

Article Citation Format

Baafi Benjamin, Longe Olumide Babatope & Joseph Budu (2023): A Human-Centered Framework for Evidence Gathering in Cybercrime Investigation.. Journal of Digital Innovations & Contemporary Research in Science, Engineering & Technology. Vol. 11, No. 2. Pp 57-75
www.isteams.net/digitaljournal.
dx.doi.org/10.22624/AIMS/DIGITAL/V11N2P5

Article Progress Time Stamps

Article Type: Research Article
Manuscript Received: 12th April, 2023
Review Type: Blind Peer
Final Acceptance: 6th June, 2023

A Human-Centered Framework for Evidence Gathering in Cybercrime Investigation.

¹Baafi Benjamin, Longe Olumide 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

¹E-mail: benjaminbaafi@ymail.com

¹Phone: +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 thrives. Additionally, the integration of computers and the development of communication technologies has altered social interactions and criminal behavior. This thesis utilizes the Routine Activity Theory (RAT), a foundational paradigm in the study of criminal behavior. Within the context of RAT, we focused on cybercrime in Ghana, more specifically on the problem of advance fee fraud. It contended that there are three necessary conditions for criminal activity to occur: a motivated criminal, a victim who is easy to manipulate, and the lack of a responsible caretaker. In the thesis, we looked at how what drives a criminal, and what characteristics make a person (or computer) an attractive target. The method involves evaluating the credibility of a law enforcement official. What role does Ghana Police Service and the criminal investigative department in Ghana play as effective watchdogs, and what constraints limit its ability to do so? decreasing the impact of cybercriminal actions. The study is based on a relativist philosophical perspective and an interpretivist paradigm. emphasize a qualitative inductive strategy, such as semi-structured interviews and careful recording. Policymakers, legislators, and regulators in the fields of telecommunications and information and communication technology all took part in these. on the one hand, and professionals in the fields of investigation, prosecution, forensic analysis, and the media, The multi-dimensional evidence explains the role played by each of the stakeholders, the measures and partnerships deployed in tackling cybercrime, and the challenges and recommendations needed in the international effort to tackle cybercrime globally. Findings suggest that the proliferation and lack of effective policing of the internet enabled by the greed of individuals and lack of enforcement and collaboration of relevant stakeholders has led to financial losses to victims. We equally extend the criminological understanding of online deviant behaviors and furthers the current discussion on the role of law enforcement in policing the Internet.

Keywords: Human-Centered Framework, Evidence Gathering, Cybercrime Investigation, Ghana.

I. INTRODUCTION

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.

2. RESEARCH PERSPECTIVES

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, & Vantrois, 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).

3. DATA ANALYSIS, INTERPRETATION AND DISCUSSION

The data analysis chapter presents the numerous study participants as well as the design and development of the research interview questions. The chapter also looks at the role of the interviewer and how the participants were handled during the interview. With a focus on theme analysis, a summary of the interview transcription and data coding is further developed. The results analysis and the themes' interpretation are also included in the chapter. A summary of the facts and conclusions is then built upon and debated.

Research Participant Representation

After receiving ethics permission, the researcher began collecting data. According to Patton (2002), the number of interviews necessary for qualitative research varies on the study's objectives, available resources, and time. Since Myers (2013:123) claims that "no new insights are being uncovered in the interviews," the data gathering method in this study was carried out until it achieved saturation and stopped revealing any new nodes. The first interview took place on August 1st, 2022, and the last interview took place on August 25th, 2022.

Before beginning the data analysis process, the following procedures were taken:

- For transcription, every interview was digitally recorded and then uploaded to a computer.
- On a laptop, all soft copies of the recordings were renamed and encrypted.
- Using Microsoft Word, every interview was completely verbatim transcribed.
- To accurately capture every dialogue, every interview was transcribed without grammatical correction, repetitive word removal, or sentence completion (Bazeley, 2007).
- The transcript was then altered, with replies having the "Quote" heading and questions having the Microsoft Heading 3.
-

The NVivo software was used to rename and import all interview transcripts for coding.

To maintain identity and confidentiality, each interviewee was given a code, ranging from Participant 1 to 25.

All 25 interviewees and their pertinent demographic information are included in Table 4.1 below. The attendees represented the fields of law enforcement, telecommunications, information and communication technology, and the IT industry. Members of law enforcement were organized into four specialized divisions, each of which plays an essential role in tracing the sources of cybercrime. The investigative, forensic, information technology, and legal teams. The researcher spoke with the unit and department leaders, as well as section heads and team leads, from each of the four primary departments. Both proponents and detractors of the NVivo software have been voiced by academics. Time spent learning the program may not be proportional to the benefits gained from utilizing computer-assisted qualitative data analysis software (CAQDAS), as stated by Budding and Cools (2008). They also claim that tiny data sets are not worth utilizing the program on since they can be handled faster and more manually. The researcher found that file corruption and system crashes were common when using NVivo Software, hence it is imperative that users always have a backup.

Table 4.1: Showing Interviewees Relevant Demographics

CODE NAME	SECTOR	DEPARTMENTS/UNIT/SECTION	DATE
Participant 1	LAW ENFORCEMENT	INVESTIGATION	01/08/2022
Participant 2	LAW ENFORCEMENT	INVESTIGATION	01/08/2022
Participant 3	LAW ENFORCEMENT	INVESTIGATION	03/08/2022
Participant 4	LAW ENFORCEMENT	Cyber Intelligence (Cyber patrol)	04/08/2022
Participant 5	LAW ENFORCEMENT	Cyber Intelligence (Cyber patrol)	04/08/2022
Participant 6	LAW ENFORCEMENT	Cyber Intelligence (Cyber patrol)	06/08/2022
Participant 7	LAW ENFORCEMENT	INVESTIGATION	07/08/2022
Participant 8	LAW ENFORCEMENT	FORENSICS	08/08/2022
Participant 9	LAW ENFORCEMENT	FORENSICS	09/08/2022
Participant 10	LAW ENFORCEMENT	FORENSICS	10/08/2022
Participant 11	LAW ENFORCEMENT	FORENSICS	11/08/2022
Participant 12	LAW ENFORCEMENT	INVESTIGATION	12/08/2022
Participant 13	LAW ENFORCEMENT	INVESTIGATION	12/08/2022
Participant 14	LAW ENFORCEMENT	Cyber Investigations	14/08/2022
Participant 15	LAW ENFORCEMENT	Cyber Investigations	15/08/2022
Participant 16	LAW ENFORCEMENT	Cyber Investigations	16/08/2022
Participant 17	LAW ENFORCEMENT	Cyber Investigations	16/08/2022
Participant 18	LAW ENFORCEMENT	Cyber Investigations	18/08/2022
Participant 19	ICT SECTOR	CYBERSECURITY	19/08/2022
Participant 20	ICT SECTOR	CYBERSECURITY	20/08/2022
Participant 21	TELECOMMUNICATION	CYBERSECURITY	21/08/2022
Participant 22	TELECOMMUNICATION	CYBERSECURITY	22/08/2022
Participant 23	TELECOMMUNICATION	the Child Protection Digital Forensics Laboratory.	23/08/2022
Participant 24	LAW ENFORCEMENT	ICT	24/08/2022
Participant 25	LAW ENFORCEMENT	ICT	25/08/2022

NVivo was used, nevertheless, because to the benefits listed below (Bringer, Johnston, & Brackenridge, 2004):

- The capacity to organize facts to assist with analysis
- The capability to secure data from loss or theft by using a password and several backups.
- Providing easy access for data retrieval and coding
- Automation gives researchers more time to conduct analyses
- Aids in sophisticated "Boolean" searches, which are very difficult to do using manual tools (e.g., and, or, not).
- It promotes transparency by linking papers, memos, nodes, and modes, which may be challenging when using manual approaches.

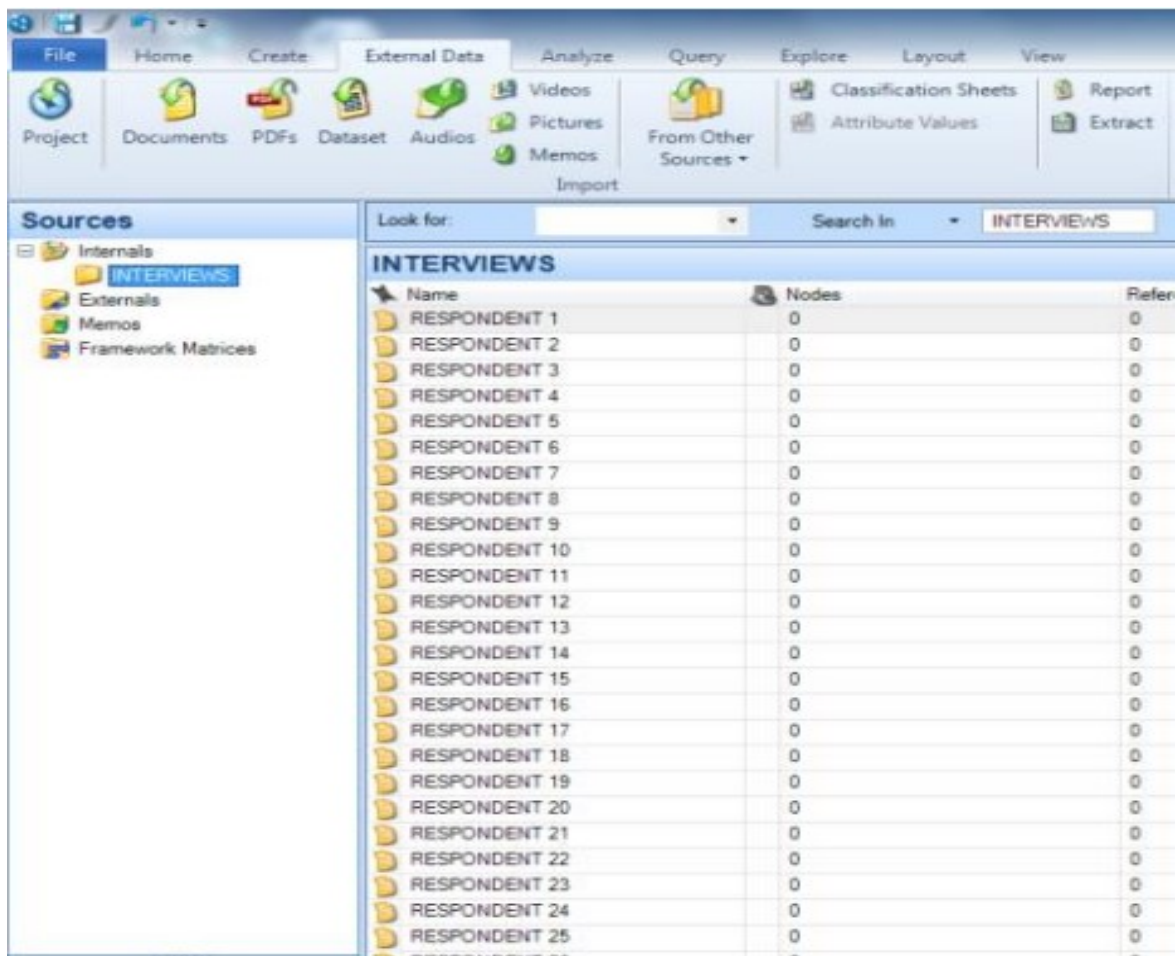
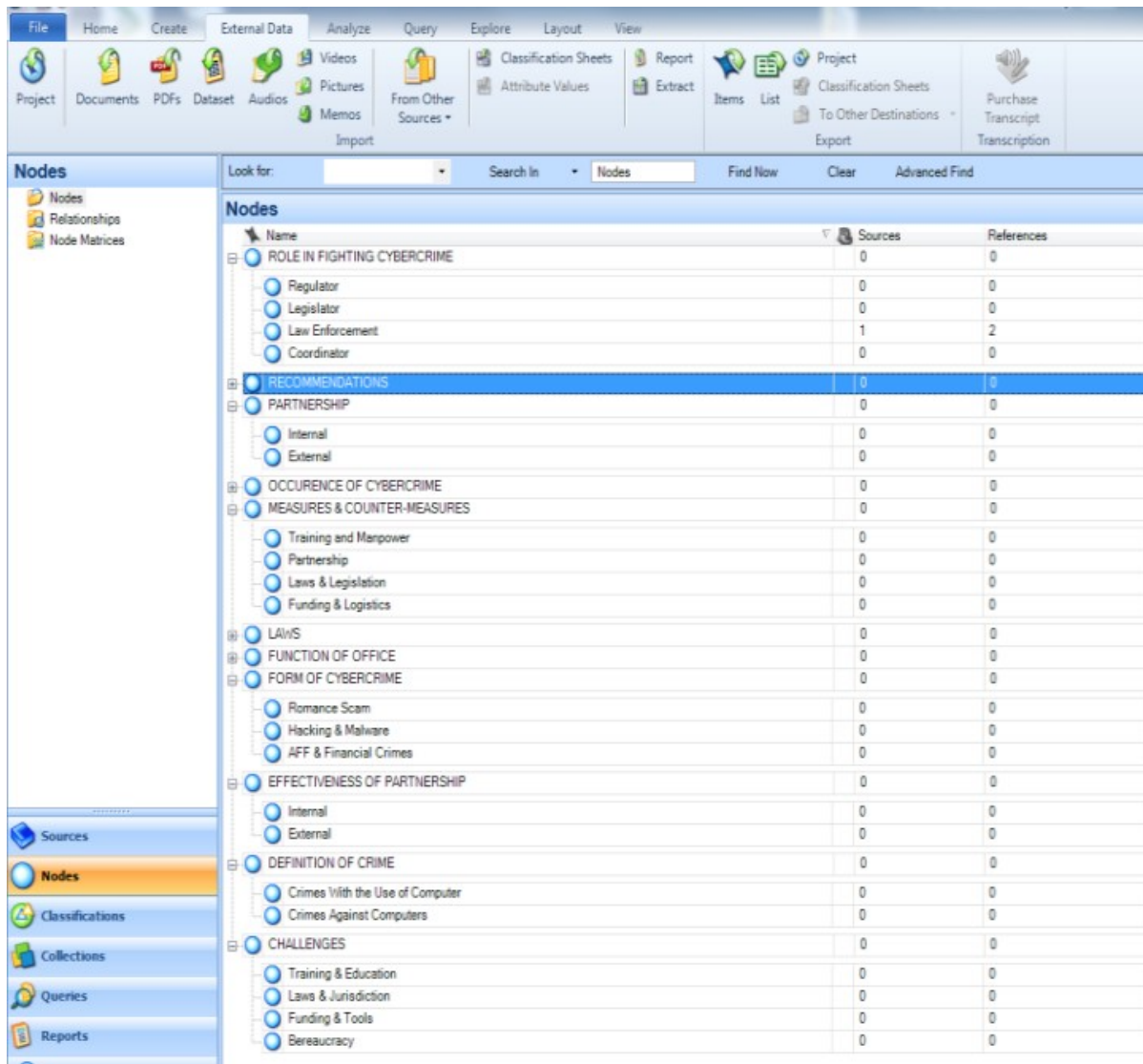


Figure I: NVivo Explorer screenshot showing all the Interviews after transcription

Figure I displays each interview's transcription that was loaded into the NVivo program. The interview folder, labeled Participant 1 to 25, is shown on the left panel under source and internal. The list of all the interviews and the creation date are shown in the right panel. The nodes and sub-nodes are all shown in Figure I. The study questions, literature review, and theoretical framework served as the nodes, which represent the themes, while the majority of the sub-nodes represent replies provided by respondents to interview questions.



Name	Sources	References
ROLE IN FIGHTING CYBERCRIME	0	0
Regulator	0	0
Legislator	0	0
Law Enforcement	1	2
Coordinator	0	0
RECOMMENDATIONS	0	0
PARTNERSHIP	0	0
Internal	0	0
External	0	0
OCCURENCE OF CYBERCRIME	0	0
MEASURES & COUNTER-MEASURES	0	0
Training and Manpower	0	0
Partnership	0	0
Laws & Legislation	0	0
Funding & Logistics	0	0
LAWS	0	0
FUNCTION OF OFFICE	0	0
FORM OF CYBERCRIME	0	0
Romance Scam	0	0
Hacking & Malware	0	0
AFF & Financial Crimes	0	0
EFFECTIVENESS OF PARTNERSHIP	0	0
Internal	0	0
External	0	0
DEFINITION OF CRIME	0	0
Crimes With the Use of Computer	0	0
Crimes Against Computers	0	0
CHALLENGES	0	0
Training & Education	0	0
Laws & Jurisdiction	0	0
Funding & Tools	0	0
Bureaucracy	0	0

Figure 2: NVivo explorer screenshots showing all the nodes and sub-nodes

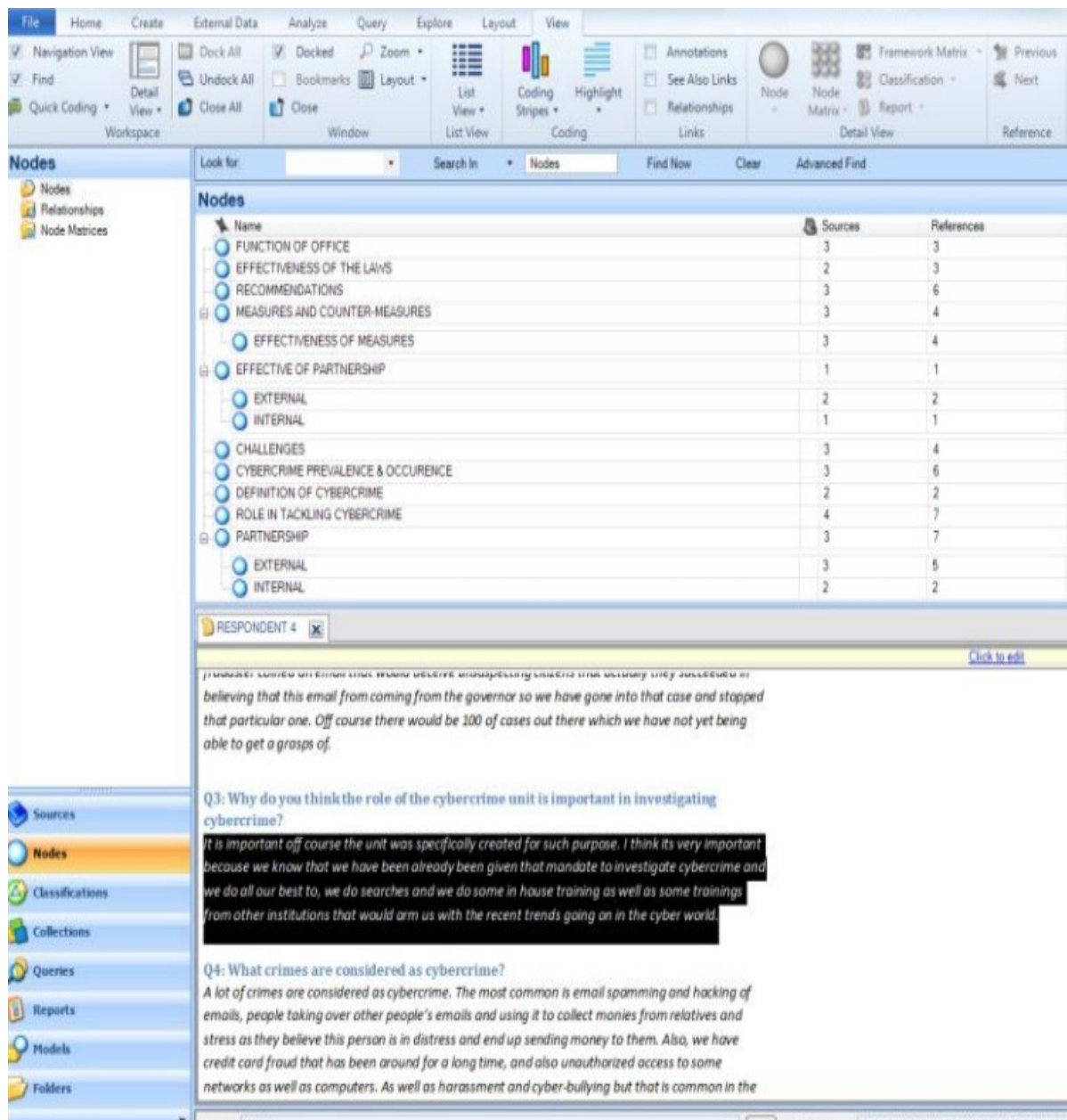


Figure 3: NVivo explorer illustrating the coding of an interviewee response

Figure 3 shows the coding process done on a particular interview. A portion of the transcript was used to code it to a particular node and sub-node respectively.



Figure 4: NVivo screenshot of word cloud generated from interviewees response

Design and Development of Interview Questions

The concepts and concerns informed the development of the interview questions:

- When developing the questions, the study's overarching goals and objectives (Chapter 1 - Introduction) and research questions were taken into account (Chapter 3: Methodology).
- The researcher made sure the eleven topics that emerged from the literature analysis were adequately represented in the interview questions.
- Routine Activity Theory was taken into mind while creating the questions (RAT)
- Background information and targeted questions were utilized to allow participants to contextualize the occurrence within their own organizations.

Function of Interviewer and Interview Administration

According to McCracken (1998), interviewers are crucial to the process of gathering data and must choose how much they will actively engage. Therefore, the researcher must choose whether to play a "backseat" role and let the interviewee talk candidly or organically or to be actively engaged and contribute to the design of the process by which the interviewee's data is gathered. Wengraf (2011) contends that the choices the interviewer makes throughout the interview may have varied consequences on the outcomes and that the skill of interviewing is one that needs thorough evaluation and practice.

Table 2: Interview Administration Variables and Description⁵⁴

VARIABLES	DESCRIPTION
Location of Interviews	Ghana, Accra
Number of Participants	25 Interviewees
Method of Interview	Face-to-Face (32); Phone Interview (2)
Storage of Data	Digitally Recorded and Stored
Duration of Interviews	Average of 25-30 Minutes
Documents Presented	Interviewer sheet and Consent Form
Dates	August 1st - August 25 th

Demographic Interview Findings

Organisation A – Ghana Police Cyber Crime Unit

The Ghana Police Service's Criminal Investigations Department has a specialized unit called the Cyber Crime Unit. Its main responsibility is the detection and investigation of crimes where the target(s) or means of the crime involve one or more digital device(s), networks, other telecommunication devices, or the internet. The Cybercrime Unit also looks into delicate issues like online child abuse and exploitation, as well as any other instances involving women and children in cyberspace. The Cyber Crime Unit is outfitted with a cutting-edge Digital Forensics Laboratory for conducting digital forensics examinations and a Cyber Patrol Section for conducting advanced online monitoring and surveillance of Ghana's cyberspace in order to discover crimes.

The participation of the Cyber Crime Unit goes beyond investigations into more conventional offenses including fraud, threats, and other severe crimes where a digital device was utilized, such as hacking and other crimes often linked with technology. Unquestionably, the Cybercrime Unit has never failed to investigate child abuse that occurs online. With assistance from UNICEF and the National Center for Missing & Exploited Children, the Cyber Crime Unit has been working all year to look into, apprehend, and punish suspected of online child abuse and cyberbullying.

The primary law enforcement organization in Ghana is called the Ghana Police Service (GPS). Over 30,000 officers are employed by the agency, which is run by the Ghanaian Ministry of the Interior throughout its 651 stations.

Functions and Responsibilities

All of the following duties and obligations, individually or in combination:

- Investigations into and prosecution of cybercrime
- Data gathering and forensic analysis
- collection, analysis, and distribution of cyber intelligence
- Evaluation and examination of the phenomenon of cybercrime
- help for other police forces that is specialized
- Cyber monitoring and surveillance

The respondent interview for this research are majorly from Ghana Police Cyber Crime Unit office

Interview Findings – Analysis and Interpretation of Themes

Theme 1: Role in Fighting Cybercrime

The interviewees were separated into their departments, units, and sections, respectively, in order to analyze this subject. Participants were divided into sub nodes, which were these distinct departments. The second theme focused on particular tasks that each department or area had in combating cybercrime. This issue was then broken down into nine (9) subthemes for analysis including: Telecommunications Regulation, ICT Regulation, Investigation, Forensics and Legal. One participant each from the National Coordinator, Legislation, Telecoms Regulator, and ICT. In light of the participant responses, "Theme 2: Role in Fighting Cybercrime" was examined.

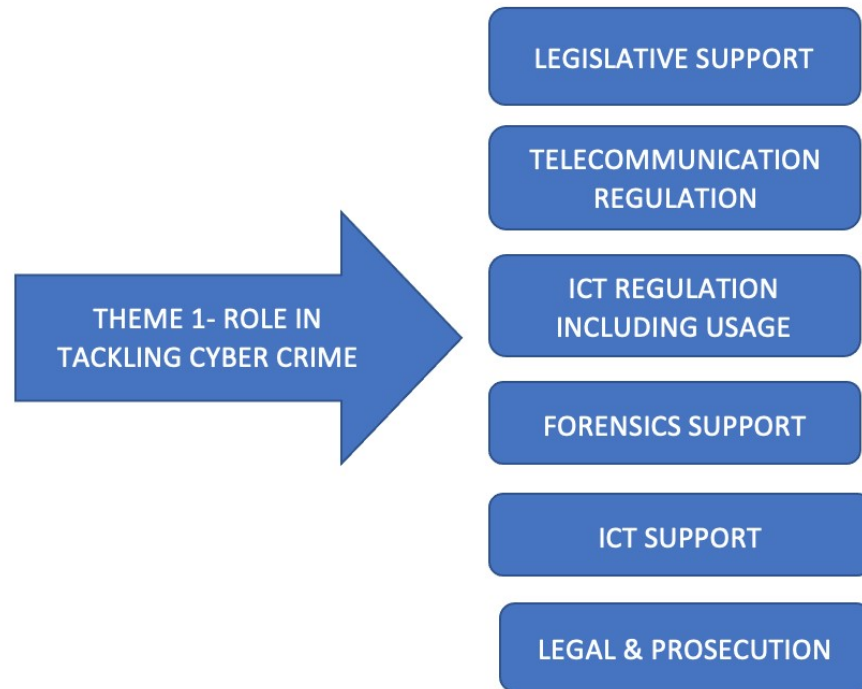


Figure 5: Measures, Benefits of Measures & Sub-Themes

Investigation

Eight participants, who all worked for law enforcement agencies, make up the "Investigation" category. The majority of the Investigators' responses focused on the precise responsibilities they undertook in accordance with their mandates to investigate severe cybercrimes. Participants were also questioned on the significance of their roles in examining computer- or cyber-related crimes.

The mandate of the section is in line with the mandate of the Ghana cyber unit only as it relates to where we narrow it down to. The overall mandate is to rid Ghana of the scourge of cybercrime. Create awareness of the negative impact of cybercrime on the Ghana economy, and on Ghana themselves. (Participant 1, Cybercrime Investigator, (September 8th, 2022)

Most Ghana investigators interviews gave the same response six times. One of the Investigators responded as follows when further questioned on the applicability of their particular section in combating cybercrime:

Obviously, it's crucial that the device was designed with this function in mind. I believe it is crucial since we have been assigned the responsibility of investigating cybercrime. To fulfill this duty, we conduct extensive searches, as well as attend in-house and external training designed to prepare us for the latest developments in this field. (Cybercrime Expert 1), (September 18th, 2022).

Forensics Support

Six people, all from a Ghana police department, are included in the "Forensics Support" group. Respondents from the Ghana forensics community discussed their distinct functions in the investigation of cybercrimes. Participants were also questioned on the significance of their positions in the investigation of cybercrime and other computer-related offenses.

We provide operational support; the operatives constantly ask for assistance and training on how to utilize computers, software, and systems. We also offer training for specific topics, such as cybercrime awareness for members of the Operations unit, Legal unit, and other units we have. Additionally, we provide logistics. ICT Team Lead, (Participant 2,) (September 4th, 2022).

Four (4) respondents made the same point regarding providing operational assistance, while two (2) others talked particularly about how ICT performed research and trained investigators.

Additionally, it seeks to identify patterns in cybercrime, train the investigative cybercrime section, and, in general, attempt to bridge the digital divide between law enforcement and technology. (ICT Team Lead, Participant 20, 23 August 2016)

When questioned about the usefulness of ICT in pursuing cybercrime, all six (6) respondents emphasized the significance of understanding ICT in conducting thorough investigations.

It's a technology crime, and the IT department should be involved because you can't even look into cybercrime without IT since it's a technology crime, so you'd have to utilize the same technology to look into those types of crimes. ICT Team Lead, (Participant 5) (September 9th, 2022).

Legislative Support

The Parliament of Ghana is in charge of passing legislation. The Sub Committee in charge of creating new cyber laws and revising already-existing regulations pertaining to ICT and cybercrime. The participant's responses were based on the committee's oversight role over all MDAs that dealt with ICT and cybercrime-related concerns. The participant was also questioned on the significance of their work in Ghana's fight against computer-related crimes.

There has been a continuous review of the current legislation on cybercrime the last law was passed in 2020, which we now feel is insufficient to address the global cybercrime that is now occurring since it requires several agreements with other nations to function or be successful. (Participant 10)) (September 16th, 2022).

The participant's response focused on the need to evaluate current laws to make them more useful in combating cybercrime in Ghana. The interviewee's reaction to the Parliament Committee's applicability in combating cybercrime.

Telecommunications Regulation

National Communications Authority Ghana, which is in charge of regulating the country's telecoms industry, was represented by only one person. The participant is from the organization's cybersecurity section, and their duties are centered on their mission to provide ISPs and telecom firms, who offer internet and communication services that are regularly misused by cybercriminals, rules and cybersecurity plans. The participant was also questioned on the applicability of their role in tackling Ghana problems with computer-related offenses and breaches.

The major channel of communication between the Commission's cybersecurity section and Law enforcement organizations and telecommunications companies in Ghana respect for telecommunications-related crimes and investigations services. (Telecoms Regulator, Participant 12)) (September 23th, 2022).

The participant said that when law enforcement was looking into cyber-related crimes, the unit acted as the main point of contact. The participant said when questioned about the unit's applicability in combating cybercrime

First of all, the body is in charge of issuing the rules that govern the operations of telecom companies in Ghana. Since mobile telephony is the main form of communication in Ghana and as you are aware, the telecommunications sector is governed by the Commission, telecommunications are crucial to the country's cybercrime issues. (Telecoms Regulator, Participant 14) (September 5th, 2022).

The response provided highlighted the role performed by the cybersecurity unit and the significance of the telecoms industry in tackling the problem of cybercrime in Ghana.

4. CONCLUSION

This chapter's conclusion revisits the research's justification and examines its methodology. The chapter examines the contributions to theory, practice, policy, and knowledge. This chapter also describes how the study was evaluated using Klein and Myers' (1999) interpretative field research principles. The chapter's last section focuses on the research's limits and possible future possibilities.

Research Summary

There is a dearth of literature on law enforcement and the responsibilities of members of the Cybercrime Advisory Council in combating cybercrime jointly, as stated in the introduction and literature review. Most previous studies (Hassan et al., 2012; Adesina, 2017) concentrated on the causes and effects of cybercrime in Ghana; laws that penalize computer misuse (Olusola et al., 2013b; Saulawa and Abubakar, 2014); and focused relatively on the financial cost and socio-economic effects of cybercrime (WITFOR, 2005; Sesan et al., 2012). The present research combines all these many elements and makes an effort to comprehend cybercrime from the perspective of Ghana law enforcement, similar to the studies done by Maghairah (2009) and Alkaabi (2010).

Furthermore, Yar (2005) has stated that Routine Activity Theory may be taken into account in comprehending cybercrime, thus the study adopts this framework to examine the theory's relevance to cyberspace. In Chapter 4, the rationale for choosing the theory was thoroughly covered. The research was conceptualized using an interpretivist paradigm and a relativist philosophical perspective, which adapts the approach to the present study's exploratory and explanatory character.

Since the study issue is social in nature, a qualitative technique was employed to gather information via interviews. 25 participants, the majority of whom were from a law enforcement agency, were interviewed. According to study evidence, members of the Ghana Cybercrime Units have made an effort to address obstacles in the investigation of cybercrime via collaboration, training, and the enforcement of relevant laws and policies. Finally, the research advances the present debate on the role of law enforcement in policing cybercrime in Ghana and broadens the criminological perspective on online deviant behavior. The study's contributions are divided into the following categories:

Theory Contribution

The research tackles the gap in Routine Activity Theory's (RAT) application to deviant By expanding the criminological framework to include online behaviors like advance fee fraud in Ghana knowledge of a target's eligibility, a determined perpetrator, and the lack of a competition under the purview of law enforcement, a guardian. This research improved comprehension of the following three RAT components:

Suitable Target

According to Yar (2005), the more accessible a target is, the more appropriate it is, and the offender's decision-making process while selecting a suitable target is predicated on whether the target is being chosen for "personal, enjoyment, for sale," or to be utilized in committing another crime. This research has strengthened the case made by Yar (2005) by demonstrating how vulnerable Ghana's computer systems were, making it easier for thieves to target specific people and organizations. The research has also improved RAT target appropriateness since it discovered that one of the factors that increases a person's vulnerability to being a victim of an online crime is their ignorance about potential targets, such as people. However, the discovery also made a theoretical contribution by challenging RAT hypotheses on the convergence of the three criteria for crime to occur and by including the existence of lax laws as a factor in making a target acceptable for a motivated perpetrator.

Motivated Offender

According to Grabosky (2001), the assumptions regarding a cybercriminal's motivations as a human element to conduct crime remain the same. The results of this research support Grabosky's (2001) thesis that Ghana's cybercriminals are driven by avarice and the potential financial benefit of committing crimes. The research made a contribution to RAT by claiming that the high rates of poverty and unemployment among Ghana's smart youngsters are what drives them to engage in cybercrime.

Absence of a Capable Guardian

Due to responsibility sharing among law enforcement officials, information security experts, and individual users, regulating crime in both terrestrial and cyberspace has evolved into a "pluralistic endeavor" (Grabosky, 2001). This research adds to RAT but broadens the notion of a competent guardian by addressing problems including the lack of resources, equipment, training, and education for Ghana law enforcement officials, which prevents them from becoming effective guardians of prospective cybercriminal victims. Additionally, the study adds to RAT by stating that the borderless nature of cybercrime has made the application of laws and jurisdictions a difficult problem for policing cybercrime in Ghana. Law enforcement officers now have to "catch up" to criminals due to the continuous evolution of technology.

Knowledge Contribution

The area of cybercrime policing, particularly in Ghana, has benefited from the research examination. The discovery of the eleven themes that emerged from this study's results is useful because they provide a conceptual framework for comprehending the complex connections and interconnections between the many components. Some of these topics were the subject of earlier research (Khanafseh et al., 2019).but the eleven themes were not fully taken into account. Future study on cybercrime policing in Ghana will have a comprehensive framework thanks to the topics that have been identified.

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. Finally, the research advances knowledge by offering suggestions for combating cybercrime. By claiming that enhanced public awareness combined with law enforcement agency education may be a successful strategy for crime control and crime prevention, the research adds to the body of existing literature on the subject.

Research Limitation

All research studies have their own set of restrictions. Although this research study's design, data collecting, and analysis phases included careful deliberation, there are some general limitations. The following categories apply to the limitations:

Theoretical Limitation

The Routine Activity Theory was the sole criminological theory included in the theoretical framework of this study. Although they were taken into consideration and evaluated in Chapter 3: Others criminological Theoretical Framework, general deterrence theory was not employed in this research.

Logistical Limitations

Despite the researcher's desire to use mixed methods and combine quantitative information from the public with qualitative information from law enforcement agencies, the study was only able to use a qualitative approach because of practical limitations and getting the necessary approval to interview law enforcement in other regions outside Accra

Limitation of the Research's Scope

The research's coverage was restricted to the actions of law enforcement organizations, particularly the Ghana Cybercrime Unit & Digital Forensic in its capacity as a specialized unit at the Criminal Investigations Department of the Ghana Police Service.

Methodological Limitation

This Research was constrained by a methodological limitation that used an interpretive paradigm and a relativist philosophical premise. The data was gathered via interviews and documentation as part of a purely qualitative, inductive research methodology. NVivo was only utilized in the study to organize the information; manual coding was also used. The interviews were placed across time, although cross-sectional research may have given different results.

Future Research

Future cybercrime research has a wide range of promises. The development of technology and crime itself is to blame for this. A future study might be undertaken based on the following categorizations as this research was constrained by its scope, context, and other constraints listed above:

Theory

To ascertain if the laws are effective, future studies might make use of the general deterrence theory. a deterrence to criminals when utilized in the punishment of cyber criminals. Additional study may be relevant. Routine Activity Theory to another kind of cybercrime, such cyberstalking or Because these are established crimes that technology has made even more possible, cyberbullying.

Topology of Crime

To learn about the difficulties encountered by cyber security experts, research might be done on a variety of criminal behaviors, such as online grooming or cyberterrorism.

Scope: Research on victims of cybercrime rather than law enforcement agencies might be conducted to learn more about how they see the actions of both criminals and law enforcement. The depth of the data might be utilized to assist the present research study. This could be done by surveys, interviews, or focus groups.

Practice and Policy Contribution

There were fresh policy-related revelations from the present investigation, according to the study. The findings revealed that criminals were not sufficiently discouraged from committing crimes by the arrest and conviction offenders. The research's conclusions placed a strong focus on the need to educate those engaged in cybercrime investigation, prosecution, and prevention via specialized training. It was suggested that the general public's knowledge of self-protection be raised. Additionally, some significant concerns were brought up in the misapplication of the Cybersecurity Act, 2020 (Act 1038) to help in cybersecurity development and in response to cybersecurity challenges. Online bloggers who criticize public authorities have been arrested and prosecuted under this legal authority. This was because the bill was enacted into law without the involvement of numerous stakeholders, despite further data that revealed it required major modification.

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). Determining Validity in Qualitative Inquiry. *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](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., Giannakoulis, 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/IJoNS>
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/ijemdcasai.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.