# DIGITAL EVIDENCE – AN APPROACH TO SAFEGUARD FROM CYBERCRIME IN BANGLADESH

**Brigadier General Shaikh Muhammad Rizwan Ali, ndc, psc, te**

## Introduction

Cybercrimes are committed but due to lack of professional investigation and follow up of providing digital evidence, the case become weak. A comprehensive guideline and framework to computer forensic investigators and analysts is missing for Bangladesh. Therefore, there is a need for a proper digital evidence based crime scene investigation framework of processes to prevent Cybercrime in Bangladesh.

The extensive usage of computer 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 corporate employee, and so on. The speedygrowth of computer connectivity has provided openings for criminals to exploit security weaknesses in the on-line background. Most harmful are malicious and exploit codes that interfere computer operations on a global scale and along with other cyber-crimes that threaten online based e-commerce. 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. The law and investigation perspective of the digital evidence management in ensuring the appropriateness of the evidence into the court of law is a concern. (Subramaniam, 2017).

The Information and Communication Technology Act 2006 mainly deals cybercrimes in Bangladesh. The Key areas of the Act encompasses–matters related to electronic record and digital signature, categories of offence and penalties, and composition with jurisdiction of cybercrime tribunal and cyber appellate tribunal in Bangladesh. Cybercrime is a crime which is often conducted over the Internet

and it could be in various forms against the government agencies, corporate and against any person. The law enforcement agencies are facing difficulties in dealing with cybercrime.

## Review of Digital Evidence Based Investigation Processes

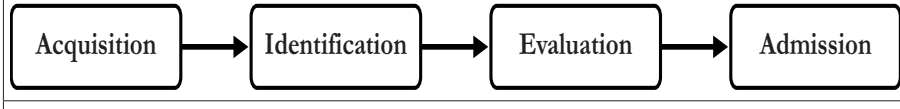
### Introduction of Digital Evidence Based Investigation Processes

Few numbers of suggested and proposed digital forensics and investigation models have been reviewed. We are not suggesting selected models are better or superior than the other models. First we try to identify and extract the phases and gaps in the investigation models and proposed a new digital evidence based crime scene investigation framework for Bangladesh. We are discussing few models below:

### Computer Forensic Investigative Process (CFIP)

In 1995 Pollitt has proposed a methodology for dealing with digital evidence investigation so that the results with be scientifically reliable and legally acceptable. It comprises of four distinct phases as shown in figure 1.

**Figure 1:** Computer Forensic Investigative Process

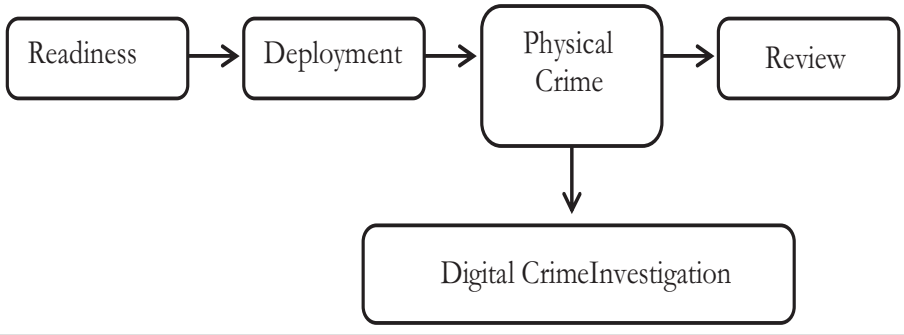



Source: Pollitt: 1995, p 561

### Integrated Digital Investigation Process (IDIP)

In 2003, this investigation process was proposed by (Spafford, 2003), with the intention to combine the various available investigative processes into one integrated model. The authors introduced the concept of digital crime scene which refers to the virtual environment created by software and hardware where digital evidence of a crime or incident exists. The digital crime scene is therefore derived from the physical crime. This initial framework includes seventeen phases that are based on the existing to date frameworks and is organised in the following five groups as shown in figure 2.

**Figure 2:** Integrated Digital Investigation Process

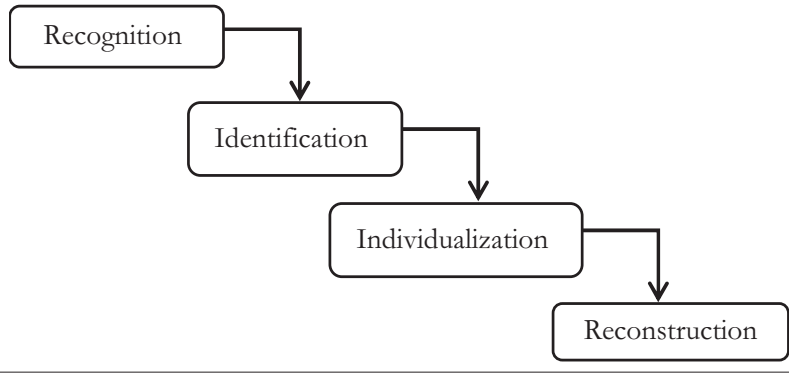



Source: Spafford: 2003, p 3

## Scientific Crime Scene Investigation Model

In year 2004, (Casey, 2004)is regarded published the essence of computer forensic investigations on Digital Evidence and Computer Crime. He provided an overall computer forensics framework which describes the relationships among computer science, forensic science, law, and behavioural analysis. The model Casey presents four phases as shown in figure 3.

**Figure 3:** Scientific Crime Scene Investigation Model (SCSI)




Source: Casey: 2004, p 430

## End to End Digital Investigation (EEDI)

There are 6 classes in Digital Forensic Research Work Shop (DFRWS). Stephenson modified classes into 9 steps for a comprehensive digital investigation process (Stephenson, 2003) and referred it as End to End Digital Investigation (EEDI)

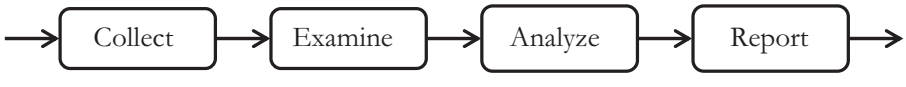
model. Steps are as following:

- Collecting evidence
- Analysis of individual events
- Preliminary correlation
- Event normalizing
- Event de-confliction
- Second level correlation (consider both normalized and non-normalized events)
- Timeline analysis
- Chain of evidence construction
- Corroboration (consider only non-normalized events)

## Law Enforcement Process Model

This model (Brian Carrier, 2003) is based on the standard crime scene investigation protocol and comprises of four steps those are; the collection, examination, analysis and reporting keeping preparatory in built. The collection stage finds out various kinds of evidence and collecting it. The examination stage is linked to data mining in order to disclose considerable evidence of meaningful nature. The analysis stage basically deals with interpreting data or explaining the data in relation to the questions under investigation to reach a conceivable conclusion. The last step is reporting or presenting of evidence in the court of law. The simplest schematic workflow is shown in figure4.

**Figure 4:** The US Department of Justice (USDOJ) Model

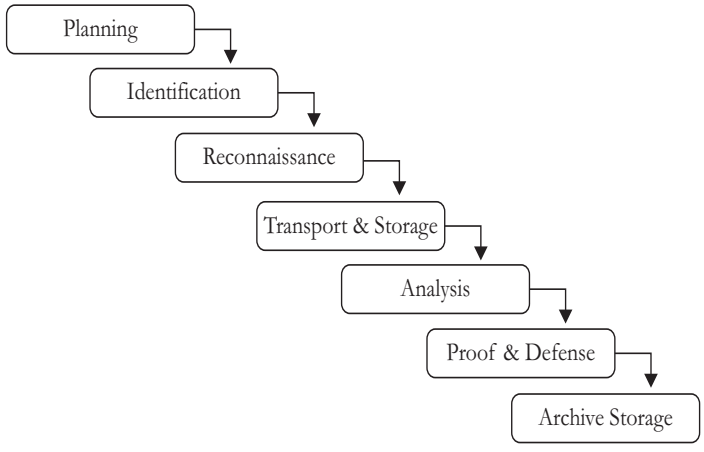



Source: Brian Carrier & Eugene H. Spafford: 2003,p 2-3

## Digital Forensic Model based on Malaysian Investigation Process (DFMMIP)

In 2009 (Perumal, 2009), Perumal, S. proposed yet another digital forensic investigation model which is based on the Malaysian investigation processes. The DFMMIP model consists of 7 phases and shown in figure 5.

**Figure 5:** DFMMIP Model




Source: Perumal: 2009, p 42

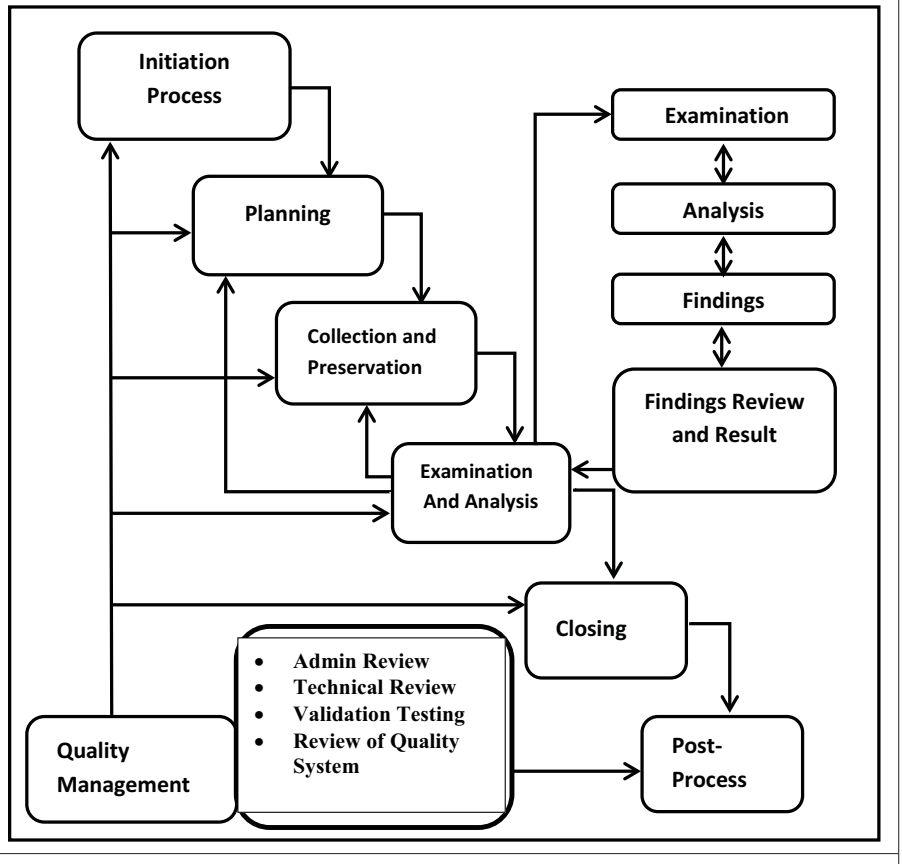
Upon completion of the 1st phase, Planning, the next phase, Identification, followed. After that, Reconnaissance phase is conducted. This phase deals with conducting the investigation while the devices are still running (in operation) which is similar to performing live forensics. The author argued that the presence of live data acquisition that focuses on fragile evidence does increase the chances of positive prosecution. Before data can be analyzed, they must be securely transported to the investigation site and be properly stored. This is indeed done in Transport and Storage phase. Once the data is ready, Analysis phase is invoked and the data will be analyzed and examined using the appropriate tools and techniques. Similar to the Presentation phase in the previous models, the investigators will be required to show the proof to support the presented case. This is done in Proof & Defense phase. Finally, Archive Storage phase is performed, whereby relevant evidence are properly stored for future references and perhaps can also be used for training purposes.

## Proposed Digital Forensic Conceptual Framework for Investigation of Cybercrime

Based on the presented computer forensic investigation processes, we are able 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 scenario may require certain levels or types of details steps. Based on

the grouping of the overlapping, similar phases and considering strengths and weaknesses of those models, we have proposed, a new model, Digital Forensic Framework in Bangladesh for Investigation of Cyber Crime. It is hoped that new Digital Forensic Framework 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 own methodologies or framework. It should also serve as a good starting point for the development of new computer forensic investigation methodology. The proposed Digital Forensic Conceptual Framework in Bangladesh for cybercrime is shown in figure 6.

**Figure 6:** Proposed Digital Forensic Conceptual Framework in Bangladesh for Cybercrime




Source: Researcher

## Framework Layout

**Table 1:** Framework Layout

| Phase Name | Sub Process | Activities | Output |
|---|---|---|---|
| Phase 1: Process Initiation | Identification Approval | • Define type of investigation required (criminal/routine etc)<br>• Define case type<br>• Type of intrusion (Through network/ stand-alone/ handheld device)<br>• Type of Data (static, Live/ dynamic)<br>• Type of Approval required.<br>• Define evidence requirement | Initiation Note |
| Phase 2: Planning | Scope Of Investigation Personnel Involvement/ Team Formation Data and Device assessment Risk Assessment Digital Forensic Capability and Skill Gap analysis | • Case identifier or submission number<br>• Forensic Documentation<br>• Identity of the reporting organization<br>• Identity of the submitter<br>• Relevant dates for forensic work, to include date of report<br>• Scope Of Investigation<br>• Descriptive list of the evidence examined<br>• Examination requested<br>• Description of the examination<br>• Name and signature of the examiner<br>• Results, conclusions, and derived items<br>• Monitoring authorization and management support, and obtain authorization to do the<br>• investigation<br>• Ensuring the operations and infrastructure are able to support an investigation<br>• Provide a mechanism for the incident to be detected and confirmed<br>• Identify the strategy, policies and previous investigations | Planning Document, Timeline, Team Info Authorization, Risk Assessment, Confirmation |

| **Table 1:** Framework Layout | | | |
|---|---|---|---|
| | | • Informing the subject of an investigation or other concerned parties that the investigation is taking place<br>• Formal Planning Document submission and approval. | |
| Phase 3: Collection and Preservation or Data Acquisition | Investigation Data/ Evidence Collection Secure Evidence Transport Evidence Store Evidence | • Determine what a particular piece of digital evidence<br>• Identifying possible sources of data<br>• Translated the media into data<br>• Identify suspect devices and peripherals (digital, manual)<br>• Ensuring integrity and authenticity of the digital evidence<br>• Record the physical scene<br>• Physically protect and preserve crime scene<br>• Capture image of the scene<br>• Preserve copy and analyses pertinent data<br>• Make forensic copies of all evidence<br>• Authenticate all evidence as identical to the original.<br>• Record the physical scene<br>• Secure all relevant logs & data<br>• Securely transport evidence.<br>• Preserve chain of custody in storage.<br>• Ensuring the validity and integrity of evidence for later use. | Crime type, Potential, Evidence Sources, Media, Devices, Log Files, File, Events log, Data, Information |
| Phase 4: Examination and Analysis | Examination | • Determine how the data produced, when and by whom<br>• Determine and validate the techniques to find and interpret significant data<br>• Extracting hidden data, Discovering the hidden data, and Matching the pattern<br>• Transform the data into a more manageable size and form for analysis<br>• Confirming or refuting allegations of suspicious activity | Output formal document |

| **Table 1:** Framework Layout | | | |
|---|---|---|---|
| | | • Identifying and locating potential evidence, possibly within unconventional locations<br>• Test and reject theories based on the digital evidence<br>• Determining the significant evidence | |
| | Analysis | • Reconstruct sequence of events.<br>• Define criteria to prove or disprove the hypothesis.<br>• Analyze evidence using the most suitable tools available.<br>• Organizing the analysis results from the collected evidence<br>• Eliminate duplication of analysis.<br>• Construct detailed documentation for analysis and Draw conclusions based on evidence found<br>• Compare evidence with other known facts. | |
| | Findings | • Make a finding that is consistent with all the evidence.<br>• Document the finding | Output formal document |
| | Findings Review and Final Result | • Review the results<br>• Review the findings<br>• Submit for final report<br>• Enter Final documentation into safe custody. | Output formal document |
| Phase 5: Closing | Review | • Determine which information should be included/excluded<br>• Identify which evidence should be presented<br>• Determine piece of evidence is relevant and admissible | Review report |

| **Table 1:** Framework Layout | | | |
|---|---|---|---|
| | Presentation | • Prove the validity of the hypothesis<br>• Clarify the evidence, and Document the findings<br>• Communicate relevance findings to a variety of audiences<br>• Present evidence in a logical, understandable way to ensure that the court can critically assess every bit of information and understand the relevance to the case.<br>• Presenting the evidence to management or court or authority. | Evidence |
| | Reporting | • Inventory of all items seized and analyzed<br>• Inventory of all equipment used in the investigation process<br>• Inventory of all tools used in the investigation<br>• Archiving and storage<br>• Reconstruction of the crime scene<br>• Formal investigation report | Report, Investigation Closed |
| Phase 6: Post-Process or Disseminating the case | • Disposal<br>• Database | • Ensuring physical and digital property is returned to proper owner<br>• Determine how and what criminal evidence must be removed<br>• Reviewing the investigation to identify areas of improvement<br>• Disseminate the information from the investigation<br>• Close out the investigation and preserve knowledge gained<br>• Document all aspects of the case<br>• Create attacker profile | Evidence Explanation, New Policies, New Investigation Procedures, Evidence Disposed, Lesson learnt |

| **Table 1:** Framework Layout | | | |
|---|---|---|---|
| Phase 7:<br><br>Quality Management | Administrative Review | • All reports should be administratively reviewed | Check list |
| | Technical Review | • Perform peer review<br>• Check report is clear and understandable.<br>• Examiner follow process review and document review check list | Check list |
| | Validation Testing | • Trusted tools are used?<br>• validation testing | Check list |
| | Review of Quality System | • Reviewing the investigation process to identify improvement area<br>• Review lesson learn from the investigation. | Check list, Policies, Procedures |

## Survey Findings - Investigators, Law Makers, White Hackers

A survey was carried out amongst the CID and PBI crime scene investigators and forensic experts along with Law makers as well as related to present ICT ACT 2006 (amendment 2013) and latest amendment needed for new forms of crime and white hackers.

### Investigators

### Digital Evidence Management Framework (DEMF)

Though there were many models of DEMF to provide digital evidence, most suitable from the experience of dealing cases related to Hacking, Phishing, Cyber Fraud, Identity Theft by PBI/CID is NIJ 2004. NIJ 2004 is most preferred DEMF model adopted unofficially by the investigators from CID and PBI. However, while interviewing it was asked whether they have any own national framework for prosecution through cyber tribunal or not and the answer was negative.

### Determination of Time- stamps for Digital Evidence

While examining the methodology for time- stamps for digital evidence, it was found that none of the investigators follow trusted time stamp or non- trusted time stamps for authenticating their digital evidence. Basically, it gives a wrong feedback about the authenticity of digital evidence being produced before the cyber tribunal.

## Use of GPS Location as an Identification

While examining the methodology for GPS location in case of presenting initial collection of digital evidence as an identification, it was found that none of the investigators follow GPS location as an Identification for authenticating their identification of digital evidence.

## Use of Hash Function

To calculate a finger print in DEMF, there is a need for hash function to lock the evidence. While examining the methodology for using Hash functions, it was found that the latest Hash function SHA-2 is not used. Instead SHA-1 is used by CID and PBI for authenticating their digital evidence.

## Template Database for all Persons who Handles Digital Evidence

It is expected to have a template database for all persons who handles digital evidence be ready for a prolonged case or typical cases. While examining, it was found that no such template for database is available in CID and PBI w.r.t first responders, forensic investigators, court expenditure, law enforcement personnel, and police officer. Everybody agreed to about the need for database template for handling their digital evidence.

## Use of Radio-frequency Identification (RFID) to Trace Digital Evidence

While examining the methodology, it was found that none of the investigators use RFID to trace their digital evidence.

## Cases Handled By Investigators

As per the interview, it came out that most cases filed under ICT Act 2006 is defamation. Side by side, Hacking cases were mostly handled by the investigators. However, other crimes like phishing, cyber fraud or identity theft are not addressed by the investigators. Most cases of PBI are under trial in cyber tribunal. Also, PBI handles less cases than CID.

## Most Common Cybercrime Reported and Tried in the Court of Law

While interviewing and from TV reporting, it was known that till July 2017, approximately 500 cases are reported and 200 cases are tried. However, exact figures are unknown to the persons interviewed. In this case everybody referred his/her own investigation figures.

## View on Existing Law to Solve Common Cybercrime

There existed huge uncertainty and confusion on existing law ICT Act 2006 and amendment in 2013. The law makers were informed about the loopholes of the various rules and it was learnt that in the next amendments along with other information related laws will address this issues. Cyber fraud, phishing and Identity theft will be addressed clearly in future ICT acts.

## View on Digital Evidence to Safeguard Cybercrime in Bangladesh

While examining the view on whether the digital evidence can safeguard cybercrime or not, it was opined positively by all about its role to curb cybercrime in Bangladesh.

## View on Availability of Sufficient Fund and Expertise to Handle Cybercrime

Investigation using digital evidence required very sophisticated equipment, training and exclusive laboratory. It was learnt that most of the cases the investigators suffer from fund constraint. They are also complained about the lack of expert training on digital forensic and advanced investigation process.

## Certified Ethical Hacker (CEH) Qualified Technicians in Organization

There is a need to counter the hackers through ethical hacking process. The CEH qualified technicians are very negligible. However, it is expected that CID or PBI keep a database of qualified white hackers from home and abroad. Also they should take the support of other CEH qualified personnel.

### Support Taken from CEH Qualified Personnel (White Hackers)

It is learnt that most support to expedite the cybercrime investigation came from CEH qualified experts from foreign countries. The CEH qualified personnel within Bangladesh were not consulted due to non-availability of proper information.

### Availability of Digital Forensic Labs in Organizations

The modern digital forensic laboratory is needed for identification and presentation of chain of evidence. CID and PBI has forensic laboratory (one each) but lacks modern equipment. The procedure for procurement of digital forensic laboratory is complex and time consuming.

### View on Effectiveness of Used Forensic Software Tools

In addition to modern digital forensic laboratory, there is also a need for a forensic software tools. Licensed versions are more effective than free version and open source. Some CID investigators uses Kali Linux and other software as software tool in forensic laboratory but PBI involves FTK and Encase. In addition freeware Kali Linux are also used as a redundant one.

### Availability of CIRT in Bangladesh

Computer Incident Response Team (CIRT) plays and important role in monitoring, detecting, analysing and inverting cyber threats and incident. There is no CIRT in CID or PBI. The efforts are in process to establish one for each of the organization.

### Law Makers View on Digital Evidence to Safeguard Cybercrime in Bangladesh

While examining the view on whether the digital evidence can safeguard cybercrime or not, it was opined positively by all about its role to curb cybercrime in Bangladesh. All law makers positively opined on digital evidence to safeguard cybercrime in Bangladesh.

### Investigators Response to Each Cyber-crime as per Existing Law

The law makers of cyber related laws were asked about the case of cybercrime related to Hacking, Phishing, Cyber Fraud, and Identity Theft, how investigators

should provide digital evidence for making a proper justice. In response to this question, it was found that no such things were done so far. Rather age old procedure of penal codes are widely used. In addition different views came out. With present law, digital evidence for hacking lies on the preservation of evidence and proper framework as suggested was consulted. They supported it as a good proposal for discussion in the law making process. The other form of cybercrimes like phishing, Cyber Fraud, Identity theft, involvement of financial perfect laws should be in place for further details of framework.

## Effectiveness of Digital Evidence against Cybercrime in Bangladesh

Being new phenomenon in Law sector, with repeated change in punishment and motive behind bringing cases in forefront, submitting digital evidence against cybercrime in Bangladesh is not effective.

### Suitable DEMF for Defending Cybercrime Cases

Though there were many models of DEMF to provide digital evidence, most suitable from the experience of dealing cases related to Hacking, Phishing, Cyber Fraud, and Identity. It is seen instead of following any specific DEMF models, a combination of preferred phases and tasks are to be included in our DEMF model for Justice. While interviewing it was asked whether they have any own national framework for prosecution through cyber tribunal or not and the answer was negative. The proposed DEMF model of the researcher is highly appreciated as it covered the gaps of each DEMF models.

### Need for Time-stamps for Digital Evidence

While examining the methodology for time- stamps for digital evidence, it was found that all law makers opted for having Trusted Time Stamps for Digital evidence to be effective and trustworthy.

### Need for GPS Location as an Identifier

While examining the methodology for GPS location in case of presenting initial collection of digital evidence as an identifier, it was found that all Law makers preferred GPS location as an Identification for authenticating their identification of digital evidence.

## Law against Anti-forensics

While examining the existence of law against anti- forensics in case of presenting of digital evidence, it was found that all Law makers preferred to incorporate in ICT Act 2006 or in next draft digital security Act 2016.

## Gap in Existing Penal Code and ICT Act 2006

Section 23 of the Penal Code 1860 defines the "wrongful loss" as "is the loss by unlawful means of property to which the person losing it is legally entitled. But in section 56 of ICT Act 2006, it defines" whoever, with intent to cause or knowing that he is likely to cause "wrongful loss' or damage to the public or any person, does any Act and thereby destroys, deletes or alters any information residing in a computer source or diminishes its value or utility or affects it injuriously by any means, commits the offence of 'hacking'. The law against hacking under section 56 and section 23 involve mens-era and suit for damage, common parlance against Contravention and question the motive whether amounts to Theft and/ or criminal Trespass. According to section 441 of the penal code committing criminal trespass overlaps with section 56 also.

Again implementing global cyber law, section 84 does not clearly define how and which manner it can deal with the netizens., Mutual Legal Assistant Treaty (MLAT) is required to establish occurrence of cybercrime in borderless cyber world. There are many instances of Identity Theft happened on online purchases using falsifying credit card numbers by the cybercriminal. In ICT Act 2006, there is no provision exists tackle this problem. Also the Act doesn't cover the electronic payment. Under section 10 of ICT Act 2006, no person can insist that a form or document should be in an electronic form or the issue of a license, or payment fee may also be in an electronic form under section 7(1) and 7(2) of the Act. As such cyber fraud, phishing – all can't be addressed following ICT Act 2006. More so, anti-spamming provisions are also missing involving part of phishing technique.

## White Hackers View on Digital Evidence to Safeguard Cybercrime in Bangladesh

While examining the view on whether the digital evidence can safeguard cybercrime or not, it was opined positively by white hackers about its role to curb cybercrime in Bangladesh.

### Supporting Forensic Experts of CID/PBI

The forensic experts though need support from white hackers but usually do not take support from them. Rather other intelligence organizations like DGFI, NSI etc who pursue on cybercriminal for long term basis as a preventive measure takes support. PBI as a new organization takes support form ethical hackers.

### View on Ethical Hackers Support

The CEH qualified experts urges for a systematic inclusion to the DEMF process with a proper legal authentication. They opined that national integration process is to be started in Bangladesh.

### Use of Hash Function

To calculate a finger print in DEMF, there is a need for hash function to lock the evidence. While examining the methodology for using Hash functions, it was opined by the ethical or white hackers that the latest Hash function SHA-2 is most effective hash function and should be adopted as an authentication of digital evidence.

### Use of RFID to Trace Digital Evidence

While examining the methodology for tracing a digital evidence, it was suggested by the white hackers that for tracing the digital evidence RFID is a better method and are to be followed as a preferred means to trace.

## Recommendations

The Proposed crime scene investigation model should be practically validated through CID and PBI. The implementation is expected to improve present digital evidence based crime investigation procedure.

### Future Work

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

## Conclusion

Through different questionnaire and interviews from three prime involved agencies (Investigators, Cyber Law Makers and Ethical Hackers/ White collar Hackers), efforts were made to know the practised system of gathering digital evidence. The paper also aimed to study practical and theoretical models/ frameworks for the digital forensic investigation, validate conceptual framework with different stakeholders and finally proposed a digital evidence based investigation management framework (Figure 6) in order to safeguard cybercrime in Bangladesh.

Digital forensics is a dynamic field and currently faced with a number of issues. This paper introduces a framework for digital forensics helpful for a crime investigator. It also outlined properly selected cybercrime based digital evidence along with crime scene investigation process in commensuration with cyber law to safeguard cybercrime in Bangladesh.

Usually cybercrimes are committed but due to lack of professional investigation processes and follow up of providing digital evidence, the case become weak. There is always a deficit of information about different computer related crime, and investigation process. A comprehensive guideline and framework to computer forensic investigators and analysts is provided for Bangladesh. Also, Mutual Legal Assistance Treaty (MLAT) is required to establish occurrence of cybercrime in borderless cyber world.

## Bibliography

1. Brian Carrier, E. H. S., 2003. Getting Physical with the Digital Investigation Process. International Journal of Digital Evidence , 2(2), pp. 1-20.

2. Broadhurst, R., 2006. Policing: An International Journal of Police Strategies and Mangement. Developments in the global law enforcement of cyber-crime , 29(2), pp. 408-433.

3. Casey, E., 2004. Digital Evidence and Computer Crime. 2nd ed. USA: Elsevier Academic Press.

4. Perumal, S., 2009. Digital Forensic Model Based On Malaysian Investigation. IJCSNS International Journal of Computer Science and Network Security,, August, 9(8), pp. 38-44.

5. Pollitt, M. M., 1995. Computer forensics: An approach to evidence in cyberspace. in Proceeding of the National Information Systems Security Conference, Baltimore, II(Nil), pp. 487-491.

6. Spafford, E. C. a. B., 2003. Getting Physical with the Digital Investigation Process. International Journal of Digital Evidence, 2(2).

7. Stephenson, P., 2003. A Comprehensive Approach to Digital Incident Investigation. Information Security Technical Report, 8(2), pp. 42-54.

8. Subramaniam, S., 2017. www.forensicfocus.com. [Online] Available at: http://www.forensicfocus.com/Content/pid=98/[Accessed 15 April 2017].

## Author

Brigadier General Shaikh Muhammad Rizwan Ali, psc, te was commissioned in 25 December 1987 in the Corps of Signals. He has completed Bsc Engr (Telecommunications) from KUET, Master of Technology on Electronics Engineering from India and done specialization on communication field in home and abroad. As an instructor in School of Signals for 7 years, he trained officers and troops in computer proficiency and basics of signal communications. As staff officer at Army Headquarters Signal Directorate and Information Technology Directorate he contributed in formulating IT policy for Bangladesh, drafting technical specifications and standards. He has done his UN mission in UNAMSIL and Chief Communication Officer at Force HQ at ONUCI. As GM (SS), worked closely with Chairman, BTTB and worked for the formation of BTCL. He served as Head of Department of Electrical, Electronic and Communication Engineering at MIST and Dean of Faculty of Science and Technology at BUP.