ICS 35.240.01
A 92

GA

中华人民共和国公共安全行业标准

GA/T 976—2012

电子数据法庭科学鉴定通用方法

General method for electronic data identification of forensic

2012-02-01 发布　　2012-02-01 实施

中华人民共和国公安部　发布

前　言

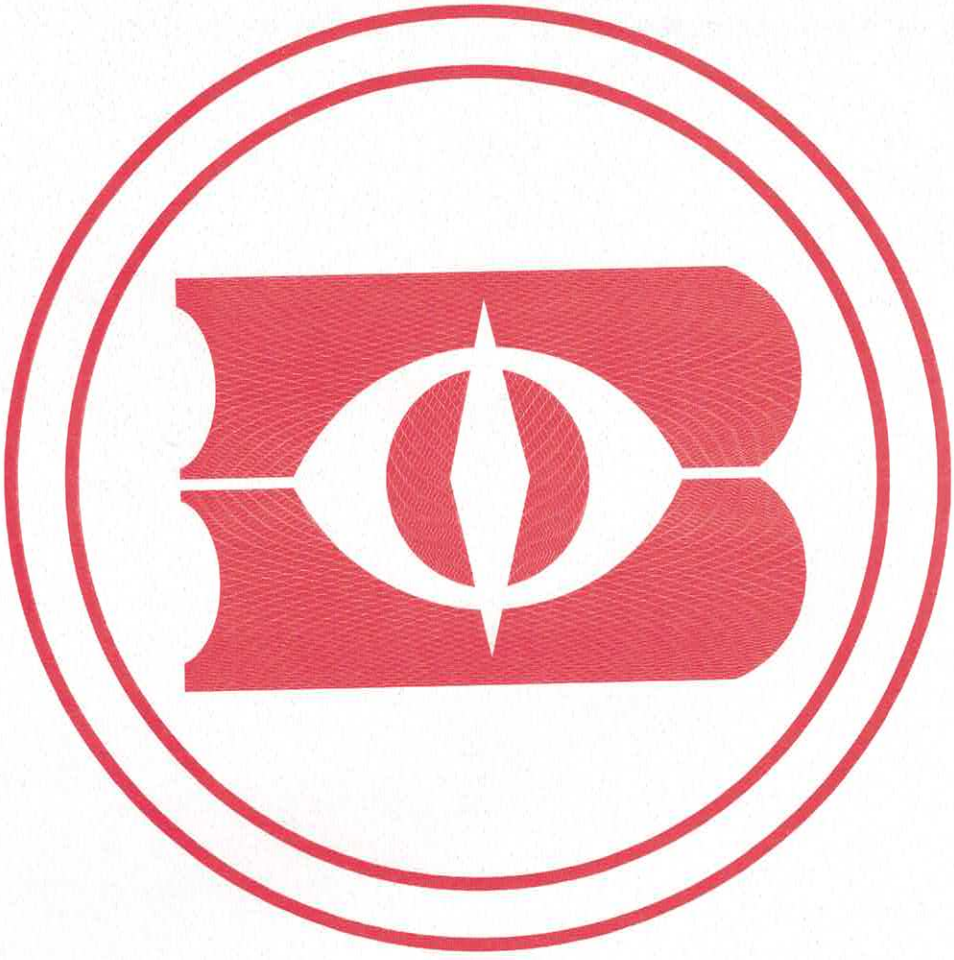
本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由公安部网络安全保卫局提出。

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：公安部网络安全保卫局、公安部第三研究所。

本标准主要起草人：许剑卓、郭弘、侯钧雷、金波、黄道丽、沙晶、杭强伟、徐隽。



电子数据法庭科学鉴定通用方法

1 范围

本标准规定了法庭科学鉴定时，电子证据数据的获取、检验分析与呈现的通用方法。

本标准适用于法庭科学鉴定工作中，获取、检验分析与呈现电子证据数据。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

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

GA/T 756—2008 数字化设备证据数据发现提取固定方法

3 术语和定义

GA/T 754—2008、GA/T 755—2008 和 GA/T 756—2008 界定的以及下列术语和定义适用于本文件。

3.1

电子证据数据 electronic evidence data

被作为证据使用的、能够证明案件相关事实的电子数据。

3.2

电子文件 electronic records

基于电子技术生成、以数字化形式存在于磁盘、磁带等介质，其内容可与载体分离，并可多次复制到其他介质的文件。

3.3

电子数据存储介质 electronic data storage

能写入数据、保留数据和重新读出数据的电子存储设备。

3.4

证据数据获取 evidence data acquisition

对电子设备存储、处理、传输的数据进行搜索、分析、截获，获得证据数据的过程。

3.5

哈希值 hash data

使用安全的哈希算法对数据进行计算获得的数据。

4 领域

电子数据法庭科学鉴定的领域包括从本地数字化设备或远程数字化设备提取固定证据数据，从本地数字化设备恢复证据数据，证据数据的分析与鉴定以及信息系统分析与鉴定等。

5 人员和设备

5.1 人员

从事电子数据法庭科学鉴定的人员应具有电子数据鉴定业务相关的高级专业技术职务资格；或者具有计算机科学与技术专业、电子技术专业或者相关专业本科以上学历，从事电子数据鉴定工作五年以上；或者具有电子数据鉴定业务相关工作十年以上经历和较强的专业技能。

5.2 设备

用于电子数据法庭科学鉴定的设备应符合以下要求：

a) 应确保设备能够满足电子数据法庭科学鉴定的要求；
b) 自行研制的设备应通过确认；
c) 用于鉴定的计算机系统或网络系统应进行合理配置；
d) 鉴定所使用的软硬件检测工具应进行运行检查和期间核查，以保持其状态的可靠性。

6 原则

6.1 及时性原则

证据数据的获取具有时效性，一旦确定对象后，应尽快提取证据，防止证据变更和丢失。

6.2 依法原则

鉴定应依法进行，确保鉴定主体、客体和程序的合法性。

6.3 备份原则

对可以制作副本或镜像的原始电子数据存储介质应制作副本或镜像。

6.4 证据原始性原则

获取、分析证据数据时不能改变其原始性。

6.5 环境安全原则

证据数据应妥善保存，以备随时重建、试验或者展示。

6.6 监督原则

整个证据数据获取、分析、鉴定过程应受到监督和控制，确保鉴定结果准确、有效。

7 步骤

7.1 证据数据的获取

电子数据法庭科学鉴定中，证据数据的获取过程应按照以下步骤操作：

a) 制定证据获取的计划。计划包括人员、仪器设备、采用的标准规范、证据获取的顺序等；
b) 对可能存在证据数据的电子数据存储介质进行拍照，编号并贴上标签标识；
c) 证据的获取应符合 GA/T 756—2008 中证据数据发现提取固定步骤的要求；

d) 计算获取的证据数据文件和原始的证据数据文件的哈希值，验证两者的一致性，确保所获取的证据数据文件和原始的证据数据文件是相同的。

7.2 证据数据的检验分析

7.2.1 检验分析过程

电子数据法庭科学鉴定中，证据数据的检验分析过程应符合以下要求：

a) 在鉴定过程中应记录鉴定内容、操作条件、原始观察结果、计算和取得的数据等，作为鉴定结果的来源；

b) 检验分析所参照的基本原理、技术方法和标准规范应被证明是正确、成熟和可靠的，已经被广大同行所接受和认可。

7.2.2 检出数据

电子数据法庭科学鉴定的检出数据应注意：

a) 记录文件的哈希值，记录检出文件哈希值的文件应保证其完整性并作为过程记录保存；

b) 复制到专用的电子数据存储介质中，并检验数据的完整性。

7.3 记录

电子数据法庭科学鉴定中，记录应贯穿整个鉴定过程，所有记录应注意：

a) 委托、受理检材的移交、存放、使用和归还应登记，登记记录应妥善保存以便随时查阅；

b) 可以用摄像、截屏、照片、文档等方式存放于任何一种存储介质中；

c) 应实时有效、清晰明了，应包含足够的信息，以便于鉴定、检验工作可以追溯、重复；

d) 鉴定过程中的所有记录在完成鉴定后应随案卷及时归档，妥善保存。

8 鉴定结论和意见

鉴定结论和意见应符合以下要求：

a) 直接、明确的对委托事项进行答复；

b) 结论准确无误，不允许使用有歧义的字、词、句；

c) 文字简练，用词准确，语句通顺，描述确切无误；

d) 语气上客观中立，不应出现明显带有感情色彩的字、词、句；

e) 使用统一的专业术语；

f) 使用国家标准计量单位和符号，使用国家标准简体汉字；

g) 必要时应附有图表、照片、参考文献等说明性附件。

中华人民共和国公共安全
行业标准
电子数据法庭科学鉴定通用方法
GA/T 976—2012
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100013)
北京市西城区三里河北街16号(100045)
网址 www.spc.net.cn
总编室:(010)64275323 发行中心:(010)51780235
读者服务部:(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 0.5 字数 7 千字
2012年4月第一版 2012年4月第一次印刷
*
书号:155066·2-23318 定价 14.00元

GA/T 976-2012