Creative Research Publishers
https://www.crossref.org/06members/50go-live.html

Journal of Behavioral Informatics
Digital Humanities & Development Research
Vol 8, No 4, December 2022 Series

Towards A Human-Centered Framework for Evidence Gathering in Cybercrime Investigation – A Research Agenda

[1]Baafi Benjamin, Longe Olumimide Babatope (PhD) & Joseph Budu (PhD)
Department Of Information Systems and Innovation
Master Of Science in Digital Forensics and Cybersecurity
Ghana Institute of Management and Public Administration
[1]E-mail: benjaminbaafi@ymail.com
[1]Phone: +2330244058435

ABSTRACT

While the global economy is expanding quickly, the Internet is developing at a diametrically opposed pace, resulting in entirely new surroundings where conventional criminal activity have been given a new platform to thrive. The integration of computers and the development of communication technologies has also altered social interactions making more people vulnerable in an online environment that is rife with a sizeable number of and criminally intentioned personalities. Techniques for mitigating criminal activities are among others are Law, Education/Enlightenment and Technical deterrence. Today law enforcement is faced with the herculean task of identifying faceless criminals online and digital evidence gathering is part of the first line of arrest and prosecution. This paper sets out to research agenda for the development of a Human-Centered Framework for evidence gathering in cybercrime investigation. We captured the research objectives, related works, rationale for the research, chllanges to forensics and digitl evidence, research problems and set directions for the research

Keywords: Human-Centered Framework, Evidence, cybercrime investigation, Criminals, Research Victimization, Deterrence

Journal Reference Format:
Benjamin Baafi & SUPERVISORS: **Professor Longe Olumimide Babatope, Dr. Joseph Budu (**2022): Towards A Human-Centered Framework for evidence gathering in cybercrime investigation – A Research Agenda. Journal of Behavioural Informatics, Digital Humanities and Development Research. Vol 8, No 4, Pp 61-75.
Available online at https://www.isteams.net/behavioralinformaticsjournal. dx.doi.org/10.22624/AIMS/BHI/V8N4P7

1. BACKGROUND TO THE STUDY

The internet may be thought of as a distinct dimension of civilization that is devoid of legal restrictions and was created to operate independently from all other infrastructures in times of emergency. In modern times, the internet is used for more than just communication; it also makes it possible to handle public services efficiently and accurately, to grow businesses, and to protect national security (Pollitt, Casey, Jaquet-Chiffelle, & Gladyshev, 2018). There is a huge need for technologically sophisticated answers to the problems confronting modern society, yet legal protection on the internet is still mostly in its infancy.

Cyberspace's international nature and a lack of legal security provide an atmosphere where illegal activity may go unnoticed by using encryption or other techniques to protect anonymity (Arpita Singh, 2022). Despite the mysticism surrounding the crime, digital traces are often left behind that may be discovered and utilized as proof in court. Developing investigative tactics, forming task groups, and tracking down digital evidence are some of the measures employed to combat cybercrimes (Katos & Bednar, 2008). But among other things, legislative restrictions on personal integrity and legal ambiguity sometimes impede attempts to combat cybercrime. When obtaining digital evidence in a foreign country is necessary for a case, for example, the need for dual criminalization might be problematic since it is illegal to do so unless both countries have criminalized cybercrime (Okutan & Çebi, 2019). The issue of jurisdiction and legal application in the digital domain is another significant challenge. Given the global extent and complexity of cybercrimes, it is crucial to have efficient means of gathering digital evidence without violating people's rights to privacy (Okutan & Çebi, 2019).

Cybercrimes are a common occurrence nowadays, however, because of a weak investigative procedure and lack of follow-up in supplying digital evidence, the case suffers. Unfortunately, there is not enough information available on how to conduct a digital evidence-based investigation or what constitutes a computer-related crime. Most poor nations lack comprehensive guidelines and frameworks for computer forensic investigators and analysts owing to a lack of advanced technology, experienced labor, and limited financial resources. In order to avoid the nexus of cybercrime, an appropriate framework for delinquency investigation based on digital evidence is required (Subair, Yosif, Ahmed, & Thron, 2022).

Users may now decide who can access, manage, and receive their data, giving them complete control over it. People's lifestyles are changing as a result of technology advancements. For instance, most people now choose online payment over traditional payment methods, social media access, phone or video chat medical consultations, online schooling, and other services. The number of internet users rises as a result of new services being available and technological advancements, and the exponential increase of information encourages its misuse and abuse, which culminates in cyberattacks and cybercrime. Cyberattacks have an impact on the economic systems of our country. According to (Subair et al., 2022) study, India loses over 24,630 crores a year to cybercrime. Technical advancements have made assaults more sophisticated, making it more difficult to defend oneself by just installing anti-virus software.

Although the original investigation process could have altered, the essential idea of evidence preservation in the chain of custody has not. The preparation, inspection, identification, collection, analysis, validation, acquisition, documentation, and forensic reporting of digital evidence in a court of law are all parts of the digital forensics investigative process (Mensah, 2019). A crucial part of digital forensic investigation is the technique of analysing and taking pictures of digital evidence from various electronic devices utilizing methods that are both scientifically sound and well-established. A rapidly growing field called "digital forensics" uses a variety of analytical tools and computer research methods to find relevant legal evidence and recommendations (Ennin & Mensah, 2019).

Digital forensics, in general, is a process that involves retrieving data about an incident that has been reported, as well as properly processing that data so that experts can gather all pertinent hints and evidence, which can then be used to advance your legal interests against someone or in any other circumstance.

Gathering evidence, keeping it, accurately documenting it, and presenting it in court are all steps in the digital forensic process (Subair et al., 2022). However, since this is not a straightforward procedure, it may take years to resolve the problem. Furthermore, sophisticated systems make it more difficult to strike these days. We now have a complicated approach, as well as improved tools and methodologies, to establish whether or not evidence is there. In order to determine if a criminal case has occurred, we now use a complicated methodology, new technology, and processes, and considerable sums of money are used to solve the case (Horan & Saiedian, 2021).

Cyber-attacks and cybercrime are major concerns for big nations such as the United States and the United Kingdom, which have created a variety of security measures to fight them. Every country is attempting to safeguard and adapt to cyberspace security. Countries must prioritize the security of key infrastructure. In the year 2020, data stolen from Airbus Company's computer system was offered for sale on the dark web. Many municipalities have declared emergencies due to the theft of millions of people's medical records. (Mensah, 2019). With each passing day, the workforce's capacity to resist cyber-attacks dwindles, prompting the hunt for new solutions.

Researchers are employing machine learning algorithms to detect blackouts brought on by cyberattacks and to lessen the impact of assaults on the Internet of Things. Other applications include the detection of spam and network attacks, the identification of phishing attempts against financial institutions, and the detection of the rising number of sexual crimes committed through social media. Numerous businesses have made use of such systems for tasks like stock forecasting, risk mapping, and customer profiling in the realm of cyber security. Areas of use include crime trend and pattern prediction, criminal identity detection, and crime prevention (Ennin & Mensah, 2019).

When a security incident happens, many businesses lack the necessary criteria to perform a forensic investigation, which often prevents the investigation from being successful (Bouchaud, Grimaud, & Vantroys, 2018). Forensic investigations are not often given top priority by organizations. The main goal of computer forensics is to preserve, gather, and present evidence. The ability of the organization to look into every abuse case and bring the abuser to justice depends on the preservation of all relevant evidence (Elavarasi & Elango, 2017). It is crucial to identify the incident's cause and the perpetrator.

Many companies struggle to conduct an effective forensic investigation after a security incident because they lack the requisite criteria (Bouchaud et al., 2018). However, forensic investigations seldom get top attention from businesses. One of the primary functions of computer forensics is the collection, analysis, and presentation of evidence. If all documentation relating to allegations of abuse is lost, the organization will be unable to investigate these claims or bring the perpetrators to justice (Elavarasi & Elango, 2017) In the military and aviation industries, computer forensics is well-established. One use is the recovery and examination of flight data from an aircraft's "black box" after an accident.

Digital forensics (DF), as described by the two guiding principles, is a more expansive field than computer forensics:

- Computer forensics is the use of analytical and investigative techniques to locate, get, examine, and preserve information or evidence that is magnetically stored or encoded (Louwrens & von Solms, 2005).
- Digital forensics (DF) is the scientific theory of the procedures used to retrieve, preserve, and examine digital evidence, including audio, picture, and communication devices (TC-11, 2006).

2. GLOBAL COMPUTER FORENSICS ENVIRONMENT

In recent years, digital forensics has emerged as a critical tool for government and private sector security agencies. Digital forensics may seem like a brand-new field, but it really has a lengthy history, as Pollitt explains. Prehistory, infancy (1985–1995), childhood (1995–2005), adolescence (2005–2010), adolescence (2005–2010), and ultimately the future, where he forecasts the entrance of strong tools, software, instructors, certificates, and legal frameworks. In the early 1980s, the United States pioneered the discipline of digital forensics, with several nations following and embracing this unique approach to a criminal investigation. However, not all nations have the same degree of competence and resources when it comes to digital forensics. The G8 nations (France, Germany, Italy, the UK, Japan, the US, Canada, and Russia) are digital forensics leaders due to their superior resources (human and otherwise) and infrastructure.

South Africa is rising on the African digital forensics landscape, but practitioners, like in other poor nations, lack training, competence, and expertise to review and interpret evidence. Important international bodies directing the worldwide growth of digital forensics include the International Criminal Police Organization (INTERPOL), the International Organization on Computer Evidence (IOCE), and the International Association of Computer Investigative Specialists (IACIS). The lack of a universally accepted and legally binding definition of what constitutes cybercrime is the primary obstacle to a thorough understanding of the phenomenon (Baror, Venter, & Adeyemi, 2020) . Attempting to define cybercrime introduces conceptual complexity and a wealth of knowledge. It's hard to pin down exactly what it is, yet it goes by many names: cybercrime, cybercrime, cybercrime, cybercrime, cybercrime, cybercrime, cybercrime, cybercrime, cybercrime, cybercrime, cybercrime, cybercrime, cybercrime, cybercrime, cybercrime. Cybercrime might conceivably contain a broad variety of illegal actions, and it seems that researchers, authors, and law enforcement organizations prefer to describe the many parts that comprise cyber-crime rather than define the word (Horan & Saiedian, 2021).

"Unlawful activity in which the computer serves as either a tool or a target, or both," as defined by Suman, Srivastava, and Pandit (Horan & Saiedian, 2021). One scenario is a computer becoming the object of criminal activity due to the theft of hardware or software. When computers are used for illegal activities such as theft, extortion, or the distribution of pornographic material to minors, or when they are infected with malicious software, they may become victims of crime. According to (Okutan & Çebi, 2019), cybercrime is be refers as an act of theft through the use of digital device such as computer.

Usually identified in two categories: Computer age cybercrimes such as hacking, sniffing. Phishing and viruses' injection; and Ancient crime strategies which as a result of involvement of computer has now gained stronger domain such as scam, theft etc.

Cyber Law Regulation in Ghana

The government of Ghana, acting via the Ministry of Communications, has passed laws to regulate citizens' actions in cyberspace in response to the growing threat posed by cybercrime. Act 772 of 2008 pertaining to electronic transactions; Act 771 establishing the National Information Technology Agency; Act 843 of 2012 pertaining to data protection; and other relevant provisions of the Criminal Offences Act, Act 29 of 1960. The parts will provide hints as to the intentions and scope of these laws.

Electronic Transactions Act (ETA), 2008 (Act 772)

In December 2008, the Parliament of Ghana passed and the President of Ghana signed into law the Electronic Transaction Bill. The primary objective of the ETA is to protect the cyber environment in an effort to lower the frequency of criminal activity, which may harm locals' ability to generate economic value. Twelve sections comprise the Act. You may find instances of them everywhere from online shopping to government services to the Domain Name System to court appeals to certification bodies. The industry forum, service provider and intermediary liability, cyber inspectors' roles, cybercrimes, and other matters are also addressed.

The Act allows security agencies to seize a computer, electronic record, program, information document, or thing during the execution of court warrants if they have probable cause to believe that an offense has been or is about to be committed, as detailed in the tenth set of provisions (which deals with law enforcement) (ETA 2008, Act 772, clause 98). When requested by law enforcement, suppliers of wire or electronic communication services or remote computer services must keep some data secure until a court order is issued (ETA 2008, Act 772, clause 100). If the contents of an electronic communication are relevant to an investigation concerning matters of national security, the courts may order an electronic communication service provider to disclose the contents of such communication while it is in transit, while it is being held, maintained, or while it has been stored electronically in an electronic communications system (ETA 2008, Act 772, clause 101). Nonetheless, article 142 (2) establishes jurisdictional limits on the Act's reach:

That this Act applies if, for the offense at hand:

a. The defendant was in the nation at the crucial moment;
b. the computer, electronic record, or electronic payment device was created, located, or maintained in the nation at issue; and
c. A local banking institution issued the electronic payment method.
d. Regardless of whether paragraphs (a), (b), or (c) apply, the crime was committed inside the country, on a ship or aircraft with a Ghanaian registration, or on a trip or flight to or from this country at the time the offense was committed.

Traditionally, legal jurisdiction encompasses territory, with the extent of a nation determined by its borders. To punish cybercriminals, this geographical concept is useless. Because the attackers and victims may be in various countries, determining where cybercrime is done may be challenging. Offenders may even use computer systems from other nations to assault their victims. Another flaw in the Act is that, unlike the drug trafficking statute, penalty is not explicitly established, allowing judges to use their discretion to make decisions on cyber offenses. For example, Section 2(2) of the Narcotics Drugs Act (P. N. D. C. L 236) stipulates that " If convicted, a person facing charges related to illegal drugs faces a mandatory minimum term of ten years in jail." Furthermore, unlike the Drugs Law, Sections 11 to 14, which mandated that assets obtained by drug smugglers must be taken, properties obtained by con artists via illegal means are not subject to forfeiture or seizure. Obviously, this legislation gives the criminal a way out since the severity of the sentence does not correspond to the nature of the cybercrime.

According to the Ministry of Communications' final draft report on Cyber Security Policy (2014), "while the ETA has measures for law agencies to combat cyberattacks, this is insufficient since it does not take into account the multi stakeholder's approach to cyber security problems. " (Ministry of Communication final draft on Cyber Security in Ghana, 2014:). It has been more than 10 years since the Act was passed, and the National Cyber Security Advisor has just emphasized that certain gaps should be addressed to better position the country to deal with the increasing incidences of cybercrime (Daily Graphic, 5/12/18, page 45).

The Ghanaian Cybersecurity Act, 2020 (Act 1038), establishes the Cyber Security Authority (CSA) to regulate cybersecurity activities, and empowers it to investigate cyber incidents and cybercrime, including providing technical support to law enforcement for prosecution. Here's a more detailed overview of the Act's provisions relating to investigation: The 2020 Cybersecurity Act is a 67-page document enacted on 29 December 2020 to establish the Cyber Security Authority, regulate cybersecurity activities in the country, promote the development of cybersecurity in the country, and provide for related matters. The Act, divided into 100 sections split across 17 parts, has 3 schedules dedicated to an explanation of the Cyber Security Services, a table of administrative penalties, and the oath of secrecy.

3. COMPUTER & CYBER FORENSICS IN GHANA

The needs for forensics investigations, the law bindings investigation domain, the growth in cybercrime, and certain regulations and actions the made by the government to encourage digital investigations are explored in earlier studies concerning computer forensics in Ghana. These pieces of literature regarding forensics in Ghana are listed below. The evolution of forensic science in Ghana from the establishment of the Ghana Police Service in 1894 is explored in the journal article History of forensic science in Ghana by Amankwah. It looks at how Ghana's forensic science has developed, which has been heavily influenced by biology and chemistry and makes a suggestion on the need for digital forensics in the modern world. In their study Awareness and Understanding of Computer Forensics in the Ghana Legal System, Michael Adjei Frempong & Kamal examined that forensics investigation is necessary, particularly in the court in Ghana.

This literature investigates Ghana's legal system, the acceptance of electronic evidence in court utilizing digital forensics, and judges' ignorance of digital forensics. The study investigating the use of digital forensics in courts of law included twenty judges. It was discovered that the majority of judges are not familiar with digital forensics, which made it difficult for judges to comprehend digital evidence. Cyber Crime and Criminality in Ghana analyzes the growth of cybercrime in Ghana by looking at data from the Ghana Police Service and the criminal investigation department there. What kind of cybercrimes are prevalent in Ghana? These are the two main issues that were addressed in the study.

What steps is Ghana doing to combat alleged cybercrime? It also discusses how the Ghana Police Service lacks the knowledge necessary to obtain digital evidence, which leads to incomplete or fruitless investigations. Daniel Enin's work, Cybercrime in Ghana: A Study of Criminals, Victims, and the Law, takes the conversation about cybercrime a step further by examining victims' interactions with offenders and law enforcement. According to his study, criminals now feel more confident in their ability to commit crimes since there is a lack of trust in the criminal justice system. In their subsequent study Computer & Cyber Forensics: A Case Study of Ghana, Mohammed & Adjei focused on several technological considerations of cybercrime in Ghana. The report highlights the significance of computer and cyber forensics research in the battle against cybercrime while highlighting particular technologies, like VPN, that are used by cybercriminals to conceal their identities online.

The use of computers has permeated every aspect of contemporary life and opened doors to possibilities that were previously unimaginable. In many facets of daily life, from communication to financial transactions, people rely on their portable electronic devices (Smith, 2011). Streaming media services give on-demand entertainment twenty-four (24) hours a day, while social networking sites like Facebook, WhatsApp, Viber, and many more have allowed us to contact with loved ones across the world to share and exchange ideas.

Technology advancements and the proliferation of online communication have led to a sharp spike in crime rates as well as the appearance of what seem to be new types of criminal activity, which provide difficulties for both the legal system and the law enforcement community (Brenner, 2007). A well-known newspaper in Ghana, the Daily Graphic, highlighted in its edition dated December 7th, 2017, that the development of the information and communication technology, including the introduction of online transaction system, cashless systems, top-up money, and online learning among others, has resulted in a sharp increase in cyber-related threats. James Oppong-Boanuh, the immediate past Inspector-General of Police in Ghana, has also expressed concern that the rise of ICT-facilitated crimes has turned into one of the many difficulties facing the adjudication of criminal offenses, particularly in accordance to provision of sufficient evidence to attain proper procession of a criminal in the court (Daily Graphic, 25/10/2017). The research aims to investigate how cybercrimes are being investigated in legal system especially, the police and the court in the nation in light of these factors.

4. RATIONALE FOR RESEARCH

According to (Jerman-Blažič & Klobučar, 2019) it is crucial that the research question and goals constitute a compelling justification for the study. As a resource for researchers, they suggested the following checklist:

i. Does the research study provide value by addressing a new issue, offering fresh perspectives on existing phenomena, or doing further research to support previous findings?
ii. Does the study address the theory and application of the subject matter?
iii. Is there a relationship between the study topic and the applicable theory and literature?
iv. Will the researcher use the information gathered to reach a study goal to make insightful deductions and recommendations?

Consequently, the justification for undertaking this study is distilled into three variables using Rojon and Saunders' (2012) reasoning. These criteria are based on the lack of theoretical applicability to the phenomena of cybercrime within the purview of this study, practical and policy gaps, and the knowledge gap in the body of current literature.

Knowledge Gap

Despite being a "vastly relevant and newsworthy issue" (Wall, 2004), cybercrime is still changing as a result of technological developments and people's increasing dependence on digital technologies for communication (Jerman-Blažič & Klobučar, 2019). Previous research has mostly focused on the financial costs of the cybercrime (Blažič & Klobučar, 2020), regulations and legal frameworks (Al-Tamimi, Marni, & Shehab, 2022), as well as its origins and consequences (Selvarajah & Mailvagnam, 2021). There is a divide between policymakers, academics, and law enforcement since there is not enough study on the Human-Centered Framework for evidence gathering in cybercrime investigation.

Practice and Policy Gap

In the worldwide effort to combat cybercrime, there must be some degree of commonality in practice and legislation since certain practical and policy concerns vary across states (Kumar, 2022). The inability of the stakeholders and nations to operate under uniform operational principles and standards prevents the effective investigation and punishment of cyber criminals.

The laws against cybercrime in Ghana at the moment are either insufficient (Elavarasi & Elango, 2017), or they need to be adequately implemented (Arpita Singh, 2022). In Ghana's criminal justice system, the primary participants have a considerable information-sharing gap, in accordance with the researchers' professional experience. Many cybercrime cases have been left unresolved in the courts as a result of training and knowledge gaps, according to (Hamad & Eleyan, 2022) since the majority of prosecutors and judges lack the necessary expertise to comprehend the dynamics of cybercrime.

Theoretical Application

Only a little quantity of literature has been written on the theoretical applications of cybercrime in Ghana. (Elavarasi & Elango, 2017) made some efforts to explain criminal trends, while (Shah & Chudasama, 2021) discussed the socio-technological study of cybercrime. Therefore, the paucity of literature on the use of regular activity theory served as one basis for carrying out this investigation.

Challenges to Digital Forensics

We identified the following five difficulties based on the literature reviewed

Challenge 1

Inadequate Evidence

Organizations do not consider proactive gathering of appropriate, acceptable evidence prior to an occurrence because it is seen to be too costly (Rowlingson, 2004). However, if evidence is there and procedures are well-defined, the cost and effect of an inquiry are reduced (Louwrens et al., 2006b).

Challenge 2

Continuity plans do not take evidence or procedural needs into account

The incident response plan (IRP) often fails to take evidence processing and preservation into account, nor does it verify that the method followed is forensically sound (Sommer, 1999). The absence of proof jeopardizes inquiries. When an event happens, there is insufficient relevant and legally admissible material to adequately launch and finish an inquiry (Thomas, 2005).

Challenge 3

The need for active or live investigative frameworks

When the frequency of 'live' attacks rises, conventional DF frameworks are no longer sufficient for conducting effective investigations. Rapid response is required not only to contain the crisis or prevent attacks but also to gather essential volatile and key facts in real-time. Live or dynamic evidence is more important in investigations as crimes grow more complex and targeted. Cybercriminals often launch their attacks through the Internet. (Blažič & Klobučar, 2020) state that there is an issue with the certification and acceptance of live evidence, that there is no definition for live forensics, and that there are no standard processes for conducting live investigations (Avinash Singh, Ikuesan, & Venter, 2019)

Challenge 4

The need for new DF Tools and Technology

As new hardware and software become available, traditional DF tools and methods become outdated. To illustrate, consider the following: Bitlocker disk encryption is available in Windows® Vista Ultimate and Enterprise versions. This is a whole disk encryption feature that use the AES (advanced encryption standard) encryption algorithm in CBC (cipher-block chaining) mode with a 128 / 256-bit key, in conjunction with the elephant diffuser1 for extra disk encryption-specific security that AES does not give (Rahman, 2021). Another barrier is that Bitlocker® has no backdoor, making it very difficult for an investigator to get access to an encrypted disc (Kumar, 2022) . When the material is encrypted, investigators must wait for a suitable opportunity to analyse a suspicious computer in a 'live' condition.

Therefore, it is essential for businesses to keep abreast of technological developments for the purpose of planning and preparing for such probes. Challenge 5: Non-investigative use of DF techniques and technology**.** Measuring the effectiveness of internal and technological controls is crucial. Corporate governance rules and reports like (Kaur, Bijalwan, Joshi, & Awasthi, 2018)require management to demonstrate control efficiency and effectiveness. DF tools and technology can be used to provide recorded verification of due diligence.

5. RESEARCH DIRECTION

Problem Statement
There is currently no human-centered digital framework for acquiring evidence in cybercrime investigations inside organizations, as shown by the difficulties mentioned in paragraph 1.2 and the research conducted for this research (Subair et al., 2022)

Research Question

i. in context of Routine Activity Theory, what motivates people to engage in cybercrime?
ii. In view of the Routine Activity Theory, how effective are Ghana's law enforcement agencies in stopping and investigating cybercrime?
iii. How well-suited is Ghana's present legal and conceptual frameworks to tackling cybercrime?
iv. What changes are necessary to the Ghana's efforts to combat cybercrime?

Objective of the Research

This research aims to establish a human-centered digital framework for collecting evidence in the investigation of cybercrime inside an organization. The following are ancillary objectives we've set up to help us reach the primary objective:

- Formulate a Digital framework for evidence gathering model
- Examine the interdependencies of the identified parts. Model of evidence collecting in a digital context
- Identify challenges to the Digital framework for evidence gathering model and further research
- Identify challenges hindering the implementation of Digital framework for evidence gathering model and identify further research opportunities

Expected Research Outcomes and Direction

The present study contributes to the body of knowledge about the particular contributions made by The Cybercrime Unit & Digital Forensic Laboratory to the fight against cybercrime in Ghana. The research on the precise responsibilities these actors play in combating cybercrime in Ghana is presently few or nonexistent, making this a significant addition. The present study advances our understanding of the advantages of internal and external collaboration between the Ghana Cybercrime Unit & Digital Forensic and external stakeholders. Additionally, the actions taken by Cybercrime Unit & Digital Forensic unit to investigate and punish cybercrime adds to the body of information about the strategies used to thwart cybercriminals' operations in Ghana.

The present study also advances knowledge by demonstrating the many ways that investigators, prosecutors, regulators, and lawmakers define "cybercrime". This contributes to the body of knowledge on the definitions and classifications of cybercrime.

BIBIOGRAPHY

1. Aguinis, H., & Solarino, A. M. (2019). Transparency and replicability in qualitative research: The case of interviews with elite informants. *Strategic Management Journal*. https://doi.org/10.1002/smj.3015
2. Al-Tamimi, K. H. S. S., Marni, N. Bin, & Shehab, A. (2022). Legal regulation of evidence in cybercrimes in UAE legislations. *International Journal of Health Sciences*, *6*(S1), 765–776. https://doi.org/10.53730/ijhs.v6ns1.4827
3. Baror, S. O., Venter, H. S., & Adeyemi, R. (2020). A natural human language framework for digital forensic readiness in the public cloud. *Australian Journal of Forensic Sciences*, 1–26. https://doi.org/10.1080/00450618.2020.1789742
4. Blažič, B. J., & Klobučar, T. (2020). Removing the barriers in cross-border crime investigation by gathering e-evidence in an interconnected society. *Information and Communications Technology Law*, *29*(1), 66–81. https://doi.org/10.1080/13600834.2020.1705035
5. Bouchaud, F., Grimaud, G., & Vantroys, T. (2018). IoT Forensic, (June), 1–9. https://doi.org/10.1145/3230833.3233257
6. Concoles, C. R., Cristobal, N., Felonia Jr, E., Tadtad, V. M., & Villafuerte, K. A. (2022). Cybercrime Awareness and Cybercrime Prevention Attitude of Criminology Students. *Southeast Asian Journal of Multidisciplinary Studies*, *1*(1).
7. Crawford, F. W., Wu, J., & Heimer, R. (2018). Hidden Population Size Estimation From Respondent-Driven Sampling: A Network Approach. *Journal of the American Statistical Association*, *113*(522), 755–766. https://doi.org/10.1080/01621459.2017.1285775
8. Creswell, J. W., & Miller, D. L. (2000a). D e t e r m i n i n g Vali d i t y i n Q u ali t a t ive I n q u i r y. *Theory into Practice*, *39*(3).
9. Creswell, J. W., & Miller, D. L. (2000b). in Qualitative Inquiry. *Theory and Practice*, *39*(3), 124–130.
10. Elavarasi, M., & Elango, N. M. (2017). Analysis of Cybercrime Investigation Mechanism in India. *Indian Journal of Science and Technology*, *10*(40), 1–4. https://doi.org/10.17485/ijst/2017/v10i40/119416
11. Elgohary, H. M., Darwish, S. M., & Elkaffas, S. M. (2022). Improving Uncertainty in Chain of Custody for Image Forensics Investigation Applications. *IEEE Access*, *10*(1), 14669–14679. https://doi.org/10.1109/ACCESS.2022.3147809
12. Emerson, R. W. (2018). Convenience Sampling, Random Sampling, and Snowball Sampling: How Does Sampling Affect the Validity of Research? *Journal of Visual Impairment & Blindness*, *109*(2), 164–168. https://doi.org/10.1177/0145482x1510900215
13. Ennin, D., & Mensah, R. O. (2019). Cybercrime in Ghana and the Reaction of the Law. *Journal of Law, Policy and Globalization*, *84*, 36–45. https://doi.org/10.7176/jlpg/84-04

14. Etikan, I., Alkassim, R., & Abubakar, S. (2015). Comparision of Snowball Sampling and Sequential Sampling Technique. *Biometrics & Biostatistics International Journal*, *3*(1), 1–2. https://doi.org/10.15406/bbij.2016.03.00055
15. Etikan, I. (2017). Sampling and Sampling Methods. *Biometrics & Biostatistics International Journal*, *5*(6), 5–7. https://doi.org/10.15406/bbij.2017.05.00149
16. Fakiha, B. S. (2021). Effectiveness of OSForensic in Digital Forensic Investigation to Curb cybercrime. *Indian Journal of Forensic Medicine & Toxicology*, *15*(3), 2149–2153. https://doi.org/10.37506/ijfmt.v15i3.15633
17. Fletcher, A. J., Macphee, M., & Dickson, G. (2015). Doing Participatory Action Research in a Multicase Study : A Methodological Example, 1–9. https://doi.org/10.1177/1609406915621405
18. Forman, J., & Damschroder, L. (2007). Qualitative Content Analysis. *Advances in Bioethics*, *11*, 39–62. https://doi.org/10.1016/S1479-3709(07)11003-7
19. Górny, A., & Napierała, J. (2016). Comparing the effectiveness of respondent-driven sampling and quota sampling in migration research. *International Journal of Social Research Methodology*, *19*(6), 645–661. https://doi.org/10.1080/13645579.2015.1077614
20. Hamad, N., & Eleyan, D. (2022). Digital Forensics Tools Used in Cybercrime Investigation-Comparative Analysis. *Journal of Xi'an University of Architecture & Technology*, *xiv*(May), 113–127. https://doi.org/10.37896/JXAT14.04/314909
21. Hamilton, J. B. (2019). Rigor in Qualitative Methods: An Evaluation of Strategies Among Underrepresented Rural Communities. *Qualitative Health Research*, 104973231986026. https://doi.org/10.1177/1049732319860267
22. Hays, D. G., Wood, C., Dahl, H., & Kirk-Jenkins, A. (2016). Methodological Rigor in Journal of Counseling & Development Qualitative Research Articles: A 15-Year Review. *Journal of Counseling and Development*, *94*(2), 172–183. https://doi.org/10.1002/jcad.12074
23. Heckathorn, D. D. (2011). COMMENT: SNOWBALL VERSUS RESPONDENT-DRIVEN SAMPLING Douglas D. Heckathorn*. *Sociological Methodology*, 355–366.
24. Horan, C., & Saiedian, H. (2021). Cyber Crime Investigation: Landscape, Challenges, and Future Research Directions. *Journal of Cybersecurity and Privacy*, *1*(4), 580–596. https://doi.org/10.3390/jcp1040029
25. Ilemona, S. A., Nweze, A., & State, G. (2021). FORENSIC INVESTIGATION AND EVIDENCE GATHERING PROCEDURE FOR FRAUD DETECTION AND REPORTING : A, *2*(1), 72–86.
26. Jerman-Blažič, B., & Klobučar, T. (2019). A new legal framework for cross-border data collection in crime investigation amongst selected European countries. *International Journal of Cyber Criminology*, *13*(2), 270–289. https://doi.org/10.5281/zenodo.3698359
27. Katos, V., & Bednar, P. M. (2008). A cyber-crime investigation framework. *Computer Standards and Interfaces*, *30*(4), 223–228. https://doi.org/10.1016/j.csi.2007.10.003
28. Kaur, P., Bijalwan, A., Joshi, R. C., & Awasthi, A. (2018). Network forensic process model and framework: An alternative scenario. *Advances in Intelligent Systems and Computing*, *624*(July), 493–502. https://doi.org/10.1007/978-981-10-5903-2_50
29. Kaya, Y. (2013). Comparison of Quantitative and Qualitative Research Traditions : epistemological , theoretical. *European Journal of Education*, *48*(2), 311–325. https://doi.org/doi:10.1111/ejed.12014

30. Khanafseh, M., Qatawneh, M., & Almobaideen, W. (2019). A survey of various frameworks and solutions in all branches of digital forensics with a focus on cloud forensics. *International Journal of Advanced Computer Science and Applications*, *10*(8), 610–629. https://doi.org/10.14569/ijacsa.2019.0100880
31. Kotsiuba, I., Skarga-Bandurova, I., Giannakoulias, A., & Bulda, O. (2019). Basic Forensic Procedures for Cyber Crime Investigation in Smart Grid Networks. *Proceedings - 2019 IEEE International Conference on Big Data, Big Data 2019*, 4255–4264. https://doi.org/10.1109/BigData47090.2019.9006215
32. Kumar, N. (2022). c, *3*(8), 56–58.
33. Mackieson, P., Shlonsky, A., & Connolly, M. (2018). Increasing rigor and reducing bias in qualitative research: A document analysis of parliamentary debates using applied thematic analysis. *Qualitative Social Work*, 147332501878699. https://doi.org/10.1177/1473325018786996
34. Maguire, M., & Delahunt, B. (2017). Doing a Thematic Analysis : A Practical , Step-by-Step Guide for Learning and Teaching Scholars ., *3*(3).
35. Meland, P. H., Tokas, S., Erdogan, G., Bernsmed, K., & Omerovic, A. (2021). A systematic mapping study on cyber security indicator data. *Electronics (Switzerland)*, *10*(9), 1–26. https://doi.org/10.3390/electronics10091092
36. Mensah, R. O. (2019). Cybercrime in Ghana and the Reaction of the Law. *Journal of Law, Policy and Globalization*, (April). https://doi.org/10.7176/jlpg/84-04
37. Mifsud Bonnici, J. P., Tudorica, M., & Cannataci, J. A. (2018). *The European Legal Framework on Electronic Evidence: Complex and in Need of Reform*. *Law, Governance and Technology Series* (Vol. 39). https://doi.org/10.1007/978-3-319-74872-6_11
38. Morse, J. M. (2015). Critical Analysis of Strategies for Determining Rigor in Qualitative Inquiry. *Qualitative Health Research*, *25*(9), 1212–1222. https://doi.org/10.1177/1049732315588501
39. Murray, J. (2021). an Assessment of Fuzzy Temporal Event Correlation Towards Cyber Crime Investigation. *International Research Journal of Engineering & Applied Sciences*, *9*(2), 10–14. https://doi.org/10.55083/irjeas.2021.v09i02006
40. Okutan, A., & Çebi, Y. (2019). A Framework for Cyber Crime Investigation. *Procedia Computer Science*, *158*, 287–294. https://doi.org/10.1016/j.procs.2019.09.054
41. Pedrero-Pérez, E. J., Morales-Alonso, S., Rodríguez-Rives, E., Díaz-Olalla, J. M., Álvarez-Crespo, B., & Benítez-Robredo, M. T. (2019). Smartphone nonusers: Associated sociodemographic and health variables. *Cyberpsychology, Behavior, and Social Networking*, *22*(9), 597–603. https://doi.org/10.1089/cyber.2019.0130
42. Pohoretskyi, M., Cherniak, A., Serhieieva, D., Chernysh, R., & Toporetska, Z. (2022). Detection and proof of cybercrime. *Revista Amazonia Investiga*, *11*(53), 259–269. https://doi.org/10.34069/ai/2022.53.05.26
43. Pollitt, M., Casey, E., Jaquet-Chiffelle, D.-O., & Gladyshev, P. (2018). A Framework for Harmonizing Forensic Science Practices and Digital/Multimedia Evidence. *The Organization of Scientific Area Committees for Forensic Science (OSAC)*, 1–29.
44. Rahi, S. (2017). Research Design and Methods: A Systematic Review of Research Paradigms, Sampling Issues and Instruments Development. *International Journal of Economics & Management Sciences*, *06*(02). https://doi.org/10.4172/2162-6359.1000403

45. Rahman, M. (2021). International Journal of Research Publication and Reviews Digital Evidence Sanctuary from Cybercrime : A Valuable Slant for Developing Countries, *2*(12), 400–407.
46. Rekha, G., & Sudha, T. (2022). A Study on Iot Forensic Investigation in the New Age of Intelligent Crimes, *71*(4), 3274–3281.
47. Safdar, M. A., & Afzal, W. (2022). ANALYSIS OF DIGITAL DEVICES AND TOOLS INVOLVED IN, *6*(1), 284–289.
48. Sargeant, J. (2013). Qualitative Research Part II: Participants, Analysis, and Quality Assurance. *Journal of Graduate Medical Education*, *4*(1), 1–3. https://doi.org/10.4300/jgme-d-11-00307.1
49. Selvarajah, V., & Mailvagnam, J. (2021). A framework for handling digital forensic evidence and evaluation on cyber resilience. *J Appl Technol Innovat*. Retrieved from https://www.academia.edu/download/83032257/Volume5_Issue4_Paper2_2021.pdf
50. Setthapirom, W. (2021). The Collection of Electronic Evidence in the Prevention of Cybercrimes.
51. Shah, A., & Chudasama, D. M. (2021). Investigating Various Approaches and Ways to Detect Cybercrime, (November). https://doi.org/10.37591/JoNS
52. Sidhu, K., Jones, R., & Stevenson, F. (2017). Publishing qualitative research in medical journals. *British Journal of General Practice*, *67*(658), 229–230. https://doi.org/10.3399/bjgp17x690821
53. Singh, Arpita. (2022). A Framework for Crime Detection and Reduction in Digital Forensics. *SSRN Electronic Journal*, *71*(4), 531–552. https://doi.org/10.2139/ssrn.4082975
54. Singh, Avinash, Ikuesan, A. R., & Venter, H. S. (2019). Digital Forensic Readiness Framework for Ransomware Investigation. *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST*, *259*, 91–105. https://doi.org/10.1007/978-3-030-05487-8_5
55. Smith, B., & McGannon, K. R. (2018). Developing rigor in qualitative research: problems and opportunities within sport and exercise psychology. *International Review of Sport and Exercise Psychology*, *11*(1), 101–121. https://doi.org/10.1080/1750984X.2017.1317357
56. Subair, S., Yosif, D., Ahmed, A., & Thron, C. (2022). Cyber Crime Forensics. *International Journal of Emerging Multidisciplinaries: Computer Science & Artificial Intelligence*, *1*(1), 41–49. https://doi.org/10.54938/ijemdcsai.2022.01.1.37
57. Sundler, A. J., Lindberg, E., Nilsson, C., & Palmér, L. (2019). Qualitative thematic analysis based on descriptive phenomenology. *Nursing Open*, (September 2018), 733–739. https://doi.org/10.1002/nop2.275
58. Taherdoost, H. (2018). Sampling Methods in Research Methodology; How to Choose a Sampling Technique for Research. *SSRN Electronic Journal*, *5*(2), 18–27. https://doi.org/10.2139/ssrn.3205035
59. TenHouten, W. D. (2017). Site Sampling and Snowball Sampling - Methodology for Accessing Hard-to-reach Populations. *BMS Bulletin of Sociological Methodology/ Bulletin de Methodologie Sociologique*, *134*(1), 58–61. https://doi.org/10.1177/0759106317693790
60. Thakar, A. A., Kumar, K., & Patel, B. (2021). Next Generation Digital Forensic Investigation Model (NGDFIM) - Enhanced, Time Reducing and Comprehensive Framework. *Journal of Physics: Conference Series*, *1767*(1). https://doi.org/10.1088/1742-6596/1767/1/012054
61. Understanding Reliability and Validity in Qualitative Research. (2003). *Qualitative Report*, *8*(4), 597–607.

62. Vashistha, A., Cutrell, E., & Thies, W. (2015). Increasing the Reach of Snowball Sampling: The Impact of Fixed versus Lottery Incentives. *Cscw*, 1359–1363. https://doi.org/10.1145/2675133.2675148
63. Walsham, G. (1995). ISR emergence of interpretivism in IS research Walsham.pdf. *Information Systems Research*, *6*(4), 376–394.
64. Walsham, G. (2006). Doing interpretive research. *European Journal of Information Systems*, *15*(3), 320–330. https://doi.org/10.1057/palgrave.ejis.3000589
65. "An Overview of Ghana's Cyber Security Act, 2020 - Act 1038." DICKSON & FOLI CENTER FOR STRATEGIC AND DEFENCE STUDIES, AFRICA , 2021.