The Importance of Web Activities for Computer Forensics

Prof. Dr. Asaf VAROL  
Fırat University, Faculty of Technology  
Elazığ, Türkiye  
varol.asaf@gmail.com

Yeşim ÜLGEN SÖNMEZ  
Fırat University, Faculty of Technology  
Elazığ, Türkiye  
yesimulgen123@gmail.com

Abstract— Web activities are big data revealing the thoughts and intentions of users. Every file that is downloaded, and each searching word in the search engine are thought as reflections of the user’s tendencies. Web activities are used to analyze in traces of crime in all kinds of information systems such as computers and mobile phones which are electromagnetic optical devices.

The use of smart systems or statistical inference models in the electronic evidence analysis will contribute to the development of digital forensic tools and information technology law. The evidence analysis stage will be faster and automatic. The aim is to extract web browsing data by starting from search engine browsing data with appropriate methods, and sort out the data pointing crime by applying various techniques.

Keywords — Web activities, computer forensics, web browsers

I. INTRODUCTION

Computer forensics is a process of technical examination conducted in any kind of information system. Computer forensics does not involve an interpretation activity.

This process includes stages of identification of scene, protection, collection, analyzing and reporting of digital evidence, respectively [1, 2]. These stages and the instruments used for research or commercial purposes are shown in Figure 1 [3, 4].

Figure 1. Computer forensics process and evidence analysis stage
The purpose of computer forensics is to transform the digital evidence, which is considered as a potential for criminal investigation, into legal digital evidence [5]. These legal digital evidences may contain information for any criminal case, ranging from a suicide case to the discovery of communications between narcotics traffickers, to offenses of libel in social media and to seizure of information in a bank database by attackers [6].

Forensic investigations in information systems are not always based on realized crime. These forensic analyzes can also carry out a potential crime which is predictive or proactive, performing estimation and prevention at the same time.

When recent literature is examined, involving prior identification and prevention of crime (predictive - proactive) models become more important as much as committing or repeating a crime (active - reactive) models in the field of computer forensics.

II. DIGITAL FORENSICS

For this study, computer forensics science, all subdisciplines and computer forensics process are examined in the literature. In the evidence analysis stage of the computer forensics process, methods such as intelligent systems [7], clustering, association rules, support vector machines [8], artificial neural networks [9] and bayesian networks [10, 11] have been studied. The aim of this study is to classify the evidences, to work better on the suspicious evidence and to remove the possibilities in results. Efforts to accelerate the process of evidence analysis and to automate it by releasing from human dependency continue. In particular, studies on intelligent crime prevention models contribute to this area [12].

In the computer forensics process, the web activity of the people is also examined during the analysis stage where the evidence is examined in depth. Sites that the person visits while using the internet, files downloaded or even a word they searched are stored on their computer. They carry traces of a committed or suspected suicide. As in Figure 2, internet, web browsers and search engines are tools that are used to commit a crime, so that they can be used as gates that give certain information about the crime [13]. In addition, web browsers are the interface between the internet and the user. Therefore, web browsers, the gateways, are important in computer forensics.

This study aims to develop a new model to detect criminal tendency by taking advantage of one's web activities by considering the most used web browsers. For web activities, search engine browsing data will be used primarily; but if the data for the predefined crime definition cannot be found in the search engine, all web activities will be examined.

III. EVIDENCE ANALYSIS STAGE IN WEB FORENSICS

When the literature is examined, it is seen that studies for accelerating the evidence analysis stage of the computer forensics process is gaining importance. These studies contribute to the quick and accurate decision making of both computer forensics specialist and judicial decision makers [14]. Findings and criminal predictions or predictive models which are obtained before the crime are as important as the detection of digital evidence after the crime.

The most important problem for such models is whether the definition of crime is done in the most correct way, i.e. in accordance with the law. The aim is to extract web browsing data, starting from search engine browsing data by appropriate means and sorting out the data pointing crime by applying various techniques such as similarity and correlation. For this reason, it is necessary to determine which web activities indicate which crime well. Existing search engine analysis software tools and studies have been examined to solve these problems. These tools expose the user's web activities with methods such as similarity and correlation; but the specialist's job is to find data about crime. For this reason, it is necessary to simplify the work of the specialist by selecting well methods applying on the browsing data.

Web browsers and search engine browsing data should be examined for resolving these problems and for the progress of the work. Research from web browser information to software tools which analyze web activities is presented in this section.

Google Chrome, Mozilla Firefox, Internet Explorer, Opera, Safari are the most popular web browsers in the world today. Searches made on the search engine, sites browsed, documents and sites downloaded by the users are kept as web storage records. The places where these records are kept according to the operating system and web browser.

Web activities are kept in browsers' internet history, bookmarks, downloads, cache, cookies folders. Figure 3 [15], shows which of these folders provide an answer to which of these questions for web analysis.
These data are in SQLite, SNSS (Session Saver), JSON (Java Script Object Notation) and XML formats. They are viewed by SQLite Viewer program [16]. Figure 3 shows web storage file types are given [17].

**Table 1. Web computer forensic tools**

<table>
<thead>
<tr>
<th>COMPUTER FORENSICS TOOLS</th>
<th>WEB CONTENT ANALYZED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phrozen Browser Forensics Tool</td>
<td>Scans history and words</td>
</tr>
<tr>
<td>History Viewer</td>
<td>History, cookies, key words, downloads</td>
</tr>
<tr>
<td>MyLastSearch</td>
<td>Search queries</td>
</tr>
<tr>
<td>ChromeCookie View</td>
<td>Cookies</td>
</tr>
<tr>
<td>Chrome Password Decryptor</td>
<td>Password decryption</td>
</tr>
<tr>
<td>ChromeCache View</td>
<td>Cache</td>
</tr>
<tr>
<td>Internet Evidence Finder</td>
<td>Unallocated space, default folders</td>
</tr>
<tr>
<td>Cookie Cutter</td>
<td>Google Analytics cookies, search words</td>
</tr>
<tr>
<td>Chrome Analysis</td>
<td>History, bookmarks, cookies, search words, downloads</td>
</tr>
<tr>
<td>Web Historian</td>
<td>History</td>
</tr>
<tr>
<td>Access Data FTK Imager</td>
<td>Web analysis, finds data deleted by “Delete History” command</td>
</tr>
</tbody>
</table>

Web browsers have normal, incognito, and portable modes. While the web activity of the person is saved in normal mode, the purpose in private/incognito mode is to hide these activities [18]. Although web browsers have private modes, traces of crime can be obtained with live (RAM) analysis [19].

For example, a suspect who uses private mode enters to some sites in private mode and then closes the browser. Belkasoft RAM Capturer software is used by the forensic specialist to taken an image of the RAM in this system, then the web activity of this suspect is accessed when the image is viewed with Winhex software [20].
Table 1 presents the forensic tools used for the web. Web activity of the suspect is detected by these tools. The most important of these activities is history. The evidence that reveals the intentions of the suspect is found in the “History”. Which sites are entered, which words are searched on the search engine, when and how many times a site is looked at is detected by the “History” in Figure 5 [16].

With the Internet Evidence Finder program, visited site information and search engine search can be accessed via RAM image [21]. These studies in the literature are used to reveal the web activities that people have in their systems. The specialist distinguish the evidence from these activities by accurate and systematic methods.

In particular, the information in the History folder can be used to reveal a crime or to prevent a criminal intent. Again, it is noteworthy that intelligent systems or statistical methods are not used in this field.

Another problem is that the suspect's web activity can be monitored without the knowledge of suspect. For this reason, the live analysis on the suspect's information system can be done with remote access computer forensic methods [22].

Live analysis is RAM memory analysis. Various hardware and software tools are used for memory analysis and the most appropriate tools can be selected from studies that compare these tools for integrity and accuracy [23].

New methods are carried out on the traces which are dropped by web browsers on the web servers, even the similarity features of browsers are being compared. There are approaches to use these methods in computer forensics [24].

IV. FORENSICS SOFTWARES FOR WEB ACTIVITIES

Studies on electronic evidence research based on the analysis of users' behavioral correlations [25] and studies on the suspect's web browser activities using the Appriori algorithm [26] will also be utilized.

Figure 6 shows the examination of web browsing data as computer forensics and the simulation of this work.

Web browsing data can be obtained via Web Browser Forensics Tools and especially History Viewer program used on the hard disk and RAM images obtained by programs such as Encase, Access Data FTK Imager, Belkasoft RAM Capturer, Internet Evidence Finder, etc. These tools only present electronic activities of the person, not list possible evidence concerning the crime. There are studies that use classifiers on Internet history [27]; but more contribution is needed in this field.

In addition to contributing to the computer forensics science, if the desired success in detecting a crime or criminal intent is achieved, it will also contribute to areas such as security and information technology law.

![Figure 5. History file opened with History Viewer Program](image-url)
V. CONCLUSION

This study will be a new model in order to improve the existing computer forensics process by starting with the literature reviews. Thus, accurate, fast and reliable evidences will be provided to the courts, and the decision-making process of the courts will be facilitated. Information technologies will be an application that can be used and improved on many fields, such as computers forensics and information technology law.

When the studies in the literature are examined, it is seen that the evidence analysis stage of process has not been automated. In evidence analysis stage, web activities should be examined in more detail and a model that makes criminal prediction should be developed. In this predictive model, which involves smart and/or statistical methods, will contribute to web browsing forensics field. If the desired success is achieved with this model, maybe a new study field such as search engine data computer forensics will be able to be produced.

REFERENCES


Y. Bolat, Memory Forensics, İstanbul Bilgi Üniversitesi, Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezsi, 2015.


