Computer Forensics Tool Testing Handbook

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

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

HAVE YOUR COMPUTER FORENSICS TOOLS BEEN TESTED?

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

Benefits:

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

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

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

Revised Date: 8/6/2015

TABLE OF CONTENTS

Disk Imaging

- Tableau TD3 Forensic Imager 1.3.0
- MacQuisition 2013R2
- Paladin 4.0
- DCFLDD 1.3.4-1
- X-Ways Forensics 16.2 SR-5
- Image MASSter Solo-4 Forensic
- IXImager v3.0.nov.12.12
- Fast Disk Acquisition System (FDAS) 2.0.2
- FTK Imager CLI 2.9.0 Debian
- Paladin 3.0
- Paladin 2.06
- X-Ways Forensic 14.8
- ASR Data SMART version 2010-11-03
- VOOM HardCopy 3P – Firmware Version 2-04
- Imager MASSter Solo-3 Forensics, Software Version 2.0.10.23f
- Tableau TD1 Forensic Duplicator, Firmware Version 2.34 Feb. 17, 2011
- Tableau Imager (TIM) Version 1.11
- SubRosaSoft MacForensics Lab 2.5.5
- Logicube Forensic Talon Software Version 2.43
- BlackBag MacQuisition 2.2
- EnCase 6.5
- EnCase LinEn 6.01
- EnCase 5.05f
- FTK Imager 2.5.3.14
- DCCIdd (Version 2.0)
- EnCase 4.22a
- EnCase LinEn 5.05f
- IXimager (Version 2.0)
- dd FreeBSD
- EnCase 3.20
- Safeback 2.18
- Safeback (Sydex) 2.0
- dd GNU fileutils 4.0.36

Forensic Media Preparation

- dc3dd: Version 7.0.0
- Image MASSter Solo-4 Forensics, Software Version 4.2.63.0
- Tableau TDW1 Drive Tool/Drive Wiper; Firmware Version 04/07/10 18:21:33
- Disk Jockey PRO Forensic Edition (version 1.20)
- Drive eRazer Pro SE Bundle 12/03/2009
- Tableau Forensic Duplicator Model TD1 (Firmware Version 3.10)
- Logicube Omniclone 2Xi
- Darik's Boot and Nuke 1.0.7
- Voom HardCopy II (Model XLHCPL-2PD Version 1.11)
- WiebeTech Drive eRazer: DRZR-2-VBND & Drive eRazer PRO Bundle

Write Block (Software)

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

Write Block (Hardware)

- T4 Forensic SCSI Bridge (FireWire Interface)
- T4 Forensic SCSI Bridge (USB Interface)
- Tableau T8 Forensic USB Bridge (FireWire Interface)
- Tableau T8 Forensic USB Bridge (USB Interface)
- FastBloc FE (USB Interface)
- FastBloc FE (FireWire Interface)
- Tableau T5 Forensic IDE Bridge (USB Interface)
- Tableau T5 Forensic IDE Bridge (FireWire Interface)
- Tableau Forensic SATA Bridge T3u (USB Interface)
- Tableau Forensic SATA Bridge T3u (FireWire Interface)
- Tableau Forensic IDE Pocket Bridge T14 (FireWire Interface)
- WiebeTech Forensic SATADock (FireWire Interface)
- WiebeTech Forensic SATADock (USB Interface)

- WiebeTech Forensic ComboDock (USB Interface)
- WiebeTech Forensic ComboDock (FireWire Interface)
- WiebeTech Bus Powered Forensic ComboDock (USB Interface)
- WiebeTech Bus Powered Forensic ComboDock (FireWire Interface)
- Digital Intelligence UltraBlock SATA (FireWire Interface)
- FastBloc IDE (Firmware Version 16)
- MyKey NoWrite (Firmware Version 1.05)
- ICS ImageMasster DriveLock IDE (Firmware Version 17)
- WiebeTech FireWire DriveDock Combo (FireWire Interface)
- Digital Intelligence Firefly 800 IDE (FireWire Interface)
- Digital Intelligence UltraBlock SATA (USB Interface)

Mobile Devices

- Device Seizure v6.8
- Lantern v4.5.6
- EnCase Smartphone Examiner v7.10.00.103
- Oxygen Forensics Suite 2015 – Analyst v7.0.0.408
- Secure View v3.16.4
- viaExtract v2.5
- Mobile Phone Examiner Plus v5.5.3.73
- iOS Crime Lab v1.0.1
- UFED Physical Analyzer v3.9.6.7
- XRY/XACT v6.10.1
- EnCase Smartphone Examiner v7.0
- Device Seizure v5.0 build 4582.15907
- Lantern v2.3
- Micro Systemation XRY v6.3.1
- Secure View 3v3.8.0
- CelleBrite UFED 1.1.8.6 – Report Manager 1.8.3/UFED Physical Analyzer 2.3.0
- Mobile Phone Examiner Plus (MPE+) 4.6.0.2
- 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

Deleted File Recovery

- ILooKIX v2.2.3.151
- The Sleuth Kit (TSK) 3.2.2 / Autopsy 2.24
- X-Ways Forensics Version 16.0 SR-4
- SMART for Linux Version 2011-02-02 (Revised)
- FTK Version 3.3.0.33124
- EnCase Version 6.18.0.59

Forensic File Carving

Graphic

- Adroit Photo Forensics 2013 v3.1d
- EnCase Forensic v6.18.0.59
- EnCase Forensic v7.09.05
- FTK v4.1
- iLook v2.2.7
- PhotoRec v7.0-WIP
- Recover My Files v5.2.1
- R-Studio v6.2
- Scalpel v2.0
- X-Ways Forensics v17.6

Video

- Defraser v1.3
- EnCase v7.09.05
- iLook v.2.2.7
- Photo Rec v7.0-WIP
- Recover My Files v5.2.1

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

TEST REPORT FOR:
TABLEAU TD3 FORENSIC IMAGER 1.3.0

July 2014

The CFTT Project tested the Tableau TD3 Forensic Imager against the Digital Data Acquisition Tool Specification available at: http://www.cftt.nist.gov/disk_imaging.htm

Our results are:

The Tableau TD3 Forensic Imager is a modular multi-function standalone device. The TD3 Forensic Imager was only tested for its forensic imaging ability. Except for one test case, the tool acquired all visible and hidden sectors completely and accurately from the test media. In test case DA-09-standard100 when the tool was executed with Error Granularity set to Standard and faulty sectors were encountered, readable sectors in the same 64-sector imaging block as the faulty sectors were replaced by zeros in the created clone. This is the intended tool behavior as specified by the tool vendor. When Error Granularity was set to Exhaustive (default), all readable sectors were acquired by the tool and zeros were written to the clone in place of the faulty sectors (test cases DA-09-exh100, DA-09-exhdonot and DA-09-exhtryonce).

Note on test case DA-08-DCO, imaging a drive containing a Device Configuration Overlay or DCO. 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 "HPA/DCO Disable" menu option. In test case DA-08-DCO the "HPA/DCO Disable" menu option was exercised to remove the DCO and all sectors of the source drive were successfully acquired.

For a complete copy of the report, go to:
https://cyberfetch.org/groups/community/test-results-digital-data-acquisition-tool-tableau-td3-forensic-imager-130

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

TEST REPORT FOR:
MACQUISITION 2013R2

July 2014

The CFTT Project tested the MacQuisition 2013R2 against the Digital Data Acquisition Tool Specification available at: http://www.cftt.nist.gov/disk_imaging.htm

Our results are:

MacQuisition 2013R2 is a USB-based live data acquisition, data collection, and forensic imaging tool. The tool boots and collects data from various models of Macintosh computers. MacQuisition 2013R2 was only tested for its forensic imaging ability. The tool acquired the test media completely and accurately. When acquiring a hard drive with known faulty sectors, the tool wrote forensically benign content to the image in place of the faulty sectors.

For a complete copy of the report, go to:
https://cyberfetch.org/groups/community/test-results-digital-data-acquisition-tool-macquisition-2013r2

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

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

TEST REPORT FOR:
PALADIN 4.0

May 2014

The CFTT Project tested the Paladin 4.0 against the Digital Data Acquisition Tool Specification available at: http://www.cftt.nist.gov/disk_imaging.htm

Our results are:

Paladin 4.0 is a modified Live Linux distribution designed to simplify the process of creating forensic images in a forensically sound manner. Paladin 4.0 is designed to image, clone and restore data from hard drives and other secondary storage. Except for the following anomaly, the tool acquired the test media completely and accurately. The tool wrote only the contents of the first image segment when restoring a segmented raw (.dd) image to a clone. The clone operation completed after writing the first 2 GB segment of the image. Data from the four remaining segments were not written to the clone (test case DA-14-SCSI).

An additional observation was made for clone operations where the destination device or partition was larger than the source. When Paladin 4.0 was used to clone a smaller drive to a larger one or a smaller partition to a larger one, the tool wrote 32 sectors of 0's followed by a sector of unknown content to the end of the larger drive or partition. Of the excess sectors on the destination drive or partition, only the last 33 sectors were written to by the tool. This behavior is seen in test cases DA-01, DA-02 and DA-09.

For a complete copy of the report, go to:
https://www.cyberfetch.org/groups/community/test-results-digital-data-acquisition-tool-paladin-40

Vendor information:
Sumuri LLC
http://sumuri.com

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

TEST REPORT FOR:
DCFLDD 1.3.4-1

December 2013

The CFTT Project tested the DCFLDD 1.3.4-1 against the Digital Data Acquisition Tool Specification available at: http://www.cftt.nist.gov/disk_imaging.htm

Our results are:

DCFLDD is an enhanced version of GNU dd with features useful for forensics and security. Based on the dd program found in the GNU Coreutils package, dcfldd has the following additional features: hashing on-the-fly, status output, flexible disk wipes, image/wipe verify, multiple outputs, split output and piped output and logs. DCFLDD was tested only for its disk imaging capabilities and, except for the following anomaly the tool acquired the test media completely and accurately.

- When a drive with faulty sectors was imaged (test case DA-09) the tool failed to completely acquire all readable sectors near the location of the faulty sectors. In test case DA-09, a source drive with faulty sectors was cloned to a target drive. Readable sectors that were near faulty sectors on the source drive were not acquired. The tool wrote zeros to the target drive in place of these sectors.

- When a drive with faulty sectors was imaged (test case DA-09) the data cloned to the target drive became misaligned after faulty sectors were encountered on the source drive. For example, sector 6,160,448 on the target drive contained the contents of sector 6,160,392 from the source, sector 6,160,449 on the target contained the contents of source sector 6,160,393, and so on. The size of the offset or misalignment between the data on the source and target drives grew as more faulty sectors were encountered on the source.

For a complete copy of the report, go to:
https://www.cyberfetch.org/groups/community/test-results-digital-data-acquisition-tool-dcfldd-134-1

Vendor information:
Sourceforge.net
http://dcfldd.sourceforge.net

TEST REPORT FOR:
X-WAYS FORENSICS 16.2 SR-5

November 2013

The CFTT Project tested the X-Ways Forensics 16.2 SR-5 against the Digital Data Acquisition Tool Specification available at: http://www.cftt.nist.gov/disk_imaging.htm

Our results are:

X-Ways Forensics version 16.2 SR-5 is designed to image, clone and restore data from hard drives and other secondary storage. Except for three test cases involving NTFS partitions, the tool acquired test media completely and accurately. When the tool cloned an NTFS partition (test case DA-02-NT) and when the images of previously acquired NTFS partitions were restored (test cases DA-14-NT and DA-14-NT-ALT), some sectors on the target partitions did not match the partitions that were acquired. The differences appear to be changes made by Windows; an artifact of the tool's operating environment (Windows 7 and Windows XP). The tool had no control over these changes. The vendor references this issue in the X-Ways user manual; "An image is usually preferable to a clone, as all data (and metadata such as timestamps) in an image file is protected from the operating system."

Additional observations:

- The tool allows the user to restore the image of a partition. For FAT32 and exFAT file system types, if the user selects a Windows drive letter (e.g., c: or e:) or a partition containing a file system as the destination, Windows may make some changes to file system metadata on the destination partition causing a difference of several sectors between the source partition and the destination partition it was restored to. No changes are made if a partition with no file system is selected as the destination. This is not an issue with the tool; this result is noted to make the reader aware of the difference between restoring an image of a partition to a logical

drive vs. restoring an image of a partition to a partition formatted with a file system vs. restoring an image of a partition to an unformatted destination partition.

- Selecting to acquire a Windows drive letter or logical drive (e.g., c: or e:) does not acquire volume slack. To acquire volume slack the partition must be selected and not the drive letter. This result is noted to make the reader aware of the difference between choosing a logical vs. a partition acquisition.

For a complete copy of the report, go to:
https://www.cyberfetch.org/groups/community/digital-data-acquisition-tool-test-results-x-ways-forensics-162-sr-5

Vendor information:
X-Ways AG
http://www.x-ways.com

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

TEST REPORT FOR:
IMAGE MASSTER SOLO-4 FORENSIC

November 2013

The CFTT Project tested the Image MASSter Solo-4 Forensic against the Digital Data Acquisition Tool Specification available at: http://www.cftt.nist.gov/disk_imaging.htm

Our results are:

The Imager MASSter Solo-4 Forensic system is a portable data acquisition device. The unit provides native interface support for SAS, SATA and USB drives in addition to supporting PATA. The tool acquired the test media completely and accurately. The following restore anomaly was observed.

- In test case DA-10-encrypt the tool's "Encrypt Destination Files" setting was used to acquire a source drive to an encrypted image file. In DA-14-encrypt, the image file created in DA-10-encrypt was restored to a drive. When the restored drive was compared to the source, only 1,571,229 sectors out of 156,301,488 sectors matched. The vendor plans to address this issue in a future software release and recommends not using the "Encrypt Destination Files" setting until it is corrected.

For a complete copy of the report, go to:
https://www.cyberfetch.org/groups/community/digital-data-acquisition-tool-image-masster-solo-4-forensic

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

TEST REPORT FOR:
IXIMAGER V3.0.NOV.12.12

November 2013

The CFTT Project tested the IXImager v3.0.nov.12.12 against the Digital Data Acquisition Tool Specification available at: http://www.cftt.nist.gov/disk_imaging.htm

Our results are:

IXImager is a bootable forensics imaging and analysis system that runs from CD-ROM or flash media. When acquiring a hard drive with 35 known faulty sectors, the tool wrote forensically benign content to the image in place of the faulty sectors. The tool acquired all visible and hidden sectors completely and accurately from the test media. For more test result details see section 5.

For a complete copy of the report, go to:
https://www.cyberfetch.org/groups/community/digital-data-acquisition-tool-iximager-v30nov1212

Vendor information:
Perlustro, L.P.
http://www.perlustro.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

TEST REPORT FOR:

FAST DISK ACQUITION SYSTEM (FDAS) 2.0.2

July 2013

The CFTT Project tested the Fast Disk Acquisition System (FDAS) 2.0.2 against the Digital Data Acquisition Tool Specification available at: http://www.cftt.nist.gov/disk_imaging.htm

Our results are:

FDAS Fast Disk Acquisition System from CyanLine is a portable all in one acquisition tool. Connect a source drive to the unit and then it transfers the image directly to storage media internal to the device. FDAS also provides source drive write blocking. Except for the following anomalies, the tool acquired the test media completely and accurately.

- When a drive with faulty sectors was imaged (test cases DA-09-option1 & DA-09-option2) the tool failed to completely acquire all readable sectors near the location of the faulty sectors. Option 1 tries to skip around faulty sectors and omitted 422 readable sectors. Option 2 retries reading faulty sectors (at the expense of slower acquisition speed) and omitted 10 readable sectors.

- The tool failed to acquire sectors in a hidden area of a hard drive (test cases DA-08-DCO, DA-08-ATA28 & DA-08-ATA48).

For a complete copy of the report, go to:
https://www.cyberfetch.org/groups/community/test-results-digital-data-acquisition-tool-fast-disk-acquisition-system-fdas-202

Vendor information:
CyanLine LLC
http://cyanline.com

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

TEST REPORT FOR:
FTK IMAGER CLI 2.9.0_DEBIAN

May 2013

The CFTT Project tested the FTK Imager CLI 2.9.0_Debian against the Digital Data Acquisition Tool Specification available at: http://www.cftt.nist.gov/disk_imaging.htm

Our results are:

AccessData's FTK Imager CLI v2.9 Debian is designed to image and restore hard drives and other secondary storage. It uses the Debian command line interface to image, clone and restore acquired data. Except for the case where a drive with faulty sectors was imaged (test case DA-09), the tool acquired all sectors of the test media completely and accurately. In test cases DA-04 and DA-17 that measure how a tool behaves when the destination media has insufficient space for a clone or restore task, the tool failed to display a message indicating that the destination drive had insufficient space.

Refer to sections 3.1 and 3.2 for additional details on test cases DA-04, DA-17 and DA-09.

For a complete copy of the report, go to:
https://www.cyberfetch.org/groups/community/reporttest-results-digital-data-acquisition-toolftk-imager-cli-290debian

Vendor information:
Access Data
http://accessdata.com

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

TEST REPORT FOR:

PALADIN 3.0

March 2013

The CFTT Project tested the Paladin 3.0 against the Digital Data Acquisition Tool Specification available at: http://www.cftt.nist.gov/disk_imaging.htm

Our results are:

Paladin 3.0 is a modified Live Linux distribution designed to simplify the process of creating forensic images in a forensically sound manner. Paladin 3.0 is designed to image, clone and restore data from hard drives and other secondary storage. Except for the following anomalies, the tool acquired the test media completely and accurately.

.

- Readable sectors that were near faulty sectors on a source drive were not acquired. The tool wrote zeros to the target drive in place of these sectors (DA-09).

- The data written to a target drive became misaligned with the data on the source after faulty sectors were encountered on the source drive (DA-09).

- When a swap partition was acquired to an image file (DA-07-SWAP), seven sectors of the image file differed from the source. The tool wrote zeros for these last seven sectors in place of the appropriate source drive content. This behavior is caused by the Paladin 3.0 execution environment and CFTT has verified that the vendor has fixed this issue in Paladin version 3.0.3.

For a complete copy of the report, go to:
https://www.cyberfetch.org/groups/community/test-results-digital-data-acquisition-tool-paladin-30

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

NIJ National Institute of Justice

Vendor information:
Sumuri LLC
http://sumuri.com

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

TEST REPORT FOR:
PALADIN 2.06

March 2013

The CFTT Project tested the Paladin 2.06 against the Digital Data Acquisition Tool Specification available at: http://www.cftt.nist.gov/disk_imaging.htm

Our results are:

Paladin 2.06 is a modified Live Linux distribution designed to simplify the process of creating forensic images in a forensically sound manner. Paladin 2.06 is designed to image, clone and restore data from hard drives and other secondary storage. Except for the following anomaly, the tool acquired the test media completely and accurately.

.

- Readable sectors that were near faulty sectors on a source drive were not acquired. The tool wrote zeros to the target drive in place of these sectors (DA-09).

- The data written to a target drive became misaligned with the data on the source after faulty sectors were encountered on the source drive (DA-09).

For a complete copy of the report, go to:
https://cyberfetch.org/groups/community/test-results-digital-data-acquisition-tool-paladin-206

Vendor information:
Sumuri LLC
http://sumuri.com

TEST REPORT FOR:
X-WAYS FORENSICS 14.8

March 2013

The CFTT Project tested the X-Ways Forensics 14.8 03 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 the cases where source drives containing faulty sectors were imaged, a logical NTFS partition was imaged, or a source drive containing hidden sectors, a Host Protected Area (HPA) or Device Configuration Overlay (DCO), was imaged. The tool restored image files and created clones accurately except for clone or restore operations on certain partitions and removable media where small changes to file system metadata were observed. The following anomalies were observed:

- Some readable sectors may be intentionally skipped, controlled by a parameter setting, to improve performance during acquisition of a drive with faulty sectors (DA-09-FW, DA-09-FW-XP and DA-09-USB).

- Eight unused sectors at the end of a partition containing an NT file system are not acquired (DA-07-NTFS). This is because the tool user selected acquiring the logical drive rather than the physical drive. If the physical drive is selected, all sectors of the partition should be acquired. This is not an issue with the tool; this result is noted to make the reader aware of the differences between choosing a logical vs. a physical acquisition.

- The tool does not acquire any sectors hidden by an HPA or a DCO. However, a separate tool, X-Ways Replica, can be used to remove an HPA or a DCO to make hidden sectors visible and then acquire the formerly hidden sectors (DA-08-ATA28, DA-08-ATA48 and DA-08-

DCO).

- Small changes may be made by the operating system to file system metadata when cloning or restoring the image of a FAT32 or NTFS logical drive (DA-02-CF, DA-02-F32, DA-02-F32X, DA-14-CF, DA-14-F32, DA-14-F32X and DA-14-TFS). The tool has no control over these changes.

- Only the first 268,435,456 sectors (128GB) of a drive larger than 128GB are acquired if the tool is executed in the Windows 2000 environment (DA-08-DCO). This is because of the limitations of Windows 2000 to handle drives requiring 48bit addressing. This is not an issue with the tool; this result is noted to make the reader aware of the consequences of operating system selection.

For a complete copy of the report, go to:
https://cyberfetch.org/groups/community/test-results-digital-data-acquisition-toolx-ways-forensics-148

Vendor information:
X-Ways Software Technology AG
http://www.x-ways.com

TEST REPORT FOR:
ASR DATA SMART VERSION 2010-11-03

October 2012

The CFTT Project tested the ASR Data Smart version 2010-11-03 against the Digital Data Acquisition Tool Specification available at: http://www.cftt.nist.gov/disk_imaging.htm

Our results are:

The tool, SMART, acquired visible and hidden sectors from the test media completely and accurately with the exception of the following cases: DA-08-DCO and DA-09. In both test cases the test results document tool features and not errors in the tool.

It was also observed that the execution environment, the SMART Linux live CD version 2011-01, modified a particular source drive containing an NTFS partition that was used in three cases: DA-02-F12, DA-02-F32, and DA-06-ATA28. CFTT has verified that the problem with NTFS partitions has been fixed in the current release of SMART Linux (August 2011). Upgrading the version of the SMART Linux live CD from the version shipped to NIST by the vendor resulted in an environment that appeared to be SMART Linux, but where the treatment of Linux swap files was misconfigured. Such an environment can under certain conditions manifest anomalies with acquiring Linux swap partitions. This Linux environment displayed anomalies with the following cases: DA-02-SWAP, DA-02-SWAP-ALT, DA-07-SWAP, and DA-14-SWAP. CFTT has verified that these swap anomalies are not present in either the original version of the SMART Linux live CD shipped to NIST by the vendor (May 6, 2010) or the current version of SMART Linux (August 2011).

The following behaviors were observed:

- The sectors hidden by a *device configuration overlay* (DCO) were not acquired (DA-08-DCO).

- Some readable sectors that were near faulty sectors on the test drive were replaced by zeros in the clone that was created in test case DA-09. The number of readable sectors missed varied between 6 and 206 sectors.

- The SMART Linux live CD execution environment modified 88 sectors of the NTFS file system on the source drive used in test cases DA-02-F12, DA-02-F32, and DA-06-ATA28. In DA-06-ATA28 this resulted in 88 sectors differing between the image file created by the tool and the original unaltered source.

- In test case DA-02-SWAP, when cloning a source swap partition to a destination swap partition of the same size, the clone operation aborted without copying the last seven sectors of the source partition.

- When restoring the image of a swap partition to a destination partition that was the same size as the source, the restore operation aborted and did not copy the last seven sectors (DA-14-SWAP).

- When a source swap partition was cloned to a larger destination swap partition in test case DA-02-SWAP-ALT, the clone differed from the source by seven sectors.

- Seven sectors of the image file differed from the source when a swap partition was acquired to an image file (DA-07-SWAP).

For a complete copy of the report, go to:
http://www.nij.gov/pubs-sum/238994.htm

Vendor information:
ASR Data, Data Acquisition and Analysis, LLC
http://www.asrdata.com/

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

DISK IMAGING

TEST REPORT FOR:
VOOM HARDCOPY 3P -- FIRMWARE VERSION 2-04

October 2012

The CFTT Project tested the VOOM HardCopy 3P -- Firmware Version 2-04 against the Digital Data Acquisition Tool Specification available at: http://www.cftt.nist.gov/disk_imaging.htm

Our results are:

The VOOM HardCopy 3P – Firmware Version 2-04 is designed to handle ATA and SATA source drives. The device can copy data to either one or two destination drives.

The tool acquired visible and hidden sectors from the test media completely and accurately for all test cases. For one test case, DA-08-HPA, when acquiring a physical drive containing hidden sectors, the size of the hidden area was reported incorrectly. Refer to section 3.1 of the report for more details.

For a complete copy of the report, go to:
http://www.nij.gov/pubs-sum/238995.htm

Vendor information:
VOOM Technologies, Inc.
http://www.ics-iq.com

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).

- 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

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.

- 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

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/

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).

- 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

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/

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).

- Log files are incomplete when acquisitions are written to devices with insufficient space (DA–12).

- The sectors hidden by a device configuration overlay (DCO) or host protected area (HPA) are not acquired (DA–08–DCO, DA–08–SATA28, DA–08– SATA28–INTEL, and DA–08–SATA48).

- Data is not skipped as directed by the skip parameter (DA–07–PART).

- Good sectors in the same block as a faulty sector are not acquired, and other data is written in their place (DA–09, DA–09–INTEL, DA–09–134, and DA–09–134– INTEL).

- When a faulty sector is encountered, a block of sectors equal in size to the imaging block size is omitted from the acquisition image (DA–09, DA–09–TPIPE, and DA–09–134).

- Data for faulty sectors may be replaced in the image file with data from an undetermined source (DA–09, DA–09–INTEL, DA–09–TPIPE, and DA–09–TPIPE–INTEL).

- In the image file, sectors surrounding a faulty sector may contain data that has been previously acquired (DA–09, DA–09–INTEL, DA–09–TPIPE, and DA–09–TPIPE–INTEL).

For a complete copy of the report, go to:
http://www.ojp.usdoj.gov/nij/pubs-sum/228223.htm

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

TEST REPORT FOR:
ENCASE 6.5

September 2009

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

Our results are:

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

- If a logical acquisition is made of an NTFS partition, a small number of sectors, seven in the executed test, appear in the image file twice, replacing seven other sectors that fail to be acquired (DA–07–NTFS).

- If a logical acquisition is made of an NTFS partition, the last physical sector of the partition is not acquired (DA–07–NTFS).

- If the tool attempts to acquire a defective sector with an error granularity greater than one sector, some readable sectors near the defective sector are replaced by zeros in the created image file (DA–09–02, DA–09–16, and DA–16–64).

- HPA and DCO hidden sectors can be acquired completely if FastBlock SE is used as a write blocker (DA–08–ATA28) during an acquisition. However, use of some write blockers such as FastBlock FE that do not remove hidden areas prevent the acquisition of sectors hidden in an HPA or DCO (DA–08–ATA48 and DA–08–DCO).

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

- For some removable USB devices (Flash card and thumb drive) that have been physically acquired, there may be a small number of differences in file system metadata between the image file and the restored device (DA–14–CF and DA–14–THUMB).

For a complete copy of the report, go to:
http://www.ojp.usdoj.gov/nij/pubs-sum/228226.htm

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

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

TEST REPORT FOR:
ENCASE LINEN 6.01

October 2008

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

Our results are:

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

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

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

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

TEST REPORT FOR:
ENCASE 5.05F

June 2008

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

Our results are:

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

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

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

For a complete copy of the report, go to:
http://www.ojp.usdoj.gov/nij/pubs-sum/223433.htm

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

TEST REPORT FOR:

FTK IMAGER 2.5.3.14

June 2008

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

Our results are:

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

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

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

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

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

January 2008

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

Our results are:

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

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

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

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

TEST REPORT FOR:
ENCASE 4.22A

January 2008

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

Our results are:

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

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

For a complete copy of the report, go to:
http://www.ojp.usdoj.gov/nij/pubs-sum/221168.htm

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

TEST REPORT FOR:
ENCASE LINEN 5.05F

January 2008

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

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

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

TEST REPORT FOR:

DD FREEBSD

January 2004

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

Our results are:

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

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

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

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

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

For a complete copy of the report, go to:
http://www.ojp.usdoj.gov/nij/pubs-sum/203095.htm

Vendor information:
FreeBSD Foundation
http://www.freebsd.org

TEST REPORT FOR:
ENCASE 3.20

June 2003

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

Our results are:

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

- If the basic input/output system (BIOS) interface is chosen to access integrated drive electronics (IDE) hard drives on an older computer using a legacy BIOS that underreports the number of cylinders on the drive, then there may be a small area of sectors at the end of the drive that is not accessed. The sectors in this area are usually not used by commercial software. If direct access using the advance technology attachment (ATA) interface is chosen instead, EnCase accesses every sector of the hard drive.

- For certain partition types (FAT32 and NTFS), a logical restore of a partition is not an exact duplicate of the original. The vendor documentation states that a logical restore cannot be verified as an exact copy of the source and is not recommended when seeking to create a bit- stream duplicate of the source. For FAT32 partitions, two file system control values (not part of any data file) are adjusted during restoration of an image to a destination. This

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

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

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

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

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

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

For a complete copy of the report, go to:
http://www.ojp.usdoj.gov/nij/pubs-sum/200031.htm

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

TEST REPORT FOR:
SAFEBACK 2.18

June 2003

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

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

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

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

For a complete copy of the report, go to:
http://www.ojp.usdoj.gov/nij/pubs-sum/200032.htm

Vendor information:
New Technologies, Inc.
http://www.forensics-intl.com/

TEST REPORT FOR:
SAFEBACK (SYDEX) 2.0

April 2003

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

For a complete copy of the report, go to:
http://www.ojp.usdoj.gov/nij/pubs-sum/199000.htm

Vendor information:
New Technologies, Inc.
http://www.forensics-intl.com/

TEST REPORT FOR:
DD GNU FILEUTILS 4.0.36

August 2002

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

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/

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.

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/

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/

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:

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

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 Institute 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

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

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

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

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

NIJ National Institute of Justice

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/

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

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.

TEST REPORT FOR:

PDBLOCK VERSION 1.02 (PDB_LITE)

June 2005

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

Our results are:

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

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

The tool did not block five commands in the configuration category: Initialize Drive Parameters (0x09), PS/2 ESDI Diagnostic (0x0E), PC/XT Controller Ram Diagnostic (0x12), the controller drive diagnostic command (0x13), and Controller Internal Diagnostic (0x14). These commands are rarely used, if at all. Additionally, two commands in the miscellaneous category were not blocked (command codes 0x1A and 0x22).
Test cases: SWB–04 and SWB–06.

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

Test cases: All.

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

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

For a complete copy of the report, go to:
http://www.ojp.usdoj.gov/nij/pubs-sum/209831.htm

Vendor information:
Digital Intelligence, Inc.
http://www.digitalintelligence.com

TEST REPORT FOR:
PDBLOCK VERSION 2.00

June 2005

The CFTT Project tested the PDBLOCK Version 2.00 against the Software Write Block Specification available at: http://www.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.

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

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

Test cases: All.

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

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

For a complete copy of the report, go to:
http://www.ojp.usdoj.gov/nij/pubs-sum/209832.htm

Vendor information:
Digital Intelligence, Inc.
http://www.digitalintelligence.com

TEST REPORT FOR:
PDBLOCK VERSION 2.10

June 2005

The CFTT Project tested the PDBLOCK Version 2.10 against the Software Write Block Specification available at: http://www.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.

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

For a complete copy of the report, go to:
http://www.ojp.usdoj.gov/nij/pubs-sum/209833.htm

Vendor information:
Digital Intelligence, Inc.
http://www.digitalintelligence.com

TEST REPORT FOR:
RCMP HDL V0.4

August 2004

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

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

For a complete copy of the report, go to:
http://www.ojp.usdoj.gov/nij/pubs-sum/206231.htm

Vendor information:
Royal Canadian Mounted Police

TEST REPORT FOR:
RCMP HDL V0.5

August 2004

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

For a complete copy of the report, go to:
http://www.ojp.usdoj.gov/nij/pubs-sum/206232.htm

Vendor information:
Royal Canadian Mounted Police

TEST REPORT FOR:
RCMP HDL V0.7

August 2004

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

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

For a complete copy of the report, go to:
http://www.ojp.usdoj.gov/nij/pubs-sum/206233.htm

Vendor information:
Royal Canadian Mounted Police

TEST REPORT FOR:
RCMP HDL V0.8

February 2004

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

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

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

TEST REPORT FOR:

T4 FORENSIC SCSI BRIDGE (USB INTERFACE)

September 2009

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

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

TEST REPORT FOR:

TABLEAU T8 FORENSIC USB BRIDGE (FIREWIRE INTERFACE)

August 2008

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

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

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

August 2008

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

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

TEST REPORT FOR:
FASTBLOC FE (USB INTERFACE)

June 2007

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

Vendor information:
Guidance Software, Inc.

TEST REPORT FOR:

FASTBLOC FE (FIREWIRE INTERFACE)

June 2007

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

Vendor information:
Guidance Software, Inc.

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

June 2007

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

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

TEST REPORT FOR:

TABLEAU T5 FORENSIC IDE BRIDGE (FIREWIRE INTERFACE)

June 2007

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

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

TEST REPORT FOR:

TABLEAU FORENSIC SATA BRIDGE T3U (USB INTERFACE)

January 2007

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

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

TEST REPORT FOR:

TABLEAU FORENSIC SATA BRIDGE T3U (FIREWIRE INTERFACE)

January 2007

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

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

TEST REPORT FOR:

TABLEAU FORENSIC IDE POCKET BRIDGE T14 (FIREWIRE INTERFACE)

January 2007

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

Our results are:

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

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

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

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

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

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

TEST REPORT FOR:

WIEBETECH FORENSIC SATADOCK (FIREWIRE INTERFACE)

December 2006

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

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

TEST REPORT FOR:
WIEBETECH FORENSIC SATADOCK (USB INTERFACE)

December 2006

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

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

TEST REPORT FOR:

WIEBETECH FORENSIC COMBODOCK (USB INTERFACE)

May 2006

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

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

TEST REPORT FOR:

WIEBETECH FORENSIC COMBODOCK (FIREWIRE INTERFACE)

May 2006

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

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

TEST REPORT FOR:

WIEBETECH BUS POWERED FORENSIC COMBODOCK (USB INTERFACE)

May 2006

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

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

TEST REPORT FOR:

WIEBETECH BUS POWERED FORENSIC COMBODOCK (FIREWIRE INTERFACE)

May 2006

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

Our results are:

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

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

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

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

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

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

TEST REPORT FOR:

DIGITAL INTELLIGENCE ULTRABLOCK SATA (FIREWIRE INTERFACE)

May 2006

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

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

TEST REPORT FOR:
FASTBLOC IDE (FIRMWARE VERSION 16)

April 2006

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

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

TEST REPORT FOR:
MYKEY NOWRITE (FIRMWARE VERSION 1.05)

April 2006

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

Our results are:

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

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

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

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

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

Vendor information:
MyKey Technology, Inc.

TEST REPORT FOR:

ICS IMAGEMASSTER DRIVELOCK IDE (FIRMWARE VERSION 17)

April 2006

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

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

TEST REPORT FOR:

WIEBETECH FIREWIRE DRIVEDOCK COMBO (FIREWIRE INTERFACE)

April 2006

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

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

TEST REPORT FOR:

DIGITAL INTELLIGENCE FIREFLY 800 IDE (FIREWIRE INTERFACE)

April 2006

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

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

TEST REPORT FOR:

DIGITAL INTELLIGENCE ULTRABLOCK SATA (USB INTERFACE)

April 2006

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

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

TEST REPORT FOR:
DEVICE SEIZURE V6.8

June 2015

The CFTT Project tested the Device Seizure v6.8 tool against the Mobile Device Specification available at: http://www.cftt.nist.gov/mobile_devices.htm

Our results are:

Device Seizure is designed to perform a forensically sound extraction of data from a variety of mobile devices, such as feature phones, smart phone and other mobile devices.

The tool was tested for its ability to acquire active data from the internal memory of supported mobiles devices and UICC's. Except for the following anomalies, the tool acquired all supported data objects completely and accurately for all mobile devices tested.

Presentation:

- Acquisition of internal memory of the phone and readability was not successful. (Devices: Samsung Convoy3, LG Extravert)

Equipment / Subscriber related data:

- Subscriber related data (i.e., MSISDN) were not reported. (Devices: Galaxy S3, Galaxy S4, HTC One GSM, iPhone 5 GSM and Nexus 4)

Personal Information Management (PIM) data:

- Acquisition of calendar entries was not successful. (Device: HTC One GSM)
- Acquisition of memos was not successful. (Device: Galaxy S5, Galaxy Note 3, Nexus 4)
- Acquisition of PIM data (i.e., long memo) was partially reported. (Devices: iPhone 5S, iPad Mini CDMA, iPad CDMA, HTC One GSM, iPhone 5 GSM).

- Acquisition of PIM data (i.e., memos) was partially reported. (Devices: iPad Mini GSM, iPad GSM).
- Acquisition of PIM data (i.e., physical home address within a contact entry) was not acquired. (Devices: iOS devices).
- Stand-alone audio files were not acquired. (Devices: iPhone 5S, iPad Mini CDMA, iPad CDMA)

Call Logs:

- Active incoming, outgoing and missed calls times and status flags were not acquired. (Device: iPhone 5S)

SMS messages:

- Active SMS messages were not acquired. (Device: iPad GSM)

MMS messages:

- Incoming and outgoing messages with video file attachments were not acquired. (Device: iPhone 5S)
- Active MMS messages were not acquired. (Devices: iPad Mini GSM, iPad GSM)

Internet Related Data:

- Browser History and Bookmarks were not acquired. (Device: Galaxy Note3)
- Browser History was not acquired. (Device: iPad Mini GSM)

Social Media Data:

- Acquisition of social media data (i.e., Facebook, Twitter, LinkedIn) was partial. (Devices: Android devices, iOS devices)

Case Data Protection:

- Partial notification of modified device memory data. (Devices: Android devices, iOS devices)

GPS Related Data:

- Acquisition of longitude and latitude were not reported. (Devices: Android devices)

NOTES:

- Hash values for vendor supported data objects were reported only in the pdf report. This applies to all devices and UICCs.
- The purpose of DS hash validation is to prevent the usage of modified data from a device as evidence by detecting any third-party changes in acquired data. DS uses the following levels of acquired data protection:
    - All device data is encrypted.
    - DS calculates and stores hash values for each grid, file, and the entire case data.

- To prevent modification of a file and its hash value, DS uses several interrelated levels for hash value calculation. If a modification of data with DS is done the case file will open but the data would no longer be available.

For a complete copy of the report, go to:
https://cyberfetch.org/groups/community/test-results-mobile-device-acquisition-tool-device-seizure-v68

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

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

TEST REPORT FOR:
LANTERN V4.5.6

June 2015

The CFTT Project tested the Lantern v4.5.6 103 tool against the Mobile Device Specification available at: http://www.cftt.nist.gov/mobile_devices.htm

Our results are:

Lantern v4.5.6 is mobile forensics software for data acquisition from iOS mobile devices.

The tool was tested for its ability to acquire active data from the internal memory of supported mobiles devices. Except for the following anomalies, the tool acquired all supported data objects completely and accurately for all mobile devices tested.

Personal Information Management (PIM) data:

- Contacts/address book entries containing more than a first and last name were partially reported i.e., only the first and last word of the contact. (Devices: iOS)
- Recovered MMS message attachments were partially acquired. Associated attachments (i.e., audio, graphics, video) were not reported. (Device: iPad GSM).
- Documents (i.e., text files, pdf files) were not reported. (Devices: iOS)

Social Media Related Data:

- Social media related data was partially acquired. (Device: iOS)

Case File Data Protection:

- Contents of the acquired data within a saved case file were modified for without warning. (Devices: iOS)

GPS Related Data:

- GPS data i.e. longitude/latitude coordinates or KMZ files were not reported. (Devices: iOS)

For a complete copy of the report, go to:
https://cyberfetch.org/groups/community/test-results-mobile-device-acquisition-tool-lantern-v456

Supplier information:
Katana Forensics
http://www.katanaforensics.com/

TEST REPORT FOR:
ENCASE SMARTPHONE EXAMINER V7.10.00.103

April 2015

The CFTT Project tested the EnCase Smartphone Examiner v7.10.00.103 tool against the Mobile Device Specification available at: http://www.cftt.nist.gov/mobile_devices.htm

Our results are:

EnCase Smartphone Examiner v7.10.00.103 is designed to review and collect data from smartphone and tablet devices, such as iPhone and iPad. Investigators can process and analyze smartphone device data alongside other types of digital evidence with Guidance Software tools.

The tool was tested for its ability to acquire active data from the internal memory of supported mobiles devices and UICC's. Except for the following anomalies, the tool acquired all supported data objects completely and accurately for all mobile devices tested.

Equipment/ Subscriber related data:

- Subscriber related data (i.e., MSISDN) was not reported. (Devices: Samsung Galaxy S4, Samsung Galaxy S5, HTC One GSM, HTC One CDMA, Nexus 4, iPhone 5, iPhone 5S)
- Equipment related data (i.e., IMEI, MEID) was not reported. (Devices: iOS Devices)

Personal Information Management (PIM) data:

- Contacts/address book entries were not reported. (Devices: HTC One GSM, HTC One CDMA)
- Memos were not reported (Devices: Samsung Galaxy S4, Galaxy S5, HTC One GSM, HTC One CDMA, Nexus 4 and the Galaxy Note 3)
- Long Memos were not reported (Devices: Samsung Galaxy S 3)

- Social media related data was not reported. (Devices: Samsung Galaxy S3, Galaxy S4, Galaxy S5 and the Nexus 4)
- Social media related data was partially acquired. (Devices: HTC One GSM, HTC One CDMA, Galaxy Note 3 and iOS devices)

Internet Related Data:

- Bookmarks were not acquired. (Device: Samsung Galaxy S4, Galaxy S5, Nexus 4 and the Galaxy Note 3)

Case File Data Protection:

- Contents of the acquired data within a saved case file were modified without warning. (Devices: Samsung Galaxy S3, HTC One GSM and the HTC One CDMA)

For a complete copy of the report, go to:
https://cyberfetch.org/groups/community/test-results-mobile-device-acquisition-tool-encase-smartphone-examiner-v71000103

Supplier information:
Guidance Software, Inc.
http://www.encase.com/

TEST REPORT FOR:

OXYGEN FORENSIC SUITE 2015 – ANALYST V7.0.0.408

March 2015

The CFTT Project tested the Oxygen Forensic Suite 2015 – Analyst v7.0.0.408 tool against the Mobile Device Specification available at: http://www.cftt.nist.gov/mobile_devices.htm

Our results are:

Oxygen Forensic Suite 2015 – Analyst v7.0.0.408 is mobile forensic software for data acquisition from phones, smartphones and other mobile devices.

The tool was tested for its ability to acquire active data from the internal memory of supported mobile devices. Except for the following anomalies, the tool acquired all supported data objects completely and accurately for all mobile devices tested.

Connectivity:

- Connectivity for the following supported devices was not established. The drivers were installed and the OS recognized each device. (Devices: Blackberry Q10, Blackberry Z10, Nexus 4)
- Acquisition via advanced logical method was unsuccessful -the acquisition ran for 16 hours and hung on C:\FileRelay\MobileAsset\cpio.gz. (Device: iPhone 5S CDMA)

Equipment / Subscriber related data:

- Subscriber related data (i.e., MSISDN) was not reported. (Devices: Android devices)

Personal Information Management (PIM) data:

- Contacts/address book entries were partially reported i.e., only the first and last word of the contact. (Devices: Android devices)

- Calendar entries were not reported under the "Organizer" category. (Devices: Galaxy Note 3, HTC One GSM)
- Memo/Note entries were not reported under the "Organizer" category. (Devices: Android devices)
- Acquisition of Call log data (i.e., incoming, outgoing, and missed calls) was not reported. (Devices: Galaxy Note 3, HTC One GSM)
- The status of deleted text messages were incorrectly reported as active. (Device: Galaxy S5)
- Recoverable deleted text messages were not reported. (Devices: Galaxy S4, Galaxy Note 3, HTC One - CDMA and the HTC One - GSM).

Internet Related Data:

- Bookmarks for visited Internet URLs were not reported under the category "Web Browsers". (Device: Galaxy Note 3, HTC One GSM)

Social Media Related Data:

- Social media related data was partially acquired. (Device: Galaxy S3, Galaxy S4, Galaxy S5, HTC One – GSM, iPad GSM, iPad CDMA, iPad Mini GSM, iPad Mini CDMA)

Case File Data Protection:

- Contents of the acquired data within a saved case file were modified for without warning. (Devices: Samsung Galaxy S3, HTC One GSM and the HTC One CDMA)
- Contents of the acquired data (via the Classic Logical method) within a saved case file were modified without warning. (Devices: iPhone5S CDMA)

GPS Related Data:

- GPS data i.e. longitude/latitude coordinates were not reported under the "Application" category – Navigation. (Device: Galaxy S4)

Note: After a successful acquisition of the HTC One (CDMA) the case file could not be saved to an assigned folder on the forensic workstation. The acquired device had to be opened for analysis then the case file had to be saved.

For a complete copy of the report, go to:
https://cyberfetch.org/groups/community/test-results-mobile-device-acquisition-tool-oxygen-forensic-suite-2015-analyst

Supplier information:
Oxygen Forensics
http://www.oxygen-forensic .com/en/

TEST REPORT FOR:
SECURE VIEW V3.16.4

February 2015

The CFTT Project tested the Secure View v3.16.4 tool against the Mobile Device Specification available at:
http://www.cftt.nist.gov/mobile_devices.htm

Our results are:

Secure View v3.16.4 is designed to perform a secure forensic extraction of data from a variety of mobile devices, such as iOS, Android, Windows Mobile and feature phones.

The tool was tested for its ability to acquire active data from the internal memory of supported mobile devices and UICC's. Except for the following anomalies, the tool acquired all supported data objects completely and accurately for all mobile devices tested.

Connectivity:

- Connectivity was not established for the HTC Win8x. (Devices: HTC Windows Mobile 8x)

Personal Information Management (PIM) data:

- Maximum and regular length contact entries were partially recovered (i.e., middle name and long name were not completely recovered). (Devices: Android devices, iOS devices)
- Maximum length contact entries were partially recovered (i.e., middle name and long name were not completely recovered). (Devices: Samsung Convoy 3, Samsung Rugby III)
- Memo entries were not acquired. (Devices: Galaxy S5, HTC One (CDMA), Galaxy Note 3, Nexus 4, iOS devices)
- Long Memo entries were partially acquired. (Devices: HTC One (GSM), Galaxy S3, Galaxy S4)

Call Logs:

- Duration times for incoming calls were not reported. (Device: iPhone 5 (GSM))
- Status flags for incoming calls were incorrectly reported as missed. (Device: iPhone 5S (CDMA))
- Duration time for active dialed calls were not acquired. (Device: iPhone 5S (CDMA))

Internet Related Data:

- Browser History and Bookmarks were not acquired. (Devices: Galaxy Note 3, Galaxy S4, iPad Mini (GSM), iPad (GSM))
- Bookmarks were partially acquired. (Device: Nexus 4)

Social Media Data:

- Social Media Data was not acquired. (Devices: iOS devices)

Acquisition Variation:

- Acquisition of an individual supported item (i.e, Application Data – Bookmarks and Browser History) was not successful. (Device: iPad Mini (GSM))
- Acquisition of an individual supported item (i.e., Application Data – Bookmarks and Browser History) was partially acquired. (Device: iPad (GSM)).

Non-Latin Character Presentation:

- UICC ADNs containing non-Latin characters were not presented in their native format (i.e., tool displayed Aur==lien instead of Aurèlien for one of the contacts).
- Address book entries containing non-Latin characters were not acquired. (Device: Samsung Ruby III)
- Text messages containing non-Latin characters were not acquired. (Devices: iPhone 5S (CDMA), iPhone 5 (GSM))

NOTES:

- Picture files associated with contacts for the Samsung Convoy 3 are not supported.
- When a logical acquisition is completed a message would appear saying the following: "This firmware version is not supported. If you would like to acquire deleted data, please root the phone manually and try again".
- The wrong phone manufacturer and model - for the phone to be tested - can be selected and the tool would still get the phone's data. This happens when the phone under test and the phone selected run the same OS. However, the data recovered is wrongly identified.

For a complete copy of the report, go to:
https://cyberfetch.org/groups/community/test-results-mobile-device-acquisition-tool-secure-view-v3164

Supplier information:
Susteen
http://www.secureview.us

TEST REPORT FOR:
VIAEXTRACT V2.5

December 2014

The CFTT Project tested the viaExtract v2.5 tool against the Mobile Device Specification available at: http://www.cftt.nist.gov/mobile_devices.htm

Our results are:

viaExtract is designed for logical and physical acquisitions (rooted devices), data analysis and report management from Android mobile devices.

The tool was tested for its ability to acquire active and deleted data from the internal memory of supported mobile devices. Except for the following anomalies, the tool acquired all supported data objects completely and accurately for all mobile devices tested.

Equipment / Subscriber related data:

- Equipment and subscriber related data (i.e., MSISDN) were not reported. (Devices: Android)
- The ICCID was not reported (Devices: Galaxy S3, HTC One, Galaxy S4)

Personal Information Management (PIM) data:

- Call log data was not reported. (Devices: Android)
- Graphics files associated with address book entries were not reported. (Devices: Android)
- Memo entries were not reported. (Devices: Android)

Application / Social Media related data:

- Application and Social media related data were not reported. (Devices: Android)

For a complete copy of the report, go to:
https://cyberfetch.org/groups/community/test-results-mobile-device-acquisition-tool-viaextract-v25

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

TEST REPORT FOR:
MOBILE PHONE EXAMINER PLUS V5.5.3.73

December 2014

The CFTT Project tested the Mobile Phone Examiner Plus v5.5.3.73 tool against the Mobile Device Specification available at: http://www.cftt.nist.gov/mobile_devices.htm

Our results are:

MPE+ is designed to perform a secure forensic extraction of data from a variety of mobile devices, such as smartphones and tablets.

The tool was tested for its ability to acquire data from the internal memory of supported mobile devices and UICC's. Except for the following anomalies, the tool acquired all supported data objects completely and accurately for all mobile devices tested.

Acquisition Disruption:

- There was no error message when disrupting UICC connection.

Equipment / Subscriber related data:

- Subscriber related data (i.e., MSISDN) was not reported. (Devices: HTC One CDMA, HTC One GSM, Nexus 4, Galaxy S3, Galaxy S4, Galaxy S5)

Personal Information Management (PIM) data:

- Stand-alone files (i.e., graphic, audio, video) were not reported. (Device: Nexus4)
- Stand-alone audio files were not reported. (Device: HTC One CDMA, HTC One GSM)
- Contact entries with maximum length and regular length with middle name were partially recovered (i.e., middle name was not recovered). (Devices: iOS devices)

- Calendar entries are not present when a case is saved and the data file is re-opened. (Devices: iOS devices)
- Personal Information Management (PIM) data (i.e., graphic files associated with address book entries) were not reported. (Devices: Android devices)
- Social media related data was partially acquired. (Devices: HTC One GSM, Galaxy S3)

Call Logs:

- Active incoming calls status flags were incorrectly reported as missed. (Devices: iPhone 5S)

Application Related Data:

- Application related (i.e., .txt and .pdf documents) data were not reported. (Devices: Android devices, iOS devices)

Internet Related Data:

- Browser History was not acquired. (Device: Galaxy Note3)
- Bookmarks were partially acquired. (Device: Nexus 4)
- Bookmarks were not acquired. (Device: Galaxy Note3)

MMS messages:

- Incoming and outgoing audio, video and picture messages were not reported. (Device: HTC One CDMA)

Non-Latin Character Presentation:

- Address book entries containing non-Latin characters were incorrectly reported. Characters reported in different order. (Devices: iPhone 5S CDMA, iPad Air CDMA, iPad Mini CDMA)

For a complete copy of the report, go to:
https://cyberfetch.org/groups/community/test-results-mobile-device-acquisition-tool-mobile-phone-examiner-plus-v55373

Supplier information:
Access Data
http://www.accessdata.com

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

TEST REPORT FOR:

IOS CRIME LAB V1.0.1

December 2014

The CFTT Project tested the IOS Crime Lab v1.0.1 tool against the Mobile Device Specification available at:
http://www.cftt.nist.gov/mobile_devices.htm

Our results are:

iOS Crime Lab is designed for data extractions from iOS mobile devices.

The tool was tested for its ability to acquire active and deleted data from the internal memory of iOS devices. The tool acquired all supported data objects completely and accurately for all mobile devices tested.

For a complete copy of the report, go to:
https://cyberfetch.org/groups/community/test-results-mobile-device-acquisition-tool-ios-crime-lab-v101

Supplier information:
Jonathan Zdziarski
http://www.zdziarski.com

TEST REPORT FOR:
UFED PHYSICAL ANALYZER V3.9.6.7

October 2014

The CFTT Project tested the UFED Physical Analyzer v3.9.6.7 tool against the Mobile Device Specification available at: http://www.cftt.nist.gov/mobile_devices.htm

Our results are:

The
Universal Forensic Extraction Device(UF ED) is designed for logical and physical acquisitions, data analysis and report management from mobile phones, smartphones, Universal Integrated Circuit Cards (UICCs) and GPS devices.

The tool was tested for its ability to acquire active and deleted data from the internal memory of supported mobile devices and UICCs. Except for the following anomalies, the tool acquired all supported data objects completely and accurately for all mobile devices tested.

Presentation:

- Readability and completeness of Personal Information Management (PIM) data (e.g., maximum length calendar entries, memos, contacts) were truncated within the generated report. (Devices: Galaxy S3, Galaxy S5, Galaxy Note3, HTC One, iOS, HTC Win8, Nokia Lumia 920)

Equipment / Subscriber related data:

- Equipment and subscriber related data (i.e., MSISDN, IMEI) were not reported. (Devices: BlackBerry Z10, BlackBerry Q10, HTC Win8)
- The IMEI was not reported (Device: Nokia Lumia 920)

Personal Information Management (PIM) data:

- Maximum length address book entries were partially reported. (Devices: BlackBerry Z10, BlackBerry Q10)
- Graphics files associated with address book entries were not reported. (Devices: Android, iOS, BlackBerry Z10, BlackBerry Q10, HTC Win8, Nokia Lumia 920)
- Metadata (e.g., URLs, addresses) associated with address book entries were not reported. (Devices: Android, iOS, BlackBerry Z10, BlackBerry Q10, HTC Win8, Nokia Lumia 920, Samsung Rugby 3)
- Memo entries were not reported. (Devices: Android)
- Address book entries are not reported when performing a file system extraction. (Devices: Android)

SMS messages:

- The status flags for active SMS/Chat messages were incorrectly reported when performing a file system extraction. (Devices: iPhone5S, iPad, iPad mini)
- Incoming SMS and MMS messages are not reported when performing a logical acquisition. (Device : iPhone 5S)

EMS messages:

- Text messages containing more than 160 characters were not reported. (Device: Samsung Rugby 3)

Non-Latin Character Presentation:

- Address book entries containing non-Latin characters were not reported in the generated report. (Devices: HTC Win8, Nokia Lumia 920)

Application / Social Media related data:

- Application, Internet and Social media related data were not reported when performing a logical acquisition. (Devices: Android, iOS)

Acquisition Variations:

- Acquisition of individually selected data elements (i.e, Application data) is unsuccessful and ends in errors. (Device: Galaxy Note 3)

Physical Acquisition:

- Acquisitions of recoverable deleted data (i.e., memos, call logs, audio, graphic, and video files) were not recovered. (Device: Galaxy S4)

Case File Data Protection:

- Contents of the acquired data within a saved case file were modified for all mobile devices and UIC C s without warning.

For a complete copy of the report, go to:
https://cyberfetch.org/groups/community/test-results-mobile-device-acquisition-tool-ufed-physical-analyzer-v3967

Supplier information:
Cellebrite USA Inc.
http://www.cellebrite.com

TEST REPORT FOR:
XRY/XACT V6.10.1

September 2014

The CFTT Project tested the XRY/XACT v6.10.1 tool against the Mobile Device Specification available at: http://www.cftt.nist.gov/mobile_devices.htm

Our results are:

XRY/XACT is designed for perform a secure forensic extraction of data from a wide variety of mobile devices, such as smartphones, GPS navigation units, 3G modems, portable music players and the latest tablet processors.

The tool was tested for its ability to acquire active and deleted data from the internal memory of supported mobile devices and UICCs. Except for the following anomalies, the tool acquired all supported data objects completely and accurately for all mobile devices tested.

Presentation:

- Readability and completeness of Personal Information Management (PIM) data (i.e., graphic files associated with address book entries, non-Latin address book entries) were not reported. (Devices: Galaxy S3, Galaxy S4, Galaxy S5, Galaxy Note3, HTC One, Nexus4, Samsung Rugby 3)

Equipment / Subscriber related data:

- Subscriber related data (i.e., MSISDN) were not reported. (Devices: Galaxy S3, Galaxy S4, Galaxy S5, Galaxy Note3, HTC One, Nexus4)
- The MEID was not reported (Device: iPad Air, iPad Mini)

Personal Information Management (PIM) data:

- Memo entries were not reported. (Devices: Galaxy S3, Galaxy S4, Galaxy S5, Galaxy Note3, HTC One, Nexus4)

EMS messages:

- Text messages containing more than 160 characters were not reported. (Device: Samsung Rugby 3)

MMS messages:

- Incoming and outgoing audio and picture messages were not reported. (Device: Samsung Galaxy Note3)

Non-Latin Character Presentation:

- Address book entries containing non-Latin characters were not reported in the generated report. (Devices: Galaxy S3, Galaxy S4, Galaxy S5, Galaxy Note3, HTC One, Nexus4, Samsung Rugby 3)

Physical Acquisition:

- Acquisitions of recoverable deleted data remnants (i.e., graphic, audio, video files) were not recovered. (Device: Galaxy S3, Galaxy S4)

For a complete copy of the report, go to:
https://cyberfetch.org/groups/community/test-results-mobile-device-acquisition-tool-xryxact-v6101

Supplier information:
Micro Systemation, Inc.
http://www.msab.com

TEST REPORT FOR:
ENCASE SMARTPHONE EXAMINER V7.0.3

April 2013

The CFTT Project tested the EnCase Smartphone Examiner v7.0.3 tool against the Mobile Device Specification available at: http://www.cftt.nist.gov/mobile_devices.htm

Our results are:

Smartphone Examiner is designed for logical and physical acquisitions, data analysis and report management from mobile phones, smartphones and Subscriber Identity Modules (SIM).

The tool was tested for its ability to acquire active and deleted data from the internal memory of mobile devices and Subscriber Identity Modules. Except for the following anomalies, the tool acquired all supported data objects completely and accurately for all six mobile devices tested.

Device acquisition disruption:

- When connectivity was interrupted, the tool failed to notify the user that the acquisition had been disrupted. (iPhone4 GSM, Nokia N95)

Personal Information Management (PIM) data:

- Calendar entries were not acquired. (BlackBerry Torch)

Call logs:

- Call log data: incoming, outgoing, and missed calls were not acquired. Some call data may be located in "recent contacts" (BlackBerry Torch)

SIM acquisition disruption:

- When connectivity was interrupted, the tool failed to notify the user that the acquisition had been disrupted. (SIMs)

Generated report data:

- For physical acquisitions only graphic files are reported in the generated report. (HTC Thunderbolt)

Acquisition of PIN protected SIMs:

- The tool does not prompt the user to enter the SIM PIN before acquisition begins. (SIMs)

Non-ASCII characters:

- Text messages containing the non-ASCII character 'é' were reported as '|'. (BlackBerry Torch)

PIN attempts:

- The remaining number of PIN attempts were not displayed. (SIMs)

For a complete copy of the report, go to:
https://cyberfetch.org/groups/community/test-results-mobile-device-acquisition-tool-encase-smartphone-examiner-v703

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

TEST REPORT FOR:
DEVICE SEIZURE V5.0 BUILD 4582.15907

February 2013

The CFTT Project tested the Device Seizure v5.0 build 4582.15907 tool against the Mobile Device Specification available at: http://www.cftt.nist.gov/mobile_devices.htm

Our results are:

Device Seizure is designed for logical and physical acquisitions, data analysis, and report management from mobile phones, Smart Phones, and Subscriber Identity Modules (SIMs).

The tool was tested for its ability to acquire active and deleted data from the internal memory of mobile devices and SIMs. Except for the following anomalies, the tool acquired all supported data objects completely and accurately for all six mobile devices tested.

Device connectivity:

- Connectivity to the mobile device was not established. (Nokia 6350)
- Connectivity during the acquisition ended in errors. (HTC Thunderbolt)

Subscriber and equipment related information:

- Subscriber related information was not reported. (iPhone4 GSM, iPhone4 CDMA, Palm Pre2)
- Equipment-related information was not reported. (iPhone4 CDMA, Palm Pre2)

Personal Information Management (PIM) data:

- Calendar entries and memos were not reported. (HTC Thunderbolt, Palm Pre2)
- Address book entries were not reported. (Palm Pre2)

- Graphics files associated with contacts were not reported. (iPhone4 GSM, BlackBerry Torch, iPhone4 CDMA)

Call logs:

- Call log data: incoming, outgoing, and missed calls were not acquired. (Palm Pre2)
- Missed calls were categorized as Incoming. (iPhone4 GSM, iPhone4 CDMA)

Acquisition of SMS messages:

- Unread text messages were not assigned a status. (iPhone4 GSM, iPhone4 CDMA)
- SMS messages were not reported. (Palm Pre2)

Acquisition of MMS messages:

- MMS messages were not reported. (Palm Pre2)
- MMS attachments: audio, graphic, and video files were not reported. (BlackBerry Torch)
- MMS attachments: audio files were not reported. (iPhone4 GSM, iPhone4 CDMA)
- The textual portion of MMS messages was not reported. (iPhone4 CDMA)

Acquisition of stand-alone files:

- Audio and video files were not reported. (iPhone4 GSM, iPhone4 CDMA)
- Audio, video and graphic files were not reported. (BlackBerry Torch, HTC Thunderbolt, Palm Pre2)

Application-related data:

- Application-related data (e.g., Quickoffice documents) were not acquired. (HTC Thunderbolt, Palm Pre2)

Internet-related data:

- Bookmarks and visited sites were not reported. (Palm Pre2)

Non-ASCII characters:

- Text messages containing the non-ASCII character 'é' were reported as '|'. (BlackBerry Torch)
- Contact entries containing Chinese characters were not reported. (BlackBerry Torch)

For a complete copy of the report, go to:
https://cyberfetch.org/groups/community/test-results-mobile-device-acquisition-tool-device-seizure-v50-build-458215907

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

TEST REPORT FOR:
LANTERN V2.3

February 2013

The CFTT Project tested the Lantern v2.3 tool against the Mobile Device Specification available at: http://www.cftt.nist.gov/mobile_devices.htm

Our results are:

Lantern version 2.3 is designed for logical acquisitions, data analysis, and report management from mobile devices running iOS.

The tool was tested for its ability to acquire data from the internal memory of mobile devices running iOS. Except for the following anomalies, the tool acquired all supported data objects completely and accurately for all four mobile devices tested.

Acquisition attempt of nonsupported devices:

- Attempting acquisition of a nonsupported device (i.e., iPod Nano) did not provide an error message stating the device is not supported. A force quit on the acquisition had to be performed. (iPod Nano)

Subscriber-and equipment-related information:

- Subscriber related information was not reported. (iPhone4 CDMA)
- Equipment related information was not reported. (iPhone4 CDMA)

Personal Information Management (PIM) data:

- Address book entries that contained data fields for the First, Middle and Last names only reported the First and Last name e.g., John Doe Smith was reported as: John Smith. (iPhone4 GSM, iPhone4 CDMA, iPhone_3.1.2, iPhone_3.1.3)

Acquisition of Internet related data:

- Internet related data i.e., bookmarks were not reported. (iPhone_3.1.2, iPhone_3.1.3)

For a complete copy of the report, go to:
https://cyberfetch.org/groups/community/test-results-mobile-device-acquisition-tool-lantern-v23

Supplier information:
Katana Forensics, Inc.
http://www.katanaforensics.com

TEST REPORT FOR:
MICRO SYSTEMATION XRY V6.3.1

February 2013

The CFTT Project tested the Micro Systemation XRY v6.3.1 tool against the Mobile Device Specification available at: http://www.cftt.nist.gov/mobile_devices.htm

Our results are:

The XRY is a secure forensic software application that runs on the Windows operating system. It is designed to perform data extraction on a wide variety of mobile devices, such as smartphones, gps navigation units, 3G modems, portable music players and the latest table processors such as the iPad and Subscriber Identity Modules (SIMs)

The tool was tested for its ability to acquire active and deleted data from the internal memory of mobile devices and SIMs. Except for the following anomalies, the tool acquired all supported data objects completely and accurately for all eight mobile devices tested.

Device connectivity:

- Connectivity to the mobile device was not established (Motorola Tundra).

SIM acquisition disruption:

- When connectivity was interrupted, the tool failed to notify the user that the acquisition had been disrupted for the Subscriber Identity Module. (iPhone4 GSM, BlackBerry Torch, Samsung Focus, Nokia 6350, Motorola Tundra, HTC Tilt2)

Physical acquisition:

- Deleted address book entries and calendar entries were not reported. (iPhone4 GSM, iPhone4 CDMA)

For a complete copy of the report, go to:
https://cyberfetch.org/groups/community/test-results-mobile-device-acquisition-tool-micro-systemation-xry-v631

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

TEST REPORT FOR:
SECURE VIEW 3V3.8.0

February 2013

The CFTT Project tested the Secure View 3v3.8.0 tool against the Mobile Device Specification available at: http://www.cftt.nist.gov/mobile_devices.htm

Our results are:

Secure View 3.8.0 is designed for logical acquisitions, data analysis, and report management from mobile phones, Smart Phones, and Subscriber Identity Modules (SIMs).

The tool was tested for its ability to acquire data from the internal memory of mobile devices and SIMs. Except for the following anomalies, the tool acquired all supported data objects completely and accurately for all seven mobile devices tested.

Device connectivity:

- Connectivity to the mobile device was not established (Nokia 6350).

Personal Information Management (PIM) data:

- Maximum length address book entries were truncated. (iPhone4 GSM, Black Berry Torch, iPhone4 CDMA, HTC Thunderbolt)
- Address book entries containing only one name (e.g., John) were reported as: "John John". (Motorola Tundra)
- Graphics files associated with address book entries were not reported. (iPhone4 GSM, iPhone4 CDMA, HTC Thunderbolt)
- Memo entries were not reported. (HTC Thunderbolt)

Acquisition of stand-alone files:

- Graphic, audio and video files were not reported. (HTC Thunderbolt)

Acquisition of Internet-related data:

- Internet-related data i.e., bookmarks, visited sites were not reported. (iPhone4 GSM, iPhone4 CDMA)

Acquisition of SIM subscriber-related data:

- The service provider name (SPN) was not reported. (SIMs)

Non-ASCII characters (internal phone memory):

- Contacts and text messages containing the non-ASCII characters were reported incorrectly. (BlackBerry Torch)

Non-ASCII characters (SIM memory):

- Contact entries containing the acute accented character é were reported incorrectly. (SIMs)

For a complete copy of the report, go to:
https://cyberfetch.org/groups/community/test-results-mobile-device-acquisition-tool-secure-view-3v380

Supplier information:
Susteen, Inc.
http://www.datapilot.com

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

TEST REPORT FOR:

CELLEBRITE UFED 1.1.8.6 – REPORT MANAGER 1.8.3/UFED PHYSICAL ANALYZER 2.3.0

October 2012

The CFTT Project tested the CelleBrite UFED 1.1.8.6 – Report Manager 1.8.3/ UFED Physical Analyzer 2.3.0 tool against the Mobile Device Specification available at: http://www.cftt.nist.gov/mobile_devices.htm

Our results are:

Cellebrite Universal Forensic Extraction Device (UFED) is designed for logical and physical acquisitions, data analysis and report management from mobile phones, Smart Phones, Subscriber Identity Modules (SIMs) and Global Positioning System (GPS) devices.

The tool was tested for its ability to acquire active and deleted data from the internal memory of mobile devices and SIMs. Except for the following anomalies, the tool acquired all supported data objects completely and accurately for all nine mobile devices tested.

Personal Information Management (PIM) data:

- Graphics files associated with address book entries were not reported. (iPhone4 GSM, iPhone4 CDMA, HTC Thunderbolt, Palm Pre2)
- Address book entries with fields for a first, middle and last name were reported incorrectly. The first name field was appended with a semicolon. (Samsung Focus)
- Regular-length address book entries with a value in only the first-name field were reported incorrectly. The first-name field was duplicated. (Motorola Tundra)
- Memo entries were not acquired. (Motorola Tundra)

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

NIJ National Institue of Justice

- Address book entries with fields for a first, middle and last name were reported incorrectly. The middle-name field was not reported. (Palm Pre2)
- Maximum-length address book entries were truncated — 54 out of 126 characters were reported. (Palm Pre2)
- Email addresses associated with address book entries were not reported. (Palm Pre2)

MMS Messages:

- The textual portion of MMS messages was not reported. (BlackBerry Torch, Nokia 6350, HTC Thunderbolt)

Call Logs:

- Acquisition of call log data ended in errors. (Motorola Tundra)

Subscriber and equipment related information:

- Equipment-related information was not reported. (Palm Pre2)

Address book entries containing non-ASCII characters:

- Acquisition of address book entries containing non-ASCII characters were reported incorrectly. (BlackBerry Torch)

Device acquisition disruption:

- When connectivity was interrupted, the tool failed to notify the user that the acquisition had been disrupted. (Palm Pre2)

For a complete copy of the report, go to:
http://www.nij.gov/pubs-sum/238993.htm

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

TEST REPORT FOR:
MOBILE PHONE EXAMINER PLUS (MPE+) 4.6.0.2

October 2012

The CFTT Project tested the Mobile Phone Examiner Plus (MPE+) 4.6.0.2 tool against the Mobile Device Specification available at: http://www.cftt.nist.gov/mobile_devices.htm

Our results are:

Mobile Phone Examiner Plus is designed for logical and physical acquisitions, data analysis and report management from mobile phones, Smart phones and Subscriber Identity Modules (SIMs).

The tool was tested for its ability to acquire active and deleted data from the internal memory of mobile devices and SIMs. Except for the following anomalies, the tool acquired all supported data objects completely and accurately for all six mobile devices tested.

Device Connectivity:

- Connectivity to the mobile device was inconsistent, 1 out of 20 attempts were successful. (HTC Thunderbolt)

Subscriber- and equipment-related information:

- Equipment-related information was not reported. (iPhone4 GSM, HTC Thunderbolt).

Personal Information Management (PIM) data:

- Graphics files associated with address book entries were not reported. (BlackBerry Torch)
- Calendar entries were not acquired. (BlackBerry Torch)
- One out of seven address book entries were reported. (Nokia 6350)
- Address book entries with fields for a first, middle and last name were reported incorrectly. The middle- and last-name fields were not reported. (Motorola Tundra).

Call Logs:

- Acquisition of call log data ended in errors. (BlackBerry Torch)

Abbreviated Dialing Numbers (ADN):

- Acquisition of call log data ended in errors. (BlackBerry Torch)

Non-ASCII characters:

- Text messages containing the non-ASCII character é' were reported as '|'. (BlackBerry Torch)
- Address book entries containing non-ASCII characters were reported as '?'. (Motorola Tundra)
- Acquisition of ADN containing the non-ASCII character 'é' ended in errors. (SIM)

Acquisition of internal memory data elements:

- Acquisition of the File System ended in errors. (Motorola Tundra)

Device acquisition disruption:

- When connectivity was interrupted, the tool failed to notify the user that the acquisition had been disrupted. (Motorola Tundra)

For a complete copy of the report, go to:
http://www.nij.gov/pubs-sum/238996.htm

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

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).

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

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

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

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

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

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)

- 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

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)

- 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

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)

- 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

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)

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

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)

- 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

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)

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

For a complete copy of the report, go to:
http://www.ojp.usdoj.gov/nij/pubs-sum/228982.htm

Vendor information:
BitPim
http://www.bitpim.org

TEST REPORT FOR:
MOBILEDIT! FORENSICS 3.2.0.738

January 2010

The CFTT Project tested the MOBILedit! Forensics 3.2.0.738 tool against the Mobile Device Specification available at: http://www.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

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).

- Foreign language address book entries were not displayed properly within the individual report files. Test Case: CFT–IMO–01 (MOTO V710).

- Foreign language address book entries were not displayed properly within the preview pane. Test Case: CFT–IMO–02 (LG VX5400, LG VX6100, SCH u410, SCH u740).

- Data inconsistencies existed between the preview-pane view and the generated reports. Test Case: CFT–IMO–03 (LG VX5400, LG VX6100, MOTO V710, SCH u410, SCH u740).

- Incorrect characters were displayed from the wrong character set for foreign language address book entries. Test Case: CFT–IMO–08 (LG VX5400, LG VX6100, Samsung SCH–u410, Samsung SCH–u740, Samsung SPH–a660).

For a complete copy of the report, go to:
http://www.ojp.usdoj.gov/nij/pubs-sum/228222.htm

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

TEST REPORT FOR:
FINAL DATA – FINAL MOBILE FORENSICS 2.1.0.0313

September 2009

The CFTT Project tested the Final Data – Final Mobile Forensics 2.1.0.0313 tool against the Mobile Device Specification available at: http://www.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).

- When attempting to open a case file that has been modified with a hex editor, examiners are not informed the case file has been modified. Note: While the tool does not provide a warning message, modified case files cannot be opened. Test Case: CFT–IMO–04 (LG vx5400, LG vx6100, Moto v710, SCH u410, SCH u740, SPH a660).

- Address book entries and text messages containing non-ASCII characters such as: à, é were excluded from the address book entry and text message. Contacts and Text messages containing characters such as: 阿恶哈拉 were not reported. Test Case: CFT–IMO–08 (LG vx5400, LG vx6100, Moto v710, SCH u410, SCH u740, SPH a660).

For a complete copy of the report, go to:
http://www.ojp.usdoj.gov/nij/pubs-sum/228227.htm

Vendor information:
Final Data, Inc.
http://www.finaldata.com

TEST REPORT FOR:
PARABEN DEVICE SEIZURE 3.1

September 2009

The CFTT Project tested the Paraben Device Seizure 3.1 tool against the Mobile Device Specification available at: http://www.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)

For a complete copy of the report, go to:
http://www.ojp.usdoj.gov/nij/pubs-sum/228221.htm

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

TEST REPORT FOR:
CELLEBRITE UFED 1.1.05

September 2009

The CFTT Project tested the Cellebrite UFED 1.1.05 tool against the Mobile Device Specification available at: http://www.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)

- Outgoing text messages did not contain the outgoing date/time stamp. Test Case: CFT–IM–08 (MOTO V710)

- All outgoing text messages present in internal memory were not reported. Test Case: CFT–IM–08 (MOTO V710)

For a complete copy of the report, go to:
http://www.ojp.usdoj.gov/nij/pubs-sum/228220.htm

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

TEST REPORT FOR:
MICRO SYSTEMATION .XRY 3.6

October 2008

The CFTT Project tested the Micro Systemation .XRY 3.6 tool against the Mobile Device Specification available at: http://www.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/

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/

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/

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)

- 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/

TEST REPORT FOR:
ILOOKIX V2.2.3.151

September 2014

The CFTT Project tested the ILooKIX v2.2.3.151 tool against the Deleted File Recovery Tool Specification available at: http://www.cftt.nist.gov/DeletedFileRecovery.htm

Our results are:

The focus of this report is to characterize the observed behavior of the tested tool for the recovery of deleted files based on residual file system metadata remaining after files are deleted. The tool is applied to a set of image files constructed to present a variety of common file deletion scenarios for widely used file systems. If a tool does not completely recover a file this may stem from one or more causes. These factors may include the following:

- The data are no longer present in the image, e.g., overwritten.
- Sufficient meta-data to locate the data is not present or reachable.
- The algorithm implemented by the tool does not use the meta-data that locates the missing data.
- The implementation of the tool algorithm is incorrect.

In many cases, there is no one behavior that is correct. A tool designer may choose from different algorithms that each have their own behaviors. The algorithm choices have trade offs for each file layout scenario and file system meta-data characteristics. It may be that no one algorithm is correct all the time. For example, in FAT file systems no meta-data is present to locate more than the first block of the file. The algorithms used to recover files from FAT file systems only recover the deleted file completely when certain conditions prevail on the subject media. The conditions and algorithm success are determined by the specific drive content and file system meta-data characteristics. The test images for each test case are

"dd" images of a hard drive from a cleanly shut down system. The tool must operate within the confines of the operating systems and file systems. Because the file systems tested require different algorithms for each file system and therefore produce different results for each file system, results for each file system are discussed individually.
Some general observations follow:

- For the file systems tested, deleted files were recovered from FAT12, FAT16, FAT32, NTFS, exFAT and ext2 file systems. No files were recovered from ext3, ext4 or HSF+ file systems.
- File content was always recovered in whole clusters (a cluster is a power of 2 multiple of 512 bytes, e.g., 512, 1024, 2048, 4096, . . .).
- The files recovered by the tool were composed of clusters from one or more sources. All recovered content originated either in a previously deleted file, an existing file or meta-data that had overwritten data from a deleted file (reported as from an undetermined source).
- The tool was able to list active files and directories from FAT, exFAT, NTFS, ext2, and ext3 file systems. No files were listed from ext4 or HFS+ file systems.
- Non-Latin character file names, e.g., 北京.txt, were displayed correctly for both recovered and active files.

Each file system type has different metadata structures. This leads to different tool behaviors for each file system type. Observed file system specific (FAT, ExFAT, NTFS, Ext, HFS+) tool behaviors are addressed in the report summary section.

A discussion of specific tool behavior is in Section 3, with test details presented in Section 4.

For a complete copy of the report, go to:
https://cyberfetch.org/groups/community/test-results-deleted-file-recovery-and-active-file-listing-tool-ilookix-v223151

Supplier information:
Perlustro, L.P.
http://perlustro.com/

TEST REPORT FOR:

THE SLEUTH KIT (TSK) 3.2.2 / AUTOPSY 2.24

July 2014

The CFTT Project tested The Sleuth Kit (TSK) 3.2.2 / Autopsy 2.24 tool against the Deleted File Recovery Tool Specification available at: http://www.cftt.nist.gov/DeletedFileRecovery.htm

Our results are:

The focus of this report is to characterize the observed behavior of the tested tool for the recovery of deleted files based on residual file system metadata remaining after files are deleted. The tool is applied to a set of image files constructed to present a variety of common file deletion scenarios for widely used file systems. If a tool does not completely recover a file this may stem from one or more causes. These factors may include the following:

- The data are no longer present in the image, e.g., overwritten.
- Sufficient meta-data to locate the data is not present or reachable.
- The algorithm implemented by the tool does not use the meta-data that locates the missing data.
- The implementation of the tool algorithm is incorrect.

In many cases, there is no one behavior that is correct. A tool designer may choose from different algorithms that each have their own behaviors. The algorithm choices have trade offs for each file layout scenario and file system meta-data characteristics. It may be that no one algorithm is correct all the time. For example, in FAT file systems no meta-data is present to locate more than the first block of the file. The algorithms used to recover files from FAT file systems only recover the deleted file completely when certain conditions prevail on the subject media. The conditions and algorithm success are determined by the specific drive content and file system meta-data characteristics. The test images for each test case are

"dd" images of a hard drive from a cleanly shut down system. The tool must operate within the confines of the operating systems and file systems. Because the file systems tested require different algorithms for each file system and therefore produce different results for each file system, results for each file system are discussed individually.

Some general observations follow:

- For the file systems tested, deleted files were recovered from FAT12, FAT16, FAT32, NTFS and ext2 file systems. No files were recovered from exFAT, ext3, ext4 or HSF+ file systems. However, some file names were recovered from ext3 and ext4 file systems.
- File content was always recovered in whole clusters (a cluster is a power of 2 multiple of 512 bytes, e.g., 512, 1024, 2048, 4096, . . .).
- The files recovered by the tool were composed of clusters from one or more sources. All recovered content originated either in a previously deleted file, an existing file or meta-data that had overwritten data from a deleted file (reported as from an undetermined source).
- The tool was able to list active files from the following tested file systems: FAT, NTFS, ext2, ext3, ext4 and HFS+. For the ext4 file system, the tool sometimes only listed files and directories in the root directory. The tool does not support the exFAT file system.

Each file system type has different metadata structures. This leads to different tool behaviors for each file system type. Observed file system specific (FAT, ExFAT, NTFS, Ext, HFS+) tool behaviors are addressed in the report summary section.

A discussion of specific tool behavior is in Section 3, with test details presented in Section 4.

For a complete copy of the report, go to:
https://cyberfetch.org/groups/community/test-results-deleted-file-recovery-and-active-file-listing-tool-sleuth-kit-tsk-322

Supplier information:
Brian Carrier
http://www.sleuthkit.org/

TEST REPORT FOR:
X-WAYS FORENSICS VERSION 16.0 SR-4

July 2014

The CFTT Project tested the X-Ways Forensics Version 16.0 SR-4 tool against the Deleted File Recovery Tool Specification available at: http://www.cftt.nist.gov/DeletedFileRecovery.htm

Our results are:

The focus of this report is to characterize the observed behavior of the tested tool for the recovery of deleted files based on residual file system metadata remaining after files are deleted. The tool's "Particularly Thorough File System Data Structure Search" feature was not selected for any of the tests. The tool is applied to a set of image files constructed to present a variety of common file deletion scenarios for widely used file systems. If a tool does not completely recover a file this may stem from one or more causes. These factors may include the following:

- The data are no longer present in the image, e.g., overwritten.
- Sufficient meta-data to locate the data is not present or reachable.
- The algorithm implemented by the tool does not use the meta-data that locates the missing data.
- The implementation of the tool algorithm is incorrect.

In many cases, there is no one behavior that is correct. A tool designer may choose from different algorithms that each have their own behaviors. The algorithm choices have trade offs for each file layout scenario and file system meta-data characteristics. It may be that no one algorithm is correct all the time. For example, in FAT file systems no meta-data is present to locate more than the first block of the file. The algorithms used to recover files from FAT file systems only recover the deleted file completely when certain conditions prevail on the subject media. The conditions and

algorithm success are determined by the specific drive content and file system meta-data characteristics. The test images for each test case are "dd" images of a hard drive from a cleanly shut down system. The tool must operate within the confines of the operating systems and file systems. Because the file systems tested require different algorithms for each file system and therefore produce different results for each file system, results for each file system are discussed individually.

Some general observations follow:

- For the file systems tested, deleted files were recovered from FAT12, FAT16, FAT32, NTFS, exFAT and ext2 file systems. No files were recovered from ext3, ext4 or HSF+ file systems. However, some file names were recovered from ext3 and ext4 file systems.
- File content was always recovered in whole clusters (a cluster is a power of 2 multiple of 512 bytes, e.g., 512, 1024, 2048, 4096, . . .).
- The files recovered by the tool were composed of clusters from one or more sources. All recovered content originated either in a previously deleted file, an existing file or meta-data that had overwritten data from a deleted file (reported as from an undetermined source).
- The tool was able to list active files and directories from all file systems tested (FAT, exFAT, NTFS, ext2, ext3, ext4 and HFS+ file systems).
- Non-Latin character file names, e.g., 北京.txt, were displayed correctly for both recovered and active files.

Each file system type has different metadata structures. This leads to different tool behaviors for each file system type. Observed file system specific (FAT, ExFAT, NTFS, Ext, HFS+) tool behaviors are addressed in the report summary section.

A discussion of specific tool behavior is in Section 3, with test details presented in Section 4.

For a complete copy of the report, go to:
https://cyberfetch.org/groups/community/test-results-deleted-file-recovery-and-active-file-listing-tool-x-ways-forensics

Supplier information:
X-Ways AG
http://www.x-ways.com/

TEST REPORT FOR:
SMART FOR LINUX VERSION 2011-02-02 (REVISED)

June 2014

The CFTT Project tested the SMART for Linux Version 2011-02-02 (Revised) tool against the Deleted File Recovery Tool Specification available at: http://www.cftt.nist.gov/DeletedFileRecovery.htm

Our results are:

The focus of this report is to characterize the observed behavior of the tested tool for the recovery of deleted files based on residual file system metadata remaining after files are deleted. The tested tool, ASR Data SMART for Linux Version 2011-02-02, has a flexible design that allows inclusions of individual modules for processing different file systems. The tool is applied to a set of image files constructed to present a variety of common file deletion scenarios for widely used file systems. If a tool does not completely recover a file this may stem from one or more causes. These factors may include the following:

- The data are no longer present in the image, e.g., overwritten.
- Sufficient meta-data to locate the data is not present or reachable.
- The algorithm implemented by the tool does not use the meta-data that locates the missing data.
- The implementation of the tool algorithm is incorrect.

In many cases, there is no one behavior that is correct. A tool designer may choose from different algorithms that each have their own behaviors. The algorithm choices have trade offs for each file layout scenario and file system meta-data characteristics. It may be that no one algorithm is correct all the time. For example, in FAT file systems no meta-data is present to locate more than the first block of the file. The algorithms used to recover files from FAT file systems only recover the deleted file completely when certain conditions prevail on the subject media. The conditions and

algorithm success are determined by the specific drive content and file system meta-data characteristics. The test images for each test case are "dd" images of a hard drive from a cleanly shut down system. The tool must operate within the confines of the operating systems and file systems. Because the file systems tested require different algorithms for each file system and therefore produce different results for each file system, results for each file system are discussed individually.

Some general observations follow:

- For the file systems tested, deleted files were recovered from FAT12, FAT16, FAT32, NTFS, and ext2 file systems. No files were recovered from ExFAT, ext3, ext4 or HSF+ file systems.
- File content was always recovered in whole clusters (a cluster is a power of 2 multiple of 512 bytes, e.g., 512, 1024, 2048, 4096, . . .).
- A recovered file is composed of clusters from one or more sources. All recovered content originated either in a previously deleted file, an existing file or meta-data that had overwritten data from a deleted file (reported as from an undetermined source).
- The tool was able to list active files from the following file systems: FAT, NTFS, ext2 and ext3.
- Non-Latin character file names were not displayed correctly.

Each file system type has different metadata structures. This leads to different tool behaviors for each file system type. Observed file system specific (FAT, ExFAT, NTFS, Ext, HFS+) tool behaviors are addressed in the report summary section.

A discussion of specific tool behavior is in Section 3, with test details presented in Section 4.

For a complete copy of the report, go to:
https://cyberfetch.org/groups/community/test-results-deleted-file-recovery-and-active-file-listing-tool-smart-linux-version

Supplier information:
ASR Data
http://www.asrdata.com/

TEST REPORT FOR:
FTK VERSION 3.3.0.33124 (REVISED)

June 2014

The CFTT Project tested the FTK Version 3.3.0.33124 (Revised) tool against the Deleted File Recovery Tool Specification available at: http://www.cftt.nist.gov/DeletedFileRecovery.htm

Our results are:

The focus of this report is to characterize the observed behavior of the tested tool for the recovery of deleted files based on residual file system metadata remaining after files are deleted. The tool is applied to a set of image files constructed to present a variety of common file deletion scenarios for widely used file systems. If a tool does not completely recover a file this may stem from one or more causes. These factors may include the following:

- The data are no longer present in the image, e.g., overwritten.
- Sufficient meta-data to locate the data is not present or reachable.
- The algorithm implemented by the tool does not use the meta-data that locates the missing data.
- The implementation of the tool algorithm is incorrect.

In many cases, there is no one behavior that is correct. A tool designer may choose from different algorithms that each have their own behaviors. The algorithm choices have trade offs for each file layout scenario and file system meta-data characteristics. It may be that no one algorithm is correct all the time. For example, in FAT file systems no meta-data is present to locate more than the first block of the file. The algorithms used to recover files from FAT file systems only recover the deleted file completely when certain conditions prevail on the subject media. The conditions and algorithm success are determined by the specific drive content and file system meta-data characteristics. The test images for each test case are

"dd" images of a hard drive from a cleanly shut down system. The tool must operate within the confines of the operating systems and file systems. Because the file systems tested require different algorithms for each file system and therefore produce different results for each file system, results for each file system are discussed individually.

Some general observations follow:

- For the file systems tested, deleted files were recovered from FAT12, FAT16, FAT32, NTFS, exFAT and ext2 file systems. No files were recovered from ext3, ext4 or HSF+ file systems.
- File content was always recovered in whole clusters (a cluster is a power of 2 multiple of 512 bytes, e.g., 512, 1024, 2048, 4096, . . .).
- The files recovered by the tool were composed of clusters from one or more sources. All recovered content originated either in a previously deleted file, an existing file or meta-data that had overwritten data from a deleted file (reported as from an undetermined source).
- The tool was able to list active files from all file systems tested (FAT, exFAT, NTFS, ext2, ext3, ext4 and HFS+ file systems.

Each file system type has different metadata structures. This leads to different tool behaviors for each file system type. Observed file system specific (FAT, ExFAT, NTFS, Ext, HFS+) tool behaviors are addressed in the report summary section.

A discussion of specific tool behavior is in Section 3 of the report, with test details presented in Section 4. In more recent tool versions the vendor has addressed problematic tool behaviors.

For a complete copy of the report, go to:
https://cyberfetch.org/groups/community/test-results-deleted-file-recovery-and-active-file-listing-tool-ftk-version

Supplier information:
Access Data
http://www.accessdata.com/

TEST REPORT FOR:
ENCASE FORENSIC VERSION 6.18.0.59

June 2014

The CFTT Project tested the EnCase Forensic Version 6.18.0.59 tool against the Deleted File Recovery Tool Specification available at: http://www.cftt.nist.gov/DeletedFileRecovery.htm

Our results are:

The focus of this report is to characterize the observed behavior of the tested tool for the recovery of deleted files based on residual file system metadata remaining after files are deleted. The tool is applied to a set of image files constructed to present a variety of common file deletion scenarios for widely used file systems. If a tool does not completely recover a file this may stem from one or more causes. These factors may include the following:

- The data are no longer present in the image, e.g., overwritten.
- Sufficient meta-data to locate the data is not present or reachable.
- The algorithm implemented by the tool does not use the meta-data that locates the missing data.
- The implementation of the tool algorithm is incorrect.

In many cases, there is no one behavior that is correct. A tool designer may choose from different algorithms that each have their own behaviors. It may be that no one algorithm is correct all the time. For example, in FAT file systems no meta-data is present to locate more than the first block of the file. The algorithms used to recover files from FAT file systems only recover the deleted file completely when certain conditions prevail on the subject media. The conditions and algorithm success are determined by the specific drive content. The test images for each test case are "dd" images of a hard drive from a cleanly shut down system. The tool must operate within the confines of the operating systems and file systems. Because the

file systems tested require different algorithms for each file system and therefore produce different results for each file system, results for each file system are discussed individually.

Some general observations follow:

- For the file systems tested, deleted files were recovered from FAT12, FAT16, FAT32, NTFS, exFAT and ext2 file systems. No files were recovered from ext3, ext4 or HSF+ file systems.
- File content was always recovered in whole clusters (a cluster is a power of 2 multiple of 512 bytes, e.g., 512, 1024, 2048, 4096, . . .).
- A recovered file is composed of clusters from one or more sources. All recovered content originated either in a previously deleted file, an existing file or meta-data that had overwritten data from a deleted file.
- The tool was able to list active files from FAT, exFAT, NTFS, ext2 and ext3 file systems. For HFS+ file systems, files were listed if the file system was formatted to not be case sensitive. No files were listed for ext4 files.
- Non-Latin character filenames, e.g., 北京.txt, were displayed correctly for both active files and recovered files.

Each file system type has different metadata structures. This leads to different tool behaviors for each file system type. Observed file system specific (FAT, ExFAT, NTFS, Ext, HFS+) tool behaviors are addressed in the report summary section.

A discussion of tool behavior is in Section 3 of the report, with test details presented in Section 4. The vendor in more recent tool versions has addressed problematic tool behaviors.

For a complete copy of the report, go to:
https://cyberfetch.org/groups/community/test-results-deleted-file-recovery-and-active-file-listing-encase-forensic-version

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

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

TEST REPORT FOR:

ADROIT PHOTO FORENSICS 2013 V3.1D

July 2014

The CFTT Project tested the Adroit Photo Forensics 2013 v3.1d tool against the Forensic File Carving Tool Specification available at: http://www.cftt.nist.gov/filecarving.htm

Our results are:

Adroit Photo Forensics 2013 recovers graphic files of various types utilizing proprietary SmartCarving™ and GuidedCarving™ technologies. Below are summaries on how Adroit v3.1d performed when carving raw disembodied "dd" images containing various layouts of fragmentation and ompleteness.

Adroit was mostly successful at carving bmp, png and jpg files in a viewable state. Generally, no more than 1 tiff or 2 gif files per test image were carved in a complete or viewable state with minor alteration. This anomaly has been fixed in version 3.2b. False positives occurred only for jpg files. This occurs when Adroit parses the raw "dd" image file and comes across the string "FF D8" within a file that is not a jpg.

For a complete copy of the report, go to:
https://cyberfetch.org/groups/community/test-results-graphic-file-carving-tool-adroit-photo-forensics-2013-v31d

Supplier information:
Digital Assembly
http://www.digital-assembly.com/

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

TEST REPORT FOR:

ENCASE FORENSIC V6.18.0.59

July 2014

The CFTT Project tested the EnCase Forensic v6.18.0.59 tool against the Forensic File Carving Tool Specification available at: http://www.cftt.nist.gov/filecarving.htm

Our results are:

Below are summaries on how EnCase Forensic v6.18.0.59 performed when carving raw "dd" images containing various layouts of fragmentation and completeness.

EnCase Forensic v6.18.0.59 was mostly successful at carving contiguous files (i.e., bmp, png and jpg). EnCase does not support carving fragmented files. Recovered gif files were either not viewable or partially viewable. False positives occurred only for tiff and jpg files.

The following test cases are not supported by EnCase Forensic v6.18.0.59: Fragmented in Order (section 4.3), Incomplete (section 4.4), Fragmented Out of Order (section 4.5) and Braided Pair (section 4.6). However, the test case results are included providing users with an overview for reference.

All test cases were run under Windows XP v5.1.2600 as well as Windows 7 v6. 1.7601 environments and the results were consistent.

For more test result details see section 4 of the test report.

For a complete copy of the report, go to:
https://cyberfetch.org/groups/community/test-results-graphic-file-carving-tool-encase-forensic-v618059

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

NIJ National Institue of Justice

Supplier information:
Guidance Software Inc.
http://www.encase.com/

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

TEST REPORT FOR:

ENCASE FORENSIC V7.09.05

July 2014

The CFTT Project tested the EnCase Forensic v7.09.05 tool against the Forensic File Carving Tool Specification available at: http://www.cftt.nist.gov/filecarving.htm

Our results are:

Below are summaries on how Encase Forensic v7.09.05 performed when carving raw "dd" images containing various layouts of fragmentation and completeness.

EnCase Forensic v7.09.05was mostly successful at carving contiguous files (i.e., bmp, png and jpg). EnCase does not support carving fragmented files. Recovered gif files were not viewable for most of the test cases. False positives occurred for bmp, tiff and jpg files.

The following test cases are not supported by EnCase Forensic v7.09.05: Fragmented in Order (section 4.3), Incomplete (section 4.4), Fragmented Out of Order (section 4.5) and Braided Pair (section 4.6). However, the test case results are included providing users with an overview for reference.

Test case No Padding (section 4.1), was run under Windows XP v5.1.2600 as well as Windows 7 v6.1.7601 environments and the results were not consistent. EnCase recovered more viewable files when run under Windows 7.

For more test result details see section 4 of the test report.

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:
https://cyberfetch.org/groups/community/test-results-graphic-file-carving-tool-encase-forensic-v70905

Supplier information:
Guidance Software Inc.
http://www.encase.com/

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

TEST REPORT FOR:

FTK V4.1

July 2014

The CFTT Project tested the FTK v4.1 tool against the Forensic File Carving Tool Specification available at: http://www.cftt.nist.gov/filecarving.htm

Our results are:

Below are summaries on how FTK v4.1 performed when carving raw disembodied "dd" images containing various layouts of fragmentation and completeness.

FTK 4.1 was mostly successful at carving bmp, png and jpg files across all test images in a viewable state. The majority of carved gif files were incomplete. It does not carve tiff files. Generally, no more than 1 tiff or 2 gif files per test image are carved in a complete or viewable state with minor alteration by using default settings.

For more test result details see section 4 of the test report.

For a complete copy of the report, go to:
https://cyberfetch.org/groups/community/test-results-graphic-file-carving-tool-ftk-v41

Supplier information:
Access Data
http://accessdata.com/

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

TEST REPORT FOR:
ILOOK V2.2.7

July 2014

The CFTT Project tested the iLook v2.2.7 tool against the Forensic File Carving Tool Specification available at: http://www.cftt.nist.gov/filecarving.htm

Our results are:

Below summarizes how iLook v2.2.7 performed when carving raw disembodied "dd" images containing various layouts of fragmentation and completeness.

The specific build of iLook v2.2.7 does not fully support file carving. Please refer to the iLook website (https://www.perlustro.com) for further updates.

For a complete copy of the report, go to:
https://cyberfetch.org/groups/community/test-results-graphic-file-carving-tool-ilook-v227

Supplier information:
Perlustro LP
https://www.perlustro.com/

TEST REPORT FOR:
PHOTOREC V7.0-WIP

July 2014

The CFTT Project tested the PhotoRec v7.0-WIP tool against the Forensic File Carving Tool Specification available at:
http://www.cftt.nist.gov/filecarving.htm

Our results are:

Below are summaries on how PhotoRec v7.0-WIP performed when carving raw disembodied "dd" images containing various layouts of fragmentation and completeness.

PhotoRec was mostly successful at carving gif, bmp, png, jpg and tiff files in a viewable state from the majority test cases excluding the test case: Fragmented Out of Order. Files landing on non-sector boundaries (i.e., Byte Shifted) were not recovered.

For more test result details see section 4 of the test report.

For a complete copy of the report, go to:
https://cyberfetch.org/groups/community/test-results-graphic-file-carving-tool-photorec-v70-wip

Supplier information:
GNU General Public License
http://www.cgsecurity.org/

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

TEST REPORT FOR:

RECOVER MY FILES V5.2.1

July 2014

The CFTT Project tested the Recover My Files v5.2.1 tool against the Forensic File Carving Tool Specification available at: http://www.cftt.nist.gov/filecarving.htm

Our results are:

Below are summaries on how Recover My Files v5.2.1 performed when carving raw disembodied "dd" images containing various layouts of fragmentation and completeness.

Recover My Files was mostly successful at carving bmp, jpg, png and tiff files in a viewable state. Gif files were typically viewable but incomplete. Files not aligned to sector boundaries were not carved. There were no false positives or not-viewable files carved for any test case.

For more test result details see section 4 of the test report.

For a complete copy of the report, go to:
https://cyberfetch.org/groups/community/test-results-graphic-file-carving-tool-recover-my-files-v521

Supplier information:
GetData
http://www.getdata.com/

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

TEST REPORT FOR:
R-STUDIO V6.2

July 2014

The CFTT Project tested the R-Studio v6.2 tool against the Forensic File Carving Tool Specification available at: http://www.cftt.nist.gov/filecarving.htm

Our results are:

Below are summaries on how R-Studio v6.2 performed when carving raw disembodied "dd" images containing various layouts of fragmentation and completeness.

R-Studio carved the majority of all file types (i.e., gif, bmp, png, jpg, tiff) across all test cases in a viewable state with the exception of thumbnails and files that were not aligned to sector boundaries. For these two exceptions, no files were carved. No false positives were reported.

For more test result details see section 4 of the test report.

For a complete copy of the report, go to:
https://cyberfetch.org/groups/community/test-results-graphic-file-carving-tool-r-studio-v62

Supplier information:
R-Tools Technology Inc.
http://www.r-tt.com/

TEST REPORT FOR:
SCALPEL V2.0

July 2014

The CFTT Project tested the Scalpel v2.0 tool against the Forensic File Carving Tool Specification available at: http://www.cftt.nist.gov/filecarving.htm

Our results are:

Below are summaries on how Scalpel v2.0 performed when carving raw disembodied "dd" images containing various layouts of fragmentation and completeness.

Scalpel was mostly successful at carving gif and tif files in a viewable state. The tool across all test images typically did not return carved jpg files in a viewable state. The majority of carved bmp and png files were false-positives.

For more test result details see section 4 of the test report.

For a complete copy of the report, go to:
https://cyberfetch.org/groups/community/test-results-graphic-file-carving-tool-scalpel-v20

Supplier information:
https://github.com/sleuthkit/scalpel

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

TEST REPORT FOR:

X-WAYS FORENSICS V17.6

July 2014

The CFTT Project tested the X-Ways Forensics v17.6 tool against the Forensic File Carving Tool Specification available at: http://www.cftt.nist.gov/filecarving.htm

Our results are:

Below are summaries on how X-Ways Forensics v17.6 performed when carving raw disembodied "dd" images containing various layouts of fragmentation and completeness.

X-Ways Forensics was successful at carving gif, bmp, png, jpg and tiff files in a viewable state for all non-fragmented "dd" images. Fragmented "dd" images mostly returned fewer viewable-complete ratings for all file types.

For more test result details see section 4 of the test report.

For a complete copy of the report, go to:
https://cyberfetch.org/groups/community/test-results-graphic-file-carving-tool-x-ways-forensics-v176

Supplier information:
X-Ways Forensics
http://x-ways.net/

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

TEST REPORT FOR:
DEFRASER V1.3

October 2014

The CFTT Project tested the Defraser v1.3 tool against the Forensic File Carving Tool Specification available at: http://www.cftt.nist.gov/filecarving.htm

Our results are:

Below are summaries on how Defraser v1.3 performed when carving raw "dd" images containing various layouts of fragmentation and completeness.

Defraser was most successful at carving video files (i.e., mov, avi, wmv and 3gp) files from no padding, cluster padded, and byte shifted "dd" images. The tool had a reduced ability to recover viewable complete files from fragmented in order, incomplete, fragmented out of order and braided pair test cases. The majority of recovered mp4 files were not viewable. Ogv files were not recovered.

For more test result details, see section 4 of the complete test report.

For a complete copy of the report, go to:
https://cyberfetch.org/groups/community/test-results-video-file-carving-tool-defraser-v13

Supplier information:
Netherlands Forensic Institute

TEST REPORT FOR:
ENCASE V7.09.05

October 2014

The CFTT Project tested the EnCase v7.09.05 tool against the Forensic File Carving Tool Specification available at: http://www.cftt.nist.gov/filecarving.htm

Our results are:

Below are summaries on how EnCase v7.09.05 performed when carving raw "dd" images containing various layouts of fragmentation and completeness.

EnCase was most successful at carving video file types mp4, mov, avi, wmv in a viewable state. The carved mp4, mov, avi and wmv files were classified as Not Viewable or False Positive for all test cases. Video file types 3gp and ogv were not recovered.

For more test result details, see section 4 of the complete test report.

For a complete copy of the report, go to:
https://cyberfetch.org/groups/community/test-results-video-file-carving-tool-encase-v70905

Supplier information:
Guidance Software
http://www.guidancesoftware.com/

TEST REPORT FOR:
ILOOK V.2.2.7

October 2014

The CFTT Project tested the iLook v.2.2.7 tool against the Forensic File Carving Tool Specification available at: http://www.cftt.nist.gov/filecarving.htm

Our results are:

Below are summaries on how iLook v2.2.7 performed when carving raw "dd" images containing various layouts of fragmentation and completeness.

The specific build of iLook v2.2.7 does not fully support file carving. Please refer to the iLook website (https://www.perlustro.com) for further updates. However, the results included in this report could be used as reference for video file carving.

The majority of files recovered by iLook were mostly classified as either Viewable-Incomplete or False Positive. No mp4 and 3gp files were recovered.

For more test result details, see section 4 of the complete test report.

For a complete copy of the report, go to:
https://cyberfetch.org/groups/community/test-results-video-file-carving-tool-ilook-v227

Supplier information:
Perlustro Product Company
http://www.perlustro.com/

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

TEST REPORT FOR:
PHOTOREC V7.0-WIP

October 2014

The CFTT Project tested the PhotoRec v7.0-WIP tool against the Forensic File Carving Tool Specification available at:
http://www.cftt.nist.gov/filecarving.htm

Our results are:

Below are summaries on how PhotoRec v7.0-WIP performed when carving raw "dd" images containing various layouts of fragmentation and completeness.

PhotoRec was most successful at carving video files (i.e., mp4, mov, avi, wmv, 3gp and ogv) from no padding, cluster padded, fragmented in order, incomplete and braided pair "dd" images. The tool had a reduced ability to recover viewable complete files from fragmented out of order and braided pair test cases. No files were recovered from files not aligned to sector boundaries.

For more test result details, see section 4 of the complete test report.

For a complete copy of the report, go to:
https://cyberfetch.org/groups/community/test-results-video-file-carving-tool-photorec-v70-wip

Supplier information:
Christophe Grenier (developer)
http://www.cgsecurity.org/

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

TEST REPORT FOR:
RECOVER MY FILES V5.2.1

October 2014

The CFTT Project tested the Recover My Files v5.2.1 tool against the Forensic File Carving Tool Specification available at: http://www.cftt.nist.gov/filecarving.htm

Our results are:

Below are summaries on how Recover My Files v5.2.1 performed when carving raw "dd" images containing various layouts of fragmentation and completeness.

RMF was most successful at carving mp4, mov, avi, wmv, 3gp and ogv from no padding braided pair and cluster padded "dd" images. Recovering video files from fragmented images (i.e., Simple, Partial, Disordered) returned an increase in Viewable-Incomplete and Not Viewable rankings. The Non-Sector boundary "dd" image containing a total of 36 files, recovered only 6 files all of which were classified as False Positive.

For more test result details, see section 4 of the complete test report.

For a complete copy of the report, go to:
https://cyberfetch.org/groups/community/test-results-video-file-carving-tool-recover-my-files-v521

Supplier information:
Get Data
http://www.getdata.com/