ICS 35.240.01
A 92

GA

中华人民共和国公共安全行业标准

GA/T 1174—2014

电子证据数据现场获取通用方法

General methods for capture of live electronic evidence data

2014-07-09 发布　　2014-07-09 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。

本标准由公安部第三研究所提出。

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：公安部第三研究所。

本标准主要起草人：张颖、金波、郭弘、黄道丽、崔宇寅、雷云婷。

电子证据数据现场获取通用方法

1 目的和范围

本标准规定了电子证据数据现场搜索、获取、固定和保存的通用方法。

本标准适用于在电子数据现场取证的工作中，搜索、获取、固定和保存电子证据数据。

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 756—2008 数字化设备证据数据发现提取固定方法

GA/T 976—2012 电子数据法庭科学鉴定通用方法

3 术语和定义

GA/T 756—2008 和 GA/T 976—2012 界定的以及下列术语和定义适用于本文件。

3.1

随机存取内存转储 random access memory dump (RAM dump)

将随机存取内存(RAM)中的部分或者全部内容传送到某种类型的存储介质上。

3.2

逻辑文件 logical file

用户所观察到的文件组织形式，是可以直接处理的数据及结构。

4 步骤

4.1 制定证据获取方案

在进行电子证据数据现场获取之前，需制定详细的计划，包括：

a) 现场获取的目的和范围；

b) 参加电子证据数据现场获取的人员，需明确分工，落实责任；

c) 进行电子证据数据现场获取需携带的移动仪器设备；

d) 现场获取采用的方法和步骤；

e) 电子证据数据现场获取的顺序；

f) 现场获取操作可能造成的影响。

4.2 记录现场状况

对现场状况应通过拍照和录像的方式进行记录，并予以编号保存。

4.3 电子设备和存储介质的封存

对于已经关闭的系统，在法律允许的范围内并在获得授权的情况下，应对相关电子设备和存储介质