

ICS 13.310
CCS A 92

GA

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

GA/T 1570-2019

**Forensic sciences - Technical specifications for database
authentication
(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 Inspection steps
4.1 Preparation
4.2 Fixation and security
4.3 Search and Recovery
4.4 Inspection and analysis
5 Inspection records
6 Inspection results
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. 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).

This standard is under the jurisdiction of the National Criminal Technology Standardization Technical Committee (SAC/TC179).

This standard was drafted. Scientific Research Institute of Forensic Sciences, Material Evidence Identification Center of the Ministry of Public Security, Shanghai Chenxing Electronic Data Judicial Identification Center.

1 Scope

This standard specifies the technical methods for authenticity testing of database data 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 5271.17-2010 Vocabulary for information technology-Part 17. Database GB/T 29360 Electronic Material Evidence Data Recovery Inspection Procedures GB/T 29362 Electronic material evidence data search and inspection procedures GA/T 976 General Method for Scientific Identification of Electronic Data Courts

3 Terms and definitions

The terms and definitions defined in GB/T 5271.17-2010, GA/T 976 and the following apply to this document.

Database authentication Examine and analyze the formation and modification of specified data in the database. Usually used to determine whether the formation of specified data is consistent with the customer Check the facts and whether they have been modified after the fact.

Database application system; DBAS Computers and other application systems established with the support of a database management system.

Database file

Files related to database data include database data table files, database configuration files, and database log files.

Examples...mdf and .ldf files for SQL Server, .ora and .dbf files for Oracle.

4.1 Preparation

4.1.1

Understand the development, use and maintenance of the database to be inspected.

4.1.2

Understand the security management and permission configuration of the database to be checked.

4.1.3

Understand the update and upgrade of the database to be checked.

4.1.4

Understand the database encryption status, such as full database encryption, field encryption, and table encryption.

GA/T xxxx-xxxx

4.1.5

Understand the backup status of the database to be checked, such as the frequency of backups, the location of backup files, and the last backup time.

4.2 Fixation and security

4.2.1

Uniquely number the equipment and storage media running the database system to be inspected, and take pictures or videos if conditions permit.

4.2.2

Where conditions permit, it is advisable to perform a security backup of the storage medium where the inspection database is located.

4.2.3

If security backup cannot be performed, the required files or data in the database system can be directly extracted, and the extraction process can be performed.

Full recording.

4.2.4

Calculate a hash value for the data formed by the fixed security process.

4.3 Search and Recovery

Search and restore the data in the storage media related to the database to be checked according to the inspection requirements according to GB/T 29360 and GB/T 29362 Library data files and data.

4.4 Inspection and analysis

According to the specific conditions of the inspection materials, the following all or part of the contents in the database are inspected and analyzed according to the inspection needs.

- a) attributes of data files, backup files, log files and other related files;
- b) data dictionary;
- c) Automatically triggered content such as stored procedures, method functions, and table structure triggers;

- d) the correspondence between data tables, records, fields and data displayed by the application system;
- e) whether the data structure and data are abnormal;
- f) whether there is a contradiction in the chronological order of the data;
- g) whether there is any contradiction between the log content and the data;
- h) whether there is any conflict between backup and data;
- i) whether the hard copy of the data (such as exported data, paper prints obtained from the database application system, etc.) is inconsistent with the data;
- j) user rights grants and changes;
- k) Other data that may form a corroborative relationship with the database to be inspected.

5 Inspection records

Information related to the inspection shall be recorded in a timely, objective and comprehensive manner to ensure the traceability of the inspection process and results.

6 Inspection results

According to the inspection findings, the formation and modification of the data in the database to be inspected are described objectively, generalized, and targeted. Right where inspection conditions are prepared, the reasons shall be stated.

7 Supplementary Provisions

7.1

During the inspection, the difference between the system time and the standard time shall be noted.

7.2

The extraction process should pay attention to maintaining the integrity of the database data, and avoid changing the database structure and adding, modifying, and deleting database data.

7.3

Database data should be inspected from multiple angles to form a mutually confirmed relationship.

7.4

During the inspection process, the database data files and data containing time information should be focused on.