ICS 35.220.20
A 90

GA

中华人民共和国社会公共安全行业标准

GA/T 756—2008

数字化设备证据数据发现提取固定方法

Discovering, extraction and preservation method of

evidence data on digital device

2008-03-24 发布　　2008-03-24 实施

中华人民共和国公安部 发布

前　言

本标准由公安部公共信息网络安全监察局提出。
本标准由公安部信息系统安全标准化技术委员会归口。
本标准起草单位：公安部公共信息网络安全监察局、福建厦门美亚柏科公司。
本标准主要起草人：许剑卓、黄春健、耿涛、何星。

数字化设备证据数据发现提取固定方法

1 范围

本标准规定了从数字化设备发现提取固定证据数据，并保证证据数据原始性和证据数据完整性的方法。

本标准适用于在电子数据检验鉴定工作中，从本地数字化设备或远程数字化设备发现提取固定证据数据。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本标准，然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

GA/T 754-2008 电子数据存储介质复制工具要求及检测方法

GA/T 755-2008 电子数据存储介质写保护设备要求及检测方法

3 术语和定义

下列术语和定义适用于本标准。

3.1

数字化设备 digital device

存储、处理和传输二进制数据的设备，包括计算机、通信设备、网络设备、电子数据存储设备等。

3.1.1

本地数字化设备 local digital device

检验人员能物理接触、操作的数字化设备。

3.1.2

远程数字化设备 remote digital device

能通过网络访问的数字化设备。

3.2

证据数据 evidence data

作为证据使用的电子数据。

3.3

证据数据发现提取 evidence data discovering and extraction

对数字化设备存储、处理、传输的数据进行搜索、分析、截获，获得证据数据的过程。

3.4

固定证据数据 preserve evidence data

在证据数据发现提取过程中，采取技术措施或记录相关信息，保护证据数据完整性。

3.5

逐比特一致 bit-based identicalness

两组数据每一比特位数值相同。

3.6

含义一致 content-based identicalness

就检验鉴定结论所下断言而言，两组数据所表示的含义相同。

示例：两张图片展示相同的文字信息，虽然其数据并非逐比特一致，但如果检验鉴定结论所下断言评价的是其包含的文字信息，则其数据含义一致。

3.7

可再现数据 reproducible data

如果重复证据数据发现提取过程，可重新获得逐比特一致或含义一致的证据数据，则称该证据数据为可再现数据。

3.8

不可再现数据 irreproducible data

如果证据数据发现提取过程无法重复，或证据数据发现提取相关环境条件无法复原，重复证据数据发现提取过程无法重新获得逐比特一致或含义一致的证据数据，则称该证据数据为不可再现数据。

3.9

证据数据原始性 evidence data originality

证据数据是按照所描述的步骤从被检验数字化设备中发现提取获得的。

注：保护证据数据原始性是指采取技术措施，保证通过展示相关记录信息或重新实施证据数据发现提取过程，能证实证据数据是按照所描述的发现提取步骤从被检验数字化设备中发现提取获得的。

3.10

证据数据完整性 evidence data integrity

证据数据在发现提取后未被修改。

注：保护证据数据完整性是指采取技术措施，保证通过展示相关记录信息，能证实证据数据在发现提取后是否被修改。

3.11

哈希值 hash data

使用MD5等哈希算法对数据进行计算获得的数值。

3.12

原始电子数据存储介质 original digital data storage

被检验数字化设备中包含的电子数据存储介质。

3.13

检验用例 inspection case

规定如何发现证据数据的文档化的细则。包括：

a) 目标证据数据；

b) 检验设备和软件；

c) 证据数据发现提取操作步骤；

d) 检验环境条件。

3.14

屏幕录像软件 computer screen capture

用于截获计算机屏幕上显示的内容，并生成视频文件的软件。

4 证据数据发现提取固定步骤

4.1 记录检材情况

a) 对检材进行编号；

b) 对送检数字化设备逐一拍照，并记录检材的特征。

4.2 设计检验用例

根据目标证据数据设计检验用例。检验用例应符合以下要求：

a) 对具备复制条件的，应使用符合 GA/T 754—2008 要求的电子数据存储介质复制工具复制原始电子数据存储介质，将复制生成的克隆或镜像文件作为检验对象；
b) 对于具备写保护条件的，应使用符合 GA/T 755—2008 要求的写保护设备，将电子数据存储介质通过写保护设备接入到检验设备上；
c) 对于不启动被检验数字化设备的操作系统，能发现提取固定的证据数据，应优先选择在不启动被检验数字化设备的操作系统的条件下发现提取固定证据数据。

4.3 发现提取固定证据数据

a) 根据检验用例准备检验环境条件、数字照相机和数字摄像机。
b) 对于检验设备为计算机的，在检验设备上安装屏幕录像软件，使用杀毒软件查杀计算机上的病毒程序。
c) 对于以下情形，启动数字摄像机或屏幕录像软件，记录检验设备屏幕上显示的内容：
   1) 目标证据数据为不可再现数据的；
   2) 检验对象为远程数字化设备的；
   3) 检验对象为原始电子数据存储介质且不具备写保护条件的；
   4) 检验过程中启动被检验数字化设备的操作系统且不具备写保护条件的。
d) 对于目标证据数据为可再现数据的，可不启动数字摄像机或屏幕录像软件。
e) 根据检验用例规定的证据数据发现提取操作步骤，搜索、分析、截获证据数据。
f) 对于能复制导出成为数据文件的证据数据，将数据文件复制导出作为证据数据。
g) 对于在被检验设备屏幕上显示的，无法截获转换成数据文件的信息，使用数字照相机或数字摄像机拍摄屏幕显示内容，将拍摄获得的图像文件和视频文件导出作为证据数据。
h) 计算导出的证据数据文件的哈希值。
i) 对于启动数字摄像机或屏幕录像软件的，在检验设备屏幕上显示导出的数据文件名称和哈希值并予以录像。
j) 对于启动屏幕录像软件的，停止屏幕录像软件，将生成的视频文件导出并计算其哈希值。
k) 对于使用数字摄像机录像的，停止录像，将录像带封存并编号，或将录像结果导出成数据文件并计算其哈希值。

4.4 检验记录

4.4.1 对于检材，应记录以下内容：

a) 检材类别；
b) 检材型号；
c) 检材出厂时唯一性编号（如果适用）；
d) 检材的照片。

4.4.2 对于证据数据，应记录以下内容：

a) 检验目的；
b) 检验设备和软件；
c) 证据数据发现提取操作步骤；
d) 检验环境条件；
e) 导出的证据数据文件的存储位置、文件名、文件哈希值和数据的可再现特性；
f) 检验时间；
g) 检验人员。

4.4.3 对于导出的录像文件，应记录：

a) 录像文件名;
b) 录像开始时间;
c) 录像结束时间;

d） 录像文件哈希值；

e） 检验人员。

4.4.4 对于记录检验过程的录像带，应记录：

a） 录像带编号

b） 录像开始时间；

c） 录像结束时间；

d） 检验人员。

参考文献

RFC 1321 The MD5 Message-Digest Algorithm