© 2017 IJSRST | Volume 3 | Issue 6 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X
Themed Section: Science and Technology

Post-Genesis Digital Forensics Investigation

Suci Ramadhani[1], Yasmirah Mandasari Saragih[2], Robbi Rahim[3], Andysah Putera Utama Siahaan[4]

[1,2,4]Faculty of Computer Science, Universitas Pembangunan Panca Budi, Medan, Indonesia
[3]Department of Health Information, Akademi Perekam Medik dan Infokes Imelda, Medan, Indonesia
[3,4]Student of Universiti Malaysia Perlis, Kangar, Malaysia

ABSTRACT

Digital Forensics is a technique used to search for evidence of events that have occurred. This quest aims to reveal the hidden truth. The existence of digital forensic activities due to the occurrence of crimes both in the field of computers or other. Legal treatment in digital forensic field makes this area of science a compulsory device to dismantle crimes involving the computer world. In general, the cyber crime leaves a digital footprint, so it is necessary for a computer forensics expert to secure digital evidence. Computer forensics necessarily requires a standard operational procedure in taking digital evidence so as not to be contaminated or modified when the data is analyzed. The application of digital forensic is beneficial to the legal process going well and correctly.

Keywords: Digital Signature, Cyber Crime

I. INTRODUCTION

Forensics in the computer world has a relationship with the judiciary or the judiciary. While in medicine, forensics is a branch of medical science related to the application of medical facts to legal matters [1]. However, the forensic term is a scientific process of collecting, analyzing and presenting various evidence in a court of law regarding the existence of a legal case. The field of forensics has been growing for a long time. The legal method of today continues to increase until it eventually uses human DNA. The forensics method is always involved with computer science to strengthen the digital evidence collected from crime [2]. As computer crimes arise such as fake photos and immoral videos, digital forensics will help to reveal the facts. However, how to dismantle crime and find actual evidence is not easy to do. By applying computer science to forensics, this is expected to help the legal process take place quickly and precisely.

II. THEORIES

2.1 Computer Forensics

Computer forensics is the implementation of the scientific method to digital media to reconstruct the factual information for judicial review. Another term for computer forensics is the collection and analysis of data from various computer resources including computer systems, computer networks, communication lines, and appropriate storage media for trial. The existence of computer science of forensics is much needed nowadays especially in the future because the number of computer-based crimes can not be proven in real terms, so sometimes it is not recognized as evidence in court for such cases [3]. So no wonder at institutions like the police has a special department for this computer forensics. Various digital behaviors and digitalization that has penetrated in every human activity become a behavior that must be observed properly. Computer forensics or digital forensics are widely deployed in a variety of purposes, not just criminal cases involving the law. In general, the need for computer forensics can be classified as follows:

1. The need for criminal investigations and lawlessness cases.
2. Reconstruction sitting case of computer security incident.
3. Recovery efforts will damage the system.
4. Troubleshooting involving both hardware and software.
5. The need to understand the system or various

digital devices better.

The more complex the crime in the computer field, the higher the computer science of forensics extends the study of science from various aspects [4][5]. Therefore, it is necessary to divide the concentration of science in the field of computer forensics; it is intended that in investigating to uncover the crime and even restore the system after the damage can easily be done because it has been divided into several concentrations, such as:

- Disk Forensics
- System Forensics
- Network Forensics
- Internet Forensics

Disk forensics is the concentration of science this one has begun to develop, where disk forensics involves a variety of storage media. It has been well documented in the various literature, even IT professionals can handle the problem of the disk forensics. Suppose, get the files that have been deleted, change the hard drive partition, look for traces bad sectors, restoring windows registry modified or hidden by a virus and so forth. However, there are still many IT professionals who do not know that the above behavior is one of the computer forensic sactions.

System forensic sis the method that closes to the operating system. It is still difficult to be studied more deeply; it is due to the many operating systems that are developing today, where the operating system has different characteristics and behaviors, such as various file systems, Therefore the existing forensic methods are still difficult to be averaged. The obstacle is the current support software where as a tool to dissect the operating system is still flatform windows. It is what causes the need for the development of science.

Network forensics is a method of capturing, storing and analyzing user network data to find the source of a system security breach or information system security problem. If we are talking about this one part, it certainly involves the OSI layer, which explains how computers can communicate. It does not only involve a LAN network system but can include into a larger network system.

Internet forensics is more complicated than others because there are many computers connected to each other and its usage can be concurrent without taking into account the distance so in this section requires complex techniques. Through internet forensics, the analyzer can track who sends e-mails, when to send and where the sender is, this can be done given the increasing number of fake e-mails that are on behalf of a particular company with lucky draw mode that will harm the recipient or even a lot of threatening e-mail. Therefore internet forensics becomes a science that is very promising in revealing the facts and gather evidence.

2.2 Digital Evidence

The evidence is referred to information or data. The point of view is same, but in the case of computer forensics, the subject is the digital evidence [6]. The more complex the context of digital evidence due to media factors that embed the data, the harder it is to reveal the facts behind it. Formatting will also affect the way to digital evidence, such as digital evidence in the form of documents, which are categorized into three parts, such as:

1. Archieval Files
2. Active Files
3. Residual Data

Archived files are required for the file in the archiving function, including handling documents to be stored in the prescribed format, retrieving and distributing process for other needs, such as some documents that are digitized to be stored in TIFF format to maintain document quality.

Active files are files that are used for various purposes that are closely related to the activities that are being done, such as image files, text documents, and others. While the files belonging to the residual include the files that are produced along with computer processes and user activities, e.g., record usage in using the internet, database logs, various temporary files, and so forth.

Digital evidence is scattered in different media and contexts, so it takes more foresight than simply classifying data for forensic purposes [7][8]. Keep in mind also, the more peripherals or devices integrated

into computer systems, it will be more complex and involves many considerations to lift digital evidence. It is one of the obstacles in accessing the files that will be used as evidence.

The obstacles that may occur in the field at the time of investigation to retrieve data, such as:

1. Compressed file
2. One deliberately named the file or not
3. Incorrect in providing file format, intentionally or not
4. Password-protected files
5. Hidden Files
6. The file is encrypted
7. Watermarking

III. RESULT AND DISCUSSION

3.1 Forensic Model

The model in forensic science is applicable in many fields, and this model involves three components that are assembled, empowered and managed in such a way to be the ultimate goal with all feasibility and quality. Three components include:

- Human
- Equipment
- Protocol

Human is required in computer forensics is the perpetrator who certainly required certain qualifications to achieve the desired quality. It is easy to learn computer forensics, but to become an expert another story; it takes more than just knowledge but the experience that makes it said to be an expert. There are three groups as a computer forensics performer, Collection Specialist, Examiner, and Investigator. Collection Specialist duty to collect evidence in the form of digital evidence. For the examiner level only has the ability as a test of media and extract data while the investigator is already at the expert level or as an investigator. The equipment must be used in such a way as to obtain quality evidence. There is much required involving specific software and various hardware as well as various storage media in handling the data later. Protocol is the most critical component in computer forensics modeling, the rules of digging, obtaining, analyzing and finally presenting in the reports. The rules in computer forensics that an expert must run in four phases include:

- Collection
- Testing
- Analysis
- Reports

Collection is the first step in the forensics process to identify potential sources and how the data is collected. This collection involves increasingly complex processes and methods due to rapid technological developments, multiple computers, a wide variety of storage media and many computer networks with all the technologies attached to them. Surely this complexity requires different handling. After conducting the data collection process, a further step is to conduct testing, including in assessing and extracting relevant information from the data collected. Once the information is extracted, the examiner performs an analysis to formulate the conclusions in describing the data. The analysis in question certainly takes a methodical approach in generating quality conclusions based on the availability of data. Documentation and reporting are the final stages of computer forensics. In this stage, the information is the result of the analysis process.

3.2 Computer Surgery

In performing computer surgery, we need to know what part we should have surgical in collecting information, in the previous chapter has been discussed about the four concentrations in computer forensics and in this section, which in surgery is Disk Forensics.

3.2.1 Windows Registry

When accessing the windows registry, this process is also called computer surgery because the registry is a substantial system configuration and is a single logical and store. The registry is divided into three separate databases and allocated to handle users, systems, and network settings, where these sections hold precious information. To dismantle the registry should be known in advance structure than the windows registry. The registry consists of seven root keys, such as:

- HKEY_CLASSES_ROOT

- HKEY_CURRENT_USER
- HKEY_LOCAL_MACHINE
- HKEY_USERS
- HKEY_CURRENT_CONFIG
- HKEY_DYN_DATA
- HKEY_PERFORMANCE_DATA

In this registry will be seen anything just the information stored in it, for example, Figure 1 illustrates the internet activity can access registry key as follows: HKEY_CURRENT_USER\ Software\Microsoft\InternetExplorer\TypedUrl.

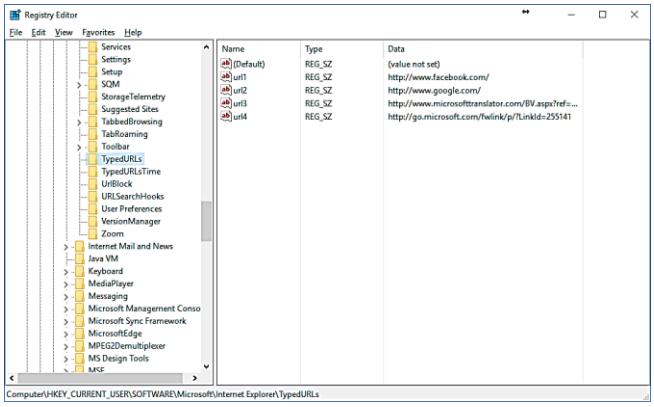

Figure 1. Internet Activity Registry

3.2.2 Post-Damage Handling

In repairing a damaged system, it needs software to recover a damaged system. Damage to the system that occurs can be caused by factors of the carelessness of humans and viruses that infect the computer and need to know also the parts of the computer that must be restored. In this section, it will be given a simple example of damage to the registry that modifies the recycle bin name.

If this is the case, an analyzer usually has been able to analyze the causes and ways of recovery. There are two causal factors, which can be due to viruses and can be deliberate by the user. Moreover, that needs to know is if this is because the virus is usually the main purpose of a virus maker is the windows registry because with this section the virus can disable the computer system by destroying, modify or to hide the registry.

3.3 The legal role of digital forensics

Electronic information can be distinguished from electronic documents, but can not be separated from each other. Electronic information is information contained in a medium. This information is news, sound recordings, pictures, videos or things that refer to an event. Meanwhile, electronic documents are how the information is stored or wrapped. Some keep the recorded conversation in MP3 or WAV format, or there is a secret information stored in an encrypted image file.

The expansion of evidence is set in the laws of each country. It includes corporate document law, terrorism, corruption eradication, money laundering crime. The electronic law confirms that in all applicable procedural laws of each country electronic information, document and prints may be used as legal evidence in court. Thus, email, chatting files over chats, and various other electronic documents can be used as valid evidence. In some court decisions, there are decisions concerning the position and acknowledgment of electronic evidence presented in the tribunal.

Presentation of digital evidence is a trial process in which digital evidence will be verified and linkage between one and the other with the current case. It is the appointment of digital evidence related to the ongoing crime. The process of investigation takes a long time to reveal the truth and find the cause of a case. It takes a long time to go through the trial process. Digital evidence is expected to remain original and unmodified when identified by the investigator at the time the evidence is found.

The important thing investigators need to know to protect evidence is the chain of custody. It is to keep the evidence obtained at the time of the crime or case by minimizing the damage caused by investigation and analysis. Evidence must be genuine. When the investigator examines the evidence, it must not be defective or physically or non-physically altered so that the messages arising from such evidence are not lost or modified.

The goals of the chain of custody are:

- The evidence is original
- At the time of the trial, the evidence is still as it was found.

IV. CONCLUSION

There are much more areas of computer forensics that must be explored deeper. This field has become a significant part in exposing computer crimes. It is not part of it because the science is increasingly advanced rapidly coupled with human morals are becoming more degenerate and far from the values of religion. It is necessary for the monitoring of any human activities that concern the interests of the community, especially with the easy internet access, even from mobile phones, people can access whatever is in this world. Another important thing is that the existence of the law does not necessarily make everyone become themselves as perpetrators in computer forensics. There are already rules set to become authors of computer forensics. Only the authorized officers as police, an attorney is entitled to investigate to obtain evidence of digital evidence from other persons unless the competent authority has designated it. It is therefore advisable not to take action in previous chapters above for personal benefit except for learning for science and technology development.

V. REFERENCES

[1]. R. Kaur and A. Kaur, "Digital Forensics," International Journal of Computer Applications, vol. 50, no. 5, pp. 5-9, 2012.

[2]. F. Jafari and R. S. Satti, "Comparative Analysis of Digital Forensic Models," Journal of Advances in Computer Networks, vol. 3, no. 1, pp. 82-86, 2015.

[3]. R. Rowlingson, "A Ten Step Process for Forensic Readiness," International Journal of Digital Evidence, vol. 2, no. 3, pp. 1-28, 2004.

[4]. S. Perumal, "Digital Forensic Model Based On Malaysian Investigation Process," International Journal of Computer Science and Network Security, vol. 9, no. 8, pp. 38-44, 2009.

[5]. M. R. Chourasiya and A. P. Wadhe, "Implementation of Video Forensics Frame Work for Video Source Identification," in International Conference on Science and Technology for Sustainable Development, Kuala Lumpur, 2016.

[6]. H. K. Siburian, "A Study of Internet and Cyber Crime," International Journal of Scientific Research in Science and Technology, vol. 2, no. 6, pp. 223-226, 2016.

[7]. Y. M. Saragih and A. P. U. Siahaan, "Cyber Crime Prevention Strategy in Indonesia," International Journal of Humanities and Social Science, vol. 3, no. 6, pp. 22-26, 2016.

[8]. H. K. Siburian, "Emerging Issue in Cyber Crime: Case Study Cyber Crime in Indonesia," International Journal of Science and Research, vol. 5, no. 11, pp. 511-514, 2016.