Superbio

苏博医学

诚信/务实/创新/高效

Electronic Evidence Testing Laboratory

Jiangsu Superbio Biomedical Co., Ltd.

Definition

Electronic Data

Information data formed based on electronic technologies such as computer applications and communications, including static data and dynamic data stored, processed, transmitted, and expressed in electronic form.

Excerpt from: *General Code of Practice for the Judicial Appraisal of Electronic Data*
SF/Z JD0400001-2014

Background

The development of computers, communication and other technologies in current society makes people inseparable from informatization, and thus forms a digital space field that is gradually and comprehensively covered. Nor is it surprising that criminal offenses have infiltrated the field or have inevitably left digital traces of crime in the field. Therefore, it is gradually becoming the norm for the current investigating agencies to detect cases by finding criminal traces through electronic data information. Electronic evidence has become one of the powerful weapons for public security organs to handle cases. Compared with traditional evidence, electronic data has many characteristics such as concealment, virtuality and easy-tampering, which poses a huge challenge for the prosecutorial and judicial authorities to review this new type of evidence. Due to the lack of relevant professional knowledge, most case handling personnel often neglect the examination of electronic evidence, which may lead to unjust, false and wrong cases.

In 2012, electronic data was written into the new Criminal Procedure Law and the Civil Procedure Law, officially becoming one of the statutory evidence types.

Application

Electronic Evidence

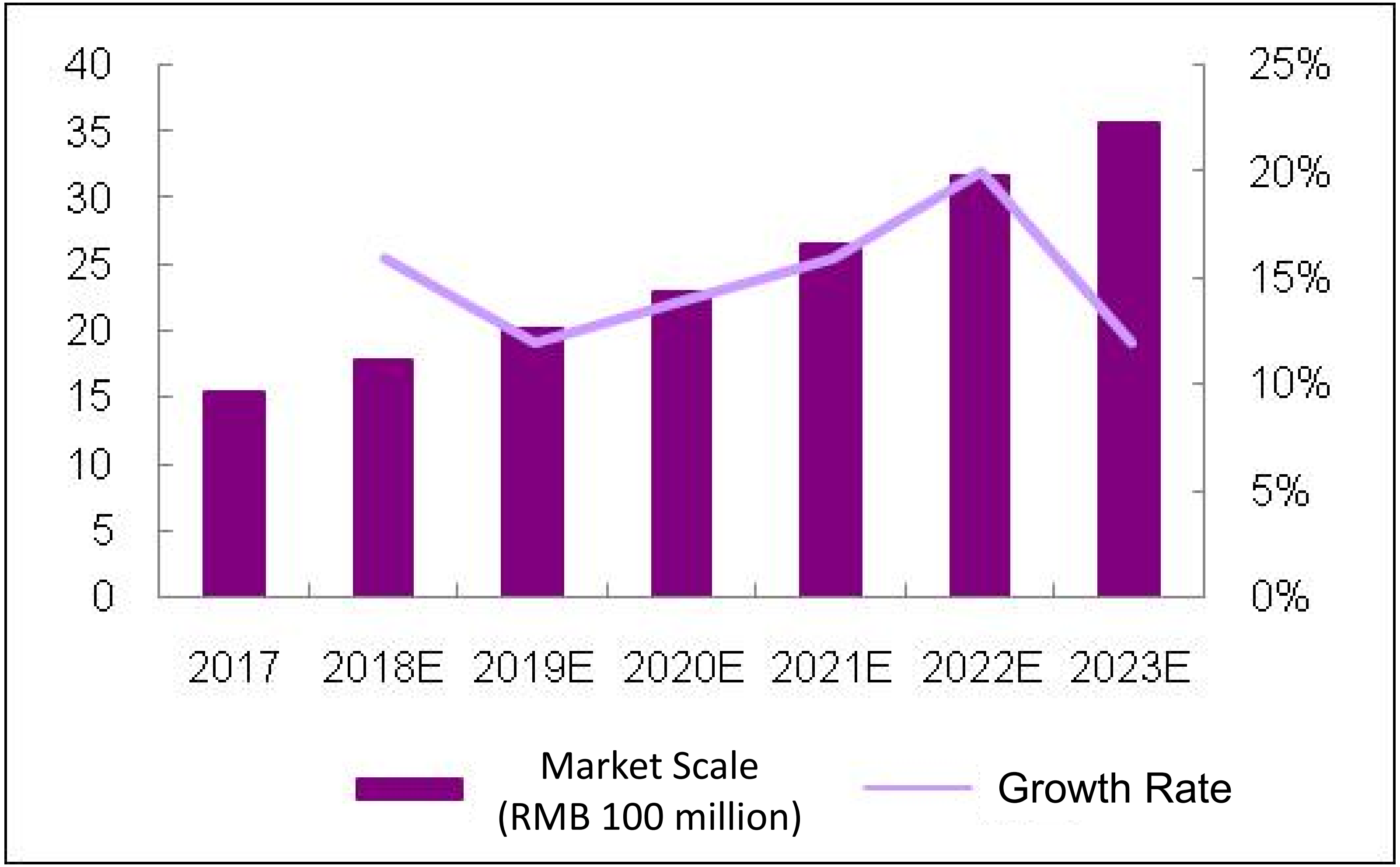
Collect and analyze electronic data in mobile phones, computers, mobile hard disks, USB flash drives, memory cards, cloud storage, and various electronic data storage devices to form electronic evidence that is consistent with judicial effectiveness.

Electronic data forensic identification can prove the facts of criminal cases, administrative cases and civil cases, and can also serve non-litigation activities.

Public Security Bureau, Procuratorate, Supervision Committee, Industry and Commerce Bureau, Taxation Bureau, Customs, Securities Regulatory Bureau, etc.

Prospect

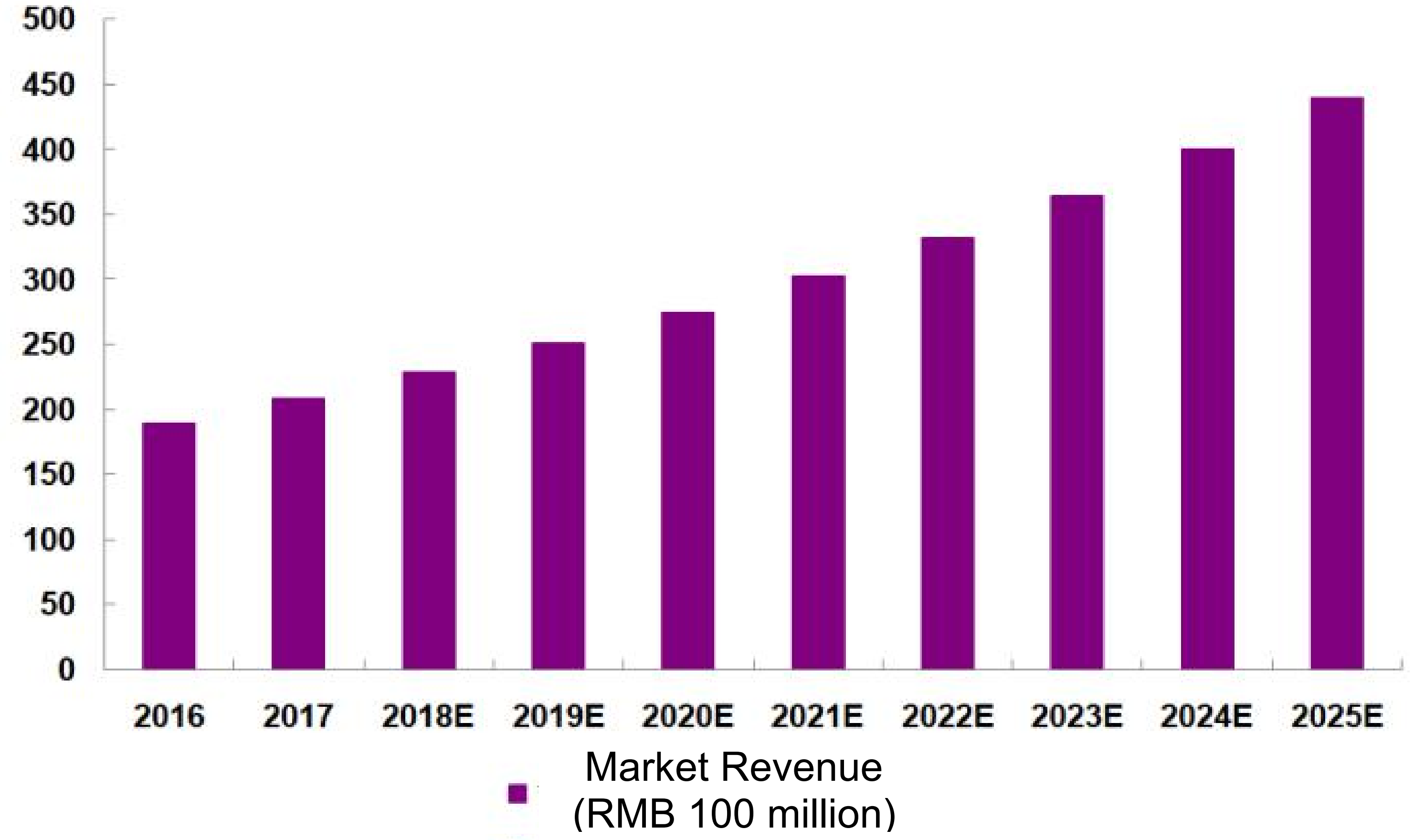
According to the “2017-2023 China Electronic Data Forensics Industry Market Operation Situation and Development Prospect Forecast Report” released by Zhiyan Consulting in 2017, the scale of China's electronic data forensics market will reach RMB 3.562 billion by 2023, with a CAGR of 15%.



Prospect

According to the Electronic Forensics Industry Report of TMR Research Institute in New York, the global market for electronic data forensics in 2016 is close to RMB 18.9 billion. It is expected to reach RMB 43.9 billion in 2025, with a CAGR of 9.8%. In terms of market distribution, the United States leads the world, followed by Europe, and the Asia-Pacific region is developing rapidly and will continue to contribute considerable revenue in the future.

Global Electronic Data Forensics Market Revenue 2016-2025



Multi-Functional Computer Forensics and Analysis System

The Multi-Functional Computer Forensics and Analysis System adopts high-speed parallel hardware design, which can solve the problem of large capacity and quantity of hard disk in forensic analysis. It is a “one-stop” forensic platform of the laboratory.

Main Functions of Multi-Functional Computer Forensics and Analysis System

□ High-speed Data Parallel Collection

- ➢ Provides four SAS/SATA hard disk read-only interfaces, one multi-function read-only interface, one multi-function memory card read-only interface, having the ability of parallel collection with six read-only interfaces.

□ Computer Forensics Analysis

- ➢ 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.

Main Functions of Multi-Functional Computer Forensics and Analysis System

□ Dynamic Simulation Analysis

- Integrates target operating system simulation software, supporting 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.

□ In-depth Data Recovery

- Supports recovery of fragmented file data after corruption coverage.
- Supports automatic/manual reorganization and recovery of server array data such as raid0, raid1, raid5, raid6, raid10, etc.
- One-click detection to quickly diagnose problems with storage media (PCB, firmware, hidden sector, encryption, utility time, hard disk reading errors, etc.)
- Fast fix common firmware issues, fix hidden sectors, and decrypt hard drives.

Portable Integrated Forensics Device

Portable Integrated Forensics Device is a portable comprehensive forensic analysis device that integrates various types of electronic evidence fixation, forensic analysis and report generation, including storage media, computers, intelligent terminals, and hard disk recorders.

Storage Media Copier

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 disk, mobile hard disk, memory card and various types of optical disks.

□ Basic Functions

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

Multi-Channel Parallel Forensics Equipment

The device is designed for quick 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.

Cell Phone Forensics System

The cell 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.

Main Functions of Cell Phone Forensics System

□ Comprehensive Data Extraction of Intelligent Terminal

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

Main Functions of Cell Phone Forensics System

□ Android Phone Unlock

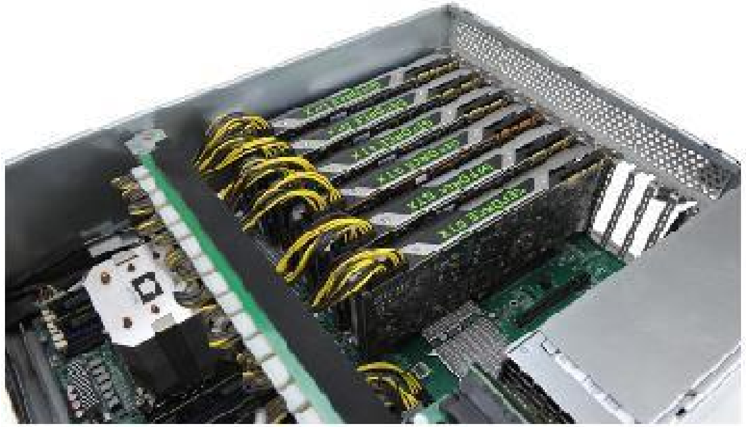
- Supports for most Android cell phone forensics with lock screen password using Qualcomm SOC solution.
- Supports for most Android cell phone forensics with lock screen password using MTK SOC solution.
- Supports for most Android cell phone forensics with lock screen password of Samsung.

□ Android Intelligent Terminal Simulation

- Supports 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.

Distributed Deciphering and Decryption System

The distributed deciphering and decryption system mainly solves the problem of deciphering and recovering encrypted data such as encrypted files, operating system passwords, and Hash algorithms. The system uses GPU hardware acceleration technology and combines distributed parallel computing technology to improve the efficiency and ability of deciphering and decrypting. The system currently supports more than 200 types of encrypted data/algorithm cracking.



Main Functions of Distributed Deciphering and Decryption System

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.

□ Dictionary Attack

- Attacks using locally accumulated large-capacity cryptographic dictionary libraries.

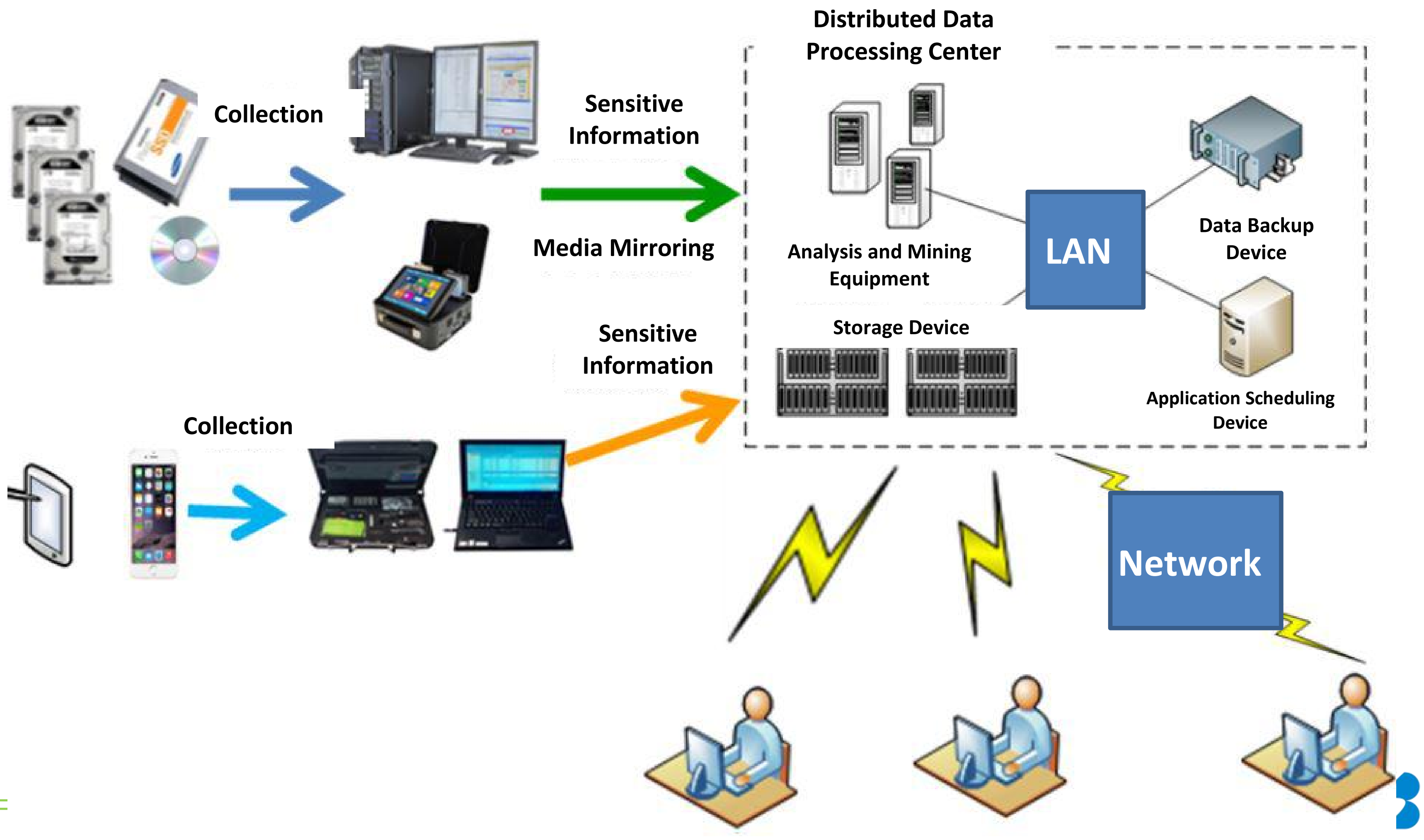
□ Dictionary Expansion Attack

- 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.

Electronic Forensic Data Analysis System



Main Functions of Electronic Forensic Data Analysis System

□ Data Early-warning

- ➢ Supports 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.

□ Correlation Analysis

- ➢ Supports the analysis of the communication relationships such as telephone, instant messaging, and mail in the collected data. Provides two methods of starting point analysis and scope analysis, and presents the network of communication relations in a graphical way. Meanwhile, the analysis result graph can be manually edited, and the graph can be linked to the original record.
- ➢ Provides business mining models such as middlemen, accomplices, and intimacy for mining structured business data, and displays the mining results in a graphical way. Self-built models are supported.

Main Functions of Electronic Forensic Data Analysis System

□ Common Feature Mining

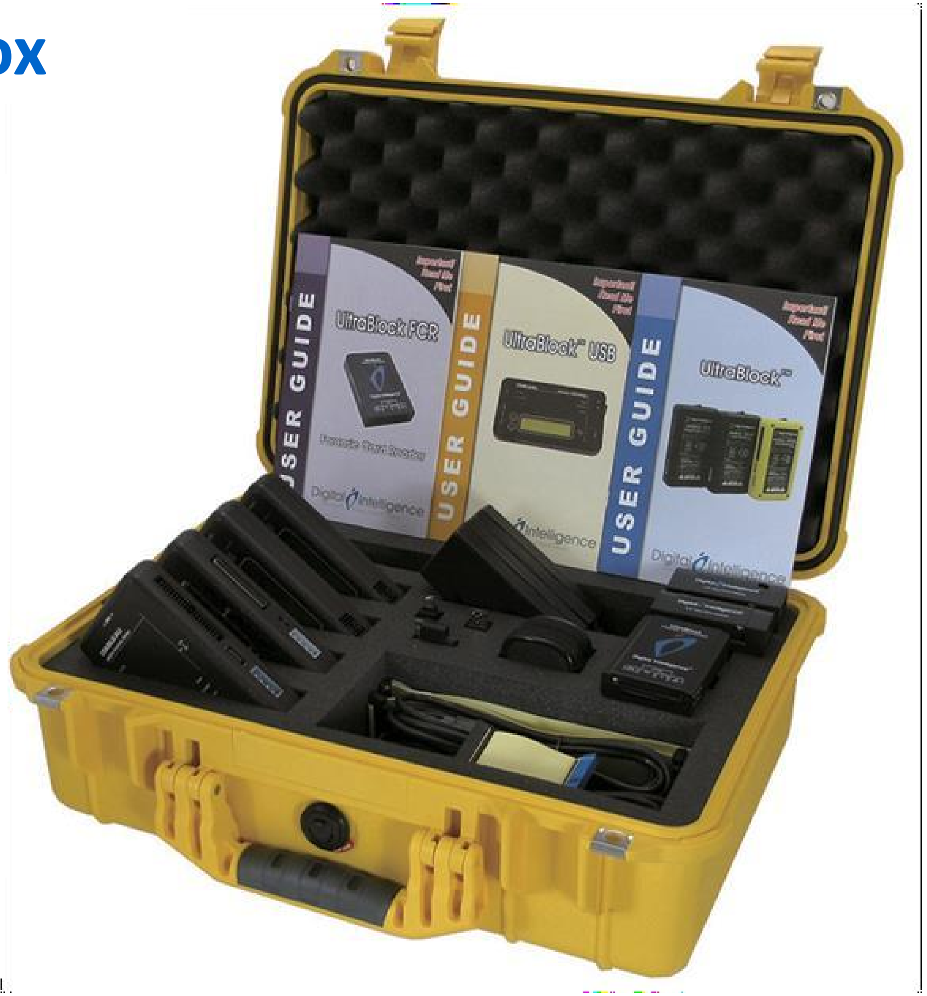
- Supports mining common features such as common contacts, software, USB storage device (USB serial number), etc. in multiple cases and hard disks.

□ Collaborative Forensics

- Supports multi-person collaborative forensics, that is, multiple people in different laboratories and different regions, and simultaneously conduct forensic analysis of a case data, and the analysis results are shared in real time.
- Supports remote assistance for forensics, that is, the expert remotely accesses the local forensic 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 forensic device.

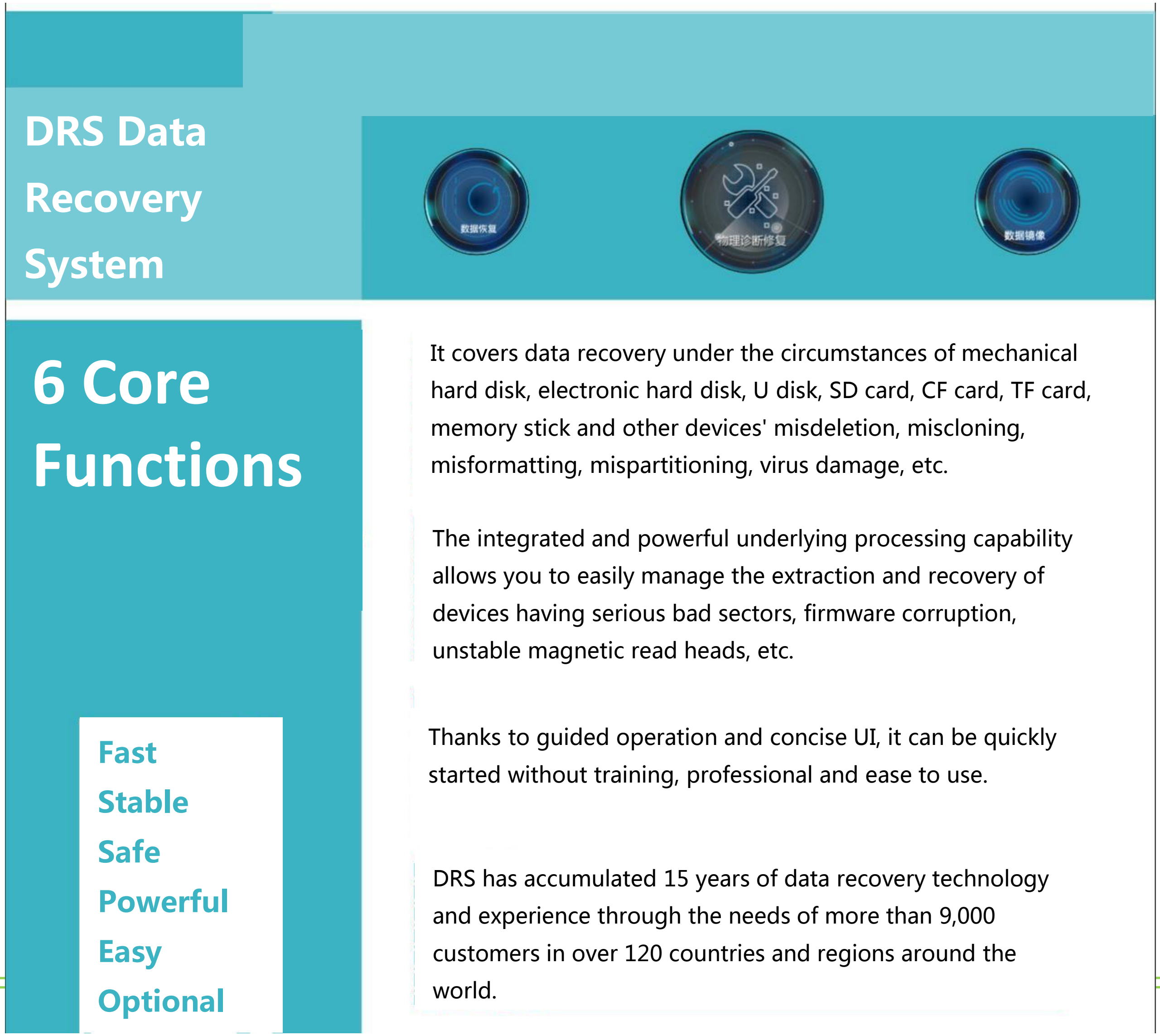
UltraKit Write-Protect Interface Box

UltraKit Write-Protect Interface Box is a portable survey box that integrates various media write protection functions such as IDE, SATA, SAS, USB, 1394 and memory card. The suspect storage medium is connected to the computer to ensure that the suspect data is not falsified and the judicial validity is ensured.



Product Series

Electronic Evidence



数据恢复
物理诊断修复
数据镜像

DRS Data Recovery System

6 Core Functions

Fast
Stable
Safe
Powerful
Easy
Optional

It covers data recovery under the circumstances of mechanical hard disk, electronic hard disk, U disk, SD card, CF card, TF card, memory stick and other devices' misdeletion, miscloning, misformatting, mispartitioning, virus damage, etc.

The integrated and powerful underlying processing capability allows you to easily manage the extraction and recovery of devices having serious bad sectors, firmware corruption, unstable magnetic read heads, etc.

Thanks to guided operation and concise UI, it can be quickly started without training, professional and ease to use.

DRS has accumulated 15 years of data recovery technology and experience through the needs of more than 9,000 customers in over 120 countries and regions around the world.

Laboratory Area Settings

Electronic Evidence

1. Business Acceptance/Pre-inspection Area

Used for the acceptance of the case inspection, and accepts the client, including the acceptance, registration, unique number and photo taking of the inspection materials.

2. Storage Media Recovery Area

Used to repair and extract data from damaged storage media through dedicated technical means.

3. Data Acquisition Area

Used to perform a bit-aligned backup of the sample or obtain it as an evidence file.

4. Comprehensive Inspection Area

Used for comprehensive inspection of electronic data in electronic devices (storage media) such as computers and surveillance video recorders, including data analysis, search, recovery, etc.

5. Mobile Terminal Inspection Area

Used to inspect mobile terminals such as mobile phones.

Laboratory Area Settings

6. Data Decryption Area

Used for decryption and inspection of electronic devices, data files, etc.

7. Physical Evidence Storage Area

Used for storing case-related electronic equipment, storage media and data backup generated in the inspection process.

8. Central Computer Room Area

Used to store servers, network devices, storage devices, etc.

9. Clean Room

Used for opening inspection of hard disk.

10. Shielding Room

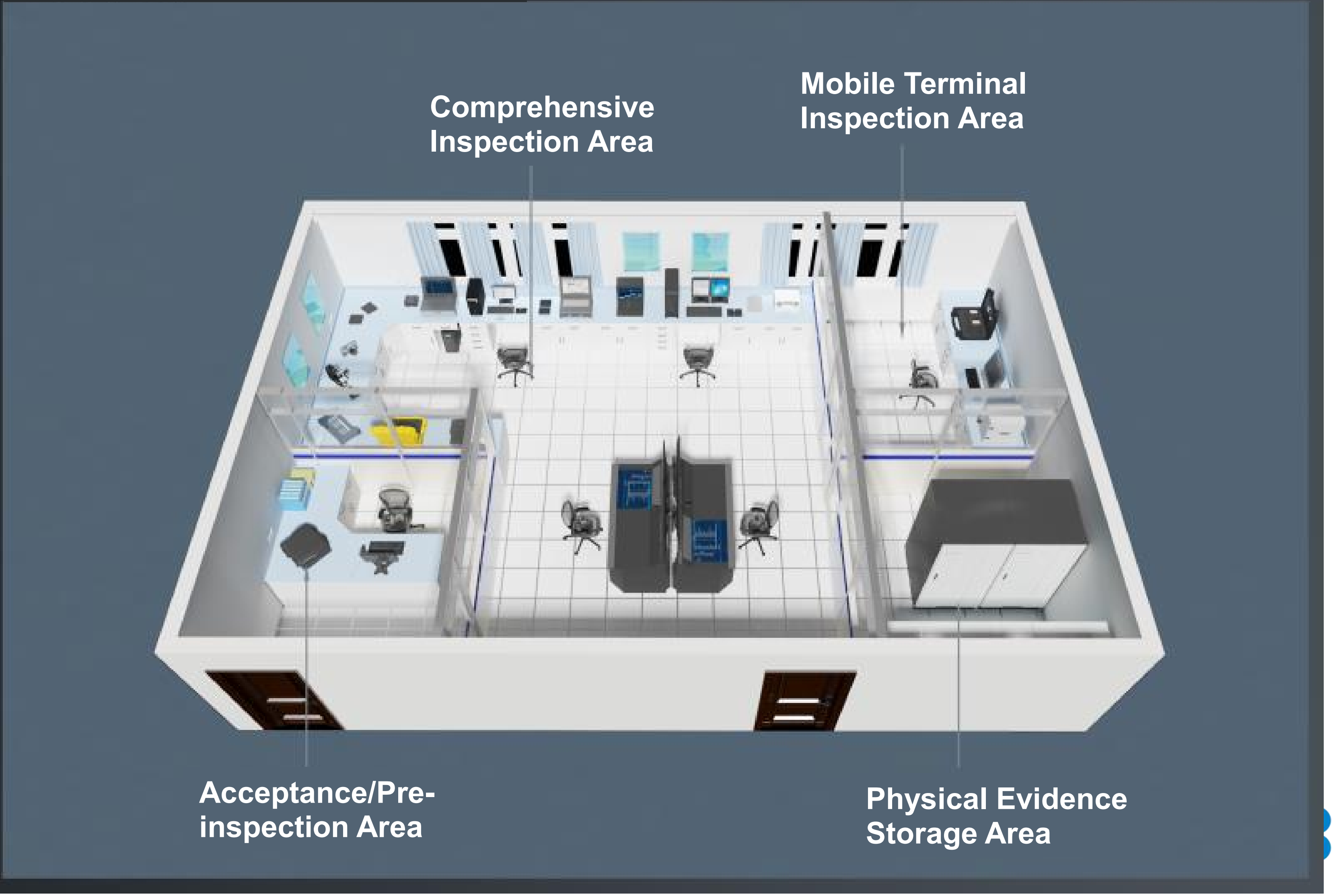
Used for inspection of samples that require shielding of wireless signals.

Laboratory Area

Electronic Evidence

Area Setting		Tier of Laboratory		
		Tier 1	Tier 2	Tier 3
Area Name	Business Acceptance/Pre-inspection Area	≥20	≥15	≥10
	Storage Media Recovery Area	≥10	Optional	Optional
	Data Acquisition Area	≥30	≥15	Optional
	Comprehensive Inspection Area	≥100	≥70	≥40
	Mobile Terminal Inspection Area	≥30	≥20	≥10
	Data Decryption Area	≥20	Optional	Optional
	Physical Evidence Storage Area	≥50	≥20	≥10
	Central Computer Room Area	≥40	≥30	Optional
	Clean Room	Optional	Optional	Optional
	Shielding Room	Optional	Optional	Optional
Total Area		≥300	≥170	≥70

Indoor Aerial View

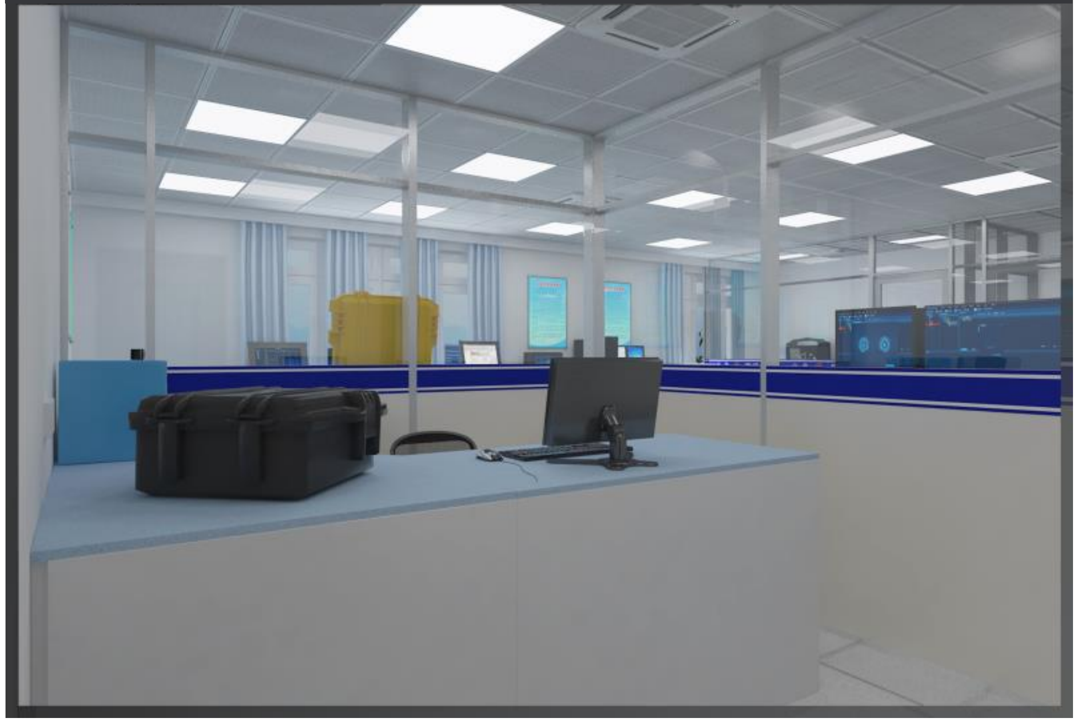


Comprehensive Inspection Area
Mobile Terminal Inspection Area
Acceptance/Pre-inspection Area
Physical Evidence Storage Area

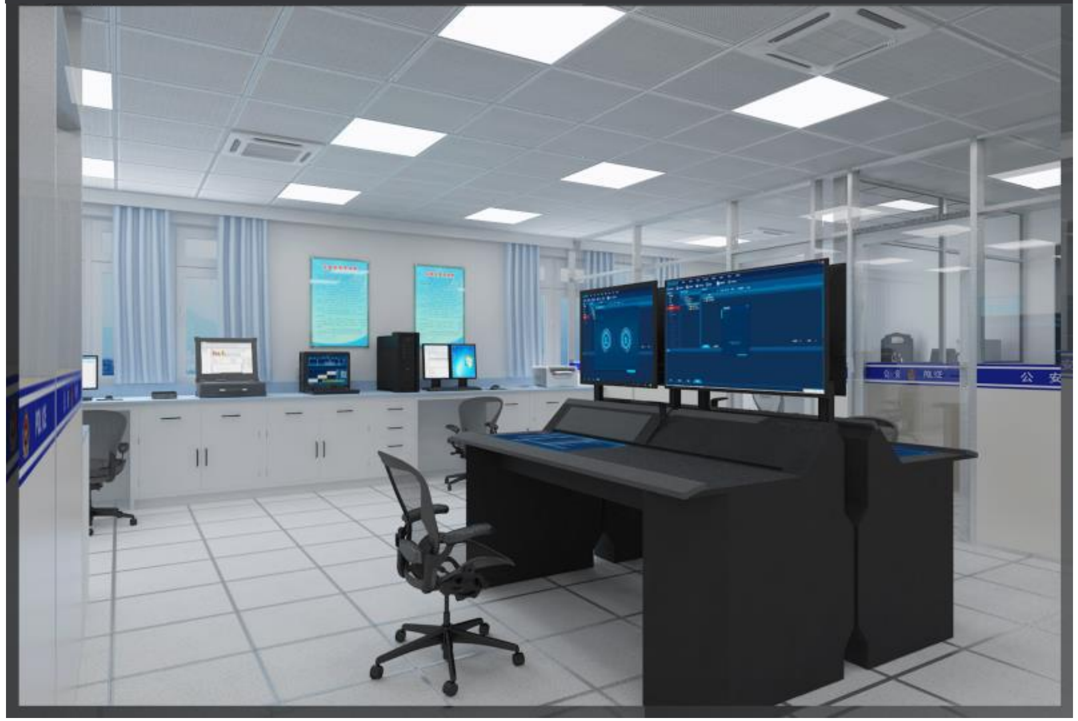
Laboratory Area Settings

Electronic Evidence

Acceptance/Pre-inspection Area



Comprehensive Inspection Area



Laboratory Area Settings

Electronic Evidence

Mobile Terminal Inspection Area

Physical Evidence Storage Area

POLICE
公 安
POLICE
公 安
POLICE
01
02
03
04

Sphere of Business

1. Extraction and Fixation of Electronic Evidence

Discovery, identification, extraction and fixation of electronic evidence and related items.

2. On-site Preservation

On-site preservation or back-up of extracted electronic evidence.

3. Volatile Data Extraction

Extract and fix data transmitted in the network or the data running in electronic devices such as computers that disappear with the power cut-off or shutdown.

4. Data Recovery

A recovery of unaccessible operating system or unrecognizable file data in sample material.

5. Data Search

A search in the material based on relevant keywords or known content.

Sphere of Business

Electronic Evidence

6. Document Consistency Check

A check that compares whether the data contents of two files are identical.

7. Software Function Inspection

A test to determine whether the software has a certain function(s).

8. Software Consistency Check

A check that compares two pieces of software to see whether their functions are identical (or similar).

9. Time Attribute Inspection

Inspection of file time attributes, system time attributes, power-on/off time attributes, etc.

10. Internet Record Inspection

Inspection of various records formed on the Internet.

Sphere of Business

Electronic Evidence

11. E-mail Inspection

Inspection of E-mail content or its attributes.

12. Instant Messaging Inspection

Inspection of instant messaging content or its attributes.

13. Log Inspection

Inspection of log contents of computer operating system, database, application system, etc.

14. Database Inspection

Inspection of database content or attributes.

15. Password Cracking

Decryption of the operating system, files, storage media, etc. with password protection.

Sphere of Business

Electronic Evidence

16. Mobile Phone Inspection

Inspection of mobile phone body and the data in mobile phone user identification card and extended memory card.

17. Video Surveillance Equipment Inspection

Inspection of data extraction and analysis in video surveillance equipment.

18. Pseudo Base Station Inspection

Perform functional inspection and data transmission inspection on the pseudo base station equipment.

19. Damaged Storage Medium Inspection

Extract data stored in damaged hard disk, CD, flash disk, memory card and other storage media.

20. Medium Data Erasure

Write specific data bit by bit to storage media such as hard disks.

21. Mobile Phone Information Associative Analysis

The associative analysis is performed on information such as address book, short messages, call records and instant messaging chat records in the cell phone.

22. Network Information Associative Analysis

The associative analysis is performed by using the information detected from the sample material and the information in the shared resource network.

Case

Guangdong destroyed a number of illegal online pyramid sales groups, the amount involved was as high as 2 billion yuan.

Case

Electronic Evidence

Guangxi cracked an exceptionally large pyramid sales case and seized bundles of cash on the spot.

Case

Electronic Evidence

Chaoshan police cracked the "mobile phone dating APP fraud case", the amount involved was as high as more than 43 million yuan.

Superbio 苏博医学

诚信/务实/创新/高效

Thank You！

Jiangsu Superbio Biomedical Co., Ltd.