

ICS 12.310
CCS A 90

GA

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

GA/T 1568-2019

**Forensic sciences - Terminology for electronic evidence
examination**

法庭科学 电子物证检验术语

(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 Terms and definitions

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 Technical Committee for Criminal Technical Standardization of Electronic Material Evidence Inspection Sub-Committee (SAC/TC 179/SC 7).

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

This standard was drafted. Material Evidence Identification Center of the Ministry of Public Security, Procuratorate Technology Information Research Center of the Supreme People's Procuratorate, and Ministry of Public Security Reconnaissance Technology R & D Center, Heilongjiang Provincial Public Security Department, Beijing Public Security Bureau, China Criminal Police Academy.

1 Scope

This standard specifies the terms for electronic physical evidence inspection.

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

2 Terms and definitions

Electronic data

Numbers that are formed during the occurrence of a case (event), are stored, processed, and transmitted in digital form, and can prove the facts according to.

Electronic evidence

Storage media and electronic data related to the case.

Original electronic data Electronic data contained in the materials or samples submitted for inspection.

Duplication of electronic data Through bit-by-bit copying, data that is completely consistent with the copied data is obtained.

Storage medium

Electronic devices, hard disks, compact discs, USB flash drives, memory sticks, memory cards, memory chips and other carriers with data information storage functions.

Harddisk interface

A connection part that transfers data between a hard disk and a computer.

IDE interface integrated drive electronics Interface for transmitting data in 16-bit parallel mode.

SATA interface serial advanced technology attachment Interface for serial data transmission.

SCSI interface small computer system interface High-speed interface for transmitting data in parallel.

2.10

SAS interface serial attached SCSI SCSI interface with serial connection.

2.11

USB interface universal serial bus Interface for serial bus data transmission.

2.12

Data area

Area where file data is stored.

2.13

Partition

A divided logical storage area in a storage medium.

2.14

Sector

Each track on the disk is equally divided.

2.15

Cluster

The smallest unit of file storage management consisting of sectors.

2.16

Master boot record

Contains the code of the system boot, partition table information, and master boot valid flags.

2.17

Boot sector

The first sector of the storage medium is used to load and give processor control to the operating system.

2.18

File directory table Directory entries that store subdirectories or files.

2.19

File allocation table Registers for managing and recording files using clusters.

2.20

Unallocated space

Unused or freed space on a storage medium after file deletion.

2.21

Slack space

The remaining space in the cluster that has not been filled with data.

2.22

Random access memory dump Transfer some or all of the contents of the memory (RAM) to the storage medium.

2.23

External equipment

A device responsible for data transmission, transfer, and storage before and after the host computer processes the data.

2.24

Computer switch-on time System time when the computer boots into the operating system.

2.25

Computer switch-off time System time when the computer shuts down and exits the

operating system.

2.26

Registry

Stores important data such as operating system information, installed software and hardware information, security policy settings, user accounts and settings, and network configuration document.

2.27

Operating system log the operation of the object specified by the operating system and its operation result are a time-ordered collection. Includes application logs, security logs, and System log.

2.28

Internet favorite

The folder where the website address link information is saved.

2.29

Instant messaging

A comprehensive communication method integrating sound, text, and graphics that uses the network for real-time conversation and mutual information transmission.

2.30

Instant messaging client an application that operates in conjunction with an instant messaging server and is used to receive instant messaging services in a local operating system or smart terminal program.

2.31

Instant messaging protocol Rules for controlling the instant messaging process and data transmission.

2.32

Instant messaging data Text messages, files transferred, and voice call logs passed in instant messaging.

2.33

Instant messenger

An application with the ability to send and receive network messages in real time.

2.34