

ICS 13.310
CCS A 92

GA

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

GA/T 1572-2019

**Forensic sciences - Technical specifications for examination of
location information of mobile terminals**

法庭科学 移动终端地理位置信息检验技术方法

(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 Inspection material and sample number	
5.2 Inspection of materials and samples	
5.3 Data inspection	
5.4 Data presentation	
5.5 Calculating the hash value	
6 Inspection content	
7 Inspection records	
7.1 Inspection information record	
7.2 Inspection process records	
8 Expression of test results	
9 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. The issuer of this document 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 (SAC/TC179/SC7) Get out and back.

This standard was drafted. Cyber Security Bureau of the Ministry of Public Security, Jilin Province Public Security Department, the Third Institute of the Ministry of Public Security, Northeast Normal University, Material Identification Center of the Ministry of Public Security.

1 Scope

This standard specifies the inspection and analysis methods for geographic location information in mobile terminals in the forensic sciences.

This standard applies to electronic physical evidence inspection in the field of forensic science.

2 Normative references

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

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

GB/T 29360-2012 Electronic physical evidence data recovery inspection procedures GB/T 29362-2012 Electronic material evidence data search and inspection procedures GA/T 756-2008 Digital Equipment Evidence Data Discovery Extraction Fixed Method

3 Terms and definitions

The following terms and definitions apply to this document.

Mobile terminal

Computer equipment that can be used on the move, with operating system, communication function, GPS, Beidou and other radio navigation modules Block and location recording devices and their storage media.

Geographic trace

During the use of the mobile terminal, the mobile terminal and the installed applications use GPS positioning, Beidou positioning, Glonass positioning, Wifi Positioning, base station positioning, linear accelerator, gyroscope, and other locations such as geographic coordinate data, azimuth data, and altitude data the data and the time of obtaining the geographical position, and the geographical position data can be converted into specific position information, and the trajectory route is formed in time series.

4.1 Hardware

Electronic physical evidence inspection workstation, mobile phone inspection workstation, electronic data storage medium duplication equipment, electronic data storage medium write protection device Devices, dedicated storage media, digital cameras, etc.

4.2.1 Operating System

Windows, Unix/Linux, Mac OS, Android, iOS, etc.

4.2.2 Software tools

Data synchronization software, location reproduction software or mobile terminal simulation software, special viewing tools for system files, special viewing for user files Class tools.

5.1 Inspection material and sample number

Uniquely number the materials (samples) to be inspected.

5.2 Inspection of materials and samples

Take a photo of the sample (sample) submitted for inspection, and record the characteristics of the sample.

5.3.1 Equipment inspection

Equipment inspection includes at least the following.

- a) It should be read-only connected to the electronic physical evidence inspection workstation or mobile phone inspection workstation through a data cable;
- b) Start anti-virus software to disinfect the inspection workstation system;
- c) Run the data synchronization software or forensics software, and copy the electronic data stored in the inspection materials to a dedicated storage medium.

5.3.2 Inspection of storage media

The storage media inspection shall include at least the following.

- a) Connect the storage medium to the electronic physical evidence inspection workstation in a read-only manner;
- b) Make a safe backup of the electronic data in the storage medium and check it according to GB/T 29362-2012 or GB/T 29360-2012 Check and obtain electronic data in the storage medium;
- c) Copy the obtained electronic data files to a dedicated storage medium.

5.3.3 Inspection of Geographic Track Data Cache File

Obtain the geographic track data cache file according to the requirements of GA/T 756-2008.

- a) Check the mobile terminal cache. Find the directory storage path of the operating system

cache geographic track positioning data in the inspection material, and obtain the cached Geo-track data cache files and file creation time, modification time, and last access time information, and Extract the recorded location information, positioning method and positioning time from the record;

b) Verify the mobile terminal application software data. Find the number of mobile terminal application software and application software with positioning authority in the inspection material Data storage directory. Find the file containing the positioning cache data from the data storage directory of the application software, the user account information file Information about the creation time, modification time, and last access time of files and files, and extract users from the user account information file Detailed account information, extract location information, location method and location time from the location cache data file;

c) Record and verify the acquired geographic track data files, and copy the acquired electronic data files to a dedicated storage medium.

5.4 Data presentation

5.4.1

Run position reproduction software or mobile simulation software in the workstation to interpret and present the position and trajectory information recorded in the electronic data.

5.4.2

Fixed results.

5.5 Calculating the hash value

Calculates a hash of the checked out and rendered data.

6 Inspection content

Data inspection content should include.

- a) the name and storage path of the geographic track data file;
- b) the source of the geographic trajectory data;
- c) user account, nickname, mobile phone number and other related information related to geographic track data;
- d) Geographic trajectory history records, including positioning data, positioning time, positioning method, Wifi and base station assisted positioning information.