司　法　鉴　定　技　术　规　范

SF/Z JD0403001—2014

软件相似性鉴定实施规范

2014－3－17 发布　　2014－3－17 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

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：金波、郭弘、高峰、张颖、张晓、崔宇寅、蔡立明、黄道丽、沙晶、孙杨、雷云婷、张云集。

本技术规范为首次发布。

软件相似性鉴定实施规范

1 范围

本技术规范规定了软件相似性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工作中的软件的相似性检验。

2 术语和定义

2.1

检材 software for examination

电子数据检验鉴定中需检验的软件。

2.2

样本 software for comparison

电子数据检验鉴定中用于同检材进行比对检验的软件。

2.3

数字化设备 digital device

存储、处理和传输二进制数据的设备，包括计算机、通信设备、网络设备、电子数据存储设备等。

2.4

源代码 source code

未经编译的、按照一定的程序设计语言规范书写的、人类可读的计算机指令语言指令。

2.5

目标程序 object code

编译器或汇编器处理源代码后所生成的、可被直接被计算机运行的机器码集合。

2.6

运行环境 runtime environment

一种把执行码在目标机器上运行的环境。

2.7

哈希值 hash value

使用安全的哈希算法对数据进行计算获得的数据。常用哈希算法包括MD5、SHA1和SHA256等。

2.8

反编译 decompile

将已编译的程序文件还原成汇编或者高级语言代码的过程。

3 仪器设备

3.1 硬件

电子数据存储设备、保全备份设备、检验设备。

3.2 软件

送检软件所需的运行环境、文件比对工具、反编译工具、源代码分析工具等。

4 检验步骤

4.1 记录检材和样本情况

4.1.1 对送检的检材/样本进行唯一性编号，编号方法为 XXXX(年度)-XXX(受理号)-XX(流水号)，如 2012-39-2 表示 2012 年受理的编号 39 案件的第 2 个检材。

4.1.2 对检材/样本为数字化设备的，对数字化设备进行拍照，并记录其特征。

4.2 检材和样本的保全备份

对具备保全条件的检材和样本进行保全备份，并计算保全备份的副本或镜像的哈希值。

4.3 检验项目的选择

分析检材和样本，根据检材和样本的内容选择以下一项或多项内容进行检验:

a) 源代码间的比对；
b) 目标程序间的比对；
c) 源代码和目标程序间的比对；
d) 文档的比对（如适用）；
e) 文档和源代码/目标程序间的比对。

注：文档包括开发文档、需求说明书、总体设计方案、详细设计方案等。

4.4 程序的比对检验

4.4.1 要求

对检材和样本进行比对检验时，需先排除影响比对的内容（如公共程序库文件、第三方库文件和GNU通用公共许可的程序等）。

4.4.2 源代码间的比对

对检材和样本的源代码的目录结构、文件名、文件内容、变量、函数、宏定义等进行比对检验。检验时，应排除自定义的文件名、变量名、函数名等名称被修改的影响，对程序逻辑与结构等内容进行比对检验。

4.4.3 目标程序间的比对

分别对检材和样本中的目标程序文件计算哈希值。若所有对应文件的哈希值相同，则软件相同。若对应文件的哈希值不相同，按下列步骤进行：

a) 安装程序检验（如适用），对检材和样本的安装程序进行下列比对检验：
   1) 目录结构及目录名；
   2) 各组成文件的文件名、文件哈希值、文件内容、文件结构和文件属性等。
b) 安装过程检验（如适用）

分别运行检材和样本的安装程序，观察安装过程的屏幕显示、软件信息、使用功能键后的屏幕显示以及安装步骤，并进行比对检验。

c） 安装后的程序检验，对安装成功的检材和样本的程序进行下列比对检验：
   1） 安装后产生的目录结构及目录名；
   2） 安装后产生的文件的文件名、文件哈希值、文件内容、文件结构和文件属性等；
   3） 安装后的软件的配置过程和运行方式。
d） 程序的使用过程检验：运行该程序，对使用过程中的屏幕显示、功能、功能键和使用方法等进行比对检验。
e） 核心程序的逆向分析：必要时，对目标程序的核心程序进行反编译，对反编译后的代码进行比对检验。

4.4.4 源代码和目标程序间的比对

将源代码编译成目标程序后再进行比对检验，检验过程按照目标程序间的比对进行。

注：源代码编译过程中，由于编译软件、编译环境等不同，相同的源代码每次编译产生的文件可能会有差异。

4.5 文档的比对

对检材和样本的文档的目录结构、内容以及属性进行比对。

5 检验记录

5.1 与鉴定活动有关的情况应及时、客观、全面地记录，保证鉴定过程和结果的可追溯性。

5.2 对于检材/样本为数字化设备的，应记录：
   a） 检材/样本的类别；
   b） 检材/样本的型号；
   c） 检材/样本出厂时的唯一性编号（如适用）；
   d） 检材/样本的固件版本号（如适用）；
   e） 检材/样本中软件的名称、版本等属性信息（如适用）；
   f） 检材/样本的照片。

5.3 对于检材/样本为独立于数字化设备的软件的，应记录：
   a） 软件的名称、版本、大小等属性信息；
   b） 软件的哈希值；
   c） 软件的运行环境。

5.4 对于检验的结果，应记录：
   a） 检材与样本的相同部分，如目录结构、目录名、文件、文件名、文件内容等；
   b） 检材与样本的相似部分，如安装或使用过程中的屏幕显示等；

6 检验结果

6.1 列出检材与样本的相似比例，并对存在相同或相似的部分进行说明。

6.2 若检材与样本中存在软件署名、开发者的姓名、单位、废程序段、独特的代码序列等相同时，需在检验结果中单独列出。

7 附则

7.1 对检验用的软件工具的适用性应进行适当确认。

7.2　在检验过程中，检出的数据应存储在专用的存储介质中并妥善保管。

7.3　对送检的检材和样本要做好防震、防水、防磁、防静电等保护。