International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Protection Against Cybercrime Through Digital Evidence: A Worthwhile Approach For Developing Countries

Md Rajib*

*Department of CSE, Military Institute of Science and Technology (MIST), Dhaka, Bangladesh

ABSTRACT

The wide-ranging usage of computer-based applications in our day-to-day life in all activities starting from business and pleasure has endangered us from numerous security threats like web-based social crimes, industrial espionage, burglary associated with intellectual properties, transgression by the corporate employee, and so on. Nowadays, individual persons, as well as public and private institutions, are frequently maltreated with varied sorts of cybercrimes. However, due to the absence of the required level of proficient investigation and follow-up of providing digital evidence, the case has become weak. It is more applicable for developing countries having a lack of technological advancement embraced with inclusive guidelines and framework to computer forensic investigators and analysts. The speedy growth of computer connectivity has provided openings for criminals to exploit security weaknesses in the online background. Most harmful are malicious and exploit codes that interfere with computer operations on a global scale and along with other cyber-crimes that threaten online-based e-commerce Therefore, there is a need for incorporating an implementable digital evidence-based crime scene investigation framework for developing countries to thwart Cybercrimes. The study has commenced with exploring the present-day Digital Evidence Management Framework (DEMF) of varied developing countries like India, Pakistan through Extended Model of Cybercrime Investigation Process (EMCIP), reviewed available DEMF in literature, and formulate a viable DEMF with effectual digital evidence to safeguard from cybercrime in developing nations with limited technology and resources

Keywords:

Cybercrime, Digital evidence(DE), Enhanced Digital Investigation Process(EDIP), Digital Evidence Management Framework(DEMF), Information and Communication Technology(ICT), Computer Forensic Investigative Process (CFIP) Certified Ethical Hacker (CEH)

1. INTRODUCTION

NowadaysCybercrimes are dyed-in-the-wool, however, due to lack of proficient investigation process and follow up of providing digital evidence, the case becomes feeble. Unfortunately, there is an insufficiency of information about the crime related to a computer is, and how to conduct a digital evidence-based investigation. A comprehensive guideline and framework for computer forensic investigators and analysts are missing for most of the developing countries due to lack of cutting-edge technology, skilled manpower, and economic scantiness. Therefore, there is a need for an apposite digital evidence-based delinquency investigation framework due to prevent the nexus of Cybercrime.In the process of developing the scope of the paper, fourteen different Digital Evidence-based Investigation processes have been reviewed. Crime scene investigators and forensic experts of different organizations were consulted utilizing varied online platforms (Google form). Four different types of cybercrimes like Hacking, Identity Theft, Cyber Fraud, and Phishing were taken out of numerous types of cybercrimes. Gaps within the existing law and involvements of white hackers are identified. In addition, the glitches of prevailing DEMF of different developing countries were patterned out at large to formulate an apposite digital evidence-based crime scene investigation framework viable for most of the developing nations fighting ceaselessly against the supercilious cybercrime of recent times.

1.1. ***Objectives of the paper*** The objectives of the paper are as follows:

1.1.1. To consult the cybercrime investigator, cyber lawmakers, and ethical hackers to know the practiced system of gathering digital evidence.

1.1.2. To examine the existing crime scene investigation framework or model available in other countries to provide the digital evidence.

1.1.3. To suggest a proper generally accepted crime scene investigation framework or models for digital evidence to safeguard cybercrime.

GLIMPSE ON DIGITAL EVIDENCE

2. Basic steps of Digital Evidence Management Procedure

2.1 "The *digital forensics process* involves the: search, acquisition, preservation, and maintenance of digital evidence; description, explanation, and establishment of the origin of digital evidence and its significance." [6]. With the passage of time varied digital forensics approaches have been formulated and embraced. In 2001, the Digital Forensic Research Workshop outlined an exhaustive DIP comprisedof seven phases all illustrated in figure 1 below:

Identification	Preservation	Collection	Examination	Analysis	Presentation	Decision
Event/Crime Detection	Case Management	Preservation	Preservation	Preservation	Documentation	
Resolve Signature	Imaging Technologies	Approved Methods	Traceability	Traceability	Expert Testimony	
Profile Detection	Chain of Custody	Approved Software	Validation Techniques	Statistical	Clarification	
Anomalous Detection	Time Synch	Approved Hardware	Filtering Techniques	Protocols	Mission Impact Statement	
Complaints		Legal Authority	Pattern Matching	Data Mining	Recommended Countermeasure	
System Monitoring		Losses Compression	Hidden Data Discovery	Timeline	Statistical Interpretation	
Audit Analysis		Sampling	Hidden Data Extraction	Link		

Figure-1: Basic steps of Digital Evidence Management Procedure
(Authors' self Construct)

In 2006, the United States National Institute of Standards and Technology proposed a four-phase digital forensics model (see Figure 3) in its Guide to Integrating Forensic Techniques into Incident Response (SP 800-86) (Kent et al., 2006, 3-1). Major Three steps are illustrated below:

2.2. *Capture/Acquisition*

To preserve the data and attain the best substantiation, these items need to be handled and seized aptly and should be treated with as much care as any other item that is to be forensically examined. Proportionality issues relating to the seizure, measures before and when attending a scene to capture digital evidence are to be kept in mind.[7] This is the most crucial part of the whole investigation process where the investigator presenting the case must be able to prove the following:

2.2.1. The data is authentic.
2.2.2. The copy of the data used for analysis is reliable.
2.2.3. The data was not modified during acquisition or analysis (chain of custody).
2.2.4. The tools used to analyze the data are valid tools.
2.2.5. Sufficient evidence, both incriminating and exculpatory, has been acquired and analyzed to support the proffered conclusion.
2.2.6. The conclusions are drawn are consistent with the data collected and analyzed.
2.2.7. People involved in the collection and analysis of the data are properly trained and qualified to do their job.

2.3. *Analyze*

It is impossible or undesirable to extract or retrieve all data from devices, due to the huge volume and intricacy of data stored on digital devices. A proper forensic strategy needs to be articulated to permit the investigation to be engrossed in the relevant data as an alternate means. Usually, "close coordination and collaboration with the Digital Forensic Unit will confirm that the importance of any premeditated data is not misinterpreted."[8].

2.4. *Presentation*

The proclamation or report is the final product of the total Digital Investigation Process(DIP). It should rough draft the overall investigation and evaluation process with substantial data which has already recovered. "At the same time as an initial report may be relatively brief, the practitioner should be in a position to produce a full technical report should one later be required." [9]

2.5 As shown in figure-2, the four steps are further broken down into more granular levels that represent processes that occur within each step. A more thorough study expands the model to six steps, as follows:

2.5.1. Identification/assessment
2.5.2. Collection/acquisition
2.5.3. Preservation
2.5.4. Examination
2.5.5. Analysis
2.5.6. Reporting

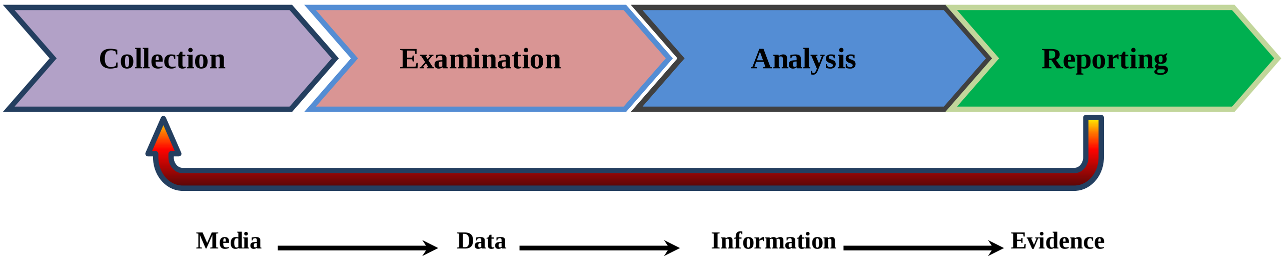


Figure-2: Digital Investigation Process(DIP)

3. Characteristics of Cybercrime

3.1 Given the unusual nature and impacts of cybercrime, its characteristics are all in all different from that of a conventional crime. In addition, The characteristics of cybercriminals, cybercrime victims, and law enforcement agencies have a reinforcing effect on each other, leading to a vicious circle of cybercrime. The characteristics of cybercriminals, cybercrime victims, and law enforcement agencies have created a vicious circle of cybercrime(Illustrated with figure –x below) which possesses a significant implication with overall characteristics of cybercrime and formulate a viable scheme of DIP in this regard. The main “characteristics of cybercrime.”[10] are appended in table 1 below:

3.1.1. Low risk high rewarding ventures.
3.1.2. Lack of awareness among victims.
3.1.3. Physical presence not required.
3.1.4. Victims refrain from reporting cases.
3.1.5. Non-violence approach.
3.1.6. Anonymity and Openness.
3.1.7. Paucity of authentic evidence.

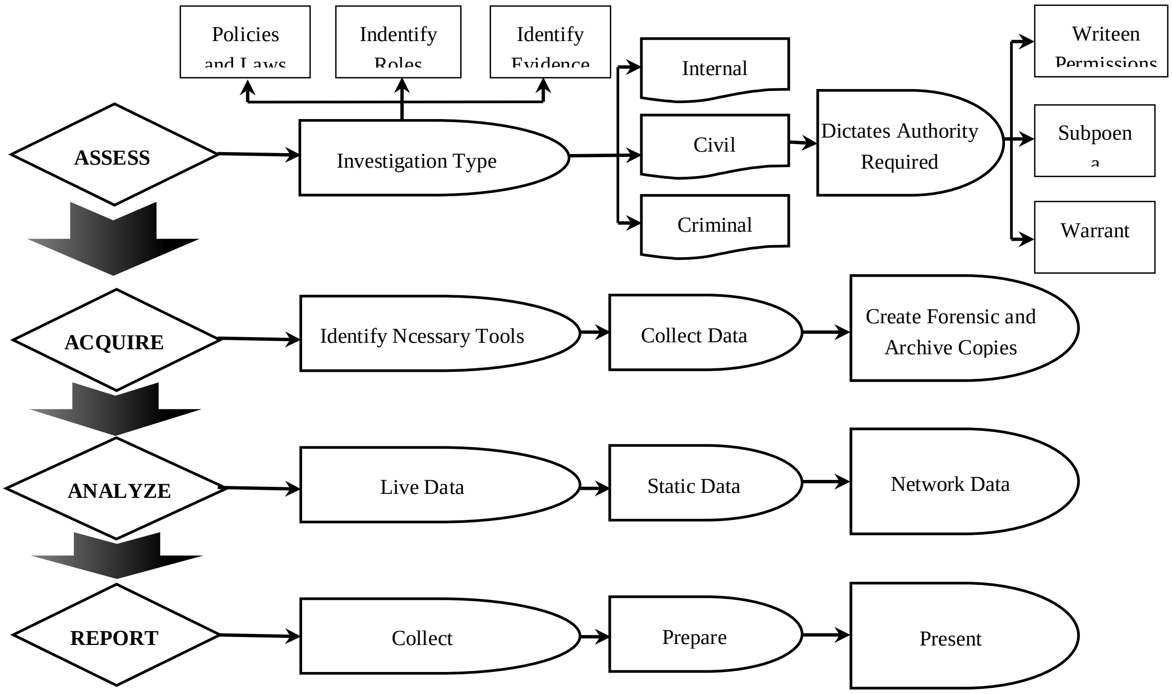


Figure-3: DEMF basing on trends of Cybercrime

3.2. In addition, The characteristics of cybercriminals, cybercrime victims, and law enforcement agencies have a reinforcing effect on each other, leading to a vicious circle of cybercrime. The characteristics of cybercriminals, cybercrime victims, and law enforcement agencies have created a vicious circle of cybercrime(Illustrated with figure 4 below) which possesses a significant implication with overall characteristics of cybercrime and formulate a viable scheme of DIP in this regard.

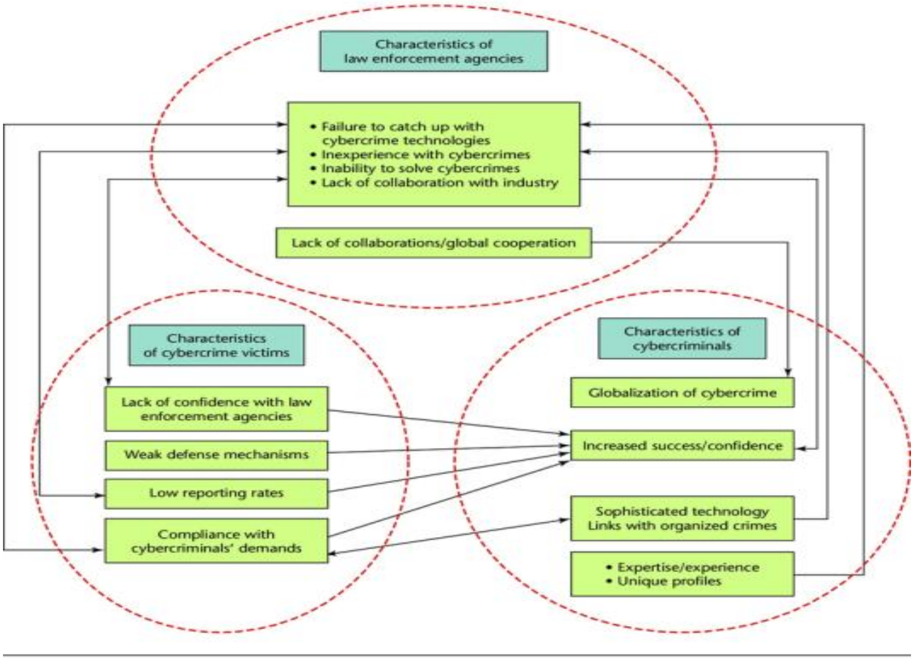

Characteristics of law enforcement agencies
• Failure to catch up with cybercrime technologies
• Inexperience with cybercrimes
• Inability to solve cybercrimes
• Lack of collaboration with industry
Lack of collaborations/global cooperation
Characteristics of cybercrime victims
Lack of confidence with law enforcement agencies
Weak defense mechanisms
Low reporting rates
Compliance with cybercriminals' demands
Characteristics of cybercriminals
Globalization of cybercrime
Increased success/confidence
Sophisticated technology Links with organized crimes
• Expertise/experience
• Unique profiles

Figure-4: The vicious circle of cybercrimes
(Source: https://www.researchgate.net/figure/The-vicious-circle-of-cybercrimes-The-proposed-framework-outlines)

4. Digital Evidence(DE) Assessment

“DE can disclose the signature behaviors of cybercriminals.” [11] ”A *signature behavior* is a decipherable and unique pattern of movement and actions that can be ascribed to a source providing some form of psychosomatic or emotional benefit.” [12].”During this phase, courts determine whether the appropriate legal authorization was used to search and seize information and communication technology (ICT) and related data.”[13]. “The legal order required to obtain ICT and ICT-related data varies by jurisdiction and is determined by national laws.” [14].

5. Cyber Laws of Different Countries

5.1 *The French Law of Digital Evidence*

“Under French law, digital evidence must fulfill two conditions: integrity of the document and identification of the author. In practice, three main issues arise with digital evidence”. [15]

4.1.1 The technical means to ensure its reliability (the market supply)

4.1.2. The legal standards to ensure its trustworthiness (the legal demands, which are often disproportionate)

4.1.3. How to preserve in a long term both previous requirements (digital archiving, the core issue in digital evidence)

5.2 *The Malaysian Law of Digital Evidence*

“In Malaysia, digital evidence is admissible as documentary evidence and primary evidence. The admissibility of digital output is established under sections 90A, 90B, and 90C of the Evidence Act 1950 (amendment 2012).Digital evidence is any probative information stored or transmitted in digital form that a party to a court case may use during trials. The court will determine if the digital evidence is relevant, authentic, and original. In Malaysia, an organization named Cyber Security (an agency under the Ministry of Science, Technology, and Innovation) takes care of the digital evidence derived from digital sources. To date, Cyber Forensics has contributed to solving numerous forensics cases” [16]

REVIEW OF DIGITAL EVIDENCE-BASED INVESTIGATION PROCESSES(DEBIP)

6. Computer Forensic Investigative Process (CFIP)

This methodology was proposed by Pollitt,[19] in 1995 for dealing with digital evidence investigation.and obtaining reliable and legally acceptable results. It can be subdivided into four distinct phases as shown in figure5 below:

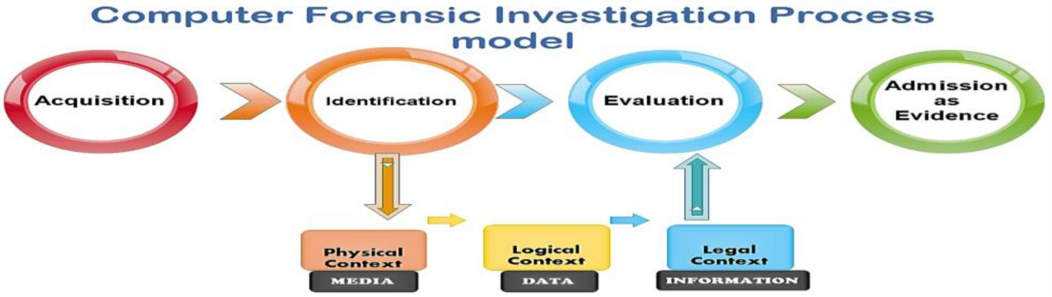


Figure-5 Fundamental Conceptual framework of CFIP

“In the acquisition phase, the collected evidence ware conformed and assimilated conventionally with apposite approval from concern authority, It is shadowed by Identification phase where the responsibilities to identify the digital constituents from the assimilated evidence and transfiguring them to humanly understood format. The Evaluation phase is encompassed with the task of determining the components identified in the previous phase, is undeniably pertinent to the case being inspected, and can be well-thought-out as legitimate evidence. In the final phase, Admission, the picked-up & evidence is presented in the court of law.” [20]

7. Integrated Digital Investigation Process (IDIP)

This investigation process was recommended by Spafford in 2003, , The aim and intention of IDIP were to combine thevaried investigative processes into one integrated single platform. The IDIP contemplated on the computer as the crime scene to provide the DE. The digital crime scene is consequently derived from physical crime. This preliminary IDIP structure comprises as many as seventeen phases that are based on concurrent frameworks. It was also systematized in the following five groups as illustrated in figure 6 below:

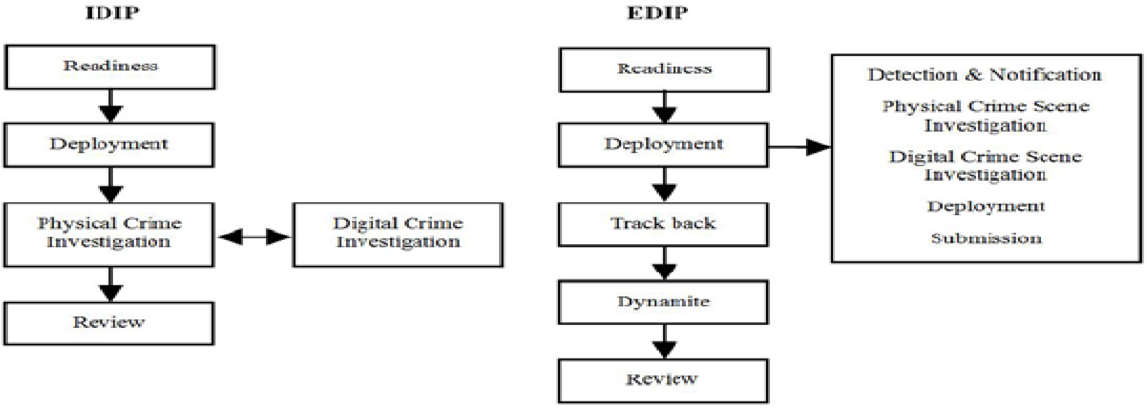

IDIP
Readiness
Deployment
Physical Crime Investigation
Digital Crime Investigation
Review
EDIP
Readiness
Deployment
Track back
Dynamite
Review
Detection & Notification
Physical Crime Scene Investigation
Digital Crime Scene Investigation
Deployment
Submission

Figure-6 Integrated Digital Investigation Process

8. End to End Digital Investigation (EEDI)

8.1. There are 6 classes in Digital Forensics Research Workshop(DFRWS) which were modified and redefined by Stephenson into 9 steps. This comprehensive digital investigation process modified by Stephenson is commonly known as the EEDI model. Steps are Collecting evidence, Analysis of individual events, Preliminary correlation, Event normalizing, Event de-confliction Second level correlation, Timeline analysis, Chain of evidence construction, and lastly Corroboration (considering as non-normalized events).

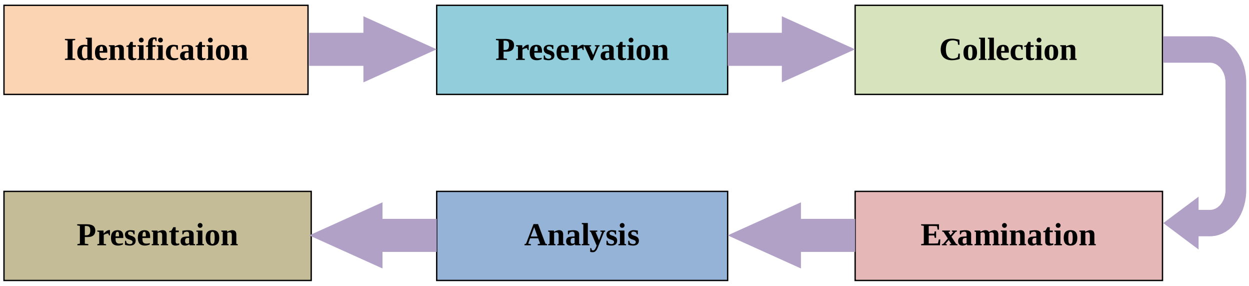


Figure-7 End to End Digital Investigation

8.2. *Advantages and Disadvantages*

The model stresses the hardcore essentials of a forensic investigation process. Besides, it provides a fundamental framework and modalities for investigating a wid-range of cases in the ever-evolving arena of ICT. The model offers flexibility and facilitates acclimate in different scenarios. On contrary, this model is only valued as a guideline framework rather than a model thatis implementable and viable in an untangible investigation scenario.

9. Kruse and Heiser Model

This widely used DIP model was constructed on three fundamental phases. The first phase embraces acquiring the data evidence. It is suggested that data integrity needs to be guaranteed. The next step is to carryout a crisscross match on the legitimacy, validity of the collected data by the authentication process. The final phase refers tothe data analysis part.It is much needed to keep data intactness, integrity, and validity. A widespread view of the framework is given in table1 below.

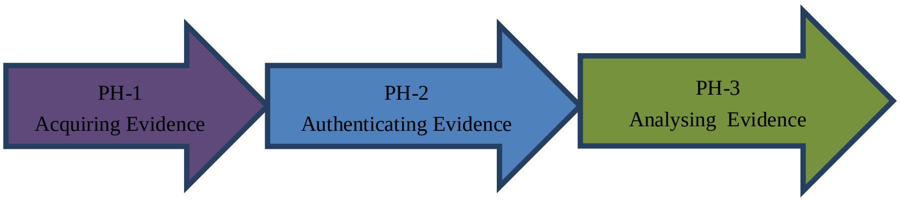


Figure-8: Kruse and Heiser Model(Source: Kruse and Heiser: 2002, p 8)

9..1 *Advantages and Disadvantages*

The Kruse and Heiser model are the simplest and widely used amongst all the models as illustrated earlier.However, this model also has some limitations and shortcomings. It places a key emphasis on keeping the integrity and originality of data during the process of investigation. As a result, the other essential parts like reporting and presenting the evidence before the law may sometimes be omitted and resulting in a significant lack in the overall investigatory process.

PROPOSED DIGITAL FORENSIC CONCEPTUAL FRAMEWORK FOR INVESTIGATION OF CYBERCRIME :

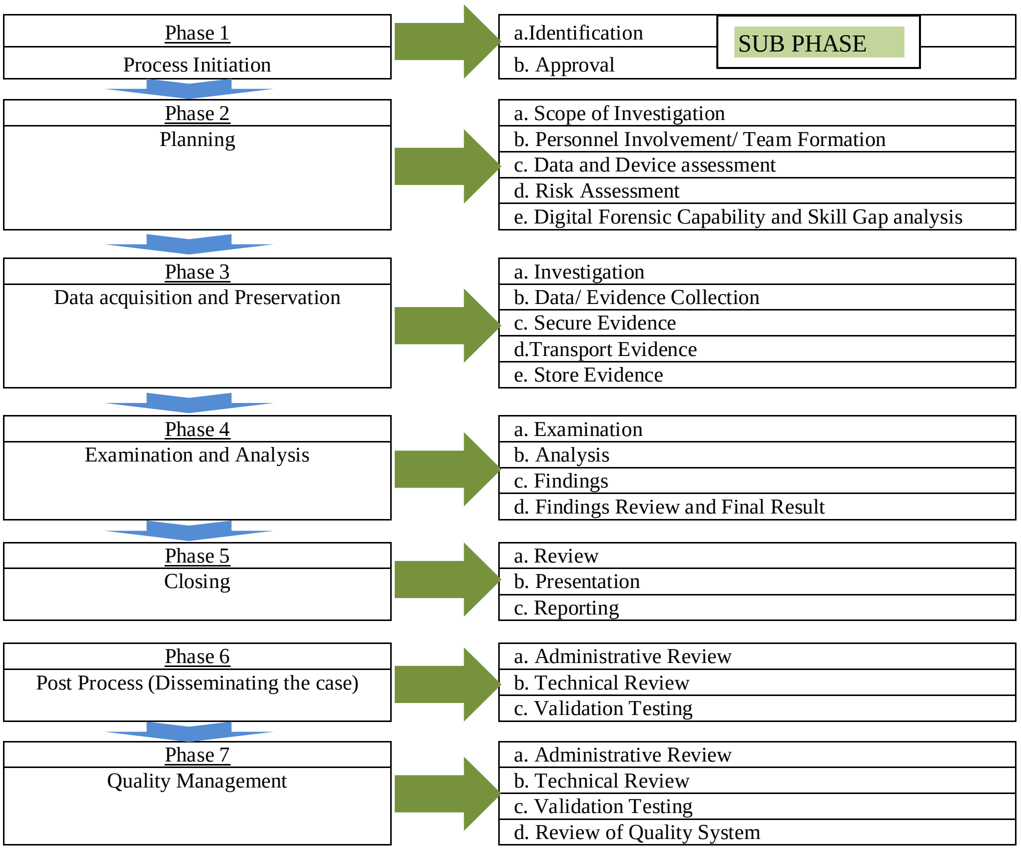
10. Overview

In this write-up, an exhaustive competitive analysis has been carried out among all commonly available DEMF of developing as well as developed countries to extract the basic common digital forensic investigation phases that are shared among all models. The differences are in the content of each phase whereby certain scenarios may require certain levels or types of detailed steps. Based on the grouping of the overlapping, similar phases and considering strengths and weaknesses of those models. Therefore, through this paper, an endeavor has been taken to w proposed a new DEMF which will be viable and implementableby most of the developing countries.Since cybercrime has evolved with numerous new-fangled risk and detrimental issues quite frequently on the world wide web, therefore, concurrent DEMF should be enormously addressing all relevant issues in this regard.It is quite certain that our proposed DEMF can serve as the basic and high-level investigation models for any future computer forensic investigation. This becomes difficult with different personnel and organizations developing their methodologies or framework. It should also serve as a good starting point for the development of a new computer forensic investigation methodology.

.

11. Framework Layout

In this write-up an IDIP based multifaceted platform has been proposed as a preferred option to carry out a wide-ranging in-depth Digital Evidence investigation process. This proposed framework will operate in seven phases. Each phase is expanded in various sub-phaseswith some pre-designated activities and suggested templatesas illustrated in the figure-5, table-2 and figure 7 respectively.



Phase 1 Process Initiation	a.Identification b. Approval
Phase 2 Planning	a. Scope of Investigation b. Personnel Involvement/ Team Formation c. Data and Device assessment d. Risk Assessment e. Digital Forensic Capability and Skill Gap analysis
Phase 3 Data acquisition and Preservation	a. Investigation b. Data/ Evidence Collection c. Secure Evidence d.Transport Evidence e. Store Evidence
Phase 4 Examination and Analysis	a. Examination b. Analysis c. Findings d. Findings Review and Final Result
Phase 5 Closing	a. Review b. Presentation c. Reporting
Phase 6 Post Process (Disseminating the case)	a. Administrative Review b. Technical Review c. Validation Testing
Phase 7 Quality Management	a. Administrative Review b. Technical Review c. Validation Testing d. Review of Quality System

:

Figure-9. Structural Framework of proposed DEMF Model(Authors' Self Construct)

11.1. The detailed activities in each phase and surface with probable outcomes are appended in table 1 below:

Phase	Sub-phase	Task	Output
1	A & B	**Define the type of investigation required (criminal/routine etc)** • Define case type • Type of intrusion and Data (static, Live/dynamic) • Type of Approval required. • Define evidence requirement	Initiation Note
2	A & B	• Case identifier or submission number • Forensic Documentation • Identity of the reporting organization	Planning Document, Timeline, Team Info
	C-E	• Identity of the submitter • Relevant dates for forensic work, include the date of the report • Descriptive list of the evidence examined • Identify the strategy, policies, and previous investigations	Authorization, Risk Assessment, Confirmation
3	A-D	• Determine what a particular piece of digital evidence • Identifying possible sources of data • Translated the media into data • Secure all relevant logs & data and preserve the chain of custody in storage.	Crime type, Potential, Evidence Sources, Media, Devices, Log Files, File, Events log, Data, Information
4	A	• Determine how the data is produced, when and by whom • Determine and validate the	Output formal document
	B	• Test and reject theories based on the digital evidence • Reconstruct the sequence of events and define criteria to prove or disprove the hypothesis. • Analyze evidence using the most suitable tools available. • Eliminate duplication of analysis.	
	C	• Make a finding that is consistent with all the evidence. • Document the finding	
	D	• Review the results and findings • Submit for the final report • Enter Final documentation into safe custody.	
5	A	• Determine which information should be included/excluded • Identify which evidence should be presented • Determine piece of evidence is relevant and admissible	Review report
	B	• Prove the validity of the hypothesis • Communicate relevant findings to a variety of audiences	Evidence
	C	• Archiving and storage • Reconstruction of the crime scene • Formal investigation report	Report, Investigation Closed
6	A-B	• Ensuring the physical and digital property is returned • Create attacker profile	Evidence Explanation, New Policies, New Investigation
	C	All reports should be administratively reviewed	
7	A& B	• Perform peer review • Check report is clear and understandable.	Checklist, Policies, Procedures
	C	• Trusted tools are used? validation testing	
	D	• Reviewing the investigation process to identify improvement area • Review lesson learns from the investigation.	

Table-1 Phase wise detail pre-designated activities of LHRS

11.2. The conceptualframework ofthe proposed DEMF is appended in figure-9below.

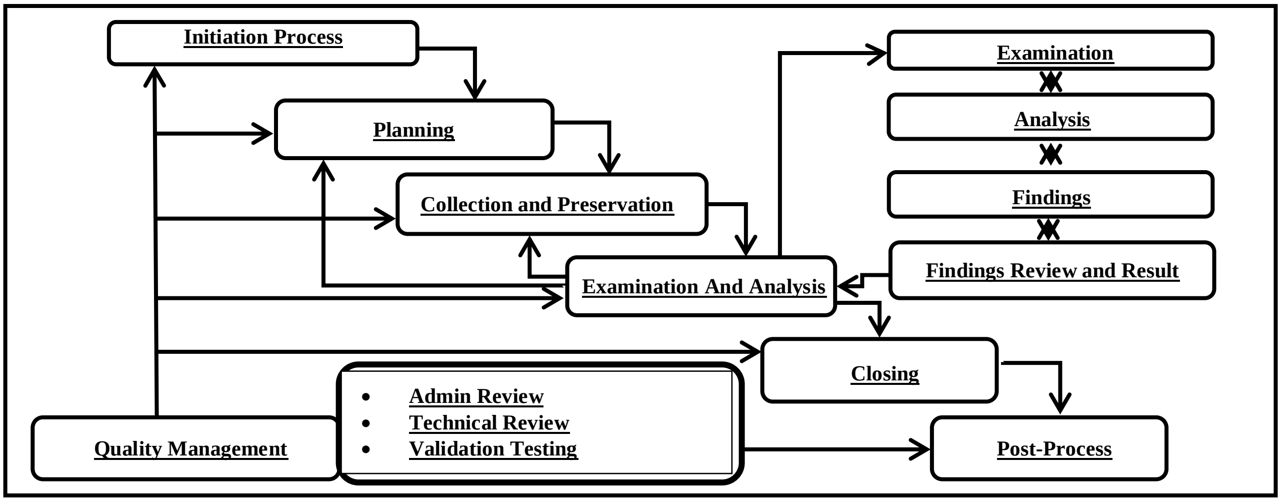


Figure-9: The conceptual framework of proposed DEMF

12. Conclusion

The extensive usage of computers in our daily life for business and pleasure has exposed us to security threats such as computer crimes, industrial espionage, theft related to intellectual property, misconduct by a corporate employee, and so on[1]. Most harmful are malicious and exploit codes that interfere with computer operations on a global scale and along with other cyber-crimes that threaten online-based e-commerce[1]. Cyber-crime is often old-styled crime (i.e. child pornography, fraud, identify theft) even though implemented speedily and to immense numbers of prospective victims, as well as unlawful access, damage, and interference to computer systems (Broadhurst, 2006) In a plain and approachable manner, there is a need for a standard method for the application of computer forensic particularly usage of the digital evidence.

If a proper crime scene investigation processes framework existed, then less effort would be required for the crime scene and digital forensic investigators to resolve a case and help Judge to deliver adequate judgment. This measure ensures the model is accurate and reliable from a legal and scientific perspective and adaptable for most of the developing countries lagging significantly in this regard.

Future Work

Cybercrime involves a wide range of crimes and major procedural works need law is consonant to each type of crime. Detail exploration and validation is needed to match different existing laws along with the proposal of news rules within the law

REFERENCES

[1] S.R.Ali., ‘Digital Evidence – An Approach to Safeguard from Cyber Crime in Bangladesh’, *NDC Journal,*pp1-77,2017.

[2] A.K Subramaniam, ‘Digital forensics of the physical memory’, *Forensic Focus, 2005*

[3] https://www.coursehero.com/file/p639hp/B-Upon-seizing-digital-evidence-actions-taken-should-not-change-that-evidence

[4] www.tandfonline.com

[5] Forensics in Telecommunications, Information, and Multimedia", Springer Science and Business Media LLC, 2011.

[6] (Maras, 2014).

[7] ACPO., Good Practice Guide for Computer-Based Electronic evidence V5, 2012

[8] www.acpo.police.UK.

[9] www.acpo.police.uk..

[10] http://shodhganga.inflibnet.ac.in/bitstream/10603/7829/12/12_chapter%203.pdf

[11] Casey et al, ‘Behavioural and Neural Correlates of Delay of Gratification’, January 2011

[12] ibid

[13] ibid

[14]. ‘Cybercrime Module 7: International Cooperation against Cybercrime’, *The Doha Declaration,* UNODC,2017

[15] journals.sas.ac.uk

[16]Malaysia,-Cybersecurity[online] http://www.cybersecurity.my/en/our_services/digital_forensics

[17] www.unodc.org

[18] J.Brezinski and T. Killalea., ‘*Guidelines for Evidence Collection and Archiving’,2002. https://www.unodc.org/e4j/en/cybercrime/module-6/key-issues/handling-of-digital-evidence.html*

[19] Pollitt, Computer forensics: An approach to evidence in cyberspace, 1995in

[20]Y. Yusoff et al, “Common Phases of Computer Forensics Investigation Models”, *International Journal of Computer Science & Information Technology (IJCSIT),* Vol 3, No 3, June 2011.