JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Cybersecurity: Evaluation of Digital Forensic Models

Rajesh Kumar Goutam
Department of Computer Science
University of Lucknow

Abstract: Cyber forensic refers to scientifically proven investigative process and practices to uncover the facts, connecting the time-stamped events and reconstructing the crime-scene to assist court to recognize criminals. Evidences are legally documented and ensuring its admissibility in court. The basic aim of digital forensic is to investigate digital artifacts and accurately determine what had happened, how it happened, and who is responsible for these actions. Digital forensic represents the sequence of actions to carryout structured investigations, securing artifacts and to have forensic information. In this paper, we present a brief overview of three popular forensic models; evaluate their applicability with their key insights and phases.

IndexTerms **- Cybersecurity, Forensic Models, Digital Forensic**

I. CYBER CRIME

Cybercrime means a crime using internet enabled digital devices. It includes having illegal access to digital devices, e-repositories, e-accounts and impersonating someone else in web environment. Committing offences with internet against the property such as documentary frauds and forgery, crimes against person such as money extortion, blackmailing, harassing, threatening, and embarrassing, crime against the government such as espionage, smuggling, terrorism, and other cross-border crimes comes under the cybercrime. The activities responsible to cause national, racial or religious disgust and constitutes incitement to discrimination also comes under the coverage of cybercrime.

II. DIGITAL FORENSICS

As cybercrime is triggered in virtual environment, against unseen target with the help of virtual intermediaries to cause real damages so its investigation is not an easy task and often leverages criminals undetected. Digital forensic is scientifically proven process to identify, collect, preserve, obtain, and investigate computers, e-resources and writing the results in well documentation form and making it admissible to court of law. It interconnects the dots, reconstructs the events, understands the chronology behind the crime to identify and apprehend criminals. As digital forensics has a crucial role in legal prosecution and helps to uncover the truth and makes the criminal accountable for crime so it must be robust, accurate, and efficient with proven integrity.

III. DIGITAL FORENSIC MODELS

Model is a human construct that does not represents an object in reality yet still helps us to understand real object in better way. Model encapsulates real object with all its components to assist learners to study its functioning and behavior. A model with more phases and activities presents a well sequenced series of actions and provides much guidance to robust investigation process. Although it is very difficult or almost impossible to design a perfect process model to make entire investigation process consistent and standardized but few researchers have contributed with their models with a group of essential steps to execute investigation process to make it convenient and accurate.

3.1 Integrated Digital Investigation Model (IDIP)

Brian Carrier and Eugene H. Spafford [1] believe that laws of nature bind the physical world while the hardware components and software programming instructions bind digital and virtual world. Security personals use laws of nature to gather physical evidences while digital activities, timestamps and interactions with hardware and software components are noticed to have digital evidences. Brian Carrier and Eugene H. Spafford [1] grouped seventeen activities in five phases as shown in following figure 1.

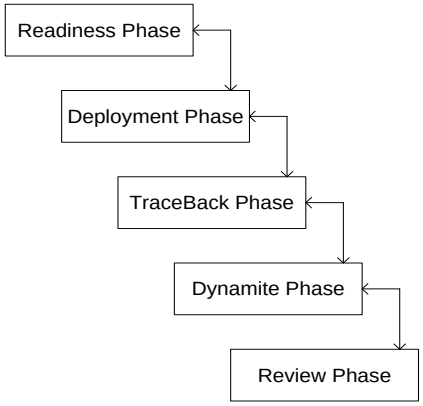

FIG.1: IDIP PHASES

Readiness Phase

The basic aim of readiness phases is to ensure that operations and infrastructure are capable to run investigation and emphasizes on fact that digital and physical evidences can be lost or tempered if these are not protected and handled properly. The readiness phase constitutes two activities as detailed following:

Operation Readiness Phase: It examines human resources and ensures that these are skilled and well equipped with appropriate tools to tackle nefarious incidents [6].

***Infrastructure Readiness Phase*:** This phase evaluates whether underlying infrastructure is capable to tackle nefarious incidents or not.

Deployment Phase

The goal of this phase is either to suggest or choose most appropriate mechanism to detect and confirm nefarious and malevolent incidents. The Deployment phase has following two activities:

Detection and Notification Phase: As relevant and suspected evidence is detected then it is notified to appropriate personal.

Confirmation and Authorization Phase: This phase confirms the relevancy of evidences and attempts to seek authorization for further legal prosecution.

Physical Crime Scene Investigation Phase

This phase mainly deals with collection and analysis of physical evidences and attempts to reconstruct the chain of incidents that took place at the time of incident happening. This phase consists of six activities as detailed following:

***Preservation Phase*:** It attempts to preserve and secure crime scene to protect evidences to not to be contaminated or destroyed. If crime scene is not protected before its forensic analysis, the evidences may deteriorate and can be meaningless as a key source of information [2] [7].

Survey Phase: This activity suggests to have visit and to investigate crime scene to indentify key locations from which different pieces of relevant evidences can be obtained.

Documentation Phase: This activity is concerned to preserve crime scene as document by taking several photographs and sketches with all possible angles.

Search and Collection Phase: It is an attempt to seek additional physical evidences to pave investigations.

Reconstruction Phase: On the basis of all collected evidences, it attempts to frame out same surroundings as it was at the time of crime with intention to develop a theory of crime.

Presentation Phase: Its basic aim is to present evidences to court to help in legal proceeding to make reach to criminals.

Digital Crime Scene Investigation Phase

The basic aim is to analyze digital evidences which have been collected during physical investigation process. It contains as same six activities as mentioned in Physical Crime Scene Investigation Phases the only difference is that it deals with digital evidences while the previous one tackles physical evidences [8].

***Preservation Phase*:** To preserve all the digital evidences at crime scene so that these can be synchronized and utilized further as evidence.

Survey Phase: It is an attempt to seek all possible digital evidences from different components of hardware and digital devices that can be crucial to frame charges against criminals in court [9].

Documentation Phase: This activity is responsible for physical documentation of all digital evidences and making it admissible to court.

Search and Collection Phase: This activity performs in-depth analysis of digital evidences to uncover hidden, deleted and tempered facts and to establish relationship against timeline to have complete replica of crime [10].

Reconstruction Phase: All the digital events are connected with real time-line to track criminals' actions during crime.

Presentation Phase: This activity ensures the admissibility of digital evidences in court.

Review Phase

This activity presents entire investigation as a whole and highlights key areas in results to assist court. IDIP shows the real time interactions between physical and digital realms and helps law enforcement agencies to have complete understanding of physical crime scene.

3.2 Extended Model of Cybercrime investigation (EMCI)

Séamus Ó Ciardhuáin [3] believes that digital forensic models such as Digital Forensic Investigation Model (DFIM), Forensic Process Model (FPM), Abstract Digital Forensic Model (ADFM) and Integrated Digital Investigation Model (IDIP) do not focus to information flows in investigations. The author also believes that previous models were confined to collection and examination phases of investigation and left some earlier and later stages untouched during investigation of evidences. Extended Model of Cybercrime investigation (EMCI) constitutes thirteen stages as shown in figure 2. EMCI proceeds in "waterfall" fashion with a fixed sequence of activities where backtracking is allowed. This model has several advantages, most notably information flows among the activities in investigation process and excellent representation of various key actions. The backtracking inherent in model makes it more realistic as investigations do not proceed in a simple linear fashion. Two separate phases named 'hypotheses' and 'dissemination' makes it more effective as these puts control over information flows in legal proceedings.

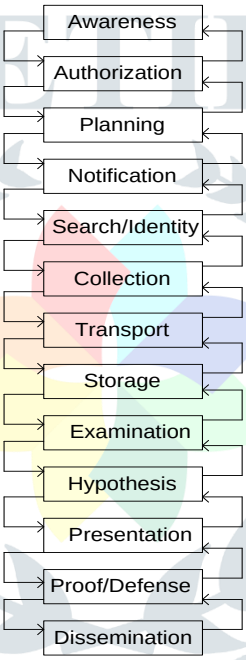

FIG. 2: EMCI PHASES

3.3 Enhanced Digital Investigation Process Model (EDIPM)

The two main attractions of IDIP model are the reconstruction of the events that were responsible to lead incident to happen and reviewing the whole task repeatedly. Baryamureeba and F. Tushable [2] also highlight its criticisms as its deployment phase shows independency over physical and digital evidences, which is practically not possible. IDIP neither offer sufficient specificity nor makes proper distinctions between victim's scene and suspect scene. EDIPM has five phases as shown in following figure 3.

Readiness Phase

This phase deals with equipments and keeps them ever ready while ensuring that personals shall be able to utilize them effectively [4].

Deployment Phase

This phase includes a mechanism used to detect an incident and making its confirmation too.

Traceback Phase

This phase is responsible to map complete crime scene and attempts to find the root cause and surroundings used in crime. Its goal is to tracked down resource used in crime chronically. This phase is also supported with two activities named Digital Crime Investigation and Authorization.

Dynamite Phase

This phase examine primary crime scene, collects the evidences and performs a close inspection of all these to obtain new facts and secondary evidences to make final interpretations and conclusions to accuse potential culprits.

Review Phase

This phase is responsible for reviewing entire investigation process and to find out the areas need to be improved.

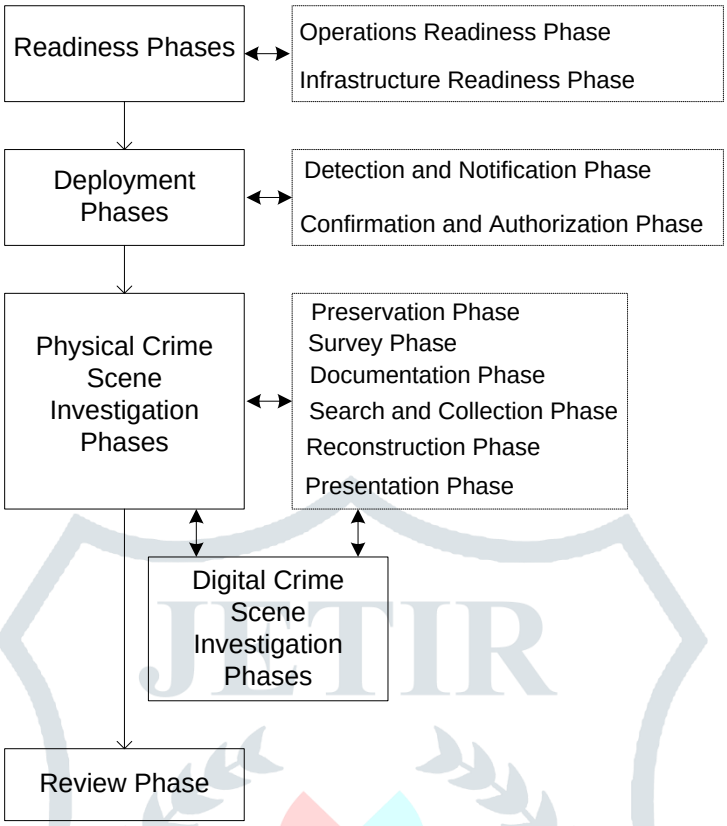

FIG. 3: EDIPM PHASES

IV. DISCUSSION AND COMPARISON OF IDIP, EMCI AND EDIPM

IDIP believes that computer is itself a crime scene and implements crime scene forensic techniques. Data saved to devices or even deleted becomes the part of investigations and often leaves digital evidences behind [1] [5]. B. Carrier et al. [1] consider each connected digital device as a separate crime scene and analysis of each device is sent to IDIP reconstruction phase where linkage and chronology among the devices is established to form primary digital crime scene. Preservation phase in IDIP ensures secure entrance and exits to primary digital crime scene, isolates its related devices and collects all the volatile data to protect entire scene. IDIP takes all the actions that have historically fallen and relates to an incident in consideration and performs reconstruction activity to make investigation process more robust and accurate. Its investigation statistics are capable to compute dedicated investigation efforts to a digital incident. Séamus Ó Ciardhuáin [3] not only believes in incident chronology and events reconstruction but also considers information flows to make investigation process more reliable. EMCI emphasizes on awareness and attempts to have a clarification about what to be investigated before to begin forensics. In EMCI, authorization is another vital activity that recognizes the role of personals in an investigation and helps to frame out primary investigation scene. EDIPM is capable to identify potential evidences, to develop preliminary theory and to establish relationships among different pieces of physical evidences in chronological order. It ensures in its preservation phase that crime scene investigation process is being performed with skilled personals. EDIPM presents more realistic statistics than IDIP and EMCI both as its tracebacke phase is capable to frame the replica of actual crime scene on the basis of separate evidence pieces collected from different digital devices. EDIPM made a close separation between primary crime scene and secondary crime scene, and considered constituted phases as iterative instead of being linear.

EDIPM is an extended version of IDIP in which deployment phase consist of five activities. The physical crime scene investigation and digital crime scene investigation have been added to have reconstruction of crime scene in chronological order. Action authorization is part of deployment phase in IDIP while it is performed in TraceBack phase in EDIPM. The different phases and activities of these three models have been summarized in following table 1.

Table 1: Forensic Models Activities

Investigation Phases	**Phases**	**Activity**
Integrated Digital Investigation Model (IDIP)	Readiness Phase	Operations Readiness Infrastructure Readiness Phase
	Deployment Phase	Detection and Notification Phase Confirmation and Authorization Phase
	Physical Crime Scene Investigation Phase	Preservation Phase Survey Phase Documentation Phase

		Search and Collection Phase Reconstruction Phase Presentation Phase
	Digital Crime Scene Investigation Phases	Preservation Phase Survey Phase Documentation Phase Search and Collection Phase Reconstruction Phase Presentation Phase
	Review Phase	Nil
Extended Model of Cybercrime investigation (EMCI)	Awareness	Nil
	Authenticated	Nil
	Planning	Nil
	Notification	Nil
	Search/identity	Nil
	Collection	Nil
	Transport	Nil
	Storage	Nil
	Examination	Nil
	Hypothesis	Nil
	Presentation	Nil
	Proff/Defense	Nil
	Dissemination	Nil
Enhanced Digital Investigation Process Model (EDIPM)	Readiness Phase	Operations Readiness Infrastructure Readiness Phase
	Deployment Phase	Detection and Notification Phase Physical Crime Scene Investigation Digital Crime Scene Investigation Confirmation Phase Submission Phase
	TraceBack Phase	Digital Crime Scene Investigation Authorization
	Dynamite Phase	Physical Crime Scene Investigation Digital Crime Scene Investigation Reconstruction Phase Communication Phase
	Review Phase	Nil

Table 2: Activity Based Comparison

Phase/Activity	IDIP	EMCI	EDIPM
Preparation	✔	✔	✔
Planning	✔	✔	✔
Operation Readiness		✔	✔
Awareness	✔	✔	✔
Survey		✔	✔
Authentication		✔	✔
Notification	✔		✔
Search/Identity		✔	✔
Collection	✔		✔
Transport		✔	✔
Storage			✔
Examination		✔	✔
Hypothesis	✔	✔	✔
Presentation			✔

Proof/Defense			✔
Dissemination	✔	✔	✔

EDIPM considers physical crime scene investigation as activity not a complete phase and emphasize to traceback to have reconstruction of crime scene replica. EMCI emphasizes on awareness about the resources from where data is required to be collected from crime scene. Its hypothesis phase examines the direction of investigation and validates the forensic process. Dissemination phase completes the documentation process and ensures its admissibility in legal prosecution. The following table 2 shows the activity based comparison.

V. CONCLUSIONS

The most challenging issue with digital forensic models is lack of standardization due to which each model has its own phases and activities to perform forensic of digital crime scene. Each model decides its own course of action in dissimilar way and results in loss of efficiency and time in conducting investigations and sometimes to lose critical evidences too. IDIP and EDIPM both emphasizes on readiness phase and examines the capability of human resources and potential of infrastructures to decide whether an organizations is capable to perform investigation or not. EDIPM merged physical crime scene investigation and digital crime scene investigation phases mentioned in IDIP together and covered in its single phase named deployment. EDIPM is capable to authorize activities and validate events to make investigation process accurate while IDIP and EMCI do not have such kind of provision. EMCI looks effective over EDIPM and IDIP due to its awareness and hypothesis phases and uses scientific procedure to collect and preserve forensic evidences.

REFERENCES

[1] Brian Carrier and Eugene H. Spafford, “Getting Physical with the Digital Investigation Process”, International Journal of Digital Evidence, 2003.

[2] Venansius Baryamureeba and Florence Tushabe, “ The Enhanced Digital Investigation Process Model”, Institute of Computer Science, Makerere University, Digital Forensic Research Conference, 2004.

[3] Séamus Ó Ciardhuáin, “An Extended Model of Cybercrime Investigations”, International Journal of Digital Evidence, Vol 3(1), 2004

[4] Yunus Yusoff, Roslan Ismail and Zainuddin Hassan, “Common Phases of Computer Forensics Investigation Models”, International Journal of Computer Science & Information Technology (IJCSIT), Vol 3, No 3, June 2011

[5] M.D. Kohn, M.M. Eloff, J.H.P. Eloff, "Integrated digital forensic process model", Computers and Security, Vol. 38, October 2013, pp. 103-115

[6]Michael Kohn, JHP Eloff and MS Olivier, “Framework for a Digital Forensic Investigation”, Proceedings of the ISSA-2006 from Insight to Foresight Conference, Sandton, South Africa, July 2006

[7] R.B. van Baar, H.M.A van Beek, E.J van Eijk, “Digital Forensics as a Service: A game changer”, Digital Investigation, 2014

[8]Xiaoyu Du, Nhien-An Le-Khac, Mark Scanlon, “Evaluation of Digital Forensic Process Models with Respect to Digital Forensics as a Service”, 16th European Conference on Cyber Warfare and Security (ECCWS 2017), 2017.

[9]Rechard Bassett, Linda Bass and Paul O’Brien, “Computer Forensics: An Essential Ingredient for Cyber Security”, Journal of Information Science and Technology, 2006

[10]M.D Kohn, M.M. Eloff, and J.H.P Eloff, “Integrated Digital Forensic Process Model”, Computers & Security,vol.38, October 2013