BOOK CHAPTER | *"Chains of Reactions "*

Application Information for Forensic Analysis

Considerations for Registered Host / Users / Device Name & Bearer Tokens

Rosemond O. Addo-Sampong
Digital Forensics and Cyber Security Graduate Programme
Department of Information Systems & Innovations
Ghana Institute of Management & Public Administration
Greenhill, Accra, Ghana
E-mail: rosemonddartey@gmail.com
Phone: +233242615658

ABSTRACT

As the dependence on digital information and the Internet continues to grow, it changes the way of computer crime. The number of computer crimes increases dramatically in recent years and investigators have been facing the difficulty of admissibility of digital evidence. To solve this problem, we must collect evidence by digital forensics techniques and analyze the digital data or recover the damaged data. One place to collect evidence is from application software. This paper seeks to find out how to collect, store and analyze application information for forensic purposes. This is also to determine gaps in current research works and proffer recommendations on what future works relate to application forensics.

Keywords: Digital Forensics, Evidence, Application Information, Analysis, Registered Host

BOOK Chapter | Research Nexus in IT, Law, Cyber Security & Forensics. Open Access. Distributed Free

Citation: Rosemond O. Addo-Sampong (2022): Application Information for Forensic Analysis
(Considerations for Registered Host / Users / Device Name & Bearer Tokens)
Book Chapter Series on Research Nexus in IT, Law, Cyber Security & Forensics. Pp 167-172
www.isteams.net/ITlawbookchapter2022. dx.doi.org/10.22624/AIMS/CRP-BK3-P27

1. INTRODUCTION

The world is a rapidly changing one in which digitalization is the driving force of every activity. This digitalization has brought about the desire to consume information at such exponentially increasing speed and intensity. Thus, the world is termed an Information Society. Data and information have now become the gold of every organization. In most organizations and workplaces, using common or compatible technology for a wide range of personal, social, educational, and business activities, and the ability to transmit, receive and exchange digital data rapidly between places irrespective of distance. Simply put, Information Society is a term for a society in which the creation, distribution, and manipulation of information have become the most significant economic and cultural activity through the use of ICTs.
The Internet is the most popular application in modern society. It brings a lot of convenience of communication to humans. It literally bridges the physical gaps in basic human

communications. The Internet is a space where massive amounts of data and information are shared between multiple entities every second of the day. On the back of the exponential consumption of data and information are the various software applications. There are millions of software applications for various uses. In any part of the world, there are at least a hundred applications supporting whatever digital activity an entity finds itself. Be it social media, banking, education, public sector, transportation agriculture, mining, health, etc. these applications have become part of the human being's everyday life. All applications have databases that support, store, and manipulate data/information for the smooth running of these applications.

The value of data and information stored in these databases of applications has kept the rate of cyber-attacks and cyber-related crime at an all-time high. Reports from the FBI, CISA, and a host of security firms indicate that such crimes will continue to rise along with their negative impacts on people and organizations. The reason is that crimes can be committed remotely, and criminals can assume faceless individuals because the internet allows it. Evidence is volatile and can be difficult to trace. This means that technology in one country is used to perpetuate a crime in another. Also, national law enforcement is governed by geography, and as such international assistance needs proper legal channels. Another reason is that cooperation deals with different countries with different legal frameworks. Thus, some activities are not defined as criminal in some jurisdictions. When cybercrime such as a software application attack, or hack occurs, the gathering of evidence is very crucial for the establishment of the crime or otherwise, how it happened and the prosecution of the accused. It has become difficult to obtain and analyze data/information from the application. This is where the need for forensic analysis or investigations is very important.

Fig 1: Media Information Carrier Used for Digital Forensic Analysis

Source: https://en.wikipedia.org/wiki/Computer_forensics#/media/File:PersonalStorageDevices.agr.jpg

1.1 Background into the Study

Digital forensics is defined as the analysis of data, such as audio, video, etc., obtained after the examination of electronic devices, to help the legal process by obtaining digital evidence to establish the occurrence of a crime or otherwise. Sengul & Erhan (2017) defines digital forensics as a branch of forensic science encompassing the recovery, investigation, examination, and analysis of material found in digital devices, often in relation to mobile devices and computer crime. Digital forensics investigations have a variety of applications. The most common is to support or refute a hypothesis before criminal or civil courts. Today, with the advancement of technology, electronic devices are diversified such as tablets, flash memory, and memory cards. Generally, the purpose of digital forensics is to investigate the evidence, and might include computer intrusion, unauthorized access, child pornography, etc.

Fundamentals of the computer forensics analysis process as falling into three distinct areas acquisition, analysis, and Presentation.

1. Acquisition Phase: This phase is focused on obtaining the states of systems that have storage devices and all the digital data for later analysis. We usually used forensic tools to create an image of the disk.
2. Analysis Phase: Identification of the pieces of evidence collected, which include file types, contexts of a directory, and rescue data for finding the relation between evidence and incident.
3. Presentation Phase: Documentation of analyzing data for assisting the prosecutors to reference.

During the investigation, the investigator should assure that digital evidence is not modified without proper authorization. The typical goal of an investigation is to collect evidence using generally accepted methods to make the evidence accepted and admitted to the court.

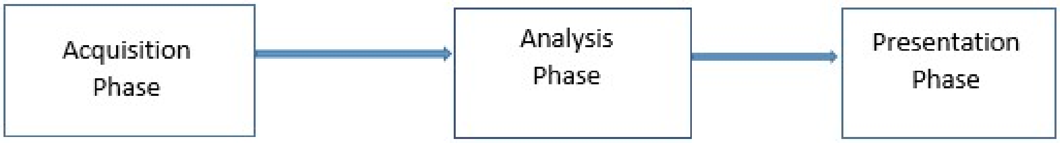

Fig 1.1 Digital Forensic Process

Any step in the process must be carefully recorded to prove the electronic records were not altered in the investigation procedure. Digital forensics can be classified into live analysis and dead analysis A live analysis occurs when the suspect system is being analyzed while it is running while a dead analysis occurs when a dedicated analysis system is used to examine the data from a suspect system.

According to Wikipedia, digital forensics investigation is not restricted to retrieving data merely from the computer, as laws are breached by the criminals and small digital devices (e.g., tablets, smartphones, flash drives) are now extensively used. This has given rise to several branches of digital forensics to cater to all types of mobile devices, uses, and applications.

The branches of digital forensics are.

1. Computer Forensics: Hany F. Atlam et.al postulates that the goal of computer forensics is to explain the current state of a digital artifact, such as a computer system, storage medium, or electronic document. The discipline usually covers computers, embedded systems (digital devices with rudimentary computing power and onboard memory), and static memory (such as USB pen drives). Computer forensics can deal with a broad range of information; from logs (such as internet history) through to the actual files on the drive.
2. Mobile device forensics is a sub-branch of digital forensics relating to the recovery of digital evidence or data from a mobile device. It differs from Computer forensics in that a mobile device will have an inbuilt communication system (e.g., GSM) and, usually, proprietary storage mechanisms. Investigations usually focus on simple data such as call data and communications (SMS/Email) rather than in-depth recovery of deleted data.
3. Network forensics is concerned with the monitoring and analysis of computer network traffic, both local and WAN/internet, for the purposes of information gathering, evidence collection, or intrusion detection. Traffic is usually intercepted at the packet level, and either stored for later analysis or filtered in real-time. Unlike other areas of digital forensics, network data is often volatile and rarely logged, making the discipline often reactionary.
4. Software forensics is the science of analyzing software source code or binary code to determine whether intellectual property infringement or theft occurred. It is the centerpiece of lawsuits, trials, and settlements when companies are in dispute over issues involving software patents, copyrights, and trade secrets.

2. RELATED LITERATURE

Many researchers are focused on application forensics of specific applications and software. For example, in Sengul & Erhan (2017), the authors focused on how to evaluate the examination and analysis of mobile phones in terms of digital forensics. The research highlighted the rapid rise in digital crimes and the need to tackle the day-to-day rise of such crimes to ensure and aid in getting justice. It also talked about the mobile phone holding tons of information and data which can easily be erased or destroyed. The research also talked about the threats detected on mobile devices can be classified as direct attacks, malware, data interception, exploitation, and social engineering. It also highlighted at the same time, insufficient knowledge of users of these mobile phones. This poses a security threat to the user/owner of such devices.

Other research such as Ziad A. Al-Sharif, et al (2018) on *Live forensics of software attacks on cyber-physical systems,* focused on exploring RAM artifacts of Java programs. Because JVMs can run on various platforms and compare the same program on three different implementations of JVM from forensic perspectives. Some other works like Lin & Li (2016) in *Preprocessing Reference Sensor Pattern Noise via Spectrum Equalization*, were on specialized tools used to conduct digital forensics on users, devices, hostnames to obtain evidence of a crime that has taken place or otherwise. In this paper, a proposal was made to seek and develop a novel preprocessing approach for attenuating the influence of the non-unique artifacts on the reference SPN to reduce the false identification rate.

Hany F. Atlam , et-al (2020) postulates In the review of IoT devices this paper provides a detailed review of IoT forensics. The research talked about the IoT and how it has become part of life. Their research noted that the major issue associated with IoT applications is the capability to ensure the trustworthiness and protection of private data. Due to the complex, distributed, and heterogeneous nature of the IoT system, it faces several challenges regarding security and privacy.

3. RESEARCH GAPS AND FINDINGS

From the review of the above-related literature on the project topic, it was discovered most of the research focused on other aspects of technology and not software application forensics. The closest research was research specific into one application. The gap also identified was that there was no or little research that focused on how to obtain evidence forensically on any application. Thus, there was no generic guidelines or template to guide future research into application or software forensics. This is probably because, in digital forensics, most of the focus in acquiring evidence is on the computer or mobile device itself as the physical storage holds most of the data/information that a forensic expert or analyst would need to analyze to determine whether a crime has taken place or not and to help in the prosecution of court cases.

4. CONCLUSION

The world has become a global village with more people having access to mobile and computing devices. The internet has become the means for communication between entities across different geographical locations. Cybercrimes have increased with the increasing dependence on digital products in the work and personal lives of people. Most of our activities in cyberspace run on various software applications and as such, there is the need to conduct more research into application software forensics.

5. Recommendation and Implications for Policy, Practices, and Internet Safety In Africa

Some recommendations on policies and practices surrounding the development of applications stem from the fact that obtaining digital evidence from applications is very key. Another issue is storing the acquired evidence without tampering and can be admissible in court. Policies and practices of software application development should include having logs of all events on the software, storing information on the details of users, host names, bearer tokens, etc. This will enhance the collection of information / data on from an application software. Organizations should adopt two different environments for software development and testing and production. Implications of not having separate environments could hamper modifications, vulnerability assessments, risk assessments and upgrades of applications. With the spate of internet and cyber crimes on the increase, more cyber awareness trainings, seminars and teasers need to be conducted to make users of applications aware of the dangers of unsafe online practices. Data privacy and identity theft should be the main reasons for such awareness.

6. DIRECTION FOR FUTURE WORKS.

Future works ought to focus on research and development of a standardized procedure, policy, and frameworks on how to conduct application forensics. Such research would go a long way to help other forensic experts to know how to conduct forensic investigations on applications. For Africa,

REFERENCES

1. Sengul Dogan, and Erhan Akbal (2017) *Analysis of Mobile Phones in Digital Forensics*
2. Z.A. Al-Sharif, M.I. Al-Saleh, L.M. Alawneh, Y.I. Jararweh, B. Gupta, (2018) *Live forensics of software attacks on cyber physical systems, Future Generation Computer Systems*.
3. Xufeng Lin and Chang-Tsun Li (2016) *Preprocessing Reference SPN Via Spectrum Equalization*
4. Hany F. Atlam , Ezz El-Din Hemdan , Ahmed Alenezi , Madini O. Alassafi , Gary B. Wills , *"Internet of Things Forensics: A Review, Internet of Things (2020)*