Independent Validation and Verification (IV&V) of AccessData’s Forensic Toolkit (FTK) Imager v.2.5.1.
TEST PLAN

Test Number: FTKimager-2.5.1
Test Title: Independent Validation and Verification (IV&V) of FTK Imager v.2.5.1.
Test Date: 5/14/2007

Purpose and Scope:

Access Data’s FTK (Forensic Toolkit) Imager is a software-based forensic imaging tool that allows the capture of digital data from FAT, NTFS, EXT 2-3, as well as HFS and HPFS file systems. FTK Imager allows the generation of E01, DD, and SMART image formats, the image standard(s) for many current digital forensic applications.

This test plan will test the ability of FTK Imager to successfully and accurately create and MD5 hash independent E01, DD, and SMART images of an NTFS formatted hard disk drive (HDD). This test plan will evaluate version 2.5.1 and will consist of three test scenarios:

Requirements:
1) FTK Imager should accurately and successfully create a DD image and perform a MD5 hash an NTFS formatted hard disk drive.
2) FTK Imager should accurately and successfully create a SMART (ASR Data’s Linux-based tool format) image and MD5 hash an NTFS formatted hard disk drive.
3) FTK Imager should accurately and successfully create an E01 (Guidance Software’s EnCase format) image and MD5 hash an NTFS formatted hard disk drive.

Description of Methodology:

An 18.6 GB parallel-ATA (PATA) NTFS (New Technology File System) formatted source hard disk will be attached to a FastBloc 2 FE (Field Edition) hardware write block device and FTK Imager application will be launched. Using the Create Disk Image function, this physical source evidence drive will be selected for DD image creation. Upon conclusion of the capture, the MD5 hash calculation will be verified by comparing the original MD5 calculation of the source disk (previously created with a separate hashing tool) to the MD5 hash calculation generated by FTK Imager. The same procedure will be used to create and verify subsequent .E01 and SMART (.S01) images.

FTK Imager must successfully image the source hard disk drive into DD, SMART, and E01 image format(s). FTK Imager must also successfully produce an MD5 hash calculation that is consistent with the previously verified MD5 hash calculation of the source hard disk drive.

Expected Results:
1) FTK Imager will successfully create a DD Image of the NTFS formatted hard disk drive.

2) FTK Imager will produce an MD5 hash value following a DD capture that is consistent with the validated hash value of the source hard disk drive.

3) FTK Imager will successfully create a SMART Image of the NTFS formatted hard disk drive.

4) FTK Imager will produce an MD5 hash value following a SMART capture that is consistent with the validated hash value of the source hard disk drive.

5) FTK Imager will successfully create an E01 Image of the NTFS formatted hard disk drive.

6) FTK Imager will produce an MD5 hash value following an E01 capture that is consistent with the validated hash value of the source hard disk drive.

### Test Scenarios:

<table>
<thead>
<tr>
<th>Test Number</th>
<th>Environment:</th>
<th>Actions:</th>
<th>Assigned Reqt’s</th>
<th>Expected Results:</th>
</tr>
</thead>
<tbody>
<tr>
<td>01-01</td>
<td>NTFS formatted source HDD; FastBloc 2 FE; FTK Imager v.2.5.1</td>
<td>DD image created using software</td>
<td>1</td>
<td>DD image successfully created.</td>
</tr>
<tr>
<td>01-02</td>
<td>NTFS source HDD; FastBloc 2 FE; FTK Imager v.2.5.1</td>
<td>MD5 hash calculation performed on source HDD</td>
<td>1</td>
<td>MD5 hash calculation of HDD matches that of previously verified hash</td>
</tr>
<tr>
<td>01-03</td>
<td>NTFS formatted source HDD; FastBloc 2 FE; FTK Imager v.2.5.1</td>
<td>SMART image created using software</td>
<td>2</td>
<td>SMART image successfully created.</td>
</tr>
<tr>
<td>01-04</td>
<td>NTFS source HDD; FastBloc 2 FE; FTK Imager v.2.5.1</td>
<td>MD5 hash calculation performed on source HDD</td>
<td>2</td>
<td>MD5 hash calculation of HDD matches that of previously verified hash</td>
</tr>
<tr>
<td>01-05</td>
<td>NTFS formatted source HDD; FastBloc 2 FE; FTK Imager v.2.5.1</td>
<td>E01 image created using software</td>
<td>3</td>
<td>E01 image successfully created.</td>
</tr>
<tr>
<td>01-06</td>
<td>NTFS formatted source HDD; FastBloc 2 FE; FTK Imager v.2.5.1</td>
<td>MD5 hash calculation performed on source HDD</td>
<td>3</td>
<td>MD5 hash calculation of HDD matches that of previously verified hash</td>
</tr>
</tbody>
</table>
Test Data Description:

Test Data Set:

Seagate Barracuda ATA III
Model: ST320414A
Serial Number: 7EC0AS9Y
Part Number: 9R3004-301
Firmware Number: 3.05
20 Gigabyte Ultra ATA HDD

Drive Parameters:

Cylinders: 16383
Heads: 16
Sectors: 63
Addressable Sectors: 39,102,336

Installed Software:

Windows XP 32 Bit O/S w/ SP2
Microsoft Office 2003 Pro
Dell GX270 Drivers and Utilities Disk

MD5 hash value (Validated)

f2fe69015f701475863293a71ddda0d7

MD5 hash value (DD Image Capture)

f2fe69015f701475863293a71ddda0d7

MD5 hash value (SMART Image Capture)

f2fe69015f701475863293a71ddda0d7

MD5 hash value (E01 image Capture)

f2fe69015f701475863293a71ddda0d7
# SUMMARY REPORT

**Test Number:** FTKImager-2.5.1  
**Test Title:** Independent Validation and Verification (IV&V) of FTK Imager v.2.5.1.  
**Test Date:** 5/14/2007

## Test Description:

This test documents the ability FTK Imager v.2.5.1 to successfully and accurately create and MD5 hash independent E01, DD, and SMART images of an NTFS formatted hard disk drive. Additionally, this test plan will validate FTK Imager’s ability to successfully generate an MD5 hash value that is consistent with the original/validated MD5 hash value of the source HDD.

## Forensic Software/Tool:

| Title: Forensic Toolkit (FTK) Imager  
| Manufacturer: AccessData Corp.  
| Version: 2.5.1  
| Build: 06.07.27  
| Size: 8.61 Mbytes  

(Write Blocking Device for Validation HDD):  
| Title: FastBloc 2 Field Edition (FE)  
| Manufacturer: Guidance Software  
| Model Number: F.G.-0501-000A  
| Serial Number: 171483

## Test Results:

<table>
<thead>
<tr>
<th>Test Number</th>
<th>Environment: NTFS formatted source HDD; FastBloc 2 FE; FTK Imager v.2.5.1</th>
<th>Actions</th>
<th>Assigned Req's</th>
<th>Expected Results</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>01-01</td>
<td>DD Image created using software</td>
<td>1</td>
<td>DD image succesfully created</td>
<td>Pass</td>
<td></td>
</tr>
<tr>
<td>01-02</td>
<td>MD5 hash calculation performed on source HDD</td>
<td>1</td>
<td>MD5 hash calculation of HDD matches that of previously verified hash</td>
<td>Pass</td>
<td></td>
</tr>
<tr>
<td>01-03</td>
<td>SMART Image created using software</td>
<td>2</td>
<td>SMART image succesfully created</td>
<td>Pass</td>
<td></td>
</tr>
<tr>
<td>01-04</td>
<td>MD5 hash calculation performed on source</td>
<td>2</td>
<td>MD5 hash calculation of HDD matches that of previously verified</td>
<td>Pass</td>
<td></td>
</tr>
</tbody>
</table>
Independent Validation and Verification (IV&V) of FTK Imager (5/14/2007)

This document includes a cover page with the MISDE disclaimer
Figure 1.1- Results of DD Image Capture

![DD Image Capture Result]

Figure 1.2- Results of SMART Image Capture

![SMART Image Capture Result]
Figure 1.3 - Results of E01 Image Capture