



# 中华人民共和国公共安全行业标准

GA/T 1176—2014

---

## 网页浏览器历史数据检验技术方法

Technical methods for examination of web browser history 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：孙永清、林九川、金波、郭弘、黄道丽、沙晶、蔡立明。

# 网页浏览器历史数据检验技术方法

## 1 范围

本标准规定了从网页浏览器中提取历史数据,并对提取的历史数据进行固定保全和检验分析的技术方法。

本标准适用于电子数据检验鉴定工作中,提取、固定和检验网页浏览器历史数据。

## 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

RFC 1738 国际工程任务组织(IFTF)对统一资源定位器的详细说明

## 3 术语和定义

下列术语和定义适用于本文件。

### 3.1

**网页浏览器 web browser**

一种访问和展示互联网信息资源的网络应用软件,通过该软件可向 web 服务器发送各种请求,并对从服务器发来的超文本信息和各种多媒体数据格式进行解释、显示和播放。

### 3.2

**网页浏览器缓存 web browser cache**

一些临时保存网页浏览器最近访问信息的文档,当访问者再次请求这个页面时,网页浏览器就从本地磁盘显示文档。

### 3.3

**网站 website**

在互联网上,根据一定的规则制作的,用于展示特定内容的相关网页的集合,网站可用于展示内容和提供网络服务,展示的内容包括文本、视频、声音、图片等。

### 3.4

**历史数据 history data**

访问者通过网页浏览器访问网站留下的数据记录,既包括访问者本地的缓存文件、历史记录、临时文件等,也包括服务器端和代理服务器的日志记录等。

### 3.5

**统一资源标志符 uniform resource identifier(URI)**

对互联网上的资源进行统一定位的字符串,并规定了所有协议都必须遵循的通用文法规则。

### 3.6

**统一资源定位符 uniform resource locator(URL)**

RFC 1738 中规定的用于描述互联网上可用资源的字符串,也称网页地址。

### 3.7

#### 泄漏记录 leak record

记录在网页浏览器缓存中的记录,当删除访问过的 URL 记录时,如果缓存记录没有被删除,就会产生一条泄漏记录。

## 4 检验步骤

### 4.1 记录检材情况

对送检检材情况进行详细的记录,包括:

- a) 对送检检材进行唯一性编号;
- b) 对送检检材进行逐一拍照,并记录检材特征;
- c) 对具备保全条件的送检检材进行保全备份,保全备份应按照各种电子数据存储介质复制工具的使用说明书进行操作。

### 4.2 制定历史数据获取方案

在进行历史数据获取之前,需制定详细的获取方案,包括:

- a) 历史数据的获取目的和范围;
- b) 产生历史数据的网页浏览器的名称和版本;
- c) 运行网页浏览器的操作系统名称和版本;
- d) 历史数据的保存路径和文件格式;
- e) 获取历史数据需用到的软硬件设备;
- f) 规定历史数据获取的顺序;
- g) 如需要对浏览内容进行溯源,要制定溯源的范围和注意事项;
- h) 如果有条件从代理服务器或网站服务器获取历史数据,需明确获取范围;
- i) 由于检材或网页浏览器对象不同,而需特别注意的事项;
- j) 如需获取已删除的历史数据,应制定数据恢复的方法。

### 4.3 发现提取历史数据

从送检检材中发现提取历史数据,形成可供检验的数据文件,包括:

- a) 按照 4.2 中制定的方案和 GA/T 756—2008 对发现提取固定证据数据的要求,对网页浏览器历史数据进行发现提取;
- b) 在检材中相同文件目录下的历史数据,应保存在同一文件目录下,并记录检材中的目录全路径;不同文件目录下的历史数据,应保存在不同文件目录下;
- c) 计算获取的历史数据文件和原始的历史数据文件的哈希值,验证一致性,确保两者是相同的。

### 4.4 网页浏览器历史数据的检验

对 4.3 发现提取的历史数据文件进行检验,包括:

- a) 将获取的历史数据文件导出为检出文件,记录检出文件的哈希值;
- b) 保存检出文件的哈希值到文件中,保证其完整性并作为过程记录保存下来;
- c) 将检出文件复制到专用的电子数据存储介质中,并检验数据的完整性;
- d) 对历史数据文件进行分析,可依据但不限于以下数据内容:
  - 1) 网页浏览器缓存文件头,该文件头包含了网页浏览器的版本信息;
  - 2) 访问 URL 时收到的 http 头;

- 3) 用户通过网页浏览器曾经访问过的 URL 记录;
- 4) 用户直接和通过重定向方式访问过的 URL 记录。
- 5) 被保存的网站文件的最后修改时间;
- 6) 访问网站的时间;
- 7) 网站对应的本地文件夹和文件名称;
- 8) 网页浏览器缓存位置的非网页文件,如扩展名为 rar、doc 和 pdf 等格式的文件;
- 9) 泄漏记录;
- 10) 特定网站的访问内容;
- 11) 服务器和本地数据的对比;
- 12) 伪造数据检验;
- 13) cookie 信息检验。

#### 4.5 记录

在网页浏览器历史数据检验中,应按照 GA/T 756—2008 中检验记录的要求,记录整个检验过程。

### 5 检验报告

检验报告应包含所有与案件相关的必要信息,并列出检验结果。检验报告应包含以下信息:

- a) 获取网页浏览器历史数据目的和范围;
  - b) 发现提取网页浏览器历史数据的过程和结果;
  - c) 网页浏览器历史数据的分析检验结果。
-

中华人民共和国公共安全  
行业标准  
网页浏览器历史数据检验技术方法  
GA/T 1176—2014

\*

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.net.cn](http://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 8 千字  
2014年9月第一版 2014年9月第一次印刷

\*

书号: 155066·2-27346 定价 14.00 元

如有印装差错 由本社发行中心调换  
版权专有 侵权必究  
举报电话:(010)68510107



GA/T 1176-2014