Web-based real-time forensics system

Shi Yong Xiong[1, 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, [b]149664012@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.

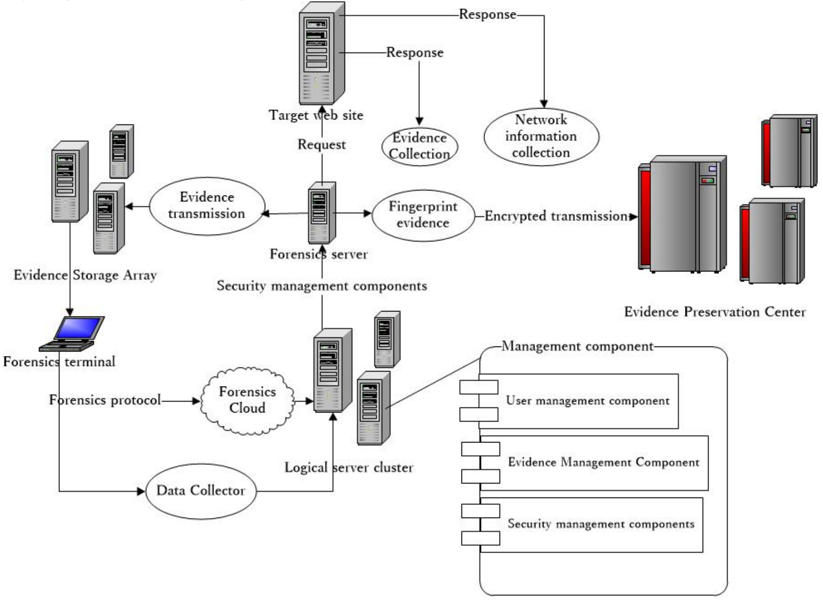


Fig 1. Forensics Model

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， and responding to the business process in the process of forensics by managing component.

Evidence Management Conponent. 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.

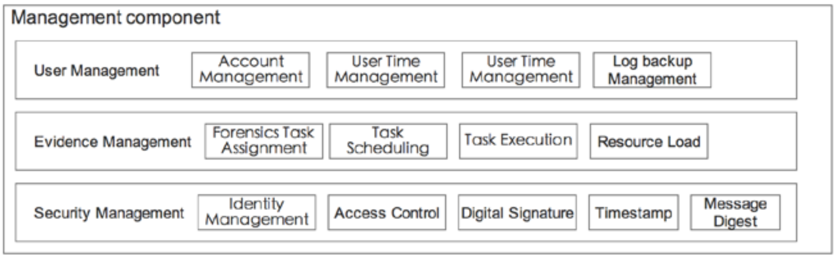


Fig 2. The detail of theEvidence Management Conponent.

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.

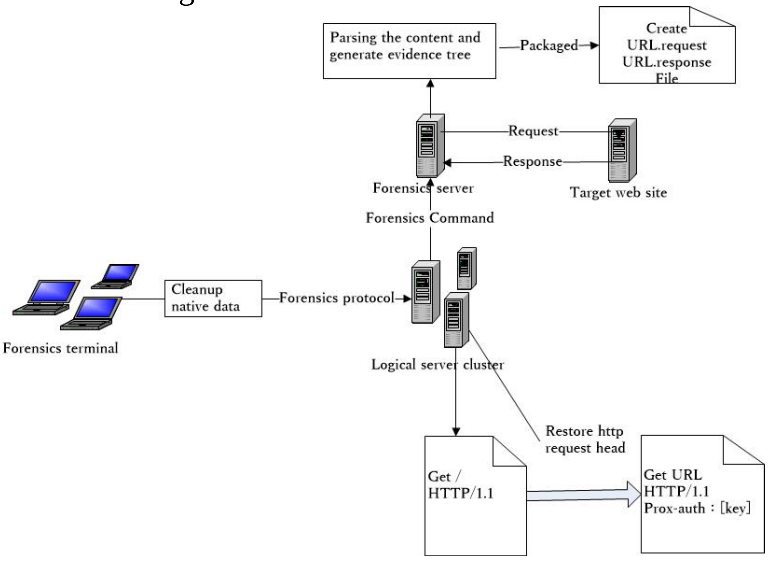
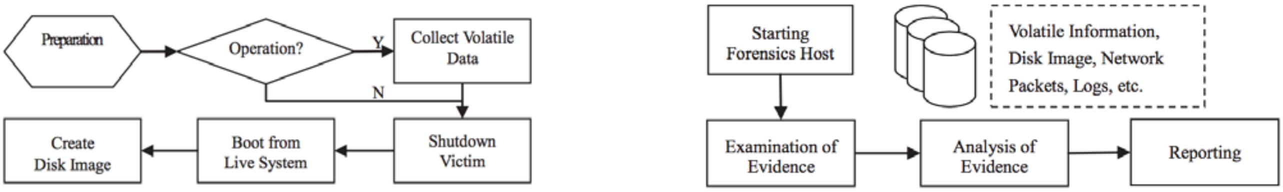


Fig 3. Evidence acquisition



Phase I - Preserve evidence work

Phase II - Analysis of forensics

Fig 4. Evidence acquisition flow chart

Transmission processing. Data acquisition module of forensics agent i(FA^i) sends the original collected evidence e-vidata the data transmission module which will processes the e- vidata and sends it. SK^1 and PK^1 represent private and public keys of FA^i respectively; SK^2 and PK^2 represent the private and public key of data receiver module respectively. So, interactive processes between the data receiver module and FA^i 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 (ev-idata);

Step 2. Signing the signature for h,s = DSK^1 (h);

Step 3. Encrypting the entire message (including evidata and s) to obtain the ciphertext c equates to c = EPK^2 (FA^i, ev-idata, s);

Step 4. Send the ciphertext c.

The Receiver

Step 1. Decrypting the received ciphertext c to obtain the plaintext p, p = DSK^2 (c) = DSK^2 (EPK^2 (FA^i, 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 EPK^1 (s) = EPK^1 (DSK^1 (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 recepted data is indeed sent by FA^i.

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 SK^2, PK^2 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 EPK^2 (last.s) = EPK^2 (DSK^2 (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.) = EPK^2 (DSK^2 (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 EPK^2 (rj-1.s) = EPK^2 (DSK^2 (hj-1)) = hj-1;

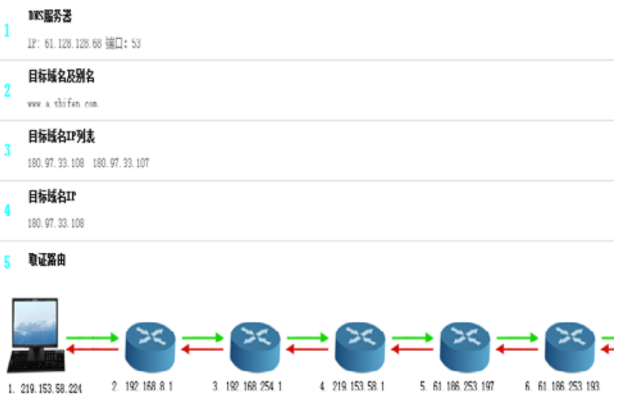
Step 3. Using one-way hash function H which is also used in storing data to calculate the evidence data field(rj.data) of record rj and the hash value hj ' of hj-1, i.e. hj' = H (rj.data, hj-1);

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.



1 DNS服务器

IP: 61.128.128.68 端口: 53

2 目标域名及别名

www.a.shifen.com

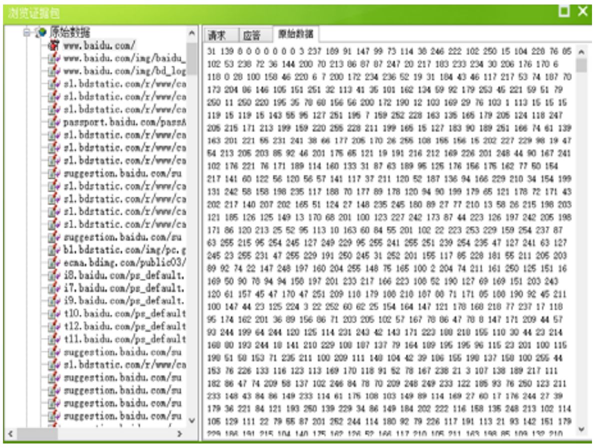
3 目标域名IP列表

180.97.33.108 180.97.33.107

4 目标域名IP

180.97.33.108

5 取证路由



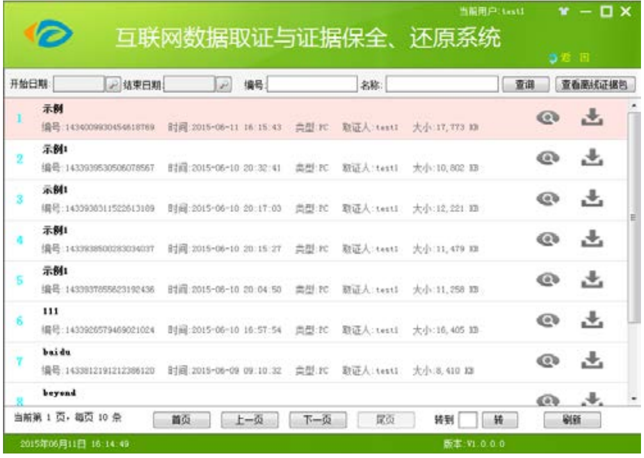
```
www.baidu.com/
www.baidu.com/img/baidu_
www.baidu.com/img/bd_log
s1.bdstatic.com/r/www/ca
s1.bdstatic.com/r/www/ca
s1.bdstatic.com/r/www/ca
passport.baidu.com/passA
s1.bdstatic.com/r/www/ca
s1.bdstatic.com/r/www/ca
s1.bdstatic.com/r/www/ca
suggestion.baidu.com/su
s1.bdstatic.com/r/www/ca
s1.bdstatic.com/r/www/ca
s1.bdstatic.com/r/www/ca
s1.bdstatic.com/r/www/ca
suggestion.baidu.com/su
b1.bdstatic.com/img/pc.g
ecma.bdimg.com/public03/
i8.baidu.com/ps_default.
i7.baidu.com/ps_default.
i9.baidu.com/ps_default.
t10.baidu.com/ps_default
t12.baidu.com/ps_default
t11.baidu.com/ps_default
suggestion.baidu.com/su
s1.bdstatic.com/r/www/ca
suggestion.baidu.com/su
suggestion.baidu.com/su
suggestion.baidu.com/su
suggestion.baidu.com/su
```

```
31 139 8 0 0 0 0 0 0 3 237 189 91 147 99 73 114 38 246 222 102 250 15 104 220 76 85
102 53 238 72 36 144 200 70 213 86 87 87 247 20 217 183 233 234 30 206 176 170 6
118 0 28 100 158 46 220 6 7 200 172 234 236 52 19 31 184 43 46 117 217 53 74 187 70
173 204 86 146 105 151 251 32 113 41 35 101 162 134 59 92 179 253 45 221 59 51 79
250 11 250 220 195 35 78 68 156 56 200 172 190 12 103 169 29 76 103 1 113 15 15 15
119 15 119 15 143 55 95 127 251 195 7 159 252 228 163 135 165 179 205 124 118 247
205 215 171 213 199 159 220 255 228 211 199 165 15 127 183 90 189 251 166 74 61 139
163 201 221 55 231 241 38 66 177 205 170 26 255 108 165 156 15 202 227 229 98 19 47
54 213 205 203 85 92 46 201 175 65 121 19 191 216 212 169 226 201 248 44 90 167 241
102 176 221 76 171 189 114 160 133 31 87 63 189 95 125 176 156 175 162 77 50 154
217 141 60 122 56 120 56 57 141 117 37 211 120 52 187 136 94 166 229 210 34 154 199
131 242 58 158 198 235 117 188 70 177 89 178 120 94 90 199 179 65 121 178 72 171 43
202 217 140 207 202 165 51 124 27 148 235 245 180 89 27 77 210 13 58 26 215 198 203
121 185 126 125 149 13 170 68 201 100 123 227 242 173 87 44 223 126 197 242 205 198
171 86 120 213 25 52 95 113 10 163 60 84 55 201 102 22 223 253 229 159 254 237 87
63 255 215 95 254 245 127 249 229 95 255 241 255 251 239 254 235 47 127 241 63 127
245 23 255 231 47 255 229 191 250 245 31 252 201 155 117 85 228 181 55 211 205 203
89 92 74 22 147 248 197 160 204 255 148 75 165 100 2 204 74 211 161 250 125 151 16
169 50 90 78 94 94 158 197 201 233 217 166 223 108 52 190 127 69 169 151 203 243
120 61 157 45 47 170 47 251 209 118 179 188 218 187 88 71 171 85 188 190 92 45 211
100 147 44 23 125 224 3 22 252 60 62 25 154 164 147 121 178 168 218 77 237 17 118
95 174 162 201 36 89 156 86 71 203 205 102 57 167 78 86 47 78 8 147 171 209 44 57
93 244 199 64 244 120 125 114 231 243 42 143 171 223 188 218 155 110 30 44 23 214
168 80 193 244 18 141 210 229 108 187 137 79 164 189 195 195 96 115 23 201 100 115
190 51 58 153 71 235 211 100 209 111 148 104 42 39 186 155 198 137 158 100 255 44
153 76 226 133 116 123 113 169 170 118 91 52 78 167 238 21 3 107 138 189 217 111
182 86 47 74 209 58 137 102 246 84 78 70 209 248 249 233 122 185 93 76 250 123 211
233 148 43 84 86 149 233 114 61 175 108 103 149 89 114 169 27 60 17 176 244 27 39
179 36 221 84 121 193 250 139 229 34 86 149 184 202 222 116 158 135 248 213 102 114
105 129 111 22 79 55 87 201 252 244 114 180 92 79 226 117 191 113 21 93 142 151 179
```

Fig 5. Routing information record acquisition　　　　　　Fig 6. Original data acquisition

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.



1 示例
编号:14340099304546l8769 时间:2015-06-11 16:15:43 类型:PC 取证人:test1 大小:17,773 KB

2 示例1
编号:1433939530506078567 时间:2015-06-10 20:32:41 类型:PC 取证人:test1 大小:10,802 KB

3 示例1
编号:1433938311522613109 时间:2015-06-10 20:17:03 类型:PC 取证人:test1 大小:12,221 KB

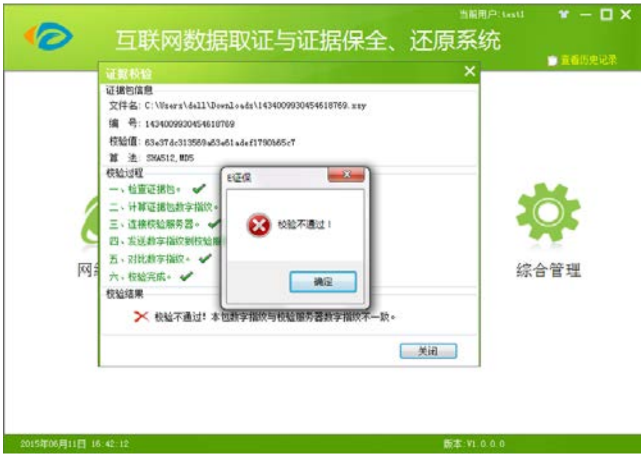
4 示例1
编号:1433938500283034037 时间:2015-06-10 20:15:27 类型:PC 取证人:test1 大小:11,479 KB

5 示例1
编号:1433937855623192436 时间:2015-06-10 20:04:50 类型:PC 取证人:test1 大小:11,258 KB

6 111
编号:1433926579469021024 时间:2015-06-10 16:57:54 类型:PC 取证人:test1 大小:16,405 KB

7 baidu
编号:1433812191212386120 时间:2015-06-09 09:10:32 类型:PC 取证人:test1 大小:8,410 KB

8 beyond



证据包信息

文件名: C:\Users\dell\Downloads\1434009930454618769.zzy

编　号: 1434009930454618769

校验值: 63e37dc313569a83e61adef1790b65c7

算　法: SHA512,MD5

校验过程

一、检查证据包。✓

二、计算证据包数字指纹。✓

三、连接校验服务器。✓

四、发送数字指纹到校验服务器。✓

五、对比数字指纹。✓

六、校验完成。✓

校验结果

✗ 校验不通过！本包数字指纹与校验服务器数字指纹不一致。

校验不通过！

Fig 7. Evidence Management　　　　　　Fig 8. Evidence Verification

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

[1] Teaching Materia Writing and Editing Council in Ministry of Public Security.Security Supervise on Network Information.The Mass Press,2000.

[2] Warren G.Krusell,Jay G.Heiser.Computer forensics:incident response essentials.1st Edition.ISBN:0201707195,Pearson Education,Inc,USA.

[3] Heather M. Online and Out of Line Why is Cyber Crime on the Rise, and Who’s Responsible[EB/OL]. (2002-01-01).

[4] Michael R.Anderson. Computer evidence processing:the important first step—safe seizure of the computer.http://www,forensics-intl.comm.

[5] Anderson Michael R. Electronic fingerprints-computer evidence comes of age,http://www.forensics-intl.com.

[6] A. Lazzez, “A Survey about Network Forensics Tools”, International Journal of Computer and Information Technology, vol. 2, issue 1, pp. 74-81, January 2013.

[7] Report From the First Digital Forensic Research Workshop (DFRWS), November 6th 2001.

[8] A. Yasinsac and Y. Manzano, "Honeytraps, A Network Forensic Tool," Proceedings of the 6th World Multi-Conference on Systemics, Cybernetics, and Informatics (SCI 02) 2002.

[9] M. Cohen, "PyFlag - An advanced network forensic framework," Digital Investigation, vol. 5, pp. 112-120, 2008.

[10] SWDGE and IOCE, Digital Evidence: Standards and Principles, 1999.

[11] E. Casey, Digital Evidence and Computer Crime: Forensic Science, Computer and the Internet, ACADEMIC PRESS, 2000.

[12] W. G. Kruse and J. G. Heiser, Computer Forensic: Incident Response Essentials, Addison Wesley, 2002.

[13] Michael M. Cloud Computing: Web-based Applications that Chan- ge the Way You Work and Collaborate Online[M]. [S. l.]: Que Publishing, 2009.