CprE 592-YG
Computer and Network Forensics

Test Results from NIST's Computer Forensics Tool Testing (CFTT) project

Yong Guan
3216 Coover
Tel: (515) 294-8378
Email: guan@ee.iastate.edu

November 4, 2003

Homework Assignment

- Group-reading the following the document (available at http://www.ojp.usdoj.gov/nij/sciencetech/ecrime.htm):
  - Group1 (3 students) : Test Results for Disk Imaging Tools: EnCase 3.20
  - Group2 (2 students) Test Results for Disk Imaging Tools: dd Provided with FreeBSD 4.4
  - Group3 (2 students) Test Results for Disk Imaging Tools: dd GNU fileutils 4.0.36, Provided with Red Hat Linux 7.1
  - Group4 (2 students) Partial Results from Prototype Testing Efforts for Disk Imaging Tools: SafeBack 2.0
  - Group 5 (3 students) Test Results for Disk Imaging Tools: SafeBack 2.18
  - Group 6 (2 students) Disk Imaging (http://www.cftt.nist.gov/disk_imaging.htm)
- Each group has 15 minutes to present the report assigned, either by one student or all the students in the group.

Test Results for Disk Imaging Tools: EnCase 3.20

Group 1 Members:

Brylan C. Alexander
Noah Korba
Micheal Williams

Introduction

This document reports the results from testing EnCase 3.20, a commonly used disk imaging tool, against *Disk Imaging Tool Specification, Version 3.1.6,* developed by CFTT staff. This specification identifies the top- level disk imaging tool requirements as—

- The tool shall make a bit-stream duplicate or an image of an original disk or partition.
- The tool shall not alter the original disk.
- The tool shall log I/O errors.
- The tool's documentation shall be correct.

Note: The test methodology is for software tools that copy or image hard disk drives. It does not cover analog media or digital media such as cell phones or personal digital assistants (PDAs).

Test Results for Disk ImagingTools: EnCase 3.20

Tool Tested:	EnCase 3.20
Operating Systems:	Windows 2000 (5.00.2195), Windows 98, and Windows 98 DOS (Version 4.10.2222)
Supplier:	Guidance Software
Address:	572 East Green Street, Suite 300 Pasadena, CA 91101
Phone:	626–229–9191
Web:	*http://www.guidancesoftware.com*

Results Summary by Requirements

Section 1

7

Results Summary by Requirements

- "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.

  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.

8

Results Summary by Requirements

- EnCase, with two other exceptions, correctly and completely restored all disk sectors to a destination drive in the test cases that were run.

For certain partition types (FAT32 and NTFS), a logical restore of a partition is not an exact duplicate of the original.

In the Windows 2000 environment, a hard drive may appear to have fewer sectors than are actually available on the drive.

9

Results Summary by Requirements

- "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.

10

Results Summary by Requirements

- "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.

Anomalies

Section 2

Anomalies

- **BIOS anomaly**. For IDE hard drives on computers with a legacy BIOS, if the legacy BIOS underreports the number of cylinders on the drive and the BIOS is used to access the drive, then there may be a small area of sectors at the end of the drive that is not accessed.

13

Anomalies

- **Logical restore anomaly**. For certain partition types (FAT32 and NTFS), a logical restore of a partition is not an exact duplicate of the original.
- **Restore size anomaly**. In the Windows 2000 environment, a hard drive may appear to have fewer sectors than are actually available on the drive.

14

Anomalies

Table 2-1. Scope of Anomalies

Anomaly	Scope
BIOS	Image and restored copy.
Logical restore	Restored copy. By examining the image file, it was verified that the anomaly is only in the restored copy.
Restore size	Restored copy only.

Anomalies

Table 2-2. Example of Direct ATA versus BIOS Hard Drive Geometry

Access	Cylinders	Heads	Sectors per Head	Sectors per Cylinder	Total Sectors
Direct	3,309	16	63	1,008	3,335,472
BIOS	826	64	63	4,032	3,330,432

Note that 5,040 more sectors (3,335,472 minus 3,330,432) can be accessed through direct ATA than are reported by the legacy BIOS.

Test Case Selection

Section 3

17

Inapplicable Test Cases

Test cases that met the following criteria were designated as not applying to EnCase testing:

- Some test cases assume a feature not supported by EnCase. These include copy operation, removable destination media, NTFS partitions (in DOS), and advanced SCSI programming interface (ASPI).
- Logical acquisition and restore of Linux EXT2 partitions were not tested.

18

Inapplicable Test Cases

- Some test cases are going to be deleted from the test specification and are not ever used to test any disk imaging tools. For example, cases involving deleted file recovery are being deleted from the specification because deleted file recovery tools will be tested separately.
- Some test cases require support software or other tools that are not available. For example, some test cases specify I/O error simulation beyond the scope of the current tools, such as destination write error or image read error in a Windows environment.
- Some of the corrupt image cases are redundant for EnCase.

19

Modified Test Cases

Several test cases were modified to increase the coverage of EnCase testing. The test cases in *Disk Imaging Tool Specification, Version 3.1.6* do not provide for the following:

- Acquisition of an image through an interface other than IDE or SCSI (e.g., FastBloc acquisition of an IDE drive via a SCSI interface in Windows).
- Filling of excess sectors after an image restore.

20

Modified Test Cases

- Using direct ATA access to acquire an image and then restoring with a Windows interface.
- Cylinder alignment of a restored copy.

To address these issues, several changes were made to selected test cases.

Test Results by Assertion

Section 4

Mandatory Assertions

"If a source is accessed by the tool, then the source will not be altered"

- SHA-1 used to test this
- 50 tests performed, all passed

23

Mandatory Assertions

"If there are no errors reading from a source or errors writing to a destination, then a bit-stream duplicate of the source will be created on the destination"

- 31 tests performed, 12 errors
- Errors are anomalies. Some are due to file system sector allocation problems, and some are due to BIOS bit-transferring problems.
- EnCase's physical bit acquire reduces these anomolies

24

Mandatory Assertions

- "If there are errors reading from a source or writing to a destination, then a qualified bit-stream duplicate of the source will be created on the destination. The identified areas are replaced by values specified by the tools' documentation."
  - If errors are found, it should be known that there were errors, and the errors should be recorded as per-documentation of the tool.
  - EnCase passed this.

25

Mandatory Assertions

- "If there are errors reading from a source or writing to a destination, then the error types and locations are logged."

  - EnCase passed this as well

  - The tool must classify and report errors (block read, write errors, etc) to the user

26

Mandatory Assertions

- "If the source or destination is an IDE or SCSI drive and an image or bit-stream duplicate is created, then the interface used is presumed to be well-defined."

27

Mandatory Assertions

- "If a bit-stream duplicate of the source is created on a larger destination, then the contents of areas on the destination that are not part of the duplicate are set to values as specified in the tool documentation."

  - Protects a case from inheriting data that did not belong to the case

28

Mandatory Assertions

- "If a bit-stream duplicate of a source is created on a smaller destination, then the duplicate is qualified by omitted portions of the bit-stream, and the tools will notify the user that the source is larger than the destination"

  - "Drive is too small" errors reported by EnCase
  - EnCase also reports via pop-up window

29

Optional Assertions

- "If a hash of one or more blocks from the source is computer before duplication and is compared to a hash of the same blocks from the destination, they will be equal"

  -This is an extension of the first mandatory assertion

  - EnCase gives a general block range of where the corruption takes place

30

Optional Assertions

- "If more than one partition exists on the source disk, the tools will produce a duplicate of any user-selected source partition on the destination."

  -EnCase did well with FAT16, but were not always exact in FAT32 (file system control information was inaccurate, but data was OK)

31

Optional Assertions

- "If a partition exists on the source, the tools will display or log a message indicating that the partition exists and display or log one or more items of information from the following list: drive indicator, device type, device address, or mount point, size, space used, and free space."
  - Basically reports information about a partition
  - No anomalies with EnCase

32

Optional Assertions

- "If the tool logs the tool version, it will be the version referred to in the implementation's documentation."
  - EnCase passed this as well.

33

More Optional Assertions

- There are 10 more optional assertions that EnCase passed. They center around:
  - **Time indication**
  - **Error logging**
  - **General Logging**
  - **Image file portability**
  - **Image file verification**

Testing Environment

Section 5

35

Testing Environment

- 15 Computers Used
- 35 hard drives (16 unique models, 6 unique brands)
- Hard drives were arranged in one of several configurations

36

Extended BIOS Host Computers

- Four host computers
- Intel PIII – 933Mhz
- 512MB RAM
- 2 removable IDE slots
- 2 removable SCSI slots
- LS-120 Super Floppy

37

Legacy BIOS Host Computers

Nexar Computers: Beta 1, 3, 4, 6, & 7

- 166MHz processor speed
- 256MB RAM;
- Two hard disk drive bays
- CD–ROM & 1.44MB floppy drives
- ISA/PCI P54C Hewlett-Packard motherboard

38

Nexar Tests

- Delta1: used to compute SHA-1 values for tests on Nexar systems
- 888Mhz & 256MB RAM
- Hard disk drive bay with 15.37GB
- a CD–ROM, 1.44MB floppy, & 250MB zip drives

BIOS is PhoenixBios 4.0 Release 6.0.

39

Hard Disk Drives

40

Test Configurations

Host computer and hard drive setup determined by the test case parameters.

- 2 or 3 disk drives required for each test case
- Media disks required for most test cases
- Sources disk allowed something to copy
- Destination disk allowed a place for copy

41

Test Configurations

Test case run-time environment was created by one of two DOS boot floppies

- CD-Rom contained support and utility S/W
- Support S/W provided:

setup of test data

measurement of test results

control of the test process

42

Test Configurations

"The type of BIOS required for the test case determined the selection of the host computer."

- For extended BIOS requirement
  - 1 of the 15 extended BIOS computer systems selected

For legacy BIOS requirement

- 1 of the Nexar computers was selected

43

Test Configurations
-Source Disk-

- Source disk interface & source partition to use were factors determines source disk
- From this:

  A disk was selected with matching interface

  Additionally, a partition type needed for the test

44

Test Configurations
-Destination Drive-

- Destination interface & relative size parameters were factors in the selection of the destination drive.
- From this:

  A drive was selected with specified interface

  A size relative to the source disk was selected

  After the source and destination drives were selected, the media disk was selected for 1 of 2 drive slots

45

Test Configurations
-System Hard Drive-

- **Example of hard drive configuration used for the tests is provided**

ID	Step	Source	Destination	Media
1	Wipe		IDE primary 1	IDE primary 0
2	Wipe		SCSI ID 1	IDE primary 0
3	Acquire	IDE primary 0		IDE primary 1
4	Acquire	SCSI ID 0		IDE primary 0
5	Restore		IDE primary 1	IDE primary 0
6	Restore		SCSI ID 1	IDE primary 0
7	Compare	IDE primary 0	IDE primary 1	
8	Compare	IDE primary 0	SCSI ID 1	

46

Support Software

FS-TST Release 1.0 was developed to support the testing of disk imaging tools. [*http://www.cftt.nist.gov*]

- Software serves five main functions:
  - **initialization of a disk to a known value**
  - **comparison of a source with a destination**
  - **detection of changes to a disk**
  - **corruption of an image file**
  - **simulation of a faulty disk**

In addition to S/W, Win 98 DOS boot floppies created a run-time environment for the test case. One to create an environment to execute support S/W and the other to provide the source acquisition environment.

Test Case Structure

- A test case has five parts:
  - **setup**
  - **execution of the tool to acquire an image**
  - **execution of the tool to add the image to the case file**
  - **execution of the tool to restore the image to a destination drive**
  - **measurement of the results**

  Setup was completed in the DOS environment
  [Steps of setup provided in handout (List 1.1)]

Test Results Summary Key

Section 6

Test Results Key

- A table key is provided to explain the description of each section of the test results summary.

[Table Summary Key provided in handout (Table 1.1)]

Heading	Description
Actual Results:	List of any anomalies observed.
Analysis:	Whether or not the expected results were achieved.

Interpretation of Test Results

Section 7

51

Interpretation of Test Results

"There are six main questions of interest when examining the results of a test case:"

- Is the source disk unchanged?
- Has the correct number of sectors been accurately copied?
- Has the tool alerted the user to a destination smaller than the source?
- Has the tool handled excess destination sectors correctly as specified?
- Has the tool detected changes to an image file?
- Has the tool alerted the user to any I/O errors?

52

Test Results Interpretation

Source Disk

"Source disk integrity is checked by comparing the hash of the source disk computed before any tests run with after the tool is used. If the two hash values are not the same, then there has been a change to the source disk by the tool. The reference hash is recorded in the Source disk setup **box and the hash computed after the tool is run is recorded in the** Log file highlights **box."**

Small Destination Detection

"The tool should issue a message indicating that the destination is smaller than the source for any test case defined for a smaller destination. The message appears in a pop-up box on screen and is not logged to the EnCase report."

53

Test Results Interpretation

- Excess Sectors

  For disk operations, the tool should either backfill excess sectors or leave the contents as is. The tool action can be verified by the entries labeled *Zero fill, Other fill* and *Dst byte fill*, giving the count of sectors in each category.

  Changes to an Image File

  The Error Setup **box presents the command used to change the image file and the absolute LBA of the corrupted sector. If the tool detects that the image file has been changed, the** Log File Highlights **box has a message indicating, "The integrity of the following sector groups could not be verified: . . . ."I/O Errors**

54

Test Results Interpretation

- I/O Errors

  "The Error Setup **box presents the command used to setup an I/O error. If the tool detects the I/O error, the** Log File Highlights **box has a message indicating the type and location of the error."**

55

Test Results for Disk Imaging Tools: dd Provided with FreeBSD 4.4

Group 2 Members:

Kurt Niggemeyer
Michael Perkins

56

Computer Forensics Testing Tool (CFTT)

- The tool shall make a bit-stream duplicate or an image of an original disk or partition.
- Tool shall verify integrity of disk image file. *
- The tool shall not alter the original disk.
- The tool shall log I/O errors.
- The tool's documentation shall be correct.

57

Summary of Results

- Tool tested: dd Operating System: FreeBSD 4.4-RELEASE #0 released 9/01
- 32 test cases bit stream was accurate or image of disk or partition copied sectors perfectly.
- Integrity verification not applicable.
- SHA-1 hash of disks before and after duplication matched.
- Read/Write errors not tested. Log successful when src > dest.
- No errors found in documentation.

58

Methods

- Used DITS 3.1.6 for Linux – 32 of 52 tests
- Skipped tests which need image verification. Use md5 sum.
- Skipped tests of corrupted image files. Not supported.
- Skipped removable media such as magnetic tape. Media not available.

59

Operations

- 32 tests on IDE/SCSI drives basically composed of the following operations
  - **disk->disk or image**
  - **partition (NTFS, Linux, Fat 16, FAT 32)->disk or image**
  - **permutations**
    - **src = dest; src < dest; src > dest**
    - **disks**
      - ide->ide or scsi
      - scsi->scsi or ide

60

DITS 3.1.6 Mandatory Assertions

- **AM-1. If a source is accessed by the tool, then the source will not be altered.**
  - **1. SHA-1 hash values of sources from all 32 cases matched.**
- **AM-2. If no errors reading or writing, then a bit-stream duplicate of the source will be created on the destination.**
  - **Sector by sector comparison of all that was copied from each test case matched.**
- **AM-3. If errors happen when reading or writing, errors are replaced by values according to documentation.**
  - **Not tested. Presumably, a lot of work to create errors.**

61

More Assertions

- **AM-4. If there are errors reading from the source or writing to the destination, then the error types and locations are logged.**
  This assertion was not tested.
- **AM-5. If the source or destination is an IDE or SCSI drive and an image or bit-stream duplicate is created, then the interface used is presumed to be *well defined*.**
  See all test cases.
- **AM-6. If the expected results are achieved by following the documentation, then the documentation is presumed correct.**
  No errors were observed in the documentation.

62

Final Mandatory Assertions

- **AM-7. if src < dest, the parts of destination not written by source must = documentation**
  No change in FAT excess sectors.
  NTFS & Linux have excess dest sectors = source by hash.
- **AM-8. If src < dest, tool will notify the user that the source is larger than the destination.**
  All cases where dest < src gave a message /dev/*name*: end of device.

63

Optional Assertions

- AO-2 : if > 1 partitions, tool can copy all partitions
- AO-14: when no errors read/write, bit stream of image file = src

64

TESTING ENVIRONMENT

- Computers
  - **4 Pentium III 933Mhz machines w/ 2 IDE & 2 SCSI Slots**
  - **4 Pentium IV 2 Ghz w/ 512 MB Ram w/ 3 IDE & 2 SCSI slots**
  - **All computers: CDRW, Floppy, ½ w/ jazz drives?!?!?**

65

Testing Environment Continued

- Hard Drives
  - **6 brands w/ 13 different models from 6 GB to 41 GB**
  - **Seagate (SCSI), Fujitsu (SCSI), Quantum (SCSI), Western Digital (IDE), IBM (IDE), and Maxtor (IDE)**
- Actual Test
  - **Src & dest disks, media (img. & bsd), DOS Boot Floppy for Initialization, and CDROM w/ utilities**
    - **Init disk, cmp src/dest, detect changes w/ hash, img corruption, simulate bad disks**

66

Test steps

- Init and hash src disk.
- Init dest disk.
- Create dest partition if necessary. Hash excess if NTFS/Linux.
- If dest = img, format media disk.
- Restore src from media if img or copy src to dest disk.

67

Conclusions

- Missing Results
  - **Bad disks**
  - **Only IDE/SCSI**
- Test Problem
  - **Preconceived Notions**
  - **Redundant Information**

68

Test Results for Disk Imaging Tools: dd GNU fileutils 4.0.36, Provided with Red Hat Linux 7.1

Group 3 Members:

Casey Averill
Scott Borre

69

Computer Forensics Tool Testing

- NIJ
- NIST
- DoD
- Related Agencies

70

dd GNU fileutils 4.0.36

- What is it?
  - **A Disk Imaging Tool**

71

Disk Imaging Tool Specification

- Specifications are developed by CFTT
  - **Make a bit-stream duplicate or an image of an original disk or partition**
  - **Must not alter the disk**
  - **Log I/O errors**
  - **Documentation must be correct**

Note: Test methodology is for software tools that copy or image hard disk drives. It does not cover analog media or digital media such as cell phones or PDAs

72

Results Summary

- Tool shall not alter the original disk
  - **Passed**
  - **SHA-1 hashes matched**

73

Results Cont'd

- Tool shall make a bit-stream duplicate or an image of an original disk or partition
  - **Accurate**
  - **Failed to copy last sector of disk drives or partitions with an odd number of sectors**

74

Results Cont'd

- The tool shall log I/O errors
  - **dd produced a log message that there was no space left on the destination when the source was greater than the destination**
  - **Read/write errors were not tested**

75

Results Cont'd

- The tool's documentation shall be correct
  - **No errors were found**

76

Testing Environment

- Tests were run on five host computers
- More then 20 hard drives were used
  - **7 different models**
  - **5 different brands**
- Hard drives arranged in one of five possible configurations
  - **Based on Source interface, Dest. Interface, boot/media, and BIOS Boot Order.**

77

Support Software

- Used software in order to test the drives
  - **DISKCMP**
  - **PARTCMP**
  - **ADJCMP**
  - **SECCMP**
  - **PARTAB**
  - **BADDISK**
  - **BADX13**

78

Testing Methodology

- Setup
  - **Initialize a source disk to a known value**
  - **Hash the source disk and save the value**
  - **Initialize a destination disk**
  - **If the test requires a partition on the destination, create and format a partition on the destination disk**
  - **If the test uses an image file, partition and format a media disk.**

Methodology cont'd

- Execution of the tool
  - **If the test requires a disk I/O error, setup disk error simulation**
  - **If the test requires an image file, use the tool to create an image file of the source on the media disk**
  - **If the test requires a corrupted image file, corrupt the image file.**
  - **Use the disk imaging tool to create destination disk**
    - **From source disk directly**

      or
    - **By restoring an image file of the source**

Methodology cont'd

- Evaluation
  - **Compare the source to the destination**
    - **See what bits match**
  - **Compute a hash of the source media to verify it was unchanged**

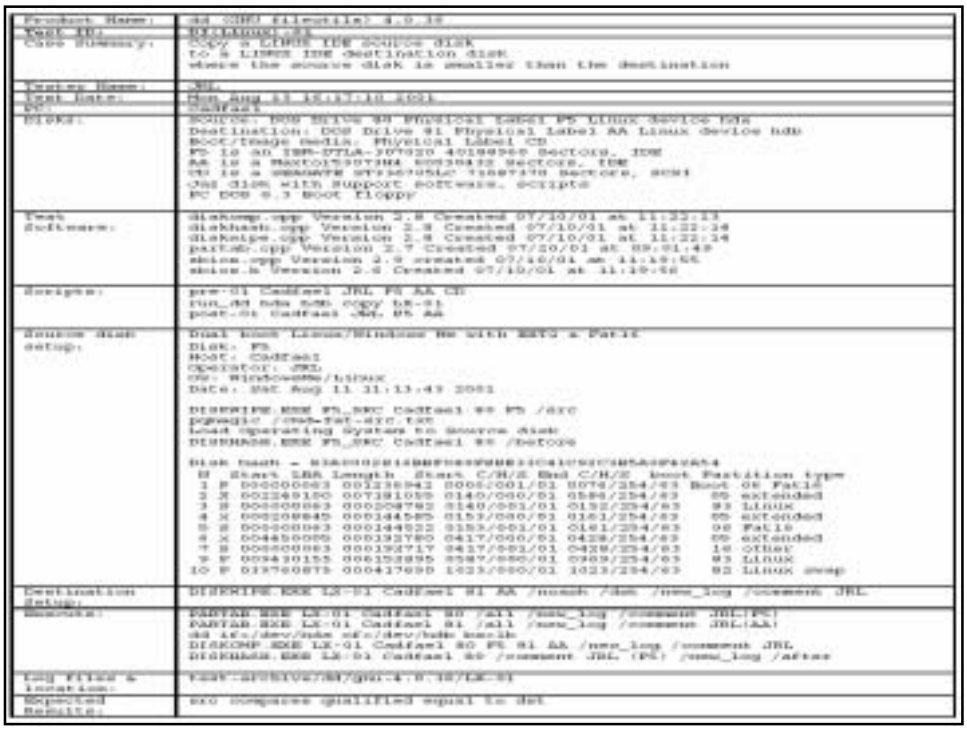
Testing Results Report Key

Heading	Description	Example
Product Name:	Name and version of software tested	[illegible]
Test ID:	Test case ID from Disk Imaging Tool Specification, version 3.1.6	[illegible]
Case Summary:	Test case summary from Disk Imaging Tool Specification, version 3.1.6	Copy a [illegible] source disk to a [illegible] destination disk where the source disk is smaller than the destination
Tester Name:	Name or initials of person executing test procedure	[illegible]
Test Date:	Time and date that test was started	[illegible]
PC:	Name of computer where tool under test was executed	[illegible]
Disks:	Description of the hard and removable disks used in the test as the source, destination, and boot/media including the identifiers used by the operating system. For parts of the test procedure that are executed under DOS, the BIOS assigned drive number is in hexadecimal. The physical device label and Linux device name are also included.	[illegible]
Test Software:	List of the support software with versions that was used for testing	[illegible]
Scripts:	Listing of the pre-test, tool execution, and post-test scripts used for the tests. The format of the pre-test script is: ID computer person source destination boot/media The format for the tool execution script is: [illegible] The format for the post-test is: ID computer person source destination	[illegible]
Source disk setup:	Documentation of the creation of the source disk including the disk label, the computer used for setup, person creating the source, time and date, partitions and operating systems installed, diskwipe command, disk hash after created and the partition table for the source disk	[illegible]

		N Start LBA Length Start C/H/S End C/H/S boot Partition type 1 P [illegible] Boot 06 Fat16 2 X [illegible] 0F extended 3 S [illegible] 83 Linux 4 x [illegible] 05 extended 5 S [illegible] 06 Fat16 6 x [illegible] 05 extended 7 S [illegible] 16 other 9 P [illegible] 83 Linux 10 P [illegible] 82 Linux swap
Destination setup:	Documentation of the creation of the destination disk including the diskwipe command and a listing of the partition table if required for the test.	[illegible] LX-01 CadFael 81 AA /noask /dst /new_log /comment JRL
Execute:	Documentation of each command executed during the test	PARTAB.EXE LX-01 CadFael 80 /all /new_log /comment JRL(F5) PARTAB.EXE LX-01 CadFael 81 /all /new_log /comment JRL(AA) dd if=/dev/hda of=/dev/hdb bs=1b DISKCMP.EXE LX-01 CadFael 80 F5 81 AA /new_log /comment JRL DISKHASH.EXE LX-01 CadFael 80 /comment JRL (F5) /new_log /after
Log files & Location:	Name and location of the log files in the test file archive	test-archive/[illegible]/LX-01
Expected Results:	Expected results listed in Disk Imaging Tool Specification, Version [illegible]	src compares qualified equal to dst Source disk unchanged
Actual Results:	Summary of test case results	src compares qualified equal to dst Source disk is unchanged
Log File Highlights:	Selected entries from three of the test case log files, the comparison of source and destination, the hash of the source after test, and any relevant messages logged during the test run.	Sectors compared [illegible] Sectors differ 0 Diffs range Source ([illegible]) has [illegible] fewer sectors than destination ([illegible]) Zero fill: 0 Src Byte fill (F5): 0 Dst Byte fill (AA): [illegible] Other fill: 0 Other no fill: 0 Hash after test: [illegible]
Analysis:	Whether the expected results were achieved	Expected results achieved

Interpretation of Test Results

- Three main items of interest for examining the results for a test case
  - **Is the source disk unchanged?**
  - **Have the correct number of sectors been copied accurately?**
  - **Has the tool alerted the user to a destination smaller than the source?**



	Source disk unchanged
Actual Results:	src compares qualified equal to dst Source disk is unchanged
Log File Highlights:	Sectors Compared 40188960 Sectors Differ 0 Diffs range Source (40188960) has 19841472 fewer sectors than destination (60030432) Zero fill: 0 Src Byte fill (F5): 0 Dst Byte fill (AA): 19841472 Other fill: 0 Other no fill: 0 Hash after test: 83A0002816BBF089F8BE33C41C92C3B5A0F42A54
Analysis:	Expected results achieved

87

Conclusions

- dd Consistently produced the expected results
- However, everything was not tested
- Tools do not have to have all features to pass

- Any questions?

88

Partial Results from Prototype Testing Efforts for Disk Imaging Tools: SafeBack 2.0

Group 4 Members:

Doug Houghton
Jason Richard

89

Tool Tested

Tool Tested: SafeBack
Version: 2.0 (January 31, 2000)
Operating System: PC DOS 6.30
Supplier: New Technologies, Inc.
(SafeBack formerly owned by Sydex, Incorporated)
Address: 2075 NE Division Street
Gresham, OR 97030
Phone: 503-661-6912
Web: *http://www.forensics-intl.com*

90

Key Issues

- **The tool shall not alter the original disk.**
  - **Passed using SHA-1 hash codes**
- **The tool shall make a bit-stream duplicate or an image of an original disk or partition.**
  - **Most cases accurate bit stream**
  - **Legacy BIOS or SCSI Disks with ASPI Drivers caused a number of errors**

91

Key Issues Cont'd

- **The tool shall log I/O errors.**
  - **Read, write and corrupt errors properly flagged and logged**
  - **This area not fully tested**
- **The tool's documentation shall be correct.**
  - **Only partial documentation available**

92

Major Anomalies (1 of 4)
Zero Fill Anomaly

If an entire physical disk is duplicated on a larger physical disk, SafeBack allows the specification of either filling the remainder of the destination with zeros or leaving the destination as is. In two test cases, SafeBack performed some zero filling when the requested option was to leave the remainder of the disk as is.

93

Major Anomalies (2 of 4)
Cylinder Adjustment Anomaly

If SafeBack is used to copy a physical disk to another physical disk of a different geometry, SafeBack optionally can reposition partitions to disk cylinder boundaries. The partition repositioning changes the contents of the first sector of each partition as documented but also repositions the last sector of the source partition to the last position of the destination partition.

94

Major Anomalies (3 of 4)
BIOS Anomaly

If a disk is being accessed by the BIOS, and the physical source disk contains more than 1,024 cylinders, and the BIOS presents an adjusted (logical) disk geometry with fewer than 1,024 cylinders by increasing the heads per cylinder value, then the tool accesses one more logical cylinder beyond the last disk cylinder indicated by the BIOS.

95

Major Anomalies (4 of 4)
Checksum Verify Message

A direct SCSI disk copy, using the ASPI driver for the SCSI adapter, copied only 2,097,270 sectors from a source disk with 17,921,835 sectors to an equal-size disk, leaving 15,824,565 sectors of the destination disk unchanged. SafeBack gave no indication of any problems and indicated a successful copy.

96

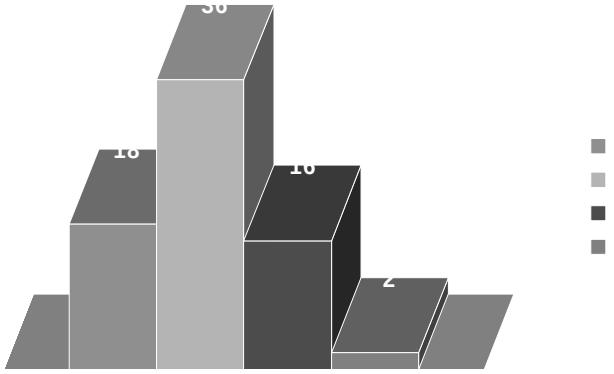
Report Information

- Detailed testing environment
  - **A number of machines of various setups & configurations**
  - **A large number of disks of various types**

Label	Model	Use	Cyl	Hd	Sec	Total Sectors	MB
D1	Quantum Sirocco 1700A	DOS source	826	64	63	3,330,432	1,705
D2	Quantum Sirocco 1700A	Destination	826	64	63	3,330,432	1,705
D3	Fujitsu MPE3064AT	Dest or image media	787	255	63	12,643,155	6,473
D4	Quantum Sirocco 1700A	Linux source	826	64	63	3,330,432	1,705
D5	Seagate	Destination	619	64	63	2,495,808	1,277
D7	Quantum Sirocco 1700A	Destination	826	64	63	3,330,432	1,705
D9	Quantum Sirocco 1700A	SmWinNT src	826	64	63	3,330,432	1,705
D11	Fujitsu MPE3064AT	Dest or image media	787	255	63	12,643,155	6,473
F1	Quantum Sirocco 1700A	Win 95 src	826	64	63	3,330,432	1,705
F2	Quantum Sirocco 1700A	Win 98 src	826	64	63	3,330,432	1,705
B0	Fujitsu MPF3153AT	Destination	16,383	16	63	30,023,280	1,537
B1	Fujitsu MPF3153AT	W2000 lrg NTFS src	16,383	16	63	30,023,280	1,537
C0	Seagate ST39204	No OS, source	SCSI			17,921,835	9,176
C1	Seagate ST39204	Destination	SCSI			17,921,835	9,176

97

Individual Test Assertions



98

Tests by Assertions

#	Assertion	Pass	Fail	Reason
1	If a duplicate copy is created directly from a source disk of the same geometry, then the disks must compare equal.	7	0	
2	If a duplicate copy is created directly from a source disk of a smaller geometry and cylinder adjustment is enabled, then the disks must compare adjusted equal.	0	2	Zero fill done but not requested. Cylinder adjustment and BIOS anomalies
3	If a duplicate copy is created directly from a source disk of a smaller geometry and cylinder adjustment is not enabled, then the disks must compare equal.	0	2	Zero fill done but not requested. BIOS anomaly

99

#	Assertion	Pass	Fail	Reason
4	If a duplicate copy is created directly from a source disk of smaller geometry, then the contents of the destination disk sectors not corresponding to source disk sectors must be as specified by the tool (if the tool allows such a specification). Otherwise each bit of such sectors must be set to zero.	0	4	Zero fill done but not requested. Cylinder adjustment and BIOS anomalies.
5	If a duplicate copy is created directly from a source disk with the destination disk having a smaller geometry, then the tool must notify the user.	1	0	
6	If a duplicate copy is created directly from a source disk with the destination disk having a smaller geometry, then every sector of the destination disk must compare equal to the corresponding sector on the source disk.	1	0	

100

#	Assertion	Pass	Fail	Reason
7	If a duplicate destination disk is created from an image file of a source disk with the same geometry, then the disks must compare equal.	5	0	
8	If a duplicate destination disk is created from an image file of a source disk with a smaller geometry and cylinder adjustment is enabled, then the disks must compare adjusted equal.	0	2	Zero fill done but not requested. Cylinder adjustment and BIOS anomalies
9	If a duplicate destination disk is created from an image file of a source disk with a smaller geometry and cylinder adjustment is not enabled, then the disks must compare equal.	0	2	Zero fill done but not requested. BIOS anomaly

101

#	Assertion	Pass	Fail	Reason
10	If a duplicate destination disk is created from an image file of a source disk with a smaller geometry, then the contents of the destination disk sectors not corresponding to source disk sectors must be as specified by the tool (if the tool allows such a specification). Otherwise each bit of such sectors must be set to zero.	0	4	Zero fill done but not requested. Cylinder adjustment and BIOS anomalies
11	If a duplicate destination disk is created from an image file of a source disk with a larger geometry, then the tool must notify the user.	0	1	Checksum verify message missing
12	If a duplicate destination disk is created from an image file of a source disk with a larger geometry, then every sector of the destination disk must compare equal to the corresponding sector on the source disk.	0	1	Checksum verify message missing

102

#	Assertion	Pass	Fail	Reason
13	If a duplicate destination partition is created directly from a source partition of the same size, then each sector of the source partition must compare equal to the logical block address (LBA) corresponding sector of the destination partition.	1	0	
14	If a duplicate destination partition is created directly from a smaller source partition, then each sector of the source partition must compare equal to the LBA corresponding sector of the destination partition.	2	0	
15	If a duplicate destination partition is created directly from a smaller source partition, then each sector of the destination partition with no LBA corresponding sector in the source partition must be as specified by the tool (if the tool allows such a specification). Otherwise each bit of each sector must be set to zero.	2	0	

103

#	Assertion	Pass	Fail	Reason
16	If a duplicate destination partition is created directly from a larger source partition, then each sector of the destination partition must compare equal to the LBA corresponding sector of the source partition.	2	0	
17	If a duplicate destination partition is created directly from a larger source partition, then the tool must notify the user.	2	0	
18	If a duplicate destination partition is created from an image file of a source partition of the same size, then each sector of the source partition must compare equal to the LBA corresponding sector of the destination partition.	1	0	

#	Assertion	Pass	Fail	Reason
19	If a duplicate destination partition is created from an image file of a smaller source partition, then each sector of the source partition must compare equal to the LBA corresponding sector of the destination partition.	2	0	
20	If a duplicate destination partition is created from an image file of a smaller source partition, then each sector of the destination partition with no LBA corresponding sector in the source partition must be as specified by the tool (if the tool allows such a specification). Otherwise each bit of each sector must be set to zero.	2	0	
21	If a duplicate destination partition is created from an image file of a larger source partition, then each sector of the destination partition must compare equal to the LBA corresponding sector of the source partition.	0	2	Checksum verify message missing

104

#	Assertion	Pass	Fail	Reason 105
22	If a duplicate destination partition is created from an image file of a larger source partition, then the tool must notify the user.	0	2	Checksum verify message missing
23	If the tool encounters any read errors while reading from the source, then the tool must detect and identify the error and notify the user.	3	2	Zero fill done but not requested. BIOS anomaly
24	If the tool encounters any read errors while reading from an image file, then the tool must detect and identify the error and notify the user.	1	0	
25	If the tool encounters any write errors while creating an image file, then the tool must detect and identify the error and notify the user.	1	0	

#	Assertion	Pass	Fail	Reason 106
26	If the tool encounters any write errors while writing to the destination, then the tool must detect and identify the error and notify the user.	1	2	Cylinder adjustment and BIOS anomalies
27	If the tool is able to create a destination from an image file that contains read errors, the destination sectors corresponding to the unreadable data must be treated as fill sectors (the tool may allow a specified action or may fill the sectors with zeros).	6	2	Zero fill done but not requested. BIOS anomaly
28	The source before using the tool must be equal to the source after tool use.	All	None	
29	The results of any remote tool use must be equal to the results of local identical tool use.	4	3	Zero fill done but not requested. BIOS anomaly Checksum verify message missing

#	Assertion	Pass	Fail	Reason 107
30	If deleted files exist that are recoverable on the source, then these files must be recoverable on the destination.	1	0	
31	If the logical disk as presented by the BIOS is smaller than the physical disk, then the tool must not access any sectors outside the logical disk.	0	1	BIOS anomaly
32	If the tool has a feature to verify the integrity of the image file, the tool shall detect and identify the anomaly and notify the user if the image file has been changed.	4	0	
33	If a duplicate copy is created directly, without using the BIOS, from a source disk of the same geometry, then the disks must compare equal.	2	0	

108

#	Assertion	Pass	Fail	Reason
34	If a duplicate copy is created directly, without using the BIOS, from a source disk of a smaller geometry and cylinder adjustment is enabled, then the disks must compare adjusted equal.	None	None	
35	If a duplicate copy is created directly, without using the BIOS, from a source disk with the destination disk having a smaller geometry, then the tool must notify the user.	1	0	

109

Test Results for Disk Imaging Tools: SafeBack 2.18

Group 5 Members:

Joel Cardo
Matthew Regennitter
Zhen Yu

110

Outline

- Introduction
- Results Summary by Requirements
- Anomalies
- Test Case Selection
- Test Results by Assertion
- Testing Environment
- Interpretation of Test Results

111

Introduction

- Tool: SafeBack 2.18
- OS: PC-DOS 6.3 & Win98 DOS
- Supplier: New Technologies, Inc.
- Newest: Version 3.03
  - **Fixes the problems in Version 2.0**
  - **More powerful hash: SHA256 *vs* SHA-1(160 bits)**

112

Results Summary by Requirements

- Shall make a bit-stream or an image copy
  - **Almost OK with two exceptions**
    - **For FAT32 partition type, two file system control values are adjusted as a side effect of copy.**
    - **Using BIOS access interface on IDE hard drives in computers using a legacy BIOS, some sectors are not accessed correctly; OK when using direct access through ATA interface**

Results Summary by Requirements

- ✓ Shall not alter the original disk
- ✓ Shall verify the integrity of image file
- ✓ Shall log I/O errors
- ◆ Documentation shall be correct
  - **Some behavior was not documented correctly**
  - **Manual only for Version 2.0 (October 2001)**

Anomalies

1. Sectors missed in legacy BIOS access (9/112)
   - **A legacy BIOS may underreport the number of cylinders on a IDE hard drive.**
     - **Legacy BIOS does not implement extensions of INT13h**
     - **Small area of sectors at end of drive not accessed**
   - **An extended BIOS implements the extension of INT13h according to ANSI INCITS 347-2001.**

Table 2-2. Example of Direct ATA versus BIOS Hard Drive Geometry

Access	Cylinders	Heads	Sectors per Head	Sectors per Cylinder	Total Sectors
Direct	3,309	16	63	1,008	3,335,472
BIOS	826	64	63	4,032	3,330,432

Anomalies

2. Backfill not as expected (31/112)

If enabled writes binary 00 to unused space

Disk copy **and** restore **operations to a larger destination were zero backfilled even when option was not enabled.**

Occurred in correlation to adjust partitions option

There was no zero backfilling of partition operations as specified by documentation.

Anomalies

3. Cylinder alignment anomaly (4/112)

Add sectors to the end of partition so that each destination partition uses up all the sectors of the last cylinder.

Test Case: copy 4 boot tracks, 6 partitions and 5 unallocated regions with cylinder alignment

Table 2-3. Test Case DI-003 Comparison Summary

Boot tracks	4	252 diffs	4		
Partitions	6	2,241,540 diffs	9		
Unallocated	5	1,093,680 diffs	1,009		
Total src sectors		3,335,472			
Partition excess		76,671 zero	74,189 non-zero		2,482
Disk excess		9,260,307 zero	10,363 non-zero		9,249,944
Total dst sectors		12,672,450			

Anomalies

3. Cylinder alignment anomaly (Cont.)

Behavior of Cylinder Alignment

Partition table adjustments are expected.

Except for BIOS anomaly, all sectors not requiring partition table adjustments are copied correctly.

The last sector of a FAT source partition is relocated to the last excess destination sector.

The zero backfill results are unclear.

Test Cases: DI-003, DI-004, DI-046, and DI-047.

Anomalies

4. Sector change in FAT32 operation (19/112)

In FAT32 operations, sector 1 (FSInfo **sector) differs in 4 to 8 bytes from sector 1 of source.**

Contains control information about file system

FSI_Free_Count**, containing the last know free cluster count, is set 0xFFFFFFFF (unknown).**

FSI_Next_Free**, where to start looking for free cluster, is also adjusted.**

119

Test Case Selection

112/168 test cases in *Disk Imaging Tool Specification* were selected.

SafeBack doesn't support partition operations on NTFS or Linux ext2 partitions

Some cases are going to be deleted

Some cases require support software that are not available

120

Test Results by Assertion (Mandatory)

- AM-1: The source should not be altered.

  OK by comparing hash code before & after

- AM-2: If no errors while reading or writing, a bit stream duplicate will be created on destination

  2 BIOS anomalies & 9 FAT32 anomalies

121

Test Results by Assertion (Mandatory)

- AM-3: With errors reading or writing, a qualified bit stream duplicate should be created

  6 BIOS anomalies & 9 FAT32 anomalies

- AM-4: Any errors while reading or writing should be logged
- AM-5: If IDE/SCSI drive involved and image or bit stream duplicate is created, the interface is determined to be well defined.

122

Test Results by Assertion (Mandatory)

- AM-6: Documentation should be correct.

  Some behavior was not well documented or was ambiguous.

- AM-7: If the destination drive is larger than the source, the excess area should be set as specified.

  2 BIOS anomalies & many backfill anomalies

123

Test Results by Assertion (Mandatory)

- AM-8: If the destination is smaller, the duplicate is qualified by omitted portion of the bit-stream

  User should be notified by SafeBack.

124

Test Results by Assertion (Optional)

- AO-1: Before duplication the hash of one or more blocks of the source must be equal to the hash of the same blocks of the duplicated created if no read or write errors occur.
- AO-2: If more than one partition exists, the tool should produce any user-selected partition on the destination.

  NTFS and Linux ext2 are not supported.

  A lot of FAT32 anomalies exist.

125

Test Results by Assertion (Optional)

- AO-3 to AO-11: No anomaly, omitted
- AO-12 to AO-14: Contain anomalies, omitted

126

Models Tested

Forty hard drives were tested:

•11 models in 6 different brands
Western Digital, Quantum, Maxtor, Fujitsu, Seagate,IBM

•Range of memory capacities
1.62 – 37.60 GB

Additionally, there were 3 important system configurations of interest:

•Extended BIOS

•Legacy BIOS

•Special SCSI

127

Setting up the system

There are always 2 hard disks in each test:

•Source and destination

•May be a third image disk for certain tests

Booting up:

A runtime environment is created by using a DOS boot floppy. The floppy also has the necessary control scripts and log files.

If the hard drive is to have FAT32 partitions, then the machine is booted with a WIN98 boot disk; otherwise a DOS 6.3 disk is used.

128

Other Software

CD-ROM Drive
Holds Safeback program, support software, and utilities

Support Software
- Handles setup of test data
- Measures the test results
- Controls the testing process

Choosing Pairs
Source drive chosen based on interface, partition type; then the corresponding destination drive was chosen based on interface and relative size of source drive.

129

Testing Environment

- Support software: (from FS-TST testing suite, NIST)

  DISKWIPE: **initialization to a known value**

  DISKCMP, PARTCMP, ADJCMP & SECCMP: **comparison of source to destination**

  DISKHASH & SECAHSH: **detection of changes**

  CORRUPT: **corruption of an image file**

  BADDISK & BADX13: **simulation of a faulty disk**

130

Testing Environment

- Testing steps:

  Setup: **Initialize source to a known value, hash disk, initialize destination or media to a known value, and format if necessary.**

  Execution: **Create an error simulation, an image file, or corrupted image file, and move to the destination drive.**

  Measurement: **Hash the destination drive, check for extra sectors or logged errors.**

Interpretation of Test Results

- Examines:
  - **Any changes on source disk?**
  - **Sectors copied correctly?**
  - **Alerts user if destination is smaller.**
  - **Excess sectors handled as specified?**
  - **Detects any changes to an image file?**
  - **Alerts user to any I/O errors?**

Interpretation of Test Results

Case DI-007 for SafeRack 2.10	
Case Summary:	Copy a BIOS-IDE source disk to a BIOS-IDE destination disk where the source disk is the same size as the destination
Tester Name:	JRL
Test Date:	Thu Oct 18 13:45:57 2001
PC:	Beta3
Disks:	Source: DOS Drive 80 Physical Label A1 Destination: DOS Drive 81 Physical Label D7 Image media: DOS Drive 82 Physical Label none A1 is a Quantum Sirocco1700A with 3335472 sectors D7 is a Quantum Sirocco1700A with 3335472 sectors Jaz disk with partition magic and scripts FS-TST Release 1.0 CD-ROM + haddisk Version 3.2
Source disk setup:	Linux EXT2 & DOS Fat16 Disk: A1 Host: JudgeDee Operator: JRL OS: Windows/Me Options: Typical Date: Tue Oct 16 11:24:16 2001 cmd: Z:\as\DISKWIPE.EXE A1 JudgeDee 80 A1 /src /new_log X:\pm\pqmagic /cmd=X:\pm\nex-src.txt Load Operating System to Source disk cmd: Z:\as\DISKHASH.EXE A1 JudgeDee 80 /before /new_log Disk hash = D0FC573FFT74FG897BE520153C98F770E990429F

Interpretation of Test Results

Destination Setup:	Z:\ss\DISKWIPE.EXE DI-007 Beta3 81 D7 /noask /dst /new_log /comment JRL No partition table defined
Error Setup:	none
Execute:	Z:\ss\PARTAB.EXE DI-007 Beta3 80 /all /new_log /comment JRL(A1) z:\sb\master (copy) Z:\ss\DISKCMP.EXE DI-007 Beta3 80 A1 81 D7 /new_log /comment JRL Z:\ss\DISKHASH.EXE DI-007 beta3 80 /comment JRL(A1) /new_log /after
Log files loc:	test-archive/sb/sb-2.18/DI-007
Log File Highlights:	Safeback log: DI-007/SB_007C.TXT SafeBack 2.18 13Feb01 execution started on Oct 18, 2001 14:08. 14:08:46 Menu selections: Function: Copy Direct access: No Use XBIOS: No Adjust partitions: No Backfill on restore: No 14:08:59 Copy from Local drive 0: to local drive 1: 14:09:04 Copy of Local drive 0: to drive 1: begun on Oct 18, 2001 14:09 14:09:04 Local SafeBack is running on DOS 6.30

Interpretation of Test Results

	14:09:04 Partition table for drive 0: Source drive 0: Capacity.....1629 MB Cylinders.....827 Heads.....64 Destination drive 1: Capacity.....1629 MB Cylinders.....827 Heads.....64 14:17:54 Copy of drive 0: to drive 1: completed on Oct 18, 2001 14:17 SafeBack execution ended on Oct 18, 2001 14:18. * * * * Measurement Logs * * * * Sectors Compared 3335472 Sectors Differ 1008 Diffs range 3334464-3335471 Hash after test: D0FC573FF774F697BE520153C9BF770E998428F
Expected Results:	Source disk is unchanged src compares equal to dst
Actual Results:	BIOS anomaly
Analysis:	Expected results not achieved

Overview of test results

Out of about 112 tests performed with Safeback:

- 9 exhibited the Legacy BIOS missed sectors anomaly
- 31 exhibited the unexpected backfill anomaly
- 4 exhibited the cylinder alignment anomaly
- 19 exhibited the FAT32 sector change anomaly

Disk Imaging Tool Specification & FS-TST: Forensic Software Testing Support Tools

Group 6 Members:

Brett Myers
Rob Shanley

137

Introduction

- Computer Forensics Tool Verification Project at NIST
- Tests to insure reliability of forensics tools used in investigations

138

Purpose and Scope

- Purpose:
  - **Define disk imaging tools' requirements**
    - **Requirements used to derive assertions that will be tested**
  - **Define test methods**
- Scope:
  - **Software tools that copy or image hard disk drives** (no floppy, zip, analog, cell phone, or pager media)

139

Glossary

- Bit-stream duplicate
  - **Bit-for-bit digital copy of an object**
- Disk compares equal
  - **No differences between original and duplicate**
  - **Result of bit-stream duplicate**

140

Glossary (cont.)

- Qualified bit-stream duplicate
  - **Duplicate, except in areas documented by the tool**
  - **Tool Adds: partition table, boot records, or excess disk space values in deplicate if necessary**
- Disk compares qualified equal
  - **Only differences are document by the tool**
  - **Result of bit-stream duplicate**

141

Requirements

- The tool shall…
  - **Make a bit-stream duplicate or an image of an original disk or partition**
  - **Not alter the original disk**
  - **Be able to verify the integrity of a disk image file**
  - **Log I/O errors**
- The tool's documentation shall be correct

*These requirements proved to be too ambiguous and more specific requirements were developed

142

Mandatory Requirements

- Basically, same as earlier with more specifics
  - **No errors = duplicate**
  - **Errors = qualified duplicate and logging**
  - **Must have 1 or more well-defined interface**
  - **If documentation followed expected result produced**
  - **Source < destination: document excess space**
  - **Source > destination: notify, truncate, and log**

*All disk imaging tools must meet these requirements

143

Optional Requirements

- If present, will be tested as a mandatory requirement
- If not provided, the requirement does not apply
- Examples
  - **Compute a hash value of the original and duplicate**
  - **Compute hash values "block-by-block"**
  - **Extensive logging of the duplication process**
  - **Etc.**

144

Assertions

- Each provides conditions that can be tested and the result expected
- Both mandatory and optional assertions
- Example:
  - **Requirement – The tool shall not alter the original**
  - **Assertion – If a source is accessed by the tool, then the source will not be altered**

*Abstract test cases are used to test the assertions

145

Test Parameters

- Tool action
  - **Create a copy or image, or verify an image**
- Firmware interface
- Subject entity
  - **Entire disk or partition**
- Relative disk sizes
- Destination Media
  - **Fixed or removable**
- I/O errors

146

Test Cases

- Format
  - **Test ID**
  - **Description**
  - **Expected Results**
- Non-Linux cases = 168
- Linux cases = 52

147

FS –TST

Forensic Software Testing Support Tools

- Aid in testing disk imaging tool testing
- Use the interrupt 13h BIOS disk interface
  - **Initialize disk drives**
  - **Detect disk content changes**
  - **Compare pairs of disks**
  - **Simulate bad sectors on a disk**
- Runs in DOS 6.3 environment
  - **Set up the drives, measure the results, aid in documenting results**
- Written in C++

148

Support Tools

DISKWIPE

diskwipe test-case host drive fill [/opts]

- Sets up the known unique content for each sector and then writes the content for the given track to the disk

BADDISK

baddisk drive cyl head sec command error_code > log_file

- Simulate a faulty hard disk accessed by the legacy interrupt 13 BIOS by returning an error code for specified address

149

Support Tools (cont.)

CORRUPT

corrupt test-case host image-file index value [/opts]

- Used to change a single byte of an image file.

ADJCMP

adjcmp case host src-drv src-fill dst-drv dst-fill [/opts]

- Used to compare two disks where the partitions copied to the destination are adjusted so that the copy is aligned on a cylinder boundary

150

Support Tools (cont.)

DISKCMP

diskcmp case host src-drv src-fill dst-drv dst-fill [/opts]

- Used to evaluate the accuracy of a disk duplication operation.

PARTCMP

partcmp case host src-drv src-fill dst-drv dst-fill [/opts]

- Used to evaluate the accuracy of a partition duplication operation.

151

Support Tools (cont.)

DISKHASH

diskhash case host drive [/opts]

- For a designated hard drive, the diskhash program computes a SHA-1 hash on a specified hard drive.

SECHASH

sechash case host drive [/opts]

- For a designated hard drive, the sechash program computes a SHA-1 on a block of contiguous sectors from the specified hard drive.

152

Support Tools (cont.)

LOGCASE

logcase test-case host operator src dst media

- Used to create a log file recording basic information about the test case. (Case ID, host, operator, source disk drive, destination drive, other drive, date and time)

LOGSETUP

logsetup disk host operator OS

- Used to create a log file recording basic information about the test case. (disk label, host, operator, OS loaded, date and time)

153

Support Tools (cont.)

PARTAB

partab case host drive [/opts]

- Used to print the partition table for a hard drive
- **DISKCHG**

diskchg test-case host drive [/opts]

- Used to setup hard disk drives for the testing and other support programs. Can set a single byte to a given value, can set a sector to all zeros or diskwipe style fill. Can also be used to examine the contents of a sector.

154

Support Tools (cont.)

SECCMP

seccmp case host src-drv src-fill dst-drv dst-fill [/opts]

- Used to compare two disk sectors.

SECCOPY

seccopy test-case host src_drive src_addr dst_drive dst_addr dst_length [/opts]

- Used to copy blocks of sectors from one hard drive to another. Used to setup drives for the testing of the other support programs

Thanks to all of you!!!

See you next time.