

ICS 13.310
CCS A 92

GA

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

GA/T 1569-2019

**Forensic sciences - Specifications for building laboratories for
electronic evidence examination**

法庭科学 电子物证检验实验室建设规范

(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 Reference standards
3 Laboratory classification
4 Business Scope
4.1 Electronic physical evidence extraction and fixation
4.3 Volatile Data Extraction
4.4 Data Recovery
4.5 Data search
4.6 Document consistency check
4.7 Software function test
4.8 Software consistency check
4.9 Time attribute test
4.10 Online Record Inspection
4.11 Email Inspection
4.12 Instant messaging inspection
4.13 Log Inspection
4.14 Database Inspection
4.15 Password cracking
4.16 Mobile phone inspection
4.17 Video surveillance equipment inspection
4.18 Pseudo base station inspection
4.19 Inspection of damaged storage media
4.20 Media Data Erase
4.21 Mobile Phone Information Correlation Analysis
4.22 Network Information Association Analysis
4.23 Lab Business Project Settings
5 Data search must-have
6 Document consistency check
7 Software function test must be optional
8 Software Consistency Check Mandatory Optional
9 Time attribute inspection

- 10 Necessary Essentials for Online Record Inspection
- 11 Email Inspection Mandatory Mandatory Optional
- 12 Essentials for Instant Messaging
- 13 Necessary and optional for log inspection
- 14 Database Inspection Mandatory Optional
- 15 Password cracking required optional
- 16 Necessary Essentials for Mobile Phone Inspection
- 17 Necessary Essentials for Inspection of Video Surveillance Equipment
- 19 Necessary optional for inspection of damaged storage media
- 20 Required Data Wipe
- 21 Necessary and optional for mobile phone information correlation analysis
- 22 Network Information Association Analysis Mandatory Optional
- 24 Electronic physical evidence inspection integrated workstation set 4 2 1 3-5 years
- 25 Electronic data inspection and analysis software suite 1 1 1 3-5 years
- 26 Electronic data distributed analysis system set 1 1 Optional 3-5 years
- 27 Various types of genuine operating system software packages 1 1 1 3-5 years
- 28 Mobile Forensic Analysis System Set 3 2 1 3-5 years
- 29 Mobile phone chip extraction equipment set 1 1 optional 3-5 years
- 30 Mobile password cracking software suite 1 1 1 3-5 years
- 31 Simulation software set 2 1 Optional 3-5 years
- 32 Visual Association Analysis System 2 1 1 3-5 years
- 33 Electronic data analysis system set 1 optional 5-10 years
- 34 Electronic data destruction machine 1 1 Optional 3-5 years
- 35 CD data destruction machine 1 1 Optional 3-5 years
- 36 Shielding boxes 2 1 1 5-10 years
- 37 CD burner station 2 2 optional 3-5 years
- 38 Scanner table 1 1 1 3-5 years
- 39 Color printing copier table 1 1 1 3-5 years
- 40 Electronic data analysis server station 1 1 Optional 3-5 years
- 41 Storage array table 1 1 optional 3-5 years
- 42 Anti-magnetic anti-static cabinets 2 1 1 5-10 years
- 43 Electronic physical evidence safes 3 2 1 5-10 years
- 44 UPS uninterruptible power supply set 1 1 1 3-5 years
- 45 Laboratory Quality Management System Set 1 1 1 3-5 years
- 46 Mobile phone sample library options optional options optional 3-5 years

47 Hard disk sample library set optional 3-5 years

48 Electronic Material Evidence Mobile Lab Kit Option Option Option 5-10 Years

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) Out.

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

This standard was drafted. Material Evidence Identification Center of the Ministry of Public Security, Procuratorate Technical Information Research Center of the Supreme People's Procuratorate, Heilongjiang Public Security Department, Chongqing Public Security Bureau, Tianjin Public Security Bureau.

1 Scope

This standard specifies the specifications for the construction of electronic physical evidence inspection laboratories.

This standard applies to the construction of electronic physical evidence testing laboratories in the field of forensic science.

2 Reference standards

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 50015-2010 design code for water supply and drainage of buildings GB 50016-2014 fire protection code for building design GB 50019-2015 design code for heating, ventilation and air conditioning GB 50057-2016 building lightning protection design code GB 50073-2013 clean plant design code GB 50116-2013 design code for automatic fire alarm system GB 50174-2016 Design Specification for Electronic Information System Room GB 50222-2015 code for fire protection design of building interior decoration GB 50311-2015 Engineering Design Specification for Integrated Cabling System GB 50343-2015 Technical

Specifications for Lightning Protection of Building Electronic Information Systems

3 Laboratory classification

Electronic physical evidence laboratory is divided into three levels.

- a) Level I Electronic Material Evidence Laboratory;
- b) secondary electronic physical evidence laboratory;
- c) Level 3 Electronic Material Evidence Laboratory.

4.1 Electronic physical evidence extraction and fixation

Discover, identify, extract and secure electronic physical evidence and related items.

4.2 On-site security Keep or backup the extracted electronic physical evidence at the scene.

4.3 Volatile Data Extraction

Extracts and fixes data that disappears with power off or off in electronic devices such as computers that are transmitted over the network.

4.4 Data Recovery

Verify the restoration of file data that cannot be accessed or recognized by the operating system in the sample.

4.5 Data search

Inspection based on relevant keywords or known content in the inspection material.

4.6 Document consistency check

Check whether the data content of two files is the same.

4.7 Software function test

GA/T xxxx-xxxx

A test to determine whether the software has a function (some).

4.8 Software consistency check

A test comparing whether two software functions are identical (or similar).