BOOK CHAPTER | SIFTING Through

SIFT Multi-Purpose Forensic Operating System For Digital Forensic Process.

Francis Wodugah
Digital Forensics and Cyber Security Graduate Programme
Department of Information Systems & Innovations
Ghana Institute of Management & Public Administration
Greenhill, Accra, Ghana
E-mail: francis.wodugah@st.gimpa.edu.gh
Phone: +233243992299

ABSTRACT

The number of cyber incidents in which computer system or device is currently increasing every day. This requiring the opening up of forensic investigations in to multi-purpose forensic operating system for digital forensic process, a research that can shed light on what has occurred, In order to be able to provide investigators with proper solutions. for performing complete and efficient examinations in this new environment, operating systems platform and devices are being studied from a forensic perspective so that tools and procedures can be designed accordingly

Keywords: Forensic Investigations, Cyber Forensic, Multi-Purpose Forensic Operating.

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

Citation: Francis Wodugah (2022): SIFT Multi-Purpose Forensic Operating System For Digital Forensic Process. SMART-IEEE-Creative Research Publications Book Chapter Series on Research Nexus in IT, Law, Cyber Security & Forensics. Pp 55-58. www.isteams.net/ITlawbookchapter2022. dx.doi.org/10.22624/AIMS/CRP-BK3-P9

1. INTRODUCTION

The environment in which to conduct forensic investigations has introduced a great variety of new systems and devices that had never been analyzed before. Computers and smart phones have given way to smart switches, televisions, cars, and personal assistants. New contexts, such as eHealth, smart cities, and smart industries, have appeared, and operating system being present in almost every aspect of it. As a result, forensic investigators find it extraordinarily difficult to conduct an investigation in this environment. Although all these systems are quite dissimilar to each other, and have been developed to perform very different tasks. Aspects such as the operating system or firmware that they run, whether their memory is accessible or the way in which the investigator can access them are crucial for properly performing an examination.

For example, the approach that needs to be followed when analyzing a device running a real-time operating system (RTOS is not the same as when studying a general-purpose operating system (GPOS). Therefore, in order to provide investigators with guidelines on how to deal with them, the research community need to studies all these devices and describes what information can be recovered from them and how to do so.

1.1 Background to the Study.

In this regard, this paper presents a forensic analysis for a SIFT multi-purpose forensic operating system for digital forensic process, developed by Canonical, namely Ubuntu Core. Since it is based on one of the most widely used Linux distributions for desktops and servers, added to the fact that it has a multi-purpose nature, meaning that it can be used in many device.

Fig 1: A multi-purpose forensic operating system Scenario
Source: http://computer-forensics.sans.org/blog

2. RELATED LITERATURE

Threat modeling is a traditional practice in software security with rich literature and tools. In recent years, there have been efforts toward adopting threat modeling for security assessment of more complex targets other than a single application. Cyber-physical systems An abstract definition of security architecture defines it as a high level identification and description of components involved in providing system's security requirements. Security architecture frameworks has often been studied in the context of enterprise architecture

Fig 2: Security architecture frameworks
Source: https://www.nstec.com/cybersecurity

Investigation is presented, describing both the offline and online methods for the three main types of evidence that can be acquired, namely storage, RAM, and network traffic. Regardless of the platform in which the operating system is running, the approach to perform an online acquisition of the storage, RAM and Network information remains the same. In fact, the investigator should proceed, as they would do with any other operating system.

3. CONCLUSIONS

With a young population that is rapidly adopting new technologies, Africa is on the verge of an internet boom. To keep pace, Africa needs to urgently address efforts to combat cyber crime and improve its cyber security posture. The current cyber threat landscape in Africa shows that users are being impacted both by threats that are trending globally as well as some that more specific to the region. It will take a concerted effort from international governments, industry, and civil society to fight cyber crime and improve cyber security so that Africa can reach its full potential and stay on track to be a major driver of the global economy [7]

In this paper, we have addressed the issue of multi-purpose forensic operating system for digital forensic process and how the research community is dealing with the emergence of the insecurity with OS's with systems and devices that comprise it in order to develop solutions for conducting complete and efficient forensic investigations. In this regard, one of the approaches followed is the study of these systems and devices with the purpose of understanding what information they contain and how to extract it, thus providing investigators with guidelines on how to examine them.

4. RECOMMENDATION FOR POLICY AND PRACTICES

Policy and Procedure Development, the specialist must follow procedures and protocols as provided by the law enforcement agencies for the investigation. There must be detailed planning done which need to be followed by the specialist on every aspect so that the authenticity of investigation can be proved.

5. DIRECTION FOR FUTURE WORKS

The main problem after the investigation is to prove the evidence in the court of law. There is also a problem in regard to the collection of the evidence due to the rapid enhancement of technology. There must be an expert to present the opinion on how the information is used while investigation. The digital evidence is only admissible if it is proved that it is not tampered with, since it is most difficult as digital evidences can be tampered easily due to cybercrimes.

REFERENCES

[1] Koen, R. (2009). The development of an open-source forensics platform. Pretoria, South Africa: University of Pretoria.

[2] Garfinkel, S.L. (2010). Digital forensics research: The next 10 years. Digital Investigation, 7, 64-73

[3] Cohen, M.I., Bilby, D. & Caronni, G. (2011). Distributed forensics and incident response in the enterprise. Digital Investigation, 8, 101-110.

[4] Hibshi, H., Vidas, T. & Cranor, L. (2011). Usability of Forensics Tools: A User Study. Sixth International Conference on IT Security Incident Management and IT Forensics, conference publications (Page 81-91). Stuttgart, Germany: Institute of Electrical and Electronics Engineers.

[5] Federici, C. (2013). AlmaNebula: a computer forensics framework for the Cloud. Procedia Computer Science 19, 139 – 146.

[6] Garfinkel, S.L. (2009). Automating Disk Forensic Processing with SleuthKit, XML and Python. Fourth International Systematic Approaches to Digital Foren

[7] Cyber Crime & Cyber Security Trends In Africa. November, 2016 https://securitydelta.nl/media/com_hsd/report/135/document/Cyber-security-trends-report-Africa-en.pdf