

ICS 13.310
CCS A 92

GA

**INDUSTRY STANDARD OF THE
PEOPLE'S REPUBLIC OF CHINA**

GA/T 1571-2019

**Forensic sciences - Examination methods for functions of
Android applications**

法庭科学 Android系统应用程序功能检验方法
(English Translation)

Issued on: January 1, 1970

Implemented on: June 15, 2019

Issued by: Ministry of Public Security

Table of Contents

- Foreword
- 1 Scope
- 2 Normative references
- 3 Terms and definitions
- 4 Equipment
 - 4.1 Hardware
 - 4.2 Software
- 5 Inspection steps
 - 5.1 Record and inspect the situation of materials
 - 5.2 Taking photos of inspection materials
 - 5.3 Keep a backup copy of the application sample
 - 5.4 Program code function analysis and inspection
- 6 Inspection opinions
- 7 Supplementary Provisions

Foreword

This standard was drafted in accordance with the rules given in GB/T 1.1-2009.

Please note that some elements of this document may involve patents. Publication of this document the agency is not responsible for identifying these patents.

This standard was proposed by the National Criminal Technical Standardization Technical Committee Electronic Material Evidence Inspection Sub-Technical Committee Out.

This standard is under the jurisdiction of the National Criminal Technology Standardization Technical Committee (SAC/TC 179).

This standard was drafted. Cyber Security Bureau of the Ministry of Public Security, Chongqing Public Security Bureau.

1 Scope

This standard specifies the methods used in the field of forensic science to test the functionality of Android system applications.

This standard applies to the functional testing of specific applications of the Android system in the field of forensic science.

2 Normative references

The following documents are indispensable for the application of this document. For dated references, only the dated version applies to this document.

Pieces. For undated references, the latest version (including all amendments) applies to this document.

GA/T 756-2008 Digital Equipment Evidence Data Discovery Extraction Fixed Method
GA/T 757-2008 Program Function Inspection Method
GA/T 828-2009 Technical Specification for Electronic Material Evidence Software Inspection

3 Terms and definitions

The terms and definitions defined in GA/T 756-2008, GA/T 757-2008, GA/T 828-2009 and the following apply to this document.

Android application

Programs running on the Android system with one or more specific functions.

Decompile

The process of restoring application files into assembly or high-level language code.

4.1 Hardware

Special interface data connection line, intelligent terminal inspection workstation.

4.2 Software

Screenshot software, running environment required for inspection application, decompilation tools, tool software required for analysis and inspection, etc.

5.1 Record and inspect the situation of materials

Uniquely number the inspection materials submitted for inspection.

5.2 Taking photos of inspection materials

Take pictures of the materials submitted for inspection.

5.3 Keep a backup copy of the application sample

5.3.1

For a single application file whose material is tested, calculate the hash value of the file and fix the application file.

5.3.2

For smart terminals with applications installed in the inspection materials, the application should be used to backup the application in a signal blocking environment.

The program always extracts and calculates the hash value of the backup program file.

5.4.1 Get the basic attributes of the program file

Get the file name, file size, file last modification time, file hash value, and other attributes of the program.

5.4.2 Static Analysis Program

Use a decompilation tool to decompile the application file.

The program has package name, authority, and certificate information, and analyzes the program code according to the test target and the function tested.

For malicious applications, analyze whether the program has. sending emails, intercepting and forwarding short messages, monitoring and modifying outgoing calls, Get (such as GPS) positioning and other functions. Use screenshots, photos or videos to fix the test results.

5.4.3 Dynamic Analysis Program

Use a virtual simulation environment such as an Android system device or Android SDK (Android-specific software development kit) Test targets and test functions dynamically check application files, and if necessary, capture and analyze application network behaviors Analysis, mainly analyzing the server IP, email account, password and other information that communicates with the application. Use screenshots, photos or videos the test results are fixed.

6 Inspection opinions

List the detected application functions in order according to the inspection. Such as checking out applications with sending emails, listening to intercepting and forwarding short messages, the functions of monitoring and modifying outgoing calls and obtaining (such as GPS) positioning should be listed separately.

7 Supplementary Provisions

7.1

The inspection process meets the following requirements.

a) Inspection records should be made;

- b) the data in the inspection object should not be changed;
- c) The detected data should be stored in a dedicated storage medium;
- d) The inspection process should be recorded simultaneously.

7.2

The objects to be submitted for inspection shall be protected against water, magnetism, static electricity and shock.