ICS 13.310
A 92

GA

中华人民共和国公共安全行业标准

GA/T 1476—2018

法庭科学远程主机数据获取技术规范

Technical specifications for remote host data acquisition in forensics

2018-04-13 发布　　2018-04-13 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。

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这些专利的责任。

本标准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。

本标准起草单位:公安部网络侦察技术研发中心、上海弘连网络科技有限公司、盘石软件(上海)有限公司、厦门美亚柏科信息股份有限公司。

本标准主要起草人:刘晓宇、翟晓飞、陆道宏、宋庆飞、赵庸。

法庭科学远程主机数据获取技术规范

1 范围

本标准规定了以远程访问的方式获取远程主机数据的方法。

本标准适用于法庭科学领域电子物证检验中对远程主机数据的获取检验。

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。

GB/T 5271.1—2000 信息技术 词汇 第1部分：基本术语

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

GA/T 977—2012 取证与鉴定文书电子签名

3 术语和定义

GB/T 5271.1—2000、GA/T 756—2008、GA/T 976—2012 和 GA/T 977—2012 界定的以及下列术语和定义适用于本文件。

3.1

远程主机 remote host

通过网络进行访问、远端控制的计算机。

3.2

虚拟主机 virtual host

在网络服务器上分出一定的磁盘空间，供用户放置站点、应用组件等，以提供必要的站点功能、数据存放和传输功能。

4 检验步骤

4.1 时间校对

在远程主机数据获取时，应与国家授时中心等标准时间源进行时间校对，记录准确的开始时间和结束时间。

4.2 远程主机外部网络信息记录

查询并记录相关的域名信息、路由跟踪信息以及常用服务端口开放情况等。

4.3 远程主机操作系统信息获取

4.3.1 系统基本信息和授权用户信息

使用提供的用户名/密码进行远程主机访问，记录系统当前时间、开机时间、操作系统版本、当前连