ICS 35.240.01
A 92

GA

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

GA/T 1176—2014

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
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

GA/T 1176-2014

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

对送检检材情况要进行详细的记录，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；

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。