Generic System Forensics Investigation Model

K.P. Kaliyamurthie*1, D. Parameswari2

1* Corresponding Author, HOD, Department of CSE, Bharath University, Chennai, India
2 Associate Professor and Head, Dept. of MCA, Jerusalem College of Engineering, Chennai, India

ABSTRACT: The increasing criminal activities exploitation digital data because the suggests that or targets warrant for a structured manner in addressing them. Since 1984 once a formalized method been introduced, a good variety of recent and improved System rhetorical investigation processes are developed. during this paper, we tend to reviewed some designated investigation processes that are made throughout the years and so known the usually shared processes. Hopefully, with the identification of the usually sherd method, it'd build it easier for the new users to know the processes and conjointly to function the fundamental underlying construct for the event of a brand new set of processes. supported the usually shared processes, we tend to planned a generic System forensics investigation model, referred to as GCFIM.

KEYWORDS: Computer rhetorical Models, System rhetorical Investigation

I. INTRODUCTION

The increasing criminal activities exploitation digital data because the suggests that or targets warrant for a structured manner in addressing them. As additional data is keep in digital type, it's terribly possible that the proof required to prosecute the criminals is additionally in digital type. As early as 1984, the Federal Bureau of Investigation Laboratory and different enforcement agencies began developing programs to look at System proof [1]. the method or procedure adopted in performing arts the pc rhetorical investigation encompasses a direct influence to the end result of the investigation. selecting the inappropriate fact-finding processes might result in incomplete or missing proof. Bypassing one step or change any of the steps might result in inconclusive results; thus bring about to invalid conclusions. Evidences captured in a billboard hoc or unstructured manner might risks of not being allowable within the court of law. it's so terribly crucial for the pc forensics investigator to conduct their work properly as all of their actions square measure subjected to scrutiny by the judiciary ought to the case be given within the court. The presence of a typical structured method will during a means offer an appropriate mechanism to be followed by the pc rhetorical investigators. Over the years, there have been variety of investigation models being planned by varied authors. supported our observation, a number of the models tend to be applicable to a really specific situation whereas different is also applied to a wider scope. a number of the models tend to be quite detail et al is also too general. it's going to be to a small degree tough or perhaps confusing, particularly to the junior rhetorical investigator to adopt the right or accepSystem investigation model. it's of our intention to analyse the assorted accessible models and extract the common phases and propose a brand new general purpose model so we are able to have a typical beginning model that may be applicable to any situations.

1.1. Terminologies
In the course of performing arts the reviews, we've got discovered that completely different terms were utilized by varied authors, so as to mirror the processes taken to perform the planned investigation. Among the terms used were model, procedure, process, phase, tasks, etc. so as to not be drawn into a prolonged discussion on that terms is best to be used, we decide to still maintain no matter terms utilized by the first authors, once describing their various processes. However, once conducting comparison and indentifying common characteristics, we’d like to use one term solely (for the aim of standardization) and selected the term “model” to represent the whole activities performed during a System rhetorical investigation.

DOI: 10.15680/IJIRSET.2014.0311101

Copyright to IJIRSET
www.ijirset.com 17316
investigation. The term “phase” is employed to represent the high level element of the investigation model and also the term “tasks” is employed to represent activities to be performed in every of the phases.

II. INVESTIGATION PROCESS REVIEWED

The number of prompt and planned investigation models isn't tiny, as such, it'd be quite an discouraging exercise to review all of them. we've got so, designated the models to be reviewed supported the written account order, making certain a minimum of one planned model each year. we tend to aren't suggesting that the chosen models square measure higher or superior than the opposite models that were conjointly introduced within the same year. Our objective is to spot and extract the phases within the investigation models instead of choosing that model is that the best.


Acquisition Identification analysis Admission

In Acquisition section, proof was nonheriSystem in accepSystem manner with correct approval from authority. it's followed by Identification section whereby the tasks to spot the digital elements from the nonheriSystem proof and changing it to the format understood by human. The analysis section comprise of the task to work out whether or not the elements indentified within the previous section, is so relevant to the case being investigated and might be thought-about as a legitimate proof.

within the final section, Admission, the nonheriSystem & extracted proof is given within the court of law.

2.2. DFRWS fact-finding Model

DFRWS fact-finding model started with associate Identification section, within which profile detection, system observation, audit analysis, etc, were performed. It is now followed by Preservation section, involving tasks like putting in place a correct case management and making certain an appropriate chain of custody. This section is crucial therefore on make sure that the info collected is free from contamination. subsequent section is thought as assortment, within which relevant knowledge square measure being collected supported the approved ways utilizing varied recovery techniques. Following this section square measure 2 crucial phases, namely, Examination section and Analysis section. In these 2 phases, tasks like proof tracing, proof validation, recovery of hidden/encrypted knowledge, data mining, timeline, etc, were performed. The last section is Presentation. Tasks associated with this section square measure documentation, professional testimony, etc.


Inspired by DFRWS fact-finding model, Reith, Carr & Gunsch [5], planned associate increased model referred to as Abstract Digital rhetorical Model. during this model, the author introduced 3 extra phases, so increasing the quantity of phases to 9, the three vital phases introduced during this model were Preparation, Approach Strategy and Returning proof.

In Preparation section, activity like making ready tools, establish techniques and obtaining management support, were done. Approach Strategy was introduced with the target to maximise the acquisition of un tarnished proof and at identical time to attenuate any negative impact to the victim and encompassing individuals, so as to confirm that evidences square measure safely come back to the rightful owner or properly disposed, the Returning proof section was conjointly introduced. the first section in ADFM is Identification section. during this section, the task to acknowledge and verify variety of incident is performed. Once the incident kind was discovered, subsequent section, Preparation, is conducted, followed by Approach Strategy section. Physical and digital knowledge nonheriSystem should be properly isolated, secured and preserved. there's conjointly a desire to listen to a correct chain of custody. All of those tasks square measure performed below Preservation section. Next is that the assortment section, whereby, knowledge extraction and duplication were done. Identification and locating the potential proof from the collected knowledge, employing a systematic approach square measure conducted within the next following section, referred to as Examination section. The task of decisive the many of
proof and drawing conclusion supported the proof found is completed in Analysis section. within the following section, Presentation section, the findings square measure summarized and given. The investigation processes is completed with the concluding of Returning proof section.

This investigation method was planned by Carrier & Spafford [6] in 2003, with the intention to mix the assorted accessible fact-finding processes into one integrated model. The author introduces the construct of digital crime scene that refers to the virtual surroundings created by code and hardware wherever digital proof of a criminal offense or incident exists.

The process started with a section that need for the physical and operational infrastructure to be ready to support any future investigation. during this Readiness section, the equipments should be ever ready and also the personnel should be capable to use it effectively. This section is so associate in progress section throughout the lifecycle of a corporation. It conjointly consists of two sub-phases particularly, Operation Readiness and Infrastructure Readiness. now following the Readiness section, is readying section, which offer a mechanism for a happening to be detected and confirmed. 2 sub-phases square measure additional introduced, namely, Detection &amp; Notification and Confirmation &amp; Authorization. aggregation and analyzing physical proof square measure drained Physical Crime Scene Investigation section. The sub-phases introduced square measure Preservation, Survey, Documentation, Search &amp; assortment, Reconstruction and Presentation. Digital Crime Scene Investigation is comparable to Physical Crime Scene Investigation with exception that it's currently specializing in the digital proof in digital surroundings. The last section is Review section. The whole investigation processes square measure reviewed to spot areas of improvement which will ends up in new procedures or new coaching necessities.

2.5. increased Digital Investigation method Model (EDIP)
As the name implies, this fact-finding model is predicated on the previous model, Integrated Digital Investigation method (IDIP), as planned by Carrier &amp; Spafford. the improved Digital Investigation method Model, conjointly referred to as EDIP [7] introduces one vital section referred to as Traceback section, this can be to alter the investigator to trace back all the thanks to the particular devices/computer utilized by the criminal to perform the crime.

The investigation method started with Readiness section and also the tasks performed square measure identical as in IDIP. The second section, readying section, provides a mechanism for a happening to be detected and confirmed. It consists of five sub-phases particularly Detection &amp; Notification, Physical Crime Scene Investigation, Digital Crime Scene Investigation, Confirmation and finally, Submission. Unlike DIP, this section includes each physical and digital crime scene investigations and presentation of findings to legal entities (via Submission phase). In Tracebak section, pursuit down the supply crime scene, together with the devices and placement is that the main objective. it's supported by 2 sub-phases particularly, Digital Crime Scene Investigation and Authorization (obtaining approval to perform investigation and accessing information). Following Traceback section is Dynamite section, during this section, investigation square measure conducted at the first crime scene, with the aim of distinctive the potential culprit(s), encompass four sub-phases, namely, Physical Crime Scene Investigation, Digital Crime Scene Investigation, Reconstruction and Communication. In Reconstruction, sub-phase, items of data collected square measure place along therefore on construct to doable events that would have happened. The Communication sub-phase is comparable to the previous Submission section. The investigation method over with Readiness section and also the tasks performed square measure identical as in IDIP.

2.6. System Forensics Field sorting method Model (CFFTPM)
The CTTTPM [8] proposes associate onsite approach to providing the identification, analysis and interpretation of digital proof during a comparatively short time-frame while not the necessity to require back the devices or media back to the science lab. Nor will it need taking the entire rhetorical pictures. The CFFTPM encompass half dozen primary phases that square measure then additional divided into another half dozen sub-phases.
CFPTPM started with a well-recognized section, coming up with section. Correct coming up with before embarking on associate investigation can for sure improve the success rate of associate investigation. Following coming up with with section is sorting section. During this section, the proof square measure known and stratified in terms of importance or priority. Proof with the foremost necessary and volatile ought to be processed initial. The User Usage Profile section focus its attention to analyse user activity and profile with the target of relating proof to the suspect. Building the crime case from written account perspective by creating use of macintosh time (for example) to sequence the probable crime activities is that the main objective of Chronology Timeline section. Within the web section, the tasks of examining the artefacts of web connected services square measure performed. Lastly, just in case Specific proof section, the investigator will alter the main target of the examination to the specifics of the case like the main target in kid porn would so show a discrepancy than that of monetary crime cases. Upon completion of the first section, Planning, subsequent section, Identification, allowed[4]. After that, intelligence activity section is conducted. This section deals with conducting the investigation while the devices square measure still running (in operation) that is comparable to performing arts live forensics[5]. The author argued that the presence of live knowledge acquisition that focuses on fragile proof will increase the possibilities of positive prosecution. Before knowledge will be analyzed, they need to be firmly transported to the investigation website and be properly keep. This can be so drained Transport & Storage section. Once the info is prepared, Analysis section is invoked and the proof are analyzed and examined exploitation the accepSystem tools and techniques. Just like the Presentation introduce the previous models, the investigators are needed to point out the proof to support the given case. this can be drained Proof & Defense section. Finally, Archive Storage section is performed, whereby relevant proof square measure properly keep for future references and maybe also can be used for coaching functions[6].

II. OTHER INVESTIGATION METHOD REVIEWED

Due to the impractically of reviewing additional models with identical details as on top of, we've got determined to form this section to still discuss on different investigation models. However, during this section, we tend to solely highlight the phases that square measure the top level of the investigation method. There are given within the written account order and also the reality they're mentioned during this section doesn't indicate that they're inferior to those investigation processes discuss in Once the investigation processes were known, subsequent step is to extract all of the phases inside every of the investigation processes. Extracted phases were allotted with distinctive id. Phases with similar tasks square measure sorted along. The result's displayed in System a pair of, below[7].

System 2: List of phases
ID Name of phases accessible in
P01 Access M12
P02 Acquisition M01,M12
P03 Admission M01
P04 Analysis M02,M04,M13, M14,M06,M09,M15 P05 Approach Strategy M04
P06 Archive Storage M14 P07 Authorization M08 P08 Awareness M08 P09 Case Specific Analysis M10 P10 Chronology Timeline Analysis M10
P11 assortment M02,M04,M06,M08,M09,M15 P12 readying M05,M07
P13 Detection M15
P14 Digital Crime Investigation M05 P15 Dissemination of knowledge M08 P16 Dynamite M07 P17 analysis M01
P18 Examination M02,M04,M06,M08,M15
P19 Hypothesis creation M08
P20 Identification M01,M02,M04, M14,M03,M06 P21 Incident Closure M09
P22 Incident Response M09,M15
P23 secernment M03

DOI: 10.15680/IJRSET.2014.0311101

Copyright to IJIRSET www.ijirset.com 17319
Based on the on top list of phases it's apparent that variety of these phases do so duplicated or overlapped one another. Taking into consideration of the tasks performed in every of the phases, and not simply looking forward to the particular naming, we tend to were able to observe that the phases will be sorted into five generic grouping particularly, pre-process, acquisition & preservation, analysis, presentation and post-process. however the phases were sorted into their various generic grouping[8].

System 3: Generic Phases
Generic Phases accessible phases
Pre-Process P01, P05, P07, P08, P26, P28, P30, P31, P35, P36;
Acquisition & Preservation P02, P11, P12, P13, P20, P30, P33, P42, P44
Analysis P04, P09, P10, P13, P14, P16, P17, P18, P19, P23, P24, P25, P27, P37, P38, P42, P43, P45, P46
Presentation P03, P29, P32, P34, P39,
Post-Process P06, P15, P21, P22, P40, P41,

Based on our study of different investigation models, not mentioned in here, every of their suggested phases also can be placed in a minimum of one among the on top of generic phases. Therefore, we tend to planned the below generic investigation method, to be referred to as Generic System section one of GCFIM is thought as Pre-Process[9]. The tasks performed during this section relates to all or any of the works that require to be done before the particular investigation and official assortment of information. Among the tasks to be performed have gotten the mandatory approval from relevant authority, making ready and setting-up of the tools to be used, etc[10].

Phase a pair of is thought as Acquisition & Preservation. Tasks performed below this section associated with the distinctive, acquiring, collecting, transporting, storing and protective of information. In general, this section is wherever all relevant knowledge square measure captured, keep and be created accessible for subsequent section[11].

Phase three is thought as Analysis. this can be the most and also the center of the pc rhetorical investigation processes. it's the foremost variety of sections in its cluster so reflective the main target of most models reviewed square measure so on
the analysis phase varied kinds of analysis square measure performed on the nonheriSystem knowledge to spot the supply of crime and ultimately discovering the person behind the crime.

Phase four is thought as Presentation. The finding from analysis section square measure documented and given to the authority. Obviously, this section is crucial because the case should not solely be given during a manner well understood by the party given to, it should even be supported with adequate and accepSystem proof. the most output of this section is either to prove or refute the alleged criminal acts Phase five is thought as Post-Process. This section relates to the correct closing of the investigation exercise. Digital and physical proof ought to be properly came back to the rightful owner and unbroken in safe place, if necessary. Review of the fact-finding method ought to be done so the lesson will be learnt and used for improvement of the long run investigations[12].

Instead of moving consecutive from one section to a different, the power to travel back to the previous phases should always be gift. we tend to square measure addressing the things that square measure forever ever-changing in terms of the crimes scenes (physical and digital), the fact-finding tools used, the crime tools used and also the level of experience for the investigators. As such, it’s abundant desired to be able to return to the previous phases that we’ve got done, not solely to correct any weaknesses however conjointly to accumulate new things/information. we tend to would like to notice that section numbered P22 (in System 2) was place in Post-Process section that is because of our belief, that action or response to any incident ought to be done once the incident was properly analyzed and given to the authority. all the same, ought to the investigator found a really risky and high impact incident, perquisite is up to the authority. all the same, ought to the investigator found a really risky and high impact incident, perquisite is up to the investigator to require any correct immediate actions. However, this can be a deviation to a traditional method and may be treated on a case to case basis[13].

IV. CONCLUSIONS

Based on the given System rhetorical investigation processes, we tend to square measure able to extract the fundamental common investigation phases that square measure shared among all models. The variations square measure within the content of every section whereby bound situation might need bound levels or kinds of details steps. supported the grouping of the overlapping and similar phases, we’ve got planned, a brand new model. Generic System rhetorical Investigation Model (GCFIM), we tend to hope that GCFIM will function the fundamental and high level investigation models for any future System rhetorical investigation. It ought to conjointly function an honest start line for the event of recent System rhetorical investigation methodology.

REFERENCES


DOI: 10.15680/IJIRSET.2014.0311101

Copyright to IJIRSET

www.ijirset.com 17321