司　法　鉴　定　技　术　规　范

SF/Z JD0404001——2018

伪基站检验操作规范

2018-11-08 发布　　2019-01-01 实施

中华人民共和国司法部公共法律服务管理局　发布

目　次

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公共法律服务管理局归口。

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，沙晶，杨涛，郭弘，张晓，崔宇寅。

本技术规范为首次发布。

伪基站检验操作规范

1 范围

本技术规范规定了伪基站检验的技术方法和步骤。

本技术规范适用于电子数据司法鉴定领域中伪基站的检验。

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。

SF/Z JD0100000-2012 电子数据司法鉴定通用实施规范

3 术语和定义

SF/Z JD0100000-2012 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

基站 base station

基站即公用移动通信基站，是指在一定的无线电覆盖区中，通过移动通信交换中心，与移动电话终端之间进行信息传递的无线电收发信电台。

3.2

伪基站 pseudo base station

伪基站即假基站，一般由发射主机、伪基站主控端及伪基站软件等部分组成。通过搜取以其为中心一定半径范围内的手机信息，干扰或屏蔽一定范围内的运营商信号，并伪装成运营商的基站，冒用任意号码强行向不特定用户发送信息。

3.3

伪基站主控端 controller of pseudo base station

指伪基站控制设备，通常为便携式计算机，并安装有伪基站软件。

3.4

国际移动用户识别码 IMSI

区别移动用户的标志，储存在SIM卡中，是用于区别移动用户的有效信息。

3.5

伪基站电子数据　　data of pseudo base station

指伪伪基站主控端中存储的电子数据，一般包括伪基站发送信息的内容、伪基站信息发送IMSI记录及日志等数据。

4　鉴定步骤

4.1　固定保全

——对送检伪基站设备进行惟一性标识，并贴上标签；
——对送检伪基站设备进行拍照或录像，记录其特征；
——对送检伪基站主控端中的硬盘进行保全备份，并进行完整性校验，将复制生成的克隆或镜像文件作为检验对象。

4.2　电子数据检验

4.2.1　若伪基站主控端能正常开机，应先检验伪基站主控端的系统时间，并与北京时间进行校对，避免检出的涉案数据生成时间与实际不符。
4.2.2　检验伪基站主控端中的伪基站软件，将伪基站软件中的电子数据（如数据库中的数据）导出并保存在专用的存储介质中。
4.2.3　检验伪基站软件的日志记录文件，提取并固定日志记录文件中的伪基站短信发送内容、伪基站短信发送 IMSI 记录等数据。
4.2.4　若检材中的伪基站电子数据已被删除，可先使用数据恢复工具进行数据恢复，再从中提取并固定伪基站短信发送内容、伪基站短信发送 IMSI 记录等数据。
4.2.5　必要时可通过关键词搜索的方式，搜索检材中的伪基站电子数据，根据搜索结果提取并固定伪基站短信发送内容、伪基站短信发送 IMSI 记录等数据。
4.2.6　检验系统日志及其它与伪基站短信发送相关的文件，提取并固定其中的伪基站电子数据。
4.2.7　整理并分析提取的伪基站电子数据，统计与伪基站短信发送相关的信息，计算导出文件的哈希值。

4.3　短信发送功能检验

4.3.1　若送检伪基站设备中包含发射主机、伪基站主控端及发射天线等伪基站短信发送必要设备，可对伪基站的短信发送功能进行功能检验。
4.3.2　根据伪基站设备（包括发射主机、伪基站主控端及发射天线等）的实际情况，在能正常收发无线电信号的环境中连接配置各设备，并准备可接收短信的测试手机，搭建伪基站短信发送功能检验的检验环境。
4.3.3　在伪基站主控端的伪基站软件中编辑测试短信，并设置测试参数（如频点、运营商、模式等），发送测试短信。
4.3.4　检验测试手机是否收到测试短信。

5　检验结果及表述

5.1　伪基站电子数据检验结果及表述

——检出伪基站相关电子数据，其中包括短信发送内容“xx”个（如存在），伪基站短信发送 IMSI 记录“xx”条（如存在），检出的伪基站相关数据保存在“xx”文件中，文件的哈希值为“xx”；
——未发现伪基站相关电子数据；
——检材不具备伪基站电子数据检验条件。

5.2 伪基站短信发送功能检验结果及表述

——检材具有伪基站的短信发送功能；
——未发现检材具有伪基站的短信发送功能；
——检材不具备伪基站短信发送功能检验条件。