**Digital Forensics Research Proposal**

Nicholas Hoats

South University

Course ID: ITS4000

Dr. Terry House

10/21/2024

**Digital Forensics Research Proposal**

**Introduction – Statement of Purpose**

As digital technology has evolved, the benefits and risks to society have only increased. It has gone on to revolutionize the way we communicate, store data and conduct commerce but it also meant that cybercrime became a very real threat! With increasing digital footprints and connected pervasive system getting more widespread, it is fundamental to adopt strong forensic methods for identification, analysis as well as eradication of cybercrime. This study seeks to examine the current trend, opportunities and challenges available in digital forensics with a focus on recent solutions that involve emerging tools, methods and techniques applied for combating cybercrime, for example cloud computing forensic analysis system; smart environment backed up by fundamental technologies. The research could help to develop new frameworks for investigators that not only meet the growing complexity of cyberattacks, but also ensure validity and efficiency in terms of obtaining digital evidence as well as conducting analyses.

**Research Questions and Hypotheses**

Research Question 1: What are the technologies, tools and current methodologies delivering significant capabilities in digital forensics to effectively address these cybercrime challenges within cloud computing environments?

Research Question 2: What is the extent of hybridization among digital forensics, and machine learning in regard to improving forensic investigation efficiency and quality?

Hypothesis 1: Cloud forensics complexity requires tools & procedures beyond current digital forensic methods to achieve accurate data capture and evidence preservation.

Hypothesis 2: The integration of machine learning within digital forensics indeed has enhanced the speed and accuracy in making them more effective primarily with respect to data-rich scenarios such as smart cities or IoT network.

**Literature Review**

With the increasing use of digital devices, there also comes a rise in the data generation. A new gold rush has beleaguered the world of cyber forensics, where experts are running at an almost impossible pace to prize nuggets from a deluge of fresh streams. This problem is exacerbated with the advancements in encryption, cloud computing and increased number of IP connected devices (i.e., IoT). These difficulties become increased barriers for investigators not only in securing the evidence, but also being able to timely return definitive results. These are the challenges that discussed literature aimed to target mainly new approaches and tools in terms of digital forensic automation, machine learning methodologies use cases as well as their implementation into cloud forensics.

The research is concentrated on improved digital forensic investigations making sure law enforcement agencies remain a step ahead of cybercriminals. While the advancement in technologies and digital systems open doors for cybercriminals to perpetrate such activities, it equally implies they are leaving behind traces as well; hence Digital Forensics department must advance its methods accordingly in order to trace these circumstances correctly. The main themes of the existing literature includes, automation and machine learning enabled digital forensic workflows, cloud forensics challenges and solutions, also it stresses on building new set of forensic tools specifically for IoT environment. The primary aim of the always-evolving research landscape is to enhance efficiency, precision and consistency in digital forensic investigation with cloud services taking over more than half of the market share.

Since digital forensics is an interdisciplinary field, there are many types of research methodologies employed in this review. For example, Beebe and Clark used a hierarchical template for digital investigations that offered a good discipline when conducting forensic analysis. This framework was intended to enhance the granularity of investigations, by enabling forensic examiners link front end evidence collection and back-end data analysis in a cohesive way (Beebe & Clark, 2005). On the other hand, Garfinkel suggested that digital forensics should take a modular and standardized approach due to scaling forensic tools (Garfinkel, 2010).

Many of the research methodologies that a literature review examined, automation and machine learning are also major aspects played. James and Gladyshev, for instance, looked into how automated forensic tools could help investigators dealing with this unprecedented proliferation of digital evidence to simultaneously retain human involvement in the interpretation-intensive complex cases by adopting a socio-technical perspective (James & Gladyshev, 2013). On the contrary, Kazaure took a descriptive approach as well and examined how efficient contemporary forensic applications assist in gathering data from computers along with smart phones by using traditional research practices (Kazaure, Yusoff, & Jantan, 2023).

The analyzed literature contains many results relevant to the digital forensic field. A hierarchical investigative framework was developed by Beebe and Clark that has been extensively adopted in forensic investigations, providing a structured approach to the collection of evidence having regard for evidential phases. This model is particularly useful for associating digital evidence with individual crimes or criminal operations, and therefore increasing the overall quality of forensic investigations (Beebe & Clark, 2005).

Casey Eoghan also described many of the traditional digital forensic methods used in criminal investigations, a must-read to acquire basic intelligence on how computer networks can be instruments of crime and evidence. This book continues to be a foundational piece of material in the field of digital forensics and specifically directed toward those as an introduction or starting point for new forensic investigators (Eoghan, 2004).

In 2010, Garfinkel predicted a coming crisis in digital forensics due to the increasing data and encryption, where it would be impossible or at least greatly difficult that all applicable forensic tools are available for every case. These newer works are also looking at producing international forensic tools and systems for flexible, adaptable capabilities to cope with an increasing amount of digital evidence (Garfinkel, 2010).

James and Gladyshev explored the incorporation of automation within forensic investigations, acknowledging the issues related to automating certain processes versus those which required expert human interpretation. The research findings indicate that automation could indeed greatly speed up parts of the forensic process but will not entirely replace expert knowledge needed to analyze complicated cases (James & Gladyshev, 2013).

According to Sibiya, Venter & Fogwill, cloud forensics have a number of specific challenges and traditional forensic tools in methodologies do not adequately cover the methodology for detecting evidence when an incident happens within Cloud environments. Their paper underlines the requirement for forensic tools in the cloud that protect data integrity and ensure a reliable chain of custody (Sibiya, Venter, & Fogwill, 2015).

The majority of the twelve articles identified are obviously reports on research studies, with empirical evidence and comprehensive analyses that raise theoretical and many practical implications for digital forensics. For instance, Kazaure et al. demonstrates comprehensive research conducted in digital evidence extraction and other forensic tools specifically preserving the integrity of evidences that is crucial for chain of custody on forensic investigations (Kazaure, Yusoff, & Jantan, 2023).

But not all of those articles were traditional research studies. For instance, James and Gladyshev offer a theoretical perspective on how automation should be used in digital forensics based upon their prior research as opposed to providing new empirical data (James & Gladyshev, 2013). Casey Eoghan also falls into this category by creating a summary of the existing forensic techniques, based on past research and without any new data or studies (Eoghan, 2004).

In summary, most of the articles examined are supported by empirical research that can be used to derive theoretical knowledge and a toolbox for advancing this field. Despite its limitations, the theoretical works incorporated in this review do however offer meaningful terminologies for subsequent studies and designing interventions.

**Conclusion**

The literature reviewed has underlined the increased difficulties that are faced by digital forensic investigators in an age when cybercrime is on a rapid rise. Cybercriminals continue to leverage new technologies; therefore, the field of digital forensics must continually evolve in light of increasing data volumes and more importantly, cloud systems & IoT devices. Fortunately, much research has been conducted in developing tools and frameworks to deal with these challenges, but gaps still exist (e.g., automation, integrating machine learning for cloud forensics or even forensic clouds). Solving these challenges will require future research ensuring that digital forensics continues to provide vital support in the battle against cybercrime.

Based on the findings of this literature review, a follow-up study is desired to investigate how machine learning can be employed in smart environment data and volume heterogeneity might meaningfully accelerate digital forensic investigations. The research should address the development and testing of machine learning models that can automatically categorize, filter and triage digital evidence so forensic analysts may concentrate on selecting relevant evidentiary artifacts for more detailed analysis. In addition, the study could refer to a creation of a scale or framework for integrating cloud forensics into existing digital forensic practices due to constraints inherent in data sovereignty and sharing arrangements.

# References

Beebe, N., & Clark, J. (2005). A hierarchical, objectives-based framework for the digital investigations process. *Digital Investigation, 2*, 147-167.

Eoghan, C. (2004). *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet.* Academic Press.

Garfinkel, S. L. (2010). Digital forensics research: The next 10 years. *Digital Investigation*, S64-S73.

Jacome-Castilla, N., & Villamizar-Nunez, C. (2019). Computer technique for the suitability of digital evidence in attacking an information system: Forensic analysis for the digital custody chain. *Journal of Physics, 1388*, 12027.

James, J., & Gladyshev, P. (2013). Challenges with Automation in Digital Forensic Investigations. *arXiv.org*.

Kazaure, A., Yusoff, M., & Jantan, A. (2023). Digital Forensics Investigation Approaches in Mitigating Cybercrimes: A Review. *Journal of Information Science Theory and Practice*, 14-39.

Kent, K., Chevalier, S., Grance , T., & Dang, H. (n.d.). *Guide to Integrating Forensic Techniques into Incident Response*. Retrieved from NIST: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf

Ligh, M., Adair, S., Hartstein, B., & Richard, M. (2010). *Malware Analyst's Cookbook and DVD: Tools and Techniques for Fighting Malicious Code.* Newark: Wiley.

Lillis, D., Becker, B., O'Sullivan, T., & Scanlon, M. (2016). Current Challenges and Future Research Areas for Digital Forensic Investigation. *ProQuest Central*, 57-75.

Quick, D., & Choo, K.-K. (2014). Data reduction and data mining framework for digital forensic evidence : storage, intelligence, review and archive. *Trends and issues in crime and criminal justice*, pp. 1-11.

Sibiya, G., Venter, H., & Fogwill, T. (2015). Digital Forensics in the Cloud: The State of the Art. *IST-Africa 2015* (pp. 1-9). Research Space.

Tageldin, L., & Venter, H. (2023). Machine-Learning Forensics: State of the Art in the Use of Machine-Learning Techniques for Digital Forensic Investigations within Smart Environments. *Applied Sciences, 13*, p. 10169.