Review Paper on Digital Forensics Practices: A Road Map for Building Digital Forensics Capability

SHAASWAT MUKHERJEE[1], SHAZIA HAQUE[2]
[1,2]*Department of Information Technology, Poornima College of Engineering, Jaipur, Rajsthan*

Abstract -- This paper gives you an insight on how to identify the needs for building and managing Digital Forensics Capability (DFC) are important because these can help organizations to stay abreast of criminal's activities and challenging pace of technological advancement. The field of Digital Forensics (DF) is witnessing rapid development in investigation procedures, tools used, and the types of digital evidence. However, several research publications confirm that a unified standard for building and managing DF capability does not exist.

I. INTRODUCTION

The increasing number of cybercrimes put a pressure on organizations to implement cyber forensics tools to fight against such activities. Many organizations spend time and money to stop such threats which are becoming harder to deal with as technology develops and its use becoming more affordable for more people.

Deciding on a suitable research methodology is challenging for researchers. In the paper, grounded theory is presented as a systematic and comprehensive qualitative methodology in the emergent field of digital forensics research. The paper applies grounded theory in a digital forensics research project undertaken to study how organizations build and manage digital forensics capabilities. The paper gives a step-by-step guideline to explain the procedures and techniques of using grounded theory in digital forensics research. The paper gives a detailed explanation of how the three grounded theory coding methods can be used in digital forensics research. Grounded theory offers a rich and detailed methodology for theorizing while presenting and exploring the How and Why questions at every stage of the research. The method shared in this paper provided a detailed critique, making it a valuable contribution to the discussion of methods of analysis in the field of digital forensics.

Several researchers show that there is no unified standard or framework for developing, managing, and implementing DFC in organizations with proper staffing, training, education, selecting tools, management, and governance.

II. OBJECTIVE OF THE PAPER

This research identifies, documents, and analyses existing DF frameworks and the attitudes of organizations for establishing their team, staffing and training, and acquiring and employing effective tools in practice.

It also looks into various leading approaches and practices in the DF community for carrying out digital investigations and more importantly the precise steps for setting up the laboratories.

It provides an introduction to the research states the problems, explains research aims and objectives and contribution to knowledge. It discusses the review of the literature.

It explains the research methodology by defining the research methodology implemented. It explains methods and instruments adopted in the research providing justification for the selection of each instrument and method.

It describes the pilot study and initial data collection design including explanation of the organizations. It describes data analysis and explains how the researcher applied grounded theory using straussian procedures and techniques to analyze data collection. It reports the outcomes of the research data. It proposes a framework, which expresses the relationships among abstract concepts in DFOs.

III. DIGITAL FORENSICS

Digital forensics is the process of uncovering and interpreting electronic data.

The goal of the process is to preserve any evidence in its most original form while performing a structured investigation by collecting, identifying and validating the digital information for the purpose of reconstructing past events.

The context is most often for usage of data in a court of law, though digital forensics can be used in other instances. The actual collection of evidence is a critical step in the investigative process.

Each piece of evidence collected must be handled in a way that preserves its integrity and any trace evidence, and that provides for a detailed record of its whereabouts from the time of collection to the time it arrives in a court room.

Failure to pay proper attention to any one of these areas can easily result in one or more pieces of evidence having no value in court or in administrative proceedings.

IV. RESEARCH METHODOLOGY

Pickard (2007) classified research methodology in a hierarchical structure; this hierarchy provides levels of views to the research methodology. The figure below shows the hierarchy of research methodology according to Pickard's classification providing examples for each level.

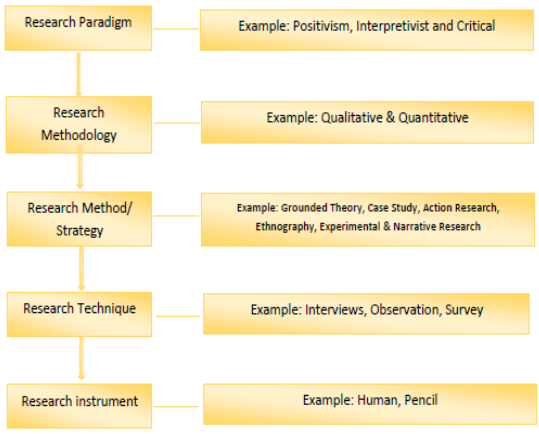


Fig. 1 Research Methodology

V. GROUNDED THEORY

According to Glaser & Strauss (1967), a researcher may use Grounded Theory to generate or discover a theory based on an analysis of data.

Martin and Turner (1986) defined the methodology as "an inductive, theory discovery methodology that allows the researcher to develop a theoretical account of the general features of a topic while simultaneously grounding the account in empirical observations or data."

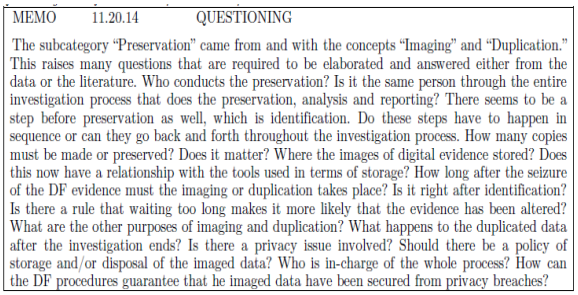
The researcher deals with the data in two stages: (1) the selection of data, which involves theoretical sampling of data based on the potential contribution to development theory; and (2) data analysis and coding into categories.

The second process involves:

- Identifying categories in data
- Building relationship between categories
- Grouping categories together to form a theoretical construct

VI. DATA ANALYSIS

To collect the data, the researcher employed the questioning technique which allowed the researcher to consider potential categories, their properties and dimensions. The basic types of questions that the researcher used as a guide were the 5Ws plus 2H, or Who, What, Where, When, and Why plus How and How much? Of course, many questions came naturally as the researcher responded to the data. The researcher applied the memo creation process while employing the questioning technique to make the process systematic and documented for later referencing. An example is presented below.



MEMO 11.20.14 QUESTIONING

The subcategory "Preservation" came from and with the concepts "Imaging" and "Duplication." This raises many questions that are required to be elaborated and answered either from the data or the literature. Who conducts the preservation? Is it the same person through the entire investigation process that does the preservation, analysis and reporting? There seems to be a step before preservation as well, which is identification. Do these steps have to happen in sequence or can they go back and forth throughout the investigation process. How many copies must be made or preserved? Does it matter? Where the images of digital evidence stored? Does this now have a relationship with the tools used in terms of storage? How long after the seizure of the DF evidence must the imaging or duplication takes place? Is it right after identification? Is there a rule that waiting too long makes it more likely that the evidence has been altered? What are the other purposes of imaging and duplication? What happens to the duplicated data after the investigation ends? Is there a privacy issue involved? Should there be a policy of storage and/or disposal of the imaged data? Who is in-charge of the whole process? How can the DF procedures guarantee that he imaged data have been secured from privacy breaches?

Fig. 2 Data Analysis Questionnaire

VII. APPLICATION OF AXIAL CODING PROCEDURE

Axial coding is the process of putting the data back together in new ways by making connections between categories and subcategories. Simply put, it is the "process of relating categories to their subcategories". It comes after identifying categories in the open coding process by finding relationship between the categories and subcategories. The researcher applied axial coding to the data using the paradigm model, and then by developing the categories using the paradigm model and identifying the properties and dimensions of the categories and subcategories.

VIII. THE PARADIGM MODEL

In the axial coding process, the relationships among the subcategories and categories are linked by identifying the (1) causal condition, (2) phenomenon or concept, (3) context, (4) intervening conditions, (5) action/interaction strategies, and (6) consequences.

The paradigm model has been commonly referred to in the following simplified diagram:

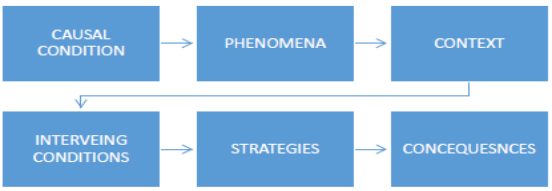


Fig. 3 Paradigm Model

It is important to use this model in any GT analysis because failure to do so will lead to a "lack of density and precision" in the analysis. The researcher used the paradigm model to link relationships among subcategories and categories. An example of the use of the paradigm model is shown in the following table:

Paradigm Model Sample

Causal Condition	Phenomena	Context	Intervening Conditions	Strategies	Consequences
Crime	Investigation	Digital or electronic evidence	Destruction of Digital Evidence	DF Investigation Framework	Finding of Evidence/ solving case
Finding digital device at crime scene	Type of DF investigation	Inside PC/ Mobile/ Flash Drive	Challenges to Investigation	Identification	Not finding evidence
Receiving request from client	Type of DF laboratory			Preservation	Reporting of findings
Request for research and development	Length of investigation			Analysis	Court testimony
Request to test security	Recurrence			Tool specific strategies	Eliminate security breach
Security breach (ie hacking, or misuse of information	Type of crime				Create mechanism to prevent future breaches

Fig. 4 Model Sample

IX. DIGITAL FORENSICS ORGANIZATIONS CORE CAPABILITY FRAMEWORK

"A digital forensics organization's capability is the sum of a digital forensics organization's core capabilities of people, infrastructure, and investigative capability governed by a comprehensive set of policies leading to a unique capability"

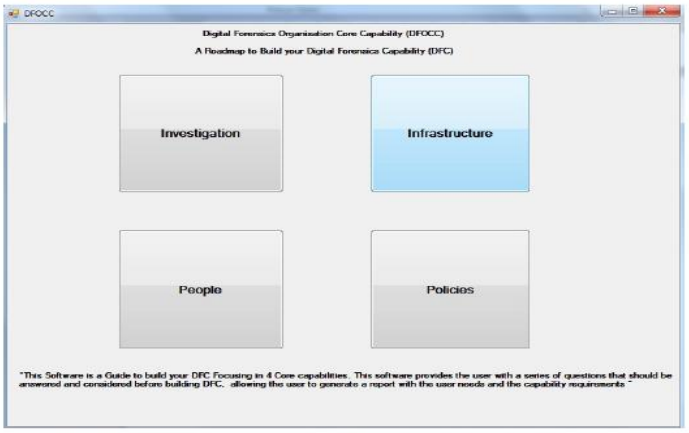


Fig. 5 The framework page

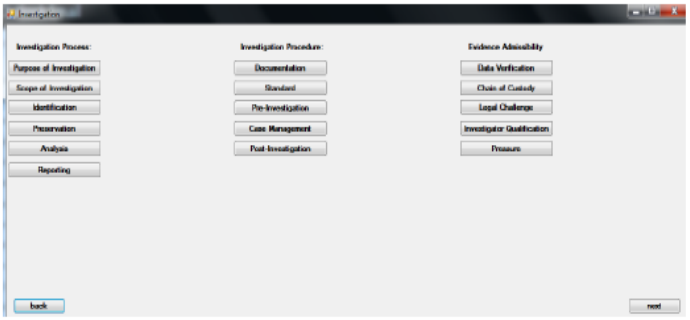


Fig. 6 The Investigation Page

Fig. 7 The Infrastructure Page

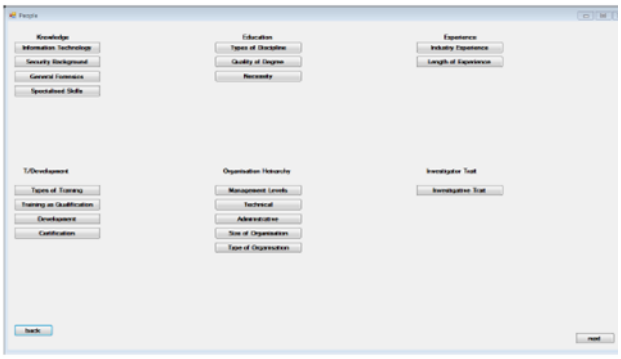


Fig. 8 The People Page

Investigation	Infrastructure
--->Incident Handling Pre-Investigation --->Evidence Status	Forensic Analysis Software --->Open Source Process --->Requirement Analysis
People	**Policies**
Specialised Skills --->Task based jobs ----------	Lab Accrediation --->-Reason for accreditation Technology Use --->-Use of Mobile Phones

Fig. 9 The Final Report

X. CONCLUSION

The paper shows how to apply GT methods using the Straussian approach in DF research.

Researchers demonstrated how they grounded the data in their categories, properties and dimensions. The grounding to the data is what gives the research method its integrity and strengthens the theory the researcher arrives at. Researchers should not forget that the GT method is ultimately about theorizing. It is more important, however, to explain how one arrived at such theory with the research data.

Such theorizing must be demonstrated through an explanation of the story line and then grounded in both the literature and the data. Digital Forensic Organization Core Capability (DFOCC) is the framework derived from analyzing data using grounded theory. DFOCC enhances the admissibility of evidence as it requires that a DF organization has made certain procedures part of its business process. The framework is simple because it is narrowed down to four variables (Policy, People, Infrastructure, and Investigation) that are required for a DF organization to be DF capable. The DFOCC framework will help the entire digital forensic investigation process prove the guilt of a perpetrator because the DFOCC will help organizations ensure that they have the correct resources and procedures in place to carry out investigations efficiently. The DFOCC framework aims to reduce the possibility of successful challenges to DF evidence presented in courts.

Finally, what is important in grounded theory is not the result but the process.

"The grounded theory method emphasizes the process of analysis and the development of theoretical categories, rather than focusing solely on the results of inquiry"