Chinastandards.org

ICS 35.220.20
CCS A 90

GA

INDUSTRY STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GA/T 756-2008

Forensic sciences - Technical specifications for collection and acquisition of digital evidence

数字化设备证据数据发现提取固定方法

(English Translation)

Issued on: January 1, 1970 **Implemented on: January 1, 1970**

Issued by: Ministry of Public Security

Preview: page 1 of 4 shown, 5 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/ga-t-756-2008

Chinastandards.org

Table of Contents

Foreword
1 Scope
2 Normative references
3 Terms and Definitions

Foreword

This document is in accordance with the provisions of GB/T 1.1-2020 "Guidelines for Standardization Work Part 1: Structure and Drafting Rules of Standardization Documents" drafted.

This document replaces GA/T 756-2008 "Fixed Methods for Discovery and Extraction of Digital Equipment Evidence Data", which is consistent with GA/T 756-2008 in addition to editorial changes, the main technical changes are as follows.

--- Changed the scope (see Chapter 1, Chapter 1 of the 2008 edition);

--- Changed normative references (see Chapter 2, Chapter 2 of the 2008 edition);

--- Delete the terms and definitions "digital equipment", "local digitizing equipment", "remote digitizing equipment", "evidence data", "evidence data" Discovery Extract" "Fixed Evidence Data" "Bit-by-Bit Consistency" "Meaning Consistent" "Reproducible Data" "Non-reproducible Data" "Evidence Data" Originality, Evidence Data Integrity, Hash Value, Original Electronic Data Storage Medium, Test Cases (see 2008 edition of 3.1, 3.1.1, 3.1.2, 3.2~3.13);

--- Added terms and definitions "computer information system", "local computer information system", "electronic data collection and extraction", "freeze" (see 3.1~3.4);

--- Added the content of recording the inspection materials (see 4.1.1, 4.1.2);

--- Changed the "Design Test Case", the title name was changed to "Collection Extraction Method", and changed some contents [see 4.2, 4.2.1~ 4.2.11, 4.2, 4.2a)~c) of the 2008 edition];

--- Changed "Finding and extracting fixed evidence data", the title name was changed to "Steps for collecting and extracting electronic data", and changed the section Content [see 4.3, 4.3.1~4.3.9, 4.3, 4.3a)~k) of the 2008 edition];

--- Changed the "inspection record", the title name was changed to "record", and changed part of the content (see Chapter 5, 5.1~5.6, 2008 edition 4.4, 4.4.1~4.4.4);

Preview: page 2 of 4 shown, 5 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/ga-t-756-2008

--- Added "representation of collection and extraction results" (see Chapter 6).

Please note that some content of this document may be patented. The issuing agency of this document assumes no responsibility for identifying patents.

1 Scope

This document specifies terms and definitions for electronic data collection and extraction in the field of forensic science, general requirements, collection and extraction steps, collection and extraction Take records and express results.

This document applies to the collection and extraction of electronic data in the field of forensic science.

2 Normative references

The contents of the following documents constitute essential provisions of this document through normative references in the text. Among them, dated citations documents, only the version corresponding to that date applies to this document; for undated references, the latest edition (including all amendments) applies to this document.

GB/T 31167 Information Security Technology Cloud Computing Service Security Guide GA/T 754 Electronic data storage medium reproduction tool requirements and testing methods GA/T 755 Electronic data storage medium write protection equipment requirements and testing methods GA/T 1069 Forensic Science Electronic Evidence Mobile Phone Inspection Technical Specification GA/T 1174 General method for on-site acquisition of electronic evidence data GA/T 1476 Forensic Science Remote Host Data Acquisition Technical Specification GA/T 1478 Technical Specification for Data Acquisition for Forensic Science Websites GA/T 1568 Forensic Science Electronic Evidence Examination Terminology

3 Terms and Definitions

The terms and definitions defined in GB/T 31167 and GA/T 1568 and the following terms and definitions apply to this document.

A system with the function of automatically processing data, including computers, network equipment, communication equipment, automatic control equipment and the software it contains system, etc.

Collect and extract computer information systems that can be physically contacted and operated by personnel.

Search, analyze and intercept the electronic data stored, processed and transmitted in the computer information system, and collect and extract the electronic data the process of performing an integrity check.

Preview: page 3 of 4 shown, 5 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/ga-t-756-2008

Chinastandards.org

freeze

It is a measure to fix the data in a computer information system in a specific state at a specific time to ensure that it will not change.

Preview: page 4 of 4 shown, 5 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/ga-t-756-2008