# 司　法　鉴　定　技　术　规　范

SF/Z JD0403002——2015

# 破坏性程序检验操作规范

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

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、郭弘、杨涛、沙晶、崔宇寅、张云集。

本技术规范为首次发布。

# 破坏性程序检验操作规范

## 1 范围

本技术规范规定了对计算机信息系统中的破坏性程序进行检验、分析的操作规范和步骤。

本技术规范适用于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

下列文件对于本技术规范的应用是必不可少的。凡是注日期的引用文件，仅所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 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

**计算机信息系统 computer information system**

指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 programs**

对计算机信息系统的功能或计算机信息系统中存储、处理或者传输的数据等进行未授权地获取、删除、增加、修改、干扰及破坏等的应用程序。

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**

在没有真正执行程序的情况下，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 reversing 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。

## 4 检验步骤

### 4.1 待检破坏性程序的固定保全

4.1.1 当检材为电子文件时，对电子文件进行备份，并计算哈希值。

4.1.2 当检材为数字化设备时：

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。

4.1.2.1 当检材为开机状态时：

a) 对检材屏幕的显示内容进行拍照或录像；

b) 在条件允许的情况下，获取检材内存镜像并计算哈希值；

c) 对检材存储介质中的待检破坏性程序进行备份，并计算哈希值。

4.1.2.2 当检材为关机状态时：

a) 对于具有写保护条件的，应将检材中的存储介质通过写保护设备连接至检验设备上；

b) 关闭检验设备上的各种安全防护软件，防止安全防护软件自动将待检破坏性程序删除；

c) 对待检破坏性程序进行固定保全时，应将待检破坏性程序与检验设备上的其它程序及文件等进行隔离，防止待检破坏性程序对检验设备上的系统、程序、文件等造成破坏；

d) 计算待检破坏性程序的哈希值。

## 4.2 待检破坏性程序检验环境的搭建

4.2.1 根据待检破坏性程序的运行环境，搭建相应的检验环境，搭建的检验环境应确保其具备触发待检破坏性程序运行的条件，并确保待检破坏性程序能够正常运行。

4.2.2 在检验环境中安装必要的系统监控、网络监控和程序分析等工具。

4.2.3 避免安装与待检破坏性程序检验无关的软件程序等，以免影响待检破坏性程序的正常运行。

4.2.4 在条件允许的情况下，可搭建虚拟检验环境对待检破坏性程序进行实验分析。

## 4.3 待检破坏性程序的检验分析

### 4.3.1 待检破坏性程序的静态分析

根据待检破坏性程序的具体情况，对待检破坏性程序进行静态分析，分析内容可包括：

a) 待检破坏性程序的基本信息，包括文件的大小、创建时间、修改时间和版本号等；

b) 检验待检破坏性程序文件的文件类型，以帮助了解待检破坏性程序的本质和意图；

c) 将待检破坏性程序与已知样本破坏性程序进行相似性比对，或使用反病毒软件和反间谍软件扫描待检破坏性程序文件，以确定待检破坏性程序文件是否具有已知恶意代码的特征码；

d) 检测待检破坏性程序是否具有防检测分析的保护工具，如加壳、加密等情况。若存在防检测分析的保护工具，可根据需要先去除保护工具。

### 4.3.2 待检破坏性程序的动态分析

根据待检破坏性程序的具体情况，对待检破坏性程序进行动态分析，分析内容可包括：

#### 4.3.2.1 待检破坏性程序行为监控

a) 执行待检破坏性程序，在待检破坏性程序运行过程中，通过观察屏显等方法检验计算机信息系统中是否发生异常情况，若存在异常情况，应分析异常情况的产生是否与待检破坏性程序有关；

b) 在待检破坏性程序运行过程中，可使用监控软件对其行为进行监控，通过监控软件记录并分析待检破坏性程序的程序行为；

c) 若发现待检破坏性程序在运行过程中存在网络通讯行为的，应使用网络通讯监控软件对其收发的网络数据包进行检验分析，分析内容可包括其收发网络数据包的网络通讯地址、内容、收发时间等信息，从而判断待检破坏性程序的网络程序行为。

#### 4.3.2.2 日志文件的分析

在执行待检破坏性程序后，检验分析系统日志文件是否存在异常情况，若存在异常情况，分析判断异常情况的产生是否与待检破坏性程序有关。

#### 4.3.2.3 系统内存的检验分析

在待检破坏性程序运行过程中，检验分析计算机信息系统内存中的相关信息是否存在异常情况，如指定进程相关的内存数据、隐藏的进程、网络连接等相关信息，并分析判断异常情况的产生是否与待检破坏性程序有关。

#### 4.3.2.4 其它相关信息分析

在待检破坏性程序运行过程中，检验计算机信息系统中存储、处理或者传输的数据、配置文件以及应用程序等的异常情况，并分析异常情况产生的原因。

#### 4.3.2.5 待检破坏性程序的逆向分析

必要时，可对待检破坏性程序进行逆向分析，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。

#### 4.3.2.6 实验分析

必要时，可通过设计实验对待检破坏性程序仍存疑的程序行为或功能进行分析。

#### 4.3.2.7 综合分析判断

将待检破坏性程序运行过程中发现的所有异常情况进行综合分析，分析各种异常情况之间的相关性，判断异常情况的出现是否与待检破坏性程序有关联。

## 5 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应包括：

a) 检材固定保全情况；
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) 待检程序对计算机系统造成的破坏情况（如存在）；
f) 其它相关情况。

## 6 检验结果

待检程序的检验结果可以是以下四种之一：

a） 确定为破坏性程序；

判断依据：发现待检程序存在对计算机信息系统的功能或计算机信息系统中存储、处理或者传输的数据等进行未授权地获取、删除、增加、修改、干扰及破坏等的的行为。检验结果一般表述为:待检程序为破坏性程序。

b） 确定为非破坏性程序；

判断依据：未发现待检程序存在对计算机信息系统的功能或计算机信息系统中存储、处理或者传输的数据等进行未授权地获取、删除、增加、修改、干扰及破坏等的的行为，并分析不存在通过现有技术手段无法发现的有对计算机信息系统的功能或计算机信息系统中存储、处理或者传输的数据等进行未授权地获取、删除、增加、修改、干扰及破坏等的可能性。检验结果一般表述为:待检程序不是破坏性程序。

c） 未发现待检程序具有破坏性；

判断依据：未发现待检程序存在对计算机信息系统的功能或计算机信息系统中存储、处理或者传输的数据等进行未授权地获取、删除、增加、修改、干扰及破坏等的的行为，但尚不能完全排除存在根据现有技术手段难以发现的情况。检验结果一般表述为：未发现待检程序具有破坏性。

d） 无法判断是否为破坏性程序。

根据检验结果和综合分析无法判断是否为破坏性程序，或经综合分析亦无法形成明确性意见的，检验结果一般表述为:无法判断是否为破坏性程序。