BOOK CHAPTER | Two Sides of a Coin

Analysing and Reconstructing Data for Forensic Inference and Conclusion

Rufus Larbi Okyere
Digital Forensics and Cyber Security Graduate Programme
Department of Information Systems & Innovations
Ghana Institute of Management & Public Administration
Greenhill, Accra, Ghana
E-mail: rokyere@yahoo.com
Phone: +233244378932

ABSTRACT

Forensic science is important in helping to Analyze and Reconstruct evidence gathered to come to a logical conclusion of an investigation. Crime is not always committed in a straightforward or easily decipherable manner. Nor is it always possible for the investigator to prove what they suspect occurred with the evidence left behind. Analyzing has to do with the piecing of data or evidence together and processed so as to enable the investigator get a fair idea of what one might be looking for. Reconstruction refers to the systematic process of piecing together evidence and information gathered during an investigation to gain a better understanding of what transpired between the victim and the offender during a crime.

Keywords: Africa, Cybercrimes, Cyber Security, Digital Forensics, Safety, Online

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

Citation: Rufus Larbi Okyere (2022): Analysing and Reconstructing Data for Forensic Inference and Conclusion SMART-IEEE-Creative Research Publications Book Chapter Series on Research Nexus in IT, Law, Cyber Security & Forensics. Pp 51-54. www.isteams.net/ITlawbookchapter2022. dx.doi.org/10.22624/AIMS/CRP-BK3-P8

1. INTRODUCTION

In Forensics, investigators are required to analyze suspected devices that come their way and come to a logical conclusion as to what data the suspected devices had and what the outcome was. These devices include mobile phones, computers and all other IT devices that are capable in connecting to a network. It also involves tracking and analyzing every data concerned. We know that every investigation when started has to come to an end. Its logical conclusion is important as that addresses all findings made in the investigation. Before any investigation can take place, data has to be analyzed to make the investigator more informed as to what target area to concentrate in the course of investigation. Before data can be analyzed, the devices supposedly used has to be retrieved and examined before they can be reconstructed to get to

the final conclusion. Time and time again, we trumpet the incredible value of advanced data analytics in forensic investigations – often, it is the key to finding the needle in the haystack.
To utilise the significant potential of trace material for robust forensic reconstructions, it is important to also incorporate an understanding of the role of human decision-making in any inferences and conclusions drawn from the detection, identification and analysis of trace materials. Human decision-making can be identified at each stage of the forensic process, for example identifying where to search at a crime scene, deciding the best strategy for evidence analysis in the laboratory, ascertaining the important factors integral to interpreting what the evidence means in a particular case, and assessing the means of presenting those findings to investigators as intelligence or to the court as evidence.

As such, human decision-making is a fundamental part of any forensic reconstruction and this must be understood in a way that incorporates the different components that make up 'expertise' (skills, experience, routines, and technical knowledge [24]). Whilst automated systems can be built and trained to identify specific components or accurately measure the composition of a material, the role of the expert is integral to the reconstruction approach.

1.1 Background to the study

This is to give us the insight of how data is analyzed and reconstructed in the course of the investigation. Since crime has evolved over time, criminals tend to become more sophisticated in hiding their activities. The use of mobile phones and other IT related equipment's are being upgraded daily and this makes it a perfect hiding place for crime. We need to understand the processes of how data is manipulated through mobile devices and other equipment.

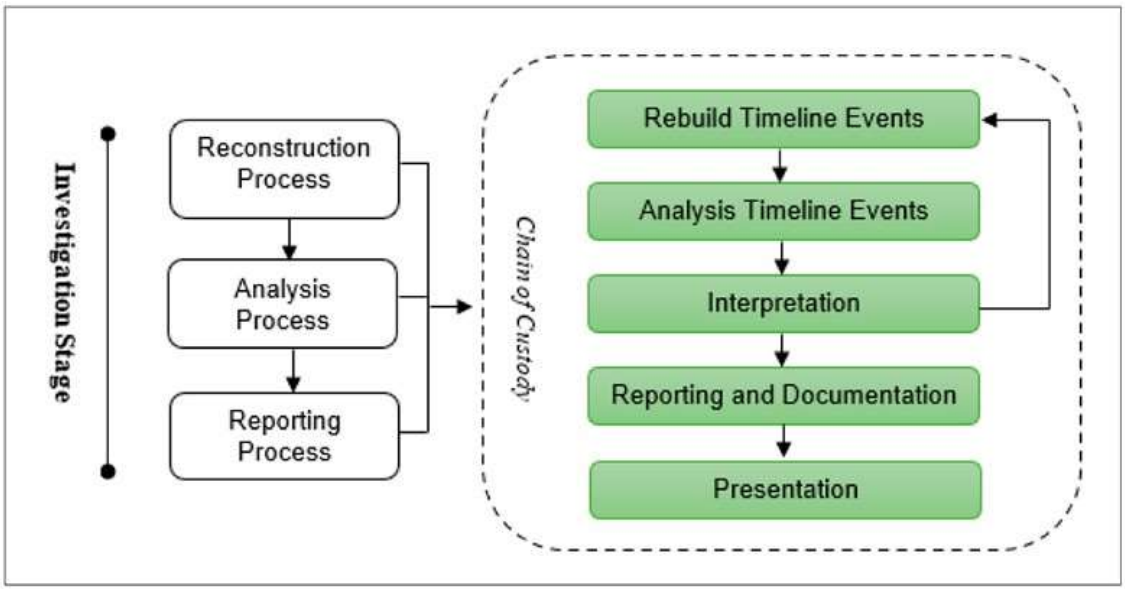

Fig 1: Framework for Analyzing And Reconstructing Data And Its Conclusion For Forensics

A core tenet of this process is that, when they commit a crime, criminals leave an imprint of themselves at the scene. The study is to bring to the fore the series of events that take place at certain times by the criminals and these have to be put together to enable the investigator to

understand and know what transactions, routes that were used and as well as understand the motive of the criminal in perpetuating the crime.
After all these have been achieved the investigator has to finally bring closure to the investigation. These might be in the form of recommendations, being able to know the true nature of the crime committed.

2. RELATED LITERATURE

The article by John Ahearne (2021) titled Digital Forensic Process—Analysis - delves into each step of the digital forensic process and opined that Forensic digital analysis is the in-depth analysis and examination of electronically stored information with the purpose of identifying information that may support or contest matters in a civil or criminal investigation in a court proceeding

3. RESEARCH GAPS/FINDINGS

In the analysis phase, examiners connect all the dots and paint a complete picture for the requester. For every item on the Relevant Data List, examiners answer questions like who, what, when, where, and how. They try to explain which user or application created, edited, received, or sent each item, and how it originally came into existence. Examiners also explain where they found it. Most importantly, they explain why all this information is significant and what it means to the case.

4. RECOMMENDATION FOR POLICY AND PRACTICES

4.1 Implications for Practice, Research, Policies & Cyber Safety In Africa

Africa has been among the fastest growing regions in terms of cybercrime activities. The continent is also a source of significant cyberattacks targeting the rest of the world. However, a number of measures have been taken to address cyber-threats and improve cybersecurity in the continent. Many countries in the continent have developed legislation to fight cyber-threats. They have also strengthened enforcement measures. Private sector efforts have also been undertaken to strengthen cybersecurity.

According to a survey carried out by the African Union Commission (AUC) in 2018[2], out of the 54 African states, only 8 countries have a national strategy on cybersecurity. The situation has improved since then though. In a recent study I've completed but yet to be published titled "Cybersecurity Strategies in Africa – The Need for a Regional Approach to Support the Vision of the African Continental Free Trade Area", I found that 13 African countries have now published their national cybersecurity strategies with 1 still in draft..

The 2018 AUC survey report also found that only 13 states have a Computer Emergency Response Team (CERT) or Computer Security Incident Response Teams (CSIRTs), 14 with personal data protection laws, and only 11 with cybercrime laws[2]. A similar report by Deloitte [3] expresses similar concerns Money stolen via cyber-attacks drives the financial sector to mitigate the risk of falling victim to cybercrime. They already spend hundreds of millions of dollars and hire the brightest minds to protect their customers and themselves. However, cybercrime continues to rise, and the methods cybercriminals use to attack the infrastructure of financial institutions constantly evolves.

Recommendation for cyber safety for Africa are as follows

1. Education. This must be carried out in most schools and media across Africa to educate both students and the citizens.
2. Training. Security Services must be trained on Cyber Security so as to enable them track and arrest culprits involved.
3. Cyber Security policies, legislations, practices and regulations must be implemented and brought into law.

4.2 Implications for Policy, Practice and Research

For cyber security policies, practices and research to be concrete as mentioned above we need to have these documents passed into law by the Government. This will then enhance the security to be fully involved with the curbing down of the rate of crimes within the nations. Cybersecurity policies are important because cyberattacks and data breaches are potentially costly and the weak links are those who have no idea of what they do on the websites. Encouragement must be given for further research to be done to help in the fight of cybercrime.

Direction for Future Works

Future works should take into consideration both the Analysis and Conclusion of the findings in terms of the investigation and also give us an example of a case and how it was solved. The example could be referenced to a site or an uploaded case for which we can watch and review the case to support the article.

REFERENCES

1. Amel Ali Alhussan , Arafat Al-Dhaqm , Wael M. S. Yafooz , Abdel-Hamid M. Emara, Shukor Bin Abd Razak and Doaa Sami Khafaga (2022); A Unified Forensic Model Applicable to the Database Forensics Field. *Electronics 2022, 11(9), 1347; https://doi.org/10.3390/electronics11091347*
2. de Eoghan Casey (2011): Investigative Reconstruction with Digital Evidence. Digital Evidence and Computer Crime, Third Edition. https://www.amazon.com/Digital-Evidence-Computer-Crime-Computers/dp/0123742684
3. John Ahearne (2017): Forensic Analysis. https://drivesaversdatarecovery.com/digital-forensic-process-presentation/
4. Lindsay Gill (2018): The power (and variety) of data in forensic investigations. https://www.forensicstrategic.com/the-power-and-variety-of-data-in-forensic-investigations/
5. Morgan, R.M. (2019): Conceptualising forensic science and forensic reconstruction. Part I: A conceptual model. Sci Justice. 2017 Nov;57(6):455-459. doi: 10.1016/j.scijus.2017.06.002. Epub 2017 Jun 10.
6. Kshetri, Nir (2019). “Cybercrime and Cybersecurity in Africa,” Journal of Global Information Technology Management. DOI: 10.1080/1097198X.2019.1603527Tomslin Samme-Nazir (2020): Cyberspace security in Africa-where do we stand by August 18, 2020