ICS 35.220.20
CCS A 90

GA

中华人民共和国公共安全行业标准

GA/T 756—2021
代替 GA/T 756—2008

法庭科学　电子数据收集提取技术规范

Forensic sciences—Technical specifications for collection and acquisition of digital evidence

2021-10-14 发布　　2022-05-01 实施

中华人民共和国公安部　　发 布

中华人民共和国公共安全
行业标准
法庭科学　电子数据收集提取技术规范
GA/T 756—2021
*
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(100029)
北京市西城区三里河北街16号(100045)
网址:www.spc.org.cn
服务热线:400-168-0010
2022年3月第一版
*
书号:155066·2-36532

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件代替GA/T 756－2008《数字化设备证据数据发现提取固定方法》，与GA/T 756－2008相比，除编辑性修改外，主要技术变化如下：

——更改了范围（见第1章，2008年版的第1章）；

——更改了规范性引用文件（见第2章，2008年版的第2章）；

——删除了术语和定义“数字化设备”“本地数字化设备”“远程数字化设备”“证据数据”“证据数据发现提取”“固定证据数据”“逐比特一致”“含义一致”“可再现数据”“不可再现数据”“证据数据原始性”“证据数据完整性”“哈希值”“原始电子数据存储介质”“检验用例”（见2008年版的3.1、3.1.1、3.1.2，3.2～3.13）；

——增加了术语和定义“计算机信息系统”“本地计算机信息系统”“电子数据收集提取”“冻结”（见3.1～3.4）；

——增加了记录检材情况内容（见4.1.1、4.1.2）；

——更改了“设计检验用例”，标题名称改为“收集提取方法”，并更改了部分内容[见4.2、4.2.1～4.2.11，2008年版的4.2、4.2 a)～ c)]；

——更改了“发现提取固定证据数据”，标题名称改为“收集提取电子数据的步骤”，并更改了部分内容[见4.3、4.3.1～4.3.9，2008年版的4.3、4.3 a)～ k)]；

——更改了“检验记录”，标题名称改为“记录”，并更改了部分内容（见第5章、5.1～5.6，2008年版的4.4、4.4.1～4.4.4）；

——增加了“收集提取结果表述”（见第6章）。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由全国刑事技术标准化技术委员会电子物证检验分技术委员会（SAC/TC 179/SC 7）提出并归口。

本文件起草单位：公安部网络安全保卫局、大连市公安局、天津市公安刑事侦查局、司法鉴定科学研究院、厦门市美亚柏科信息股份有限公司。

本文件主要起草人：许剑卓、刘晓宇、何星、翟晓飞、侯钧雷、刘浩阳、范玮、田钊、万江山、吴倩、王艺筱、姚伟、姜有亮、朱国锋、郭弘、张辉极。

本文件所代替文件的历次版本发布情况为：

——GA/T 756—2008。

法庭科学　电子数据收集提取技术规范

1　范围

本文件规定了法庭科学领域中电子数据收集提取的术语和定义、通用要求、收集提取步骤、收集提取记录、结果表述。

本文件适用于法庭科学领域中电子数据的收集提取。

2　规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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。

GB/T 31167　信息安全技术　云计算服务安全指南

GA/T 754　电子数据存储介质复制工具要求及检测方法

GA/T 755　电子数据存储介质写保护设备要求及检测方法

GA/T 1069　法庭科学　电子物证手机检验技术规范

GA/T 1174　电子证据数据现场获取通用方法

GA/T 1476　法庭科学远程主机数据获取技术规范

GA/T 1478　法庭科学网站数据获取技术规范

GA/T 1568　法庭科学　电子物证检验术语

3　术语和定义

GB/T 31167 和 GA/T 1568 界定的以及下列术语和定义适用于本文件。

3.1

计算机信息系统　computer information system

具备自动处理数据功能的系统，包括计算机、网络设备、通信设备、自动化控制设备及其包含的软件系统等。

3.2

本地计算机信息系统　local computer information system

收集提取人员能物理接触、操作的计算机信息系统。

3.3

电子数据收集提取　collection and acquisition of digital evidence

对计算机信息系统中存储、处理、传输的电子数据进行搜索、分析、截获，并对收集提取的电子数据进行完整性校验的过程。

3.4

冻结　freeze

将计算机信息系统中的数据在特定时间以特定状态进行固定，保证其不再改变的措施。