ICS 35.240.01
A 92

GA

中华人民共和国公共安全行业标准

GA/T 1713—2020

法庭科学　破坏性程序检验技术方法

Forensic science—Technical methods for examination of destructive programs

2020-03-05 发布　　2020-05-01 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
法庭科学　破坏性程序检验技术方法
GA/T 1713—2020
*
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.org.cn
服务热线:400-168-0010
2021年1月第一版
*
书号:155066·2-35750

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。

本标准主要起草人：蔡立明、金波、杨涛、沙晶、崔宇寅、张云集、孙杨。

法庭科学　破坏性程序检验技术方法

1　范围

本标准规定了对计算机信息系统中的破坏性程序进行检验、分析的技术方法和步骤。

本标准适用于法庭科学计算机信息系统中的破坏性程序的检验鉴定。

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。

GA/T 756—2008　数字化设备证据数据发现提取固定方法

GA/T 976—2012　电子数据法庭科学鉴定通用方法

3　术语和定义

GA/T 756—2008 和 GA/T 976—2012 界定的以及下列术语和定义适用于本文件。

3.1

计算机信息系统　computer information system

具备自动处理数据功能的系统，包括计算机、网络设备、通信设备、自动化控制设备等。

3.2

破坏性程序　destructive program

能够在预先设定条件下自动触发，并破坏计算机信息系统功能、数据或者应用程序的程序；或者可以通过网络、存储介质、文件等媒介，将自身的部分、全部或变种进行复制、传播，并破坏计算机信息系统功能、数据或者应用程序的程序；以及其他专门设计用于破坏计算机信息系统功能、数据或者应用程序的程序。

3.3

程序行为　program behavior

程序在运行期间与计算机信息系统的交互及其对计算机信息系统产生的影响。

3.4

静态分析　static analysis

在程序没有运行的情况下，对可执行程序进行的分析。

3.5

动态分析　dynamic analysis

在程序运行过程中，对可执行程序的程序行为进行的分析。

3.6

逆向分析　reverse analysis

对可执行程序进行反编译，通过分析反编译代码获知可执行程序的程序行为及其实现过程。