive without modification.

Any error condition reported by the storage device to the HWB device shall be reported to the host: For all test cases run, the HWB device always returned error codes from the protected drive without modification.

For a complete copy of the report, go to:
<http://www.ojp.usdoj.gov/nij/pubs-sum/216981.htm>

Vendor information:

Tableau, LLC

<http://www.tableau.com/>

TEST REPORT FOR:
**TABLEAU FORENSIC SATA BRIDGE T3U (FIREWIRE
INTERFACE)**

January 2007

The CFTT Project tested the Tableau Forensic SATA Bridge T3u (FireWire Interface) against the Hardware Write Block Specification available at: http://www.cfft.nist.gov/hardware_write_block.htm

Our results are:

An HWB device shall not transmit a command to a protected storage device that modifies the data on the storage device: For all test cases run, the device always blocked any commands that would have changed user or operating system data stored on a protected drive.

An HWB device shall return the data requested by a read operation: For all test cases run, the device always allowed commands to read the protected drive.

An HWB device shall return without modification any access-significant information requested from the drive: For all test cases run, the device always returned access-significant information from the protected drive without modification.

Any error condition reported by the storage device to the HWB device shall be reported to the host: For all test cases run, the device always returned error codes from the protected drive without modification.

For a complete copy of the report, go to:
<http://www.ojp.usdoj.gov/nij/pubs-sum/216982.htm>

Vendor information:

Tableau, LLC

<http://www.tableau.com/>

TEST REPORT FOR:
**TABLEAU FORENSIC IDE POCKET BRIDGE T14
(FIREWIRE INTERFACE)**

January 2007

The CFTT Project tested the Tableau Forensic IDE Pocket Bridge T14 (FireWire Interface) against the Hardware Write Block Specification available at: http://www.cftt.nist.gov/hardware_write_block.htm

Our results are:

An HWB device shall not transmit a command to a protected storage device that modifies the data on the storage device: For all test cases run, the HWB device always blocked any commands that would have changed user or operating system data stored on a protected drive.

An HWB device shall return the data requested by a read operation: For all test cases run, the HWB device always allowed commands to read the protected drive.

An HWB device shall return without modification any access-significant information requested from the drive: For all test cases run, the HWB device always returned access-significant information from the protected drive without modification.

Any error condition reported by the storage device to the HWB device shall be reported to the host: For all test cases run, the HWB device always returned error codes from the protected drive without modification.

For a complete copy of the report, go to:
<http://www.ojp.usdoj.gov/nij/pubs-sum/216983.htm>

Vendor information:

Tableau, LLC

<http://www.tableau.com/>

TEST REPORT FOR:
**WIEBETECH FORENSIC SATADOCK (FIREWIRE
INTERFACE)**

December 2006

The CFTT Project tested the WiebeTech Forensic SATADock (FireWire Interface) against the Hardware Write Block Specification available at: http://www.cfft.nist.gov/hardware_write_block.htm

Our results are:

An HWB device shall not transmit a command to a protected storage device that modifies the data on the storage device: For all test cases run, the device always blocked any commands that would have changed user or operating system data stored on a protected drive.

An HWB device shall return the data requested by a read operation: For all test cases run, the device always allowed commands to read the protected drive.

An HWB device shall return without modification any access-significant information requested from the drive: For all test cases run, the device always returned access-significant information from the protected drive without modification.

Any error condition reported by the storage device to the HWB device shall be reported to the host: For all test cases run, the device always returned error codes from the protected drive without modification.

For a complete copy of the report, go to:
<http://www.ojp.usdoj.gov/nij/pubs-sum/216300.htm>

Vendor information:

WiebeTech, LLC

<http://www.wiebetech.com/>

TEST REPORT FOR: **WIEBETECH FORENSIC SATADOCK (USB INTERFACE)**

December 2006

The CFTT Project tested the WiebeTech Forensic SATADock (USB Interface) against the Hardware Write Block Specification available at:
http://www.cfft.nist.gov/hardware_write_block.htm

Our results are:

An HWB device shall not transmit a command to a protected storage device that modifies the data on the storage device: For all test cases run, the device always blocked any commands that would have changed user or operating system data stored on a protected drive.

An HWB device shall return the data requested by a read operation: For all test cases run, the device always allowed commands to read the protected drive.

An HWB device shall return without modification any access-significant information requested from the drive: For all test cases run, the device always returned access-significant information from the protected drive without modification.

Any error condition reported by the storage device to the HWB device shall be reported to the host: For all test cases run, the device always returned error codes from the protected drive without modification.

For a complete copy of the report, go to:
<http://www.ojp.usdoj.gov/nij/pubs-sum/216299.htm>

Vendor information:

WiebeTech, LLC

<http://www.wiebetech.com/>

TEST REPORT FOR:
**WIEBETECH FORENSIC COMBODOCK (USB
INTERFACE)**

May 2006

The CFTT Project tested the WiebeTech Forensic ComboDock (USB Interface) against the Hardware Write Block Specification available at: http://www.cfft.nist.gov/hardware_write_block.htm

Our results are:

An HWB device shall not transmit a command to a protected storage device that modifies the data on the storage device: For all test cases run, the device always blocked any commands that would have changed user or operating system data stored on a protected drive.

An HWB device shall return the data requested by a read operation: For all test cases run, the device always allowed commands to read the protected drive.

An HWB device shall return without modification any access-significant information requested from the drive: For all test cases run, the device always returned access-significant information from the protected drive without modification.

Any error condition reported by the storage device to the HWB device shall be reported to the host: For all test cases run, the device always returned error codes from the protected drive without modification.

For a complete copy of the report, go to:
<http://www.ojp.usdoj.gov/nij/pubs-sum/214063.htm>

Vendor information:

WiebeTech, LLC

<http://www.wiebetech.com/>

TEST REPORT FOR:
**WIEBETECH FORENSIC COMBODOCK (FIREWIRE
INTERFACE)**

May 2006

The CFTT Project tested the WiebeTech Forensic ComboDock (FireWire Interface) against the Hardware Write Block Specification available at: http://www.cfft.nist.gov/hardware_write_block.htm

Our results are:

An HWB device shall not transmit a command to a protected storage device that modifies the data on the storage device: For all test cases run, the device always blocked any commands that would have changed user or operating system data stored on a protected drive.

An HWB device shall return the data requested by a read operation: For all test cases run, the device always allowed commands to read the protected drive.

An HWB device shall return without modification any access-significant information requested from the drive: For all test cases run, the device always returned access-significant information from the protected drive without modification.

Any error condition reported by the storage device to the HWB device shall be reported to the host: For all test cases run, the device always returned error codes from the protected drive without modification.

For a complete copy of the report, go to:
<http://www.ojp.usdoj.gov/nij/pubs-sum/214064.htm>

Vendor information:

WiebeTech, LLC

<http://www.wiebetech.com/>

TEST REPORT FOR:
**WIEBETECH BUS POWERED FORENSIC COMBODOCK
(USB INTERFACE)**

May 2006

The CFTT Project tested the WiebeTech Bus Powered Forensic ComboDock (USB Interface) against the Hardware Write Block Specification available at: http://www.cfft.nist.gov/hardware_write_block.htm

Our results are:

An HWB device shall not transmit a command to a protected storage device that modifies the data on the storage device: For all test cases run, the device always blocked any commands that would have changed user or operating system data stored on a protected drive.

An HWB device shall return the data requested by a read operation: For all test cases run, the device always allowed commands to read the protected drive.

An HWB device shall return without modification any access-significant information requested from the drive: For all test cases run, the device always returned access-significant information from the protected drive without modification.

Any error condition reported by the storage device to the HWB device shall be reported to the host: For all test cases run, the device always returned error codes from the protected drive without modification.

For a complete copy of the report, go to:
<http://www.ojp.usdoj.gov/nij/pubs-sum/214065.htm>

Vendor information:

WiebeTech, LLC

<http://www.wiebetech.com/>

TEST REPORT FOR:
**WIEBETECH BUS POWERED FORENSIC COMBODOCK
(FIREWIRE INTERFACE)**

May 2006

The CFTT Project tested the WiebeTech Bus Powered Forensic ComboDock (FireWire Interface) against the Hardware Write Block Specification available at: http://www.cftt.nist.gov/hardware_write_block.htm

Our results are:

An HWB device shall not transmit a command to a protected storage device that modifies the data on the storage device: For all test cases run, the device always blocked any commands that would have changed user or operating system data stored on a protected drive.

An HWB device shall return the data requested by a read operation: For all test cases run, the device always allowed commands to read the protected drive.

An HWB device shall return without modification any access-significant information requested from the drive: For all test cases run, the device always returned access-significant information from the protected drive without modification.

Any error condition reported by the storage device to the HWB device shall be reported to the host: For all test cases run, the device always returned error codes from the protected drive without modification.

For a complete copy of the report, go to:
<http://www.ojp.usdoj.gov/nij/pubs-sum/214066.htm>

Vendor information:

WiebeTech, LLC

<http://www.wiebetech.com/>

TEST REPORT FOR:
**DIGITAL INTELLIGENCE ULTRABLOCK SATA (FIREWIRE
INTERFACE)**

May 2006

The CFTT Project tested the Digital Intelligence UltraBlock SATA (FireWire Interface) against the Hardware Write Block Specification available at: http://www.cfft.nist.gov/hardware_write_block.htm

Our results are:

An HWB device shall not transmit a command to a protected storage device that modifies the data on the storage device: For all test cases run, the device always blocked any commands that would have changed user or operating system data stored on a protected drive.

An HWB device shall return the data requested by a read operation: For all test cases run, the device always allowed commands to read the protected drive.

An HWB device shall return without modification any access-significant information requested from the drive: For all test cases run, the device always returned access-significant information from the protected drive without modification.

Any error condition reported by the storage device to the HWB device shall be reported to the host: For all test cases run, the device always returned error codes from the protected drive without modification.

For a complete copy of the report, go to:
<http://www.ojp.usdoj.gov/nij/pubs-sum/214067.htm>

Vendor information:

Digital Intelligence

<http://www.DigitalIntelligence.com/>

TEST REPORT FOR:
FASTBLOC IDE (FIRMWARE VERSION 16)

April 2006

The CFTT Project tested the FastBloc IDE (Firmware Version 16) against the Hardware Write Block Specification available at:
http://www.cfft.nist.gov/hardware_write_block.htm

Our results are:

An HWB device shall not transmit a command to a protected storage device that modifies the data on the storage device: For all test cases run, the HWB device always blocked any commands that would have changed user or operating system data stored on a protected drive.

An HWB device shall return the data requested by a read operation: For all test cases run, the HWB device always allowed commands to read the protected drive.

An HWB device shall return without modification any access-significant information requested from the drive: For all test cases run, the HWB device always returned access-significant information from the protected drive without modification.

Any error condition reported by the storage device to the HWB device shall be reported to the host: For all test cases run, the HWB device always returned error codes from the protected drive without modification.

For a complete copy of the report, go to:
<http://www.ojp.usdoj.gov/nij/pubs-sum/212956.htm>

Vendor information:

Guidance Software, Inc.

<http://www.guidancesoftware.com/>

TEST REPORT FOR:
MYKEY NOWRITE (FIRMWARE VERSION 1.05)

April 2006

The CFTT Project tested the MyKey NoWrite (Firmware Version 1.05) against the Hardware Write Block Specification available at:
http://www.cftt.nist.gov/hardware_write_block.htm

Our results are:

An HWB device shall not transmit a command to a protected storage device that modifies the data on the storage device: For all test cases run, the HWB device always blocked any commands that would have changed user or operating system data stored on a protected drive.

An HWB device shall return the data requested by a read operation: For all test cases run, the HWB device always allowed commands to read the protected drive.

An HWB device shall return without modification any access-significant information requested from the drive: For all test cases run, the HWB device always returned access-significant information from the protected drive without modification.

Any error condition reported by the storage device to the HWB device shall be reported to the host: For all test cases run, the HWB device always returned error codes from the protected drive without modification.

For a complete copy of the report, go to:
<http://www.ojp.usdoj.gov/nij/pubs-sum/212958.htm>

Vendor information:

MyKey Technology, Inc.

TEST REPORT FOR:
**ICS IMAGEMASSTER DRIVELOCK IDE (FIRMWARE
VERSION 17)**

April 2006

The CFTT Project tested the ICS ImageMasster DriveLock IDE (Firmware Version 17) against the Hardware Write Block Specification available at: http://www.cfft.nist.gov/hardware_write_block.htm

Our results are:

An HWB device shall not transmit a command to a protected storage device that modifies the data on the storage device: For all test cases run, the HWB device always blocked any commands that would have changed user or operating system data stored on a protected drive.

An HWB device shall return the data requested by a read operation: For all test cases run, the HWB device always allowed commands to read the protected drive.

An HWB device shall return without modification any access-significant information requested from the drive: For all test cases run, the HWB device always returned access-significant information from the protected drive without modification.

Any error condition reported by the storage device to the HWB device shall be reported to the host: For all test cases run, the HWB device always returned error codes from the protected drive without modification.

For a complete copy of the report, go to:
<http://www.ojp.usdoj.gov/nij/pubs-sum/212959.htm>

Vendor information:

Intelligent Computer Solutions, Inc.

<http://www.ics-iq.com/>

TEST REPORT FOR:
**WIEBETECH FIREWIRE DRIVEDOCK COMBO
(FIREWIRE INTERFACE)**

April 2006

The CFTT Project tested the WiebeTech FireWire DriveDock Combo (FireWire Interface) against the Hardware Write Block Specification available at: http://www.cfft.nist.gov/hardware_write_block.htm

Our results are:

An HWB device shall not transmit a command to a protected storage device that modifies the data on the storage device: For all test cases run, the HWB device always blocked any commands that would have changed user or operating system data stored on a protected drive.

An HWB device shall return the data requested by a read operation: For all test cases run, the HWB device always allowed commands to read the protected drive.

An HWB device shall return without modification any access-significant information requested from the drive: For all test cases run, the HWB device always returned access-significant information from the protected drive without modification.

Any error condition reported by the storage device to the HWB device shall be reported to the host: For all test cases run, the HWB device always returned error codes from the protected drive without modification.

For a complete copy of the report, go to:
<http://www.ojp.usdoj.gov/nij/pubs-sum/212960.htm>

Vendor information:

WiebeTech LLC

<http://www.wiebetech.com/>

TEST REPORT FOR:
**DIGITAL INTELLIGENCE FIREFLY 800 IDE (FIREWIRE
INTERFACE)**

April 2006

The CFTT Project tested the Digital Intelligence Firefly 800 IDE (FireWire Interface) against the Hardware Write Block Specification available at: http://www.cfft.nist.gov/hardware_write_block.htm

Our results are:

An HWB device shall not transmit a command to a protected storage device that modifies the data on the storage device: For all test cases run, the HWB device always blocked any commands that would have changed user or operating system data stored on a protected drive.

An HWB device shall return the data requested by a read operation: For all test cases run, the HWB device always allowed commands to read the protected drive.

An HWB device shall return without modification any access-significant information requested from the drive: For all test cases run, the HWB device always returned access-significant information from the protected drive without modification.

Any error condition reported by the storage device to the HWB device shall be reported to the host: For all test cases run, the HWB device always returned error codes from the protected drive without modification.

For a complete copy of the report, go to:
<http://www.ojp.usdoj.gov/nij/pubs-sum/212957.htm>

Vendor information:

Digital Intelligence

<http://www.DigitalIntelligence.com/>

TEST REPORT FOR:
**DIGITAL INTELLIGENCE ULTRABLOCK SATA (USB
INTERFACE)**

April 2006

The CFTT Project tested the Digital Intelligence UltraBlock SATA (USB Interface) against the Hardware Write Block Specification available at: http://www.cfft.nist.gov/hardware_write_block.htm

Our results are:

An HWB device shall not transmit a command to a protected storage device that modifies the data on the storage device: For all test cases run, the HWB device always blocked any commands that would have changed user or operating system data stored on a protected drive.

An HWB device shall return the data requested by a read operation: For all test cases run, the HWB device always allowed commands to read the protected drive.

An HWB device shall return without modification any access-significant information requested from the drive: For all test cases run, the HWB device always returned access significant information from the protected drive without modification.

Any error condition reported by the storage device to the HWB device shall be reported to the host: For all test cases run, the HWB device always returned error codes from the protected drive without modification.

For a complete copy of the report, go to:
<http://www.ojp.usdoj.gov/nij/pubs-sum/212961.htm>

Vendor information:

Digital Intelligence

<http://www.DigitalIntelligence.com/>

TEST REPORT FOR:
BITPIM – 1.0.6 OFFICIAL

January 2010

The CFTT Project tested the BitPim – 1.0.6-official tool against the Mobile Device Specification available at:
http://www.cfft.nist.gov/mobile_devices.htm

Our results are:

Except for the following test cases: CFT-IM-01 (LG vx6100), CFT-IM-08 (LG vx5400, Moto v710, SCH u740, SPH a660), the tested tool acquired all supported data objects completely and accurately from the selected test mobile devices (i.e., LG vx5400, MOTO v710, Samsung SCH u410, Samsung SCH u740, Samsung SPH a660). The exceptions are the following:

- Connectivity was not established via the supported cable interface; therefore, acquisition of device memory was not successful. Test Case: CFT-IM-01 (LG VX6100)
- Address book entries and text messages containing non-ASCII characters such as: à, é were excluded from the address book entry. Test Case: CFT-IMO-08 (LG VX5400, SCH-u740)
- Address book entries containing non-ASCII characters such as: 阿恶哈拉 were not reported. Text messages containing non-ASCII characters such as: à, é, 阿恶 哈拉 were not reported. Test Case: CFT-IMO-08 (Moto v710)

- Text messages containing containing non-ASCII characters such as: à, é were excluded from text message. Test Case: CFT-IMO-08 (SPH-a660)

For a complete copy of the report, go to:

<http://www.ojp.usdoj.gov/nij/pubs-sum/228982.htm>

Vendor information:

BitPim

<http://www.bitpim.org>

TEST REPORT FOR:
MOBILEdit! FORENSICS 3.2.0.738

January 2010

The CFTT Project tested the MOBILEdit! Forensics 3.2.0.738 tool against the Mobile Device Specification available at: http://www.cfft.nist.gov/mobile_devices.htm

Our results are:

Except for the following test cases: CFT-IM-01 (LG vx6100, SPH a660), CFT-IM-05 (Moto v710), CFT-IM-06 (Moto v710), CFT-IM-09 (Moto v710), CFT-IM-10 (Moto v710), and CFT-IMO-04 (Moto v710), the tested tool acquired all supported data objects completely and accurately from the selected test mobile device: Motorola v710. The exceptions are the following:

- Connectivity was not established for two supported (specified by MOBILEdit! Forensic documentation) mobile devices over the supported cable interface; therefore, acquisition of device memory was not successful. Test Case: CFT-IM- 01 (LG vx6100, SPH a660) – NOTE: The LG vx6100 must be in Brew mode – this is undocumented in the tested version – future releases will switch modes automatically for the device.
- The MEID was not reported for the Motorola v710. Test Case: CFT-IM-05 (Moto v710).
- PIM data was not reported for the Motorola v710. Test Case: CFT-IM-06 (Moto v710).
- MMS messages and corresponding attachments (audio, video, and graphic files) were not reported for the Motorola v710. Test Case: CFT-IM-09 (Moto v710).

- Stand-alone files (audio, video, and graphic files) were not reported for the Motorola v710. Test Case: CFT-IM-10 (Moto v710).
- An informative message is not returned when altering the case file data via a hex editor. Test Case: CFT-IMO-04 (Moto v710)

For a complete copy of the report, go to:

<http://www.ojp.usdoj.gov/nij/pubs-sum/228979.htm>

Vendor information:

Compelson Labs

<http://www.mobiledit.com>

TEST REPORT FOR: SUSTEEN DATAPILOT SECURE VIEW 1.12.0

September 2009

**The CFTT Project tested the Susteen DataPilot Secure View 1.12.0 tool against the Mobile Device Specification available at:
http://www.cfft.nist.gov/mobile_devices.htm**

Our results are:

Except for the following test cases: CFT-IM-05 (Samsung SCH-u410, Samsung SCH- u740), CFT-IM-06 (Samsung SPH-a660), CFT-IM-07 (Samsung SCH-u740), CFT- IM-08 (MOTO V710), CFT-IMO-01 (MOTO V710), CFT-IMO-02 (LG VX5400, LG VX6100, Samsung SCH-u410, Samsung SCH-u740), CFT-IMO-03 (LG VX5400, LG VX6100, MOTO V710, Samsung SCH-u410, Samsung SCH-u740), CFT-IMO-08 (LG VX5400, LG VX6100, Samsung SCH-u410, Samsung SCH-u740, Samsung SPH-a660), the tested tool acquired all supported data objects completely and accurately from the selected test mobile devices (i.e., LG VX5400, LG VX6100, MOTO V710, Samsung SCH-u410, Samsung SCH-u740, Samsung SPH-a660). The exceptions are the following:

- The MSISDN was reported incorrectly. Test Case: CFT-IM-05 (SCH u410, SCH u740).
- All active address book entries were not acquired and reported. Test Case: CFT- IM-06 (SPH a660).
- Connectivity was disrupted when attempting to acquire call logs. Test Case: CFT- IM-07 (SCH u740).
- SMS messages were not acquired. Test Case: CFT-IM-08 (MOTO V710).

- Foreign language address book entries were not displayed properly within the individual report files. Test Case: CFT-IMO-01 (MOTO V710).
- Foreign language address book entries were not displayed properly within the preview pane. Test Case: CFT-IMO-02 (LG VX5400, LG VX6100, SCH u410, SCH u740).
- Data inconsistencies existed between the preview-pane view and the generated reports. Test Case: CFT-IMO-03 (LG VX5400, LG VX6100, MOTO V710, SCH u410, SCH u740).
- Incorrect characters were displayed from the wrong character set for foreign language address book entries. Test Case: CFT-IMO-08 (LG VX5400, LG VX6100, Samsung SCH-u410, Samsung SCH-u740, Samsung SPH-a660).

For a complete copy of the report, go to:

<http://www.ojp.usdoj.gov/nij/pubs-sum/228222.htm>

Vendor information:

Susteen, Inc.

<http://www.susteen.com/>

TEST REPORT FOR:
FINAL DATA – FINAL MOBILE FORENSICS 2.1.0.0313

September 2009

The CFTT Project tested the Final Data – Final Mobile Forensics 2.1.0.0313 tool against the Mobile Device Specification available at: http://www.cfft.nist.gov/mobile_devices.htm

Our results are:

Except for the following test cases: CFT-IM-03 (LG vx5400, LG vx6100, MOTO v710, SCH u410, SCH u740, SPH a660), CFT-IM-06 (LG vx6100, SPH a660), CFT-IMO-04 (LG vx5400, LG vx6100, Moto V710, SCH u410, SCH u740, SPH a660), CFT-IMO-08 (LG vx5400, LG vx6100, Moto v710, SCH u410, SCH u740, SPH a660), the tested tool acquired all supported data objects completely and accurately from the selected test mobile devices (i.e., LG vx5400, LG vx6100, Moto v710, Samsung SCH u410, Samsung SCH u740, Samsung SPH a660). The exceptions are the following:

- The user is not informed when connectivity is disrupted (i.e., the cable is removed from the mobile device). Test Case: CFT-IM-03 (LG VX5400, LG VX6100, Moto V710, Samsung SCH u410, SCH u740, SPH a660).
- Address book entries are not reported properly when using the function: “separated names and numbers” for the LG vx6100. Reported address book do not provide an association between contact name and contact number for the SPH a660. Test Case: CFT-IM-06 (LG vx6100, SPH a660).

- When attempting to open a case file that has been modified with a hex editor, examiners are not informed the case file has been modified. Note: While the tool does not provide a warning message, modified case files cannot be opened. Test Case: CFT-IMO-04 (LG vx5400, LG vx6100, Moto v710, SCH u410, SCH u740, SPH a660).
- Address book entries and text messages containing non-ASCII characters such as: à, é were excluded from the address book entry and text message. Contacts and Text messages containing characters such as: 阿恶哈拉 were not reported. Test Case: CFT-IMO-08 (LG vx5400, LG vx6100, Moto v710, SCH u410, SCH u740, SPH a660).

For a complete copy of the report, go to:

<http://www.ojp.usdoj.gov/nij/pubs-sum/228227.htm>

Vendor information:

Final Data, Inc.

<http://www.finaldata.com>

TEST REPORT FOR: **PARABEN DEVICE SEIZURE 3.1**

September 2009

**The CFTT Project tested the Paraben Device Seizure 3.1 tool against the Mobile Device Specification available at:
http://www.cfft.nist.gov/mobile_devices.htm**

Our results are:

Except for the following test cases: CFT-IM-06 (LG VX6100), CFT-IM-07 (Samsung SCH-u40), CFT-IM-08 (LG VX5400, LG VX6100, Samsung SPH-a660), CFT-IM-09 (LG VX5400), CFT-IMO-05 (LG VX6100, Samsung SCH-u410, SCH-u740), the tested tool acquired all supported data objects completely and accurately from the selected test mobile devices (i.e., LG VX5400, LG VX6100, MOTO V710, Samsung SCH-u410, Samsung SCH-u740, Samsung SPH-a660). The exceptions are the following:

- Active address book entries were not acquired and reported. Test Case: CFT-IM- 06 (LG VX6100)
- Meta data (i.e., Status flags [Read, Unread], Phone Number [Sender, Receipt]) were incorrectly reported. Test Case: CFT-IM-08 (LG VX5400, LG VX6100, Samsung SPH-a660)
- Graphical images associated with MMS data were not displayed. Test Case: CFT-IM-09 (LG VX5400)
- Physical acquisitions (i.e., Memory Dump, GUID Properties) ended in errors. Test Case: CFT-IMO-05 (LG VX6100, Samsung SCH-u410, SCH-u740)

For a complete copy of the report, go to:

<http://www.ojp.usdoj.gov/nij/pubs-sum/228221.htm>

Vendor information:

Paraben Corporation

<http://www.paraben.com>

TEST REPORT FOR: CELLEBRITE UFED 1.1.05

September 2009

**The CFTT Project tested the Cellebrite UFED 1.1.05 tool against the Mobile Device Specification available at:
http://www.cfft.nist.gov/mobile_devices.htm**

Our results are:

Except for the following test cases: CFT-IM-03 (LG VX6100), CFT-IM-05 (SCH-u410, SCH-u740, SPH-a660), CFT-IM-07 (MOTO V710), CFT-IM-08 (MOTO V710), the tested tool acquired all supported data objects completely and accurately from the selected test mobile devices (i.e., LG VX5400, LG VX6100, Motorola V710, Samsung SCH-u410, Samsung SCH-u740, Samsung SPH-a660). The exceptions are the following:

- Connectivity disruptions between the mobile device (i.e., LG VX6100) and interface were not adequately presented to the examiner. Test Case: CFT-IM-03 (LG VX6100)
- The MIN was extracted instead of the MSISDN for the following Samsung devices: SCH-u410, SCH-u740, SPH-a660. Test Case: CFT-IM-05 (SCH-u410, SCH-u740,SPH-a660)
- Missed calls are reported as both Incoming and Missed, representing two calls rather than one. Test Case: CFT-IM-07 (MOTO V710)
- Text messages with a status of UNREAD were altered to READ. Test Case: CFT-IM-08 (MOTO V710)

- Outgoing text messages did not contain the outgoing date/time stamp. Test Case: CFT-IM-08 (MOTO V710)
- All outgoing text messages present in internal memory were not reported. Test Case: CFT-IM-08 (MOTO V710)

For a complete copy of the report, go to:

<http://www.ojp.usdoj.gov/nij/pubs-sum/228220.htm>

Vendor information:

Cellebrite USA Corp.

<http://www.cellebrite.com/>

TEST REPORT FOR:
MICRO SYSTEMATION .XRY 3.6

October 2008

**The CFTT Project tested the Micro Systemation .XRY 3.6 tool against the Mobile Device Specification available at:
http://www.cfft.nist.gov/mobile_devices.htm**

Our results are:

Except for the following test cases (CFT-IM-05, CFT-IM-06), the tested tool acquired all supported data objects completely and accurately from the selected test mobile devices and associated media (i.e., Nokia 6101, T-Mobile SIM, Motorola RAZR V3, AT&T SIM). The exceptions are the following:

- The MSISDN was not reported for the Nokia 6101 after a successful internal memory acquisition. (CFT-IM-05: Nokia 6101)
- Maximum length Notes created on the Nokia 6101 were truncated preventing the entire message to be acquired. The tool reports a maximum of 184 characters within a Note. (CFT-IM-06: Nokia 6101)

For a complete copy of the report, go to:
<http://www.ncjrs.gov/pdffiles1/nij/224148.pdf>

Vendor information:
Micro Systemation
<http://www.msab.com/>

TEST REPORT FOR: GUIDANCE SOFTWARE NEUTRINO 1.4.14

October 2008

The CFTT Project tested the Guidance Software Neutrino 1.4.14 tool against the Mobile Device Specification available at:
http://www.cfft.nist.gov/mobile_devices.htm

Our results are:

Except for the following test cases (CFT-IM-08, CFT-SIM-07, CFT-IMO-10), the tested tool acquired all supported data objects completely and accurately from the selected test mobile devices and associated media (i.e., Nokia 6101, T-Mobile SIM, Motorola RAZR V3, AT&T SIM). The exceptions are the following:

- EMS messages (text messages over 160 characters were not acquired for the Motorola RAZR V3). (CFT-IM-08)
- Maximum length ADNs and ADNs that contain special characters for the name (i.e., '@') were not reported. (CFT-SIM-07)
- Stand-alone internal memory acquisitions alter the status flags of 'unread' text messages present on the SIM to 'read'. (CFT-IMO-10)

For a complete copy of the report, go to:
<http://www.ncjrs.gov/pdffiles1/nij/224150.pdf>

Vendor information:
Guidance Software Neutrino
<http://www.guidancesoftware.com/>

TEST REPORT FOR:
PARABEN DEVICE SEIZURE 2.1

October 2008

**The CFTT Project tested the Paraben Device Seizure 2.1 tool against the Mobile Device Specification available at:
http://www.cfft.nist.gov/mobile_devices.htm**

Our results are:

All supported data objects completely and accurately from the Nokia 6101, T-Mobile SIM, Motorola RAZR V3, and AT&T SIM.

For a complete copy of the report, go to:
<http://www.ncjrs.gov/pdffiles1/nij/224149.pdf>

Vendor information:
Paraben Corporation
<http://www.paraben.com/>

TEST REPORT FOR: SUSTEEN DATAPILOT SECURE VIEW 1.8.0

October 2008

**The CFTT Project tested the Susteen DataPilot Secure View 1.8.0 tool against the Mobile Device Specification available at:
http://www.cfft.nist.gov/mobile_devices.htm**

Our results are:

Except for the following test cases (CFT-IM-05, CFT-IM-08, CFT-IMO-09, CFT-SIM-03, CFT-SIM-06, CFT-SIM-09, CFT-SIMO-01, CFT-SIMO-05), the tested tool acquired all supported data objects completely and accurately from the selected test mobile devices and associated media (i.e., Nokia 6101, T-Mobile SIM, Motorola RAZR V3, AT&T SIM). The exceptions are the following:

- The MSISDN was not acquired from the Nokia 6101. (CFT-IM-05)
- EMS messages (messages over 160 characters) are not reported in their entirety. Messages are truncated after the 160th character. (CFT-IM-08)
- Address book entries (i.e., Device Internal Memory-contacts) containing foreign characters (i.e., Chinese) are not displayed. Foreign text messages (i.e., French, Chinese) present in the device internal memory are either partially acquired but not properly displayed, or not reported (i.e., Chinese text messages – Motorola RAZR). (CFT-IMO-09)
- No warning messages are displayed to the examiner of SIM connectivity issues during acquisition, if the SIM is pulled from the reader. (CFT-SIM-03)

- The Service Provider Name (SPN) is not reported from the SIM acquisitions. (CFT-SIM-06)
- EMS messages present on the AT&T SIM, with the status of Unread were acquired but not properly presented (i.e., the text characters were not consistent with the pre-defined data set. The reported characters were random ASCII characters and symbols. (CFT-SIM-09)
- Complete representation of known data contained on the internal memory of the AT&T SIM presented via generated reports was not consistent with the pre-defined dataset. (CFT-SIMO-01)
- Deleted EMS messages present on the AT&T SIM were partially acquired but not properly presented. (CFT-SIMO-05)
-

For a complete copy of the report, go to:

<http://www.ncjrs.gov/pdffiles1/nij/223997.pdf>

Vendor information:

Susteen, Inc.

<http://www.susteen.com/>