Domain Specific Cyber Forensic Investigation Process Model

Rabail Shafique Satti and Fakeeha Jafari

***Abstract*—Digital Forensics can be defined as a field of study involving the usage of technical and proved procedures for collecting, preserving, validating, analyzing, interpreting and presenting the digital evidences extracted from the digital sources for presenting those in the court of law. Different process models have been proposed by the researchers for cyber crimes' investigation process, each having its own suitability to environments where they are applicable and other pros and cons. The paper includes the tailoring of existing process models to the particular domain of higher education institutes. With the growing access of computing resources and internet to the students, employees and overall citizens, it is the need of time that organizations should establish and maintain their cyber forensics analysis policy along with whole process to be followed in case of any cyber crime scene reporting.**

***Index Terms*—Cyber forensics investigation, cyber forensics investigation process models, domain specific, comparative analysis, law compliance.**

I. Introduction

Digital forensics investigation is not a new field but still based on new practices and new threats encountered; it is an evolving one. Forensics investigation is the vital phase for Cyber forensic analysis because the analysis totally depends upon the quality, fine granularity, effectiveness, systematic and legal investigation process being carried out by the computer forensics experts. The most critical part in forensic investigations is to dig out and relate the "relevant" information for a forensic case by the investigators. So, for that purpose the investigations should be systematic, expert, customized and sound enough making it a process been done in less time and therefore causing more relevant information to be collected and subsequently being investigated. Among so many forensic investigation processes being proposed, there are few phases which are common to all of them; consisting of some pre-process tasks which may consist of formal permissions and legal issues before starting the actual investigations proceeded by the evidences acquired and preserved from the crime scene. The analysis is performed on the acquired evidences, the results are documented and presented (in courts etc) and finally some post processing is performed in which evidences are again preserved for any future reference and records are maintained.

Manuscript received October 19, 2014; revised December 20, 2014.

Rabail Shafique Satti is with the Department of Software Engineering, Fatima Jinnah Women University (FJWU), Rawalpindi, Pakistan (e-mail:emailrabail@gmail.com).

Fakeeha Jafari is with the Department of Computer Sciences, Fatima Jinnah Women University (FJWU), Rawalpindi, Pakistan (e-mail:fakeehajafari@gmail.com).

In this paper, a reference model has been proposed for cyber forensics investigation process for a university domain. To provide an ethical, secure and monitored computing environment, the educational institutions (particularly higher education institutes) should maintain a cyber forensics investigation policy along with the standard practices conforming to the legal restrictions and the rules & regulations imposed at institute or government level.

II. Literature Review

Many process models have been proposed for digital investigation procedures and researchers have mainly focused on the nature and number of steps involved in the investigations process of cyber crimes. For the literature review, many proposed digital forensics investigation processes have been reviewed and the main focus would be on discussing the salient features of those models and comparing those features for their implementation in other models.

A. Kruse and Heiser Model

The earliest known methodical approach employed to computer forensics. It was based on three fundamental phases. The first phase involves acquiring the data evidence. It is recommended that the data integrity should be ensured. The second step is to check the validity of the collected data by authentication process. The third phase is the analysis of data keeping intact the data integrity and validity. A generalized view of the framework is given in Fig. 1 below.

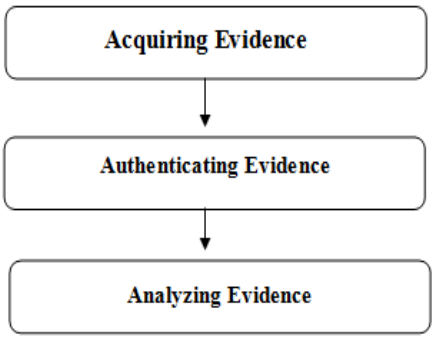

Fig. 1. Kruse and Heiser model [1].

- Advantages and disadvantages:

The Kruse and Heiser model is the simplest of above all and hence prone to many limitations and shortcomings. This model puts main emphasis on the integrity of data during investigation. It lacks a key step of investigatory practice though i.e. reporting or presenting the evidence before law.

B. US department of Justice (USDOJ) Model [2]

This model is primarily based on the standard crime scene

DOI: 10.7763/JACN.2015.V3.145

investigation protocol and comprises of four steps, the collection, examination, analysis and reporting. The collection stage involves looking out for various kinds of evidence and collecting it. The examination stage is related to data mining in order to reveal substantial evidence of meaningful nature. The analysis stage deals with interpreting the data in relation to the questions under investigation to reach a plausible conclusion. The fourth step is reporting or presenting of evidence in the court of law [3]. The simplest schematic workflow is shown in Fig. 2.

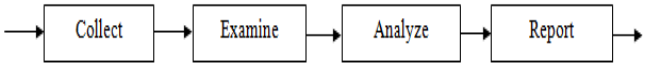

Fig. 2. The US department of Justice Model.

- Advantages and disadvantages:

This model represents an adaptation of Kruse and Weiser model for use in judicial environment. The stages of evidence collection, its examination and analysis are almost parallel with those proposed in the earlier model. However the vital component of reporting of evidence, which was missing in Kruse model, was incorporated in department of Justice Framework. But still this model lacks the depth to address the needs of an ever evolving landscape of cyber forensics investigations.

C. Digital Forensic Research Workshops (DFRWS) Model

The first DFRW in 2001 was an initiative of academia that largely served to bring together the wide spectrum of communities involved in digital forensic research; from academics to practitioners, from civilian as well as military institutions. The consensus paper of these proceedings drew the first images of the state of digital forensic investigation at that point in time. It outlined the process of digital investigation into seven action classes or steps namely; identification, preservation, collection, examination, analysis, presentation and decision. The framework is represented in the form of a table which includes columns for each activity class whereas each row represents the candidate techniques that could be employed (Table I). These techniques are variable and could be performed in context of goal to be achieved through that action class [4].

- Advantages:

It provides a consistent and standardized framework for further enhancement of digital forensic investigatory models. This model also proposes the mechanism for application of same framework to upcoming digital technologies. The model is generalized to accommodate usage by non-technical observers like judiciary and prosecution. It also identifies a tentative set of tools to be used, taking help from a similar scenario from previous experience.

TABLE I: BASIC MATRIX OF A DFRWS FRAMEWORK [5]

Identification	Preservation	Collection	Examination	Analysis	Presentation	Decision
Event/Crime Detection	Case Management	Preservation	Preservation	Preservation	Documentation	
Resolve Signture	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		Lossless Compression	Hidden Data Discovery	Timeline	Statistical Interpretation	
Audit Analysis		Sampling	Hidden Data Extraction	Link		
Etc.		Data Reduction		Spacial		
		Recovery Techniques				

- Disadvantages:

The categories definition could be too general to be practical. It is not easy to be tested through available comparative tools. The number of sub-categories added to the matrix further complicates it.

The DFRWS model appears to be bit rigid, but serves well when different steps of investigative activity are well-known to the investigator.

D. Abstract Digital Forensics Model (ADFM) [2]

The researchers at US Air Force proposed an abstract forensic investigation model in 2002. Although it incorporated many of the common processes from existing models but, assumed to be largely inspired by the DFRW framework, rather an extension of it. It adds three more phases to the process resulting in nine stages namely: identification; preparation, approach, strategy, preservation, collection, examination, analysis, presentation, and returning of the evidence (Fig. 3).

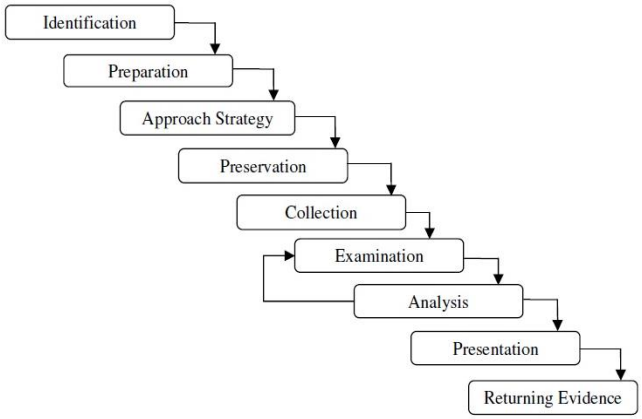

Fig. 3. Abstract digital forensic model [6].

• Advantages

The key features of this model are comprehensive pre- and post-investigation procedures in addition to the actual investigatory exercise. These three stages are preparation, approach strategy and returning evidence. The first stage defines the preparation of tools, techniques and securing management support. The approach strategy deals with means to acquire maximum amount of meaningful and genuine evidence and the return evidence stage is introduced for safe storage of evidence for subsequent retrieval.

• Disadvantages

Although this model combines the features of most prevalent models of the time yet is not applicable to many real-time situations and serves only to provide a guideline for future digital investigatory model designing.

E. Integrated Digital Forensic Investigation Process (IDIP) Model [7]

In 2003, Brian D. Carrier and Eugene H. Spafford integrated the digital investigation to physical forensic investigation process. They introduced a concept of digital crime scene in a virtual environment created with the help of soft and hardware. This model organizes the investigatory process to five groups and 17 phases (Fig. 4).

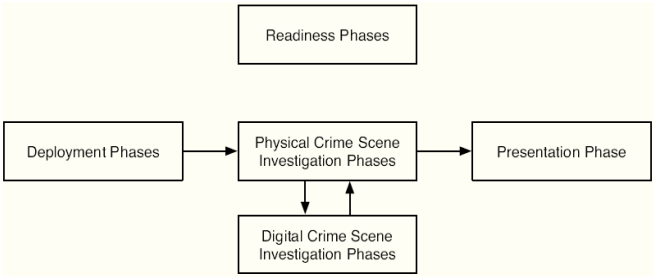

Fig. 4. Graphical representation of IDIP model [7].

The readiness phase emphasizes on the inclination of the operational and infrastructural support. The deployment phase provides mechanism to detect and confirm an incident or event. It can be split into detection/notification phase and a confirmation/ authorization phase. The collection of physical evidence is done in physical crime scene investigation under sub-phases of preservation, survey, documentation, search and collection of physical evidence. The digital crime scene investigation also follows the same stages but in a digital context. Lastly in review phase the evidence is reconstructed and presented before the court.

• Advantages

This model outlines principles for digital investigations based on those practiced for physical crime scene investigations. It defines computer and the digital activity as a separate crime scene and not as an object of mere physical evidence. It also points towards methods to be devised for establishing an interaction between the digital and physical investigation. This model contains many of the same ideas as the DFRWS and ADFM models presented in different categories e.g. the DFRWS does not differentiate between preservation and preservation phases. Similarly the boundaries between examination and analysis phases are neither vivid nor the need for event reconstruction has been highlighted.

• Disadvantages

This proposed model was though comprehensive, yet too abstract to be applied successfully into two different scenarios (physical and digital). The means of interactions suggested to link both tiers of investigations may not necessarily be applicable to many situations as such. A further enhanced model adds further complexity by introducing a trace back option to each process.

F. Systemic Digital Forensic Investigation (SRDIFM) Model [5]

Agarwal and colleagues in 2011 proposed a systemic approach to digital forensic investigation. There are 11 phases in this model named Preparation, securing the scene, survey and recognition, documentation of scene, communication shielding, evidence (both volatile and non-volatile) collection, preservation, examination, analysis, presentation, result and review (Fig. 5).

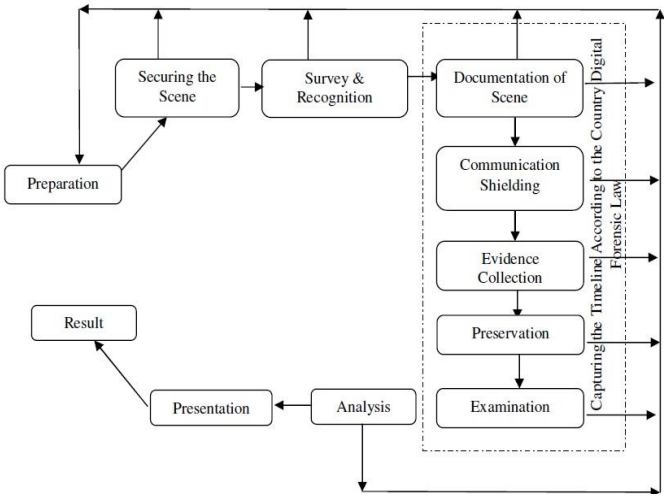

Fig. 5. A systemic digital forensic investigation model [5].

• Advantages

This model is the most comprehensive in terms of flexibility and practicality. The model is divided into 11 phases with each step looping back to add more flexibility. It incorporates the key practices in investigatory process and simultaneously realizes the properties of reliability and testability during analysis of digital crime. This might serve as a generalized solution to the increasingly complex needs of an ever-evolving digital technology world.

• Disadvantages

The incorporation of additional phases adds to the complexity and timeline of investigatory process, which in certain cases is the rate limiting step in combating cyber crimes.

G. Cyber Forensics Field Triage Process Model (CFFTPM)

This model was proposed by Rogers *et al*. in 2006 to provide an on-site field approach for identification, analysis and interpretation of digital data (evidence) bypassing the immediate need for bringing it back to lab. The model consists of 6 primary phases which can be further divided into 6 sub-classes. The process is claimed to be in compliance with the widely practiced forensic principles. This model emphasizes on the need to collect maximum informative

evidence from the site at the earliest possible time, without support of digital forensic lab.

- Advantages

The computer forensics field triage process model proposed for the first time an on-site investigation process in the field, which reduces much of time loss and logistics hurdles. Besides it does not preclude the possibility to transfer/transport evidence and system or storage media back to the lab for a thorough investigation. There is also an emphasis on the specificities of the case.

- Disadvantages

Despite its utility in the field, this model fails to entertain a diverse array of scenarios and cases. Moreover it resembles more to a computer-based digital forensic model and prone to ignore physical evidence which limits its utility (in Fig. 6).

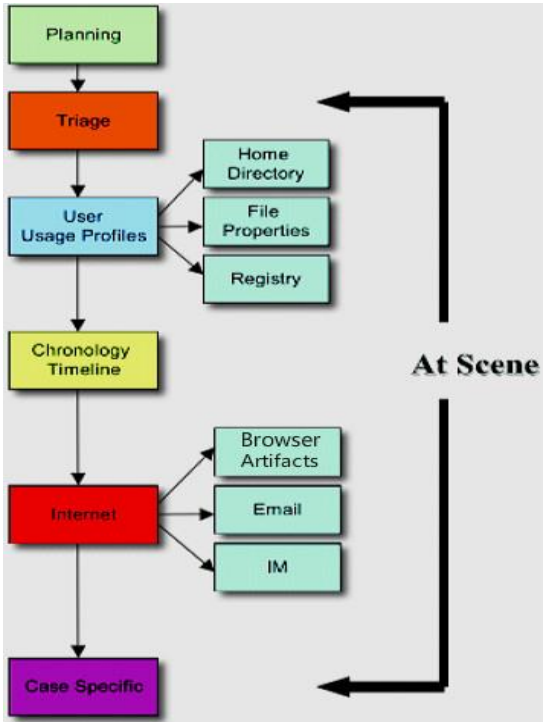

Fig. 6. Cyber forensics field triage process model (CFFTPM) [8].

H. Digital Forensic Model based on Malaysian Investigation Process (DFMMIP) [9]

Sundresan Perumal, in 2009, proposed a digital forensic investigation model which was the digital investigation practices in Malaysia. This model consists of 7 phases named; planning, identification, reconnaissance, transport and storage, analysis, proof and defense and archive storage. One of the salient features of this model is reconnaissance phase which deals with investigation being carried on active devices in order to increase the possibility of acquiring fragile data in a live scenario.

- Advantages

This model being implemented by law enforcing agencies in Malaysia, is more apt to the needs of the chain of custody and authorization to handle fragile digital data. Furthermore it emphasizes more on acquisition of both live and static digital data.

- Disadvantages

As this framework is designed to augment the capacity of law enforcing agencies to investigate cyber crimes, therefore its target is more towards traditional crime scene investigation than a scientific inquisition. It adds legal documentations like search warrants and reconnaissance. (See in Fig. 7).

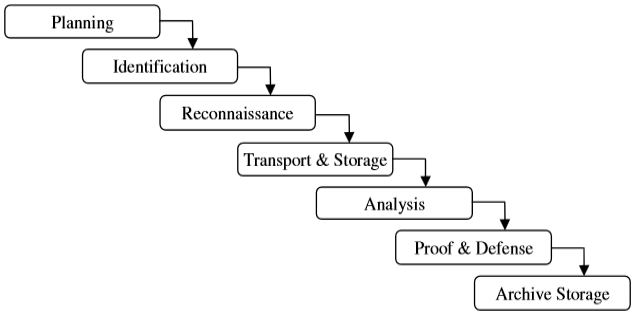

Fig. 7. Digital Forensic Model based on Malaysian Investigation Process [6].

I. Generic Computer Investigation Model (GCFIM)

Recently Yunus Yusoff and his colleagues came up with a review of digital investigation models from 1985 till 2011. They examined the pre-existing models for sorting of common phases and then proposed a generic computer investigation model, consisting of 5 generic phases shown in Fig. 8. Each of these generic phases represent the main phases present in most of the digital investigation models [10].

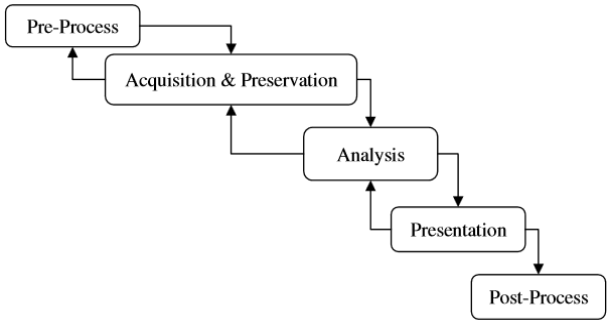

Fig. 8. Generic computer forensic investigation model (GCFIM) [6].

- Advantages

The model emphasizes on the hardcore essentials of a forensic investigation process and provides a basis for investigating a wide variety of cases in the ever-evolving field of information technology. The simplicity of the model offers a flexibility to adapt to different scenarios.

- Disadvantages

Owing to its extreme simplicity this model is rated as more of a guideline framework rather than a model as the phases presented in the model are too general to be implemented in a real-life investigation scenario.

III. Domain Specific Cyber Forensic Investigation Process Model (DSCFIPM)

After reviewing multiple existing models, important phases of cyber investigation process have been identified and some other phases which are specific to the domain, are also been added in the proposed model. Domain Specific Cyber Forensics Investigation Model has been proposed as a starting step towards establishing a policy and process flow of the forensics investigation in case of cyber crime scene reporting. In the university domain, hundred percent students have access to internet in university labs and on their laptops etc.

Also, correspondents from different positions have also confidentially revealed that they have been sent bogus emails, threats, and unethical content through their emails etc. So cyber crimes are present but there is no reporting cell inside the university where they can get help from. So this model is being presented to address the particular domain of university which operates under the judicial, government laws and university charter, so during all phases of cyber investigations, the restrictions and limitations enforced by these laws, regulations and SOPs would be considered.

The proposed model is being shown below in Fig. 9.

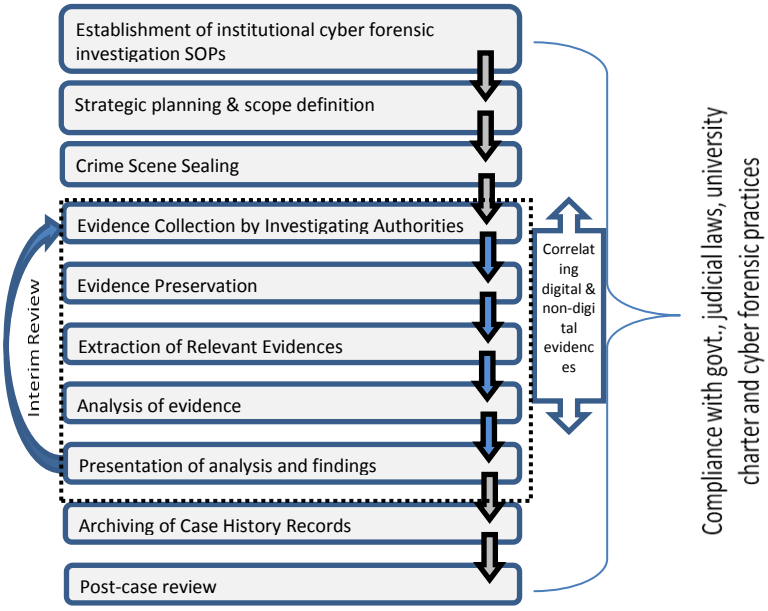

Fig. 9. Domain specific cyber forensics investigation process model.

First phase of DSCFIPM is the establishment of Cyber forensics investigations SOPs for university domain. It has been confirmed by university officials that there are no such SOPs in place up till now, so the first and most important step is to formulate a policy regarding the cyber crimes handling at institute level and disseminating that information to the students and employees. Once a cyber crime has been reported, then the strategic level planning is done to handle the situation; and the scope of cyber investigations is determined. University management will take services of expert cyber forensics analysts who will investigate the case in consultation with the university management and relevant officials who will guide them for university SOPs and other legalities applicable in the scenarios. The crime scene will be sealed for avoiding the tampering of evidences present in that area. Then possible evidences will be collected and preserved by Cyber Forensics Investigators (CFIs). Relevant evidences will be extracted and analyzed using their expert judgments and cyber forensics investigations tools like Encase, Autopsy, and Access data FTK etc. The analysis results and findings will be presented to university officials and afterwards in the court of law (if required). The interim review can be done on any phase starting from evidence collection up till presentation of results e.g. if the presented results need more elaboration (if required by university officials) and evidences need more correlation to be specified, then cyber forensics expert can review his work and rework on any intermediate phase as and when required. In the selected domain, it is up to the expertise of CFI, to correlate the digital and non digital evidences; which can reasonably help in investigations process and reaching the exact initiator of the cyber crime. Necessary documentation will be done on every phase of the process. The case history will be maintained for archiving and future reference purposes. Digital evidences can also be preserved again or can be returned to authorize people as and when required. In the post-case review phase, the updates in security policy and cyber forensics investigation policy are being done, as and when required. The awareness is being given about the changes e.g. if some firewall security policy has been tightened and as a result internet browsing speed slowed down; so people should be given awareness about the need and importance of changes in firewall policy/settings.

During the whole process of cyber forensics investigations, the judicial and government laws should be kept in consideration so that the investigation process cannot be objected and its results are admissible to courts (if required). University charter should be known to investigators so that they do not go beyond jurisdictions while investigation process. SOPs should be followed and at least one senior level university official should be designated to facilitate the CFIs understand and comply with university SOPs. Standard processes and practices of Cyber forensic analysis should be followed to avoid any misunderstandings or objections.

IV. Comparative Analysis

The comparison of different forensics investigation models shown in Table II depicts that different researchers defined their digital forensic process models consisting of multiple steps. Some just limited the number of steps to a few number while others presented quite elaborative process models, like SRDIFM consisted of 11 phases whereas Kruse and Heiser's model consisted of only 3 main steps, but detailed insight shows that even in those concise 3 steps, they had to follow

almost all phases presented in SRDIFM model. So we can generalize the digital forensics investigation model to must have the evidence acquisition, Evidence analysis and result presentation phases.

TABLE II: DIGITAL FORENSIC INVESTIGATION PHASES IN DIFFERENT MODELS

Kruse and Heiser	**Department of Justice**	**DFRWS**	**ADFM**	**IDIP**	**SRDIFM**	**DSCFIPM (Domain Specific Cyber Forensics Investigation Process Model)**
2001	**2001**	**2001**	**2002**	**2003**	**2011**	**2014**
3 phases	**4 phases**	**6 phases**	**9 phases**	**5 phases**	**11 phases**	**10 phases**
Acquiring Evidence	Collection	Identification	Identification	Readiness	Preparation	Establishment of institutional cyber forensics investigations SOPs
Authenticating Evidence	Examination	Preservation	Preparation	Deployment	securing scene	Strategic planning & scope definition
Analyzing Evidence	Analysis	Collection	Approach strategy	Physical CSI	Survey and recognition	Crime Scene Sealing
	Reporting	Examination	Preservation	Digital CSI	documentation of scene	Evidence Collection (by Investigating Authorities)
		Analysis	Collection	Presentation	communicatio n shielding	Evidence Preservation
		Presentation	Examination		Evidence collection	Extraction of Relevant Evidences
			Analysis		Preservation	Evidence Analysis
			Presentation		Examination	Presentation of analysis and findings
			Returning Evidence		Analysis	Archiving of Case History Records
					Presentation	Post-case review
					Result and review	

Further phases are the elaborations of these main phases so these must be part of any digital forensic investigation process. Depending upon the nature of case, some further phases can also be of critical importance in the forensic investigation process. For example the preliminary investigation or preparatory investigation phase involving permissions, authorities, rules & regulations, laws and following hierarchies might be very long and strict in case of state matters or some government level official case involving cyber forensics investigation. However those can be comparatively easy and shorter process in some other case which does not involve high state officials or long hierarchies. So we can choose among many proposed forensic investigation models to best suit our nature of case and people involved [11]-[13].

The proposed model also consists of major phases used in most of the process models, and a few specific phases tailored according to the domain requirements.

The opted digital forensic investigation process model should suit the nature and requirements of the domain and moreover the particular case undertaken for investigations. The investigating organization or team can also tailor the existing process models according to their desired investigation flow. Or they can even add some new phases if they find those to fit in the flow and are significant for their investigations. That is why, the proposed DSCFIPM is elaborative and best suits the particular investigation flow to be carried out in the university domain. A further comparison of DSCFIPM with selected digital forensic investigation models is given below in Table III.

TABLE III: COMPARISON OF DSCFIPM WITH SELECTED DIGITAL FORENSIC INVESTIGATION MODELS

DSCFIPM	**Kruse and Heiser**	**Deptt. of Justice**	**DFRWS**	**ADFM**	**IDIP**	**CFFTPM**	**DFMMIP**	**GCFIM**	**SRDIFM**
Establishment of institutional cyber forensics investigation SOPs									
Strategic planning & scope definition				√	√	√	√	√	
Crime Scene Sealing					√	√			√
Identification of Relevant Evidences			√	√	√	√	√	√	√
Evidence Collection by Investigating Authorities	√	√	√	√	√	√	√	√	√
Evidence Preservation			√	√	√		√	√	√
Extraction of Relevant Evidences	√	√	√	√	√	√			√
Evidence Analysis	√	√	√	√	√	√	√	√	√
Presentation of analysis and findings		√	√	√	√	√	√	√	√
Archiving of Case History Records					√		√		
Post-case review								√	√

The comparisons helped identifying the advantages and shortcomings of each of the above mentioned models. Elaboration has been done in the previous section, so investigators should know the pros and cons of using each of these models. The comparative analysis shown above also showed that number of phases gradually increased as years advanced and more research was undertaken in the field of digital forensics.

So we may predict that in future we can see even more elaborative models for digital investigations which at one side will help the investigators have a predefined elaborative roadmap in their hands before starting their investigations, but on the other side it may add to the complexities with the addition of every new phase. Thus the investigators would have to have better knowledge and command on the details of digital forensics, and subsequently they will have to make people understand the need and purpose of the prolonged investigation process.

The proposed model has been developed using the major phases of existing models and tailoring them to suit the process flow of our selected domain.

V. Conclusion

The high number of forensic investigation models proposed and the great degree of variability among them signifies complexity of the nature of digital forensic investigation. Different models put an emphasis on a particular aspect of investigation or confined to address a limited number of scenarios. But over the last decade, a growing consensus has provided a strong foundation to digital forensic research to meet the growing challenges by offering sufficient diversity and flexibility with standardization in practices to enhance reliability and reproducibility in the outcome. The proposed model (DSCFIPM) can serve the purpose of laying foundation for providing secure and monitored computing environment to university students and employees.

References

[1] W. G. Kruse and J. G. Heiser, *Computer Forensics: Incident Response Essentials*, 1st ed., Addison Wesley, 2002.

[2] M. Reith, C. Carr, and G. Gunsch, "An examination of digital forensic models," *IJDE*, vol. 1, issue 3, 2002.

[3] *Technical Working Group Electronic Crime Scene Investigation-A Guide for First Responders*, USDOJ, July 2001

[4] G. L. Palmer, "A roadmap for digital forensic research," Technical Report DTR-T0010-01, DFRWS, Utica, New York, 2001.

[5] A. Agarwal, M. Gupta, S. Gupta, and S. C. Gupta, "Systematic digital forensic investigation model," *IJCSS*, vol. 5, issue 1, pp. 118-131, 2011.

[6] Y. B. Yunus, I. Roslan, and H. Zainuddin, "Common phases of computer forensics investigation models," *International Journal of Computer Science & Information Technology*, vol. 3, no. 3, June 2011.

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

[8] M. K. Rogers, J. Goldman, R. Mislan, T. Wedge, and S. Debrota, "Computer forensics field triage process model," *Journal of Digital Forensics, Security and Law*, vol. 1, no. 2, 2006.

[9] P. Sundresan, "Digital forensic model based on Malaysian investigation process," *International Journal of Computer Science and Network Security*, vol. 9, no. 8, 2009.

[10] V. Baryamureeba and F. Tushabe, "The enhanced digital investigation process model," *Asian Journal of Information Technology*, vol. 5, issue 7, 2006.

[11] E. Casey, G. Katz, and J. Lewthwaite, "Honing digital forensic processes," *Digital Investigation*, pp. 138-147, 2013.

[12] G. Ruibin *et al*., "Case-relevance information investigation: Binding computer intelligence to the current computer forensic framework," *IJDE*, vol. 4, issue 1, 2005.

[13] S. R. Selamat, R. Yusof, and S. Sahib, "Mapping process of digital forensic investigation framework," *IJCSNS*, vol. 8, issue 10, pp. 163-169, October 2008.

Rabail Shafique Satti was born in Rawalpindi, Pakistan. She is a higher education scholar in the field of computer engineering. She is a registered software engineer with Pakistan Engineering Council since 2007. She further pursued her MS degree in the field of computer engineering from the Center for Advanced Studies in Engineering (CASE), Islamabad, in 2014. She is currently employed at Fatima Jinnah Women University, Pakistan. Her areas of interest are computer networks, information security, cyber forensics, and data mining.

Fakeeha Jafari was born in Sialkot, Pakistan. She is a higher education scholar in the field of computer engineering. She received her bachelor's degree in the field of computer sciences in 2008 from Fatima Jinnah Women University Rawalpindi, Pakistan and further pursued her master's degree in the field of computer engineering from CASE (Center for Advanced Studies in Engineering) Islamabad, Pakistan, in 2014. She is currently employed at Fatima Jinnah Women University, Pakistan. Her areas of interest are computer networks, information security, cyber forensics, and digital image processing.