

ICS 13.310
CCS A 92

GA

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

GA/T 1564-2019

**Forensic sciences - Technical specifications for collection of
electronic evidence during scene investigation**

法庭科学 现场勘查电子物证提取技术规范

(English Translation)

Issued on: January 1, 1970

Implemented on: May 27, 2019

Issued by: Ministry of Public Security

Table of Contents

Foreword

1 Scope

2 Normative references

3 Terms and definitions

4.1 Hardware

4.2 Software

5.1 Computer Evidence Extraction

5.2 Physical extraction of cell phone physical evidence

5.3 Physical extraction of hard disk surveillance video recorder

5.4 Physical extraction of other electronic equipment

6 Electronic data extraction

6.1 Remote Survey Online Extraction

6.2 Computer and hard disk surveillance video recorder data extraction

6.3 Extraction of data from other electronic equipment

8 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. Beijing Public Security Judicial Identification Center, Material Evidence Identification Center of the Ministry of Public Security.

Drafters of this standard. Zhu Xiuyun, Yao Bo, Jia Yongsheng, Song Run, Tang Jinzhang, Xing Guidong.

GA/T xxxx-xxxx

Forensic Science Site Investigation Electronic Material Evidence Extraction Technical Specification

1 Scope

This standard specifies the technical methods for extracting electronic physical evidence during the on-site investigation of cases.

This standard applies to the on-site extraction of electronic physical evidence 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 1069-2013 Forensic Science Electronic Material Evidence Mobile Phone Inspection Technical Specification

3 Terms and definitions

The following terms and definitions apply to this document.

Scene collection of electronic evidence the process of discovering, fixing, and collecting electronic physical evidence at the scene and its place.

Volatile data

Data that exists on the network or that runs on electronic devices such as computers and disappears when the power is turned off or off.

Electronic evidence collection online the process of obtaining electronic data in a target system while the target system is running.

Remote inspection

The remote target system is surveyed through the network to extract and fix the status and stored content of the remote target system.

Mobile phone signal shielding device A special device to isolate mobile phone communication signals and block mobile phone communication.

Safe backup device

A device that performs a complete, accurate, non-destructive backup of raw data in a storage medium.

GA/T xxxx-xxxx

Read-only device

A device that is write-protected on the access storage medium.

4 On-site extraction equipment

4.1 Hardware

Video recording equipment, electronic physical evidence site survey box, mobile phone signal shielding equipment, mobile phone shielding box (bag), mobile phone forensics equipment, simulation Equipment, security backup equipment, dedicated storage media, portable computers, printers, etc.

4.2 Software

Comprehensive forensic analysis software, mobile forensic analysis software, simulation software, online forensics software, installation-free and system registration software, etc.

5 On-site physical extraction of electronic physical evidence

5.1.1 Extraction of shutdown status

5.1.1.1

Unique identification of physical evidence.

5.1.1.2

One-to-one unique numbering of physical evidence wiring and equipment interfaces.

5.1.1.3

Take photos or videos of the scene, including information such as the brand and unique number of the physical evidence.

5.1.1.4

Draw a network topology diagram.

5.1.1.5

Remove the cables and power cables between the physical evidence equipment.

5.1.1.6

Sealed physical evidence.

5.1.2 Extraction of power-on status

5.1.2.1

Uniquely number physical evidence.

5.1.2.2

Take photos or videos of the scene and screen.

5.1.2.3

For devices with a screen saver password, the password should be obtained on site or removed using the installation-free and system-free registration software. The obtained password should be Verify and document. When the screen saver password cannot be removed, the physical evidence equipment should be turned off first, and then follow the steps 5.1.1.2 ~ 5.1.1.5.

5.1.2.4

Use online forensics software to extract volatile data online, save it in a dedicated storage medium with a unique number, and calculate, Record the hash value.

5.1.2.5

The status of hard disk partitions and file display attributes shall be checked and recorded.

5.1.2.6

For devices connected to the Internet, you should check the running browser, QQ and other software settings, and close the software to exit automatically Data function settings; if special software such as virtual machines and VPNs are running, the usage status should be recorded, and the access interactions in this environment should be recorded.

IP in networking.

5.1.2.7

Record the system time and Beijing time of physical evidence.

GA/T xxxx-xxxx

5.1.2.8

Extract the running password-protected data, save it in a special storage medium with a unique number, and calculate, Record the hash value; record the equipment, software, and carrier with the password; obtain or cancel the password on-site, and verify and record the obtained password.

5.1.2.9

Record the data extraction path and the saved path.