ICS 35.240.01
A 92

GA

中华人民共和国公共安全行业标准

GA/T XXXX—XXXX

法庭科学 破坏性程序检验技术方法

Technical methods for examination of destructive programs in Forensic science

报批稿

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中华人民共和国公安部　发布

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 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。

4 检验过程

4.1 待检程序的固定保全

4.1.1 检材为电子文件时，对电子文件进行备份，并计算其完整性校验值。

4.1.2 检材为数字化设备时，应对检材进行拍照或录像，记录其特征，并对检材进行唯一性标识。根据设备状态进行固定保全：

a) 检材为开机状态时：

1) 对检材屏幕的显示内容进行拍照或录像；

2) 对检材存储介质中的待检程序进行备份并计算完整性校验值；

3) 在条件允许的情况下，可获取检材内存镜像并计算完整性校验值。

b) 检材为关机状态时：

1) 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；

2) 关闭检验设备上的安全防护软件，防止安全防护软件自动将待检程序删除；

3) 对检材存储介质中的待检程序进行备份，备份时应将待检程序与检验设备上的其他程序及文件进行隔离，防止待检程序对检验设备上的系统、程序、文件造成破坏；

4）计算待检程序的完整性校验值。

4.2 待检程序检验环境的搭建

4.2.1 根据待检程序的运行环境，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程序运行的条件，并确保待检程序能够正常运行。

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 避免安装与待检程序检验无关的软件程序等，以免影响待检程序的正常运行。

4.2.4 在条件允许的情况下，可搭建虚拟检验环境对待检程序进行实验分析。

4.3 待检程序的检验分析

4.3.1 待检程序的静态分析

根据待检程序的具体情况，对待检程序进行静态分析，内容可包括：

a）待检程序的基本信息，包括文件的大小、创建时间、修改时间和版本号等；

b）待检程序文件的文件类型，以帮助了解待检程序的性质；

c）将待检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程序文件，以确定待检程序文件是否具有已知恶意代码的特征码；

d）检验待检程序是否具有防检验分析的保护工具，如加壳、加密等情况。若存在防检验分析的保护机制，可根据需要先去除保护机制。

4.3.2 待检程序的动态分析项目的选择

根据待检程序的具体情况，选择以下一项或多项内容对待检程序进行动态分析：

a）待检程序行为监控；

b）日志文件的分析；

c）系统内存的检验分析；

d）其它相关信息分析；

e）待检程序的逆向分析；

f）实验分析；

g）综合分析判断。

4.3.3 待检程序的动态分析

4.3.3.1 待检程序行为监控

可通过以下方式对待检程序的行为进行监控：

a）运行待检程序，在待检程序运行过程中，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程序有关；

b）在待检程序运行过程中，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程序的程序行为；

c）若发现待检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，从而判断待检程序的网络程序行为。

4.3.3.2 日志文件的分析

在运行待检程序后，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程序有关。

4.3.3.3 系统内存的检验分析

在待检程序运行过程中，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程序有关。

4.3.3.4 其他相关信息分析

在待检程序运行过程中，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。

4.3.3.5 待检程序的逆向分析

必要时，可对待检程序进行逆向分析，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。

4.3.3.6 实验分析

必要时，可通过设计实验对待检程序存疑的程序行为或功能进行分析。

4.3.3.7 综合分析判断

将待检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) 其他相关情况。

6 检验结论

根据对待检程序的检验分析，描述待检程序的程序行为及其具有的功能。