f) 照片。

6.2 对于检材/样本为独立于数字化设备的软件的，应记录软件的：

a) 名称、版本、大小等属性信息；

b) 哈希值；

c) 运行环境。

6.3 对于检验的结果，应记录检材与样本的：

a) 相同部分，如目录结构、目录名、文件、文件名、文件内容等；

b) 相似部分，如安装或使用过程中的屏幕显示等。

7 检验结果

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。

如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，需在检验结果中单独列出。

8 附则

8.1 对检验用的软件工具的适用性应进行适当确认。

8.2 在检验过程中，检出的数据应存储在专用的存储介质中。

8.3 对送检的检材和样品要做好防震防水防磁防静电等保护。

GA/T 1175—2014

GA/T 1175-2014

*

书号：155066·2-27345

定价： 14.00 元

ICS 35.240.01
A 92

GA

中华人民共和国公共安全行业标准

GA/T 1175—2014

软件相似性检验技术方法

Technical methods for examination of software similarity

2014-07-09 发布 2014-07-09 实施

中华人民共和国公安部 发布

中华人民共和国公共安全
行 业 标 准
软件相似性检验技术方法
GA/T 1175—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:155066·2-27345 定价 14.00 元

5.4.3 目标程序间的比对

5.4.3.1 通则

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

5.4.3.2 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:

a) 目录结构及目录名;

b) 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。

5.4.3.3 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、软件信息以及使用功能键后的屏幕显示以及安装步骤,并进行比对检验。

5.4.3.4 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:

a) 安装后产生的目录结构及目录名;

b) 安装后产生文件的文件名、文件哈希值、文件内容、文件结构和文件属性等;

c) 安装后的软件的配置过程和运行方式。

5.4.3.5 程序的使用过程检验

运行程序,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。

5.4.3.6 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。

5.4.4 源程序和目标程序间的比对

将源程序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。

5.5 文档的比对

对检材和样本的文档的目录结构和内容等进行比对。

6 检验记录

6.1 对于检材/样本为数字化设备的,应记录检材/样本的:

a) 类别;

b) 型号;

c) 出厂时唯一性编号(如适用);

d) 固件版本号(如适用);

e) 软件的名称、版本等属性信息(如适用);

注：常用哈希算法包括 MD5 、SHA1 和 SHA256 等。

3.8

反编译　decompile

将软件中的程序文件还原成汇编或者高级语言代码的过程。

4　仪器设备

4.1　硬件

电子数据存储设备、保全备份设备、检验设备。

4.2　软件

送检软件所需的运行环境、文件比对工具、反编译工具、源程序代码分析工具等。

5　检验步骤

5.1　记录检材和样本情况

内容应包括：

a)　对送检的检材和样本进行唯一性编号；

b)　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。

5.2　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。

5.3　检验项目的选择

分析检材和样本，根据检材和样本的内容应选择以下一项或多项内容进行检验：

a)　源程序间的比对；

b)　目标程序间的比对；

c)　源程序和目标程序间的比对；

d)　文档的比对(如适用)；

e)　文档和源程序/目标程序间的比对。

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。

5.4　程序的比对检验

5.4.1　概述

对检材和样本进行比对检验时，应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)。

5.4.2　源程序间的比对

对检材和样本的源程序代码的目录结构、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、函数名等名称被刻意修改的影响，对程序逻辑与结构等内容进行比对检验。

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由公安部网络安全保卫局提出。

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：公安部网络安全保卫局、公安部第三研究所。

本标准主要起草人：高峰、郭弘、金波、张颖、蔡立明、黄道丽、孙杨。