# 数字数据采集工具测试断言和测试计划

# 摘要

本文档定义了测试断言和一种用于测试数字数据采集工具是否符合2004年10月4日在“数字数据采集工具规范”第4版中规定的要求的测试方法。这些要求是由经过培训并具有使用硬件写入阻止工具丰富经验的成员组成的焦点小组开发的，并且已经进行了依赖于这些工具结果的调查。断言被描述为在测试执行后可以检查的条件的一般陈述。 每个断言都会出现在一个或多个测试用例中，用于指定详细的参数，执行测试的过程以及预期的结果。

随着本文件通过焦点小组和其他机构的评论发展，新版本将会发布到网站<http://www.cftt.nist.gov/>上。

# 目录

# 1.简介

执法界迫切需要确保计算机取证工具的可靠性。需要有能力确保取证工具始终如一地产生准确，可重复和客观的测试结果。美国国家标准与技术研究院（NIST）的计算机取证工具测试（CFTT）项目的目标是通过开发功能规格，测试程序，测试标准，测试集和测试硬件来建立一个测试计算机取证工具的方法。这些结果为工具制造商改进工具提供了必要的信息，使用户能够在获取和使用计算机取证工具方面做出明智的选择，并让相关组织了解工具的能力。 这种测试计算机取证工具的方法是基于公认的符合性测试和质量测试的国际方法。 这个项目在<http://www.cftt.nist.gov/>上有更深入的介绍。

CFTT是美国司法部研究和发展组织的国家司法研究所（NIJ）的联合项目; NIST执法标准办公室（OLES）和NIST信息技术实验室（ITL）; 并得到其他组织的支持，其中包括联邦调查局，国防部网络犯罪中心，美国国税局刑事调查局的电子犯罪计划，国土安全部移民和海关执法局以及美国特勤局。 由于所有文件都发布在网络上供公众查阅，整个计算机取证社区都有机会参与到规范和测试方法的开发中去。

# 2.目的

本文档根据2004年10月4日发表的数字数据采集工具规范第4版中规定的要求定义测试断言和测试方法。断言是测试运行后检查的一般条件语句。每个断言都有一个或多个测试用例，用于指定详细的启动参数，执行测试的过程以及预期结果。

# 3.范围

本规范的范围仅限于从需要通过计算机作为文件系统进行访问的数字存储介质中获取数据的软件工具和硬件设备。这包括利用ATA，SCSI，USB或Firewire接口的存储介质，不包括用于对其他数字设备（如手机，传呼机或PDA）的存储介质进行成像的工具。

本规范不会去规定正确使用或者禁止滥用工具。

# 4.背景

数字源采集过程的两个关键可测量属性是准确性和完整性。准确性是一种定性的度量，用于确定采集的每个位是否与源的相应位相等。完整性是确定源的每个可访问位是否被获取的定量度量。数字源可能包含可见和隐藏的扇区，他的克隆就可能包含一些良性填充来代替一些无法获取的源数据。除了所获取的源数据之外，图像文件也可能包含其他信息，其也可能被加密或压缩。

采集的准确性和完整性受多种因素影响。为了访问数字源，包含数字源的物理设备就需要通过物理接口连接到计算机。其中，传统BIOS，扩展BIOS，ATA，SATA，SCSI，ASPI，USB，IEEE 1394，RAID，以及通过网络远程访问都是访问接口的一些示例。一些接口具有不止一个接口版本，这对采集过程有着重要的意义。例如，ATA-3不允许使用48位磁盘地址，但是ATA-6却允许。成像工具必须通过某种协议读取设备。 例如，ATA接口可能连接了一个硬盘驱动器，然后通过BIOS中断0x13命令或直接通过ATA命令进行访问。

影响采集完整性的另一个因素是确定数字资源的真实规模。根据ATA规格后期制作的硬盘驱动器可能允许创建无法访问或隐藏的区域，例如主机保护区。 例如，具有80GB空间的驱动器可能会被重新配置以至于显示只具有更小的空间。如果尝试读取隐藏区域数据，则会导致错误，除非驱动器被重新配置回原始大小。

# 5.测试断言

本节列出了采集工具应符合的测试断言。测试断言是必须经过测试以确认符合要求的条件。大多数断言都指定了一个要测试的条件。但是，有一些断言用于记录测试设置的某些方面，例如用于访问数字源的接口类型。 断言分为强制性工具特征的断言和可选特征的断言。

附录B介绍了和断言要求相关联的可追溯性矩阵以及用于测试案例的断言。

一些断言假定选择给定的参数。要执行采集，工具必须在执行环境XE中执行。 此外，必须指定数字源DS和用于源SRC-AI的访问接口。 其他测试参数包括：FS，文件系统类型和DST-AI，用于写入克隆的访问接口。其中，测试参数将在第6节“测试方法”中讨论。

# 5.1强制性特征断言

DA-AM-01. 该工具使用访问接口SRC-AI访问数字源。

DA-AM-02. 该工具获取数字源DS。

DA-AM-03. 该工具在执行环境XE中执行。

DA-AM-04. 如果指定了克隆创建，该工具会创建数字源的克隆。

DA-AM-05. 如果指定了图像文件创建，则该工具会在文件系统类型FS上创建一个图像文件。

DA-AM-06. 所有可见扇区都是从数字源获取的。

DA-AM-07. 所有隐藏扇区都是从数字源获取的。

DA-AM-08. 从数字源获取的所有扇区都可以准确获得。

DA-AM-09. 如果从所选数字源读取时发生未解决的错误，该工具会通知用户数字源内的错误类型和位置。

DA-AM-10. 如果在从所选数字源读取数据时发生未解决的错误，该工具将使用目标对象的良性填充来代替不可访问的数据。

# 5.2可选特征断言

以下测试断言适用于图像文件。

DA-AO-01. 如果该工具创建图像文件，则图像文件表示的数据与该工具获取的数据相同。

DA-AO-02. 如果指定了图像文件格式，则该工具将以指定的格式创建图像文件。

DA-AO-03. 如果在写入图像文件时发生错误，该工具会通知用户。

DA-AO-04. 如果该工具正在创建图像文件，并且图像目标设备上没有足够的空间来保存图像文件，则该工具应通知用户。

DA-AO-05. 如果该工具创建一个需要参数的多文件图像，则所有单个文件都应具有所需参数，废除某个文件可能较小。

DA-AO-06. 如果工具对创建文件后未更改的图像文件执行图像文件完整性检查，则工具应通知用户图像文件未被更改。

DA-AO-07. 如果该工具对创建文件后发生更改的图像文件执行图像文件完整性检查，则工具应通知用户图像文件已更改。

DA-AO-08. 如果该工具对创建文件后发生更改的图像文件执行图像文件完整性检查，则工具应通知用户受影响的位置。

DA-AO-09. 如果工具将源图像文件从一种格式转换为另一种格式的目标图像文件，则目标图像文件中表示的采集数据与源图像文件中采集的数据相同。

DA-AO-10. 如果没有足够的空间来存放多文件图像的所有文件，并且支持目标设备切换，则图像会在另一台设备上继续显示。

以下测试断言适用于克隆创建。

DA-AO-11. 如果需要，在采集数字源期间创建一个克隆。

DA-AO-12. 如果请求，则从图像文件创建克隆。

DA-AO-13. 使用访问接口DST-AI创建克隆以写入克隆设备。

DA-AO-14. 如果创建了未对齐的克隆，则写入克隆的每个扇区都会被精确地写入该数字源占用扇区的克隆中的相同磁盘地址。

DA-AO-15. 如果创建了一个对齐的克隆，源的相邻扇区内的每个扇区就会被精确地写入克隆设备上相同的磁盘地址，相对于原始数字源占用的扇区起点。扇区范围被定义为可安装的分区或连续的不属于可安装分区的扇区序列。扩展分区可能同时包含可挂载分区和未分配扇区，不是单独的可挂载分区。

DA-AO-16. 如果指定了图像或采集的子集，则所有子集都被克隆。

DA-AO-17. 如果需要，克隆目标设备上的任何多余扇区都不会被修改。

DA-AO-18. 如果需要，良性填充将被写入克隆的多余部分。

DA-AO-19. 如果没有足够空间创建完整克隆，则会使用克隆设备的所有可用扇区创建截断克隆。

DA-AO-20. 如果创建了截断克隆，则该工具会通知用户。

DA-AO-21. 如果在克隆创建过程中出现写入错误，该工具会通知用户。

以下断言适用于提供块哈希日志记录的工具。

DA-AO-22. 如果需要，该工具会在从数字源获取的每个块的采集期间计算指定块大小的块散列值。

以下断言适用于创建日志文件的工具。

DA-AO-23. 如果该工具记录了任何重要的日志信息，则信息将被准确记录在日志文件中。

以下断言适用于提供采集而无需数字源写保护的工具。

DA-AO-24. 如果该工具在法医学安全的执行环境中执行，则数字源在采集过程中不会改变。

# 6.测试方法

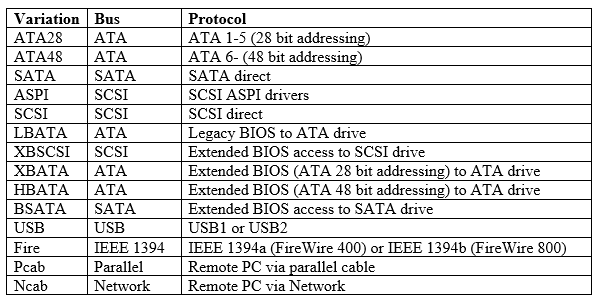
本节介绍如何测量每个测试断言。 有些断言只能确定必须为测试用例指定的参数。 其他断言定义了一个量度，以衡量工具与测试断言的一致性。

DA-AM-01. 该工具使用访问接口SRC-AI访问数字源。

这个断言记录了为测试用例指定的执行环境。

表1列出了重要的访问接口，如果被测工具可见，则要进行测试。 Variation在测试运行文档中用于指示测试运行中使用的访问接口。 Bus是实际的物理总线。Protocol是被测工具用来与物理总线交互的方法。例如，要确保使用ATA28接口，具有符合ATA5或更低级别的ATA磁盘控制器的主机将与相匹配的硬盘一起使用。为确保使用ATA48接口，具有符合ATA6或更高级别的控制器的主机将与大于140GB的硬盘一起使用。

表1 访问接口

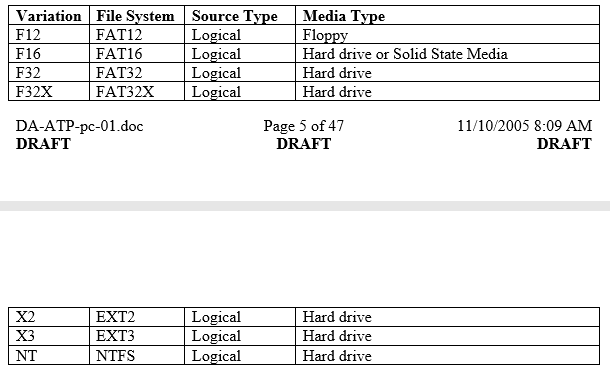


DA-AM-02. 该工具获取数字源DS。

这种断言记录了为测试用例指定的数字源的类型。

如果工具支持给定的文件系统，则应执行表2中列出的接口。表3中的执行接口是可选的。

表2必需数字源接口



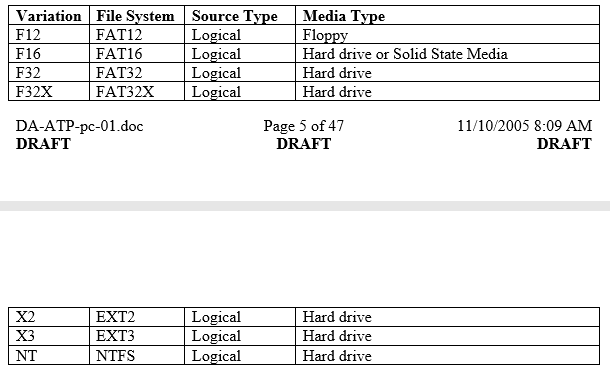
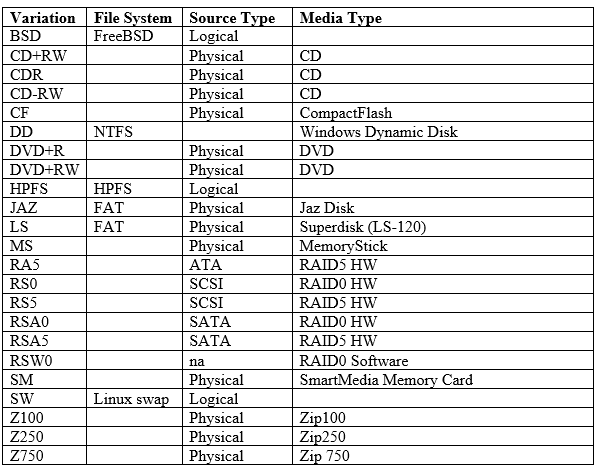
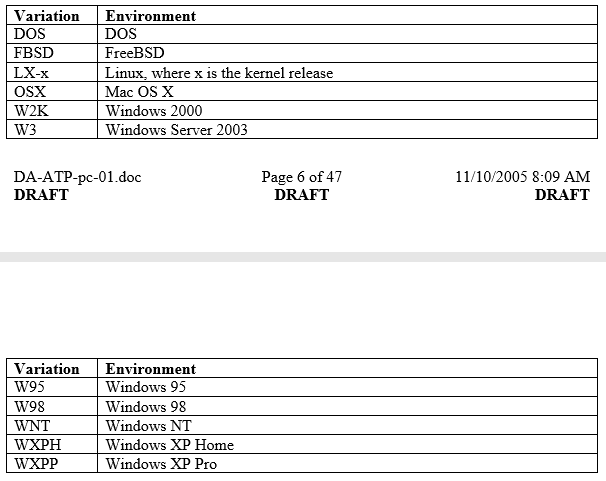
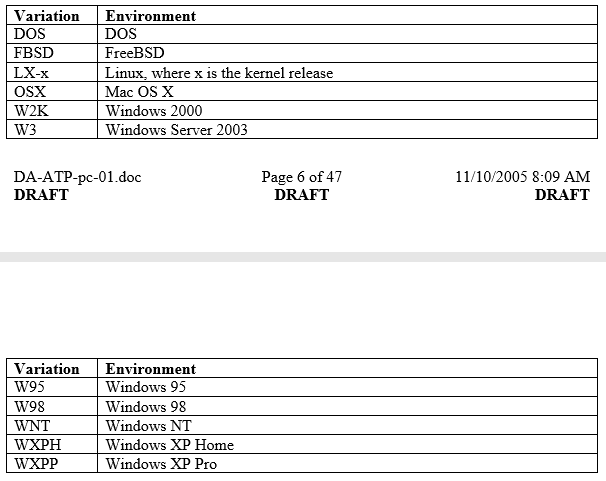


表3可选的数字源接口

DA-AM-03. 该工具在执行环境XE中执行

该断言用于记录为测试用例指定的执行环境。





DA-AM-04. 如果指定了克隆创建，该工具会创建数字源的克隆。

此断言用于记录创建克隆。

DA-AM-05. 如果指定了图像文件创建，则该工具会在文件系统类型FS上创建一个图像文件。

该断言用于记录用于为测试用例创建图像文件的文件系统的类型。

DA-AM-06. 所有可见扇区都是从数字源获取的。