Computer Forensics Tool Testing Handbook

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.

Revised Date: 02/01/2012

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

OLES

NIJ
National Institue of
Justice

TABLE OF CONTENTS

Disk Imaging

Forensic Media Preparation

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

- AFLogical 1.4
- Mobilyze 1.1
- iXAM Version 1.5.6
- Zdziarski's Method
- WinMoFo Version 2.2.38791
- SecureView 2.1.0
- Device Seizure 4.0
- XRY 5.0.2
- CelleBrite UFED 1.1.3.3
- 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

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

DISK IMAGING

TEST REPORT FOR:
IMAGE MASSTER SOLO-3 FORENSICS; SOFTWARE VERSION 2.0.10.23F

December 2011

The CFTT Project tested the Image MASSter Solo-3 Forensics; Software Version 2.0.10.23f against the Digital Data Acquisition Tool Specification available at: http://www.cftt.nist.gov/disk_imaging.htm

Our results are:

The tool acquired source drives completely and accurately with the exception of four cases: a case where a source drive containing faulty sectors was imaged and the tool was configured to skip sectors in the same block as faulty sectors; a case where the tool was configured to restore an image file to two destination drives; a case where a drive was cloned with the *Lg-XferBlk* option enabled; and a case where the tool was configured to clone a drive that had not been removed from a laptop. The tool reported incorrect hash values in two cases: a case where insufficient space existed on the destination volume and multiple destination volumes were used (i.e., drive spanning) and a case that tested restoring that image to a clone. Two test cases involve creating truncated clones. In one case a truncated clone was created from a source drive and in the other a truncated clone was created from an image file. In both cases the tool did not notify the user that a truncated clone had been created.
The following behaviors was observed:

- Less than 20 percent of source drive sectors were copied accurately when the Lg-XferBlk setting was selected (DA-01-SATA48).

- When two drives were selected as targets for a restore from a single image file, one of the clones that was created was inaccurate and incomplete (DA-14-SATA28/DA-14-SATA28-EVIDENCEII).

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

OLES

NIJ National Institue of Justice

- The Readable sectors that were in the same imaging block as faulty sectors on a source drive were not acquired when the Skip Block imaging option was selected. The tool wrote zeros to the target drive in place of these sectors. This is the behavior intended for the tool by the vendor (DA-09-SKIPBLOCK).

- The tool failed to notify the user when a truncated clone was created from a physical device (DA-04).

- The tool failed to give a meaningful error message when creating a truncated clone from an image file (DA-17).

- The hash value reported by the tool was incorrect when insufficient space existed on the destination volume and multiple destination volumes (drive spanning) were used (DA-13).

- When restoring to a clone the image that was created using multiple destination volumes and drive spanning, the hash value reported by the tool was incorrect (DA-14-HOT).

- The tool has a procedure for acquiring a drive without removing the drive from the host computer. An attempt to acquire a drive over the FireWire interface was not successful (DA-01-FWLAP).

For a complete copy of the report, go to:
http://www.nij.gov/pubs-sum/235710.htm

Vendor information:
Intelligent Computer Solutions, Inc.
http://www.ics-iq.com

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

DISK IMAGING

TEST REPORT FOR:
TABLEAU TD1 FORENSIC DUPLICATOR; FIRMWARE VERSION 2.34 FEB 17, 2011

December 2011

The CFTT Project tested the Tableau TD1 Forensic Duplicator; Firmware Version 2.34 Feb 17, 2011, against the Digital Data Acquisition Tool Specification available at: http://www.cftt.nist.gov/disk_imaging.htm

Our results are:

The tool acquired source drives completely and accurately with the exception of the following: one case where a source drive containing faulty sectors was imaged, and two cases where source drives containing hidden sectors were imaged. In addition, there were two cases where the tool generated bogus alert messages in place of alerting the user to the presence of hidden sectors on the source drive.

The following behaviors were observed:

- When the tool was executed using the fast error recovery mode and faulty sectors were encountered, some readable sectors near the faulty sectors were replaced by zeros in the created clone (test case DA-09-FAST). This is the intended tool behavior as specified by the tool vendor.

- In two cases, DA-08-ATA28 (drive containing an HPA) and DA-08-DCO-ALT (drive containing a DCO), in place of alerting the user of hidden sectors on the source drive, the tool issued bogus alerts stating that the "Source disk may be blank." In case DA-08-ATA28, the tool removed the HPA from the source and all sectors were acquired. In case DA-08-DCO-ALT, the tool did not remove the DCO from the source and hidden sectors were not acquired.

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

OLES

NIJ
National Institue of Justice

- The tool does not automatically remove DCOs from source drives but is designed to alert the user when a DCO exists. A user may cancel the duplication process and manually remove the DCO using the “Disk Utilities” *Remove DCO & HPA* menu option. In cases DA-08-DCO and DA-08-DCO-ALT, the *Remove DCO & HPA* option was not exercised and sectors hidden by a DCO were not acquired. In case DA-08-DCO-ALT-SATA, the *Remove DCO & HPA* option was exercised to remove the DCO and all sectors were successfully acquired.

For a complete copy of the report, go to:
http://www.nij.gov/pubs-sum/236223.htm

Vendor information:
Guidance Software, Inc.
http://www.tableau.com

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

DISK IMAGING

TEST REPORT FOR:
TABLEAU IMAGER (TIM) VERSION 1.11

March 2011

The CFTT Project tested the Tableau Imager (TIM) Version 1.11 against the Digital Data Acquisition Tool Specification available at: http://www.cftt.nist.gov/disk_imaging.htm

Our results are:

The Tableau Imager is designed to work only with Tableau write block devices. This allows the Tableau Imager to exploit features of the Tableau write block devices.

Except for two test cases, DA-09-FW and DA-09-USB, the tested tool acquired all visible and hidden sectors completely and accurately from the test media without anomaly. The following behavior was observed:

- If the tool is executed with the quick recovery option specified and the tool encounters a defective sector, some readable sectors near the defective sector are replaced by zeros in the created image file (test cases DA-09-FW and DA-09-USB). This is the behavior intended for the tool by the software vendor.

For a complete copy of the report, go to:
http://www.nij.gov/pubs-sum/233984.htm

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

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

OLES

NIJ
National Institue of Justice

TEST REPORT FOR:
SUBROSASOFT MACFORENSICS LAB 2.5.5

September 2010

The CFTT Project tested the SubRosaSoft MacForensics Lab 2.5.5 against the Digital Data Acquisition Tool Specification available at: http://www.cftt.nist.gov/disk_imaging.htm

Our results are:

The tool acquired source drives completely and accurately except for in the cases where source drives containing faulty sectors were imaged or where a source drive containing a Host Protected Area (HPA) was imaged through a vendor-recommend write blocker. The following anomalies were observed:

- Ranges for acquisition hashes are recorded incorrectly in the tool-generated HTML report for media and volumes larger than 2 GB.
- Ranges for block hashes are recorded incorrectly in the tool-generated HTML report for ranges that cover portions of source media beyond 2 GB (DA–06–SATA48, DA–06–USB, DA–07–EXT2, DA–07–OSXJ, DA–08–DCO).
- The sectors hidden by a Device Configuration Overlay (DCO) or HPA are not acquired (DA–08–DCO, DA–08–SATA28, DA–08–SATA28–ALT, and DA–08–SATA48).
- Visible sectors (sectors not hidden by an HPA) may not be acquired when a drive containing an HPA is imaged through a vendor-recommend write blocker (DA–08–SATA28).

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

OLES

NIJ National Institue of Justice

- The tool is inconsistent in notifying the user of read errors. After acquisitions of drives with faulty sectors are complete no tool notification or record is immediately available to alert the user that read errors occurred (DA–09–ALT, DA–09–INTEL, and DA–09–PPC).

- Good sectors that follow faulty sectors are not acquired, and other data is written in the place of these sectors (DA–09–ALT, DA–09–INTEL, and DA–09–PPC).

- Data for faulty sectors is replaced in image files with data from an undetermined source (DA–09–ALT, DA–09–INTEL, and DA–09–PPC).

For a complete copy of the report, go to:
http://www.ojp.usdoj.gov/nij/pubs-sum/231623.htm

Vendor information:
SubRosaSoft.com Inc.
http://www.macforensicslab.com

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

DISK IMAGING

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.cftt.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/

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

NIJ
National Institue of Justice

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

DISK IMAGING

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.cftt.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).

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

OLES

NIJ National Institute of Justice

- 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/

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

DISK IMAGING

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).

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

OLES

NIJ
National Institute of Justice

- 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/

Contact: James Lyle
Computer Forensics Tool Testing Program
Office of Law Enforcement Standards
National Institute of Standards and Technology

DISK IMAGING

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/

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

OLES

NIJ
National Institue of Justice

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

DISK IMAGING

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.

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

NIJ
National Institute of Justice

- 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/

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

DISK IMAGING

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

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

OLES

NIJ
National Institute of Justice

Vendor information:
AccessData
http://www.accessdata.com

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

DISK IMAGING

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/

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

NIJ
National Institue of Justice

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

DISK IMAGING

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).

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

NIJ
National Institue of Justice

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/

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

DISK IMAGING

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.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 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/

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

OLES

NIJ
National Institute of Justice

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

DISK IMAGING

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

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

NIJ
National Institue of Justice

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

DISK IMAGING

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.

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

OLES

NIJ
National Institute of Justice

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

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

DISK IMAGING

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/

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

DISK IMAGING

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.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. 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.

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

OFFICE OF LAW ENFORCEMENT STANDARDS
OLES

NIJ
National Institute of Justice

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/

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

DISK IMAGING

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.cftt.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.

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

OLES

NIJ
National Institue of Justice

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/

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

DISK IMAGING

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.cftt.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.

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

NIJ
National Institute of Justice

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:
DC3DD: VERSION 7.0.0

December 2011

The CFTT Project tested the dc3dd: Version 7.0.0 against the Forensic Media Preparation Specification available at: http://www.cftt.nist.gov/forensic_media.htm

Our results are:

The dc3dd tool can be used for a variety of forensic tasks (e.g., disk imaging or wiping media for reuse). This report only examines using the tool to overwrite media for reuse.

In all the test cases run against dc3dd version 7.0.0, all visible sectors were successfully overwritten. Sectors hidden by an HPA (FMP-03-HPA and FMP-03-DCO-HPA) were also overwritten; however, sectors hidden by a DCO were not removed (FMP-03-DCO and FMP-03-DCO-HPA). By design, the tool does not remove either Host Protected Areas (HPAs) or DCOs. However, the Linux test environment used automatically removed the HPA on test drives, allowing sectors hidden by an HPA to be overwritten by the tool.

Table 1 provides a quick overview of the test case results.

Table 1. Overview of Test Results

Test Case	Total Sectors	First Sector Overwritten	Last Sector Overwritten	Unchanged Sectors	
				First	Last
FMP-01-ATA28	156301488	0	156301487		
FMP-01-ATA48	488397168	0	488397167		
FMP-01-FW	488397168	0	488397167		
FMP-01-SATA28	78140160	0	78140159		
FMP-01-SATA48	312581808	0	312581807		
FMP-01-SCSI	71721820	0	71721819		
FMP-01-USB	488397168	0	488397167		
FMP-03-DCO	490234752	0	480234751	480234752	490234751
FMP-03-DCO-HPA	234441648	0	224441647	224441648	234441647
FMP-03-HPA	312581808	0	312581807		

For a complete copy of the report, go to:
http://www.ojp.usdoj.gov/nij/pubs-sum/236225.htm

Supplier information:
Department of Defense Cyber Crime Center
http://www.dc3.mil/dc3/dc3About.php

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

FORENSIC MEDIA PREPARATION

TEST REPORT FOR:
IMAGE MASSTER SOLO-4 FORENSICS; SOFTWARE VERSION 4.2.63.0

December 2011

The CFTT Project tested the Image MASSter Solo-4 Forensics; Software Version 4.2.63.0 against the Forensic Media Preparation Specification available at: http://www.cftt.nist.gov/forensic_media.htm

Our results are:

The Image MASSter Solo-4 Forensics is a multifunctional forensics hand-held disk duplicator. It supports disk wiping on drives attached to the Evidence Collecting interface. The wipeout function supports three modes for executing a drive wipe: single pass, full Department of Defense (DoD) Sanitization, and secure erase.

The following anomalies were observed for the Image MASSter Solo-4:

- For one particular hard drive model used in testing, Seagate ST3160815AS, the Solo-4 device halted after drive identification and did not erase any sectors. (Test case FMP-02-SATA48.)

- The Solo-4 did not handle drives correctly if there was a Device Configuration Overlay (DCO) present on the test drive. The following three behaviors were observed:

    - Test case FMP-03-DCO: The DCO was not erased and the 48 visible sectors immediately preceding the DCO also were not erased. However, the remaining visible sectors were erased.

- Test case FMP-03-DCO2: The last sector of the DCO was not erased. All other sectors, both hidden and visible, were erased.

- Test cases FMP-03-DCO-HPA and FMP-04-DCO-HPA: The sectors in the DCO were not erased. All visible sectors and all sectors in the Host Protected Area (HPA) were erased.

The following table provides a quick overview of the test case results:

Test Case	First Sector Overwritten	Last Sector Overwritten	Unchanged Sectors	
			First	Last
FMP-01-ATA28	0	156301487		
FMP-01-ATA48	0	488397167		
FMP-01-SATA28	0	78140159		
FMP-01-SATA48	0	312581807		
FMP-01-USB	0	488397167		
FMP-02-ATA28	0	156301487		
FMP-02-ATA48	0	490234751		
FMP-02-SATA28	0	156301487		
FMP-02-SATA48	N/A	N/A	0	312581807
FMP-03-DCO	0	146301439	146301440	156301487
FMP-03-DCO-2	0	156301486	156301487	156301487
FMP-03-HPA	0	390721967		

FMP-03-DCO-HPA	0	478397167	478397168	488397167
FMP-04-DCO	0	976773167		
FMP-04-DCO-HPA	0	380721967	380721968	390721967
FMP-04-HPA	0	234441647		
FMP-05	N/A	N/A	N/A	N/A

For a complete copy of the report, go to:
http://www.ojp.usdoj.gov/nij/pubs-sum/235711.htm

Vendor information:
Intelligent Computer Solutions, Inc.
http://www.ics-iq.com/

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

FORENSIC MEDIA PREPARATION

TEST REPORT FOR:
TABLEAU TDW1 DRIVE TOOL/DRIVE WIPER – FIRMWARE VERSION: 04/07/10 18:21:33

December 2011

The CFTT Project tested the Tableau TDW1 Drive Tool/Drive Wiper – Firmware Version: 04/07/10 18:21:33 against the Forensic Media Preparation Specification available at: http://www.cftt.nist.gov/forensic_media.htm

Our results are:

The Tableau TDW1 Drive Tool / Drive Wiper is a multipurpose tool designed to erase SATA hard drives. It provides single- or multi-pass drive wiping options accessible from a menu-driven interface located on the front panel of the device.

In all the test cases, the Tableau TDW1 Drive Tool / Drive Wiper - version 04/07/10 18:21:33 overwrote all visible sectors successfully.

The tool does not automatically remove hidden sectors from source drives but is designed to alert the user when hidden sectors exist. The user may either leave the hidden sectors as is or manually remove them using the “Disk Utilities” Remove DCO & HPA menu option. In cases FMP-03-DCO-2, FMP-03-DCO-HPA-2 and FMP-03-HPA-2, the Remove DCO & HPA option was not exercised and hidden sectors were not overwritten. In cases FMP-03-DCO, FMP-03-DCO-HPA and FMP-03-HPA, the Remove DCO & HPA option was exercised and all sectors were successfully overwritten.

Table 1 provides a brief overview of the test case results.

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

OLES

NIJ
National Institue of Justice

Table 1. Overview of Test Results

Test Case	Total Sectors	First Sector Overwritten	Last Sector Overwritten	Unchanged Sectors	
				First	Last
FMP-01-SATA-28	78140160	0	78140159		
FMP-01-SATA48	312581808	0	312581807		
FMP-03-DCO	234441648	0	234441647		
FMP-03-DCO-2	390721968	0	380721966	380721967	390721967
FMP-03-DCO-HPA	488397168	0	488397167		
FMP-03-DCO-HPA-2	234441648	0	209441646	209441647	234441647
FMP-03-HPA	156301488	0	156301487		
FMP-03-HPA-2	390721968	0	375721966	375721967	390721967

For a complete copy of the report, go to:
http://www.ojp.usdoj.gov/nij/pubs-sum/236222.htm

Vendor information:
Guidance Software, Inc.
http://www.tableau.com/

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

FORENSIC MEDIA PREPARATION

TEST REPORT FOR: DISK JOCKEY PRO FORENSIC EDITION (VERSION 1.20)

October 2010

The CFTT Project tested the Disk Jockey PRO Forensic Edition (version 1.20) against the Forensic Media Preparation Specification available at: http://www.cftt.nist.gov/forensic_media.htm

Our results are:

In all the test cases run against Disk Jockey Forensic, 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 as follows:

- In the two single pass mode tests (FMP–03–DCO–2 & FMP–03–DCO–HPA–2), the HPA and DCO remained intact; hidden sectors were not overwritten.

- In DoD x7 pass mode, HPA hidden sectors were removed and overwritten (FMP– 03–HPA–2).

The vendor clarified the tool behavior with the following statement:

- DATA ERASE DoD—This mode erases the data of the attached HDD by writing seven–passes per the standard established by the Department of Defense. NOTE: This mode will also remove (reset) any HPA or DCO settings before proceeding to erase/wipe the disk, therefore every usable sector of the disk, including any sectors formerly within an HPA or DCO area will also be erased/wiped.

- DATA ERASE 00x1—This mode completes a one–pass erase on the disk by writing 00h bytes in all sectors of the connected HDD. NOTE: This mode will not remove either an HPA or DCO area from the disk; nor will it erase/wipe any sectors in those areas.

For a complete copy of the report, go to:
http://www.ojp.usdoj.gov/nij/pubs-sum/231988.htm

Vendor information:
Diskology
http://www.diskology.com/

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

FORENSIC MEDIA PREPARATION

TEST REPORT FOR:
DRIVE ERAZER PRO SE BUNDLE 12-03-2009

September 2010

The CFTT Project tested the Drive eRazer Pro SE Bundle 12-03-2009 against the Forensic Media Preparation Specification available at: http://www.cftt.nist.gov/forensic_media.htm

Our results are:

The Drive eRazer Pro SE Bundle disk wiping tool supports the use of both the ATA WRITE command and the ATA SECURITY ERASE command for erasing hard drives. The use of both commands was tested.

In all the test cases run against Drive eRazer Pro SE Bundle, all visible sectors were successfully overwritten. For the test cases that used drives containing an HPA or DCO, the tool removed HPAs and DCOs and overwrote the previously hidden sectors with one exception. For test case, FMP–03–DCO–HPA, it was observed that the device removed the HPA while overwriting sectors that were previously hidden, but left the DCO intact on the target drive leaving the sectors hidden by the DCO unchanged. This behavior was limited to Fujitsu drives.

The following table provides a quick overview of the test case results:

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

NIJ
National Institue of Justice

Test Case	Drive Last Sector	Last Sector Overwritten	Unchanged Sectors	
			First	Last
FMP-01-ATA28	156301487	156301487		
FMP-01-ATA48	488397167	488397167		
FMP-01-SATA28	234441647	234441647		
FMP-01-SATA48	390721967	390721967		
FMP-02-ATA28	156301487	156301487		
FMP-02-ATA48	490234751	490234751		
FMP-02-SATA28	234441647	234441647		
FMP-02-SATA48	312581807	312581807		
FMP-03-DCO	302581807	302581807		
FMP-03-HPA	78140159	78140159		
FMP-03-DCO-HPA	156301487	146301487	146301488	156301487
FMP-04-DCO	156301487	156301487		
FMP-04-DCO-HPA	465234751	490234751		
FMP-04-HPA	297581807	312581807		
FMP-05	NA	NA	NA	

For a complete copy of the report, go to:
http://www.ojp.usdoj.gov/nij/pubs-sum/231621.htm

Vendor information:
CRU-DataPort/WiebeTech
http://www.wiebetech.com

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

FORENSIC MEDIA PREPARATION

TEST REPORT FOR:
TABLEAU FORENSIC DUPLICATOR MODEL TD1 (FIRMWARE VERSION 2.10)

September 2010

The CFTT Project tested the Tableau Forensic Duplicator Model TD1 (Firmware Version 2.10) against the Forensic Media Preparation Specification available at: http://www.cftt.nist.gov/forensic_media.htm

Our results are:

The Tableau Forensic TD1 is a multi-function forensic device that performs a variety of forensic functions including: Disk-to-Disk duplication, Disk-to-File duplication, Format Disk, Wipe Disk, Hash Disk (MD5 and SHA–1), HPA/DCO Detection and Removal, View/Save/Print Log Files and Blank Disk Check. This report only covers disk wiping and removal of HPA/DCO for wiping of hidden sectors. For disk wiping, a drive must be attached to the destination side of the unit. A user can then navigate using menu options to enter the disk utility where controls are located for removing an HPA or DCO. This process was used to successfully remove hidden sectors before a drive was wiped using the overwrite command of the unit. In all the test cases run against Tableau Forensic Duplicator Model TD1, all visible and hidden sectors were successfully overwritten.

The following table provides a quick overview of test cases, settings and findings for each test case:

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

NIJ
National Institue of Justice

Test Case	Target Fill	Last Sector	Last Sector Overwritten	Unchanged Sectors	
				First	Last
FMP-01-ATA28	00h	156301487	156301487		
FMP-01-ATA48	Random	488397167	488397167		
FMP-01-SATA28	00h	78140159	78140159		
FMP-01-SATA48	Random	312581807	312581807		
FMP-03-DCO	00h	390721967	390721967		
FMP-03-HPA	Random	156301487	156301487		
FMP-03-DCO-HPA	Random	488397167	488397167		

For a complete copy of the report, go to:
http://www.ojp.usdoj.gov/nij/pubs-sum/231622.htm

Vendor information:
Tableau, LLC
http://www.tableau.com

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

FORENSIC MEDIA PREPARATION

TEST REPORT FOR:

LOGICUBE OMNICLONE 2XI (SOFTWARE 1.53 JUNE 19, 2009, FIRMWARE VERSION 9.0)

June 2010

The CFTT Project tested the Logicube Omniclone 2Xi (Software 1.53 June 19, 2009, Firmware 9.0) against the Forensic Media Preparation Specification available at: http://www.cftt.nist.gov/forensic_media.htm

Our results are:

In all the test cases run against Logicube Omniclone 2Xi, 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/230566.htm

Vendor information:
Logicube
http://www.logicube.com

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

NIJ
National Institute of Justice

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

FORENSIC MEDIA PREPARATION

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.cftt.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

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

OLES

NIJ
National Institue of Justice

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

FORENSIC MEDIA PREPARATION

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.cftt.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

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

OLES

NIJ National Institue of Justice

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

FORENSIC MEDIA PREPARATION

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.cftt.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/

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

WRITE BLOCK (SOFTWARE)

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.cftt.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

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

NIJ
National Institue of Justice

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.cftt.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.

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

WRITE BLOCK (SOFTWARE)

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.

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

NIJ National Institue of Justice

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

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

WRITE BLOCK (SOFTWARE)

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.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. 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.

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

OLES

NIJ
National Institue of Justice

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

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

WRITE BLOCK (SOFTWARE)

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.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 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.

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

OLES

NIJ National Institue of Justice

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

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

WRITE BLOCK (SOFTWARE)

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.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 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.

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

OLES

NIJ National Institute of Justice

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

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

WRITE BLOCK (SOFTWARE)

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.cftt.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 accessability 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.

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

NIJ
National Institue of
Justice

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

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

WRITE BLOCK (SOFTWARE)

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.cftt.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 accessability 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.

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

OLES

NIJ
National Institute of Justice

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

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

WRITE BLOCK (SOFTWARE)

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.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 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

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

NIJ
National Institue of Justice

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

WRITE BLOCK (HARDWARE)

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.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/228225.htm

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

OLES

NIJ
National Institue of Justice

Vendor information:
Tableau, LLC
http://www.tableau.com/

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

WRITE BLOCK (HARDWARE)

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.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/228224.htm

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

NIJ
National Institue of Justice

Vendor information:
Tableau, LLC
http://www.tableau.com/

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

WRITE BLOCK (HARDWARE)

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.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/223431.htm

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

NIJ
National Institue of Justice

Vendor information:
Tableau, LLC
http://www.tableau.com/

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

WRITE BLOCK (HARDWARE)

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.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/223432.htm

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

OLES

NIJ National Institute of Justice

Vendor information:
Tableau, LLC
http://www.tableau.com/

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

WRITE BLOCK (HARDWARE)

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.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/218378.htm

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

NIJ National Institue of Justice

Vendor information:
Guidance Software, Inc.

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

WRITE BLOCK (HARDWARE)

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.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/218379.htm

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

OLES

NIJ
National Institue of Justice

Vendor information:
Guidance Software, Inc.

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

WRITE BLOCK (HARDWARE)

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.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/218380.htm

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

NIJ National Institue of Justice

Vendor information:
Tableau, LLC
http://www.tableau.com/

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

WRITE BLOCK (HARDWARE)

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.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/218381.htm

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

NIJ National Institue of Justice

Vendor information:
Tableau, LLC
http://www.tableau.com/

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

WRITE BLOCK (HARDWARE)

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.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/216981.htm

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

NIJ
National Institue of Justice

Vendor information:
Tableau, LLC
http://www.tableau.com/

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

WRITE BLOCK (HARDWARE)

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.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/216982.htm

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

OLES

NIJ
National Institue of
Justice

Vendor information:
Tableau, LLC
http://www.tableau.com/

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

WRITE BLOCK (HARDWARE)

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

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

NIJ National Institue of Justice

Vendor information:
Tableau, LLC
http://www.tableau.com/

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

WRITE BLOCK (HARDWARE)

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.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/216300.htm

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

NIJ
National Institue of
Justice

Vendor information:
WiebeTech, LLC
http://www.wiebetech.com/

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

WRITE BLOCK (HARDWARE)

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.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/216299.htm

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

NIJ
National Institue of Justice

Vendor information:
WiebeTech, LLC
http://www.wiebetech.com/

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

WRITE BLOCK (HARDWARE)

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.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/214063.htm

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

OLES

NIJ
National Institue of
Justice

Vendor information:
WiebeTech, LLC
http://www.wiebetech.com/

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

WRITE BLOCK (HARDWARE)

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.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/214064.htm

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

NIJ National Institue of Justice

Vendor information:
WiebeTech, LLC
http://www.wiebetech.com/

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

WRITE BLOCK (HARDWARE)

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.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/214065.htm

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

NIJ National Institute of Justice

Vendor information:
WiebeTech, LLC
http://www.wiebetech.com/

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

WRITE BLOCK (HARDWARE)

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

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

OLES

NIJ National Institue of Justice

Vendor information:
WiebeTech, LLC
http://www.wiebetech.com/

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

WRITE BLOCK (HARDWARE)

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.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/214067.htm

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

NIJ National Institue of Justice

Vendor information:
Digital Intelligence
http://www.DigitalIntelligence.com/

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

WRITE BLOCK (HARDWARE)

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.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/212956.htm

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

NIJ
National Institue of Justice

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

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

WRITE BLOCK (HARDWARE)

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

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

NIJ National Institue of Justice

Vendor information:
MyKey Technology, Inc.

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

WRITE BLOCK (HARDWARE)

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.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/212959.htm

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

NIJ
National Institue of Justice

Vendor information:
Intelligent Computer Solutions, Inc.
http://www.ics-iq.com/

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

WRITE BLOCK (HARDWARE)

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.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/212960.htm

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

NIJ National Institue of Justice

Vendor information:
WiebeTech LLC
http://www.wiebetech.com/

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

WRITE BLOCK (HARDWARE)

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.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/212957.htm

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

NIJ
National Institue of Justice

Vendor information:
Digital Intelligence
http://www.DigitalIntelligence.com/

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

WRITE BLOCK (HARDWARE)

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.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/212961.htm

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

NIJ National Institue of Justice

Vendor information:
Digital Intelligence
http://www.DigitalIntelligence.com/

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

MOBILE DEVICES

TEST REPORT FOR:
AFLOGICAL 1.4

December 2011

The CFTT Project tested the AFLogical 1.4 tool against the Mobile Device Specification available at: http://www.cftt.nist.gov/mobile_devices.htm

Our results are:

The tool logically acquired active data elements from the mobile device internal memory completely and accurately except for the following cases: a case where acquisition of Personal Information Management (PIM) data was attempted and a case where acquisition of Multimedia Messaging Service (MMS) data was attempted. Additionally, in a case that tested the tools behavior when connectivity is interrupted, the tool failed to notify the user that the acquisition had been disrupted.

The following anomalies were observed:

- Graphics files associated with address book entries were not reported. Test Case: SPT-06 (Droid 2, Droid X, Nexus One, Samsung Moment).
- Regular and maximum length PIM data (calendar entries, memos) were not reported. Test Case: SPT-06 (Droid 2, Droid X).
- Maximum length PIM data (memos) were not reported. Test Case: SPT-06 (Samsung Moment).
- The textual portions of outgoing MMS messages were not reported. Test Case: SPT-09 (Samsung Moment).
- Notification of device disruption during acquisition was not successful. Test Case: SPT-03 (Droid 2, Droid X, Nexus One, Samsung Moment).

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

NIJ
National Institue of Justice

For a complete copy of the report, go to:
http://www.nij.gov/pubs-sum/235712.htm

Supplier information:
viaForensics
http://www.viaforensics.com

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

MOBILE DEVICES

TEST REPORT FOR:
MOBILYZE VERSION 1.1

February 2011

The CFTT Project tested the Mobilyze Version 1.1 tool against the Mobile Device Specification available at: http://www.cftt.nist.gov/mobile_devices.htm

Our results are:

Except for the following test cases: SPT–03, SPT–06, SPT–08, SPT–33, the tested tool acquired all supported data objects completely and accurately from the selected test mobile device (i.e., iPhone 3Gs). The exceptions were the following:

- Notification of device acquisition disruption was not successful. Test Case: SPT-03.

- Maximum length address book entries reported in the preview-pane view were truncated. Test Case: SPT-06.

- The delivery time for text messages displayed in the “Messages” tab are not reported. Test Case: SPT-08.

- Non-ASCII address book entries and text messages are not properly reported in their native format. Test Case: SPT-33.

For a complete copy of the report, go to:
http://www.nij.gov/pubs-sum/232744.htm

Vendor information:
BlackBag Technologies, Inc.
http://www.blackbagtech.com

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

OLES

NIJ
National Institue of Justice

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

MOBILE DEVICES

TEST REPORT FOR:

IXAM VERSION 1.5.6

December 2010

The CFTT Project tested the iXAM Version 1.5.6 tool against the Mobile Device Specification available at: http://www.cftt.nist.gov/mobile_devices.htm

Our results are:

> The tested tool acquired all supported data objects completely and accurately from the selected test mobile device (i.e., iPhone 3G). No anomalies were found.

For a complete copy of the report, go to:
http://www.nij.gov/pubs-sum/232384.htm

Vendor information:
http://www.forensicts.co.uk

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

NIJ
National Institue of Justice

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

MOBILE DEVICES

TEST REPORT FOR:
ZDZIARSKI'S METHOD

December 2010

The CFTT Project tested the Zdziarski's Method tool against the Mobile Device Specification available at: http://www.cftt.nist.gov/mobile_devices.htm

Our results are:

The tested tool acquired all supported data objects completely and accurately from the selected test mobile device (i.e., iPhone 3Gs). No anomalies were found.

For a complete copy of the report, go to:
http://www.nij.gov/pubs-sum/232383.htm

Vendor information:
http://www.iphoneinsecurity.com

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

NIJ
National Institue of Justice

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

MOBILE DEVICES

TEST REPORT FOR:
WINMOFO VERSION 2.2.38791

November 2010

The CFTT Project tested the WinMoFo Version 2.2.38791 against the Mobile Device Specification available at: http://www.cftt.nist.gov/mobile_devices.htm

Our results are:

Except for the following test cases: SPT–06 (HTC Touch Pro 2), SPT–08 (HTC Tilt2, HTC Touch Pro 2), SPT–09 (HTC Tilt2, HTC Touch Pro 2), SPT–10 (HTC Tilt2, HTC Touch Pro 2) the tested tool acquired all supported data objects completely and accurately from the selected test mobile devices (i.e., HTC Tilt2, HTC Touch Pro 2). The exceptions were the following:

- Maximum length calendar entries are not reported. Test Case: SPT–06 (HTC Touch Pro 2)
- The textual portion of draft text messages was not reported. Test Case: SPT–08 (HTC Tilt2)
- The incorrect date and time was reported for draft text messages. Test Case: SPT–08 (HTC Tilt2)
- MMS attachments (audio, video, graphics) for incoming messages were not reported. Test Case: SPT–09 (HTC Tilt2)
- MMS text and attachments (video, graphics) were not reported. Test Case: SPT–09 (HTC Touch Pro 2)

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

OLES

NIJ National Institue of Justice

- Video files of type .flv were not acquired. Test Case: SPT–10 (HTC Tilt2, HTC Touch Pro 2)

For a complete copy of the report, go to:
http://www.ojp.usdoj.gov/nij/pubs-sum/232224.htm

Vendor information:
DelMar Information Technologies, LLC
http://www.winmofo.com

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

MOBILE DEVICES

TEST REPORT FOR:
SECURE VIEW 2.1.0

November 2010

The CFTT Project tested the Secure View 2.1.0 against the Mobile Device Specification available at: http://www.cftt.nist.gov/mobile_devices.htm

Our results are:

Except for the following test cases: SPT-01 (iPhone 3Gs), SPT-03 (Blackberry Bold 9700, HTC Touch Pro 2, Blackberry 9630), SPT-06 (Blackberry Bold 9700, HTC Tilt 2, Nokia e71x, HTC Touch Pro 2, Blackberry 9630), SPT-13 (HTC Touch Pro 2, Blackberry 9630), SPT-33 (Blackberry Bold 9700, HTC Tilt 2, HTC Touch Pro 2, Blackberry 9630, Samsung Moment), SPT-34 (iPhone 3Gs, Blackberry Bold 9700, HTC Tilt2, Nokia e71x), SPT-10 (Nokia e71x, HTC Touch Pro 2), SPT-12 (HTC Touch Pro 2) the tested tool acquired all supported data objects completely and accurately from the selected test mobile devices (i.e., iPhone 3Gs, Blackberry Bold 9700, HTC Tilt 2, Nokia e71x, HTC Touch Pro 2, Blackberry 9630, Samsung Moment). The exceptions were the following:

- Connectivity was not established using the supported interface. Test Case: SPT-01 (iPhone 3Gs)

- Notification of device acquisition disruption was not successful. Test Case: SPT-03 (Blackberry Bold 9700, HTC Touch Pro 2, Blackberry 9630)

- Maximum length address book entries were truncated. Test Case: SPT-06 (Blackberry Bold 9700, HTC Tilt 2, Nokia e71x, HTC Touch Pro 2, Blackberry 9630)

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

OLES

NIJ National Institute of Justice

- Calendar entries were not acquired. Test Case: SPT-06 (HTC Touch Pro 2)

- Acquisition of individual data elements causes the Secure View application to lock, forcing the examiner to terminate the process and restart the application. Test Case: SPT-13 (Blackberry Bold 9700, HTC Touch Pro 2, Blackberry 9630)

- Non-ASCII address book entries and text messages are not properly reported in their native format for supported devices. Test Case: SPT-33 (Blackberry Bold 9700, HTC Tilt 2, HTC Touch Pro 2, Blackberry 9630, Samsung Moment) and Test Case: SPT-34 (iPhone 3Gs, Blackberry Bold 9700, HTC Tilt2, Nokia e71x)

- Video files are not acquired. Test Case: SPT-10 (Nokia e71x, HTC Touch Pro 2)

- Internet related data are not acquired. Test Case: SPT-12 (HTC Touch Pro 2)

For a complete copy of the report, go to:
http://www.ojp.usdoj.gov/nij/pubs-sum/232225.htm

Vendor information:
Susteen, Inc.
http://www.susteen.com

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

MOBILE DEVICES

TEST REPORT FOR:
DEVICE SEIZURE 4.0

November 2010

The CFTT Project tested the Device Seizure 4.0 against the Mobile Device Specification available at: http://www.cftt.nist.gov/mobile_devices.htm

Our results are:

Except for the following test cases: SPT–01 (Nokia 6790), SPT–03 (iPhone 3Gs, Blackberry Bold 9700, Blackberry 9630), SPT–04 (HTC Touch Pro 2), SPT–05 (Blackberry 9630, Palm pixi), SPT–06 (iPhone 3Gs, Blackberry Bold 9700, HTC Touch Pro 2, Blackberry 9630, Palm pixi), SPT–07 (iPhone 3Gs, Palm pixi), SPT–08 (HTC Touch Pro 2), SPT–09 (Blackberry Bold 9700, HTC Touch Pro 2, Blackberry 9630, Palm pixi), SPT–10 (Blackberry Bold 9700, HTC Touch Pro 2, Blackberry 9630), SPT–11 (iPhone 3Gs, Blackberry Bold 9700, Blackberry 9630, Palm pixi), SPT–12 (Blackberry 9630), SPT–24 (HTC Touch Pro 2), SPT–28 (iPhone 3Gs, Blackberry Bold 9700, Nokia 6790), SPT–31 (HTC Touch Pro 2), SPT–33 (Blackberry 9630) the tested tool acquired all supported data objects completely and accurately from the selected test mobile devices (i.e., iPhone 3Gs, Blackberry Bold 9700, Nokia 6790, HTC Touch Pro 2, Blackberry 9630, Samsung Moment, Palm pixi). The exceptions were the following:

- Connectivity to the device was not successful. Test Case: SPT–01 (Nokia 6790)
- Notification of device acquisition disruption was not successful. Test Case: SPT– 03 (iPhone 3Gs, Blackberry Bold 9700, Blackberry 9630)
- Data acquired from the mobile device is not viewable in the preview–pane. Test Case: SPT–04 (HTC Touch Pro 2)
- Subscriber related data (MSISDN, IMEI) was not reported. Test Case: SPT–05 (Blackberry 9630, Palm pixi)

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

OLES

NIJ
National Institue of Justice

- Graphics files associated with address book entries were not reported. Test Case: SPT–06 (iPhone 3Gs, Blackberry Bold 9700, HTC Touch Pro 2, Blackberry 9630, Palm pixi)
- Duration of call (i.e., seconds, minutes, hours) not specified. Test Case: SPT–07 (iPhone 3Gs, Palm pixi)
- Text messages were not acquired. Test Case: SPT–08 (HTC Touch Pro 2)
- Acquisition of files associated with MMS messages (i.e., graphics, audio, video) were not reported. Test Case: SPT–09 (Blackberry Bold 9700, Blackberry 9630)
- MMS Messages were not acquired. Test Case: SPT–09 (HTC Touch Pro 2, Palm pixi)
- Acquisitions of stand–alone files (i.e., graphics, audio, video) were not acquired. Test Case: SPT–10 (Blackberry Bold 9700, HTC Touch Pro 2, Blackberry 9630)
- Acquisition of application related data was not successful. Test Case: SPT–11 (iPhone 3Gs, Blackberry Bold 9700, Blackberry 9630, Palm pixi)
- Acquisition of Internet related data was not successful. Test Case: SPT–12 (Blackberry 9630)
- Report generation ended in errors. Test Case: SPT–24 (HTC Touch Pro 2)
- Acquisition of a password–protected SIM was not successful. Test Case: SPT–28 (iPhone 3Gs, Blackberry Bold 9700, Nokia 6790)
- Physical acquisition was not successful; data was not decoded. Test Case: SPT–31 (HTC Touch Pro 2)
- Address book entries containing Non–ASCII characters were not acquired. Text messages containing Non–ASCII characters were not reported in their native format (messages were reported as: '? ? ? ?'). Test Case: SPT–33 (Blackberry 9630)

For a complete copy of the report, go to:
http://www.ojp.usdoj.gov/nij/pubs-sum/232230.htm

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

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

MOBILE DEVICES

TEST REPORT FOR:
XRY 5.0.2

October 2010

The CFTT Project tested the XRY 5.0.2 against the Mobile Device Specification available at: http://www.cftt.nist.gov/mobile_devices.htm

Our results are:

Except for the following test cases: SPT-03 (iPhone 3Gs), SPT-31 (iPhone 3Gs), SPT-07 (Blackberry Bold 9700), SPT-09 (Blackberry Bold 9700, Blackberry 9630), SPT-32 (HTC Touch Pro 2), SPT-10 (Blackberry 9630) the tested tool acquired all supported data objects completely and accurately from the selected test mobile devices (i.e., iPhone 3Gs, Blackberry Bold 9700, Nokia e71x, HTC Touch Pro 2, Blackberry 9630). The exceptions were the following:

- Notification of device acquisition disruption was not successful. Test Case: SPT- 03 (iPhone 3Gs)

- Physical acquisition ended in errors. Test Case: SPT-31 (iPhone 2G)

- Acquisition of call log data was not successful. Test Case: SPT-07 (Blackberry Bold 9700)

- Acquisition of MMS-related data was not successful. Test Case: SPT-09 (Blackberry Bold 9700, Blackberry 9630)

- Recovery of deleted SMS and EMS messages was not successful. Test Case: SPT-32 (HTC Touch Pro 2)

- Video files are not acquired. Test Case: SPT-10 (Blackberry 9630)

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

OLES

NIJ National Institue of Justice

For a complete copy of the report, go to:
http://www.ojp.usdoj.gov/nij/pubs-sum/232229.htm

Vendor information:
MSAB INC.
http://www.msab.com

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

MOBILE DEVICES

TEST REPORT FOR:
CELLEBRITE UFED 1.1.3.3 – REPORT MANAGER 1.6.5

October 2010

The CFTT Project tested the CelleBrite UFED 1.1.3.3 – Report Manager 1.6.5 against the Mobile Device Specification available at: http://www.cftt.nist.gov/mobile_devices.htm

Our results are:

Except for the following test cases: SPT–06 (iPhone 3Gs, HTC Tilt2, Palm pixi), SPT–10 (iPhone 3Gs, HTC Tilt2, Nokie E71x), SPT–01 (Samsung Moment), SPT–05 (Palm pixi), the tested tool acquired all supported data objects completely and accurately from the selected test mobile devices (i.e., iPhone 3Gs, Blackberry Bold 9700, HTC Tilt 2, Nokia E71x, HTC Touch Pro 2, Blackberry Tour 9630, Samsung Moment, Palm pixi).

The exceptions were the following:

- Maximum length address book entries reported were truncated. Test Case: SPT– 06 (iPhone 3Gs, HTC Tilt2, Palm pixi)
- Graphics files associated with address book entries were not reported. Test Case: SPT–06 (iPhone 3Gs, Palm pixi)
- Email addresses associated with address book entries were not reported. Test Case: SPT–06 (Palm pixi)
- Graphics files of type .gif and .bmp were not acquired. Test Case: SPT–10 (iPhone 3Gs)
- Videos of type .flv were not acquired. Test Case: SPT–10 (HTC Tilt2, Nokia E71x)

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

NIJ National Institue of Justice

- Connectivity was not established using the supported interface.
  Test Case: SPT– 01 (Samsung Moment)

- Subscriber and equipment related information was not acquired.
  Test Case: SPT– 05 (Palm pixi)

For a complete copy of the report, go to:
http://www.ojp.usdoj.gov/nij/pubs-sum/231987.htm

Vendor information:
CelleBrite USA Corp.
http://www.cellebrite.com

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

MOBILE DEVICES

TEST REPORT FOR:
BITPIM – 1.0.6 OFFICICAL

January 2010

The CFTT Project tested the BitPim – 1.0.6-official tool against the Mobile Device Specification available at: http://www.cftt.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)

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

OFFICE OF LAW ENFORCEMENT STANDARDS OLES

NIJ National Institute of Justice

- 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

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

MOBILE DEVICES

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.cftt.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

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

MOBILE DEVICES

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.cftt.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).

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

OLES

NIJ
National Institue of Justice

- 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/

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

MOBILE DEVICES

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.cftt.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).

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

OLES

NIJ National Institue of Justice

- 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

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

MOBILE DEVICES

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.cftt.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)

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

OLES

NIJ National Institute of Justice

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

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

MOBILE DEVICES

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.cftt.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)

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

NIJ National Institute of Justice

- 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/

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

MOBILE DEVICES

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.cftt.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/

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

OLES

NIJ National Institute of Justice

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

MOBILE DEVICES

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.cftt.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/

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

NIJ National Institute of Justice

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

MOBILE DEVICES

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.cftt.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/

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

NIJ
National Institue of Justice

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

MOBILE DEVICES

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.cftt.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)

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

OLES

NIJ
National Institue of Justice

- 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/