d） 照片。

6.2 检验过程记录

即时通讯记录检验中，记录应贯穿整个检验过程，记录应包括：

a） 检验过程中所使用的软、硬件工具；

b） 在搭建环境的过程中检出的检验内容、操作条件、原始观察结果、计算和取得的数据等；

c） 根据获取的即时通讯记录文件计算出的哈希值。

GA/T 1173—2014

ICS 35.240.01
A 92

GA

中华人民共和国公共安全行业标准

GA/T 1173—2014

即时通讯记录检验技术方法

Technical methods for examination of instant messaging data

2014-07-09 发布　　2014-07-09 实施

中华人民共和国公安部　发布

版权专有　侵权必究

*
书号：155066・2-27343
定价：　14.00 元

GA/T 1173-2014

4.3.2 即时通讯记录文件的环境分析

即时通讯记录文件的环境分析，包括以下内容：

a） 即时通讯记录文件等的存放路径；

b） 即时通讯客户端或者浏览器的配置信息；

c） 即时通讯客户端或者浏览器涉及的日志文件。

4.3.3 即时通讯记录文件的属性信息分析

即时通讯记录文件的属性信息分析，包括以下内容：

a） 包括文件名、文件格式、创建时间和修改时间等；

b） 即时通讯记录文件属性与其他文件属性的关联；

c） 即时通讯记录文件属性与即时通讯内容是否存在矛盾。

4.3.4 即时通讯记录的文件结构分析

即时通讯记录的文件结构分析，包括以下内容：

a） 文件呈现的拼接痕迹；

b） 文件结构的完整性；

c） 文件结构的规范性。

4.3.5 即时通讯记录的上下文语义环境分析

即时通讯记录的上下文语义环境分析，包括以下内容：

a） 语义的连续性和同一性；

b） 语义的关联性和逻辑性；

c） 语义的自然度与话题的匹配性。

5 结论表述

根据即时通讯记录的检验步骤阐述检验结果，可以包括以下内容：

a） 即时通讯记录文件固定保全的实现情况；

b） 即时通讯记录的检出结果；

c） 客户端与服务器端即时通讯记录的验证结果；

d） 针对即时通讯记录的真实性分析，结论可以是以下四种之一：

1） 发现修改；

2） 没有发现修改；

3） 没有修改；

4） 不能判定。

6 检材记录

6.1 记录检材相关信息

应记录检材的以下信息：

a） 类别；

b） 型号；

c） 出厂时唯一性编号（如果适用）；

中华人民共和国公共安全
行 业 标 准
即时通讯记录检验技术方法
GA/T 1173—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 10 千字
2014年9月第一版 2014年9月第一次印刷
*
书号:155066·2-27343 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

4 检验步骤

4.1 即时通讯记录文件的固定保全

4.1.1 确定检材

确定检材的步骤：

a) 对可能存在即时通讯记录的检材进行唯一性标识，并贴上标签；

b) 对检材拍照，并记录检材的特征。

4.1.2 获取即时通讯记录文件

根据检材，应选用适当的仪器设备，按照 GA/T 756—2008 的要求获取即时通讯记录文件：

a) 获取即时通讯记录文件的步骤：

1) 检验即时通讯客户端

查找检材中即时通讯中客户端的安装路径和相关用户目录存放路径，获取客户端的版本、用户相关信息和即时通讯记录文件；

2) 检验易失性即时通讯

查找并获取检材中浏览器的版本和浏览器缓存中即时通讯记录文件；

3) 服务器端即时通讯记录的检出

根据检材中检出的用户即时通讯账号，在有条件的情况下获取该用户在服务器端存储的即时通讯记录。

b) 计算并校验获取的即时通讯记录文件。

4.2 即时通讯记录的呈现

4.2.1 搭建检验环境

检验环境应包括：

a) 针对即时通讯客户端软件版本搭建检验环境；

b) 即时通讯记录文件为加密文件时需搭建解密环境。

4.2.2 客户端即时通讯记录的检出

根据搭建的环境将即时通讯记录检出至特定文件，检出的内容应包括：

a) 即时通讯客户端的名称、安装路径；

b) 用户目录存放路径；

c) 用户即时通讯账号、即时通讯中的昵称和即时通讯账号中关联的邮件、手机等相关信息；

d) 即时通讯历史记录和即时通讯中传递的文件、图片等；

e) 检出的文件的哈希值。

4.3 即时通讯记录的真实性分析

4.3.1 客户端与服务器端即时通讯记录的验证

验证客户端与服务器端即时通讯记录，包括以下内容：

a) 将客户端即时通讯记录与服务器端即时通讯记录的内容进行比对；

b) 将两者内容不符的部分进行分析阐述。

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、北京市公安局刑侦总队。

本标准主要起草人：高峰、郭弘、金波、徐隽、姚波、邱敏。