



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

接用户、系统配置、系统运行环境等基本信息。

4.3.2 远程主机网络信息

查询并记录主机的网络配置、网络侦听端口、当前网络连接等。

4.3.3 自启动项和远程主机服务信息记录

查询并记录远程主机开启的自启动项和服务信息,以及系统内运行的进程/线程信息。

4.3.4 用户信息

查询并记录远程主机的用户列表,同时提取每个用户的创建时间、用户目录、哈希密码、最后访问时间等信息。

4.3.5 操作系统日志

查询并记录操作系统日志数据信息,包括但不限于系统日志、安全日志。

4.4 远程主机网站数据获取

获取远程主机中网站服务器数据,包括程序名称、程序版本、配置文件、虚拟主机、网站内容文件、网站访问日志等。

4.5 远程主机数据库获取

4.5.1 数据库服务器基本信息记录

根据进程和系统配置信息,提取并记录远程服务器上的数据库应用基本信息,包括服务器程序名称、版本、服务器侦听的端口、服务器启动的参数、数据存放位置等。

4.5.2 数据库信息获取

提取并记录各个数据库的基本信息,包括数据库容量、数据表数量、数据表名称、每个数据表的记录数、每个表的结构等。

4.5.3 数据库用户信息显示

提取并记录各个数据库用户的信息,包括用户名称、权限配置等。

4.5.4 数据库数据获取

选择性提取各个数据库的数据以及数据库日志信息。

4.6 远程主机存储介质和文件获取

4.6.1 一般原则

在需要的情况下,宜获取远程主机存储介质和文件数据。

4.6.2 远程主机存储介质基本信息

查询并记录远程存储介质基本信息,包括存储介质大小和分区信息。

4.6.3 远程主机存储介质获取

选择性获取远程主机的整个存储介质或存储介质中的指定分区数据,数据的获取采用位对位的复

制方式,保证整个存储介质或分区数据的数据完整性。

4.6.4 远程主机文件获取

可选择获取分区中指定目录的文件或者整个目录,获取结果应记录完整路径。

4.7 数据获取处理

4.7.1 断点续传处理

对于不稳定的网络状态或其他意外情况,可多次连续获取相关的数据,但应保证获取数据的完整性。

4.7.2 获取数据的打包和压缩

对于多个文件或者目录的情况,可进行打包或压缩处理,但应保证获取数据的完整性。

4.8 数据完整性保护和验证

远程主机获取的数据,需进行完整性校验。

4.9 过程日志记录

远程主机数据获取过程应采取屏幕录像、摄像和文字记录等方式对关键步骤进行记录。

4.10 检验结果保存

将检出数据采用封盘刻录方式刻录在不可擦写的空白光盘上或者保存在专用存储介质中,并计算检出数据的哈希值。

5 检验记录

远程主机数据获取检验记录包括开始时间和结束时间、远程主机基本信息、远程主机上获取的各项数据、数据文件的完整性校验、过程录像和日志记录等。

6 检验结果表述

检验结果表述应符合以下规定:

- a) 检验结果分为检出、未检出、不具备检验条件 3 种;
 - b) 检验结果应根据检验要求对检验对象、检验范围、检验所得进行客观、概括、有针对性的描述;
 - c) 结果表述应包含检材编号、检出情况、检出数据文件或保存检出数据介质哈希值、保存检出数据介质编号等必要信息。
-