Relativism digital forensics investigations model: a case for the emerging economies

Relativism Digital Forensics Investigations Model: A Case for the Emerging Economies

Abel Yeboah-Ofori[1,4], Ezer Yeboah-Boateng[2,5], Herbert Gustav Yankson[3,6]
[1]School of Arch, Computing & Engineering, University of East London, United Kingdom
[2]Faculty of Informatics, Ghana Technology University College, Accra, Ghana
[3]Ghana Police Service, Cybercrime Unit, CID Head Quarters, Ghana
[4]u0118547@uel.ac.uk, [5]eyeboah-boateng@gtuc.edu.g, [6]Hgustav.yankson@gmail.com

Abstract- **Digital forensic investigations (DFI) is a process of investigating computers and its associated media to determine whether it has been used to commit a crime or gain unauthorized access. cyberattacks and cybercrimes can be committed globally but reported locally. However, DFI processes vary relative to a particular jurisdiction. Relativism is the perception of universal norms of what is right and wrong or legal and illegal. Although cybercrimes are illegal, what constitutes illegal is relative to a jurisdiction. Cyber espionage attacks may be considered legal or illegal based on economic advantage for someone or as target for attack based on motive and intent. Further, following legal procedures in evidence gathering at a digital crime scene is critical for prosecution. However, there are challenges in gathering evidence using the existing DFI models on all attacks. UNODC, report on the globalization of cybercrimes highlighted the challenges of cybercrime and ranked some emerging economies among the first 10 offending nations globally. There are existing models that are specific to certain jurisdictions and assist the judiciary, law enforcement agencies, and forensic experts. Consequently, presenting digital forensic evidence in court has proved to be challenging, due to a lack of procedures and DFI models specific to emerging economies. In this paper, we identify the phase that is relevant and could facilitate DFI processes from emerging economies' perspective. Further, we review some existing models to determine their relative procedures. This paper does not negate existing models, rather derives a relative model from existing models. We propose a model that will improve the DFI process from the result of the evaluation with inference from international standards.**

Keywords-component; Digital Forensics Investigation Models, Cybercrime, Relativism, Pre-Search Warrant, Post-Seizure Warrant.

I. I. INTRODUCTION

Digital Forensic Investigation cases are normally intended to appear in court. The challenges of implementing FDI models, techniques and processes for investigation have proved daunting. In the event of cybercrime, issues of how to apply the digital forensic methodology to crime scene investigation for the purposes of presenting the evidence in a court of law has been the most challenging. Vacca 2005, posits that digital forensics investigation is a relatively new science and the discipline involves similar techniques and principles to data recovery, but with additional guidelines and practices designed to create a legal cyber audit trail [1]. Therefore, investigators are required to follow a proper chain-of-custody in a consistent and methodical approach. Since 1984, The FBI Labs has established the Computer Analysis and Response Team to oversee the formulation of procedures for evidence seizure as survey report revealed that 70% of digital forensics procedures were without proper written procedures [2]. A group of six international law enforcement agencies met with several US federal law enforcement agencies to discuss computer forensic science and the need for a standardized approach to examination. In 1993, an International Law Enforcement Conference held on Computer Evidence and about 70 representatives of US law enforcement agencies and international law enforcement agencies attended. Other conferences were held in Maryland, and the Scientific Working Group on Digital Evidence (SWGDE) was formed after 1995, Australia 1996 and Netherlands 1997 [1]. All the participants agreed that standards for computer forensics science were lacking and are needed. However, due to the invincibility nature of cybercrimes and the evolving threat landscapes DFI remains a challenge. For a case to be admissible in court, it must meet the required, structure and accept methodical approach to digital forensic investigations. [3] Posits that the need for a standard framework for digital forensics has been realized and understood. However, little progress has been made on the accepted model to solve that challenge. Computer forensic investigations the use of scientifically derived and proven methods towards the identification, preservation, collection, validation, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources [4]. Emerging economies, in its quest to govern by the rule of law, must have a structured model that assists in electronic evidence and forensic investigations in its ecosystem to track the trails of the cybercriminals.

The goals of digital forensics are to examine digital media in a forensically sound manner with the aim of identifying, preserving, recovering, analyzing and presenting facts and opinions about the information to law enforcement agencies, to Corporations, to individuals and in a court of law[5]. The key challenges are technical, legal, and cultural.

- **Technical Challenges**: Lack of expertise, technically competent and certified investigations is a major factor. Similarly, the challenge of using obsolete tools and lack of update procedures. Further, lack of reporting platforms and information sharing platforms to create awareness of the threat landscape, vulnerabilities, risks, and impact.

978-1-7281-7417-4/19/$31.00 ©2019 IEEE
DOI 10.1109/ICSIoT47925.2019.00023

- **Cultural Challenges**: Cultural Challenges: Cultural relativism stated that what is right and wrong depends upon society's actual moral guidelines [6].
- **Legal Challenges: The** procedures **challenge** to ensure evidence gathered is authentic, accurate, complete and convincing (AACC) to the juror. The challenges of bridging the gap between the judiciary, the law enforcement agencies, and the investigators [8] [9]. Post-seizure warrant ensures due diligence is followed after DFI procedures. A case in question was. In 2012. Economic and Organized Crime Office (EOCO)-vrs-GFA [8] [9]. Nigerians-vrs-GAF [11]. The ETA 2008 is limited in its implementations.

A. Roles Computers Play in a Cybercrime

The computer can be used as a target of a crime, the instrument of a crime or as an evidence repository or play multiples roles [10]. Further, it can also play the role of a victim and a perpetrator [4]. In 2012, two men we arrested for hacking into the emails systems of the Ghana Armed Forces and intercepted, interrupted, modified and fabricated

The aim of the paper is to develop a DFI model that is able to provide standard procedures for the DFI method in emerging economies. The research focuses on these four areas: (1) Models that are specific to a particular jurisdiction, (2) Models that are specific to a particular Analysis. (3) The Models that included Pre-search and Post-seizure. (4) Models that did not include the preservation phase as a legal requirement in the first phase and the extraction phase.

The novelty contribution of this paper is threefold: First, we develop a comprehensive digital forensic investigation model that will conceptualize and provide an understanding of the nature of cybercrimes. Secondly, we provide a knowledge base in the area of DFI reforms and assist in bringing together the judiciary, the law enforcement agencies, expert witnesses, the academia as well as investigators. Finally, the proposed model that will integrate DFI standards for all stakeholders. The evaluation and applicability of the proposed model will is based on expert judgment. The phenomenon, uncertainty and invincibility nature of cybercrimes are such that there is no single investigation that would support or refute DFI cases without a hypothesis. Therefore, our result has shown the need to develop the proposed model.

II. RELATED WORKS

This section discusses the state of the art and related works on the subject of relativism in cybercrime cases, the digital forensic investigation models and the existing international standards.

A. Relativism in Cybercrime and Digital Forensics Investigations

The concept relativism considers how different ideas and opinions are relative to various perceptions. Baghramian, et al 2015, define relativism as standards of reasoning and procedures of justification and the context giving rise to them [12]. Quinn 2013, posits that relativism as universal norms of right and wrong and that every society has rules of conduct describing what people ought and ought not to do in various situations [6]. Cybercrimes can be committed from anywhere in the world. However, the relativity of laws in various countries demonstrates the legal complexities and challenges of cybercrime investigations and the need for a model that fits a system *subjectively* and culturally. UNODC 2013, report on cybercrime stated that some law enforcement agencies may have well-organized cyber units in other jurisdictions, others barely have a few trained officers [5]. Emerging economies are in the process of emerging standard models and legal framework for the law enforcement agencies, the judiciary, and forensic investigators. The rationale for committing cybercrimes are relative to different jurisdictions and can be subjective and objective. DFI procedures and guidelines may vary from place to place and from time to time. Hence, the proposed model will consider challenges from emerging economies' perspective.

B. Existing DFI Models

Digital Forensics models are a set of guidelines and processes that provide a concise concurrent, abstract and mutual understanding on which technical process can progress. [13]. There are existing models that assist various countries to arrest and prosecute cybercriminals. For instance, the FBI, United States Department of Justice and the Department of State in collaboration with other Security Agencies has put in place a model that assists in the arrest, investigation, and prosecution of cybercriminals. [1] [14]. In the United Kingdom, the Association of Chief Police Officers (ACPO) in collaboration with the other law enforcement agencies, EC Council and Council of Europe (CoE), have digital forensic investigators and Law Enforcement Agencies they use to model in cybercrime cases. [15]. The Italian Model ensures that cybercrime cases and perpetrators are investigated using their model [16]. The Malaysian Model ensures that investigators use that model in line with their legal framework [17].

C. International Standards

There are several existing bodies that provide comprehensive guidelines, collaborative support, and idealized models for all digital forensic investigations and electronic evidence. We review some of these standards and compare them qualitatively to our proposed model as follows. ISO/IEC 27037 is designed for incident responses. To maintain the integrity and authenticity of digital evidence and provides guidelines for specific activities in preserving and handling potential digital evidence 18]. ISO/IEC 27041 provides assurance that incident management, evidence handling, storage and methods used in the investigative process are appropriate for the incident under investigation and the required results [19]. ISO/IEC 27042 provides a comprehensive guide to ensure that tools, techniques, and methods used provide guidance for on the conduct of the analysis and interpretation in order to identify and evaluate digital evidence to aid understanding of an incident. in relation to ISO 27037 [20]. ISO/IEC 27043 provides guidelines for pre-incident to post-incident preparations that

encapsulate idealized models across various scenarios in order that investigations can are repeated across every scenario and may obtain the same result [21]. International Laboratory Accreditation Cooperation (ILAC) 2014, forensic science laboratory that provides accreditations, guidance on the crime scene, examination and analysis that are consistent with ISO/IEC 17020 and 17025 [22]. Convention on Electronic Evidence (CEE) 2016, is a treaty that deals with the status of electronic evidence, covering civil and criminal proceedings, investigations and examination of electronic evidence, general provisions regarding the recognition and admissibility of electronic evidence from foreign jurisdictions. The aim of CEE is to encourage judges and lawyers to appreciate the concepts of evidence in electronic form [23]. NIST SP800-86 provides guidelines for forensic capability, including the development of policies and procedures. It focuses primarily on forensic techniques in incident response and investigations [24].

D. Rationale for the Proposed Model

The rationale for the proposed model is that the challenges of preserving digital evidence in the context of cybercrime have become ever more predominant, as law enforcement agencies increasingly face the question of what it means to ensure AACC [5]. The issue raised by the UNODC and the challenges raised above provides a rationale to have a DFI model

III. APPROACH

Digital forensics investigations methodologies are continuously evolving as the threat landscapes are also evolving. Tools and techniques for attacks are becoming sophisticated and obfuscating. We reviewed the existing models, identify existing gaps and propose a relative model that incorporates the emerging economies. [26]. Data were gathered from various online sources such as journals, articles, conference papers, and books. We reviewed 32 models from 1995 to date that is in existence from various, countries, academics and researchers. We used a descriptive and narrative approach to search for journals and articles from various databases and search engines.

A. Review of Existing Digital Forensic Investigation Models

Having the right DFI model in place to carry out investigations has been the most challenging as the threat landscape keeps changing. Different models exist due to the factors of relativism. We reviewed 32 models from 1995 to 2017 and categorized them according to their use. [3] [27]. The review considered four key areas Phases, Specific, Generic, Relative.

- Process Phase: indicates the number of phases in a model used for the investigation process.
- Specific: indicates whether the model is specific to jurisdiction or type of investigation.
- General: considers the model as general to all types of investigations.
- Relative: determines whether a model is relative to an area, lacks forensic purpose, includes Pre & Post seizure warrants. Not authentic, accurate, complete and convincing (AACC) to the juror.

We discuss the relevance of the models listed figures below in relation to the four criteria listed in sections following it and the literature reviewed.

No	Digital Forensic Models	Author	Year	Process Phase
1	Computer Forensics Investigation Processes Model (CFIPM)	Pollit M. M	1984	Four Phase Process Model
2	US Department of Justice Model (USDOJ) & NIJ	Reith et al.	2001	Five Phase Process Model
3	Digital Forensic Research Workshop (DFRWS)	Palmer G.	2001	Six Phase Process Model
4	Scientific Crime Scene Investigation Models (SCSI)	Lee et al.	2001	Four Phase Process Model
5	Abstract Digital Forensic Model (ADFM)	Reith, Carr & Gunsch	2002	Nine Phase Process Model
6	Integrated Digital Investigation Process (IDIP)	Carrier & Spafford	2003	Five Phases Process Model
7	A Comprehensive Approach to Digital Incident Investigation	Stephenson	2003	Nine Phases Process Model

Figure 1. Types of Investigative Models Reviewed

Specific	Generic	Relative
	General to all types of cybercrimes. To US Standards of investigations	Did not include Physical Preservation of crime scene at first phase and extraction phase
US Legal Framework and Standards for all States		Did not include Physical Preservation of the crime scene as the first phase and extraction phase
	General to all types of cybercrimes	To International Standards. Requires Localized legal Pre & Post warrants
	General to all types of cybercrimes	Lacks digital forensics crime scene phase such as preservation phase procedures
	General to all types of cybercrimes	Expounded on the DFRWS Model by three more phases. But model looks cumbersome; may stall investigations
	General to all types of cybercrimes.	Did not include Preservation of Physical crime scene as the first phase and extraction phase
Specific to Network crimes and live analysis methods and techniques		No preservation phase. may cause evidence altering Not fit for dead analysis

Figure 2. Extension of figure 1.

No	Digital Forensic Models	Author	Year	Process Phase
8	Digital Forensics Framework Model (DFFM)	Casey	2004	Four Phase Process Model
9	Enhanced Digital Investigation Process (EDIP)	Baryameeree ba & Tusabe	2004	Five Phase Process Model
10	Extended Model of Cyber Crime Investigations (EMCI)	Ciardhuain	2004	Thirteen Phase Model
11	A Hierarchical Object-Based Framework for Digital Forensics Investigation (HOBFDFI)	Beebe and Clark	2004	Six Phase Process Model
12	Event-Based Digital Forensics Investigations (EBDFI)	Carrier & Spafford	2004	Five Phase Model
13	Case Relevance Information Model (CRIM)	Ruibin & Chan Kan Tun	2005	Five phase Model
14	Computer Forensics Field Triage Process Model (CFFTPM)	Rogers M.K. et al	2006	Six Phase Model. With three sub-phases on 3rd & 5th
15	NIST Forensic Process Model (FPM)	Kent, K. et al	2006	Four Phase Model
16	Framework For Digital Forensics Investigations Model (FDFIM)	Kohn et al.	2006	Three Phase Model

Figure 3. Continuation of types of Investigative Models Reviewed

Specific	Generic	Relative
Generic Model Preservation is more a process		No Physical Preservation of the crime scene as the first phase.
	Iterative model and can Traceback all the processes in the model	EDIP to replace the IDIP Model Did not include Preservation of Physical crime scene as the first phase and extraction phase
	Generic Expounded on different models added six more phases	Broad, may cause delays. No preservation phase. May cause evidence altering
	Generic Model and similar to those referenced in their paper.	The incident response phase does not include the preservation of the crime scene. processes may compromise on AACC
	Generic to live and dead analysis	The model did not address issues of preserving the physical crime scene
	More of the generic and conceptual model than practical	Live and dead analysis address. No preservation phase. May cause evidence altering
Specific to browser and email analysis methods. Differ when building cybertrail		Did not include the Preservation of Physical crime scene as the first phase and extraction phase. will suit Live Analysis
	Generic and may lack integrity in forensic investigation	Did not include securing the crime scene to preserve digital evidence

Figure 4. Extension of figure 3

No	Digital Forensic Models	Author	Year	Process Phase
17	Dual Data Analysis Process (DDAP)	Bem and Huebner	2007	Four Phase Model
18	Common Process Model For Incident and Computer Forensics (CPMICF)	Freilings & Schwittay	2007	Three Phase Model
19	Mapping Process of Digital Forensics (MPDF)	Rahayu et al	2008	Five Phase Model
20	Building a Digital Forensic Lab	Jones & Valli	2009	Four Phased Model
21	Digital Forensics Model Based on Malaysian Investigation Process (DFMMIP)	Perumal, S.	2009	Seven Phase Model
22	Overall Digital Forensic Investigations Process	Harrell C	2010	Six Phased Model
23	Network Forensic Generic Process Model (NFGPM)	Pelli et al	2010	Eight phased model
24	Generic Computer Forensic Investigation Model (GCFIM)	Yusoff et al.	2011	Five Phase Model

Figure 5. Continuation of types of Investigative Models Reviewed

Specific	Generic	Relative
Specific to analysis only complicated and lacks the verbs needed for the phases	.	No preservation phase may cause evidence altering. Limited in functionality as the phases lack legally required AACC
	Generic model, complicated and lacks the verbs needed for the phases	Cumbersome and may slow down investigations, does not address the issues of preservation
	Generic process model to all cases	No preservation of physical crime scene in phase 1 and preservation of digital crime scene in phase 3 as required
	Generic process model to all cases, limited in functionality	No Preservation of crime scene 1 phase, cannot correlate evidence that ensures chain of custody
Specifically for the Malaysian investigators		Adopted to Malaysian Legal Framework, No Preservation of crime scene 1 phase
	Generic and looks more of a process than a model.	Preservation should be a phase on its own not a sub-phase as it is a legal requirement
specific to live analyses		Has the collection phase before Preservation phase, which may cause evidence altering
	Generic and looks more of a process than a model.	Pre-process to post-process must be done outside a model. No preservation phase in the first phase. May cause evidence altering

Figure 6. Extension of figure 5

No	Digital Forensic Models	Author	Year	Process Phase
25	Proactive & Reactive Digital Forensics Process (PRDFP)	Alharbi. et al,	2011	Eleven Phase Model
26	Systematic Digital Forensics Investigation Model (SDFIM)	Agarwal et al	2011	Eleven phase model
27	A New Approach of Digital Forensics Model.	Ademu et al.	2011	Four Phased Model
28	Conceptual Model for Digital Forensics Investigation Readiness (CMDRIR)	Pooe & Labuschagne	2012	Four Phase Model
29	Comparative Digital Forensics Model	Kalbande & Jain	2013	Five Phases Model
30	A Model For Hybrid Evidence Investigation (MHEI)	Vlouchopulos et al	2014	Four Phase Model.
31	Domain-Specific Cyber Forensics Investigations Model (DSCFIM)	Saati & Jafari	2015	Ten phase model
32	Harmonized Process Model for Digital Forensics Inv Readiness (HPMDFIR)	Valjarevic & Venter	2017	Three phase Model

Figure 7. Continuation of types of Investigative Models Reviewed

Specific	Generic	Relative
	Generic process may require much time to implement	Limited to Live analysis only. No preservation phase as the first phase
	Generic model relatively similar to others	Minimize the stages and to reduce complexities in the investigation processes
	Generic model and not explicit.	Did not address the issues of preservation of the crime scene
	Generic model Tailored to suit an organization security policy	The people phase of the model should not be included. may limit scope of applicability, legally and in a forensically sound manner
	Generic and lacks the right verb required when emerging a model	Issues of legal warrants must be dealt with before a cybercrime incident occurs
	Generic for digital crimes.	Processes that emphasis on both physical and digital crime scene
Specific to institutions and requires rigorous policy and process flow		Functionalities specific to academic institutions
	Generic model harmonizes in implementation	Process look cumbersome lacks consistency and does not follow the scientific process

Figure 8. Extension of figure 7

B. *Synthesis Methods*

This section synthesis figure 1 to figure 8 comparatively and analyzed it quantitatively to determine the differences in the models. The rationale is to review the existing models to provide an overview of their relative importance and effectiveness.

C. *Comparative Analysis*

The study emphasized the main phase that ensures authenticity, accuracy, complete and convincing. For instance, ACPO updated the Good Practice Guide for Computer Based Electronic Evidence to include Preservation of Evidence by recognizing the phenomenon, evolving nature of cybercrime and digital evidence [12]. The study revealed seven models that are specific to a particular jurisdiction includes [17], [29], [33], [37], [40], [45], [52].

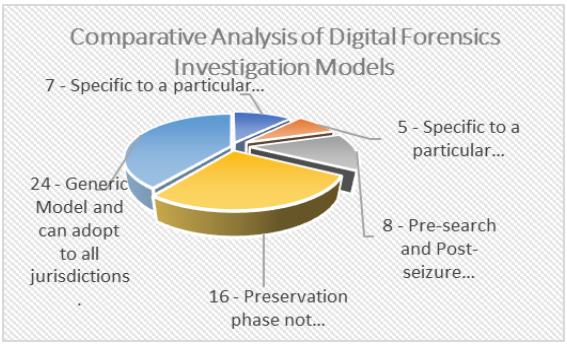

Figure 9. Comparative Analysis of Digital Forensic Investigations Models

However, two of the models are specific to particular jurisdiction [17], [31], four of them were specific to live analysis only [5], [33], [45], [45]. With models that are specific to cybercrime investigation and analysis such as cyber physical systems, network, digital and hard drive forensics, the study reveals five models [33], [36], [37], [40], [50]. However, the models did not address the issues of live and dead analysis, were generic and conceptual model.

D. *Evaluations and Findings*

There are the number of phases of each model that an investigator must apply and the specificity of a model to a particular jurisdiction determines how the model relates to others in its implementation. The comparative analysis revealed 16 of the models that did not include the Preservation phase as a legal requirement in the first phase and also at the Extraction phase comparatively to the initiative taken by the ACPO to include preservation phase [10]. Therefore, they did not ensure scientific, consistent and legally deployed DFI evidence models that ensure can authenticity, accuracy, completeness and convincing to a juror. Further, the study has also revealed the lack of standards in the models globally that indicates how that is affecting the digital forensic investigation. Furthermore, the analysis reveals that lack of standards, expertise, lack of legal framework, lack of education in the field DFI models and evidence gathering procedural tools and techniques has caused a lot of misinterpretation of cybercrime procedures. Therefore, we justify why a team of experts is required to collaborate and formulate laws and procedures for pre-

seizure and post-seizure warrants as a key requirement. However, that should not be part of the DFI model.

IV. PROPOSED-RELATIVISM DIGITAL FORENSICS INVESTIGATION MODEL

In this section, we develop the proposed model based on the existing gaps. Due to the global nature of cybercrime, the UNODC proposed a provision of the international model on investigative powers for the preservation of electronic evidence [43] with the view to supporting states in ensuring the necessary procedural tools and investigation of cybercrime are applied. We propose the model below to assist in meeting the UNODC proposal. The proposed model has seven phases namely Preservation, Identification, Transport, Extraction, Analysis and Report Writing with Documentation linked to all the six phases to ensure consistency, chain of custody and due diligence. The identification phase has two sub-phases linked to it namely Live Analysis and Dead Analysis and also the Acquisition phase has three sub-phases Digital Preservation, Extraction, and Evidence Search. We explain the processes as follows.

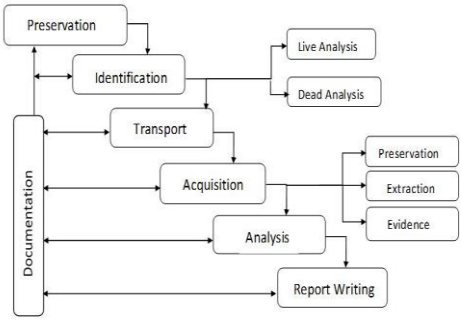

Figure 10. Relativism Digital Forensics Investigation Model (RDFIM)

The (RDFIM) model we propose that has taken into consideration the preservation of the physical crime scene and the preservation of the digital evidence. The model emphasizes the phases and not so much on the sub-processes as the nature of the cybercrime may determine the processes required. We explain the phase as specified in figure 10:

A. Preservation Phase

The preservation phase requires that the investigators preserve the state of the physical crime scene by securing the environment and prevent evidence from being altered and corrupted. Take pictures of the crime scene before the evidence is gathered. Acquire a pre-seizure warrant from authorities before the physical and digital crime scene investigation. The has to be a legal template proactively prepare by the court. However, there are no procedures in place to get a pre-search warrant, as there are no standards in place currently. This phase will consider standard references from ISO\IEC 27037, ILAC 2014, CEE 2016.

B. Identification Phase

This identification phase establishes whether cybercrime was requires live Analysis or dead Analysis after securing the crime scene. Live analysis requires the use of live forensic tools and intelligent hubs and switches to keep the systems running whilst carrying out a live investigation on the operating system or other resources under investigation to find evidence. Further, the investigator is required to unplug the hub and connect it to an intelligent one whilst investigations continue. The software can falsify evidence or maliciously hide data in situations where a spyware infection or honeypot could be involved. Furthermore, a dead analysis occurs where the incident has occurred, and the systems are shut down already. Here the investigator must secure the evidence by taking pictures of the digital device under investigation before evidence is gathered. This phase will consider standard references from ISO\IEC 27041 and NIST800-86 for identifying live or dead analysis, ISO\IEC 27042 for tools used in the live analysis.

C. Transport Phase

The transport phase requires that digital media be transported to the forensic lab for extraction of evidence in dead analysis. Evidence could be tampered with to the lack of procedures, training, and expertise. Similarly, there are issues of inappropriate forensics tools and laboratory facilities. Currently there is lack of procedures in place for law enforcement agencies and investigators to follow when handling digital evidence in transition [16]. There have been instances where the law enforcement agencies have appeared at the crime scene, arrested the criminals, seize the computers, and digital media and taken them to the police station and have left them there without further procedures. This phase will consider standard references from ISO\IEC 27037, 27043, ILAC 2017. CEE 2016 legal and standard guidelines for the preservation of evidence in transit from the crime scene to the Forensic Lab.

D. Acquisition Extraction Phase

The acquisition or extraction phase is more technical and involves the preservation of digital evidence before data extracting evidence in a live or dead analysis environment. Further, to ensure due diligence, the investigator will have to preserve the physical evidence before the extraction of digital evidence. Similarly, it is required that evidence extracted is compared with the initial preservation done in the first phase. The rationale is to answer the 'what if' questions supposed the computer has been swapped in transit. Furthermore, maintaining evidential integrity and applying due diligence as well as ensuring chain of custody include:

- Taking pictures of the computer and digital media
- Compare them against the original pictures taken at the initial preservation phase of the crime scene.
- Preserve the digital media use the write blocker tool to protect the data from being overwritten too, before the extraction of the evidence from the digital media.
- Protect the mirror image of the evidence extracted.
- Save the original evidence and apply hashing functions on the evidence.
- Calculate the cryptographic hash to check that the data has not changed from the original state.

Defining the general characteristics of the object we are searching for. Furthermore, we look for the object in the data collected that supports or refutes the hypothesis of the incident by searching through the cyber trail. For instance, in analyzing web browsing habits or files with certain extension names such as html or .jpg. that may be used to reconstruct evidence. This phase will consider standard references from ISO\IEC27037, ISO\IEC 27043, ILAC 2014. ISO\IEC:17025, ISO\IEC 17020.

E. Analysis Phases

Analyzing digital evidence involves assessing digital data objectively, hypothetically and critically, to understand what has transpired before we could draw a conclusion about the nature of a crime that supports or refutes the hypothesis. Here the source of digital objects is evaluated by applying the concepts of preservation of digital evidence, isolate the original evidence from the analysis data, correlate the evidence with the original evidence gathered and that of peers and expert witnesses. Further, we analyze the extracted data to identify unfamiliar file formats and look for the timeline to identify sequences and patterns in the time of the event. Furthermore, this is to determine what happened, where it happened. Moreover, we perform gap analysis and functional analysis to ascertain what was possible and impossible to know who was involved and how it happened. For instance, whereas a user is using the system, a 'pop up' may pop up on the screen, then whilst trying to close the pop-up, the user may end up opening it. Suppose there is a virus attached to the pop up, it may spread to other network systems. Thus, this attack may require analytical evidence to prove it. This phase will consider standard references from ISO\IEC 27042, ILAC 2014, ISO\IEC 27043, NIST 800-86 and issues of redaction.

F. Documentation Phase

Documentation of the digital forensics process ensures that there is continuity of evidence or chain of custody from the preservation of crime scene phase to report writing phase. Hence, the documentation phase is linked to all the phases. The rationale is that it ensures due diligence as it must be possible to account for all that has happened to the exhibits from the very onset of the investigation. Further, the process of documenting evidence from when the investigator appeared at the crime scene to the time the case appeared in court ensures evidential integrity. Therefore, failure to document the evidence at the crime scene in its present time could lead to incorrect record-keeping and information altering. Record dates, time, questions asked, findings, interview suspects and gather hypothesis. The evidence should be authentic, accurate, and consistent and complete such that expert witness should be able to analyze the same evidence and come up with the same result. This phase will consider standard references from ISO\IEC 27037, ILAC 2014. ISO\IEC 27043, NIST 800-86.

G. Report Writing Phase

This phase involves generating a report that is consistent with legal proceedings and documents all evidence to be used in court. It contains evidence collated, report of findings presentable to the stakeholders including law enforcement agency, court, individuals, incidence responses teams and eDiscovery. The report must be authentic, accurate, complete and convincing to the juror. The report and information contained in the documents must be correlated with the pre-seizure and post-seizure warrants document. This phase will consider standard references from ISO\IEC 27043, CEE 2016, ISO\IEC 27042, ILAC 2014, NIST 800-86. ISO\IEC 17025, ISO\IEC 17020. Moreover, these standards provide guidelines for documenting and references for the report writing phase and what is required in the report.

V. CONCLUSION

Digital Forensics investigations are concerned primarily with forensic procedures, rules of evidence gatherings and legal processes that must be applied in the digital crime scene environment. The study reviewed a causal understanding of expert opinion on digital forensics investigations models. The analysis has revealed that opinion and perception vary at every jurisdiction in that, existing digital forensic investigation models are relative to the culture, thinking patterns and the application of the legal framework. The proposed model is designed specifically to suit the culture and mindset of the emerging economies. The invincibility nature of cybercrime and digital evidence requires that experts from the judiciary, law enforcement agencies, systems security experts, expert witnesses, academics consultants, and industry practitioners are brought together to develop a scientific pre-search warrant for the court. The study has revealed that obtaining pre-search and post-seizure warrants before appearing at the crime scene will ensure legal proceedings apply in digital evidence gathering process. RDFIM, with consideration from international standards, will enhance handling electronic evidence in the emerging economies, improve investigation processes effectively and efficiently as well as support investigation procedures in handling digital evidence independently and collaboratively. RDFIM can be used to formulate and formalized security policies after investigations. The threat landscape is evolving, and threat actors are deploying sophisticated methods. The study focused mainly on the key phases of each digital forensics' investigation model and not more on the processes. Hence, further study is required to review the phases, various implementation processes and procedures to harmonize digital forensics investigations processes efficiently and effectively.

REFERENCE

[1] J. R. Vacca. "Computer Forensics – Computer Crime Scene Investigation". 2nd Edition. ISBN: 1-58450-389-0. 2005.

[2] M. G., Noblett, L. A., Presley, M. M.: Pollitt. "Recovering and Examining Computer Forensic Evidence: Forensic Science Communications". Vol 2, No. 4, 2000.

[3] B. D. Carrier, and E. H Spafford. "An Event-Based Digital Forensic Investigation Framework". Proceeding from Digital Forensics Research Workshop. Center for Education and Research in Information Assurance and Security – CERIAS. Purdue University. USA, 2004.

[4] A. Valjarevic and H. Vente. “Harmonized Process Model for Digital Forensics: Investigation Readiness”. 9th International Conference on Digital Forensics. IFIP Advances in Information and Communication Technology. AICT-40, pp, 66-82. 2013.

[5] United Nations Office on Drugs and Crime (UNODC). “A Comprehensive Study on Cybercrime: Harmonizing of National Frameworks”. 2013.

[6] M. J.: Quinn. “Relativism in IT Professional Ethics” Ethics for the Information Age, 5th Edition. Pearson Addison Wesley, 2013.

[7] S. K. Orin. “Search Warrant in An Era of Digital Evidence”. 75 Mississippi Law Journal 85. University of South Carolina Gould School of Law. 2005

[8] Economic and Organized Crime Office. Court: “EOCO raid on GFA illegal, fined Gh¢50,000”. 2015.

[9] Economic and Organized Crime Office raid GFA office. 2010.

[10] E. Casey. “Digital Evidence and Computer Crime”. Forensic Science, Computers and the Internet. 2nd. Edition. Elsevier Academic Press. ISBN: 9780080475508. 2004.

[11] Ghana Business News: “Ghana Army Emails Hacked, Two Nigerians Arrested”. 2012.

[12] M. Baghramian and J. A Carter. Relativism, “The Stanford Encyclopedia of Philosophy” Winter Edition. 2018

[13] S. Saleem, O. Popov, and I. Bagilli: “Extended Abstract Digital Forensic Model with Preservation and Protection as Umbrella Principles”. International Conference on Knowledge Based and Intelligence Information & Engineering Systems. 2014.

[14] V. Baryameereeba and F. Tusabe. “The Enhanced Digital Investigations Process Model”. In Proceeding of Digital Forensic Research Workshop, Baltimore, MD, USA. 2004.

[15] Association of Chief Police Officers. “ACPO Good Practice Guide for Digital Evidence”. 2012.

[16] G. Fenu And F. Solani. “Computer Forensics Investigations: An Approach to Evidence In Cyberspace”. 2013.

[17] S. Perumal. “Digital Forensics Model based on Malaysian Investigation Process”. IJCSNS. Vol. 9 No. 8. 2009.

[18] ISO \IEC 27037:2016. “Information Technology Security Techniques, Guidelines for Identification, Collection, Acquisition, and Preservation of Digital Evidence”. 2016.

[19] ISO \IEC 27041:2016. “Information Technology Security Techniques, Guidelines on Assurance Suitability and Adequacy of Incident Investigative Method”. 2016.

[20] ISO \IEC 27042:2016. “Information Technology Security Techniques, Guidelines for the Analysis and Interpretation of Digital Evidence”. 2016.

[21] ISO \IEC 27043:2016. “Information Technology Security Techniques, Incident Investigation Principles, and Processes”. 2016.

[22] International Laboratory Accreditation Cooperation (ILAC), (2014).https://ilac.org/latest_ilac_news/ilac-g19082014-published/

[23] Draft Convention on Electronic Evidence. (2016). http://journals.sas.ac.uk/deeslr/article/viewFile/2321/2245

[24] K. Kent, S. Chevalier, T. Grance and D. Dang. “Guide to Integrated Techniques into Incident Response”. NIST. Computer Security Division. IT Laboratory. Publication 800-86. 2006.

[25] D. Kowalczyk. “Purpose of Research: Exploratory, Descriptive and Explanatory”. 2005.

[26] M., Dolores and C. Tongo. “Purposive Sampling as a Tool for Informant Selection”. A Journal of Plants, People and Applied Research. Ethnobotany Research & Application 5-147-158. 2007.

[27] Pollitt, M. M.: Computer Forensics: An Approach to Evidence in Cyberspace: In Proceeding of the National Information Systems Security Conference, Baltimore, MD, Vol. II, pp 487-491. 1995.

[28] National Institute of Justice. Electronic Crime Scene Investigation: A Guide for First Responders. 2001.

[29] G. Palmer. “DTR-T001-01 Technical Report. A Road Map for Digital Forensics Research”. Digital Forensics Workshop, Utica, NY. 2001.

[30] H. Lee, T. Palmbach and M. T. Miller. “Crime Scene handbook”. New York. Academic Press. 2001.

[31] M. Reith, C. Carr. and G. Gunsh. “An Examination of Digital Forensics Models” IJDE, Vol, No. 3. 2002.

[32] B. Carrier and E. H. Spafford. “Getting Physical with the Digital Investigation Process”. IJDE, Vol, 2. No. 2. 2003.

[33] P. Stephenson. “A Comprehensive Approach to Digital Incident Investigation” Information Security, Technical Report, Vol, 8, Issue 2, pp42-45. IJCSIT Vol, 3 No, 3. 2003.

[34] S. Ciardhuain. “An Extended Model of Cybercrime Investigations: IJDE, Vol, 3. No. 1. pp. 1-22. 2004.

[35] N. L Beebe and J. G. Clark. “A Hierarchical, Object-Based Framework for the Digital Investigation Process” In Proceeding of Digital Forensic Research Workshop (DFRWS) Baltimore, Maryland. 2004.

[36] G. Ruibin and M. Gartner. “Case Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensics Framework”. In Proceeding of Digital Forensics Research Workshop, Baltimore, MD. 2005.

[37] M. K., Rogers, J, Goldman, R. Mislam, T. Wedge T and S. Debrota. “Computer Forensics Field Triage Process Model”. Presented at the Conference on Digital Forensics, Security and law, pp 27-44. 2006.

[38] M. J. Kohn, H. P. Eloff. And M. S. Olivier. “Framework for A Digital Forensic Investigation”, In Proceeding of ISSA 2006 from Insight to Foresight Conference, Sandton, South Africa. 2006.

[39] D Bem. And E. Huebner. “Computer Forensics Analysis in a Virtual Environment: International Journal of Digital Evidence”, Vol. 6, No. pp 1-13. 2007.

[40] Freilings F. C., Schwittay, B. “Common Process Model for Incident and Computer Forensics” In Proceeding of the Conference on IT Incident Management and IT Forensics, Stuggart, Germany, pp. 19-40. 2007.

[41] S. R. Rahayu, R. Yusof. S. Sharib. “Mapping Process of Digital Forensics Investigation Framework”. IJCSNS. Vol. 8. No. 10. 2008.

[42] A. Jones and C. Valli. “Building a Digital Forensics Laboratory Establishing and Managing a Successful Facility”. Burlington, MA. Elsevier, Inc. ISBN 13: 978-1-85617-510-4. 2009.

[43] C. Harrell. “Overall Digital Forensics Investigation Process”.2010.

[44] E. S. Pilli. R. C. Joshi and R. Niyogi. “Network Forensics Framework: Survey and Research Challenge Digital Investigation”. Vol. 7 pp. 14-27. 2010.

[45] S. Alharbi, J. Weber-Jahnke and T. Traore. “The Proactive and Reactive Digital Forensics Investigations Process: A Systematic Literature Review”. IJSA. Vol. 5 No. 4. 2011.

[46] A. Agrawal. M. Gupta and S Gupta. “Systematic Digital Forensics Investigations Model”. Vol, 5. 2011.

[47] I. O. Ademu, C. O. Imafidon and D. S.: Preston. “A New Approach of Digital Forensics Model for Digital Forensic Investigation”. IJSA. Vol 2, No. 12. 2011.

[48] A. Pooe and L. Labuschagne. “A Conceptual Model for Digital Forensic Readiness”. Information Security for South Africa. ISSA. Conference 2012

[49] A. Kalbande. N. Jain. Comparative Digital Forensics Model. International Journal of Innovation Research in Science, Engineering and Technology. Vol. 2. Issue 8. 2013.

[50] K. Vlachopoulos. E. Magkos. V. Chrissikopoulos. “Proceedings of the Seventh International Workshop on Digital Forensics & Incident Analysis”. Department of Informatics, Ionian University. Greece. 2014.

[51] Satti, R. S., Jafari, F.: Domain Specific Cyber Forensics Investigations Model: Journal of Advances in Computer Network, Vol. 3. No. 1. 2015.

[52] Yusoff, Y., Ismail, R., Hussan, Z.: “Common Phases of Computer Forensics Investigation Models” Proceeding of IJCSIT, Vol. 3. No. 3. 2011