

ICS 13.310
CCS A 92

GA

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

GA/T 829-2009

**Software identification technical specifications of electronic
forensics**

电子物证软件一致性检验技术规范

(English Translation)

Issued on: April 7, 2009

Implemented on: June 1, 2009

Issued by: Ministry of Public Security

Table of Contents

- Foreword
- 1 Scope
- 2 Normative reference documents
- 3 Terms and definitions
- 4 Equipment
 - 4.1 Hardware
 - 4.2 Software
- 5 Operating procedures
 - 5.1 Samples and sample numbers
 - 5.2 Samples and samples taken pictures
 - 5.3 Samples and sample preservation backup
 - 5.4 Inspection

Foreword

This standard by the National Criminal Technology Standardization Technical Committee Electronic Material Inspection Sub-Technical Committee (SAC/TC179/SC7) proposed and centralized.

The drafting of this standard unit. the Ministry of Public Security evidence identification center.

1 Scope

This standard specifies the method of software consistency test in electronic material inspection technology.

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

2 Normative reference documents

The terms of the following documents are hereby incorporated by reference into this standard. Whichever is the date of the reference file, which is followed by all (Excluding corrigenda) or revisions do not apply to this standard, however, encourage the parties to reach an agreement under this standard Whether you can use the latest version of these files. For undated references, the latest edition applies to this standard.

Technical specification for data search and inspection of electronic data

3 Terms and definitions

The terms and definitions established in GA/T 825-2009 apply to this standard.

4.1 Hardware

Storage media, preservation of backup equipment, electronic physical test workstations.

4.2 Software

The system operating environment required for inspection software.

5.1 Samples and sample numbers

List the samples and samples for inspection.

5.2 Samples and samples taken pictures

Take pictures of samples and samples for inspection.

5.3 Samples and sample preservation backup

The preservation of the conditions with the samples and samples of the preservation of backup.

5.4 Inspection

5.4.1

start anti-virus software on the electronic physical test workstation system antivirus.

5.4.2

respectively, the inspection of the sample and the sample software in the hash value calculation, in the sample and sample to find the same hash value of the text (Except public library files).

5.4.2.1

If all the corresponding file has the same hash value, the software is the same.

5.4.2.2

If the corresponding file hash value is different, follow the steps below.

a) the inspection of the software and sample software directly to the directory and file name comparison.

b) installation process comparison. The two sets of software installed in the same test

equipment, compared to the installation process of the screen display and function keys and so on are the same.

c) after the installation is complete, compared to the directory name after installation and file, file comparison, including file name, file length, file hash value and file Time attributes and so on.

d) run the software, the use of process comparison, should be ignored involved in the encryption and decryption, the use of the process of the screen display, function, power