Web-based real-time forensics system

Shi Yong Xiong¹, a, Hao Tang b

¹ Chongqing University of Posts and Telecommunications, Chongqing 400065, China;
² Chongqing University of Posts and Telecommunications, Chongqing 400065, China.

a xiongsy@cqupt.edu.cn, b149664012@qq.com

Keywords: Evidence Collection in Network, Electronic Evidence, Web Dynamic Forensics Model

Abstract. With the development of the Internet, the network crimes emerge in an endless stream. In addition, the features of the content on the Internet are complex and changing, which create many serious difficulties for judiciary to gather evidence of network crimes. Based on analysis of the characteristics of electronic evidence and the key issues in evidence collection process, this thesis proposes dynamic forensics system based on Web in order to achieve goal of gathering evidence in legitimate, convenient and efficient way.

Introduction

With the prevalent of the Internet in China, violations on the Internet are becoming increasingly fierce. The network leaks, defamation, rumors, spam, information interference are more and more rampant. Moreover, hacking, phishing and other kinds of criminal acts happen in a high frequency. It is "volatility ", " change easily without trace " and " uneasy to present and archive " that are three distinguished characteristics of Internet data [1]. Because of these, the administrative authorities have difficulty in gathering evidence after finding illegal activities. Offenders delay confirmation of responsibility through the abuse of the rights, finding defects of evidence and some other ways.

Currently, obtaining evidence from Internet data is inseparable to solve civil disputes that happen on the Internet, criminal and administrative violations. For instance, judicial or notary office could make preservation of evidence for infringing content of network pages; network supervision departments could fix the network crime data; The administrative department for Industry and Commerce could fixe false online advertising, etc. Gathering evidence under both of these occasions is relatively difficult. Therefore, how to get the Internet data, which meet the legal requirements is the current problems. According to Chinese national legal requirements, administrative organ should bear the burden of proof for alleged Internet Illegal Behavior when they play the role in law enforcement. So, it is necessary to obtain legal evidence so that deal with illegal websites according to the law[2].

Computer Forensics Overview

The Concept of Computer Forensics . Different researchers have different definitions on the concept of knowledge space mode. In the year of 1985, Doignon and Falmagne suggested the knowledge space theory is based on understanding science which describes a given domain knowledge of the structure of the method[3]. In 1999, Zhijin Wang et al., put forward the word: knowledge space in article” knowledge space: the concept of knowledge organization foundation” which probes the multi-dimensional model of knowledge structure[4]. On the basis of the concept of knowledge space.

Principles of Computer Forensics. Compared with the traditional forms of evidence, the characteristics of electronic data determine that forensics procedure should not only follow the general principles of legality, timeliness and comprehensiveness, etc., but also obey certain principles. In order to ensure the effectiveness of the acquired evidence, the following principles should be followed in the process of gathering evidence [5][6][7]: (1) The principle of gathering evidence according to the law : This principle requires that the process of obtaining electronic
evidence must be carried out in accordance with the law of each country. The evidence obtained in an illegal way cannot be used, and the evidence lost the probative force. (2) the principle of timeliness: Because electronic evidence is easy to be removed, destroyed, modified, etc., obtaining of electronic evidence has the certain timeliness. Evidence should be obtained before it changed by offenders. The best case is that crime evidence is found, at the same time, the evidence is obtained. (3) the principle of comprehensiveness: The process of obtaining electronic evidence must be comprehensive, multi-angle, multi-level, any electronic data associated with the facts of the case cannot be omitted in order to achieve mutual corroboration exclude the contradictions and form complete chain of evidence. (4) the principle of obtaining professional evidence[8]: The steps of obtaining electronic evidence should depend on the type of electronic evidence and follow a series of professional operations that are corresponding with the specific evidence that has been extracted and fixed in order to ensure the probative force of the electronic evidence[9]. (5) the principle of non-destructive forensic: In process of obtaining and fixing evidence, the evidence should be ensured intact[10]. First of all, we must ensure the purification of evidence in its own environment. Secondly, preventing acquired evidence from being tampered is also important to keep evidence in a non-destructive state.

Forensics Model Design

According to the characteristics and principles of electronic evidence, we design a web-based real-time forensics system that can automatically obtain the evidence, analyze evidence, and securely store evidence. At the same time, the forensics client can real-time track the router nodes of crime server and the underlying data. See Figure 1.

Forensics terminal. As the operator of the system, forensics terminal is mainly used to access forensics URL, purify the local environment, activate the forensics system logic, and graphically display geographical distribution of routing[11].

Users logical server cluster. Using way of load balancing to deal with each logical requests which are issued by different forensic terminal, and issuing instructions to the forensic server depending on the various type of requests, as the same time, responding to the business process in the process of forensics by managing component.

Evidence Management Component. User management, evidence management, security management are included. Wherein the security management is to ensure system security in the process of forensics[12]. And obtained evidence can be kept integrity by the digital signature and timestamps. See Figure 2.
Evidence preservation center. To ensure the legal effect and irreversibility of evidence, the way is that using evidence fingerprint generator to encrypt evidence and transfer to a third party preservation center (Centre of Forensic Sciences which has the national qualification).

Forensics server. Forensics server plays a very important role in the entire system. Its mainly responsibilities are sending data requests to the forensic website, collecting network information, generating fingerprint evidence, evidence storage cured.

Evidence Storage Array. Storing the obtained evidence in the evidence storage array once finishing the tamper-resistant operation, this measure can effectively prevent the loss of evidence whose reasons are natural disasters or hardware failure.

The main technical implementation

Evidence acquisition. As shown in the figure 3, after forensics terminal emptied the local cache, it issues forensics instructions through Http proxy settings and using forensics protocol to request user logical server cluster. Then, forensic server sends http request to target web site after receiving forensics command; the target web site sends back the response data; finally, after parsing the content and generating evidence tree, creating the URL.request file and URL.response file. Evidence acquisition process as shown in Figure 4.

Transmission processing. Data acquisition module of forensics agent i(FAi) sends the original collected evidence e-vidata the data transmission module which will processes the e-vidata and sends
it. SK¹ and PK¹ represent private and public keys of FAi respectively; SK² and PK² represent the private and public key of data receiver module respectively. So, interactive processes between the data receiver module and FAi is listed as follows:

**The Sender**

**Step 1.** Using a one-way hash function H to calculate the digital summary of evidata h, h = H (evidata);

**Step 2.** Signing the signature for h, s = DSK¹ (h);

**Step 3.** Encrypting the entire message (including evidata and s) to obtain the ciphertext c equates to c = EPK² (FAi, evi-data, s);

**Step 4.** Send the ciphertext c.

**The Receiver**

**Step 1.** Decrypting the received ciphertext c to obtain the plaintext p, p = DSK² (c) = DSK² (EPK² (FAi, evi-data, s)) = (FAi, evi-data, s);

**Step 2.** Looking up the certificate and public key of Fai in the certificates list of CA to decrypt s and obtain h, namely EPK¹ (s) = EPK¹ (DSK¹ (h)) = h;

**Step 3.** Using the same hash function H with Fai to calculate Digital Abstract h' of evidata, h' = H (evi-data). If h' = h, it means that evidata is not been tampered with during transmission and it also prove that recpeted data is indeed sent by FAi.

**Evidence access.** Data receiving module stores the original decrypted evidence that has been validated together with its own digital signature in the database. In order to prevent the original evidence data from being removed or tampered during the storage process[13], it is necessary to establish connection between two records (j-1, j) through digital signature in process of saving data; accordingly, when preprocessing module reads records j from the original evidence database, it is necessary to record the signature field of j-1 for inspection certificate. If the data that you want to save is evi-data, and using SK², PK² to represent private and public key of receiving module respectively, store and read operation of the interaction process is as follows:

**Step 1.** The content (last.s) of digital signature field of last record (last) in database; '

**Step 2.** To obtain the digest value (h-last) of last.s, namely EPK² (last.s) = EPK² (DSK² (h- last)) = h-last;

**Step 3.** Using one-way hash function H to calculate digital digest h of evidata and h-last, namely h = H (evi-data, h-last);

**Step 4.** Signing the signature for h. s = D (h).

**Step 5.** Appending evidata with its digital signature s to the database.

**Read.** Preprocessing module reads record rj whose record number is j in the original evidence database, and this operation needs to do the following verification:

**Step 1.** Reading digital signature field (rj.s) of rj, and calculating its digital digest hj, namely EPK2 (rj.s.) = EPK² (DSK² (hj)) = hj;

**Step 2.** Reading the digital signature field rj-1.s of record rj-1 whose record number j-1, and calculating its digital digest hj-1, namely EPK² (rj-1.s) = EPK² (DSK² (hj-1 )) = hj-1;

**Step 3.** Using one-way hash function H which is also used in storing data to calculate the evidence data field(rj.data) of record rj and the hash value hj' of hj-1, i.e. hj' = H (rj.data, hj-1);

**Step 4.** If hj' = hj, then the verification passes.

**System's core functions and testing**

**Routing information record acquisition.** The system can obtain the route node information of destination address, DNS server information, and IP address information. Both of the network information can be used to locate the geographic location information of target web site. See Figure 5.

**Original data acquisition.** Through our system, you can fetch the underlying data of the target web site and obtain the entire contents of Web pages. What's more, all kinds of data in target web site could be shown in a tree structure way. See Figure 6.
Evidence Management. The system can manage the completed evidence package. Related forensic evidence can be quickly viewed and downloaded.

Evidence verification. The system can automatically identify the evidence package to determine whether the packet is the valid evidence. The evidence packet that has been modified cannot pass test.

Summary

In this paper, a web-based real-time forensics system is studied. Through the description of capturing, transmitting, and preserving for evidence, we combine the theoretical knowledge of electronic evidence in law field with implementation of computer software systems to effectively give the solution for questions of timeliness, irreversible nature, legality, etc. in process of Internet evidence collection. However, era is constantly evolving and developing, there is still a long way for development of real-time forensics technology and building of related models to go. Therefore, further study in this field should be done in the future.

References


