### FTK Imager 软件

### 一种磁盘镜像工具的测试报告

目录

[介绍 4](#_Toc10769)

[如何阅读这份报告 5](#_Toc1485)

[工具描述 6](#_Toc3874)

[测试组织 6](#_Toc8481)

[结果汇总 6](#_Toc17199)

[测试环境和选定案例 6](#_Toc29331)

[所选测试示例 7](#_Toc2736)

[测试结果详细描述 9](#_Toc23214)

[FT-DI-01 9](#_Toc16421)

[测试实例描述 9](#_Toc29722)

[测试评估标准 9](#_Toc15640)

[测试实例结果 9](#_Toc15801)

[测试总结 10](#_Toc19065)

[FT-DI-03 10](#_Toc21504)

[测试实例描述 10](#_Toc21768)

[测试评估标准 10](#_Toc12874)

[测试实例结果 10](#_Toc3558)

[测试总结 10](#_Toc9119)

[FT-DI-05 11](#_Toc8379)

[测试实例描述 11](#_Toc1727)

[测试评估标准 11](#_Toc13342)

[测试实例结果 11](#_Toc26479)

[测试总结 11](#_Toc19997)

[FT-DI-15 11](#_Toc16227)

[测试实例描述 11](#_Toc17938)

[测试评估标准 11](#_Toc820)

[测试实例结果 12](#_Toc30256)

[测试总结 13](#_Toc1090)

[附录：额外细节 13](#_Toc12909)

[测试驱动器和分区 13](#_Toc13942)

[测试用例管理详情 13](#_Toc30638)

[测试设置和分析工具版本 14](#_Toc8508)

### 介绍

计算机取证工具测试（CFTT）计划是国土安全部（DHS），国家司法研究所(NIJ)和国家标准与技术研究院（NIST）特别计划办公室和信息技术实验室（ITL）的联合项目。CFTT得到了其他组织的支持，这些组织包括联邦调查局，美国国防部网络犯罪中心，美国国内税务局刑事侦查部分的电子犯罪计划以及美国国土安全部移民和海关执法局，美国海关边境保护和美国特勤局。CFTT计划的目标是向从业人员，研究人员和其他适用用户提供用于计算机取证调查工具的可衡量的标准以及准确的结果。实现这一点需要开发计算机取证工具的规格和测试方法，并根据这些规范对特定工具进行后续测试。

测试结果为开发人员改进工具，用户作出明智选择以及增强法律界和其他人了解工具的能力提供了必要的信息。CFTT测试计算机取证工具的方法基于公认的一致性和质量测试方法。对于计算机取证领域的有兴趣的人可以查看和评论CFTT 官方网站上发布的规范和测试方法。

联合测试是CFTT计划的扩展，为取证调查人员和实验室提供工具测试的测试材料，以支持形成共享的测试报告。联合测试的目标是帮助取证调查人员测试他们在实验室中使用的工具，并共享工具测试结果。CFTT的联合测试取证工具测试环境和包含的测试套件可以从CFTT网站下载并用于测试取证工具。测试结果可以选择与CFTT共享，由CFTT工作人员审查，然后公开分享。

本文档说明了使用用于磁盘映像的CFTT联合测试套件1.1版测试FTK Imager 3.4.2.6的磁盘镜像功能的结果。

用于磁盘映像的联合测试套件非常灵活，可以让取证实验室减少测试每种工具功能所需的时间，而不仅仅是测试特定实验室使用的镜像工具功能。本报告反映了测试某些取证实验室日常使用的功能的可能性。

其他工具的测试结果可在DHS的计算机取证网页上找到。

### 如何阅读这份报告

这份报告由以下几节组成：

1.被测试的工具说明。包括工具名称，版本，供应商信息，支持环境版本（例如，操作系统版本，设备固件版本等）。

2.测试组织。信息和联系方式。

3.结果总结。本节标识在测试运行中观察到的任何重大异常。本节提供关键性研究结果的叙述，确定工具符合预期的情况，并提供工具不符合预期的所有情形的总结。该部分还提供了关于该工具或关于测试该工具的任何意见，包括任何观察到的限制或对工具使用施加的限制。

4.测试环境。描述工具测试中使用的以满足测试组织的政策和要求的硬件和软件环境。

5.测试结果的实例详细说明。自动生成识别异常的测试结果。

6.附录：附加细节。每个测试案例的附加管理细节，例如运行测试的人员，运行测试的时间，使用的计算机等。

### 磁盘拷贝工具Access Data FTK Imager（版本3.4.2.6）的复合测试测试结果

测试已针对以下写入块方案进行了配置：

WiebeTech Forensic ComboDock FCDv5.5 通过USB连接到PC的小型(<138GB)的ATA驱动器。

Tableau T35u 通过USB连接到PC的大型(>138GB)的ATA驱动器。

WiebeTech Forensic ComboDock FCDv5.5 通过火线接口连接到PC小型（<138GB）SATA驱动器。

WiebeTech Forensic ComboDock FCDv5.5 通过火线接口连接到PC大型（> 138GB）SATA驱动器。

带有Digital Intelligence USB 3.0 Forensic读卡器的SD驱动器通过USB接口连接到PC

### 工具描述

工具名称: FTK Imager

固件版本：3.4.2.6

操作系统：Microsoft Windows Version 7 & Microsoft Windows Version 8

供应商信息：

供应商姓名：AccessData

地址： 588 West 400 South Suite 350

Lindon, Utah 84042

电话： 801.377.5410

网站：http://www.accessdata.com/

### 测试组织

此测试报告是使用CFTT的联合测试取证工具测试环境生成的，请参阅CFTT Federated Testing Project

### 结果汇总

测试的工具按预期运行，没有异常。

### 测试环境和选定案例

标记为七的PC：

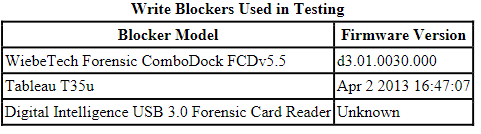
硬件：Dell Optiplex 980 PC, USB 2 ,FireWire 400 ports.

操作系统：Microsoft Windows 7

标记为八的PC：

硬件：Toshiba Satellite laptop with USB 3 port

操作系统：Microsoft Windows 8



### 所选测试示例

下列表格简要介绍了每个选用执行的测试用例。

测试用例状态

|  |  |  |
| --- | --- | --- |
| 示例 | 描述 | 状态 |
| FT-DI-01-ATA28 | 使用连接到具有给定镜像文件接口的计算机的给定写入阻止器来获取给定类型的驱动器，并计算所选数据的选定散列值。测试在创建镜像文件时准确读取给定驱动器类型的能力并正确地计算哈希。 | 完成 |
| FT-DI-01-ATA48 | 同上 | 完成 |
| FT-DI-01-SATA28 | 同上 | 完成 |
| FT-DI-01-SATA48 | 同上 | 完成 |
| FT-DI-03-SD | 使用给定的媒体读取器或连接到具有给定镜像文件接口的计算机的写入阻止器来获取给定类型的可移动媒体，并为获取的数据计算选定的散列。测试在创建镜像文件时准确读取给定可移动媒体类型并正确地散列数据的能力。 | 完成 |
| FT-DI-05-NTFS | 获取给定类型的分区给镜像文件并计算所选数据的散列值。测试在创建镜像文件时准确读取给定分区类型并正确地散列数据的能力。 | 完成 |
| FT-DI-15 | 将具有故障扇区的驱动器进行克隆。如果遇到故障扇区，则表征映像工具的行为。 | 完成 |

### 测试结果详细描述

本节介绍按功能分组的测试结果。

### FT-DI-01

### 测试实例描述

使用连接到具有给定镜像文件接口的计算机的给定写入阻止器来获取给定类型的驱动器，并计算所选数据的选定散列值。测试在创建镜像文件时准确读取给定驱动器类型的能力并正确地计算哈希。

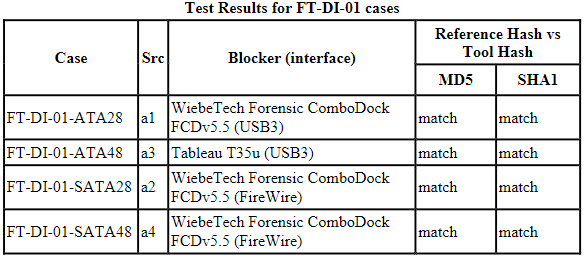
此测试可以被重复来测试多个驱动器类型的情况。此测试使用特定的写入阻止程序测试工具获取特定类型驱动器（测试的驱动器类型包含在测试用例名称中）到映像文件的能力（仅适用于硬件写入阻止程序使用的工具）以及测试计算机和写入阻止器之间的特定接口连接。下表中列出了每个测试用例所使用的写入阻止程序和测试用计算机与写入阻止程序之间的接口连接。测试ATA或SATA驱动器需要两个测试，一个测试小于138GB的驱动器（ATA28和SATA28：28位寻址），一个测试更大的驱动器（ATA48和SATA48：48位寻址）。

### 测试评估标准

工具计算出的散列值应与为源驱动器计算的散列值相匹配。

### 测试实例结果

下表列出了各个测试用例的结果。



### 测试总结

结果符合预期。

### FT-DI-03

### 测试实例描述

使用给定的媒体读取器或连接到具有给定镜像文件接口的计算机的写入阻止器来获取给定类型的可移动媒体，并为获取的数据计算选定的散列。测试在创建镜像文件时准确读取给定可移动媒体类型并正确地计算数据的哈希的能力。

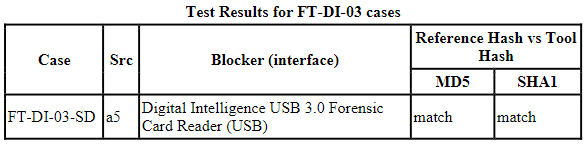
此测试可以被重复来测试多种可移动介质类型的情况。该测试使用特定的介质读取器测试该工具获取特定类型的可移动介质（测试可移动介质类型包括在测试用例名称中）到镜像文件的能力，该读取器也可以是写入阻止器和特定接口测试计算机和媒体阅读器之间的连接。下表列出了每个测试用例使用的介质读取器和测试计算机与介质读取器之间的接口连接。

### 测试评估标准

工具计算出的散列值应与为源驱动器计算的散列值相匹配。

### 测试实例结果

下列表格展示了测试的结果。



### 测试总结

结果符合预期。

### FT-DI-05

### 测试实例描述

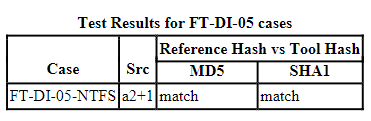
获取给定类型的分区给镜像文件并计算所选数据的散列值。测试在创建镜像文件时准确读取给定分区类型并正确地散列数据的能力。

### 测试评估标准

工具计算出的散列值应与为源驱动器计算的散列值相匹配。

### 测试实例结果

下列表格展示了测试的结果。



### 测试总结

结果符合预期。

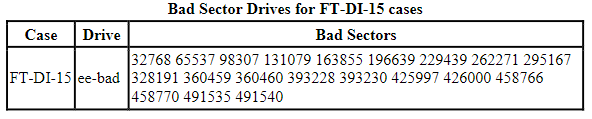
### FT-DI-15

### 测试实例描述

将具有故障扇区的驱动器进行克隆。如果遇到故障扇区，则表征映像工具的行为。

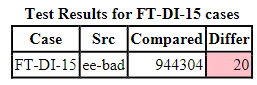
### 测试评估标准

目标驱动器和参考驱动器之间的比较结果指示获取具有故障扇区的驱动器时的工具行为。



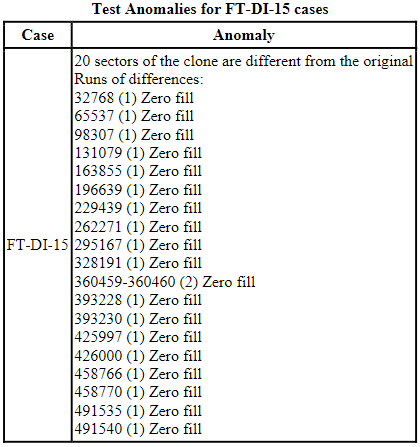
### 测试实例结果

下列表格展示了测试的结果。



异常

下表列出了所有观察到的异常情况并提供了更多详细信息。



### 测试总结

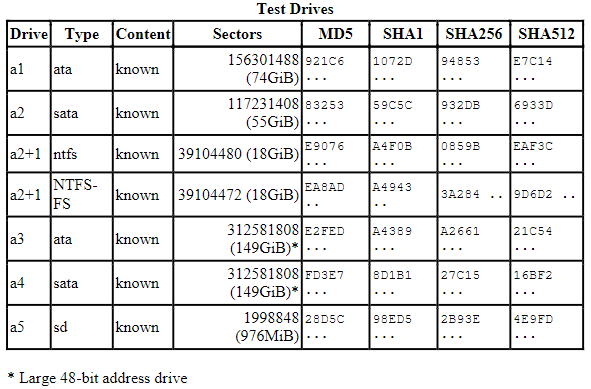
结果如预期。与原始源驱动器不同的20个扇区是无法获取的20个故障扇区。

### 附录：额外细节

### 测试驱动器和分区

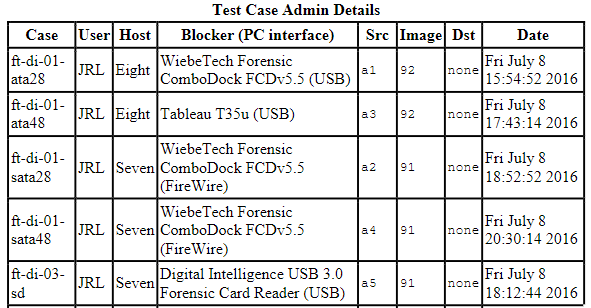
下表列出了每个源对象，驱动器或分区的状态，包括参考散列和已知内容。

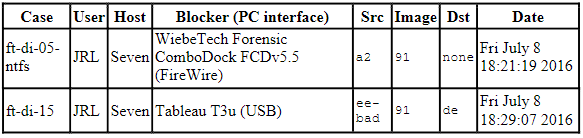
表中描述了驱动器和分区。驱动器栏中的分区由符号[drive] + [分区号]指示。其中[驱动器]是驱动器标签，[分区编号]是分区编号。例如，驱动器A3上的第一个分区将是A3 + 1。类型列记录驱动器类型，例如SATA，USB等，或者分区类型，例如NTFS，FAT32等，这取决于是否正在描述驱动器或分区。



### 测试用例管理详情

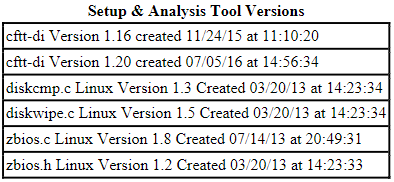
对于每次测试运行，都会列出测试计算机，测试仪，源驱动器，映像文件驱动器，目标驱动器以及测试运行日期。





### 测试设置和分析工具版本

所有工具的版本号如下所示



工具：@(#) ft-di-prt\_test\_report.py Version 1.20 created 07/05/16 at 14:57:20

系统：Linux Version 3.2.0-51-generic

Federated Testing Version 1.1-1, released 7/8/2016