OPEN ACCESS Freely available online

ISSN: 2090-2697
Journal of
Forensic Biomechanics

Short Communication

Examination of Current Systemic Forensic Framework Complications

Camacho Ricardo*

Department of Pediatric Clinics, University of São Paulo, Butanta, Brazil

DESCRIPTION

There are several investigation techniques that can be used to highlight vulnerabilities and security breaches, according to contemporary network forensics research. The majority of these investigation techniques rely on locating, catching, and analyzing traffic moving through network devices and infrastructure. When network security suspects are present, it is essential to decide the goal of the investigation [1]. The study identifies a number of investigative techniques, including responding to a particular network incident, analyzing archives in the case of an internal corporate investigation, and conducting a criminal investigation. These network investigations have a variety of goals and methods, but one thing they all have in common is the analysis of the traffic seen during network susceptibilities. These investigations are conducted in response to network attacks and clarify the effects of such attacks on networks. The investigation also examines the digital activities that take place after the alleged incident. It aids in analyzing the sequence of events that took place during the network attack. In order to reconstruct the entire attack, network forensics also entails capturing network traffic, which must then be transmitted to another device in order to be understood. However, because it involves sending a lot of data from one device to another, this process might cause forensics to take longer to complete [2].

Additionally, due to the appalling performance of network forensics, this process also has an impact on incident response. This means that network forensics must be performed more effectively, and network security must be increased. Acceptable evidence is essential in determining where the attack originated. Jeong and Lee suggested, for instance, extracting the router's traffic in order to gather the evidence [3]. This information can be used to locate the attack's starting point and potential intrusion. Regardless of the number of studies researchers have conducted on network forensic techniques, this study described the tools, process models, and implementation frameworks for network forensics. The researchers haven't yet looked into contemporary network forensic methods, particularly thorough network forensic methods for investigating cybercrime [4]. The implementation frameworks and intended datasets of the network forensic techniques were not highlighted by the scholars, according to the evidence that was also not found. While analyzing various types of network attacks, this particular study has been conducted with consideration for the variety of digital evidence and the challenges that result from that variety. Accessibility to the network artifacts and infrastructure is one of this study's primary goals, as is the gathering of evidence *via* the network against the intruder. Forensic methods to convey information about network attacks with the fewest false-negative outcomes. Setting these goals draws attention to the digital evidence, which shows that the attacker needed to spend more time and effort executing the attack. This study also aims to highlight the cutting-edge difficulties associated with using network forensic techniques. Because it could aid in the creation of uniform legal frameworks, this study is particularly important for the committees overseeing security agencies and legislators.

CONCLUSION

The importance of this study lies in its examination of network forensic techniques' fundamental architecture and how they function to determine the nature and consequences of network attacks. Based on a thorough literature review, this paper also proposes a thematic taxonomy for grouping network forensic techniques. While conducting forensic investigations, the classification was carried out based on the target datasets and implementation techniques.

A thematic taxonomy has been developed for this purpose using qualitative methods. On the basis of their objective functions, execution definition, investigation time, forensic processing, target instance, target dataset, mechanism, and framework characteristics, researchers have compared and contrasted various network forensic techniques. Finally, this study has covered the open research issues that may arise when deciding on a topic for additional network forensics research and choosing the most efficient methods.

REFERENCES

1. Paar C, Pelzl J. Understanding cryptography: a textbook for students and practitioners. 2009.

Correspondence to: Camacho Ricardo, Department of Pediatric Clinics, University of São Paulo, Butanta, Brazil, E-mail: Camachoric@gmail.com

Received: 02-Mar-2023, Manuscript No. JFB-23-20505; **Editor assigned:** 06-Mar-2023, PreQC No. JFB-23-20505 (PQ); **Reviewed:** 20-Mar-2023, QC No. JFB-23-20505; **Revised:** 27-Mar-2023, Manuscript No. JFB-23-20505 (R); **Published:** 03-Apr -2023, DOI: 10.35248/2090-2697.23.14.426

Citation: Ricardo C (2023) Examination of Current Systemic Forensic Framework Complications. J Forensic Biomech. 14:426.

2. Luckett WM. Cellular automata for dynamic S-boxes in cryptography. 2007.
3. Toorani M, Falahati A. A secure variant of the Hill cipher. 2009;313-316.
4. Qasem MH, Qatawneh M. Parallel hill cipher encryption algorithm. Int J Comput Appl.2018;179(19):16-24.
5. Huang N. An enhanced hill cipher and its application in software copy protection. J Netw. 2014;9(10):2582.