

司法鉴定技术规范

SF/Z JD0402003——2015

即时通讯记录检验操作规范

2015-11-20 发布

2015-11-20 实施

中华人民共和国司法部司法鉴定管理局 发布

目 次

前言..... I

1 目的和范围..... 1

2 规范性引用文件..... 1

3 术语和定义..... 1

4 原则..... 1

5 检验步骤..... 1

6 检验记录..... 3

7 结论表述..... 3

前 言

本技术规范按照GB/T 1.1-2009给出的规则起草。

本技术规范由上海辰星电子数据司法鉴定中心提出。

本技术规范由司法部司法鉴定管理局归口。

本技术规范起草单位：上海辰星电子数据司法鉴定中心。

本技术规范主要起草人：蔡立明、高峰、林九川、沙晶、雷云婷、孙杨。

本技术规范为首次发布。

即时通讯记录检验操作规范

1 目的和范围

本技术规范规定了即时通讯记录检验的技术方法和步骤。

本技术规范适用于在电子数据检验鉴定中的即时通讯记录鉴定。

2 规范性引用文件

下列文件对于本技术规范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技术规范。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本技术规范。

SF/Z JD0400001—2014 电子数据司法鉴定通用实施规范

3 术语和定义

SF/Z JD0400001—2014 电子数据司法鉴定通用实施规范所确立的以及下列术语和定义适用于本技术规范。

3.1

即时通讯 Instant messaging

即时通讯是一种使用网络进行实时交互信息（包括在实时条件下支持离弦、延时功能）的集声音、文字、图像等的综合性交流方式。

3.2

即时通讯客户端 Instant messaging client

安装在计算机、手机、智能设备等终端上的用于提供即时通讯服务的应用程序。

3.3

即时通讯协议 Instant messaging protocol

对即时通讯过程及数据传输进行控制的规则。

3.4

即时通讯记录 Instant messaging data

即时通讯中所传递的文字消息、传输的文件、通话记录和声像信息等。

3.5

即时通讯记录文件 Instant messaging data file

存储即时通讯记录的数据文件。

4 原则

SF/Z JD0400001—2014 电子数据司法鉴定通用实施规范所确立的原则适用于本技术规范。

5 检验步骤

5.1 了解相关情况

- 5.1.1 了解即时通讯记录的形成过程及存储方式等信息。
- 5.1.2 当即时通讯记录文件采用了加密方式保存时，了解即时通讯记录文件的加解密方式。
- 5.1.3 当无法读取通讯记录文件时，了解即时通讯客户端用户帐号及其口令信息，并获得其使用授权。

5.2 固定保全

5.2.1 确定检材的步骤

- a) 对检材进行唯一性标识，并贴上标签；
- b) 对检材进行拍照或录像，记录其特征；
- c) 对具备条件的检材进行保全备份，并进行完整性校验，之后使用备份数据进行检验。

5.2.2 即时通讯记录文件的获取

- a) 如有必要，应按照相关技术方法，搜索、恢复保存在存储介质上的即时通讯记录文件；
- b) 查找检材中即时通讯客户端的安装路径及相关用户信息存储位置，获取即时通讯客户端的版本、用户相关信息和即时通讯记录文件；
- c) 对于基于浏览器的即时通讯客户端，应查找并获取检材中浏览器的版本和浏览器缓存中的易失性即时通讯记录；
- d) 在条件允许的情况下，获取存储在服务器端的即时通讯记录；
注：在获取时不得删除保存在服务器上的即时通讯记录。
- e) 计算即时通讯记录文件的哈希值。

5.3 即时通讯记录的呈现

5.3.1 搭建检验环境

检验环境应包括：

- a) 针对获取的不同种类的即时通讯记录文件，安装相应的即时通讯客户端或搭建能正常读取即时通讯记录文件的检验环境；
- b) 当即时通讯记录文件采用了加密方式保存，需搭建解密即时通讯记录文件检验环境。

5.3.2 即时通讯记录相关信息的呈现

根据搭建的检验环境将即时通讯记录内容导出并保存为特定文件，计算导出文件的哈希值，检出的内容可以包括：

- 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) 用户即时通讯帐号、即时通讯中用户的昵称和即时通讯帐号中关联的邮件、手机等相关信息；
- d) 即时通讯记录内容和即时通讯中传递的文件、图片、语音等。

5.4 即时通讯记录的真实性检验和分析

根据检材即时通讯记录具体情况，视需要对下列全部或部分内容进行检验和分析。

5.4.1 即时通讯记录基本信息检验

检验即时通讯记录文件及其所在目录中其它即时通讯记录文件的结构、格式、内容、即时通讯对象、时间等情况。

5.4.2 即时通讯记录文件的环境分析

根据即时通讯记录的存储环境，检验分析即时通讯记录文件的存放路径、即时通讯客户端或浏览器的配置信息、日志文件等是否存在异常。

5.4.3 即时通讯记录正文分析

分析即时通讯记录的正文信息是否存在异常。重点关注正文的结构及内容的合理性和逻辑性等情况。

5.4.4 即时通讯记录文件的属性信息分析

检验即时通讯记录文件的文件名、文件格式、创建时间和修改时间等信息，分析即时通讯记录文件属性与其它文件属性以及即时通讯内容等是否存在矛盾。

5.4.5 其它相关信息分析

在检材中搜索即时通讯记录文件及即时通讯中传递的文件、图片等信息中出现的关键词和文件，分析搜索到的内容与即时通讯记录是否存在关联，相互之间的逻辑关系是否存在矛盾。

5.4.6 即时通讯服务器分析

如条件允许，对即时通讯服务器进行检验，分析其中的相关信息与检材即时通讯记录是否存在矛盾。包括保存在服务器上的即时通讯记录文件、服务器日志及备份数据等。

5.4.7 实验分析

若发现即时通讯记录存在异常现象，应按照检材环境进行实验，分析产生这些异常现象的原因，以确定这些现象的性质。

6 检验记录

与检验活动有关的情况应及时、客观、全面地记录，保证检验过程和检验结果的可追溯性。检验记录应反映出检验人、检验时间、审核人等信息。检验记录的主要内容有：

- a) 检材固定保全情况：包括检材照片或录像、登录即时通讯客户端和提取即时通讯记录文件截图或录像、检材及即时通讯记录文件的哈希值等；
- b) 检验设备和工具情况；
- c) 检验过程和发现；
- d) 对检验发现的分析和说明；
- e) 其它相关情况。

7 结论表述

根据即时通讯记录的检验步骤阐述检验结果，可以包括如下内容：

- a) 即时通讯记录文件固定保全的情况；
- 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) 即时通讯记录的真实性结论，结论可以是以下四种之一：

- 1) 确定经过伪造篡改；

判断依据：发现即时通讯记录存在异常，并分析这些异常为伪造篡改形成。

- 2) 排除经过伪造篡改;
判断依据: 未发现即时通讯记录存在异常, 并分析不存在通过现有技术手段无法发现的伪造篡改可能性。
 - 3) 未发现经过伪造篡改;
判断依据: 未发现即时通讯记录存在异常或发现的异常能够得到合理解释, 但尚不能完全排除存在根据现有技术手段难以发现的伪造篡改痕迹的可能性
 - 4) 无法判断是否经过伪造篡改。
判断依据: 即时通讯记录存在异常, 但无法准确判断其性质或形成原因; 或检材即时通讯记录信息量过少, 无法形成明确性意见; 或其它经综合分析亦无法形成明确性意见。
-