E-Forensics Application Research in the Agricultural Industry Regulator

Chen Zhenkai[1,2]， Piao Zailin[1]
1.Information and Electrical Engineering ,Shenyang University of Agricultural ：
shenyang 110161,china；
2.Liaoning administration of industry＆commerce：
shenyang 110161,china
line 3: City, Country
e-mail: 13840539312@139.com

***Abstract*—The electronic evidence is becoming increasingly popular in cracking down on Internet pornography, online gambling, phishing and other high-tech crime cases .It also takes an important part in the agricultural industry, regulatory processes and electronic forensics. Of course, electronic forensics has also encountered some legal obstacles. The obtained materials are often used for handling the case the clues rather than evidence. So how to take electronic evidence extraction technology into the food industry and improve agricultural security is particularly important. The text presented data on the target computer to restore the use of remote technology, scan the data record and in accordance with MD5 encoding effectively and quickly , record real-time, and then extract a set of electronic evidence forensics model. Form an effective, fast, flexible electronic evidence extraction method.**

Keywords-Agricultural Industry; Electronic evidence; security; Application; evidence

I. INTRODUCTION *(HEADING 1)*

With the rapid development and wide application of the technology of electronic data, the electronic forensic technology[1]has become an increasingly important means of technology in investigating case, litigation and trial justice activities. Computer crime makes the public suffer significant losses. And different from the traditional criminal evidence, electronic data evidence are more likely to disappear and be destroyed. So the focus of the fight against computer crime is to find fully reliable electronic evidence.

In a narrow, electronic forensics is "to seem the computer system as a crime scene, using advanced technology tools, following the procedures to check the computer system, to protect and analyze evidence related to computer crime,in order to initiate proceedings"[2].

Broadly speaking, Electronic evidence include but not limited to special technical means .It is on to be able to accept the court, sufficiently reliable and persuasive. It exists in identifying, protecting, extracting and archiving process of electronic evidence in computers and related peripherals[3].

Today's emerging food security crisis threatens people's health. The regulation of the industry is not only within the industry self-examination. When necessary, investigation and evidence collection should be carried out by the public security organs. And the focus of the forensic work is also the focus of supervision.

We should focus on the relevant policies and regulations. At the same time, we need to look at manifestations and more depend on the substantive issues .We can't always stay in showing cards and seeing overalls, hats. We should make it a key to pay attention to raw materials, equipment, process, and finished goods of the food[4]. Today, the agricultural products industry has been introduced the Internet of Things relations mechanism. Form a regulatory mechanism to each control from the upstream source of agricultural products, transportation, semi-finished and finished products to storage, sales process. It is matched with full computer expert system of electronic data of agricultural products. The advantage is the ability to make the system have identify, predict the new feature of the normal type or abnormal type of data. And it can also forecast some unknown data whether it is evidence of a crime in order to improve the intelligence of the data analysis.However, some wrong operation or deleting data caused the forensics difficulties.

Therefore, how to provide effective security techniques and methods for the investigation of cybercrime timely and accurate, to ensure that the network of electronic evidence objective, related and legitimate, to combat and curb cybercrime is what the network electronic evidence forensics technology needed to study.

This paper uses the remote computer data recovery technology, then provides credible, accurate and complete evidence of electronic data which is comply with laws and regulations .So we can achieve the purpose of the electronic data evidence forensics.

II. REMOTE TECHNICAL MODEL

A. Technology of Remote Data Recovery

Remote Data Recovery fundamentally depends on whether the communication mechanism is perfect.It is the basis of remote computer control data transmission. It determines the reliability and accuracy of the data transmission between the various parts of the entire

evidence collection process and the transfer speed. It also determines the control end of the processing power of the server as well as the system real-time manipulation capabilities. In order to covert and safety considerations, forensics system data transfer should transit through the transit side, to control client and server communicate directly.

By using remote thread calls the API function, it makes the main program dynamic link library DLL inserted into the address space of the target process. Use DLL file thread in the target process calls Load-Library functions to load the main program, in order to achieve the forensics subsystem implants. The main steps are: 1: Create a remote thread, to call Create Remote Thread API. 2: load the main program DLLs call Load Library function. 3: implantable main program DLL process analysis, 4: Save backdoors. Figure 1

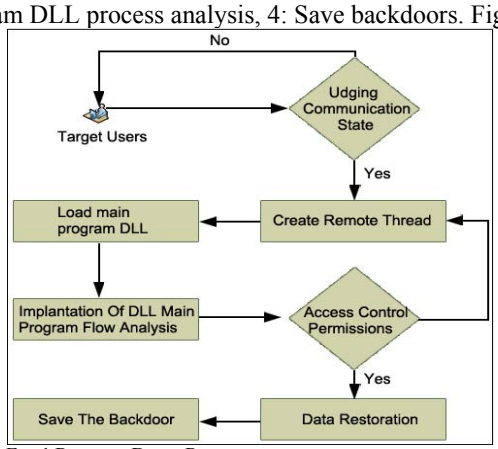

FIG.1 REMOTE DATA RECOVERY COMMUNICATION MODEL

B. *FAT32 data recovery*

When the system completely remove a file (When a file is deleted in the Recycle Bin), the computer system will make the corresponding delete files FAT entry value set to 0. It said this data clusters can resave other documents, and the root directory of the table is replaced with the ESH. In this way, the computer systems thoroughly complete the deletion of this file. In the computer system, directory and data on the system for this file is already unreadable. But we can restore the root directory table and file allocation table, to make the deleted file recovery back.

C. *NTFS format data recovery*

The file system which is NTFS type deletion Similar principles and FAT32 file system. It also has a file status flags in the file record table. When disk system file is deleted, the documentation of the head will rewrite the flag byte into 00/02H.And other attributes documented no change. While the corresponding cluster and delete files in the metafile bitmap metadata to do emptied flag, it shows this data cluster can be assigned to other documents.

From the above analysis ,we can see, when data recovery, we can completely remove data restore back as long as we rebuild the master file table the MFT system

III. ELECTRONIC EVIDENCE EXTRACTED

A. *file scanning record the importance of forensics*

For computer forensics, before carrying out data analysis and information mining, determine the file system and records in a timely manner in order to ensure the integrity of the file for help investigators breakthrough suspects Confession. It is a guarantee to provide strong evidence.

After data recovery of the system, through Quick Search scans within the system files, we can use sequential, segmented or distributed scanning, to record real-time status and integrity of the file.

From different operating systems, the key file is also unknown, we can use cryptography method to test the integrity of the file to extract key file[5-7].

B. *Data logging based on MD5 algorithm*

Senior program officer has the use of special technical means to fool the CRC process; so generally, we must adopt a more comprehensive and secure method to detect. Cyclic redundancy check (CRC check) use 32 to protect files Integrity. Therefore, we introduce the MD5 algorithm, which is unidirectional, difficult for an intruder to thrusting through the algorithm, and is extremely difficult to find random information to produce the same digest. Thereby generating a summary having degree of safety only, it is suitable for the safe and quick summary of produce. The full name of the MD5 is Message-Digest Algorithm 5; it is invented by MIT's Laboratory for Computer Science and RSA Data Security Inc. in the 9O's early 20th century and evolved through MD2, MD3 and MD4. Message-Digest refers to The Hash codes Transform of the information flow (Message). MD5 replace any length rheological with a 128bit large integer. Its transform is an irreversible information transformation algorithm. It makes arbitrary length of the information flow change into a certain length of large integer. IN other words, even if you see the algorithm described or source, you cannot make an MD5 value of anti-converter back to the original string stream. From mathematical principles, because there are infinitely many original character codes, it simply does not exist the inverse function of mathematical functions.

The hash value calculation of MD5 algorithm has become a most popular hashing algorithm, because of its high security strength and quickness. The MD5 algorithm as the input value to an arbitrary length of the information, the processing operation comprises several parts.

(1) Add the stuffing bits. It input the information for the length of the value of the padding information (number of bits) 448 mold 512 Congruence (length = 448mod512),

filled the highest bit is 1, the remaining bits to zero.
(2) Set Verify Code value length. If the initial length is greater than 64, use only the length of the lower 64 bits. Use the 64-bit representation of the initial information bit length (before filling) added after the result of step 1 (low byte first). After the treatment, the length of the value contained in the initial information in the domain is the mold 64
(3) Build MD5 environment cache. Use a 128bit cache to store intermediate and final results of the hash algorithm. The cache is represented as four registers (32bit A, B, C, D). The register is initialized to the following 32bit long integer data.
(4) Packet process sequence information. The core idea of the algorithm is able to "cycle" contains four compression functions. The 4 loop functions have a similar structure. In the description are represented by F, G, H and I, and each cycle use a different primitive logic functions. Each cycle use the current I in the 128bit cache processing and 512bit packet (Yq) ABCD as an input, and last update cached content. Building through the sine function, each cycle should use a 64-element table T [O.64] a quarter.
Value check code:

```
public static string GetMD5HashFromFile(string fileName)
        {FileStream file = new FileStream(fileName,
                        FileMode.Open);
        System.Security.Cryptography.MD5 md5 =new
System.Security.Cryptography.MD5CryptoServiceProvider(
                                        );
    byte[] retVal = md5.ComputeHash(file); file.Close();
        StringBuilder sb = new StringBuilder();
          for (int i = 0; i < retVal.Length; i++)
         {sb.Append(retVal[i].ToString("x2"));}
       return sb.ToString();                    }
```

C. extraction and analysis of electronic evidence

(1)electronic evidence extraction technology

Extracting electronic evidence in general is gathered original evidence data through investigation and site inspection. According to the needs of the current technology, we can perform Remote Abstraction. Electronic evidence discovery technology actually belongs to the investigative techniques[8-11]. It can combine general investigative techniques and computer remote technical to study. General investigative techniques and computer remote technology combined study. Research in this area include Network clue automatic traceability technology, data filtering, forensic dedicated IDS (Intrusion Detection System, Intrusion Detection System), disk mirroring technology, mining technology and so on. According to different sources of electronic evidence, electronic evidence discovery network discovery of evidence can be divided into stand-alone evidence discovery and related equipment evidence found. Figure 2 extraction models for remote electronic evidence:

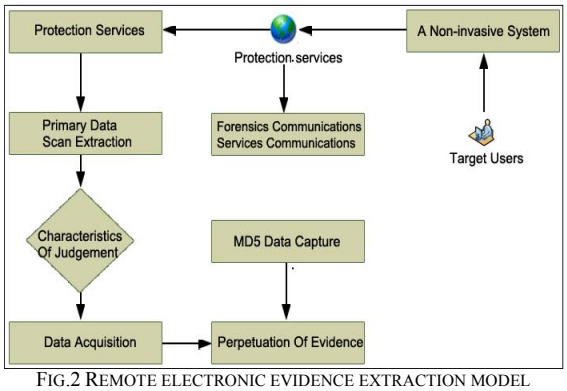

FIG.2 REMOTE ELECTRONIC EVIDENCE EXTRACTION MODEL

(2) Registry parsing

The registry is an important component of Windows. It is the core of the underlying database. Operating system parameters stored in the library control start Windows, the loading of the hardware drivers and Windows applications to run. System and user trace information is stored in the registry. This provides investigating officers a favorable way to obtain evidence. The function of the module is: Search the operating system's registry file, parse Its root key structural division and interrelation, access to the system configuration information, installed applications and user information ,and so on. Key_local_machine \ software and application software records related set of system configuration information and user installed applications corresponding to it, such as application installation, startup settings, and verify information. Hkey_local_machine \ software \ microsoft \ windows \ currentVersion \ expolrer \ user is to save the personal file folder, favorites path. API function:
std :: vector <vkey-offset> mesVahieoffeetArray :/ / key offset list
std :: veetor <R_Valuenata> m_RegvalueDataArray :/ / key-value list of data extraction and analysis of the data of the registry records.

(3) System History Log resolution

Network communication tools are endless ,and chat software in common are : Tencent QQ, MSN, mobile flying letters, etc.. At the same time, Foxmall, Microsoft Outlook and other mail processing software provides a convenient to the number of suspected cases of economic class suspects. Parse the software which contains chat logs, the communication object information, e-mail account information, we can find they are very similar. Therefore, the application of the system developed a common data structure interface. Meet these communications software to parse and generate analysis report presented to the investigating officers. The most commonly used QQ, for example.

QQ chat records are generally stored in installation

directory MsgEx.db file, each the landing QQ number will generate a file that is used to save the record. MsgEx.db file structure: Though Index.msj index, ffter encryption processing chats, CZCMsg store their communication QQ number, and chats are stored in Data.msj file, only the decryption can see. TempsessionMsg store temporary session information. SysMsg storage system session information. Matrix.db the contents of the file used to store the generated global key to decrypt the message.

(4) Disk data mining

The disk information mining Module is a very important module of the system. It is because the criminals are very cunning. They will timely cleanup system temporary files, Internet records and other important information. And once found their own criminal behavior has been found by the prosecution, they will quickly remove evidence of a crime which is stored on the hard disk, U disk. This will interfere with the investigation and evidence collection work of the investigators. This requires the module to delete the disk file recovery work. At the same time, once the other parsing module face system files are deleted, they also need the module to restore. Now, under the Windows operating system, the file system is FAT32 format and NTFS format.

(5) Text document parsing

When Word software is open abnormally, we can read binary Ultraledit and other software to open the file in binary form of debris. Use the word timestamp of the format and storage characteristics, to analysis binary code. First of all, we need to find a summary of information flow (Summary Infor-mation Stream) of the directory entry and then, through the analysis of the summary information flow directory entry directory to find a summary of the flow of information, as shown in table 1. Finally, through the flow of information directory entrance, analyze the summary of information.

TABLE.1 INFORMATION DATA STREAM OF WORD DOCUMENT

00004780h	0	0	5	0	7	0	6	0	6	0	6	0	7	0	7	0
	5	0	3	0	5	0	d	0	D	0	1	0	2	0	9	0
00004790h	4	0	6	0	6	0	6	0	7	0	6	0	6	6	7	0
	9	0	E	0	6	0	F	0	2	0	d	0	1	0	4	0
000047a0h	6	0	6	0	6	0	0	0	0	0	0	0	0	0	0	0
	9	0	F	0	E	0	0	0	0	0	0	0	0	0	0	0
000047b0h	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
000047c0h	2	0	0	0	0	0	0	0	0	0	0	0	F	F	F	F
	8	0	2	1	2	0	0	0	4	0	0	0	F	F	F	F
000047d0h	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
000047e0h	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
000047f0h	0	0	0	0	1	0	0	0	0	1	0	0	0	0	0	0
	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0

IV. THE ELECTRONIC FORENSIC TECHNOLOGY APPLICATION IN THE AGRICULTURAL INDUSTRY REGULATOR

Technology widespread application in electronic forensics can achieve automatic extraction of agricultural cultivation, storage, transportation, processing, sales and other information. As long as the computer or network has comprehensive information including: basic information of agricultural products, additives, pesticide use, sampling information, information of the cultivation and processing of agricultural products, agricultural products safety testing information, etc. They are available through the electronic evidence. Even once did delete operation, they can also extract recovery through electronic forensics technology.

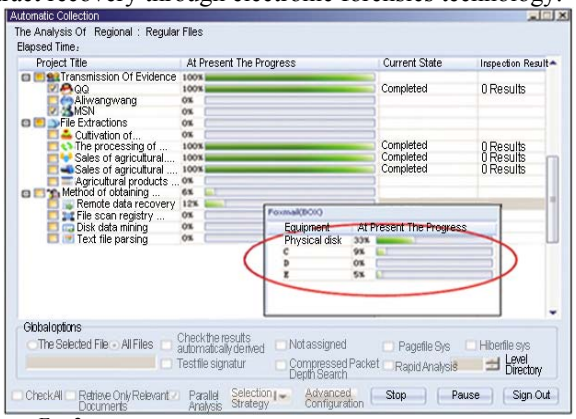

FIG.3. REGULATION OF AGRICULTURAL PRODUCTS, ELECTRONIC FORENSICS APPLICATIONS

Plugging electronic evidence equipment into the computer forensics, Evidence equipment will automatically restore all traces by forensics techniques mentioned in the papers. Then through forensic software will extract information involving agricultural products. And thus make electronic forensics software to play the biggest role in the regulation of agricultural products. Effectively combat the problem of food safety.

V. SUMMARY

In this paper, a network for electronic forensics remote data recovery and extraction terminal mining storage devices. The application results show that fast, high-speed hard disk forensics has a good prospect in terms of network information security and criminal investigations. I believe that with the development of technology, more and more computer forensics technology will be forensic work to make outstanding contributions.

REFERENCES

[1] Liu products new the electronic forensics legal regulation, 2012 (2).

[2] Specifically, the information the collection type Trojan electronic data forensic methods to explore [J]. Criminal Technology, 2011, (04).

[3] Liu Jianjun, Huang Cheng-baccarat gambling machines, electronic evidence exploration [J]. Information Network Security, 2010, (11).

[4] Specifically, malicious programs based on reverse technology analysis method [J] Journal of Computer Applications, 2011, (11).

[5] Zheng Guangming, Hu Bo: "file integrity detection software design based on MD5" "Hunan Institute of Technology 2007-3 20 -1 Vol.20 Mar.2007.

[6] Wang Baoyong, Bin Song "electronic evidence" of Computer Network Crime Investigation, digital technology and application "(2010) 07-0085-01.

[7] Yu-oriented the active storage services processing reconfigurable computing technology research [D]. Huazhong University of Science and Technology, 2010.