BOOK CHAPTER | *“Pseudo-Tractions”*

Net-Force for Email Tracing

Nana Kwame Kwakye
Digital Forensics & Cyber Security Graduate Programme
Department Of Information Systems & Innovations
Ghana Institute of Management & Public Administration
Greenhill, Accra, Ghana
E-mail: nana.kwakye@st.gimpa.edu.gh
Phone: +233244087207

ABSTRACT

Email is a widely used communication channel between businesses and individuals. Its importance has increased a lot nowadays, and the majority of the businesses prefer email as their primary communication medium to contact other businesses. Billions of emails are exchanged between businesses on a daily basis, and it is essential to note that most of them also contain spam or viruses. It is estimated that in Africa over 1 billion people use mail for their various communications. Malicious actors have also observed the lucrative advantages associated with mail communications on unsuspecting victims. They are able to reach masses and this has played a major role in the recent trend of romance scammers syndicate. The egregious impact of these cyber offenses offered the need to introduce tools to help investigate the mail communications and reveal actions of malicious actors in cyber space, this will also assist Africa in decreasing its cybercrime rate especially among home users with no or limited cyber safety knowledge. The legal implications of using NET-Force for email tracing to reveal actions of malicious actors will be assessed in this document.

Keywords: Cyber Offenses, Cybeyspace, Net-Force Suite, E-mails, legal implications, Africa

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

Citation: Nana Kwame Kwakye (2022): Net-Force for Email Tracing
Book Chapter Series on Research Nexus in IT, Law, Cyber Security & Forensics. Pp 273-278
www.isteams.net/ITlawbookchapter2022. dx.doi.org/10.22624/AIMS/CRP-BK3-P44

1. INTRODUCTION

E-mail tracer It is a product of Resource Center For Cyber Forensics (RCCF) established by govt. of India. NetForce suite is a Network Forensic Tool, collection of three tools named NeSA, CyberInvestigator and EmailTracer used for Network Forensics. NeSA is used for packet analysis, CyberInvestigator is used for log analysis and EmailTracer is used for email tracing has the functionality to fish out the location of the original email sender. In addition to showing just the location, it also shows the city, country, latitudes, longitude, and the ISP of the sender. It can also be used for retrieving emails and its details from mailbox files of local mail programs like Outlook Express(.dbx), .Microsoft Outlook(.pst), Eudora(.mbx), Pegasus(.cnm), The Bat(.tbb), Netscape Messenger(.nsm), Incredimail(.imm), KMail(MailDir), Mozilla(.mbox) and Windows7

Mail(.eml).This parameters being functions of the tools have legal implications, which this paper seeks to discuss and how it affects mitigating the action of malicious actor. [1], [2]

1.1 Background to the Study

Cybersecurity tools aid investigations immensely, they help to uncover evidence that support in adjudicating legal and organizational disputes. For this evidence to possess qualities of accuracy, authenticity and completeness, cybersecurity forensic experts adhere to adequate processes that include the use of cybersecurity tools such as NET –Force. The defined boundary in which the tool should be used versus maintaining evidential integrity of artefact retrieved informed this research.

2. RELATED LITERATURE

Evidence gathering process involved in digital forensic investigation has far-reaching effects. "Digital Evidence" [3] is a documentation that fulfils the necessities of "evidence" in a procedure; however it exists in electronic computerized structure. The process for reviewing or acquiring evidence is monotonous, digital evidence rest in minute spots on spinning platters, charged to more prominent or lesser degrees in to some degree non-volatile plan, however in any case, indiscernible with the exception of through numerous layers of reflection and document framework protocols. Digital evidence. In different cases, computerized verification of digital evidence might be charges held in unstable storage, [4] that disseminate inside seconds of lost energy to the framework. The volatile nature of digital evidence makes it necessary to use NETForce Email Tracer to store evidence to support forensic investigations.

Digital Evidence sources includes:

- Emails
- IM sessions
- Routinely keeps the access log.

3. RESEARCH GAPS/FINDINGS

Digital investigation has been defined as the use of scientifically derived and proven methods towards the identification, collection, preservation, validation, analysis, interpretation, and presentation of digital evidence derivative from digital sources to facilitate the reconstruction of events found to be criminal. [5] But these digital forensics investigation methods face some major challenges at the time of practical implementation. Digital investigations have challenges; however, for the purposes of this review, this paper will focus on resource challenges.

4. RESOURCE CHALLENGES

As the rate of crime increases, the number of data increases and the burden to analyze such huge data is also increased on a digital forensic expert because digital evidence is more sensitive as compared to physical evidence it can easily disappear. For making, the investigation process fast and useful forensic experts use various tools to check the authenticity of the data but dealing with these tools is also a challenge in itself. [6]

5. IMPLICATIONS FOR CYBER SAFETY IN AFRICA

Cyberattacks originated from African economies have a worldwide consequence. Gady (2010) has put it most strongly in his argument that Africa's "Cyber [weapon of mass destruction] WMD" potentially poses a direct threat to the world. For instance, in 2010, 80% PCs used in Africa were infected with viruses and malware (Gady, 2010). Cybercriminals often use these unprotected computers to launch cyberattacks against targets all over the world. More over some businesses from industrialized countries categorize online transactions originated from Africa as risky. However, some initiatives have been launched and carried out at various levels to improve the continent's cybersecurity landscape.

The most important of these is improving regulatory quality. According to a November 2016 report of the African Union Commission (AUC) and the cybersecurity firm Symantec, 11 countries in the continent had specific laws and provisions in place to deal with cybercrime and electronic evidence: Botswana, Cameroon, Côte d'Ivoire, Ghana, Mauritania, Mauritius, Nigeria, Senegal, Tanzania, Uganda and Zambia. Additional 12 countries had taken at least some legislative measures, albeit limited. Draft cybercrime laws had been prepared in many other countries and bills had already been presented to national Parliaments in some of the countries. There are also sector-specific regulations. For instance, banking and financial institutions are the most affected sector. In October 2018, the Bank of Ghana issued a Cyber Security Directive for Financial Institutions.

The Directive requires active involvement of senior executives and the board to strengthen cybersecurity. All banks in the country are required to appoint a Cyber and Information Security Officer (CISO) who would advise senior management and the board on cybersecurity issues, and also formulate adequate measures to manage cyber and information security risks. Cyber threat landscape needs increase investment in cybersecurity technologies, provide cybersecurity-related training to employees and appoint professionals such as CISOs. It is also important to create cybersecurity awareness among consumers. [9]

6. IMPLICATIONS FOR PRACTICE, RESEARCH AND POLICIES

Most African internet users are novice to acceptable cybersecurity measures while online, policy makers in the continent should focus on increasing public awareness of cybersecurity practices and strengthening regulatory and enforcement capabilities in this area. Regulations requiring strong cybersecurity measures in organizations need to be introduced and revised. Initiatives also need to focus on enhancing law enforcement capacities to increase certainty of punishment for those engaged in cybercrime activities. [10]

7. CONCLUSION

This paper brings an insight into the tool used to trace emails, the challenges that are confronting the email forensic investigations and acceptability of evidence. Using Net-force to trace emails, and analyzing digital evidence that ensures that the digital evidence is valid, accurate, and complete to assist anyone to make an informed decision. E-mail system is widely used and complex distributed internet application having several hardware or software components including services, protocols, server, and agents. Several threats are faced by user due to vulnerabilities present in the system.

So there is need to make it more secure by overcoming the current security flaws. Further, there is also need to adopt proactive forensics and to make systems to adopt forensic readiness. Similarly, lack of expertise in this field has further intensified the issues of inadmissibility of evidence as it impacts on due diligence and due process. Digital forensic investigation standards, tools and techniques may gather all digital evidence for admissibility. However, they may not be convincing to adjudicators until the evidence is authentic, accurate and complete following proper chain of custody and due diligence were applied. The challenges of maintaining authenticity in digital evidence gathering are more than just finding, collecting, and analyzing the data, generating a report and testifying in court. Further research is required in harmonising digital forensic investigations and the legal framework due to the advancing nature of organizational objectives, technological evolution and the evolving menace in the ecosystem.

8. RECOMMENDATION FOR POLICY AND PRACTICES

This is to provide clear policy, procedure, and guidance about operating the email forensics service based on industry standards and best practices. [7]

Evidence

From a legal perspective, evidence is used to describe items that are admitted into a court case by a judge. However, the term evidence is widely used in a much broader sense, this publication uses the less restrictive definition of evidence to include the media, and data collected and used during an email tracing investigation.

Roles and Responsibilities

All parties involved in a case must operate under the assumption that the evidence and case could come under legal scrutiny, which means everyone must always follow process, document any abnormalities from process, and preserve all evidence.

Collection and Handling

Before acquiring any evidence, the investigator should identify all the places information could be gathered from to provide answers to the questions presented in the investigation request. Individuals who have been properly trained in evidence handling will collect all physical evidence. Those with proper access will collect digital evidence to the relevant data and their methods for acquiring the data will be documented and provided to the investigator. [7]

Chain of Custody

The chain of custody will be completed for all cases involving physical evidence. The chain of custody shall be updated each time physical evidence moves between persons, is removed from storage, and/or replaced.

Law Enforcement

Handles all cases involving criminal activities.

Email Collection

All relevant emails should be exported and saved to the case file. Documentation of who exported the emails, how they did it, and who they were transferred to, as well as when and how they were transferred, and be documented to maintain integrity of the evidence.

Processes

The investigation process has four phases, which are, collection, examination, analysis, and then reporting. Pre-case activities occur during the creation of an incident and an investigation. The collection phase is where data related to the investigation request is identified, collected, and inventoried. Examination uses forensic tools to extract data. The analysis phase is where the results of examination are used to find answers to the questions that were asked in the request for investigation. Reporting is where results and methodology are described and then delivered. Finally, in the post case phase the case is reviewed and suggestions for changes to policy, procedure, or tools based on lessons learned during the case will be recorded and considered.

Pre-Case	1) Request submitted and received a. Identify reason for case 2) Approval of investigation 3) Case folder is created Collection
Collection	1) Appropriate sources of information for the case are identified 2) Chain of custody document is created if needed 3) Sources are acquired a. Physical b. b. Digital Examination
Examination	1) Searching for evidence Analysis
Analysis	1) Answer questions based on data found Reporting
Reporting	1) Write report Post Case
Post Case	1) Case Review 2) Lessons Learned

9. DIRECTION FOR FUTURE WORKS

As digital forensics regenerates to develop as a practice, so too will the best practices and standards that are presently accepted in the discipline. Technological trends such as “cloud computing” profess challenges to best practices to email tracing forensics since much of the data is located in an off-site location and cannot be extracted locally. This not only generates a mystery on the collection and validation phase, but it also professes legal challenges due to the nature in which the evidence would be apprehended (i.e. confiscating evidence from a remote server). In addition, the idea of internet data and “big data” also create impediment in setting boundary requirements because such data are large in volume, and may not be stored locally on a PC or device. [8]

REFERENCES

[1] Chhabra, G.S. and Bajwa, D.S., 2015. Review of e-mail system, security protocols and email forensics. International Journal of Computer Science & Communication Networks, 5(3), pp.201-211.

[2] Ho, W.C.C., 2010. E-mail forensics: tracing and mapping digital evidence from IP address (Doctoral dissertation, Auckland University of Technology).

[3] Quick, D., 2015. Digital forensic data and intelligence: Using data reduction to enable intelligence analysis. Journal of the Australian Institute of Professional Intelligence Officers, 23(2), pp.18-26.

[4] Venkataramanan, N. and Ravi, T.N., 2017. Proposing a Framework for Digital Network Forensic Evidence Accumulation in Cloud Environment. vol, 10, pp.2963-2972.

[5] Kruse II, W.G. and Heiser, J.G., 2001. Computer forensics: incident response essentials. Pearson Education.

[6] Vinh-Doyle, W.P., 2017. Appraising email (using digital forensics): techniques and challenges. Archives and Manuscripts, 45(1), pp.18-30.

[7] Shields, J., 2013. CWU Faculty Senate Minutes-05/29/13.

[8] Joshua L. Brunty., 2013. Best Practices for Digital Forensics.

[9] Kshetri, N., 2019. Cybercrime and cybersecurity in Africa. *Journal of Global Information Technology Management*, *22*(2), pp.77-81.

[10] Kabanda, S., Tanner, M. and Kent, C., 2018. Exploring SME cybersecurity practices in developing countries. *Journal of Organizational Computing and Electronic Commerce*, *28*(3), pp.269-282.