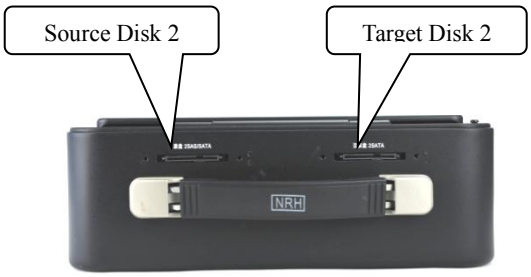
CONTENT

On-Site Forensics Equipment

Portable Computer Forensics System (XF34)

The Portable Computer Forensics System is a set of portable investigation and forensics equipment that combines multiple types of data source acquisition and multiple forensics analysis technologies. The equipment can acquire and analyze various types of hard disks, optical disks, USB flash drives, mobile hard disks and memory cards, and integrates high-speed hard disk copying, forensics analysis and dynamic simulation analysis functions, featuring fast copying speed, powerful analysis, great portability, and easy operation.

Hard Disk Channel 1



Hard Disk Channel 2

Read-only USB and Card Reader

Ordinary USB and Internet Ports

Basic Functions

- **High-Speed Data Copy**
  - ✧ Storage media copy. Portable Computer Forensics System supports copying and mirroring of IDE/SATA/SSD/SAS hard disks, mirroring of USB flash drives, mobile hard disks, memory cards and CDs, and write protection of storage media copy.
  - ✧ Data erasure. Portable Computer Forensics System supports two-way hard disk parallel erasure, and erasure of USB flash drive, mobile hard disk and memory card.

- **Static Forensics Analysis**
  - ✧ Portable Computer Forensics System supports data recovery, chat record analysis, mailbox analysis, trace analysis, relationship network analysis, keyword search, video summary, encrypted file identification, file identification of abnormal format, anti-forensics software identification, timeline analysis, etc.
  - ✧ Portable Computer Forensics System supports analysis of Windows and Mac OS operating systems.
- **Dynamic Simulation Analysis**
  - ✧ Portable Computer Forensics System supports the simulation of hard disk, mirror image and snapshot of operating systems such as Windows/Mac OS/Linux for operating system login password cracking, login password bypass, sensitive information extraction in the simulation environment.
  - ✧ Portable Computer Forensics System supports for operating system login password cracking, login password bypass, sensitive information extraction in the simulation environment.

Main Features

- **Integrated Design**
  - ✧ Integrated hardware design, compact size, easy to carry. It integrates various types of read-only interfaces required for data forensics, replacing the traditional write-protect interface box. Direct plug-in hard disk warehouse design, direct plug-in SATA and SAS hard disks, eliminating the connection of data cables, facilitating on-site case investigation.
  - ✧ Touch screen operation, one-click forensics. With the help of built-in computer forensics software, target operating system simulation software, data copy & erasure software and other specialized forensics analysis software, a series of problems such as data acquisition, forensics analysis, and material report can be solved with just one device.
- **Fast Forensics**
  - ✧ The system adopts high-speed hard disk read-only and read-write interfaces to support two-way hard disk for parallel forensics and improve data acquisition speed.
  - ✧ Hard disk copy speed for SATA is 7GB/Min, for SSD is 21GB/Min.
  - ✧ The system support MD5, SHA1 and SHA256 checksums, using optimization algorithms.

Product Composition

- Portable Computer Forensics System (built-in SATA/SAS/SSD read-only interface, USB and multi-function memory card read-only interface) 1
- Portable Tool Kit (IDE/SATA Adapter, SIM Card Reader, Data Cable) 1
- Hard Disk Copy & Erasure Software 1
- Computer Forensics Software 1
- Dynamic Simulation Software 1

Portable Integrated Forensics System (XF34I)

Portable Integrated Forensics System is a portable comprehensive forensics analysis device that integrates various types of electronic evidence fixation, forensics analysis and report generation, including storage media, computers, intelligent terminals, and hard disk recorders. The equipment is suitable for business scenarios such as site investigation and laboratory forensics. It supports evidence collection, storage media replication, computer fast forensics, data recovery, computer forensics analysis, dynamic simulation analysis, mobile phone forensics analysis, video forensics analysis and other professional forensics analysis functions, and provides write protection functions in accordance with judicial effectiveness.

Basic Functions

- **Integrated Collection**
  - ✧ Integrated multiple interfaces. Portable Integrated Forensics System provides fast hard disk write protection interface data acquisition, USB write protection interface acquisition, network interface acquisition, full interface video recording function (AV, S-Video, BNC, chromatic aberration, VGA, DVI, HDMI, SDI) on one device.
- **High-Speed Data Copy**
  - ✧ Storage media copy. Portable Integrated Forensics System supports copying and mirroring of IDE/SATA/SSD/SAS hard disks, mirroring of USB flash drives, mobile hard disks, memory cards and CDs, and write protection of storage media copy.
  - ✧ Data erasure. Portable Integrated Forensics System supports two-way hard disk parallel

erasure, and erasure of USB flash drive, mobile hard disk and memory card.

- **Static Forensics Analysis**
  - ✧ Portable Integrated Forensics System integrates computer forensics software, supporting data recovery, chat record analysis, mailbox analysis, trace analysis, relationship network analysis, keyword search, video summary, encrypted file recognition, format abnormal file identification, anti-forensics software identification, timeline analysis, etc.
  - ✧ Portable Integrated Forensics System supports analysis of Windows and Mac OS operating systems.
- **Dynamic Simulation Analysis**
  - ✧ Portable Integrated Forensics System integrates target operating system simulation software, supporting the simulation of hard disk, mirror image and snapshot of operating system such as Windows/Mac OS/Linux for operating system login password cracking, login password bypass, sensitive information extraction in the simulation environment.
- **Mobile Phone Forensics Analysis**
  - ✧ Portable Integrated Forensics System integrates mobile phone forensics software that supports for data acquisition, relationship network analysis, timeline analysis, geographic location analysis, data recovery and other functions of over 120 common APPs such as QQ and WeChat.
- **Video Forensics Analysis**
  - ✧ Portable Integrated Forensics System integrates video analysis software that supports video data management and video pre-processing.

Performance

- Data search speed is an order of magnitude faster than EnCase7.0 under the same hardware conditions.
- Hard disk copy speed for SATA is 7GB/Min, for SSD is 22GB/Min.
- Transcoding speed for D1 resolution H264 encoded video is greater than 16 times.
- Video source supports CIF to 1080P.

Main Features

- **Diversified Forensics**
  - ✧ Read-only interface compatible with storage media, computers, smart terminals, hard disk recorders and other types of electronic evidence is convenient for on-site investigation. It integrates copy & erasure, computer forensics, mobile phone forensics, video forensics and other professional forensics analysis software to achieve forensics analysis of computer data, mobile phone data, video data, etc.
- **Multi-scene Application**
  - ✧ The product design absorbs the portability of laptop and the characteristics of professional forensics equipment, suitable for on-site and front-end forensics, and forensics analysis in the laboratory.
- **Great Scalability**
  - ✧ This product is a forensics hardware platform that can install different forensics software to meet various forensics requirements.

Product Compensation

- Forensics Hardware Platform
  (built-in SATA/SAS/SSD read-only interface, USB and multi-function memory card read-only interface) 1
- Hard Disk Copy & Erasure Software 1
- Computer Forensics Software 1
- Dynamic Simulation Software 1
- Mobile Phone Forensics Software (optional) 1
- Video Analysis Software (optional) 1

Storage Media Copier (FZ5)

The Storage Media Copier is a special device for realizing fast data copying and mirroring of various storage media. The media supported by the device include IDE hard disk, SATA hard disk, SAS hard disk, USB flash drive, mobile hard disk, memory card and various types of optical disks.

Basic Functions

- Support for hard disk bit-aligned copying and mirroring.
- Support for mirroring of hard disks, USB flash drives, mobile hard disks, memory cards and optical disks.
- Mirror image format supports DD and E01 formats, and CD-ROM image supports CUE + ISO format.
- Support image restoration to hard disk.
- Support mirror image uploading to back-end analysis system through network.

Main Features

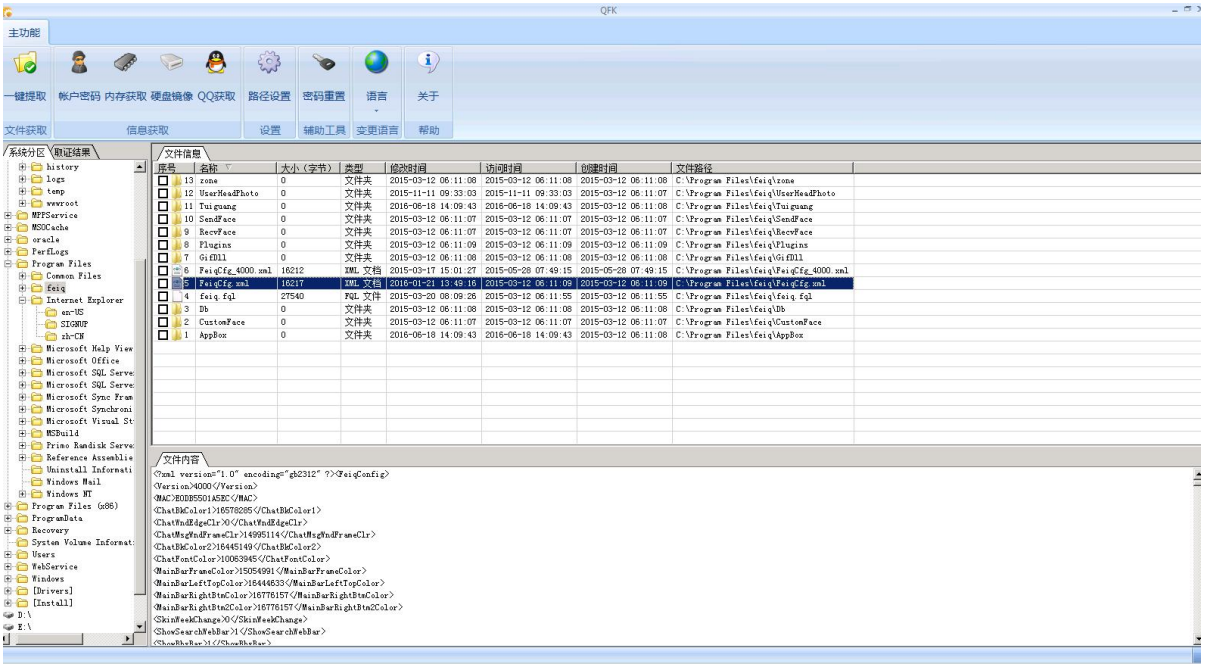
- Fast copy speed. Its hard copy speed competes with international competitors such as Solo4.
- Portable design, touch screen operation, easy to operate and carry.
- Support a wide range of media and multiple copy modes.
- Support data transfer resume from break-point.
- Automatically detects hard disk bad blocks. When encountering bad blocks, you can choose to skip or stop copying.
- Adopts MD5, SHA1 and other verification to ensure the accuracy of data replication.

Product Composition

- Storage Media Copier 1
- Hard Disk Data Cable 1

Computer On-site Fast Forensics System V3.7 (FZ1A)

The Computer On-site Fast Forensics System V3.7 is mainly used for fast computer data acquisition on-site. It is a forensics system that quickly obtains various types of evidence files in the target computer without dismantling. The system includes account password acquisition, QQ acquisition, fast search and copy of sensitive file, system snapshot, memory mirror image, PE boot, password reset, mirror production and other functions. It can be used for forensics on the Windows operating system and Mac OS X operating system (with optional Mac OS X forensics component) in the boot state, or for forensics on the computer in the off state.



System Interface

Basic Functions

❑ Account Password Acquisition

This function is mainly used to quickly obtain the account password saved on the target computer, and is only valid for the computer in the boot state.

➢ Windows

✧ Local account passwords cached by various browsers: IE4/5/6/7/8/9/10, FireFox, Opera, Chrome, etc.

✧ E-mail passwords: Outlook, Outlook Express, WinLiveMail, Foxmail, etc.

- ✧ Saved account passwords in Credential.
- ✧ Account passwords for LAN and remote login.
- ✧ Login passwords for instant messaging software such as MSN, Windows Live Messenger, Gtalk, etc.
- ✧ Dial-up connection passwords.
- ✧ Login passwords for 32/64-bit Windows XP, Windows 7, Windows 8, Windows 10 and other operating systems.
- ✧ Other passwords cached locally.

➢ Mac OS

- ✧ It can obtain multiple account passwords such as e-mail, instant messaging, and remote login included in the local key-chain.

➢ QQ

- ✧ This function can obtain QQ local record files and other information needed to crack QQ passwords. These files and information can be submitted to the computer forensics software for offline cracking of QQ passwords and chat records.

❑ **Fast Search and Copy of Sensitive File**

It mainly searches and copies sensitive information such as installation file list, chat log file, email, Internet log file, system encryption data, and mobile phone backup file existing on the computer, and supports calculating the file hash value when copying files.

❑ **Dynamic Information Acquisition**

It mainly obtains dynamic information such as process information, service list, network connection information, network sharing information, IP address information, firewall configuration information, clipboard content, and activity trace when the computer is running.

❑ **Memory Acquisition**

There are a lot of sensitive information, such as account passwords, in the computer memory, page files, and hibernation files. This feature enables fast access to memory images, page files, and hibernation files. The memory mirroring function is valid for Windows in boot status.

❑ **Media Mirror Image Acquisition**

This function mainly provides fast mirror image acquisition for hard disk media and optical media. The media mirror image acquisition supports resume from break-point.

- **Password Reset**

  This function mainly provides login password clearing and automatic recovery for Windows XP/vista/7/8/10 and other operating system.

- **Multilingual System**

  The system provides English and Chinese languages to support data acquisition for operating systems that do not have a Chinese character set installed.

Main Features

- **Fast**

  The large-capacity forensics USB flash drive supports USB 3.0 high-speed transmission; the acquisition of account password is completed within 3 minutes, and the copy of sensitive information of normal hard disk is completed within 30 minutes, which is at least 10 times faster than the full-disk copy of Solo4 and other copying machines.

- **In-Depth**

  Unique 32/64-bit Windows xp/vista/7/8/10 login account password extraction. QQ local chat record on-site quick access, supporting offline cracking after acquisition.

- **Easy Operation**

  One-click data acquisition, adapting to the special application requirements of on-site forensics.

- **High Concealment**

  The system copies and browses the file in a self-reconfigurable file system, so that the state of the file can stay completely unchanged. For the online state, the USB trace left by the operation is completely erased to ensure that the forensics process does not leave any trace.

Product Composition

- PE Boot CD (with Windows fast forensics system software) 1
- Standard On-site Forensics USB Drive (with Windows fast forensics system software) 1
- Apple on-site forensics USB drive (with Mac OS X fast forensics system software, optional module) 1
- External Storage Device 1
- Laptop 1

Multi-Channel Parallel Forensics System (FY2)

The Multi-Channel Parallel Forensics System is designed for fast copying of data from a computer's hard drive that is difficult to disassemble. It realizes copying of object hard disk data mainly through multiple channels including USB (2.0/3.0) interface, 1394 interface, eSATA interface, Thunderbolt, and Gigabit Ethernet.

Basic Functions

- Multi-channel parallel storage to fast copy files of the specified suffix type on the target computer.
- Multi-channel parallel storage to fast mirror the specified partitions and hard disks on the target computer.

Main Features

- Multi-channel Parallel Copy

  The system uses multiple channels including USB (2.0/3.0) interface, 1394 interface, eSATA interface, Thunderbolt, and Gigabit Ethernet to quickly parallel copy the object hard disk.
- Disassemble-free Copy

  The system quickly copies the target computer data without disassembling the machine.
- The system supports file copy and hard disk copy to flexibly adapt to actual needs.
- Breakpoint resume is available for mirroring.
- Fast Data Acquisition Speed

  Mirroring speed for SATA hard disk is 6GB/Min, for SSD is 30GB/Min.

Product Composition

- PE CD (containing multi-channel parallel copy software) 1
- USB Flash Drive (containing multi-channel parallel copy software) 1
- Multi-Channel Parallel Forensics Equipment 1
- Forensics Laptop 1

Laboratory Forensics Equipment

Target Operating System Simulator (FZ2)

The Target Operating System Simulator is a special device to start target operating system without original hardware environment and simulate the original computer environment. The device supports the emulation of hard disk, mirror, and snapshot of Windows XP, Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Mac OS X, Linux, etc., and provides the users of above operating systems with computer environment reproduction, and supports local user account password cracking in the character set.

Target Operating System Simulator V4.3 System Interface

Basic Functions

- Support for virtual emulation of physical disks containing operating systems.
- Support for virtual simulation of DD and E01 image files containing operating systems.
- Support for virtual simulation of system snapshots. Can be use with Computer On-site Fast Forensics System.
- Support for the operating system (including 32-bit and 64-bit) simulation of Windows 98, Windows Me, Windows NT, Windows 2000, Windows XP, Windows 2003, Windows 2008, Vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Mac OS X, common Linux operating systems based on 2.6 kernel version (such as Red Flag, Red Hat, SuSe and UbunTu).
- Support password cracking for Windows 2000, Windows XP, Windows 2003, Vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Mac OS X operating system, the support scope is as

follows:

Windows 2000-Windows 2003:

- ✧ 14-digit common alphanumeric passwords;

Windows Vista-Windows 10:

- ✧ 12-digit numerical passwords;
- ✧ 7-digit common alphanumeric passwords;
- ✧ 8-digit alphanumeric (supporting uppercase and lowercase) passwords with !* characters;
- ✧ 9-digit alphanumeric (lowercase) passwords;

Mac OS 10.4+:

- ✧ 8-digit alphanumeric passwords;
- ✧ 6-digit common alphanumeric (lowercase) passwords
- ✧ 6-digit alphanumeric (lowercase) passwords with !* characters;
- ✧ 6-digit common alphanumeric passwords;
- ✧ 7-digit alphanumeric (lowercase) passwords;

For passwords with longer password lengths or higher complexity, decryption can be performed on the Distributed Deciphering and Decryption System.

Main Features

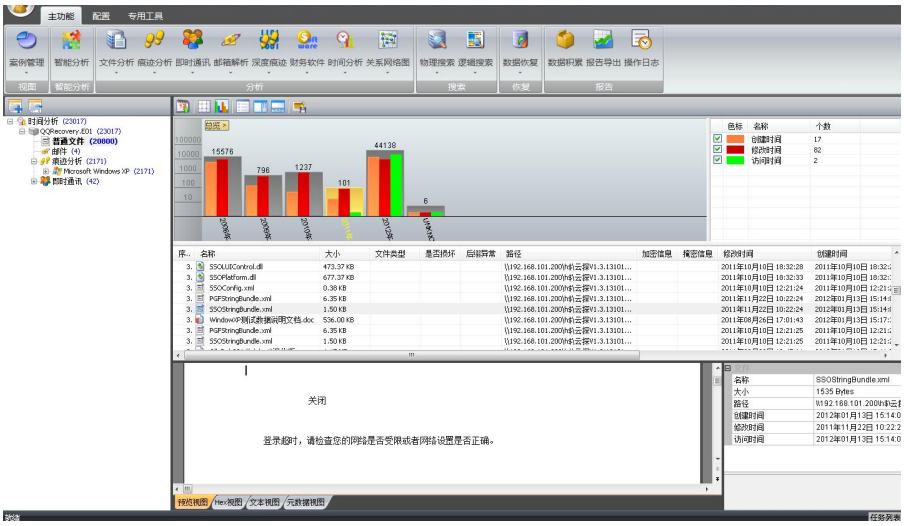
- ❑ Support simulation of the latest operating systems such as Windows 10 and Mac OS 10.12.
- ❑ Support power-on password bypass.
- ❑ Support hard disks (including SSD) with IDE and SATA interfaces.
- ❑ Support system snapshot simulation.
- ❑ Solved the certification problem of OEM operating systems of more than 30 manufacturers.
- ❑ Support direct simulation of mirror images.
- ❑ Solved the blue screen problem caused by multiple driver incompatibility.
- ❑ Meet the requirements of various business scenarios.

Product Composition

- High-performance simulator 1
- Standard simulation software (including Windows simulation module and Windows password cracking module) 1
- Simulation software for Apple (optional, including Apple simulation module and password cracking module) 1
- USB read-only interface device 1

Computer Forensics Software (XF12)

Computer Forensics Software can analyze a variety of media data such as hard disk, optical disk, USB flash drive, memory card, image file, etc. It is a comprehensive computer forensics software that integrates data recovery, anti-forensics file identification, chat record analysis, email parsing, relationship network analysis, online record analysis, keyword search, video summary, data classification, password recovery, reporting and other functions.



Software Interface

Basic Functions

- **Instant Messaging Analysis**

  Support for the analysis of chat records of more than ten kinds of software such as QQ, Taobao, Fetion, Skype, SinaUC, Doshow, YY, etc. Support offline cracking of local chat records on PC version WeChat and the latest QQ V5.3 and above.

- **E-Mail Analysis**

  Support recovery of email files such as foxmail, Outlook, Outlook Express, ThunderBird, Eudora, Netease flash email, etc., and support Chinese, English, Korean, Russian and other languages.

- **Trace Acquisition**

  Support both Windows and Mac OS operating systems, the traces obtained include Internet traces, USB plug-in records, system logs, system patch installation information, system

GHOST installation information, network card information, Thunderbolt download records, Windows boot-up auto-start software, recent access documents, application running traces, etc. Support the analysis of Baidu cloud disk and other network disks. Support the extraction of the input history of the Sogou inputting method and the QQ inputting method, and support the analysis and extraction of the media playback record.

- **Anti-Forensics File Identification**

  Support nearly 400 kinds of suffix exception files, as well as identification of multiple encrypted files, hidden files, and sensitive software.

- **Account Password Extraction**

  Support for extracting passwords from browsers such as IE6/7/8/9/10, FireFox, Opera, Chrome, etc. for Windows systems; passwords of Outlook, Outlook Express, Foxmail and other mailboxes; dial-up connection password; login passwords of 32/64-bit Windows XP/7/8/10 and other operating systems.

- **Data Recovery**

  Support file recovery by means of file system and file signature, support recovery of hard disk lost partitions, hidden tracks of disks and files.

- **Financial Software Analysis**

  Support access to financial software version information installed on the media, connection information with the server, local user account passwords, etc., and support financial software such as Kingdee, Yonyou, 4Fang, and Superdata.

- **In-Depth Trace Acquisition**

  Support page file (pagefile.sys), hibernation file (hiberfil.sys), disk unallocated space acquisition file, document usage record, Internet record, print record, search engine usage trace, cloud client trace, web mail record, chat record, etc.

- **Decompression and Restoration of Hibernation Files**

  Support decompressing and restoring hiberfil. sys to memory mirror file for forensics analysis.

- **Memory Image Analysis**

  Support memory mirror process space reconfiguration, process dump, restore Windows login password password and other functions.

- **Timeline Analysis**

  The system supports timeline analysis functions such as files, Internet records, chat logs, and

emails, and displays all the behaviors of users in a certain period of time in an intuitive way, and discovers the rules of users' behavior.

- **Text Collection**

  Support the collection of continuous text content from disk partitions or any type of file, supports Chinese, English and other languages, supports GB2312, UTF-8, Unicode encoding.

- **Keyword Search**

  Support comprehensive keyword search for hard disk, partition, disc track, sector, and file in binary system and text content. It supports regular expression search and text content search without considering keyword encoding. Support for searching for text in images.

- **File Metadata Extraction**

  Support metadata extraction for Office documents, PDF documents, JPG images and other files.

- **Video Summary**

  The system supports fast frame extraction of mpeg, mpg, wmv, rmvb, rm, vob, asf, avi, mov and other formats, enabling users to quickly view video content.

- **Language Identification**

  The system supports the recognition of nearly 30 kinds of languages such as Tibetan, Uighur and Korean.

- **Confidential File Identification**

  The system is able to scan and identify confidential documents marked with top secret, confidential, secret and other keywords.

- **Compound File Parsing**

  Support Photoshop layer parsing, Thumbs.db thumbnail extraction, image extraction from Office documents and other compound file parsing functions.

- **Relationship Network Diagram**

  The system supports displaying the link between instant messaging account and email account in a network diagram. The user can conveniently view the chat information or the email content between the accounts.

- **Registry Analysis**

  Support extracting and parsing Windows registry files in images; support recovery of deleted registry items.

- **Sensitive Information Extraction**

Support the extraction of sensitive information including mailboxes, instant messaging chat records, contacts, etc. and the standardized export of sensitive information.

- **Fast File Classification**

  The system supports dynamic and fast classification of files under the entire disk, partition, and directory.

- **Multi-View Display of Documents**

  The system provides a variety of viewing functions such as text view, preview, and Hex view of the file. Analysts can view a file from different angles.

- **Report file generation**

  The system supports the generation of survey analysis reports in html, Word, and PDF formats for easy browsing.

Main Features

- Industry-leading QQ local record recovery technology. The system supports for brute force cracking and recovery of the latest QQV5.3 and above in the unknown password state and non-networked state. It supports violent cracking of the WeChat chat record on the computer.
- Strong anti-forensics detection ability.
- The system supports the encryption and recognition of more than 20 commonly used software such as RAR, Office, PDF, Wenjie, and PrivateDisk.
- The system supports the detection of many common masking modes such as Outguess, F5, Jhide, Jspeg, etc. It supports hitching of Jpeg, RAR, Office and other formats of files based on file structure.
- The system supports the detection of CryptCD, CD Encryption Master, SecureBurn and other encrypted discs, and supports the decryption of CryptCD.
- Unique memory forensics function.
- Support for decompressing and restoring of hibernation files of Windows xp/vista/7/8.1/10/2003/2008/2008/2008 R2 to memory mirror images.
- Support for extracting login passwords from memory images. This method does not have character set and password length restrictions, and supports process space refactoring and restoration.

- Powerful mailbox file parsing capability, supporting for parsing of oversized mailbox files above 15G.
- The recovery supports for various media, including hard disks, CDs, USB flash drives, memory cards, etc. The system has a unique disc recovery technology, which supports the recovery of abnormal size files, hidden files and deleted files in the disc by file system reconstruction. The disc format supports UDF and ISO9660 file systems.
- The unique financial software login account password extraction function supports the analysis of various financial software such as Kingdee, Yonyou, Superdata, and 4Fang.
- In-depth forensics: support internal files of 17 kinds of compressed files, internal mails of 5 kinds of mailbox files, internal attachments of emails, and automatic deep search and analysis of multiple composite files.
- Support for both Windows and Mac OS operating systems.

Product Composition

- Computer Forensics Software 1
- Laptop (optional) 1

Multi-Functional Computer Forensics and Analysis System (FZ9)

Multi-functional Computer Forensics and Analysis System is a comprehensive forensics and analysis system of multiple data sources, with both software and hardware integrated. Featuring high-speed parallel hardware design, multiple interfaces, strong computing and analyzing capabilities, the system can carry out high-speed hard disk duplication, data erasure, computer forensics and analysis, as well as operating system simulation analysis. The working ability of the system is equivalent to a small forensics laboratory, with the ability to simultaneously handle multiple hard drives, which can solve the problem of large capacity and quantity of hard disks in current forensics analysis.

Basic Functions

- **High-Speed Parallel Data Duplication**
  - ✧ provide 4 read-only SAS/SATA interfaces, 1 multi-functional read-only interface and 1 multi-functional memory card read-only interface, supporting parallel acquisition of six-way read-only interfaces.
  - ✧ Support four-way hard disk parallel copy function, and support multiple copy methods such as "one-to-four" and "four-to-four".
  - ✧ Adopt multi-threading acceleration technology to accelerate the speed of data verification and compression during data acquisition.
  - ✧ Equipped with four 2TB SATA hard drives as storage media to form a RAID array to

improve overall IO performance of data.

- **High-Speed Parallel Data Processing**
  - ✧ Adopt double panel display for parallel display and processing of analysis results
  - ✧ Optional GPU high-performance graphics card to further improve the speed of search and decryption
- **Computer Forensics Analysis**
  - ✧ Integrated computer forensics software supports data recovery, chat record analysis, mailbox analysis, trace analysis, relationship network analysis, keyword search, video summary, encrypted file recognition, format abnormal file identification, anti-forensics software identification, timeline analysis, etc.
  - ✧ Support the analysis of Windows and Apple operating system.
- **Dynamic Simulation Analysis**
  - ✧ Integrated operating system simulation software supports the simulation of hard disk, mirror and snapshot of operating system such as Windows/Mac OS/Linux for operating system login password cracking, login password bypass, sensitive information extraction in the simulation environment.
- **Decoding and Decrypting**
  - ✧ Support brute force attack, which specifies character set combinations and password digit ranges
  - ✧ Support dictionary cracking method, built-in common dictionary such as phone number, birthday, etc., users can also import specific dictionary
  - ✧ Support for decryption of encrypted files or ciphertext including MD5, NTHash, SHA1, MySQL, SKYPE key, SafeBoot key, Mac user password, PDF, WinRAR, WinZip, Office document, TrueCrypt, PGP, WPA wireless network login password, QQ password, etc.
- **In-Depth Data Recovery**
  - ✧ Support for recovery of fragmented file data after corruption coverage
  - ✧ Support automatic/manual reorganization and recovery of server array data such as raid0, raid1, raid5, raid5e, raid5ee
  - ✧ One-click detection to quickly diagnose problems with storage media (board, firmware, hidden sectors, encryption, usage time, hard disk read errors, etc.)
  - ✧ Quickly fix common firmware issues, fix hidden sectors, decrypt hard disk ATA

Main Features

- **One-Stop Solution of Forensics and Analysis**

  The one-stop solution integrates multiple forensics functions such as data acquisition, static analysis, dynamic simulation analysis, transcription, etc, and is compatible with third-party forensics software such as Encase, FTK, and X-ways.

- **Independent Development of Core Software**

  Built-in self-developed computer forensics software, target operating system simulation software, data copy and erasure software, in-depth data recovery software, password recovery software and other professional forensics analysis software.

- **Compatible With Third-Party Analysis Software**

  As a set of forensics hardware platform, the system is compatible with third-party forensics software such as Encase, FTK, and X-ways.

Product Composition

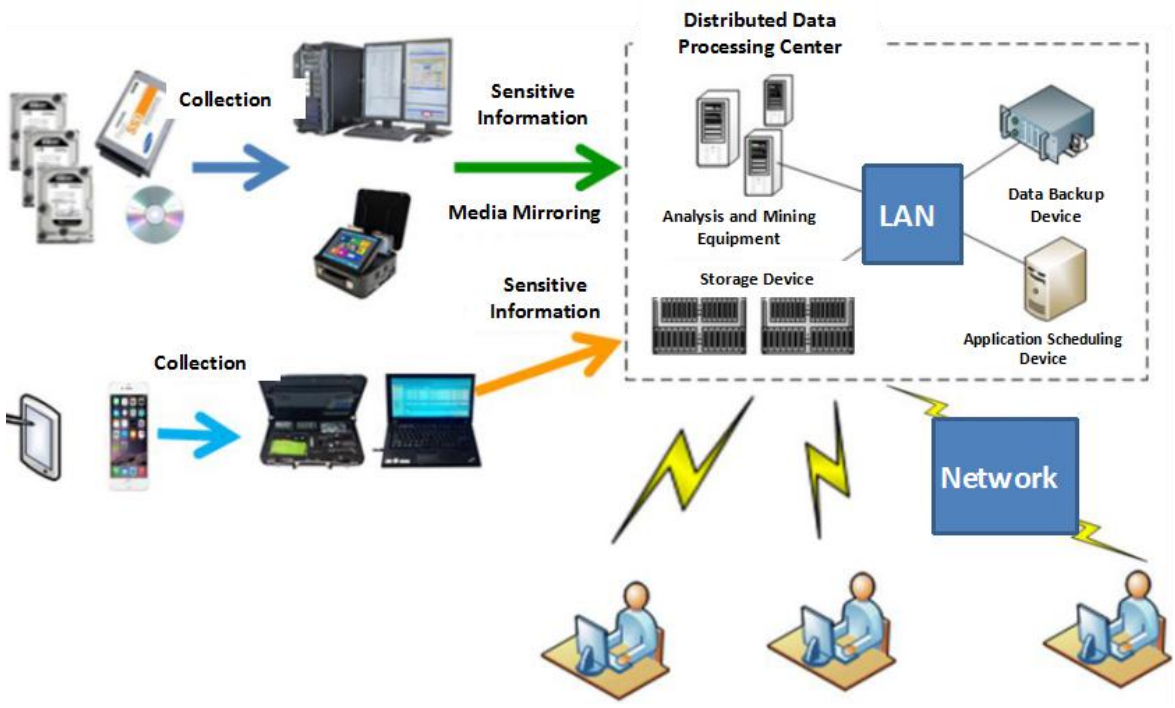
The system consists of computer forensics analysis workstation and supporting forensics analysis software. The software and hardware of the system can be flexibly expanded and customized according to user needs.

- Computer Forensics Analysis Workstation 1
- High-speed Hard Drive Copy and Erasure Software 1
- Computer Forensics Analysis Software 1
- Target Operating System Simulation Software 1
- In-depth Data Recovery Software (optional) 1
- GPU Acceleration Card and Decryption Software (optional) 1

Electronic Forensics Data Analysis System (1A01B)

Electronic Forensics Data Analysis System is used to put together data from smart terminals and computers collected by front-end acquisition devices and, including structural data (address book, instant messaging information, microblog information, mail information, etc.) and non-structural data (hard disk, CD, image file, etc.), providing unified storage of data, one-click forensics, one-click search, association mining, report output and other functions. It adopts a distributed, parallel architecture of processing, which enables multiple servers to analyze data concurrently. As such, post-processing is quickened, accumulated data resolved, history data matched, and these data can be analyzed by multi-users. All these functions contribute to the proactive detection for post-forensics processing.

While conducting operations, users can deploy the collection device of such platform outside. Multiple collectors can work in parallel with one another, and the data collected will be transmitted to local networks via fiber or other channels for storage and analysis. Local users can view and query these data for later use.



System Structure

Basic Functions

- **Data Organization and Management**
  - ✧ Define various roles based on service demands, and provide functions of user group and user

management. A head of the group can be appointed who will consequently have access to data of group members and administer multi-level services.

- ✧ Distribute access to data, access of their visibility and operational range. And different access can be distributed based on service needs.
- ✧ Administer case group, cases and persons. Each case group can cover many cases, and each case many persons. Data collected can be put under a case or a person.
- ✧ Set up name and code for cases and identify the nature of them. ***These features are extendable.***
- ✧ Set up name, phone number, mailbox account for persons. ***These features are extendable.***
- ✧ Check data of history cases: Case total number, object total number, forensics type and forensics volume.

❑ **Data Collection**

- ✧ Support non-structural data collection like hard disk, optical disk, memory card, mirror, file, directory, etc. These data can be compressed during collection, saving storage space.
- ✧ Smart collection of sensitive data. These data must comply with the Data Standards on Computer Post-forensics Processing Platform.
- ✧ Collect reports produced by third-party forensics tools, such as QFK, X-Ways, Oxygen and DC4500.
- ✧ Collection of "cards-to-pictures".

❑ **Data Early-Warning**

- ✧ Support for executing control over targeted object, keyword, bank account, cell phone number, QQ number, WeChat number, E-mail account, login IP address, electronic goods, access URL, etc. The control conditions can be set flexibly and the results are easy to access.

❑ **Object Relational Library Construction**

- ✧ Support information collection of contacts from mailbox files, such as Outlook, Thunderbird, Foxmail, Outlook Express, Windows Live Mail, Apple Mail.
- ✧ Support information collection of contacts from phone backups, such as Apple and 360.
- ✧ Support information collection of contacts from VCF files.
- ✧ Support information collection of contacts from mails.
- ✧ Support collection of accounts and virtual ID from chatting tools.

- ✧ Support information collection of contacts from “cards-to-pictures”, even if one such picture includes multiple cards.
- ✧ Open collection rules of code address, users can modify these rules and add collection types of code address.

❑ **One-Click Forensics**

- ✧ Built-in distributed engine for forensics and analysis. It can restore data, recognize anti-forensics software, and analyze chatting records, mailboxes, traces and synthesized documents. Forensics can be done automatically and through one button.
- ✧ Over 10TB of data capacity and supports server forensics.

❑ **One-Click Retrieval**

- ✧ One-click search like Google and Baidu. The backend adopts a distributed framework. Via special search engine, an index will be established after text transformation of collected structural and non-structural data. The system can fast retrieve mass data, covering simplified and traditional Chinese, English and Japanese. Text transformation of non-structural data supports Office, PDF, mail attachments, compressed files and so on.

❑ **Physical Search**

- ✧ Distributed 2-digit search for non-structural data from such things like hard disk, mirrors, light disk and memory card, and support Unicode, Utf8, Gb2312 and other encoding modes, and offer regular expressions.

❑ **Sensitive Data Match**

- ✧ Match past standardized information, code address as well as enemy information with the standardized information that were abstracted via data collection.
- ✧ Match past standardized information, code address as well as enemy information with external documents.
- ✧ Support match of standardized information and enemy among multiple cases and collections.
- ✧ Matching results can track case, source and export.

❑ **Common Feature Mining**

- ✧ Support mining common features such as common contacts, software, USB storage device (USB serial number), etc. in multiple cases and hard disks.

❑ **Differential Feature Mining**

- ✧ Support mining differential features such as differential contacts, software, USB storage device (USB serial number), etc. in multiple cases and hard disks.

❑ **Analysis of Correlation**

- ✧ Analyze how phones, instant communications, mails in collected data are inter-linked, and provide start point analysis and range analysis to display relational network in the form of graph. Besides, the graph of matching results can be edited.
- ✧ Provide service digging models in terms of intermediary, partner and intimacy for structural data mining. These results can be shown graphically. Users can self-build such models.

❑ **Pattern Analysis**

- ✧ Conduct timeline analysis on time-related data, namely, call, surfing and chatting records, mails and documents. That directly demonstrates all operations made by the object and help figure out behavior rules.
- ✧ Analyze various kinds of data, show users statistics of operations in lists and graphics, and predict assistant services. That is how the system can form a forecast of development.

❑ **Basic Database Construction**

- ✧ HASH basic database is equipped—an operational system that has a white list of frequently used software for filtering documents and changing software's verification, and a black list of sensitive software, tools and documents for fast locating important files.
- ✧ Allow users to self-build a HASH database or import a new one, and upload it to the backend.
- ✧ Allow users to import and retrieve registered info repository and other social libraries.

❑ **Terminal Activity Track Analysis**

- ✧ Support the extraction of geographical location information in APPs and pictures, including longitude, latitude, address, etc., and combines offline maps to display the activity track of end users.

❑ **Collaborative Forensics**

- ✧ Support multi-person collaborative forensics, that is, multiple people in different laboratories and different regions, and simultaneously conduct forensics analysis of a case data, and the analysis results are shared in real time.
- ✧ Support remote assistance for forensics, that is, the expert remotely accesses the local forensics equipment by accessing the remote assistance software deployed in the terminal,

and performs point-to-point analysis and processing on the electronic medium connected to the local forensics device.

- **Accumulated Percentage of Outturn**
  - ✧ Accumulate data such as documents, emails, instant messages, and traces, and share among multiple people.
  - ✧ Provide reporting function that supports one-click automatic generation of standard post-processing reports.
- **Comprehensive Fusion**
  - ✧ Fusion search supports one-click search of data between current level and upper level, and the results are uniformly displayed at current level.
  - ✧ Fusion comparison supports sensitive data comparison between current level and upper level. The comparison results hide the sensitive data content of upper level, and only provide non-code address information.
- **Aggregate Statistics**
  - ✧ Support the background to automatically aggregate the sensitive data of current level to the upper system. Users can enable or disable this function, and flexibly set the upload start time and time interval.
  - ✧ The upper system can collect statistical data such as the type and quantity of data aggregated by the lower system, and supports the display of statistical results by means of charts and lists.

Main Features

- **Comprehensive Supports for Forensics Data Aggregation**
  - ✧ Support for multiple data types: unstructured data such as hard disks, optical disks, memory cards, USB flash drives, mobile phones, directories/files, images, and structured data in TXT, CSV, and XLS formats.
  - ✧ Support for multiple data collection methods: It not only supports the direct collection of original data of key cases, but also supports multi-person collaborative forensics. It also supports only extracting structured data related to cases and reducing storage and bandwidth requirements.
- **Elastic Expansion of Computation and Storage**

- ✧ Aiming at the characteristics of forensics data and format, a distributed computing and storage framework supporting file data, mirror data and structured data analysis and mining is established by using file system technology, relational database technology, graph database technology and NOSQL technology. The framework can flexibly add analysis devices, index devices, and storage devices according to data size to improve data analysis and processing capabilities.

❑ **Comprehensive Extraction of Object Relational Library**

- ✧ Collect standardized information from telephone book, mailbox contacts, chatting contacts and account password, and bank account, mailbox account and other information of single code address. These two kinds of collection methods are mutually complementary.
- ✧ Support various formats, such as mailbox clients, phone backups, third-party forensics tool reports, etc.

❑ **Comprehensive and High-speed Search**

- ✧ Offer services of all round data retrieval. Full-text retrieving technology is adopted to transform various data to text ones and establish index, providing users with convenient, fast keyword search services. Waiting time for first batch of searching results costs less than one second, with system data covered 100%. In case of different services, routine and fuzzy search.

❑ **Standardization and Automation of Forensics Process**

- ✧ Strong built-in engine of data forensics and mining. Analyze and mine mass data from various medium like phones, computers and tablets. One-key collection and automated forensics and mining are supported.

❑ **Convenience and Security of Collaborative Forensics**

- ✧ Apply ID, encrypted transmission, RFB protocol-based long distance assistance, proxy auditing to safeguard links and data. While conducting long-distance assistance, the assistant will not be able to download files from computers of those receiving remote help, neither can they copy or paste these files. Moreover, the system has post-event examination, which can replay all operations of procedures and contents made by assistants.

Product Composition

The platform consists of computer collection device, smart terminal collection device, database server, application scheduling device, GIS map, data analysis device, full-text search device, memory array, etc. Data analysis device is scalable in accordance with data size and performance requirements

- Database Server (scalable) 1
- Application Scheduling Device 1
- GIS Map (optional) 1
- Data Analysis Device (scalable) 1
- Fiber Optic Disk Array (scalable) 1
- Computer Collection Device (scalable) 1
- Smart Terminal Collection Device (scalable) 1
- Service Terminal (scalable) 1
- Network Switch 1
- System Software 1

Mobile Phone Forensics Equipment

Mobile Phone Forensics System (FZ4B)

The mobile phone forensics system is a set of intelligent terminal forensics equipment that enables users to complete data extraction, decoding, analysis and reporting on one device, supporting physical, logical (file system) and application-level forensics on data of various devices (including deleted data), including smart phones, tablet terminals, and domestic counterfeits.

The mobile phone forensics system can quickly extract data from various smart terminals, expansion card and SIM card (or UIM card). The data covers terminal device information, phone book, SMS, call record, photo, account password, email, social activity record, geographic location, cloud client information, voice information, video information and other types of data.

Mobile Phone Forensics System V4.0

Basic Functions

- **Extraction of Smart Terminal Data**
  - ✧ Smart Terminal Basic Information

    The device basically obtains information such as basic information , address book information, call record, short message record, multimedia message record, and calendar record.
  - ✧ Instant Messaging Information

    Support the information extraction such as accounts, friends, and chat records of various

instant messaging APP, including QQ, WeChat, Fetion, EasyChat, LaiWang, WangWang, Line, MiTalk, MOMO, Skype, YY, WhatsApp, TalkBox, Voxer, Kakao and RenRen.

- ✧ Micro Blog

  Support Sina Weibo, Tencent Weibo, LOFTER, etc.

- ✧ E-mail Information

  Support the extraction of account passwords, e-mail contents and other information of system built-in mailbox, Gmail client, QQ Mail client, 163 Mailbox client, 189 Mailbox client, etc.

- ✧ Browser Information

  Support the extraction of Internet traces, account passwords, favorites and other information of system built-in browser, QQ Browser, UC Browser, Opera Browser, Baidu Browser, Dolphin Browser, 360 Browser, etc.

- ✧ Geographic Location Information

  Support the extraction of geographic locations of various applications such as Google Maps, Baidu Map, AMAP, Careland, Navidog, Ctrip Travel, and Didi Taxi.

- ✧ Electronic Commerce Information

  Support the acquisition of electronic commerce information of JD, Tmall, etc.

- ✧ Cloud Client Information

  Support the extraction of accounts, upload records and cloud information of more than 10 kinds of cloud client APP, such as Baidu Netdisk, Huawei Cloud, Tencent Micro Cloud, iCloud, OneDrive, Google Drive, and DropBox.

- ✧ Other Information

  Support the extraction of device connection information, mobile phone account passwords, file data, etc.

❑ **Unlocking Device for Android**

- ✧ Support for most Android mobile phone forensics with lock screen password using Qualcomm SOC solution.
- ✧ Support for most Android mobile phone forensics with lock screen password using MTK SOC solution.
- ✧ Support for most Android mobile phone forensics with lock screen password of Samsung.

- **Smart Terminal Simulation for Android**
  - ✧ APP Simulation for Android System

    Support simulation of system APP such as address book, SMS, and dialing.
  - ✧ Third-party APP Simulation for Android

    Support online or offline simulation of WeChat, QQ, WhatsApp, Skype, Facebook, Sina Weibo, Tencent Weibo, QQ Mail, NetEase Mail, Baidu Netdisk, Tencent Micro Cloud, Huawei Cloud, Ctyun, and 360 Cloud.
  - ✧ The simulation system supports hardware parameter simulation, which can be connected to the Internet to realize manual or automatic acquisition of cloud data.

- **Smart Terminal Data Analysis**

  Support file analysis, keyword search, relationship network analysis, timeline analysis, etc.

- **Physical Acquisition and Analysis**

  Support mirroring, mirror analysis and data recovery for mobile phone and memory card.

- **Dedicated Tools**

  Support boot password cracking, boot password bypassing, WeChat brute force cracking, temporary root, APP memory mirroring, etc. For Android.

- **Case Management**

  Support case management, report export, standardized data export, data upload and other functions.

Main Features

- Account Password Extraction: Support 17 kinds of local cache account password information such as email, WIFI, gesture, QQ, WeChat, browser, and cloud client.
- Support for commonly used international APP: Facebook, FB Messenger, FB Messenger Lite, Instagram, Kakao, Kik, Line, Skype, Telegram, Twitter, Viber, VK, Whatsapp, Zalo, etc.
- Support unlocking of Android mobile phones, covering over 85% of mobile phones including Huawei, Samsung, MI, OPPO, vivo and other mainstream brands.

Product Composition

- ❑ Mobile Phone Forensics Analysis Software 1
- ❑ Portable Forensics Kit (containing data cable, memory card, signal interference unit, etc.) 1
- ❑ Laptop 1
- ❑ Unlocking Device for Android (optional) 1
- ❑ Operating System Simulation Module for Android (optional) 1

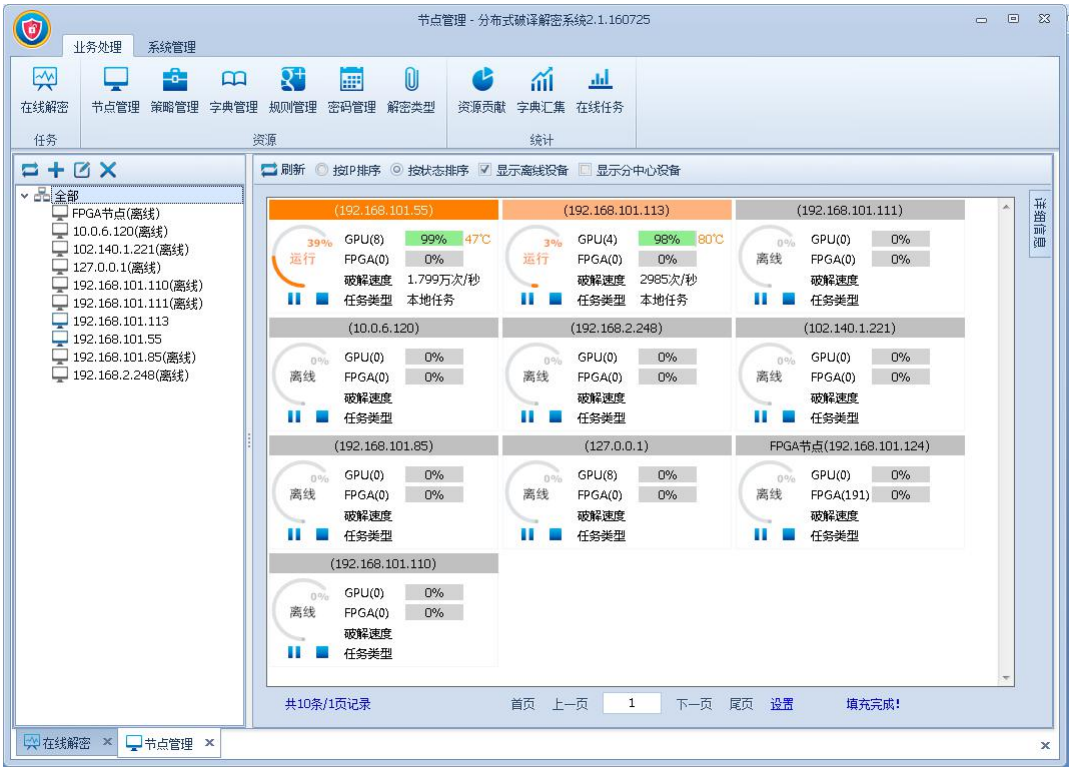
Deciphering and Decryption Equipment

Distributed Deciphering and Decryption System V3.0 (FZ6)

The Distributed Deciphering and Decryption System is a special device that applies CPU/GPU/FPGA parallel computing technology, distributed computing technology and hardware acceleration technology for deciphering and decrypting. The system uses dedicated acceleration equipment and self-developed decryption program to support the analysis of multiple types of encrypted files or cipher texts, featuring fast decryption speed, long-time stable and reliable operation, and strong scalability.

GPU Decryption Device

FPGA Decryption Device



System Interface

Basic Functions

❑ Password Cracking

The system provides a variety of password attacks, including:

✧ Dictionary Attack

Attacks using locally accumulated large-capacity cryptographic dictionary libraries.

✧ Dictionary Expansion Attack

Attacks using dictionary morphing, dictionary+dictionary, dictionary+rule, etc.

✧ Rule Attack

Performs full-space search by specifying the combination of character sets and the range of password digits. Rules are divided into primary rules and advanced rules.

The performance indicators of commonly used decryption types are as follows:

Cracking Performance of Single 4U GPU Device

No.	Decryption Type	Decryption Speed	Decryption Digits/Decryption Time
1	RAR	110,000 / sec	10-bit number passwords/2 days 7-bit common alphabetic (lower-case letters) passwords/1 day 6-bit common characters, numbers, alphabetic passwords/20 days
2	OFFICE2007	350,000 / sec	10-bit number passwords/1 day 7-bit common alphabetic (lower-case letters) passwords/1 day 6-bit common characters, numbers, alphabetic passwords/16 days
3	MD5	64 billion / sec	15-bit number passwords/1 day 11-bit common alphabetic (lower-case letters) passwords/2 day2 8-bit common characters, numbers, alphabetic passwords/1 day
4	NTHash	70 billion / sec	15-bit number passwords/1 day 11-bit common alphabetic (lower-case letters) passwords/2 day2 8-bit common characters, numbers, alphabetic passwords/1 day

Cracking Performance of Single 14U FPGA Device

No.	Decryption Type	Decryption Speed	Decryption Digits/Decryption Time
1	RAR	1.05 million / sec	10-bit number passwords/1 day 8-bit common alphabetic (lower-case letters) passwords/5 days 6-bit common characters, numbers, alphabetic passwords/3 days
2	OFFICE2007	2.7 million / sec	11-bit number passwords/1 day 8-bit common alphabetic (lower-case letters) passwords/2 days 6-bit common characters, numbers, alphabetic passwords/1 day
3	MD5	230.4 billion / sec	15-bit number passwords/1 day 11-bit common alphabetic (lower-case letters) passwords/1 day 8-bit common characters, numbers, alphabetic passwords/1 day
4	TrueCrypt (default)	4.6 million / sec	12-bit number passwords/1 day 8-bit common alphabetic (lower-case letters) passwords/1 day 6-bit common characters, numbers, alphabetic passwords/1 day

❑ **Task Management**

✧ The management of the process of submitting, approving, running, stopping, etc. of the task is realized, and the task submission includes setting the decryption upper limit time, priority, decryption strategy, etc.

✧ Realize the display of various information of the task, including decryption progress, decryption speed, running time, remaining time and decryption results.

❑ **Decryption Strategy Management**

✧ Implement the construction and management functions for password libraries, dictionary libraries, rule libraries, and strategy libraries.

✧ Intelligent analysis of decryption dictionary and decryption rules automatically evaluates decryption dictionary and decryption rules from frequency of use and probability of hitting password.

- ✧ Analyze password library to extract the law of hitting cryptography from the width of the password, the distribution of the character space, etc.

❑ **Decryption Node Management**

- ✧ Manage the adding, deleting, etc. of decryption node resources. Real-time collection and display of various operational status information, load information, and configuration information of node resources in the cluster. If the set alarm limit is exceeded, the program automatically stops the operation and alarms to prevent accidents.

❑ **Information Statistics Function**

- ✧ Statistics can be made on the submission status, approval status, decryption status, and the distribution of decryption type of the decryption task in the selected time.
- ✧ Statistics on the submission status of the decryption dictionary in the selected time.

Main Features

- ❑ The decryption type supports more than 200 algorithms, including WinRAR, WinZip, Office (2003-2013), 7Zip, TrueCrypt, PGP, HWP, MD5, NTHash, SHA1, MySQL, SKYPE keys, SafeBoot keys, Apple user passwords, PDF , WPA wireless network login password, etc.
- ❑ The system supports various decryption modes, among which brute force attacks support dictionary attacks, dictionary expansion attacks, and rule attacks. Compared with similar decryption systems, it supports more decryption modes and improves the efficiency and success rate of brute force cracking.
- ❑ Computational resources support polymorphism and support unified scheduling and joint decryption of various types of computing resources such as CPU, GPU, and FPGA. The GPU supports the graphics cards of NVIDIA and AMD.
- ❑ Great Scalability. The decryption node can be dynamically added, and the decryption module is integrated in a plug-in form to support custom development.
- ❑ High decryption performance. The performance of a single GPU and FPGA device is comparable to that of a small cluster. FPGA devices have high density and low power consumption.
- ❑ Good reliability. The dedicated hardware acceleration device guarantees the long-term stable operation of the system from the hardware and software.
  - ✧ Automatic recovery of crack progress is supported under abnormal power outages, etc.

- ✧ Professional power supply, heat dissipation and temperature control measures to prevent equipment from overheating.
- ✧ The software monitors various operating state parameters of the GPU and the FPGA server in real time. If the set alarm limit is exceeded, the program automatically stops the operation and alarms to prevent accidents.

Product Composition

❑ Dedicated GPU Decryption Equipment	1 or more (scalable)
❑ Dedicated FPGA Decryption Equipment	1 or more (optional, scalable)
❑ Node Management Server	1
❑ Software CD (containing common network cryptographic library)	2