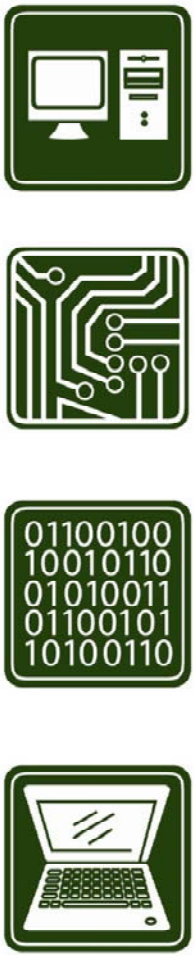
[MISDE]



October | 2006

Independent Validation and Verification (IV&V) of EnCase Forensic Edition Law Enforcement and Government Edition Version 5 (update v.5.05d)

MARSHALL
INFORMATION SECURITY
& DIGITAL EVIDENCE

MISDE

Marshall University
Forensic Science Center
1401 Forensic Science Dr.
Huntington, WV 25701
Phone: 304/690-4363
Fax: 304/690-4360

http://forensics.marshall.edu/MISDE

Disclaimer of Liability:

With respect to this document, neither the Marshall University Forensic Science Center nor any of its employees, makes any warranty, express or implied, including the warranty of fitness for a particular purpose, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed. Any mention of commercial products within the following documents is intended for information purposes only and is not intended to be used as a substitute and/or replacement for an external laboratory's own test validation. It is advised to independently verify any information prior to reliance thereon.

Redistribution Policy:

MISDE grants permission for the redistribution and use of the following posted document created by MISDE, provided that the following conditions are met.

1) Redistributions of documents, or parts of the documents, must retain the MUFSC/MISDE cover and disclaimer of liability page.
2) Neither the name of the Marshall University Forensic Science Center nor the Information Security and Digital Evidence Laboratory (MISDE) may be used to endorse or promote products derived from the following document.
3) Any reference or quote obtained from the following MISDE document must be properly annotated in the document that the reference is contained therein.

MARSHALL UNIVERSITY
FORENSIC SCIENCE CENTER
MISDE Laboratory
Official Document

1401 Forensic Science Drive
Huntington, WV, 25701
Telephone: 304-690-4363
Fax: 304-690-4360
http://forensics.marshall.edu

TEST PLAN

Test Number: EnCase5-IV&V-505d

Test Title: Independent Validation and Verification (IV&V) of EnCase Forensic Edition Law Enforcement and Government Edition Version 5 (update v.5.05d)

Test Date: 8/3/2006

Purpose and Scope:

Guidance Software's EnCase® Forensic Edition version 5 is a data forensic program that runs on both Windows and MS-DOS platforms. EnCase Forensic is recognized as a leading standard for computer forensic software and provides law enforcement, government, and corporate investigators with reliable, court-validated technology.

This test plan will test the ability of EnCase Forensic Edition Version 5 (update 5.05d) to allow normal hashing, imaging, restoring, and wiping functionality to occur using validated test media. This test plan will consist of four test scenarios:

- Verify EnCase Forensic v.5.05d hashing functionality
- Verify EnCase Forensic v.5.05d imaging functionality
- Verify EnCase Forensic v.5.05d restoring functionality
- Verify EnCase Forensic v.5.05d wiping functionality

Requirements:

1) EnCase Forensic Edition v5.05d should successfully compute an MD5 (message digest-5) hash calculation of the source media

2) EnCase Forensic Edition v5.05d should successfully image the source media.

3) EnCase Forensic Edition v5.05d should successfully wipe all data from the source media.

4) EnCase Forensic Edition v5.05d should successfully restore the test image to source media.

1401 Forensic Science Drive
Huntington, WV, 25701
Telephone: 304-690-4363
Fax: 304-690-4360
http://forensics.marshall.edu

Description of Methodology:

A 2.0 gigabyte (GB) zero-wiped Flash memory disk drive (see figure 1.1) will be connected via USB 2.0 to the acquisition/examination PC. EnCase v.5.05d will be launched and an MD5 calculation will be made to the wiped drive (see figure 2.1). A 244 megabyte (MB) image consisting of various known file types will be added to the source media using Microsoft® Windows Explorer (see figure 2.2). The media will then be disconnected from the USB 2.0 port and connected to the Tableau T8 Forensic USB Bridge to ensure write block sterility of the source media (see figure 1.2). The T8 unit will be powered on and device drivers will automatically be installed in Windows XP. EnCase Forensic Edition v.5.05d will be launched and an MD5 hash of the source media will be calculated (see figure 2.3). Using EnCase 5.05d, a disk image will be taken of the USB flash media and stored on the acquisition PC (see figure 2.4). Upon completion of the disk image, the Tableau T8 Bridge will be powered down and the USB source media will be connected directly to the PC USB port. The flash media will then be zero-wiped using EnCase v.5.05d (see figure 3.1). Upon completion of the wipe, the stored disk image will then be restored to the media using the restore functionality of EnCase v.5.05d (see figure 4.2). The USB media will then be disconnected from the PC USB port and coonected to the Tableau T8 USB Bridge. The bridge will then be powered on and an MD5 hash will be calculated using the hashing function of EnCase v.5.05d (see figure 4.3)

Expected Results:

1) EnCase Forensic Edition v5.05d will successfully calculate an MD5 hash value for the source media.
2) EnCase Forensic Edition v5.05d will successfully image the source media.
3) EnCase Forensic Edition v.5.05d will successfully restore the copied image source media.
4) EnCase Forensic Edition v5.05d will successfully wipe the source media.

Test Scenarios:

Test Number	Environment:	Actions:	Assigned Reqt's	Expected Results:
01-01	Source Media; Tableau T8 Forensic USB Bridge; EnCase Forensic v.5.05d	MD5 hash calculation performed on source drive	1	MD5 Hash calculation produced.
01-02	Source Media; Tableau T8 Forensic USB Bridge; EnCase Forensic v.5.05d	Image taken of IDE source drive using software	2	Successful image taken of drive
01-03	Source Media; Tableau T8 Forensic USB Bridge; EnCase Forensic v.5.05d	Image restored to IDE source drive using software	3	Image successfully restored to disk.
01-04	Source Media; Tableau T8 Forensic USB Bridge; EnCase Forensic v.5.05d	IDE drive zero-wiped using software	4	Disk successfully wiped

1401 Forensic Science Drive
Huntington, WV, 25701
Telephone: 304-690-4363
Fax: 304-690-4360
http://forensics.marshall.edu

Test Data Description:

Test PC:

Model: Optiplex GX270
Manufacturer: Dell ®
Processor: Intel® Pentium 4 @ 3.2 GHz
Memory: 1 GB DDR SDRAM
Operating System: Microsoft Windows XP Professional Edition w/ SP2
O/S Edition: 32 bit
USB interface: 1.1 (12.0 mbps)

Test Media (see figure 1.1):

Model: Attache USB Flash Disk Drive
Manufacturer: PNY®
Serial Number: 099133607020996B
Capacity: 2.00 GB
File System (formatted): FAT32

2.0 GB USB flash device Information as reported by Tableau USB Bridge Write-Blocker:

Mfg Name: No str available
Product Name: USB Flash Memory
Serial #: 099133607020996B
Firmware Rev: 5.00
USB Speed: High, 480 mbit/s
USB Class Info: C=8 S=6 P=50
Int. Node ID: 1
USB Address: 2
SCSI Class: 0

Files/Folders added (see figure 2.2):

- Audio folder
  - Marshall Buffalo Medley.mp3
  - Sons of Marshall.mp3
  - Superman Theme.wav
- Documents
  - Test Document.doc
  - Test Document.rtf
  - Test Spreadsheet.xls
  - Test Document.pdf
  - Test Document.txt
  - Test Document.ppt
- Video
  - Cowbell.wmv
  - Coachkpractice.avi
  - Thumbs.db

1401 Forensic Science Drive
Huntington, WV, 25701
Telephone: 304-690-4363
Fax: 304-690-4360
http://forensics.marshall.edu

- Pics
  - Test Image.pcx
  - Test Image.bmp (16 color)
  - Test Image.bmp (24 bit)
  - Test Image.bmp (256 color)
  - Test Image.pdf (Adobe pdf)
  - Test Image.pdp (Adobe pdp)
  - Test Image.art (AOL art file)
  - Test Image.pict (Apple pict file)
  - Test Image.pct (Apple pct file)
  - Test Image.gif
  - Test Image.ico (Icon)
  - Test Image.jpe (jpeg)
  - Test Image.jpeg
  - Test Image.jpg
  - Test Image.bmp (Monochrome bmp)
  - Test Image.eps (Photoshop EPS)
  - Test Image.pxr (Pixar)
  - Test Image.png
  - Test Image.raw
  - Test Image.icb (Targa)
  - Test Image.tga (Targa)
  - Test Image.vda (Targa)
  - Test Image.vst (Targa)
  - Test Image.tif (Big Endian)
  - Test Image.tiff (Little Endian)
  - Thumbs.db

- Livetri.zip
  - Liveupdt.grd
  - Liveupdt.sig
  - Liveupdt.tri

Table 1: Summary of Authentication hashes:

	2.0 GB flash source media (evidentiary)	**2.0 GB flash source media Disk (Imaged)**	**2.0 GB flash source media (Zero-Wiped)**	**2.0 GB flash source media (Restored)**
EnCase Forensic v.5.05d md5sum	87E70C91B449184BA856EB46C428A297	87E70C91B449184BA856EB46C428A297	67BE399430F6576556D3DD77C6DC30E1	87E70C91B449184BA856EB46C428A297
Known hashes (Verified)	87E70C91B449184BA856EB46C428A297	87E70C91B449184BA856EB46C428A297	67BE399430F6576556D3DD77C6DC30E1	87E70C91B449184BA856EB46C428A297

1401 Forensic Science Drive
Huntington, WV, 25701
Telephone: 304-690-4363
Fax: 304-690-4360
http://forensics.marshall.edu

SUMMARY REPORT

Test Number: EnCase5-IV&V-01

Test Title: Independent Validation and Verification of EnCase Forensic Edition V.5.05d

Test Date: 8/3/2006

Test Description:

This test documents the ability of Guidance Software's EnCase Forensic Edition v.5.05d to successfully perform the following functions uisng a USB-enabled flash media device:

- Hashing functionality
- Imaging functionality
- Wiping functionality
- Restoring functionality

Forensic Tool(s):

Title: EnCase Forensic Edition (Law Enforcement-Government)
Manufacturer: Guidance Software ®
Model Number: version 5.05d
Serial Number: 82932013 (Aladdin® HASP dongle ID)

Title: Forensic USB Bridge
Manufacturer: Tableau ®
Model Number: T8
Serial Number: T005c017391
Firmware #: 15:01:41

Test Results:

Test Number	Environment:	Actions:	Assigned Reqt's	Expected Results:	Results:
01-01	Source Media; Tableau T8 Forensic USB Bridge; EnCase Forensic v.5.05d	MD5 hash calculation performed on source drive	1	MD5 Hash calculation produced.	Pass
01-02	Source Media; Tableau T8 Forensic USB Bridge; EnCase Forensic v.5.05d	Image taken of IDE source drive using software	2	Successful image taken of drive	Pass
01-03	Source Media; Tableau T8 Forensic USB Bridge; EnCase Forensic v.5.05d	Image restored to IDE source drive using software	3	Image successfully restored to disk.	Pass
01-04	Source Media; Tableau T8 Forensic USB Bridge; EnCase	IDE drive zero-wiped using software	4	Disk successfully wiped	Pass

1401 Forensic Science Drive
Huntington, WV, 25701
Telephone: 304-690-4363
Fax: 304-690-4360
http://forensics.marshall.edu

	Forensic v.5.05d				

Requirements:

1) EnCase Forensic Edition v5.05d should successfully compute an MD5 hash calculation of the source media.

2) EnCase Forensic Edition v5.05d should successfully image the source media.

3) EnCase Forensic Edition v5.05d should successfully restore test image to source media.

4) EnCase Forensic Edition v5.05d should successfully wipe all data from the source media.

Observations:

N/A

Limitations:

N/A

Recommendations:

N/A

1401 Forensic Science Drive
Huntington, WV, 25701
Telephone: 304-690-4363
Fax: 304-690-4360
http://forensics.marshall.edu

Figure 1.1 2.0 GB USB flash source media

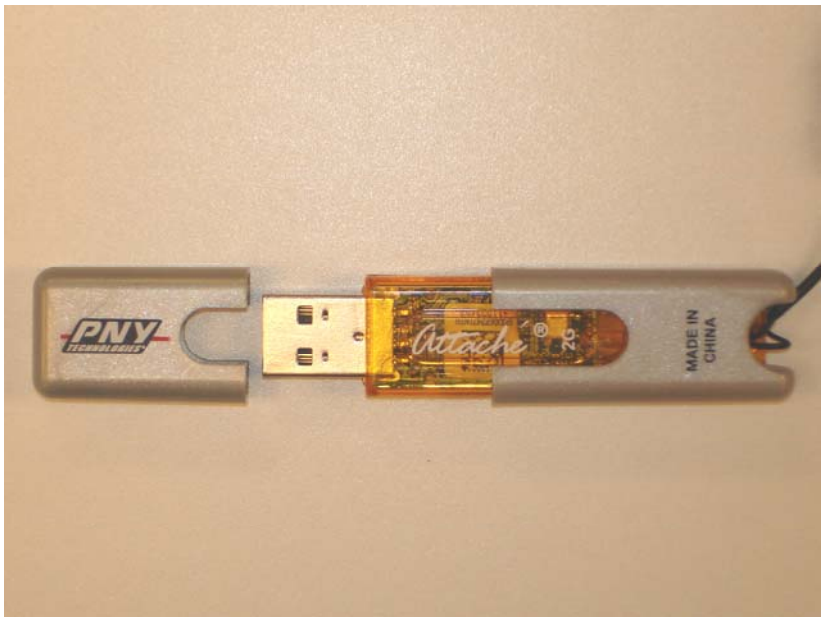


Figure 1.2 2.0 GB USB flash source media attached to Tableau T8 Forensic Bridge

1401 Forensic Science Drive
Huntington, WV, 25701
Telephone: 304-690-4363
Fax: 304-690-4360
http://forensics.marshall.edu

Figure 2.1 MD5 hash of 2.0 GB USB flash source media (no data-zero-wiped)

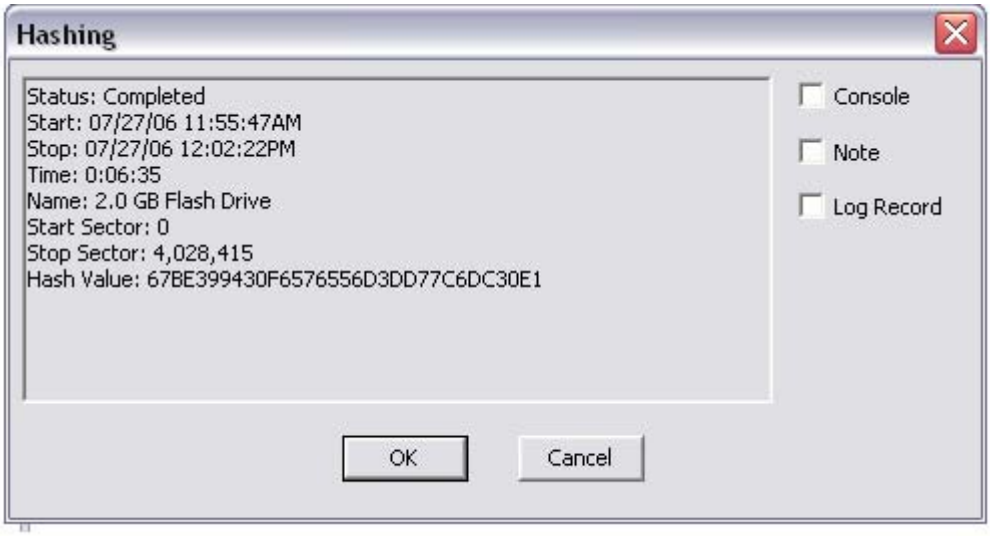
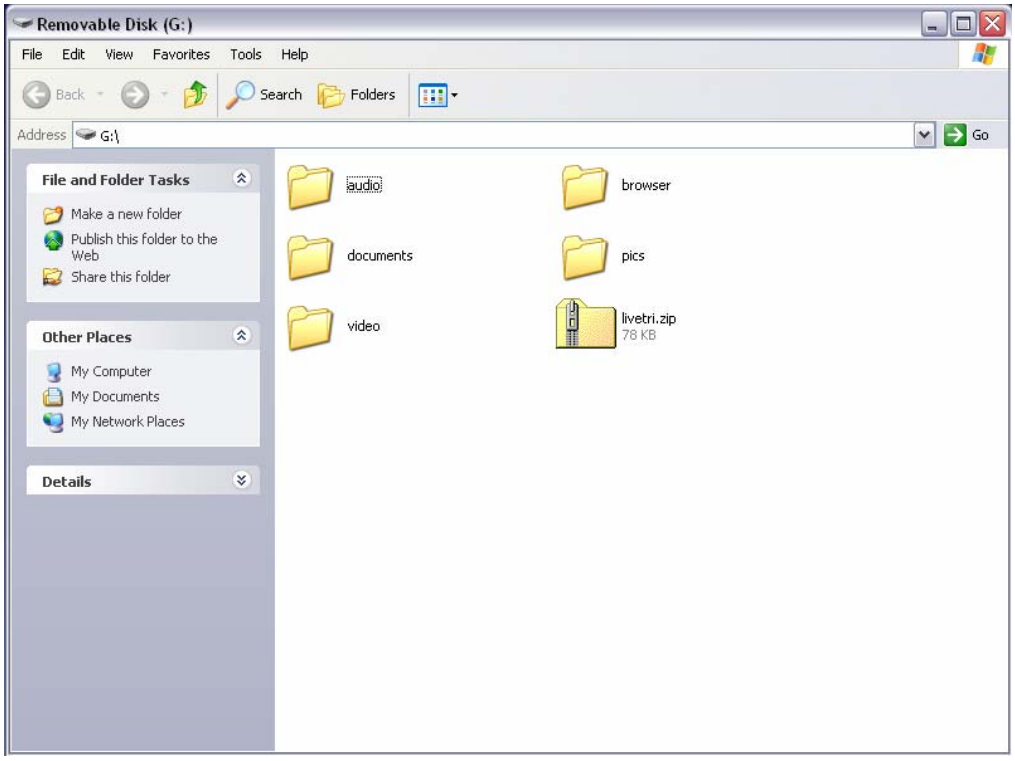


Figure 2.2 Folder structure of 2.0 GB USB flash source media (after proficiency image was added)



1401 Forensic Science Drive
Huntington, WV, 25701
Telephone: 304-690-4363
Fax: 304-690-4360
http://forensics.marshall.edu

Figure 2.3 Hash calculation of 2.0 GB USB flash media (after proficiency image added)

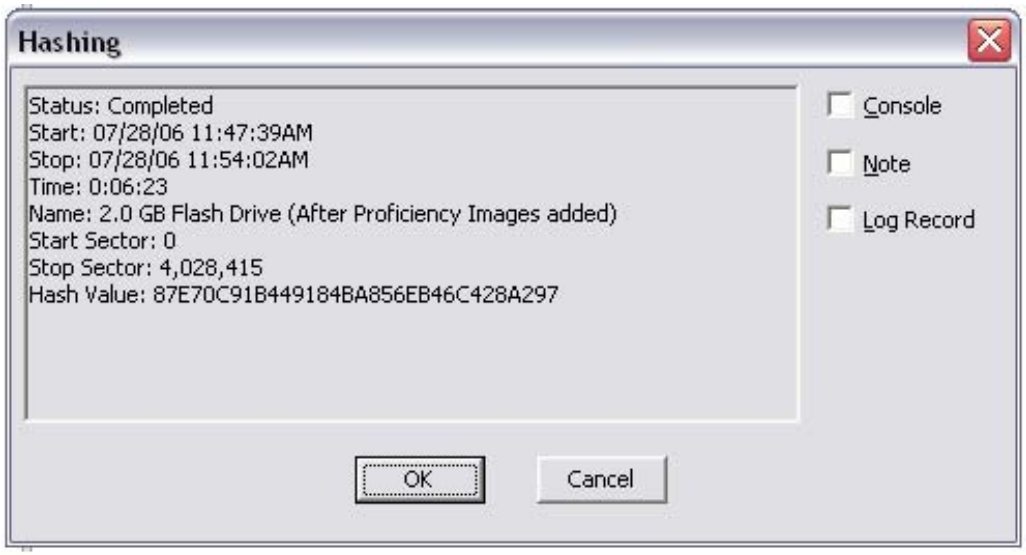
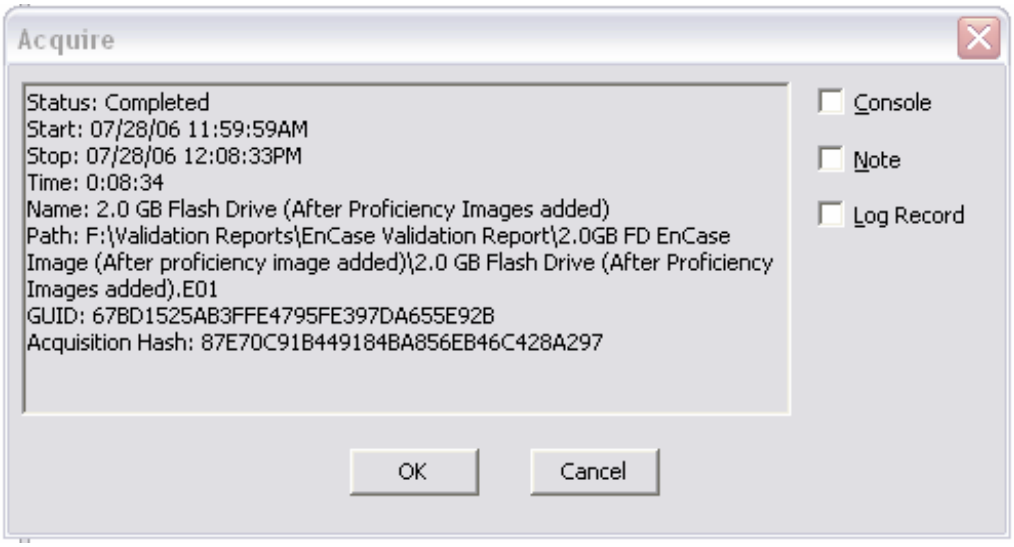


Figure 2.4 EnCase v.5.05d statistics of acquired flash media image



1401 Forensic Science Drive
Huntington, WV, 25701
Telephone: 304-690-4363
Fax: 304-690-4360
http://forensics.marshall.edu

Figure 2.5 Hash calculation of 2.0 GB USB flash media (after EnCase image taken)

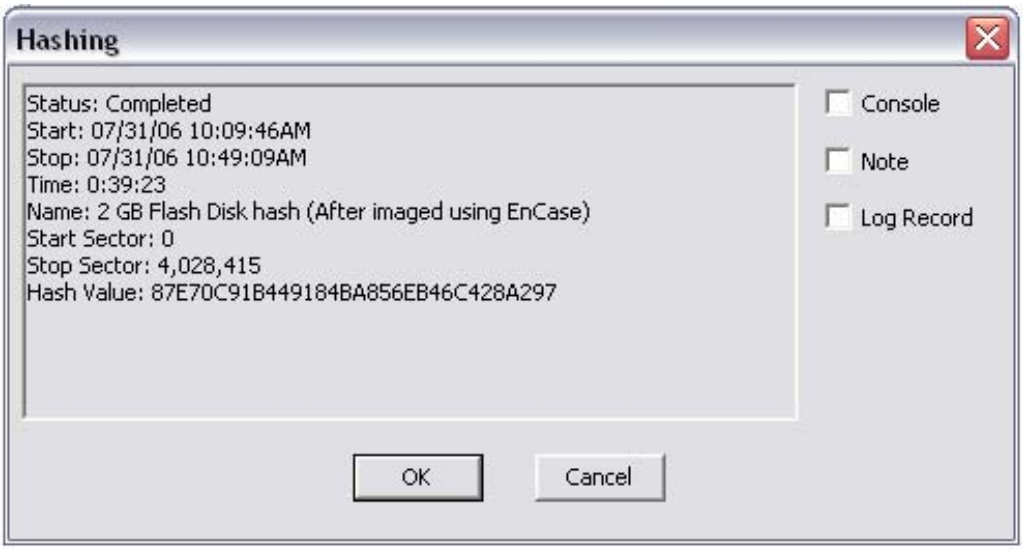
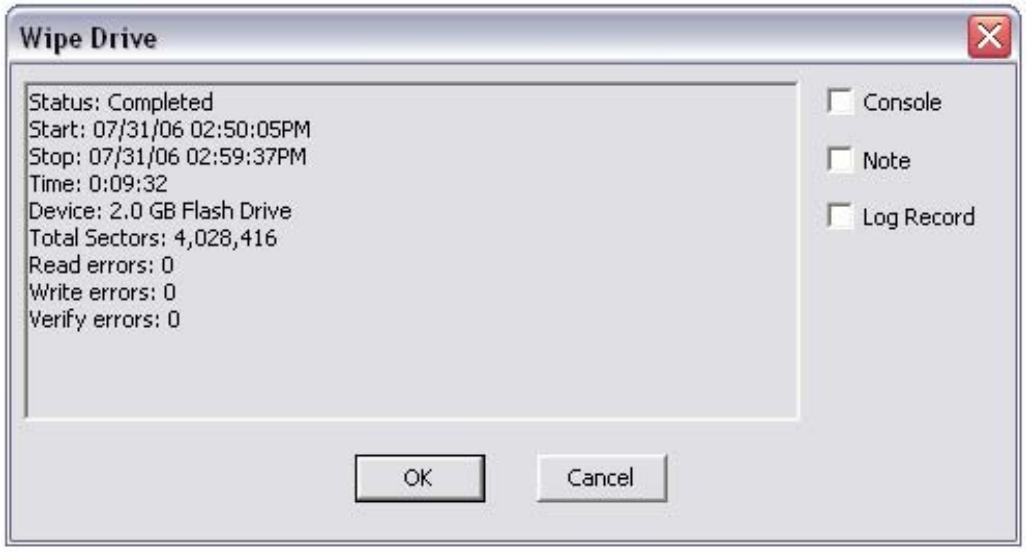


Figure 3.1 EnCase v.5.05d statistics of wiped flash source media



1401 Forensic Science Drive
Huntington, WV, 25701
Telephone: 304-690-4363
Fax: 304-690-4360
http://forensics.marshall.edu

Figure 4.1 Hash calculation of 2.0 GB USB flash media (after proficiency image wiped)

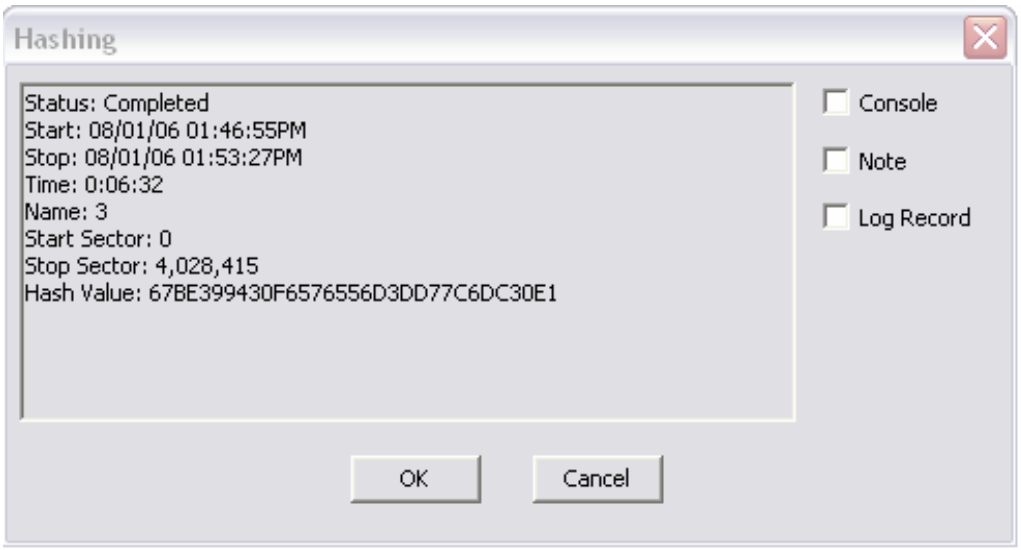
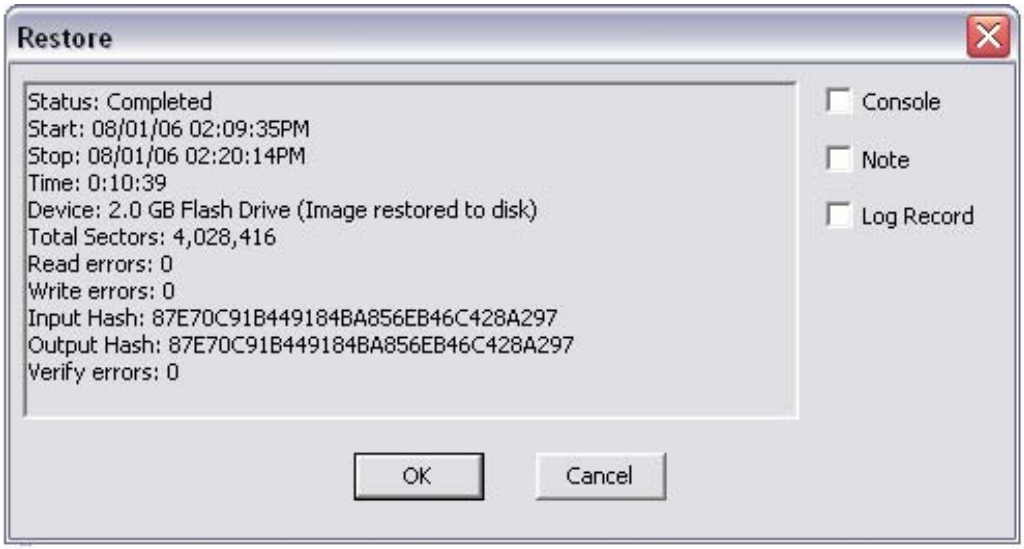


Figure 4.2 EnCase v.5.05d statistics after restoration of image to flash media



1401 Forensic Science Drive
Huntington, WV, 25701
Telephone: 304-690-4363
Fax: 304-690-4360
http://forensics.marshall.edu

Figure 4.3 Hash calculation of 2.0 GB USB flash media (after test image restored by EnCase)