

**QUANTIFICATION OF AVAILABLE DIGITAL FORENSIC  
FRAMEWORKS TO IMPROVE THE FORENSIC INVESTIGATION  
PROCEDURE – PN AS TEST SUBJECT**



By

Muhammad Yassir Mushtaq  
(Registration No: 00000359179)

Department of Cyber Security  
Pakistan Navy Engineering College (PNEC)  
National University of Sciences & Technology (NUST)  
Islamabad, Pakistan  
(2022)



**QUANTIFICATION OF AVAILABLE DIGITAL FORENSIC  
FRAMEWORKS TO IMPROVE THE FORENSIC INVESTIGATION  
PROCEDURE – PN AS TEST SUBJECT**



By

Muhammad Yassir Mushtaq  
(Registration No: 00000359179)

A thesis submitted to the National University of Sciences and Technology, Islamabad,

in partial fulfillment of the requirements for the degree of

Master of Science in Cyber Security

Supervisor: Dr. Asif Mansoor

Co Supervisor 1: Dr. Bilal Muhammad Khan

Co Supervisor 2: Muhammad Samiullah Awan

Pakistan Navy Engineering College (PNEC)

National University of Sciences & Technology (NUST)

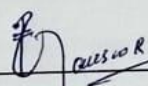
Islamabad, Pakistan

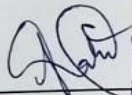
(2022)

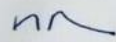


### THESIS ACCEPTANCE CERTIFICATE

Certified that final copy of MS thesis written by Lt Cdr Muhammad Yassir Mushtaq PN Reg No. 00000359179 of NUST- PNEC (College) has been vetted by undersigned, found complete in all respects as per NUST Status/Regulations, is free of plagiarism, errors, and mistakes and is accepted as partial fulfillment for award of MS degree. It is further certified that necessary amendments as pointed out by GEC members of the scholar have been incorporated in the said thesis.

Signature:  DR. ASIF MANSOOR  
Name of Supervisor Dr. Asif Mansoor Associate Professor  
Dated: 22-12-23 NUST-PNEC

Signature: HoD  AALIYA ALI  
Et Cdr Pakistan Navy  
Dated: 22-12-23 HOD CySD

Signature: (Dean/Principal):  \_\_\_\_\_  
Dated: 22-12-23 OR NAHEEM KURESHI  
Commodore  
DEAN MIS  
PNS JAUHAR

## **CERTIFICATE FOR PLAGIARISM**

1. It is certified that PhD / M.Phil / **MS** Thesis Titled **“Quantification of Available Digital Forensic Frameworks to improve the forensic investigation procedure – PN as test subject”** by **Lt Cdr Muhammad Yassir Mushtaq PN (2020-NUST-MS Cyber Security (CyS Fall 20)** has been examined by us. We undertake the follows:

- a. Thesis has significant new work / knowledge as compared already published or is under consideration to be published elsewhere. No sentence, equation, diagram, table, paragraph or section has been copied verbatim from previous work unless it is placed under quotation marks and duly referenced.
- b. The work presented is original and own work of the author (i.e. there is no plagiarism). No ideas, processes, results or words of others have been presented as Author own work.
- c. There is no fabrication of data or results which have been compiled / analyzed.
- d. There is no falsification by manipulating research materials, equipment, or processes, or changing or omitting data or results such that the research is not accurately represented in the research record.
- e. The thesis has been checked using TURNITIN (copy of originality report attached) and found within limits as per HEC Plagiarism Policy and instructions issued from time to time.

### **Name & Signature of Supervisor**

  
**DR. ASIF MANSOOR**  
Associate Professor  
NUST-PNEG

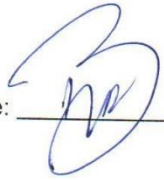
# National University of Sciences and Technology

## MASTER'S THESIS WORK


We hereby recommend that the dissertation prepared under our supervision by: (Student Name & Regn No.) Lt Cdr Muhammad Yassir Mushtaq PN (00000359179) Titled: Quantification of Available Digital Forensic Frameworks to improve the forensic investigation procedure – PN as test subject be accepted in partial fulfillment of the requirements for the award of Master's degree.

### EXAMINATION COMMITTEE MEMBERS


1. Name: Dr. Bilal Muhammad Khan

Signature: 

2. Name: Asst. Prof. M Samiullah Awan


Signature: 

Supervisor's name: Dr Asif Mansoor

Signature: 

Date: 22-12-23


**DR. ASIF MANSOOR**  
Associate Professor  
NUST-PNEC

  
**AMIN ALI**  
Head of Department  
HOD CySD

Date

### COUNTERSIGNED

Date: \_\_\_\_\_

  
Date / Principal

**DR NADEEM KURESHI**  
Commodore  
DEAN MIS  
PNS JAUHAR





### CERTIFICATE OF ORIGINALITY

I hereby declare that this submission is my own work and to the best of my knowledge it contains no materials previously published or written by another person, nor material which to as substantial extent has been accepted for the award of any degree or diploma at Department of Cyber Security at Pakistan Navy Engineering College or at any other educational institute, except where due acknowledgement has been made in the thesis. Any contribution made to the research by others, with whom I have worked at Pakistan Navy Engineering College or elsewhere, is explicitly acknowledged in the thesis. I also declare that the intellectual content of this thesis is the product of my own work, except for the assistance from others in the project's design and conception or in style, presentation and linguistics which has been acknowledged.

Author Name: M. YASSIR MUSHIAD.

Signature: \_\_\_\_\_

## **DEDICATION**

I dedicate this dissertation to my parents, colleagues, and honorable teachers  
for their love and affection

## **CERTIFICATE OF ORIGINALITY**

I hereby declare that this submission is my own work and to the best of my knowledge it contains no materials previously published or written by another person, nor material which to as substantial extent has been accepted for the award of any degree or diploma at Department of Cyber Security at Pakistan Navy Engineering College or at any other educational institute, except where due acknowledgement has been made in the thesis. Any contribution made to the research by others, with whom I have worked at Pakistan Navy Engineering College or elsewhere, is explicitly acknowledged in the thesis. I also declare that the intellectual content of this thesis is the product of my own work, except for the assistance from others in the project's design and conception or in style, presentation and linguistics which has been acknowledged.

Author Name:

Signature: \_\_\_\_\_

## **ACKNOWLEDGEMENT**

Glory be to Allah (S.W.A), the Creator, the Sustainer of the Universe. Who only has the power to honor whom He pleases, and to abase whom He pleases. Verily no one can do anything without his will. From the day, I came to NUST till the day of me. Departure, He was the only one Who blessed me and opened ways for me, and showed me the path of success. There is nothing which can payback for His bounties throughout my research period to complete it successfully

## TABLE OF CONTENTS

### CHAPTER.01

• Introduction	01
• Background	02
• Problems with Cryptography	04
• Organizational Framework	04
• The Obstacles to DF Readiness	04
• Awareness and Support from Management	04
• Tools and Training	04
• Problem Statement	05
• Background	06

### CHAPTER.02

• Digital Forensic	09
• Background	09
• Case study	09
• Step 1: Alerting and responding to incidents	10
• Physical Inquiry	10
• Digital Inquiry	10
• Step 2: The crime scene must be secured	11
• Physical Inquiry	11
• Digital Inquiry	11
• Step 3: Gather proof	11
• Physical Investigation	11
• Digital Investigation	12
• Step 4: Reconstruct the incident and analyze the evidence	12
• Physical Investigation	12
• Digital Investigation	13
• Step 5: Show the results	13
• Digital investigation	13
• Legal	15
• Internal audit	15
• Human resources	16
• Justifications for having forensically sound procedures and evidence on hand	16
• Cybercriminals	17
• War Dialers	18
• Password Crackers	18
• Keyloggers	18
• Email Capture	18
• Trojan Horses	18
• Dumpster Diving	18

• Types of attacks	18
• Definition of digital evidence	18
• Main Points from Case Study	21

### CHAPTER.03

• Df Frameworks Literature Review	25
• Frameworks that focus on the process	25
• First framework is Ó Ciardhuáin (2004)	26
• Second Framework: Carrier and Spafford (2003)	27
• Baryamureeba and Tushabe (2004) constitute the third framework	28
• Fourth Framework Beebe and Clark (2005)	29
• Louwrens et al. (2006b)	30
• Framework 6: E Casey (2004)	31
• Work in progress for our CDF ability	33
• ProDF component	33
• ActDF Component	33
• ReDF Component	34
• Crime Scene Forensic	34
• Conducting Digital Investigations	35
• FORZA (FORensic framework based on ZAchman framework)	36

### CHAPTER.04

• Pro-Active Df	38
• Introduction	38
• WHY PRODF?	38
• ProDF requirements	39
• Objectives for DF Readiness	40
• Garcia's (2005) DF Readiness Objectives	40
• Rowlingson's DF Readiness Objectives (Rowlingson, 2004)	41
• The four objectives we have for DF preparedness	41
• DF Preparedness Elements	41
• Garcia (2005)	41
• Rowlingson (2004)	42
• <i>Proposed DF readiness criteria</i>	42
• ProDF definition	43

## CHAPTER.05

- Reactive Df 46
- Introduction 46
- Redf Goals 46
- Redf Protocol 47
- Fourth Stage: Scenario Reconstruction 48
- Fifth Stage: Reporting Results 48
- Sixth Stage: Incident Closure 48

## CHAPTER.06

- Active DF 51
- Non-disruptive Nature of Systems 51
- Immediate Need for Live Evidence 52
- Crime-in-Progress Scenarios 52
- Timely Reaction 53
- Identifying Precursors 53
- Identifying the perpetrator 53
- Safety Enhancement 53
- ActDF definition 62
- Objectives for ActDF 62
- ActDF protocol 63
- Minimize User Intervention 64
- Necessary and Non-Intrusive Actions 64
- Minimal Alteration of Static Digital Evidence 64
- Order of Volatility and Priority 64
- Acquire Non-Priority or Volatile Evidence via Traditional Methods 64
- Copy or Extract Data Only When Original Data and Timestamps Remain Unaltered 64

## CHAPTER.07

- Comprehensive Df Capability 66
- DF Investigation Infrastructure 68
- To-do list 68
- Strategy for Proof Handling 69
- Proactive Identification 69
- Organizational Framework 69
- Evidence Assessment 69
- Policy Enhancement 70
- To-do list 70

• Establishing Pervasive Culture	71
• To-do list	72
• Comprehensive Strategy	72
• Policy and Procedural Framework	72
• Accreditation and Certification	72
• Tailored Programs	72
• Role-Based Training	72
• Code of Conduct	72
• Cost Effective Measure Integration	73
• To-do list	73
• Structured DFI Protocol	73
• Policy and Procedure Alignment	73
• Holistic Risk Management	73
• Cost Management Framework	74
• Utilization of DF Resources	74
• To-do list	75
• Reactive Df (Redf) Component	76
• Key Digital Forensic Phases	76
• Securing the digital evidence	79
• Second find and save any digital evidence that may be relevant	79
• Third stage, record all actions	80
• Development of Chronology	81
• Evaluation	81
• Exploration	81
• Integrating and correlating data	81
• Confirmation	81
• ReDF Presentation of findings phase	82
• Live Forensic of Real-time Evidence	83
• ActDF Phase 1: Incident response and confirmation phase	85
• ActDF Phase 2: ActDF investigation phase	86
• Acquire relevant live evidence	86
• Minimize User Intervention	87
• Necessity and Non-intrusiveness	87
• Minimal Modification	87
• Order of Volatility and Priority	87
• Traditional Evidence for Non-Priority or Volatile Data	87
• Copy or Extract Data with Minimal Impact	87
• Authenticate evidence	87
• ActDF Phase 3: Limited incident reconstruction phase	87
• To-do list	88



## CHAPTER.08

• Construction Of Quantified Df Management Framework	90
• Categorize The To-Do List	90
• Strengthening the Disaster Preparedness and Risk Management frameworks	93
• Policies	94
• Improve organizational risk administration and contingency planning	94
• Process dimension	96
• People dimension	99
• Technology dimension	100
• Consolidated View Of Our DFMF	102

## CHAPTER.09

• Conclusion	104
• Introduction	104
• ProDF component	105
• ProDF goal 1: Become DF-ready	106
• ActDF component	108
• Construction of our DFMF	109
• Possible difficulties in using Our DFMF and CDF Ability	110
• Success of the Thesis's goal	110
• Bibliography	112



# CHAPTER 1: QUANTIFICATION OF DF MANAGEMENT FRAMEWORK

## Introduction

Our world is becoming increasingly complex, with society increasingly relying on innovation and diversity (Rogers & Siegfried, 2004). The involvement of digital gadgetry in our everyday lives is undeniable. We speak with each other through email, close discussion groups, and use e-commerce products. Individuals tend to associate those on Facebook and other social media sites with proximity.

The combination of data-innovation products, frameworks, and administrations is changing the way we live. Nowadays smartphones come equipped with cameras, applications, and social organization get to, including sensitive information such as photos, emails, records, identities, etc. The loss of a smartphone can cause security and intellectual property problems outstanding results, especially in the case of Data Sec (Pieterse) , 2006) were written by him.

Organizations recognize the importance of protecting data and data products as a top business priority. Managers deal with multiple security measures, calculating security measures, canceling location policies, accessing controls, antivirus and computer programs, there is absolutely no system in place to ensure that potential threats are combatted is absolutely stupid, and security issues can still happen. These cases call for an investigation to uncover the root causes and possibly prosecute the perpetrators (Louwrens, von Solms,

Humanity has long looked to get between cause and effect, trying to figure out what happened, why, and why, and why Computer forensics has become mainstream time an expanding number of evils involve computers, making it expensive carefully proven to be far.

In 1984, the Federal Bureau of Investigation (FBI) established a research institute to develop a philosophy of cybernetic prov. In 1991, the term 'computer forensics' was introduced in the midst of a preparation at the Institute of Universal Affiliation (IACIS), an organization of experts in computer affiliation in Portland, Oregon.

The location of advanced breaches has become far more effective thanks to the use of PCs, World Wide Web, smart phones, and streak-drive remote gadgets. A search of a victim's personal computer hard drive may occur will no longer be sufficient to gather satisfactory evidence for an effective trial (Adelstein, 2006).

Proven computer dysfunction and instability are essential to identify the root causes of issues. In some cases it can be critical to monitor scheduling exercises, website usage, communication emails, and content on multi-capable phones or other sensitive devices so, computer-trained lawyers rely on agents to analyze additional information in a disclosed chain to establish links between attacker and victim (Stephenson, 2002) Presentation.

## Background

Entering a home, especially a fractured one, can stir up a mix of emotions—abuse, vulnerability, and confusion. Questions like "What did you steal?" and "Will home ever feel safe again?" flood the mind, along with worries about fortifying against future attacks. Similarly, when your computer falls victim to hacking, a similar wave of emotions crashes in. Thoughts revolve around what data has been snatched and what might be lingering, sparking concerns about the computer's future security.

While safeguarding computers for the long haul is crucial, the immediate focus gravitates towards the initial three questions, particularly if attacked system housed sensitive information or used for classified intents (Frye, 2005). This scenario underscores how both organizations and individuals grapple with cybercrime, underscoring the need to scrutinize these incidents. According to a survey, financial fraud tops list, closely followed by web-based bots and data loss, including customer ownership information (Richardson, 2008).

Despite the significance of conducting a forensic review of security issues, many organizations lack clear guidelines, often resulting in unsatisfactory outcomes (Sinangin, 2002). Forensic review doesn't always take precedence. Computer forensics plays a pivotal role in protecting, preserving, and presenting evidence, crucial in cases of abuse, enabling organizations to take appropriate action against wrongdoers (Sheldon, 2004). Identifying the reasons of the attack and understanding the assaulter's motives are paramount.

Forensics of computer includes many analytical techniques for magnetically stored evidence, whereas forensic computing includes methods from science for recovering, keeping intact, and examining various digital evidence types (TC-11, 2006).

DF covers a wide range of virtual proof, from smart phone data to changeable memory, expanding its footprint in the private sector, gaining importance for organizations. The need for strong evidence within organizations is rising, whether for disputed transactions, proving employee misconduct allegations, demonstrating legal compliance, or supporting insurance claims (Sommer, 2005).

Today, DF tools and practices are essential for every business looking to gather meaningful and legally acceptable evidence. It is essential to have forensic software, specialized technology, and rules. (Guidance Software, 2005). A forensic expert needs to ensure the authenticity of proof and outcomes, utilizing established procedures often referred to as "frameworks."

While DF tools are crucial for digital investigations and identifying loopholes in the information security framework (Richardson, 2008), organizations leverage them for other purposes. This entails strengthening information technology governance structures and demonstrating compliance with laws (Nikkel, 2006).

Existing Digital Forensics frameworks primarily focus on "post-mortem" investigations, offering guidelines on what to do and avoid during a forensic investigation. But frequently, they fail to consider how to manage or create a DF competence inside a business (Nikkel, 2006). The upcoming parts that delves into the obstacles associated with managing and implementing a Digital Forensics ability in an organization.

The review of the literature has revealed six key challenges, which are outlined below:

It's a common tendency for organizations to sideline the proactive collection of ample and admissible evidence before an incident, primarily due to apprehensions about associated costs (Rowlingson, 2004). Yet, it's crucial to recognize that having evidence readily accessible and well-defined processes can markedly diminish the usefulness of an interrogation.

This oversight in addressing evidence-related concerns undermines the efficacy of investigations. In incidents, the lack of ample, pertinent, and legally admissible evidence impedes the successful conduct and conclusion of investigations (Thomas, 2005).

The increase in active or "live" assaults has rendered the traditional DF frameworks inadequate for performing efficient incident investigations. In addition to containing the crisis or stopping current assaults, rapid measures are required to gather important, volatile, and crucial evidence in real-time in the event of these attacks. Due to the growing complexity and uniqueness of situations, the incorporation of live evidence has grown in importance within investigations. Attacks that take advantage of networks and the Internet are becoming more common, highlighting the need for gathering evidence in real-time.

The lack of a consensus on what constitutes live forensics, as well as standardized methods for conducting live investigations and difficulties in certifying and accepting live evidence, are among the significant problems highlighted by leong and Leung (2007) and others in the field.

Conventional DF methods are becoming more ineffective as new software and technology emerge at a dizzying rate. Consider the Bitlocker® disk encryption that comes standard in Windows® Vista Ultimate and Enterprise. Using the advanced encryption standard (AES) in cipher block chaining mode with a 128/256-bit key and the elephant diffuser1 adds an additional layer of protection to this strong disk encryption tool (TechNet, 2009). The fact that Bitlocker® does not have a backdoor makes it even more difficult for investigators to decrypt a device (Wikipedia, 2009). It is very uncommon for investigators to have to wait for the right time to inspect a suspicious computer in a "live" condition after decrypting the material. As a result, businesses must monitor technological developments closely and be prepared to respond to inquiries pertaining to emerging technology.

In addition, the continuing legal discussion about "decryption" obligations, especially in light of the tensions between the US and the UK, must be taken into account. The digital forensics landscape is already complicated, and this legal dispute just adds fuel to the fire by complicating investigators' access to plain text systems.

Regarding corporate governance and IT, the ancient adage "you can only manage if you can measure" is still relevant. It is critical to assess how well internal and technological controls are working. Management is required to provide evidence of the efficacy and efficiency of these controls according to corporate governance rules and reports like Sarbanes-Oxley and King III. In order to demonstrate due diligence within the context of good governance, digital forensics (DF) techniques and technology might be vital in producing recorded proof. In order to prove that you've complied with governance rules, this proof is crucial.

When it comes to building a forensic competence, Nikkel (2006) has identified a number of obstacles that businesses encounter in several domains:

**Problems with Cryptography:** An issue arises with encryption techniques that aren't commonly used because of the specific security requirements of Bitlocker™ Drive Encryption in Windows Vista Enterprise and Ultimate versions. The problem is that new ciphers need a lot of public evaluation to build confidence, yet current ciphers with extra security features are either too slow or not examined enough. A novel component dubbed the Elephant diffuser is used in conjunction with the well-established AES in CBC mode to provide speed and security in order to navigate this.

**Organizational Framework:** Crucial to the success of the DF group is establishment of its reporting structure. Choosing the appropriate department to report to, whether it's IT, managing risk, legal, and deciding whether or not to outsource of role. Additionally, it is necessary to determine the forensics team's level of engagement inside the company, whether it be leading, consulting, or providing assistance.

**The Obstacles to DF Readiness:** The acquisition of forensic resources, including qualified personnel, appropriate equipment, and a state-of-the-art forensic laboratory, is not without its difficulties. To make DF investigations easier, certain regulations like data preservation policies and investigative access policies need to be put in place

**Awareness and Support from Management:** Crucial to the success of any DF unit is the backing and understanding of upper management. Every person has to know what to do in the event of an incident and that the company has the competence to deal with disasters, and DF awareness should be a part of every procedure and workflow.

**Tools and Training:** In order to conduct effective investigations, the forensic team need training. It is also necessary to get forensic instruments that are both effective and pertinent in order to bolster the investigation.

Gathering evidence for certain situations and investigations is the main goal of companies who employ DF techniques and technology (Nikkel, 2006). Forensic investigators' legal standing is crucial, especially in matters that could go to trial. When dealing with incident-related data, investigators must be knowledgeable of privacy-related laws and their responsibilities under such legislation.

Existing DF frameworks have an emphasis on incident investigations, but they fail to acknowledge the benefits that companies may get from readily available data and forensically sound methods for reasons other than investigations, such gauging compliance with regulatory or legal mandates. This highlights

the need of a management and implementation structure that lets companies use DF skills in every part of their operations. The issue statement of the thesis will be presented in the part that follows.

## Problem Statement

The challenges highlighted in the literature review emphasize a notable gap—the lack of a comprehensive Digital Forensics (DF) framework for the effective administration and execution of a Comprehensive DF (CDF) ability within an organization. Existing literature and frameworks, fall short of offering a holistic solution for this specific purpose. The purpose of the thesis will be covered in detail in the next section.

This endeavor to formulate a comprehensive and theoretical Digital Forensics Management Framework (DFMF), specifically crafted to streamline the implementation and management of an effective Comprehensive DF (CDF) capability within an organization.

- Virtual Fraud and Virtual Proof
- Proposed CDF ability
- Determine, go over, and contrast different DF frameworks.
- Compare the DF architecture and viewpoints on DF ready to create a draft ProDF component with goals and procedures.
- Establish objectives and protocols for a ReDF research by contrasting the DF architecture.
- Create an ActDF component with DF goals and procedures by contrasting and assessing live and real-time research techniques and architectures.
- To create our CDF capability, we need to establish to-do lists and elaborate on the phases and steps that have been identified for each component.
- Talk about the connections between the specified elements of our CDF capabilities.
- Assist management in implementing the CDF capabilities by consolidating the to-do lists.

Organizations may manage and execute our CDF capabilities with the help of the framework (DFMF).

- Use combined lists as a guide while creating the DFMF.
- Determine which deliverables for each part of our CDF capabilities need to be executed, overseen, and the deliverables will be used to produce the DFMF.
- Sort the deliverables that have been identified using the DF dimensions.

- Using the connections between the DF dimensions, create a comprehensive, all-encompassing framework for DF deployment and administration (DFMF).
- An overview of "what to do, who should do it, and how it should be done" should be provided to management via our DFMF, so make sure it's simple to use.

Identify areas for further study and talk about possible obstacles to our DFMF's application.

We'll talk about the thesis's methodology in the next part.

To lay the foundation for the thesis and ensure clarity in terminology, a thorough examination of the literature is conducted. This includes defining digital evidence, exploring the concept of cybercrime, providing an explanation of Digital Forensics (DF), and assessing its necessity and relevance within organizational contexts. The objective is to create a comprehensive DF framework for the effective management and implementation of our Comprehensive DF (CDF) capacity, employing the following method.

## Background

This section of the thesis delves into existing DF frameworks to inform the development of our Comprehensive DF (CDF) competence. We will present multiple Digital Forensics and computer-based research architecture, along with recommended DF techniques from published sources. The investigated frameworks fall into three categories: a role-based framework (leong, 2006), hybrid architectures focused on processes, and auxiliary architectures that are based on processes.

In order to evaluate the extent of the recognized DF architectures, we will compare various role-based architectures with composite DF architectures that are based on procedures. This assessment will serve as a foundation for the creation and development of our CDF capability.

Three key elements will make up our intended CDF capabilities: ReDF, representing the real "post-mortem" investigation; ActDF, including the gathering and examination of real-time proof; and ProDF, aiding organizations in preparing for investigations. The key distinguishing factor among these components is the timing of the incident. An example of our CDF functionality in graphical form is shown in Figure 1.1 (below).



This section of the thesis aims to define our whole DF (CDF) capabilities and provide a comprehensive DFMF so that it may be arranged, managed, and used inside an enterprise. The following phases will be



improved in order to achieve this: • ProDF, ActDF, and ReDF: Use the information from the preceding chapters to clarify the terms and goals of each ProDF aspect and the ActDF and ReDF aspects.

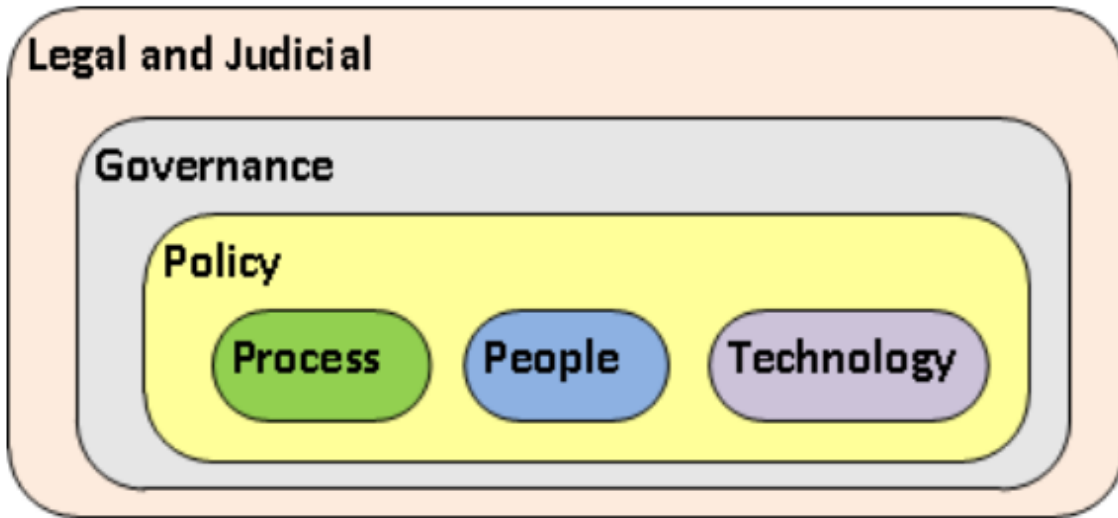
Create To-Do Lists for CDF Features: In order to direct the development of the DFMF, it is necessary to compile lists of tasks for the CDF capabilities, bearing in mind the factors discussed in the preceding chapters.

Elucidate the connections between the various parts of the CDF Describe the interdependencies between ProDF, ReDF, and ActDF, the three components that make up our CDF capabilities.

The subsequent task is to devise an execution and oversight framework for our CDF capability. The framework should offer clear instructions on deploying and maintaining the CDF capability, ensuring user-friendliness and practicality. Adherence to Casey's DF framework principles—acceptance, dependability, repeatability, ethics, causality, impact, and documentation—is crucial (Casey, 2004). According to these principles, the framework must follow professional procedures and methodologies from literature, ensuring processes are repeatable, yield reliable evidence, and meet Daubert or Frye standards. The investigation's findings must demonstrate a logical relationship between the evidence and the alleged incidents.

For effective management, we will create to-do lists for each part of our CDF capabilities (ProDF, ReDF, and ActDF). These task lists, also known as deliverables, represent tangible items that can be implemented, evaluated, and controlled. The execution of the list of outputs will be challenging, requiring a systematic methodology (framework). To structure this, relevant outputs will be combined, such connecting instructional materials and instruction with the "people area" or component.

We will formulate our DFMF using the six Digital Forensics (DF) dimensions (Grobler & Louwrens, 2006), These dimensions were determined by comparing materials from different perspectives on management and governance frameworks, aspects of information security, and issues posed by leong (leong, 2006). The dimensions require mutual assistance to yield meaningful results, with legal and judicial serving as the foundation for all other dimensions. A graphical illustration of the connection between the DF dimensions can be seen in Figure 1.2 (below).



*Figure 1. 1. Aspects of Digital Framework*

The subsequent moves involves utilizing the identified dimensions as categories to identify and group our Comprehensive DF (CDF) capabilities. By leveraging the relationships between these dimensions, we aim to design our Digital Forensics Management Framework (DFMF). This framework will be employed in the final chapter of this section to illustrate the potential benefits an organization could gain from applying our DFMF. We will discuss how the DFMF can be effectively used within an organization to manage and deploy our CDF capabilities.

## CHAPTER 2: DIGITAL FORENSIC

In our digitally interconnected world, the term "cyberspace" refers to a borderless virtual community where communication is fast and anonymous. However, these advantages also make it a breeding ground for cybercrime. The increasing importance of information has empowered criminals using computers for illicit activities, taking advantage of technical skills and the veil of anonymity.

Cybercriminals often target specific sectors, leading to financial losses for organizations. When a cyber incident occurs, a thorough investigation is essential, drawing inspiration from Locard's Exchange Principle. Digital forensics adheres to strict guidelines, such as the chain of proof and chain of ownership rules, which are essential for evaluating digital proof.

The use of scientific techniques to legal matters is emphasized in several definitions of the word forensics. The preservation of the integrity of proof in legal situations is contingent upon the investigation process in the field of digital forensics. The quality of evidence is influenced by forensic equipment, whose admissibility in court plays a crucial role. This chapter lays forth the fundamental framework for digital forensics, highlighting its applicability and important ideas.

### BACKGROUND

Numerous Pakistanis are accustomed to the investigating processes of law enforcement organizations because the country is plagued by crime and crimes are perpetrated on a daily basis. A typical forensic examination and an investigation into digital forensics are compared and contrasted using the following hypothetical situation.

#### Case study

A distressed neighbor frantically contacts the police, reporting a barrage of gunshots. Upon arrival, law enforcement discovers a lifeless body sprawled across the kitchen floor in a residence within a neighborhood protected by an independent security company. The older man victim is lying face down with a horrific gunshot injury to his head. The room, bearing signs of a struggle, is chaotic, with tables and chairs strewn about, and a mobile phone lies near the victim.

While awaiting the arrival of detectives and forensic experts, the police maintain a vigilant watch over the crime scene. Upon the investigators' arrival, scrutiny of the murder site reveals muddy footprints leading from the garden into the home, an open outdoor door to the lounge, and clear fingerprints on the patio door's window. The status of potential missing items remains uncertain, and the victim's car remains undisturbed in the garage. A preliminary theory on the incident is devised by the investigator.

To discern the motive behind the killing, investigators methodically seek evidence and potential clues. Establishing motivation involves presenting both "direct" and "indirect" proof, with the pose of the dead body serving as an example of the latter, offering insights into the suspect's location during the gunfire. Every conceivable piece of evidence, from shell casings to fingerprints, hair, and blood samples, as well as a laptop and cellphone, is meticulously filmed, bagged, and documented by the detectives for further examination at the investigative lab.

For regional surveillance, the security complex strategically deploys closed-circuit television (CCTV)

cameras at key locations. The investigators leverage camera footage and potential eyewitness accounts to glean crucial details before, during, and after the incident.

Determining the incident's motive prompts questioning of family members, neighbors, coworkers, and acquaintances to identify possible culprits and uncover motives. The victim is identified by a neighbor as John Smit, a flamboyant single accountant known for hosting gatherings and housing a sizable Rottweiler.

The primary detective initiates the compilation of an investigation file, encompassing details of the occurrence, involved detectives, and the initial responders. Included are a preliminary theory, arguments for the hypothesis, and an extensive inventory of evidence collected from the person in question and the crime scene. Conversations with associates, interview transcripts with possible suspects, press announcements, and permissions for additional evidence, such as mobile phone provider records, are carefully documented.

Establishing a motive proves challenging with limited evidence at the crime scene. The investigators recognize that understanding the victim's life, potential missing assets, and existing issues facilitates motive determination. Crafting a chronological timeline of events aids in focusing the investigation, and profiling helps identify potential culprits based on height and gender.

In line with the italicized directive, a connection between digital and physical investigations is explored by comparing the tasks of detectives and investigators. Five recommended actions are outlined: alerting and responding to incidents, securing the crime scene, gathering proof, reconstructing the incident, and analyzing the evidence before presenting the results. This approach aims to seamlessly integrate digital and physical investigative strategies for a comprehensive understanding of the unfolding case.

## **Step 1: Alerting and responding to incidents**

### **Physical Inquiry:**

In the realm of physical inquiry, the investigative process is set into motion upon the reception of an event alert. Drawing a parallel from the scenario study, where a vigilant neighbor promptly reported a crime to the police, a similar response is mirrored. In cases involving physical incidents, the involvement of external authorities is integral, and the investigation is seamlessly handed over to law enforcement. This immediate engagement with officials characterizes the typical trajectory of a physical inquiry.

### **Digital Inquiry:**

On the digital front, an incident alert emerges through various channels, possibly triggered by an advanced system like an intrusion detection system (IDS) or by an employee flagging suspicious behavior to the help desk. Unlike the swift involvement of external authorities in the physical scenario, the Internal Response (IR) team takes charge of managing and overseeing the event internally during a digital inquiry. Interestingly, in contrast to the physical case study, digital investigations often progress without immediate contact with external officials. According to the CSI security study by Richardson (2012), a mere 27% of participants reported safety events to the authorities early in the investigation.

This dichotomy underscores the distinct nature of physical and digital inquiries, where external involvement is more intrinsic to physical scenarios, while digital investigations often undergo an initial internal assessment before considering external engagement. The hesitancy to involve authorities early in digital cases may be influenced by factors such as the need for thorough internal scrutiny and the evolving landscape of cyber threats.

## **Step 2: Secured the scene of the crime:**

### **In person Inquiry:**

In the context of a physical inquiry, meticulous efforts are made to safeguard every piece of evidence. In the referenced case study, investigators implement a lockdown of the actual crime scene, creating a well-defined and protected perimeter. The "shut down" nature of the crime scene in the case study ensures that unauthorized individuals are barred from accessing the crucial evidence. This controlled and restricted environment allows investigators to preserve the integrity of the crime scene.

### **Digital Inquiry:**

Contrastingly, the virtual scene of the crime poses unique challenges as it may encompass a blend of real and virtual spaces, often eluding a clear and distinct definition. Unlike the well-delineated nature of a physical crime scene, the digital counterpart might extend across multiple nations, presenting complexities that can significantly impede the investigation. The sheer breadth and virtual nature of digital crime scenes make them susceptible to compromise, adding layers of difficulty for investigators.

#### **Preservation Challenges:**

- In the digital realm, organizations, driven by the necessity to resume operations swiftly, often prioritize minimizing the impact of an incident. Unfortunately, this urgency sometimes results in insufficient consideration given to preserving evidence or ensuring the forensic soundness of processes post-occurrence. As highlighted by Sommer (2005), this oversight in digital forensic investigations frequently exposes them to risks, with evidence being compromised or unintentionally deleted by personnel who may not fully comprehend the intricacies of preserving digital evidence. This underscores the vulnerability of digital investigations and the importance of enhancing awareness and procedures to mitigate such risks.

## **Step 3: Gather proof.**

### **Physical Investigation:**

In the initiation phase of a physical investigation, the primary focus revolves around the identification and meticulous collection of diverse forms of evidence. The designated investigators are highly skilled and follow set protocols, guaranteeing that the proof collected is not only legally acceptable but also managed precisely. These investigators use specific techniques designed to obtain different kinds of evidence, such as finger prints, samples of blood, and mobile phone records. Every category demands a

different strategy, demonstrating the analysts' attention to detail when managing various types of proof.

The investigation strategically leverages evidence derived from CCTV cameras, potential eyewitness accounts, and records from security gates at the complex's entrance. This multifaceted approach provides substantial information for the detectives to reconstruct events leading up to, during, and after the commission of the crime.

Promptly establishing a motive is a key objective for the investigators, enabling them to construct a profile of the suspect and identify specific evidence crucial for a successful prosecution. The meticulous documentation and packaging of all evidence according to predefined standards further contribute to its admissibility in court.

### **Digital Investigation:**

In the domain of digital investigations, specific Digital Forensics (DF) frameworks guide investigators through structured phases and steps for identifying, acquiring, and analyzing digital evidence. However, a limited number of organizations have the necessary structure in place for cost-effective, minimally disruptive, and efficient digital investigations. This lack of preparedness is often attributed to untrained employees unaware of digital evidence requirements, leading to potential evidence contamination.

Digital investigators have a vast array of digital evidence types at their disposal, including static (e.g., log files), live (e.g., registry content), legacy, and audio evidence. The confiscated cell phone in the present case holds potential digital information that can serve as crucial evidence, necessitating distinct DF tools and acquisition procedures to ensure its integrity.

To enhance proactive evidence gathering, organizations should consider collecting potential evidence before and during incidents, as outlined in existing DF frameworks and readiness models. The importance of extending research into live investigations is underscored, emphasizing the need to evaluate infrastructure and evidence availability.

In digital forensics, it is important to formulate an idea at an early stage, emphasizing the significance of businesses being prepared for defence in order to assess all conceivable outcomes, dangers, weaknesses, and supporting data. As mentioned by (Rowlingson, 2004), certain groups could be hesitant to incorporate criteria for proof due to financial considerations.

Even though the digital crime scenario is not the same as the real thing, some objects, including cams and proof bags, are nonetheless important for keeping digital proof safe. Authorized DF tools are necessary for the capture of digital proof on a hard drive in order to guarantee its admission in court, given the vulnerability of digital proof to manipulation or compromise. Care must be taken to maintain the authenticity of such proof in order to conduct an effective digital inquiry.

## **Step 4: Rebuild the event and examine the available data:**

### **Physical Investigation:**

In the process of a physical investigation aimed at discerning a motive and identifying the culprit,

the detectives undertake a meticulous examination of the gathered evidence. Key materials, including DNA and fingerprints, are dispatched to forensic laboratories specializing in the nuances of these types of cases. The investigative team engages in a critical evaluation to determine whether additional evidence is required or if the existing evidentiary foundation substantiates the formulated motivation or hypothesis. The outcome of this comprehensive assessment is the creation of a detailed case file meticulously compiled by the detectives overseeing the case study.

### **Digital Investigation:**

In the sphere of digital investigation, an analysis and reconstruction of the incident occur through the scrutiny of digital data. Within a Digital Forensics (DF) investigation lab, the investigator conducts a thorough examination of the digital evidence. The inquiry team, responsible for the digital investigation, evaluates whether the evidence aligns with the formulated hypothesis or motive, or if supplementary data is necessary for a more comprehensive understanding.

Similar to the physical investigation, the digital inquiry culminates in the compilation of a detailed case file by the DF investigator. This case file serves as a comprehensive repository of essential information, encapsulating the nuances of the digital evidence, the analysis conducted, and the conclusions drawn during the investigative process. The thesis generated as part of this procedure contributes valuable material to the case file, enriching the overall documentation and aiding in the resolution of the digital investigation.

### **Step 5: Show the results**

**Digital investigation:** When providing digital proof and cases in court, more care and planning must be taken. Documentation must be prepared in a way that the courts can comprehend.

The background information on the parallels between a physical and digital investigation, as well as the issues and procedures that need to be considered while carrying out a digital investigation, have all been covered in the preceding discussion. DF is the topic of the next section.

In a society heavily reliant on technology for communication and day-to-day operations, cybercriminals exploit both human vulnerabilities and technological weaknesses to launch attacks. Computer forensics was traditionally the main tool used by investigators to look into computer-related occurrences. For the purposes of evidential and root cause analysis, several definitions have been put out, including recognizing, obtaining, recording, and deciphering data from computers (Kruse & Heiser, 2004).

But as digital proof and tools continue to advance, a more comprehensive approach is required, which is why digital forensics has emerged. Digital forensics, in contrast to computer forensics, covers all digitally recorded proof and goes beyond one device. Scientifically developed procedures for the preservation, gathering, verification, examination, evaluation, recording, and display of computer proof for the purpose of recreating criminal incidents are among the meanings (Reith et al., 2002).

Many investigators see virtual forensics as the procedure of gathering proof to identify digital crime perpetrators and build a prosecutorial case. It can take two directions:

Adopting the TC-11 definition, digital forensics is a discipline supported by fundamental characteristics, such as confidentiality, integrity, and availability, similar to information security. These characteristics underpin all digital forensics activities in organizations (TC-11, 2006).

Companies have come to realise the significance of proactive steps in digital forensics, which guarantee the availability of data, rather than only reacting when an incident occurs. Despite using proactive measures to collect evidence beforehand, such as reviewing footage from closed-circuit television cameras and possible records of gate entrance, in the provided scenario report, researchers conducted a receptive, post-event examination. This methodical strategy guarantees that evidence is available in real-time.

When asked for digital proof, however, organisations frequently fail to provide it because they fail to anticipate the requirement. A Manual to Evidence-Based Investigations (Sommer, 2005) states that in order for an organisation to be ready, it is essential to comprehend the reasons for using digital forensics and to fulfil evidentiary criteria.

Nikkel (2006) classified the reasons for using DF technology, tools, and digital evidence as either internal or external.

Nikkel (2006) posits that industry standards, legal and regulatory duties are the two external factors that push organisations to implement DF.

Standards like Sarbanes-Oxley, King II, and King III highlight management's accountability for an organization's information technology infrastructure, applications, and data, While business management is governed by different statutes and ordinances in various countries. It is the responsibility of management to guarantee compliance and the efficacy of controls, which is usually proved by evidence and good practices (Parkinson & Baker, 2005).

In order to satisfy governing body standards for reliable, successful, and productive operations, policies, and operations, organizations must evaluate all pertinent elements, including methods for managing change. The Sarbanes-Oxley Act of 2002 lays out the penalties for destroying important records on purpose (Sarbanes-Oxley Act of 2002, 2002).

If you want reliable data to back up your decisions, you need reliable IT systems. Providing crucial information to help management, Digital Forensics (DF) technologies and procedures have become more important (Nikkel, 2006).

Good governance may be demonstrated using evidence, which helps management evaluate performance and compliance. The business oversight reports by King II and III place a strong focus on risk control and demand comprehensive, documented assessments of significant risks. By utilising established models of risk management and internal controls, the board must keep the risk management system robust, providing reasonable confidence with respect to things like compliance, asset protection, and operational efficiency (von Solms & von Solms, 2009).



Corporate governance requirements like as King II require organisations to handle legal and law enforcement elements, ensure efficient controls, compliance, and responsible behaviour; a strong Digital Forensics (DF) capacity may help with this. To back up their evaluations of critical risk areas, managers might use DF tools and procedures.

Regulated sectors have unique needs, including governance and compliance considerations, as well as healthcare, insurance, telecommunications, and the financial sector. Compliance with industry standards and rules such as Swiss ISP log retention (Nikkel, 2006) are examples of such measures. A complex framework for responsible and compliant organisational activities is formed at the junction of sector-specific rules and general corporate governance requirements.

The CobiT approach was created by the ISACA and is an established method in the area of governance for IT. The CobiT collection of documents serves as the basis for IT governance practices (ITGI, 2000). The Statement of Auditing Practices is used in the United States to specify security audits (SAS70) (Wikipedia, 2012b).

Evaluating processes for gathering proof and event evaluation is crucial, as reinforced by the IAAC for guaranteeing DF preparedness and industry best practices like ISO/IEC 27001 and ISO/IEC 27002 for Information Security governance (ISO/IEC17799, 2005) (Sommer, 2005). Risk management and the need to present proof of dangers that have been recognized are among the fundamental elements. The preservation of digital proof ought to be considered in data safety architectures, as per recommended practices such as ISO/IEC 27001, which stress the need for enterprises to prepare for defence against inspections and guarantee the availability of proof. By maximizing the "four Ps"—people, processes, things, and partnerships—IT service administration seeks to manage and provide IT services throughout a business (Rudd, 2004). When it comes to developing policies and processes for overseeing IT services, the ITIL is commonly recognized as the industry benchmark. To make sure that SOPs and processes follow the DF rules, it is crucial to anticipate future demands and implementations of DF criteria.

Policy, control, and procedural implementation is supported by industry best practices. Assessing these controls is a must for strong management and excellent governance. When it comes to proving the efficacy of controls and processes that have been put in place, digital proof is a crucial piece that DF helps organizations get. What follows is an examination of the internal variables that are propelling DF implementation.

The reliance on digital evidence and trustworthy procedures is growing throughout organizations. Each of the following business functions need forensic expertise:

### **Legal**

After an incident, an organization's internal legal department will require assistance gathering evidence. Ensuring adherence to local rules and regulations is also crucial.

### **Internal audit**

According to ISACA G28 (ISACA, 2004), the internal audit division must apply forensic techniques in order to provide advice on fraud and illegal usage of IT infrastructure. Organizations may demonstrate that business rules and processes are being followed

with the use of a DF capability. Since DF will make it possible to gather more pertinent evidence when needed, auditing demands and suggestions will get a boost from it.

## **Human resources**

When it comes to proving employee wrongdoing, holding internal hearings that may lead to loss of employment, and in extreme situations, gathering proof of suicide or kidnapping, human resources will employ DF as a weapon.

Risk control and risk management are additional corporate divisions or entities that can gain from event investigation.

In organizations, intellectual property (IP) is crucial. DF is going to be able to help with any inquiries regarding IP infringement or abuse. Additionally, it will be employed in the process of looking into phishing attempts and bogus websites that could jeopardize the organization's reputation.

The utilization of digital forensics (DF) within the IT division extends to various critical functions. One such application involves assessing the security posture, aiding in intrusion analysis, as illustrated by Richardson in 2008. Additionally, DF proves invaluable in scrutinizing instances of IT policy violations, security breaches, and the misuse or abuse of IT infrastructure.

The versatility of forensic tools and expertise goes beyond traditional forensic purposes. They are instrumental in validating corporate disk-wiping protocols, confirming the appropriate use of wireless or disc security, and recovering information taken from a failed disc or outdated media. Moreover, DF plays a crucial role in addressing reasonable demands for recovering passwords, supporting cryptic fixing efforts, and enhancing the overall IT architecture of the organization.

An essential prerequisite for these applications is the availability of strong, high-quality data. The driving forces outlined in the subsequent section underscore the necessity for robust data and the effective utilization of DF tools. The following section succinctly summarizes the common causes identified.

## **Justifications for having forensically sound procedures and evidence on hand:**

Due diligence on Digital Forensics (DF) should be initiated by organizations for the reasons given. This proactive strategy includes measures to avoid problems in the future, such as collecting evidence before they happen, developing appropriate protocols (such a methodology for DF investigations), and providing explicit instructions on how to use DF tools.

The research (Louwrens et al., 2006b; Rowlingson, 2004) highlights that DF preparation meets some of these objectives by emphasizing staff training, ensuring that the facilities and assets needed for investigation of incidents are available, and ensuring that evidence is available. However, it excludes the application of DF methods for anything other compliance measurement or investigational reasons.

It is clear from the discussion and the stated goals that computer forensics is no longer just an investigation technique used after an occurrence. DF investigations now extend to the examination of incidents stemming from cybercrime and cyber-criminals. The ensuing section will briefly delve into

cybercrime, providing context for this thesis, given that the majority of investigations are prompted by incidents related to cybercrime.

The definition of cybercrime varies among individuals, with one perspective characterizing it as criminal activities conducted through a network utilizing communication devices like phone lines, the Internet, and mobile networks (Wikipedia, 2008). Broadly, cybercrime is described as unlawful actions carried out through computers and the Internet, categorized into three main types:

1. Cybercrimes against individuals.
2. Cybercrimes against the government.
3. Virtual crimes contrary to property (Babu & Parishat, 2004).

Categories included in the 2001 report of the Commission on Crime Prevention and Criminal Justice about the 10th United Nations Congress on Criminal Activity Reduction and Penal Rehabilitation:

Category 1: Offenses directed towards technology and users, including unauthorized entry into computer networks, unauthorized access, data theft, dissemination of malicious software, and digital espionage.

Online kidnappings, fraud, intellectual property crimes, betting, money laundering, and industrial espionage all fall within Category 2's traditional offenses involving communications or computer technology.

Thirdly, engaging in additional criminal activities with the use of technology.

In line with these definitions, unauthorized access emerges as a common goal in cybercrime, driving various types of attacks. Systems being breached for the purpose of stealing confidential information, spyware being distributed, websites being vandalized, domain names being hijacked, child pornography being transmitted, denial of service assaults, money laundering, eavesdropping online stalking, e-terrorism, digital warfare, bullying, prejudice, fraudulent trading, and copyright infractions are cases in point (Casey, 2011).

Noteworthy is the concept of cyberwarfare, denoting actions by a state or country against private, public, or governmental entities, exemplified by the STUXNET attack. The key distinction between traditional crimes and cybercrimes lies in the use of digital devices as tools for the latter, marking a paradigm shift in criminal methodologies.

## **Cybercriminals**

Cybercriminals emerge from diverse backgrounds, assuming various personas that span disenchanted employees, deliberate insiders, temporary workers, vendors, partners, external infiltrators, hackers, malicious code writers, fraudsters, unethical competitors, terrorists, organized crime networks, dissatisfied customers, idle teenagers, or individuals engaged in industrial espionage.

These perpetrators utilize an array of attack tools to execute their illicit activities, employing strategies such as:

- **War Dialers:** Application that calls a lot of numbers in a methodical manner in an effort to reach distant databases.
- The physical act of driving around to identify insecure wireless networks.
- **Credential Decoder:** Software created to decode credentials and grant unauthorized use.
- Programs designed to identify particular data trends, frequently with malevolent intent.
- **Keyloggers:** Technology that records every keystroke made by a user.
- **Email Capture:** Techniques for capturing email communications.
- **Trojan Horses:** Concealed malicious code capable of infiltrating systems.
- **Dumpster Diving:** A physical practice involving the examination of trash bins to extract sensitive information.

## Types of attacks

As the Internet and its uses continue to expand and the Information Society develops, cybercrime also continues to be a prevalent and ever-changing menace. New dangers include misleading apps, adware, malware, spoofing, phishing, and spam (Pieterse, 2006; Turner, Entwisle & Denesiuk, 2007).

Incidents occur when cybercrimes take place or when threats turn into attacks. Organizations need to put in place established mechanisms to handle and investigate these occurrences well. All of an organization's legal, incident response, business continuity, disaster recovery, audit, and forensic investigation processes should work together without a hitch.

Digital and electronic evidence are increasingly being demanded in today's courts and internal investigations, in addition to the more conventional document-based evidence. Producing pertinent, acceptable evidence and following well defined processes are essential in criminal investigations. The capacity to detect, retrieve, analyze, and properly record digital evidence is a crucial capability of digital forensics technologies and processes. To set the stage for the thesis, the next part will define digital evidence and give a brief overview of it.

Organizations rely on robust evidence to substantiate their assertions of corporate governance due diligence and to address both internal and external challenges (ISACA, 2004). This evidence forms the foundation for both external and internal forensic investigations. It's essential to recognize that evidence is important only when utilized to assemble the facts of a specified occurrence; it inherently lacks absolute certainty. The subsequent section introduces definitions of digital proof, various types of digital proof, and the attributes of compelling evidence. Additionally, a novel definition of comprehensive digital evidence is proposed based on the literature reviewed.

## Definition of digital evidence

Documents, testimonies, and other physical items can all be considered evidence if they have the power to confirm or deny a claim, according to Chawki's (2004) definition.

To aid in the categorizing of proof, the Scientific Working Group on Digital Evidence has created guidelines. The following are the categories:

Digital Evidence (Category 1): Includes data saved or transmitted electronically or magnetically, such as email messages, backups, logging data, eavesdropped data, and forensically recovered data. The following are examples of subtypes:

- Physical things and related data objects present during collection or seizure constitute original digital evidence.

Accurate digital replicas of data items derived from a physical thing provide duplicate digital evidence.

- Copy: Reproductions of data that are exact replicas of an original physical object, created apart from the object itself.

The contents of registers, swap files, or random access memory (RAM) from certain target machines provide live evidence.

Items that store or transfer digital information using physical media, such as flash drives, are included in Physical Evidence (Category 2).

Metadata, directory information, and configuration data associated with tangible objects or digital proof make up Data Objects (Category 3).

Three types of evidence are defined by Chawki (2004) from a legal perspective:

First, there is tangible evidence, sometimes known as real or physical items.

Category 2 Testimonial Evidence: Statements made by witnesses based on their own experiences or observations.

Substantial proof is proof that leans toward supporting an assumption but does not establish it. (Category 3).

Some more types of evidence are:

1) Technical Evidence: The outcomes of operations carried out on actual or original evidence by a forensic technologist; this is not evidence from an expert, but rather their own judgment.

2) Expert Evidence: refers to the views of people who are considered authorities in a certain subject or the results of an inquiry.

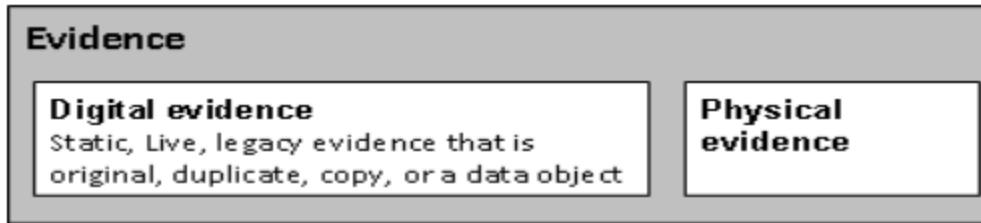
3) Derived Evidence: It includes things like charts or films made from main sources that show how conclusions were reached.

Regarding the analytical stage of an inquiry, digital proof falls into one of the following categories:

- Evidence Controversial: Claiming to back up the case's thesis.

- Incriminating Evidence: Evidence that runs counter to the case's premise.

Unrelated to the case's hypothesis, evidence of tampering suggests unlawful intervention with the system.



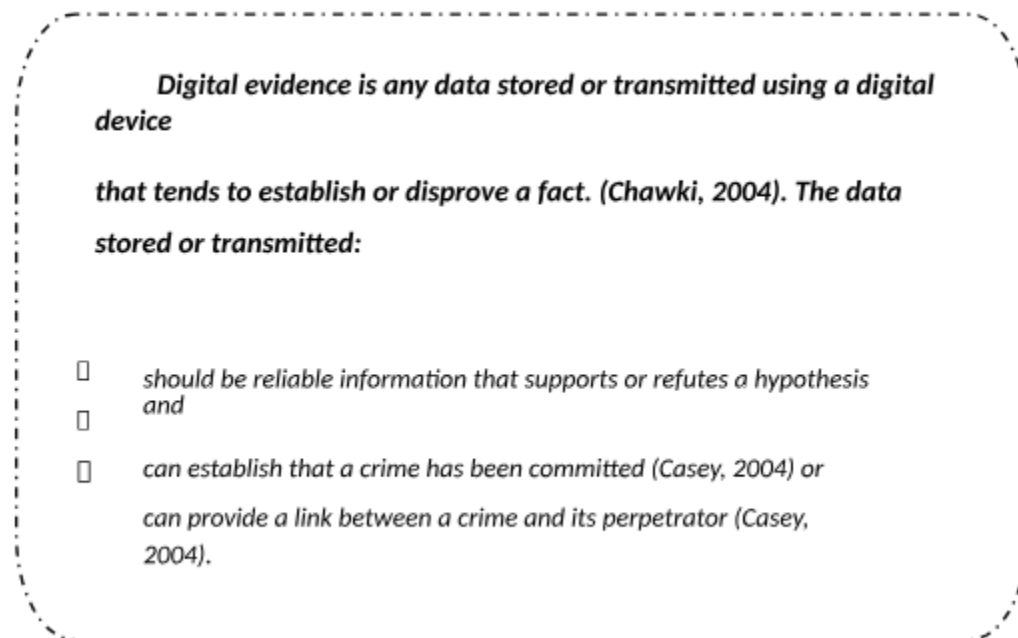
In the context of this thesis, evidence is categorized as either physical evidence or digital evidence, which includes data objects, legacy digital evidence, and live digital evidence.

According to Carrier and Spafford (2005), one of the many definitions given in the literature for Digital proof consists of information that contains credible data that either confirms or disproves a theory regarding the occurrence.

As defined by SWGDE and IOCE (2000), digital evidence includes binary-form information that has probative value, including not just traditional computers in addition to digital multimedia.

Virtual proof refers to data that can prove the commission of a crime or show a connection between the act and its culprit (Casey, 2004).

Drawing from our analysis of the research, we offer the subsequent explanation for proof:



To cover all the bases for trustworthy and worthwhile proof, we coin the acronym "CDE" (Corroborated Digital Evidence).

*Comprehensive digital evidence (CDE) is digital evidence that will have evidentiary weight in a court of law and that contains all the evidence necessary (relevant and sufficient) to establish a fact or disprove a claim (by author).*

Investigators rely on CDE to uncover the root causes of incidents, establish connections between the perpetrator and the occurrence, and ultimately lead to effective probes and charges.

Recovery of information teams, governmental and armed forces, justice agencies, and commercial enterprises are finding more and more uses for DF techniques and technologies. Each of these organizations uses digital forensics for different reasons. In this setting, evidence is increasingly becoming a key factor in company success.

To conduct an inquiry or get relevant evidence, DF analysts usually create an investigative framework in accordance with accepted best practices. The use of approved DF tools and methods is frequently necessary for a search to be successful. To guarantee the correctness of the outcomes produced by applying these tools, it might be required to use a variety of tools. We shall explore the idea of our Corroborated Digital Forensics capabilities in more detail in the next part.

Most current models in the domain of digital forensics concentrate on three primary aspects:

1. Component 1: DF Readiness Preparation: This component is all about getting your organization ready for digital forensics. Whenever something occurs, you've got to take steps to be sure that digital proof is accessible and that solid forensic procedures are followed.

2. Part 2: Collecting Real-Time Evidence: This part deals with actions like taking eyewitness statements and real-time data from sources like CCTV cameras as an incident is happening.

Thirdly, there is reactive forensic investigation, which is what happens after an incident has already happened and makes use of evidence gathered through proactive and live means .

## **Main Points from Case Study**

Activities like gathering eyewitness statements and real-time data, frequently employing CCTV footage, are part of live evidence gathering. We are classifying this as active.

Examining and analyzing the occurrence using proactive and live sources of evidence is what the reactive investigation of the incident entails. This is considered to be reactive.

A full Digital Forensics (CDF) capability, consisting of three primary parts, is what we propose:

First, there's proactive DF, or ProDF. This part makes sure that businesses are ready for DF investigations, with solid forensic processes and digital data readily available, before an event happens.

Second, there's reactive DF, or ReDF, which looks at things after they've already happened.

Thirdly, Active DF (ActDF) focuses on collecting live or extra evidence while an incident is still underway.

Figure 2-3 illustrates our CDF capabilities graphically.



The following section will delve into the details of each component, providing an initial definition for better clarity.

The majority of DF architecture under investigation are flexible, meaning that their emphasis is on DF evaluation carried out following an incident. To gather proof, assess it, determine the incident's primary cause, and present the proof in court, the processes call for the use of certain investigation and study techniques. ReDF examinations are sometimes called "dead" or "post-mortem" forensics.

The descriptions supplied by the DF investigation class, (Reith et al, 2002), (Palmer, 2001), and (Rowlingson,2004) were used to build a new concept for ReDF:

*ReDF is an application of analytical and investigative tools and techniques for the preservation, identification, extraction, documentation, analysis and interpretation of digital media for evidentiary and/or root-cause analysis and the presentation of digital evidence derived from digital sources for the purpose of facilitation or furthering the reconstruction of incidents.*

An organization's readiness for investigations and digital forensics (DF) relies heavily on the Proactive Digital Forensics (ProDF) component. The main goal is to make sure that crucial evidence is found and made accessible in a way that can be accepted and used in court before anything happens. If you want to investigate suspicious transactions or make sure everyone is following the rules, you might need easy access to transaction and network logs.

- look into occurrences, fraud, or employee conduct
- Evaluate the efficacy and efficiency of the procedures or controls.



- Assess adherence
- Utilize DF tools to enhance IT Governance frameworks for non-investigative uses.
- Evaluate how secure the organization is.

ProDF goes further than typical DF preparation by empowering businesses to becoming DF-ready and use DF tools and technology for improving business and IT oversight frameworks in addition to using them for inquiries. This holistic approach acknowledges the broader potential of digital forensics tools.

***ProDF is the forensic preparation of an organisation to ensure successful, cost-effective investigations, with minimal disruption to business activities, and the use of DF to establish and manage governance programmes.***

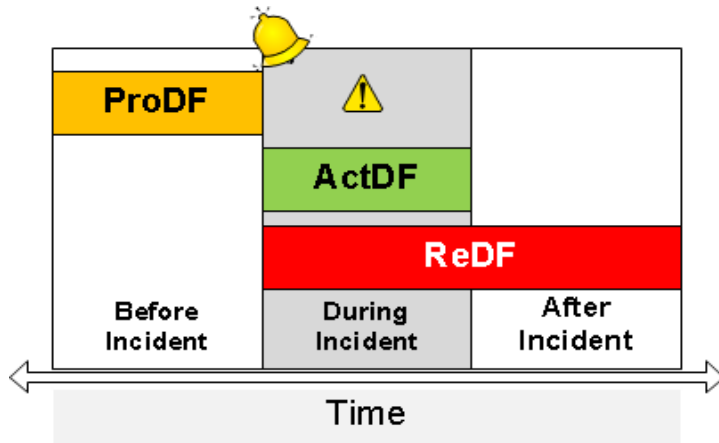
Even if it isn't feasible to anticipate every event, it is crucial to have the capacity to look at any issue, whether it be recent or continuing. The Incident Response Plan's (IRP) incident identification element is activated in certain circumstances. The Active Digital Forensics element is activated by the requirement to get real-time data and design a solid evidential basis. This, in turn, supports the ongoing Reactive Digital Forensic (ReDF) investigation.

***ActDF is the ability of an organisation to gather relevant digital evidence whilst minimising the effect of the incident during an on-going incident to facilitate a successful investigation.***

The three elements that make up our CDF capacity are interrelated and do not exist separately. The subsequent section explores the relationship between these components. Detailed discussion of ActDF will be presented in Chapter 6 of the thesis.

1. The primary focus of Proactive Digital Forensics (ProDF) is on pre-incident activities such as employee education, process restructuring, evidence identification, and control assessment.
2. The collection of "live" digital proof during active incidents is handled by Active Digital Forensics (ActDF).
3. Post-incident investigations are handled by Reactive Digital Forensics (ReDF).

Live evidence collecting is an integral aspect of the ReDF evidence acquisition process, hence there is a relationship between ActDF and ReDF. The inquiry is continued by ReDF once ActDF gathers "live" digital evidence. Figure 2-4 shows this connection.



## CHAPTER 3: DF FRAMEWORKS LITERATURE REVIEW

Success or failure is heavily dependent on how they are handled. There are various solid frameworks that can help us better understand cybercrime scenarios involving machines and multimedia. Specifically, what I've read suggests that traditional frameworks focus mostly on "post-incident investigations" (ReDF), giving less consideration to "live investigations" (ActDF) and proactive organization readiness for digital forensics (ProDF).

Two main categories of frameworks have been found from the literature review:

1. Casey (2004), Forrester & Irwin (2007), Barayumureeba & Tushabe (2004), and Louwrens et al. (2006b) are also part of the process frameworks. As part of their usual "waterfall approach," process architecture normally include steps like planning, collecting data, analysing it, reassembling it, and finally, presenting the results. It's important to remember that there could be loops between these stages to collect further proof for the hypothesis under investigation. leong (2006) has also presented a comprehensive that specifies the duties of various parties and places an emphasis on the legal environment.
2. In contrast to process-oriented methods, the role-based framework proposed by leong (2006) places emphasis on the regulatory framework and the particular responsibilities that persons ought to bear throughout the inquiry.

To build a complete Computer Digital Forensics (CDF) capacity, this chapter provides a forum for discussing and evaluating different process frameworks with the purpose of determining a full set of phases and related activities. We shall contrast and compare these systems in order to determine the relevant stages and methods. This chapter also evaluates leong's role-based architecture and contrasts it with various other approaches in order to find any potential gaps and crucial elements that should be taken into account when building our CDF capabilities or when carrying out and upholding.

### Frameworks that focus on the process

What happens in the event of an incident differs from one type of organisation to another:

1. Quickly securing the crime scene and collecting any evidence that might be crucial to the investigation are the top priorities for law enforcement when responding to a crime.
2. Organisations that come under the umbrella of "military operations" and "critical infrastructure" undertake a strategy of quick risk assessment and removal to provide a prompt recovery and, if needed, offensive actions.
3. Companies: Companies prioritise incident containment to reduce financial losses, rapid system restoration, and root cause investigation to identify the source of the issue.

The bulk of traditional Digital Forensics (DF) frameworks that are process-oriented adhere to a sequential, linear, or "waterfall" method. Most of the time, the input for the next phase is the output from the previous stage. Whenever further evidence is needed, investigators can evaluate and obtain it from

earlier phases using the iteration structures included in these frameworks. As shown in Figure 3-2, the standard procedure for a process framework consists of the following steps: incident detection, evidence collecting and identification, analysis of evidence, incident reconstruction, and presentation of results.

Utilising phases and stages from current frameworks to create new, superior composite frameworks is a prominent approach in the evolution of DF frameworks. For example, in his framework,

In what follows, we'll take a quick look at seven composite frameworks that have made important contributions to digital forensics:

1. Séamuas Ó Ciardhuáin's (2004) work.
2. Carrier and Spafford's (2003) work.
3. Baryamureeba and Tushabe, 2004.
4. Beebe and Clark's (2005) work.
5. Louwrens et al. (2006b).
6. Casey, 1994.
7. Forrester and Irwin (2007).

The suggested system consists of three parts: ActDF emphasizes instantaneous fashion evidence collection and analysis; ReDF focuses on typical DF inquiries conducted after an event; and ProDF educates organizations to utilize DF technology and methods to ensure evidence access and appropriate DF practices.

As we go through each framework, we'll utilise tags to denote the steps that are intrinsically related to each component. In particular, we will employ the following tags: (REACTIVE) for ReDF, (PROACTIVE) for ProDF, and (ACTIVE) for ActDF.

### **First framework is Ó Ciardhuáin (2004).**

The information flow that occurs throughout an investigation is the primary emphasis of the framework. In order to provide his own framework, Ó Ciardhuáin compares and contrasts the ones put out by (Lee, 2001) and (Reith et al., 2002). Much of this architecture is concerned with the research itself rather than the flow of information through it. Following an incident, the following 13 procedures were recommended by the framework:

- 1) The initial action is to increase attention of the necessity for an inquiry. (in response)
- 2) Authorization – Acquire permission to carry out the inquiry from both internal and external sources. (in response)
- 3) In this step, you'll want to identify both internal and external needs, such as legal or regulatory mandates. (in response)
- 4) Notification — Inform those who need to know that an inquiry is underway. If there's a chance that evidence may be destroyed, this action might not be the best choice. (in response)
- 5) Find and identify the evidence's source (both internally and externally). (in response)

- 6) Gathering Evidence - Gathering and preserving evidence is a methodical and lawful procedure. (in response)
- 7) The seventh step is to convey the evidence, but you must be careful that it stays intact during the journey. (in response)
- 8) Evidence Storage – Keep the evidence safe. (in response)
- 9) Evidence Examination—Analyze the evidence using appropriate methods and instruments. (in response)
- 10) Construct a Working Hypothesis Based on the Data Collected, Investigators Construct a Working Hypothesis. (in response)
- 11) Presenting the theory to the relevant local and/or outside parties is the next stage. This will determine the necessary actions. (in response)
- 12) The investigator must provide evidence to support the hypothesis in Step 12. (in response)
- 13) Sharing Information — Share the investigation's findings with those who need to know. (in response)

### **Second Framework: Carrier and Spafford (2003)**

Without a doubt, described below are the most important definitions offered by Carrier and Spafford:

1. Any material artefact that may be used to prove the existence of a criminal act is considered physical evidence. A connection between the crime, the victim, or the offender may also be established using it. Forensic investigations often rely on tangible evidence, such as hard drives, personal digital assistants (PDAs), flash drives, or mobile phones.

2. Data stored digitally that can prove a crime was committed or link a crime to a specific individual is known as digital evidence. Information linked to a suspect or the crime may be kept in many digital formats, including memory, a hard drive, or even a cell phone.

3. As a term, "physical crime scene" describes the actual location where tangible artefacts related to an incident or crime may be found. A primary crime scene is the original site of an incident or crime, whereas any additional sites connected to the same occurrence are called secondary crime scenes. The parameters and extent of the main scene are dictated by elements of nature.

4. A digital crime scene is an artificially generated setting that makes use of both software and hardware components. Digital evidence pertaining to a crime can be found in this digital world. Digital crime scenes, similar to physical ones, are classified as main when the first criminal act took place there and secondary when other places connected to the same occurrence follow.

All subsequent scenes, whether in real life or online, are considered secondary to the primary scene, which is the starting place of the crime or event. Forensic investigators can use these definitions as a guide to better comprehend the different types of proof and the contexts in which they are discovered.

### **Baryamureeba and Tushabe (2004) constitute the third framework.**

Several sources, such as Reith et al. (2002), Carrier and Spafford (2003), and the National Institute of Justice's Digital Crime Scene Analysis - A The creators of this framework, that they describe as the Improved Digital Investigative process frameworks, used an initial responders' handbook as inspiration.

One must make a clear distinction between virtual crime scene studies and actual crime scene investigations:

The real place where concrete proof of an offence or its commission could be discovered is referred to as the site of the crime.

A digital crime scene is a computer-generated model of an online crime or incident that includes physical and digital artefacts.

Virtual and actual investigation of crime scenes are distinguished by Baryamureeba and Tushabe (2004). There are five steps to the structure that Baryamureeba has suggested:

- 1) Get Ready (two-part process) (The whole thing is proactive) First, make sure your operations are ready for any kind of incident by making sure your human capacity is prepared. Prepare the infrastructure to handle future catastrophes. Make sure it's enough and suitable.
- 2) Physically investigate the scene of the crime and look for digital proof. Investigating a crime scene physically entails five distinct phases.
  - i) In order for competent individuals to find and collect evidence in the future, preservation means keeping the physical site undisturbed. Another need is the identification, removal, and isolation of observes who were present at the site of the offence.
  - ii) As they stumble around the incident scene looking for possible concrete and indirect proof, the individual who is doing the investigation establishes the limits of the investigation, formulates their initial hypothesis, and records a narrative.
  - iii) To preserve the specifics of the crime site, documentation comprises collecting as much data as possible, including videos and photos.
  - iv) Examining the site thoroughly to find further evidence and start the internet inquiry is what "examine and gather" is all about.
  - v) The presentation process comprises sending the internet investigation team all the digital evidence that has been found.
- 3) Do a digital crime scene investigation by looking at the area electronically and collecting digital evidence, taking into account the potential damage's magnitude. An inquiry into a virtual crime site consists of four stages:
  - i) Maintaining the integrity of a virtual crime scene allows for the synchronization of proof. Duplicating the forensic evidence is necessary.
  - ii) Look for possible proof in the scanned dataset.

- iii) A thorough examination of digital information employing software tools, combining data, connection, plotting, visualization, and time-lining results in the development of exploratory theories.
  - iv) From the moment as digital proof is discovered, it has to be recorded.
- 4) After confirming the occurrence and obtaining authorization from the appropriate regulatory and legal bodies, the fourth step is confirmation.
  - 5) Provide all necessary documentation, including digital and physical files, to the appropriate authorities or company executives.

#### **Fourth Framework Beebe and Clark (2005)**

For virtual investigations, this architecture provide a model based on hierarchy of goals. Palmer (2001), DOJ (Nolan et al., 2001), Reith et al. (2002), Carrier and Spafford (2003) were the structures that we employed. There are six distinct levels to this hierarchical system, and each level has its own goals and guiding principles. Each of the process's phases and sub-phases is an independent, unique step that must be completed in the correct sequence. Listed below are the six first-tier phases that the framework considers:

- 1) Get Ready (The Whole Thing Is Preventative) For the best results in preventing, identifying, researching, and prosecuting security incidents, keep the following steps in mind while working with digital evidence:
  - i) Determine the level of danger by thinking about potential weak spots, dangers, losses, and exposures.
  - ii) Think of a way to remember things before and after the event
  - iii) Create or improve an IRP (containing guidelines, processes, personnel assignments, and technological specifications)
  - iv) Acquire more technical skills
  - v) Provide employees with education
  - vi) Get the network and host devices ready.
  - vii) Create protocols for the safekeeping and processing of evidence.
  - viii) Record the outcomes of tasks
  - ix) Create a strategy for coordinating legal activities.
- 2) Responding to Incidents (The Entire Stage is Reactive)
  - i) Identify any questionable behaviour
  - ii) Notify the proper authorities of the suspected activities.
  - iii) Verify as an occurrence
  - iv) Evaluate the organizational harm or effect
  - v) Take into account the objectives and considerations of business, law, technology, and politics as you formulate a plan for containment, eradication, recovery, and inquiry.
  - vi) Coordinate the use of all available resources, including those of management, staff, and the law.

- vii) Create a rough outline of how you want to gather and analyse data for your investigation.
- 3) Collecting Data
    - i) Prepare a reaction strategy and an investigation plan by gathering evidence (REACTIVE) (ACTIVE)
    - ii) Finalize the active data collecting process for the "live response"
    - iii) Collect proof from a network (ONLY IF YOU WISH TO).
    - iv) Collect proof from hosts (REACTIVE)
    - v) Collect DETACHABLE (REACTIVE) MEDIA
    - vi) Make sure to incorporate a proactive monitoring capability.
    - vii) Verify if the evidence is genuine and of high quality (REACTIVE) (ACTIVE)
    - viii) Ensure the safe transportation and storage of digital evidence. (responsive) (dynamic)
  - 4) Data analysis, and it is a completely reactive process. Confirmation of suspicion and/or reconstruction of the occurrence are the goals.
    - i) Minimize the size of massive data sets
    - ii) Perform preliminary data survey to ascertain suspicious proficiency
    - iii) Make use of data extraction methods
    - iv) Think back on what happened and figure out what happened.
  - 5) Display of Findings, Share results with other departments, such as expert workers, legal advisers, and higher management. (in response)
  - 6) The sixth step is incident closure; this phase is entirely reactive.
    - i) A critical assessment of every step is required in order to identify and put into practice the lessons learned.
    - ii) Take choice and put it into action
    - iii) If it is allowed by law, dispose of the evidence.
    - iv) Gather and save all data pertaining to the occurrence.

### **Louwrens et al. (2006b)**

In proposing control goals as a foundation for users to apply an organised approach for incident analysis, the framework gives an example structure that is similar to the CobiT structure (2000). There are four stages to the DF process outlined by this paradigm, and each stage includes both high-level and more specific DF control objectives.

This framework offers a comprehensive, high-level conceptual structure comprising control objectives with sub-objectives. These objectives serve as guidance for the implementation of digital forensics (DF) within an organization. Although the framework acknowledges the existence of an actual scene of a crime, its primary focus is on the virtual investigative process. Furthermore, Proactive Digital Forensics (ProDF), which will be further described in Chapter 6 as a component of our Cyber Defence Framework (CDF) capabilities specification, is included in the architecture.



## **FRAMEWORK 6: E Casey (2004)**

Casey's structure fosters a thorough, rigorous inquiry, assures correct evidence processing, and reduces potential errors. The framework suggests the twelve phases below:

### 1) Incident Alert or Allegation Assessment (Reactively)

- Start with the initial incident alert or allegation to determine if it constitutes a potential crime or policy violation.

### 2) Worth Assessment and Decision-Making

- Evaluate the significance and potential worth of the incident.
- Prioritize the incident to decide whether further action is warranted, leading to one of two outcomes: concluding without further action or proceeding with a full investigation.

### 3) Incident and Crime Scene Protocols

- Implement appropriate protocols and actions, encompassing both real-world and virtual responses to the incident.

### 4) Evidence Recognition and Securement

- Identify and secure the evidentiary elements, ensuring proper packaging and preservation.

### 5) Evidence Preservation and Data Integrity Assurance

- Safeguard the integrity of evidence, preventing any potential modifications, through both reactive and proactive measures.

### 6) Comprehensive Evidence Restoration

- Collect all relevant evidence, whether information that has been concealed, erased, or was previously unavailable, using either proactive or reactive strategies.

### 7) Data Harvesting and Metadata Compilation

- Get all the information and metadata that are applicable to the occurrence.

### 8) Evidence Reduction and Relevance Analysis

- Examine the proof and remove any unnecessary components that don't relate to the matter at hand.

### 9) Data Organization and Search

- Gather the pertinent data to provide a focused examination of the occurrence and expedite the investigation process.

### 10) In-Depth Analysis

- Analyze the proof carefully to get insightful information. ● Consider the setting and nature of the evidence. The proof needs to be readable by people.
- Use the proof to ascertain the chance, the purpose, and methods.
- (REACTIVE) Evaluate the proof and try out other tools and tactics. (REACTIVE) Often, proof by itself won't provide a clue to the incident; thus, it's important to combine data from other sources to provide promising leads.
- Determining the order of time of occurrences and demonstrating the connections between data from diverse sources are crucial. (REACTIVE) Verify the analysis's conclusion to ensure that it is acceptable and acceptable in trial. (AUTHENTIC)

#### 11) Transparent Reporting of Findings

- Give a thorough overview of the investigation procedure, covering the procedures followed to gather, record, safeguard, retrieve, reassemble, arrange, and look for crucial proof.

#### 12) Convincing and testimonies

- Translate the investigative results into a comprehensible narrative for discussions with decision-makers, enhancing their understanding of the findings.

As indicated in Figure 3-3 (below), we utilized the DF architecture comparability to identify shared characteristics, rearranged phases or stages that were similar, and added steps or stages that were lacking:



## **WORK IN PROGRESS FOR OUR CDF ABILITY**

There are three possible aspects to our CDF capabilities.

### **ProDF component**

1. Ensure that DF is prepared to construct the structures. Preparing the operational infrastructure is a requirement stated by Beebe and Clark (2005), Forrester and Irwin (2007), and Louwrens et al. (2006b). Prerequisites for conducting internal investigations within an organization include the establishment of an investigative infrastructure. Infrastructure configuration to prevent anonymised and anti-forensic operations is advised by Louwrens et al. (2006b).
2. According to Beebe and Clark (2005) and Louwrens et al. (2006b), evaluate risks in all possible business situations.
3. In an effort to facilitate the early identification of relevant information, it is important to evaluate all corporate situations with the goal to detect potential dangers.
4. Create a strategy for keeping relevant data (Beebe & Clark, 2005)
5. A well-thought-out plan will guarantee systematic evidence collection while also attending to the needs of the law, the courts, regulations, and technology.
6. DF policy and procedure development.
7. Beebe and Clark (2005), Casey (2004), IR (Beebe and Clark, 2005), anti-forensic activity avoidance (Louwrens et al., 2006b), anonymous activity prevention (Louwrens et al., 2006b), and proof handling are common procedures and guidelines to develop.
8. Prepare Incident Response Plans (IRPs) for occurrences They are included in the backup plans of organizations. To avoid destroying evidence, it is imperative to design the reply with the DF criteria in mind. Beebe and Clark (2005); Louwrens et al., 2006b). As per (Louwrens et al., 2006b), the IRP ought to designate certain personnel for the purpose of constructing a CERT. An IDS (intrusion detection system) and improved or new procedures for addressing events or crime scenes are also advised, according to Louwrens et al. (2006b). Important actions to take following incident review include putting the incident control plan into practice and deciding whether to expedite the inquiry.
9. Create DF awareness and training programmes.
10. Element Record and verify a DF procedure in comparison to industry standards (Louwrens et al., 2006b).

### **ActDF Component**

1. Obtaining pertinent firsthand testimonies is the initial stage (Beebe & Clark, 2005; Carrier & Spafford, 2003; Casey, 2004; Forrester & Irwin, 2007; Louwrens et al., 2006b). It is essential to follow a known procedure and take the fluctuating series into account while gathering live proof.
2. Verify for honesty (Louwrens et al., 2006b)
3. Making a legal duplicate of the proof that that the inspector gathers and making sure it is preserved throughout the investigation are among their ethical obligations. Verify that knowledgeable individuals are employing trustworthy resources (Forrester & Irwin, 2007; Louwrens et al., 2006b). According to Beebe and Clark (2005) and Louwrens et al. (2006b), in order to protect the authenticity of proof, investigative duplicates must be checked,

signed, and maintained.

4. Phase 3, as outlined by CP Louwrens et al., 2006a, involves documenting the live acquisition process.
5. To preserve the line of control of proof, paperwork is necessary throughout the whole live proof gathering procedure.
6. In the fourth phase, known as "analyse the live data," investigators look at the data to see if they have enough evidence to start a serious investigation or find out what caused the event (CP Louwrens et al., 2006a).

## **ReDF Component**

### Ten-Step Incident Response and Confirmation Process

1. Begin by contacting Info Sec or the company's backup plan to initiate the Incident Response Plan.
2. CP Louwrens et al., 2006a states that step three is to report the occurrence.
3. As per Beebe & Clark (2005), Carrier & Spafford (2003), Casey (2004), choose an evaluation metric for the incident. An incident investigator's job is to determine whether an event has occurred and, if so, what kind of damage it might have done to the company. Verifying the event or labelling it as a "no incident" is the following step. The importance and breadth of the research must be defined. The level of formality or informality of the investigation will be determined by this.
4. Step 5: Acquire the necessary internal and external authorization.
5. Refer to Beebe and Clark (2005) and Carrier and Spafford (2003) for information on how to activate the incident containment approach
6. Make sure everything is in sync (Beebe & Clark, 2005; Louwrens et al., 2006b).
7. The inquiry should be expedited if needed, in accordance with the conditions specified by the policy (Louwrens et al., 2006b).
8. Lastly, as stated by Forrester and Irwin (2007) and O'Ciardhuain (2004), inform the appropriate persons that an inquiry is underway.

## **Crime Scene Forensic**

1. Conduct a physical examination
2. The first step is to physically secure the situation.
3. Locate any possible evidence at the location of the crime.
4. Then gather tangible proof. Photographing, bagging, labelling, and recording the individual evidential artefacts are all legitimate methods that the investigator should do when inspecting the crime scene and gathering possible evidence. According to several sources, it is crucial for the investigator to distinguish between different types of evidence, including digital data or fingerprints, in order to send them to the correct forensic lab for analysis.
5. Piece together what happened (Barayumureeba & Tushabe, 2004).
6. Get the evidence to an appropriate investigative lab to make sure everything is in order.
7. Put the proof somewhere safe. Consider a safe custody area, access controls, and the order of possession requirements when assessing storage needs.

# Conducting Virtual Investigations

## Safeguarding the virtual proof

1. First, as stated by O'Ciardhuain (2004), record the crime scene digitally.
2. Next, you need to check if the proof is reliable. (Louwrens et al., 2006b) state that examiners should be protect all media and follow the conventional DFI protocol.
3. Make a legal duplicate of any potential proof and store it securely.

## Gather Proof (Five Steps)

1. Collect the evidence that is needed. Proof that is fixed, living, concealed, or damaged must be gathered or recovered in order to do this. Gather all information and data related to the incident.
2. Use verification tools to confirm that the proof is genuine. According to Carrer and Spafford (2003) and Louwrens et al. (2006b), investigators should date every evidence in order to make time lining easier.
3. Get the evidence to the right lab to make sure it stays in the right hands (Carrier & Spafford, 2003; O'Ciardhuain, 2004).
4. O'Ciardhuain (2004) state that the evidence should be stored securely.
5. Carrier and Spafford (2003) and Louwrens et al. (2006)b state that compile the records of the acquisition operation.

## Analyse the evidence

1. Reassessment of the Initial Investigation Plan. Begin by revisiting the original investigation strategy, taking into account available data, resource allocation, and the team's expertise. Ensure that the evidence is readily understandable, drawing insights from the researched works.
2. Hypothesis Formulation and Validation Criteria. Construct a hypothesis and delineate the criteria necessary for its validation, following the guidance of Louwrens et al. and O'Ciardhuain.
3. Evidence Preprocessing. Prepare the evidence for in-depth analysis, potentially reducing large datasets to a manageable scale, considering recommendations from Beebe & Clark, Casey, and Louwrens et al.
4. Comprehensive Evidence Analysis: Conduct a thorough analysis of the available evidence, ensuring the identification of the most compelling data, as advocated by Casey, Louwrens et al., and O'Ciardhuain. Employ reduction techniques to eliminate irrelevant information in alignment with the principles of Carrier & Spafford and Casey. Evaluate the results to ascertain the means, motivation, opportunity, and the suspect's skill level. Employ multiple digital forensics (DF) tools for a holistic analysis.
5. Incident Reconstruction: Reconstruct the incident, drawing insights from the works of Barayumureeba & Tushabe, Beebe & Clark, Carrier & Spafford, and Casey.
6. Hypothesis Testing via Fusion and Correlation: Evaluate the hypothesis through the application of fusion and correlation techniques, validating it against the predefined criteria. This step aligns with recommendations from Beebe & Clark, Casey, and Louwrens et al.
7. Analysis Results Validation: Confirm the accuracy and reliability of the analysis results, as suggested by Louwrens et al.

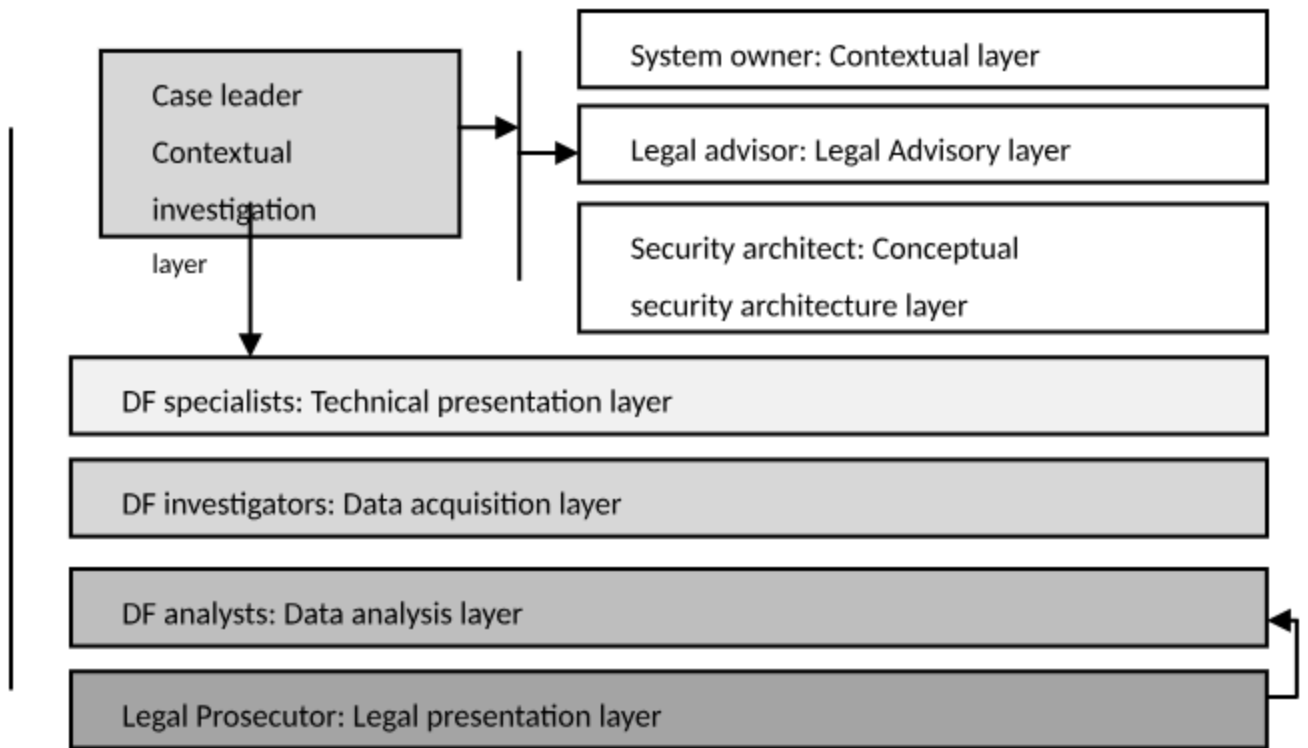
8. Thorough Recording of Results: Compile the research results in a thorough record, following the recommendations given by Casey and Louwrens et al.
9. Document Security: Safeguard the documented materials as recommended by Louwrens et al., ensuring their protection and integrity.
10. Recover the functionality as soon as possible with minimal the company's effect. Work with the company's (Info Sec) BCP groups to achieve this (Forrester & Irwin, 2007).

## **FORZA (FORensic framework based on ZAchman framework)**

A technological autonomous architecture designed to bridge the gap among technologists, legal professionals, and investigator. It was created utilizing the Zachman architecture in order to involve legal advisers and prosecutions in the larger picture. The Zachman company structure framework suggests the roles: the architect, organizer, creator, vendors, and customer. The FORZA architecture suggests the following responsibilities:

- Principal Coordinator: The individual orchestrating the complete process of virtual inquiry, responsible for steering the case and making the pivotal decision on whether to proceed with the investigation.
- System Stakeholder: The proprietor of the system under scrutiny, who may assume the roles of victim, questionable individual, or case supporter.
- Judicial Counsel: The primary coordinator's go-to attorney when looking for guidance in law.
- Security and System Architecture Expert: Proficient individuals well-versed in controls and security architecture, offering insights to the principal coordinator regarding the investigation's scope.
- Digital Forensics (DF) Strategist: The specialist responsible for devising the overarching strategy for the entire DF investigation process, adapting it dynamically as needed.
- DF Investigator and Operational Administrator: The individuals actively carrying out the investigation tasks, including data collection, extraction, and the preservation and storage of evidence.
- DF Examiner: The professional tasked with analyzing the evidence to substantiate the established hypotheses.
- Prosecution Counsel: Legal professionals involved in representing the case in legal proceedings.

Please see Figure 3-4 below for a graphic depiction of the suggested process progressions throughout each of these positions.



# CHAPTER 4: PRO-ACTIVE DF

## Introduction

The major goal of Security of Information is to safeguard the organization against potential attacks. While security checks are typically placed to deter and prevent such attacks, they often lack a focus on the requirements for gathering admissible evidence and well-defined processes. Traditionally, Digital Forensics (DF) has been predominantly reactive, primarily centered on incident investigations. However, in the organizational context, DF is undergoing a transformation from a responsive mechanism to a proactive and powerful measure.

Organizations harness DF tools for several purposes, including:

1. Obtaining digital proof in a format that is legally admissible.
2. Examining a company's networks and infrastructure.
3. Policies and processes are being validated.
4. Providing assistance in recognizing and identification of important risks.
5. Providing investigators with access to the company's most important data.
6. Providing first-aid training to prevent proof tampering.

Notably, the (CSI 2010/2011) hacking and safety research found that 40% of the participants included forensic tools in their safety tech adapt (Richardson, 2012). According to Allen (2005), DF exams and tools are becoming more important in fields including intelligence collection, corporate security, and law enforcement.

The research on DF preparedness currently in publication focuses primarily on the following topics: evidence preservation and handling, primary reaction to incidents, DF inquiry structure, tool accessibility, and education demands. However, it frequently overlooks the ways in which DF needs may be actively included to enhance organizational governance frameworks, particularly IT governance frameworks. In order to evaluate and validate controls, processes, and policies, for example, these preventative steps can be used to gather digital evidence, as mentioned in paragraph 2.5.

## WHY PRODF?

In the age of learning, information and comprehension are highly prized resources. Hackers, rivals, and even staff members exploit gaps in the current security protocols, conceal their tracks using anti-forensic tactics, and use forensic equipment and materials to get the information needed to perpetrate crimes.

In this age of learning, knowledge and understanding are highly valued resources. Digital criminals, rivals, and even staff members exploit weaknesses in current safety infrastructure, hide their traces using anti-forensic tactics and resources, and gather proof with forensic instruments and methods.

Ensuring that firms are equipped to handle crises, catastrophes, and safety incidents requires a significant investment of resources, time, and cash. They plan how to handle incidents, recover



from disasters, and keep the company running smoothly. Information security (Info Sec) and emergency plans help businesses prepare for and respond to security breaches and attacks by outlining what to do in the case of an incident and how to get back up and running as soon as possible. Finding and preserving evidence, as well as properly organising systems for future prosecution, receive less attention. The absence of "good evidence" or inadequate procedures leads to investigative failure.

Several factors that encourage businesses to use DF are discussed in Chapter 2. As mentioned organisations are required to have CDE, or full digital evidence. Businesses use DF for the following purposes:

- Investigating occurrences, deceit, or employee behaviour

While most companies are aware of their governance responsibilities, very few have acknowledged the potential benefits of DF. Collecting evidence to evaluate the efficacy of controls may be done using the DF approaches and tools. In order to set up efficient governance due diligence, the instruments can offer written proof of the evaluation. Organisational planning for DF consumption and utilisation is, hence, crucial.

The frameworks examined and debated in Chapter 3 brought attention to the necessity of becoming ready for inquiries or working toward becoming DF-ready. We will utilize the described aspects in combination with current perspectives on DF ready to ascertain whether the suggested ProDF aspect is identical.

### **ProDF requirements**

We have created a thorough inventory of eleven essential requirements by reviewing Chapter 2 and the Proactive Digital Forensics (ProDF) components described in Chapter 3.

1. Beebe and Clark (2005), Louwrens et al. (2006b), Nikkel (2006), and Rowlingson (2004) all agree that the first step is to find, gather, and manage any evidence that may exist while keeping business disturbance to a minimum.
2. Reduce the administrative and monetary costs associated with queries (Louwrens et al., 2006b).
3. Develop instructional and training initiatives.
4. To show if you're dedicated to good corporate governance, use Digital Forensics (DF) tools, methods, and procedures to prove that you did your homework
5. Make sure everything is in order legally and in terms of optimal compliance.
6. Organizations should view the efficacy of policies to improve their IT administration and data security oversight systems, according to Louwrens and von Solms (2005).
7. The rules, processes, and backup plans should incorporate the necessary evidence and protocols for DF.
8. Louwrens et al. (2006b) suggests including criteria for starting pre-set events to capture evidence in real-time.
9. Use DF instruments according to a specified protocol or method to guarantee the validity of evidence and the effectiveness of investigations (Louwrens et al., 2006b).
10. Verify that DF equipment and technologies can be supported by the operational and analytical infrastructure.

11. Develop procedures and technologies that make DF investigations easier so forensic operations may be carried out. Developing software tools and forensically sound ways to assist future DF investigations is part of this.

This is by no means an all-inclusive list, but we will utilize these eleven requirements to determine if ProDF provides a more thorough strategy than conventional DF preparedness. The following are some of the literature-based definitions of proactive forensics:

The necessary processes, methods, and technology are ensured by the active mode of DF so that action may be taken when necessary (Louwrens, von Solms, & Kannelis, 2006a).

According to Bradford et al. (2007), modern definitions and viewpoints on ProDF include DF preparedness and system structure to enable DF investigations.

The following DF definitions were deemed to be ready for use in the literature:

Rowlingson (2004) defined DF preparedness as an organization's capacity to maximize digital proof and minimizing the expenses associated with conducting an inquiry.

Garcia defines a state of preparedness for defence forces as the "art of enhancing the environment's capacity to gather credible evidence" (Garcia, 2005).

Drawing on Rowlingson (2004), we suggest the DF Capability criteria that follows:

## **Objectives for DF Readiness**

The models provided in Chapter 3 establish goals for DF preparedness. The authors (Barayumureeba & Tushabe, Beebe & Clark, Carrier & Spafford, Louwrens) have established a number of objectives throughout their preparatory or preparation phases. Three objectives were recently set forward:

1. Ensure that every aspect of processes and architecture is ready to receive an inquiry.
2. During preparation, it is important to think about how to make the most digital proof available to help in security incident identification, prosecution, examination, and deterrence (Beebe & Clark, 2005)..
3. The organizing and preparing phase offers guidance on DF preparation and readiness by mentioning keeping records, response organization, DF training, low-cost inquiries, and accelerating an investigation (Louwrens et al., 2006b).

### **Garcia's (2005) DF Readiness Objectives**

1. Developing skills for use in times of crisis is the primary objective
2. Form an emergency response team by creating suitable procedures and educational initiatives.
3. Prepare the systems and networks.
4. Contaminant planning as a fourth objective.

## **Rowlingson's DF Readiness Objectives (Rowlingson, 2004)**

Rowlingson suggests five objectives:

1. Collect acceptable proof legally and quickly, avoiding compromising with business operations.
2. The second objective is to gather proof of any wrongdoing or conflicts that could be detrimental to the organisation
3. Thirdly make it possible to undertake an investigation at a cost that is reasonable given the circumstances.
4. Make every investigation as painless as possible for the company.
5. Ensure that the proof influences every trial case's decision.

## **The four objectives we have for DF preparedness**

1. Increase the availability of CDE (Beebe & Clark, 2005; Louwrens et al., 2006b; Rowlingson, 2004).
2. Confirm that the activities and infrastructures are fully capable of supporting an inquiry.
3. Train personnel to be accountable and effective.
4. Make sure that the inquiry is affordable.

## **DF Preparedness Elements**

Compare same features of ProDF with steps by Garcia (2005) and Rowlingson (2004)

### **Garcia (2005)**

Garcia has recommended the four stages listed below:

#### Incident Response capability

1. Laboratory: Confirm there is a separated system, forensic servers, temporary and permanent servers, isolated systems, and disc servers.
2. Blank media, disc duplicators, and networking hardware are all available in a jump bag.
3. The availability of pertinent forensic instruments.

#### Incident response team preparedness

1. Define forensic clear processes, taking into account the scene of the crime protocols, chain of possession, and legalities.
2. Users should get training on forensic tools, that might include devices, programs, operating systems, commercial or free applications, and actual devices.
3. Make use of practical case studies in your instructional initiatives.

#### Hardware and communication channel preparedness

1. Make the most of your logging skills.
2. Use profiling and auditing on a regular basis.
3. Use forensic-friendly file systems to analyze forensic data.
4. Use proper file system separation procedures.

5. Turn on remote logging.

#### Confinement preparedness

1. Assess the network by employing appropriate network design methods and identifying choke spots.
2. Configure firewalls based on hosts
3. Employ a small investigating team.

#### **Rowlingson (2004)**

It proposed ten steps which are as follows:

1. Identify the business circumstances that will need the use of digital evidence.
2. Identify accessible sources and relevant evidence kinds.
3. Identify the criteria for evidence collecting.
4. Develop a capacity for gathering legally acceptable evidence in a secure manner.
5. Create a policy for safe evidence storage and management, as well as a secure evidence policy.
6. Verify that surveillance and audits are aimed at detecting and preventing big problems.
7. Describe the conditions under which a full official inquiry should be initiated.
8. Inform employees about their participation in the investigative procedure and the legal needs for proof.
9. Make a case supported by proof that explains the incident and its effects.
10. Seek counsel in order to move quickly because of the incident.

#### **Proposed DF readiness criteria**

##### Knowledge retention plan

1. Enhance the IRP (including policies, personnel assignments, and technical duties).
2. Define the conditions under which an event should be escalated to a full official inquiry and expand or construct incident handling procedures and regulations.
3. It is critical to design incident containment measures.
4. Create and establish an infrastructure for DF investigations.
5. Forensic computers, a fully-equipped DF investigation lab, and dedicated long- and short-term servers are all necessities.
6. Laboratory has to have blank media, disc duplicators, networking gear, and pertinent forensic instruments on hand. Gather and evaluate live, immutable, and legacy proof using the available tools and technologies.

##### Infrastructure preparedness

1. Making sure the operations and structure can support an investigation is DF preparation aim 1, which this feature helps with.
2. Create DF awareness, education, and training initiatives to produce good workers.
3. Staff education, training, and awareness programs, such as those for forensic tools or first responders, must be put into place.
4. This part helps with DF Readiness. Assemble a competent and responsible human resource

capability; this is the third objective.

5. Set up a system for DF administration.

### DF management capability establishment

1. A well-defined strategy for using DF and the assignment of specific responsibilities are prerequisites for managing an organization's DF deployment.
2. The Computer Emergency Response Team should be set up- The CERT and DFI teams should have their responsibilities and authority laid out clearly.
3. Determine the tasks and deadlines for external DFI experts
4. Establish a system of legal checks and balances to authorize responses to the occurrences.
5. By making sure that the framework and activities are sufficient to enable an inquiry, this part helps with DF readiness objectives 1 and 4.

## ProDF definition

*ProDF is the forensic preparation of an organisation to ensure successful, cost-effective investigations, with minimal disruption to business activities, and the use of DF to establish and manage governance programmes*

ProDF's objective is to administrate and execute DF in order to improve governance initiatives. Administration programs are implemented by companies to assist them in achieving their objectives. By ensuring CDE availability through the usage of our CDF capabilities, the company's control initiatives—such as IT and Info Sec—are strengthened. Executives will be able to demonstrate exceptional leadership oversight since documented assessments comparing the effectiveness of measures to business objectives will be available.

In general, management plans need to be created, carried out, kept up, and assessed. incremental. approaches will be employed for both management and evaluation. We'll talk about how incorporating DF might strengthen governance programs.

1. Sub-goal 1: Develop a competence for Digital Forensics management.

Companies should start by changing the way they operate to incorporate DF and assign roles and responsibilities for handling DF internally (Nikkel, 2006).

The positions and duties of data security, CERT, DF, and risk reduction teams should all be well defined. Inquiries are typically compromised when these responsibilities are ambiguous or divided.

It should be made clear when to use professional DFI assistance, and legal assistance must be available to assist with any action taken as a result of the incident.

2. Sub-goal 2: Use Digital Forensics to provide adequate confidence about organizational

objectives.

To provide appropriate confidence about organizational objectives, DF demands for proof and procedures ought to be incorporated into acknowledged risk control and management frameworks.

- Ensure the security of the organization's assets (including information). The honesty of all documents must be guaranteed by the group of directors (Hilley, 2006). According to Sarbanes-Oxley Section 802, changing documents is illegal. Since DF techniques have to adhere to legal evidence requirements, it will be simple to confirm that the content is genuine and hasn't been altered. To look at how equipment is being utilized, DF tools and methods can be employed to collect evidence. Additionally necessary is a whistleblower policy (Patzakis & Limongelli, 2004). The Info Sec team should include DF approaches into the IT audit methodologies to ensure that the proof collected can withstand judicial examination and to provide a more accurate audit route.
- Companies can benefit from DF readiness by anticipating content on their network that may be appropriate proof. Proof is a useful tool for proving conformity.
- Encourage the long-term viability of your firm in both advantageous and adverse operating environments. Critical risk zones may be analyzed using DF in normal operational conditions. The risk assessment should encompass the following risks: economic and monetary hazards, legal hazards, company stability and catastrophe recovery risks, technological risks, personnel risks, and both functional and structural risks.

Every company's system for overseeing information technology and data security will have its shortcomings. Companies conduct penetration tests using DF resources to find security holes (Richardson, 2008). To determine if existing DF tools are sufficient for incident investigation and the risks involved, organisations should evaluate all emerging technologies.

A company's technology implementation may be made more effective and efficient with the careful application of DF tools. DF technologies and procedures make it feasible to reclaim passwords, retrieve information from damaged storage devices, and erase data from storage devices before discarding them. Activities can be resumed and disruptions to company operations can be minimised after employing the tools.

The requirements of DF must be considered thoroughly while creating rules, processes, and controls for IT Governance. Based on our literature research, Table 4.4 (below) lists all of the controls that should consider DF requirements.

To ensure that there is as little interruption and effect on the company's activities as possible under challenging conditions, it is imperative to think about updating or improving contingency plans, standards, and methods, catastrophe recovery, and company continuity (some aspects were covered by Digital Forensics preparation sub-goal 1).

- Ensuring Report Accuracy

Ensuring Report Accuracy One way to help comply with the need is to use Digital Forensics tools, methods, and guidelines. This stipulation states that "The board bears

the responsibility of guaranteeing the yearly implementation of a methodical, documented evaluation of the procedures and results pertaining to significant threats." In order for the board to publicly address risk management, this evaluation is being carried out. In addition, the company must offer a thorough report that describes the occurrence, its consequences, and its evaluation in the case that it calls for an inquiry.

The trustworthiness of audit outcomes is greatly increased when DF methods are incorporated into auditing procedures. This makes it necessary for top executives to be updated on a frequent basis on the company's risk control processes and the status of current inquiries.

- Promoting Responsible Conduct Towards All Stakeholders (King, 2003)

Through these documented assessments, management can effectively demonstrate the performance of routine checks. Ensuring transparency and accountability to stakeholders is essential. This entails communicating the impact of incidents on the organization, elucidating the root causes of such incidents, and presenting the findings of investigations.

ProDF

ProDF goal 1: Become DF-ready				ProDF goal 2: Implement and manage DF to improve governance programmes	
Sub-goal 1:	Sub-goal 2:	Sub-goal 3:	Sub-goal 4:	Sub-goal 1:	Sub-goal 2:
Prepared infrastructure	Maximize CDE availability	Prepare responsible, competent employees	Ensure a cost-effective investigation	Establish a DF management capability	Apply DF to provide reasonable assurance regarding the achievement of organizational objectives

# CHAPTER 5 : REACTIVE DF

## INTRODUCTION

Forensic analysis wouldn't be required in a perfect world, but accidents happen, cyberattacks happen, and irate employees can erase data. Companies need to determine the incident's cause, the extent to which damage occurred, and how it happened.

The necessity for Comprehensive Digital Evidence (CDE) is indispensable when it comes to furnishing management with the essential answers. Nonetheless, it's critical to understand that DF functions inside a very specialized legal and regulatory environment. For proof to be considered admissible, there are strict guidelines and requirements that must be satisfied, and processes need to be carefully planned to follow the good practices of digital forensics (Louwrens et al., 2006a). A lot of DF inquiry models are quite specific and provide an organized way to accomplish tasks and follow procedures.

The Reflective Digital Forensics (ReDF) component has been subject to extensive research, and we have scrutinized several frameworks in Chapter 3. In this investigation, our goal was to use these frameworks to generate a detailed list of six stages, each of which had certain activities. Particularly, none among the architectures we looked at had every stage and action needed.

No company is ever fully equipped to handle every situation. The normal DF investigation (dead forensics) that takes place following an incident's reporting and confirmation is the main emphasis of ReDF, as we define it. Organizations, in particular emergency responders and DF researchers, must conduct the inquiry in accordance with a recognized and validated DF research protocol (Louwrens et al., 2006b). In section 2.8.1, we provided a tentative definition for ReDF as follows:

*An ReDF component is application of analytical and investigative techniques for the preservation, identification, extraction, documentation, analysis, and interpretation of digital media, for evidentiary and/or root cause analysis and the presentation of comprehensive digital evidence derived from digital sources for the purpose of facilitation or furthering the reconstruction of incidents (Kruse & Heiser, 2004; Palmer, 2001; Reith et al., 2002; Rowlingson, 2004).*

The objectives of ReDF inquiries were not stated clearly in the DF architectures discussed in Chapter 3. The next section will list ReDF's goals.

### REDF GOALS

The ReDF component becomes active upon event detection. Rowlingson (2004) and Kruse and Heiser (2004) proposed two goals for ReDF (investigations) based on the DF frameworks and ideas listed above (Reith et al., 2002; Palmer, 2001):

The completion of an investigation is the primary objective



Obtaining the correct CDE, determining the event's root cause, connecting the perpetrator to the crime, and presenting a convincing case are all necessary steps towards achieving this goal.

Objective 2 of ReDF is to lessen the impact of an incident

These goals can be more easily attained with the use of the ReDF approach. Each step of the procedure has its own set of related tasks. What follows is a synopsis of the six steps and related activities that make up the procedure.

**REDF PROTOCOL**

**FIRST STAGE:** Responding to and Confirming Incidents consist of ten steps as follows:

1. As per Casey (2004) and Louwrens et al. (2006)b, data safety or business's contingency strategy should be reviewed before initiating the incident response plan (IRP).
2. Search for activities.
3. Notify the proper authorities of the occurrence.
4. Determine the monetary worth of the occurrence.
5. Acquire all required permissions, both internal and external.
6. Implement the strategy to reduce the impact of the occurrence.
7. Management of the resources
8. Develop an approach to inquiry (Beebe & Clark, 2005). Step 1.17.1.7: Assemble all sources.
9. In accordance with the policy's specifics, step nine of 1.17.1.9 is to expedite the investigation (Louwrens et al., 2006b).
10. According to Forrester and Irwin (2007) and O'Ciardhuain (2004), notify all parties participating in the investigation.

SECOND STAGE: Physical investigation consist of seven steps

1. Securing the crime site is the initial procedure.
2. Look for evidence of criminal activity on the location.
3. The third step is for the oversight to look for and collect whatever proof they can find.
4. Gather Physical Proof
5. Recreate the occurrence (Barayumureeba & Tushabe, 2004).
6. Keep the line of command intact as you move the evidence to the proper investigation laboratory.
7. Put the evidence somewhere secure

THIRD STAGE: Digital research phase consist of four sub steps

Digital evidence securing

1. Preserving Digital Proof (four steps) Spafford and Carrier (2003)
2. Protecting a virtual scene of the crime is the initial stage (O'Ciardhuain,

2004).

3. Create a replica of the evidence in order to keep it safe.
4. Secure the evidence chain and regulate flow by recording all actions.

### Collecting Evidence

1. Collect the required proof.
2. Use validation techniques to confirm the evidence is genuine.
3. According to Carrier and Spafford (2003) and O'Ciardhuain (2004), ensure that the proof is sent to the correct laboratory while keeping the chain of custody intact.
4. The fourth step is to protect the evidence.
5. Document the technique for gathering.

### Analysis of collected evidence

1. Review the Initial Investigation Strategy
2. Create an assumption and a set of standards by which to judge it.
3. Compile all of your evidence to check the need to minimize the size of large datasets without compromising their evidential value.
4. Examine the data that is accessible.
5. Reenact the occurrence.
6. Put the theory to the test using integration and statistical approaches, Apply the established criteria to the test of the hypothesis.
7. Confirm the evaluation's results.
8. Document your findings.
9. Verify the safety of the paperwork (Louwrens et al., 2006b)

### Restoring Service

Restore service as soon as possible and minimize the impact on business, engage with the organizational information security team.

## **FOURTH STAGE: Scenario Reconstruction**

Bring together the findings of the digital and physical investigations, and then determine if the combined data supports the idea (Carrier & Spafford, 2003).

## **FIFTH STAGE: Reporting Results**

Present results to higher-ups or government authorities (three stages): (Pasey et al., 2004; Forrester & Irwin, 2007; O'Ciardhuain, 2004; etc.)

1. Initiate the case preparation phase.
2. Describe the problem.
3. Ensure the proof is securely stored (Louwrens et al., 2006b).

## **SIXTH STAGE: Incident Closure**

There are two processes to communicating the outcome of investigation:

Beebe and Clark (2005) and Forrester and Irwin (2007) state that the first step is to analyze the data in order to uncover and utilize learned insights.

A visual depiction of the six ReDF phases may be found in Figure 5-2 (below).

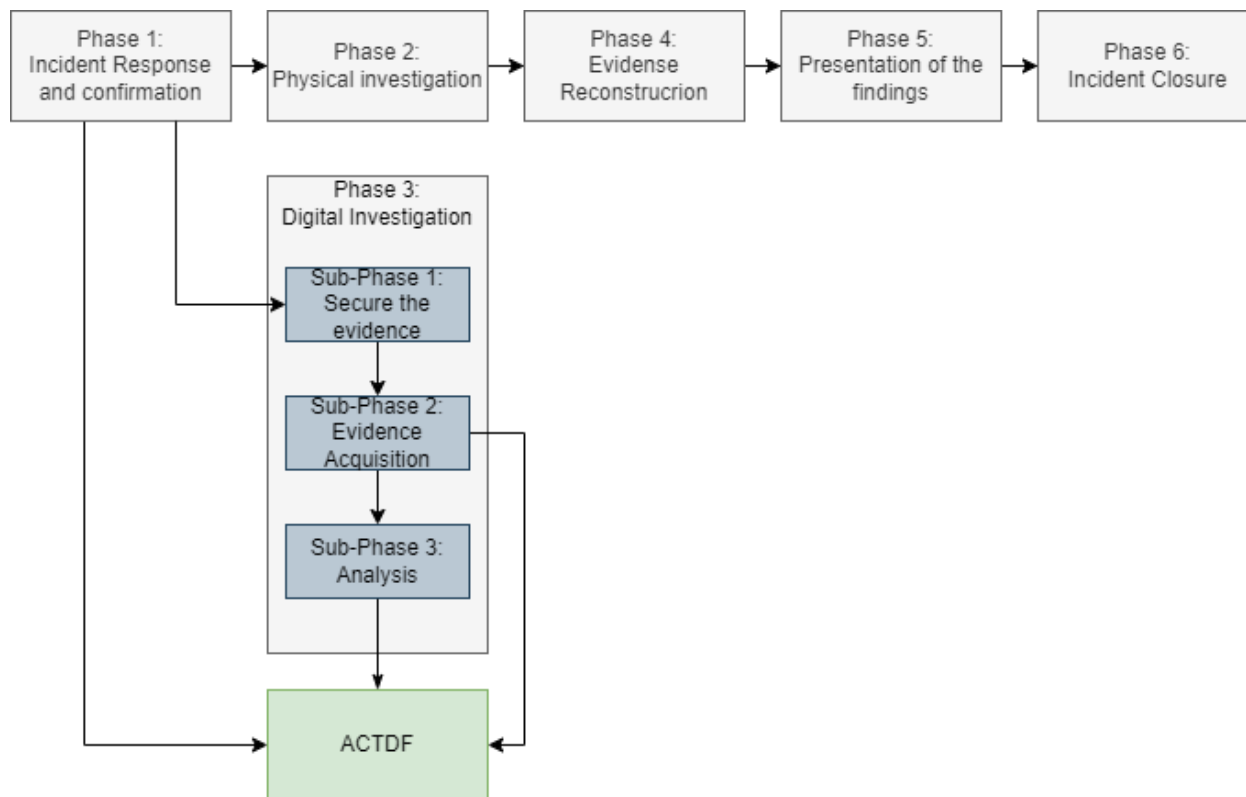


Figure An illustration for the six stages of ReDF

There are six separate phases in the ReDF protocols inside the ReDF part. The stages enable to be some revision in after they are organized using the waterfall approach. Two instances of how an inquiry could start are the physical entrance of an investigator in a crime scene and the creation of a preliminary hypothesis. Throughout this phase, proof will be collected and maybe digital proof will be located. The evidence obtained from the actual inquiry will be meticulously documented and examined in order to determine a motive, unearth the basic cause of the incident, and identify the offender. Processing different types of evidence may fall within the purview of specialized forensic investigation departments, such as digital forensics, ballistics, forensic pathology, fingerprints, and blood.

After then, it will be up to the DF investigation team to gather evidence, analyse it, piece together what happened, and find out what caused it. It may be required to merge digital data with physical evidence found at the crime scene in order to piece together what happened and find the culprit in some cases. If investigators can't find something to back up their theory, they'll have to start over with the identification, acquisition, and analysis phases of the process. After an exhaustive investigation, a thorough case file is developed and submitted to the appropriate

authorities, complete with supporting evidence. It is imperative that all case files and supporting evidence be retained once an investigation has ended.

To make sure the issue doesn't happen again, the results of the inquiry should be relayed to the company's risk management and Info Sec divisions. This allows for the possibility of developing and implementing additional controls.

An organization's conventional backup plans and the ReDF component should work in tandem without a hitch. When suspected conduct is noticed, the authorities are often notified by the Intrusion Detection System or a worker. The team responsible for responding to incidents will assess the issue as soon as it is identified to determine if it qualifies as an event. The ReDF element is turned on when an event is detected.

Incorporating DF process standards to guarantee DF-sound procedures and adhering to evidence identification and preservation guidelines are critical steps for the incident response team and first responders. Since both DF and Info Sec are engaged in reacting to an event, there is some overlap in the activities of incident response between the two. Our recommendation is that businesses supplement their current backup plans with relevant rules and procedures to make sure all methods are DF-sound and evidence is well-preserved.

It should be noted, nevertheless, that organisations may not always be quick to include DF needs into their incident response, disaster recovery, and business continuity strategies. One possible explanation for this reluctance is that organisations would rather get back to business as usual after dealing with security breaches or events, rather than spend time waiting for evidence to be located. According to the CSI computer study from 2010/2011, a quarter of respondents tried to find the criminal using their own means, while nearly six in ten wanted to fix security holes as soon as feasible (Richardson, 2012). As a result, businesses understand they need to find a middle ground between solving security breaches quickly and identifying the culprit.

For the ReDF component to work, there has to be an established protocol for DF investigations, clear rules and processes, well-trained staff, suitable technology and tools, and an investigative and operational infrastructure. The ProDF element ought to provide these requirements.

If such proof is needed for an evaluation, the ReDF element does not get any live or unstable proof. Alternatively, the ActDF feature is turned on. In the past, we have put forward a separate element for gathering real-time proof. Protocols, methods, and technology used in the ReDF component do not apply to live DF investigations. The ReDF component continues its investigation once the live evidence has been acquired.

## CHAPTER 6: ACTIVE DF

In Chapter 3, we looked at traditional DF frameworks and found that there was a requirement to collect and manage "live evidence." In order to get to the bottom of an incident and bring those responsible to justice, many investigations depend on important and pertinent live evidence, such as swap files, network operations, and volatile data (such as RAM content). To illustrate the point, consider the "Code Red worm," which never wrote to the disc but instead lived in RAM, making a "live" investigation essential. Investigations into live systems are also required since many real-time systems cannot be turned down (Adelstein, 2006; Sremack, 2005).

In most cases, when an intrusion is detected, the organization's incident response (IR) protocol The intrusion detection system (IDS) initiates this process. In order to ensure that pertinent and acceptable live Complete digital proof can be obtained for analytical reasons, live forensic investigation techniques combined with the IR approach are becoming more and more crucial. Current IR approaches often overlook the recognition, collection, and storage of real-time data as proof (Sommer, 1999).

Live forensic investigations have many obstacles, as highlighted by Loeng and Leung (2007):

The term "live forensics" has not been defined.

1. There are no conventional protocols for carrying out live examinations.
2. Validation of live proof.

Although several frameworks and tools have been created to facilitate live investigations, there are still many obstacles to overcome in this emerging area. It is important to show that the tools are trustworthy and that the evidence they collect may be accepted in court. Another need is that these tools demonstrate they do not negatively affect system performance when used (Garfinkel, 2010). Live investigation software methods inherently include data modifications, in contrast to classic ReDF investigation frameworks that guarantee no revisions to evidence and seized information. But maintaining a hierarchy of ownership and protecting proof requires accurate forensic recording of the ongoing investigation.

### GOALS

The objective of this section is to use the stages described in Chapter 3 to construct the ActDF standard for the ActDF element within a CDF ability. This chapter provides a list of live and real-time investigative frameworks, methods, and tools, as well as some possible stages and procedures that might be part of an ActDF component. This method will be useful in gaining a thorough comprehension of our CDF capacity.

The FBI presented a strong argument for the addition of active forensic investigations as normal procedure in digital forensic (DF) operations during the 2006 Digital Forensic Research Workshop (leong & Leung, 2007). This advice was driven by several compelling elements:

1. **Non-disruptive Nature of Systems:** Some systems can't be powered down due to their inherent nature or the high costs associated with shutting them down, necessitating real-time investigations.

2. **Immediate Need for Live Evidence:** Certain incidents require investigators to swiftly obtain live evidence, such as volatile data, due to their dynamic nature.
3. **Crime-in-Progress Scenarios:** The ability to detect and investigate a crime as it occurs, without alerting the suspect, is crucial (Orebaugh, 2006).

Reliability of outcomes is the primary distinction among active and dead analytic tools, that are usually used in ReDF. Applications running live analytic tools have the ability to alter evidence. Rootkits, often called "Trojan horse backdoor tools," use preexisting OS software to hide the attacker's identity and are a typical source of misleading data.

In order to conceal files or processes from investigators, rootkits sometimes place a filter into the normal data flow of an application's processing. This allows hackers to carry out their actions unnoticed. One way to combat this is to use tools that do not depend on Trojan libraries or to use trustworthy, unmodifiable tools that are packaged on a CD. Removing typical system calls and writes is another step in developing live forensic apps.

It is not feasible to obtain all real-time information, particularly dumps of memory and networking logs, due to the massive volume of information. This is why, in most cases, only pertinent data needed as proof for an ongoing inquiry is actually acquired. So, the proof usually looks like a picture of the machine or protocol stack as it is right now.

Real-time investigational evidence may not always be reproducible or repeatable, and this is something to keep in mind. However, as more and more criteria are defined, live analysis tool evidence is being accepted by courts with more acclaim.

Dealing with actual time systems—that is, anything that depends on particular timeframes to finish tasks and gauge demand—is equally important (Sremack, 2005). For these systems to function as intended, the instructions must be executed quickly and predictably. Enterprise routers, power-grid monitoring systems, medical gadgets that maintain life, and emergency contact centres are just a few examples. In the past, these systems mostly functioned in silos, with dependability taking precedence above security and incident investigation.

A major risk, however, is appearing as industrial trends bring real-time systems closer together with other people and devices. Due to the gadgets' unique data storage systems, current investigative tactics aren't always the best fit for real-time investigations. System logs are frequently missing, and accessing and recovering data that is volatile is difficult. Because of this, real-time systems must be modified to actively include security measures and take possible evidence sources into account.

In addition to active investigation tools and procedures, organisations should have a framework in place to direct their usage and provide first responders and investigators with instructions on how to behave. Specific guidance on what to do in the event of a problem should be provided via the establishment of emergency response along with other pertinent organizational structures, rules, and regulations for information technology along with data security. Making the decision to go from a live investigation to a formal reactive inquiry is part of this process.

After this section, we will discuss the connections between attack detection systems, incident response, and live inquiries, and we will further examine the overlaps that exist between all three of them.

Both human inspection and automated methods can be used to detect incidents. Incidents can take numerous forms, from system failure to incorrect transactions. Network managers can typically discover issues such as sluggish network performance, whereas the help desk may notice unexpected events and label them as incidents. Firewalls, antivirus software, host and network-based detection systems for intrusions, and other measures assist in identifying potential events (Whitman & Mattord, 2009). The main goal of IDS are to locate events with a range of anticipated consequences:

1. **Timely Reaction:** This may need personal or automatic involvement to avert major damage.
2. **Identifying Precursors:** Determining if the recorded behavior is an early precursor to a serious occurrence.
3. **Identifying the perpetrator:** determining the identity of the attacker.
4. **Safety Enhancement:** Providing greater security to systems in order to prevent future occurrences.
5. Evidence collection is the process for collecting proof to support an inquiry.

There are various automatic detection systems for intrusions on the market, some of which use proactive techniques or tools in their operation. Proactive techniques and processes for detecting events as they happen have been studied, including:

1. Active monitoring systems are continually watchful and can be either human or automated.
2. Future Forensic Investigation: Systems may be developed and configured to aid future forensic investigations while assuring that they allow forensic analysis.
3. Digital fingerprinting is the process of labelling documents or material with distinctive digital fingerprints that may be used to identify illicit use.
4. To enhance investigations, process forensics combines detection of intrusions with checkpoint technologies such as snapshots of active applications or processes.

The IDS used has a direct impact on a company's live digital forensic (DF) research approach and technique. IDSs are widely classified as either abuse detection systems or detection of anomalies systems. Misuse detection use fingerprinting to establish whether an operation is part of an attack, whereas anomaly detection specifies typical behaviour and distinguishes activities as normal or invasive. The biggest difficulty in detecting anomalies is determining what constitutes "normal" behaviour.

Foster and Wilson (2004) suggest using progressive check-pointing to develop a normal profile to overcome this issue. Profiling is critical in detecting incidents inside an organization.

The response strategy decides when something happens and whether it needs more investigation. A number of factors need to be considered, such as the attacker's background and the warning's reliability, type, effect, and intensity. The expense of stopping systems might also influence the choice. whether deciding whether to launch a review, when to let an event go unnoticed, when to put an end to events, or when to conclude an inquiry, the company risk approach and inquiry plan are essential.

It's necessary to create a detailed detecting or investigation policy as it helps specify the anticipated course of operation. Organizations may have different investigative thresholds. Some may only conduct an investigation if there is a major potential loss, whether financial, intellectual property, or public image.

Although data collection by systems that detect intrusions might aid in identifying incidents, it is crucial to emphasize that protecting data integrity and gathering data are not the main responsibilities of these devices as valid, legal proof (Sommer, 1999). Machine records, audit records, application records, network management records, network activity captures, and manual entries are common evidence sources. However, these records may be deficient in depth, insufficient for certain time periods, and incapable of distinguishing between legitimate and unauthorized access or identifying criminals efficiently. To guarantee that the logs have not been tampered with prior to, throughout, or following the gathering period, they must be tamper-proof. Processing this original data to render it more readable might be difficult since it may jeopardize the evidence.

To make IDS a reliable source of evidence, Sommer (1999) suggests several key points:

1. IDS must provide accurate and timely data about the possibility of an event so that relevant measures may be taken.
2. Evidence Acquisition Should Be Separate: Evidence collection should be a separate but linked activity.
3. numerous separate Streams: A single stream of evidence may not be enough; numerous separate streams need support each other.
4. Synchronization: All evidence streams must be synced.
5. Logging using a trustworthy Tool: Information should be logged using a trustworthy tool.
6. admission principles: Logging evidence must follow the principles of evidence admission.
7. Evidence Collection Integrity: The integrity of evidence collected during logging should not be jeopardized.
8. Raw Log Availability: Raw records ought to always be accessible for examination.
9. It is essential to uphold the evidence's uniformity or path of custody from the point of genesis to the judge.
10. Concentrate on Evidence gathering and Conservation: Additional methods or products ought to concentrate largely on evidence gathering and maintenance.

This comprehensive approach helps ensure that IDS data can serve as reliable evidence in DF investigations.

According to Carrier (2006), "dead" analysis techniques constitute the backbone of Reactive Digital Forensic (ReDF) investigations. These procedures do not include executing any software already installed on the system. However, proactive approaches are focused on getting systems, processes, and procedures ready to collect Comprehensive Digital Evidence (CDE), rather than investigating methods themselves. Having the right systems, protocols, and equipment to gather evidence is an important part of being ready.

Programmes aimed at ensuring the safety of sensitive data rely on live analysis, which is commonly linked to IR and IDS. Antivirus software is a piece of software that uses live analysis.



Research on the use of hardware devices for evidence collecting is underway, however the majority of live investigative tools and procedures are software-based.

Casey and Stanley (2004) state that remote forensic preservation and acquisition solutions like ProDiscover® and EnCase® Enterprise edition are now used in real forensic investigations. During the inquiry, these tools make use of the system's current software by employing live analytic methodologies. With these technologies, you may keep tabs on a certain machine from afar, gathering information in a forensically sound way without the user knowing. Investigative duties such as keyword searches, file copying, and data extraction can be carried out in a real-time production setting. Moving ReDF examination processes into production settings is the main goal.

Furthermore, software methods for collecting real-time evidence were highlighted by Carrier and Grand (2004):

1. Devices for Physical Memory: It is possible for attackers to take advantage of the fact that certain operating systems, such as Unix®, grant access to physical memory.
2. Sun® systems use Sparc OpenBoot® firmware, which is a method for dumping physical memory to a storage device. But it destroys any evidence that may have been in the swap file region by overwriting its contents.
3. The Process Pseudo-File System. This UNIX® system feature enables the detection of suspicious processes and the acquisition of pertinent physical memory associated with those processes. Swap files and possible evidence can be overwritten.
4. Vulnerable Computer Environments: Software such as VMware® allows users to create an imitation of a hacked virtual system and then transfer its contents to a different computer in order to gather evidence.
5. Some servers have the ability to preserve memory contents to the hard disc before turning off, a function called hibernation. You might not always have easy access to this function.

These methods depend on the OS, and more specifically the OS kernel, and are software-based. Due to the possibility of operating system compromise or accidental memory alteration during evidence collecting, this raises concerns about the trustworthiness of the evidence.

Using a PCI interface and a pre-installed hardware expansion card, a capture method for storage using hardware. An external storage device can be written to by this card once it gathers volatile evidence. While a card is activated, immediate access to memory is used to move the data inside of physical storage to an external permanent memories device of storage, interrupting CPU performance. The operating system keeps running once the memory copy is complete. An investigation of this methodology has resulted in the filing of a patent.

Forensics of Network is a tool for discovering live network evidence sources, complementing software and hardware-based approaches. Finding potential sources such as 'whois' servers,

webpages, FTP, local Ethernet, databases or SOAP servlet return messages is crucial during live investigations, even if not all network activity can be recorded (Nikkel, 2005). Defamatory websites, port scan activity, illegal downloading, routing tables, transmitting signal intensity, and direction are a few instances of evidence that might be obtained.

Different live investigation strategies take volatility order into account, whereas distant online forensic investigations capture data independent of volatility order. The reasoning behind different techniques differs. When conducting a volatile forensic investigation, it is important to follow the sequence of volatility when gathering evidence. Therefore, the most unstable proof must be obtained first, followed by the less dynamic proof, using proven tried-and-true reactive Digital Forensic techniques and tools. Figure 6-2 shows McDougal's volatility model, which investigators may use to sort evidence into four categories: very volatile, medium volatile, low volatility, and not volatile (leong & Leung, 2007).

The following types of volatility were identified using this model and the research of leong and Leung (2007):

1. Extremely Fluctuating: Consists of both real and virtual memory. Included in the medium volatility category are the following: open files, system databases, ongoing processes, and network connections.
2. Low Volatility: Includes information on the current user and the state of the network.
3. Not Volatile: This pertains to things like system settings, user profiles, lists of processes and services that have been pre-configured, logs of events, and the locations of files and folders.

The understanding that a network connection is dynamic because it interacts directly with running processes, open files, and system databases is the foundation for differentiating it from status. These parts work together as a unit that may undergo dynamic changes. While data about users' accounts and the health of the network might change quickly, it usually stays very consistent throughout an acquisition. Conversely, permanent data consists of items such as user login data, system setup, and pre-established lists of features and procedures. Such sources may be efficiently analysed using conventional Reactive Digital Forensic (ReDF) methods and tools. Remember that even if files, directories, and logs of events are initially considered to be "not volatile," using real-time forensic analysis tools can alter their data.

Another among the primary objectives of active Digital Forensics is to "Recognize an offence as it happens." This goal requires the analysis of behavioural patterns in both machines and people. Then and only then will issues be identified and resolved instantly, enabling unhindered inquiry.

According to Bradford et al. (2007), he has presented a model that can identify certain occurrences automatically. Rather than serving as an intrusion detection system (IDS), this approach provides a structure for gathering useful information that can improve the efficiency of investigations and help zero in on new patterns in search. Even if there is a rising demand for IDS automation, this method should do more than just find occurrences. As highlighted in Taylor's suggested approach (Orebaugh, 2006), expert systems should be expanded and

improved so that they can detect occurrences and decide when more evidence collecting is needed.

The next section will outline the proactive Digital Forensic element while taking into consideration the variations in various tools and methodologies. The next part will assess a number of well-known live inquiry frameworks that have been documented in the available research.

Payer (2004) presented a novel architecture based on Network Intrusion Detection Systems that are stacked. IDS methods are seamlessly integrated into the networking layer in the prototypes developed under this architecture. To improve detection abilities, this integration makes use of already-existing state changes, storage content, header data, and packet contents.

As opposed to traditional NIDS techniques like analytic rule-driven detection of anomalies and signature-based detection, the stack-based authoritative method adds an extra layer of awareness that is perceptive to observed patterns. To accommodate real-time requirements, it relies on compact signatures and rapid scanning processes.

In this model, intrusion detection is centered on state changes rather than transitional shifts between states, thus utilizing unique state transitions stored as sequential state-based signatures in a database. The primary focus is on analyzing the behavior of state transitions rather than scrutinizing content. The framework empowers a scanner to traverse all states, efficiently seeking predefined signatures associated with specific intrusions.

In essence, this architecture allows state-driven detection methods to be effortlessly integrated into the overall network stack. It views every protocol up to the app layer as separate machines that implement application procedures.

The architecture use a multifaceted NIDS methods to find fingerprints and saves crucial forensic data. Contrary to conflicting opinions, Payer's approach advocates for the active role of the IDS in evidence collection during an attack, suggesting that the operating system itself should timely and systematically respond, ensuring the careful and methodical preservation of evidence.

Furthermore, the framework proposes that the suite of detection mechanisms be well-equipped to address issues such as IP spoofing, operating system identification, network stack obfuscation, as well as the detection of shell code and polymorphic shellcode.

Ren and Jin (2005) introduced an inventive approach to adaptive forensic and real-time investigations based on HoneyNet® technology. HoneyNet® systems are strategically designed to attract malicious actors, thereby revealing valuable information about these intruders and their illicit activities. This framework encompasses a network forensic system responsible for the comprehensive analysis and reconstruction of attack behavior.

While an ongoing cyberattack, the main goal is to quickly and effectively gather system and log information and then customize the evaluation to match the needs of individual users. This forensic method is made up of many essential parts:

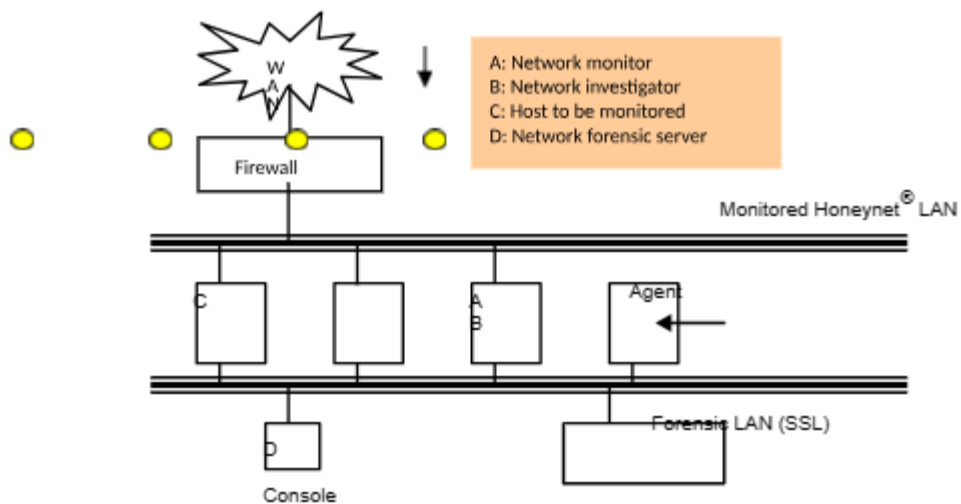


Figure 6-3 Architecture 2

Fraud services, the utilization of purposefully compromised systems, strengthening systems by applying OS patches, and functional servers encased inside the host running system's application space—are some of the techniques used to deploy Honeynet® technology. strengthened systems using user control servers often integrate firewalls and detection of intrusions systems.

In this structure, a networking forensic server is essential. It creates a structured database by combining IDS alarms with log and audit data. To glean valuable insights from this data, information mining methods are used. Given the extensive storage requirements, careful data selection is essential. Filtering mechanisms can be employed to eliminate unnecessary traffic. Moreover, the server demonstrates the ability to adapt data collection policies according to network traffic patterns. The analysis results are instrumental in creating attacker profiles. Notably, this framework primarily relies on deception technology

Foster and Wilson pioneered the concept of process forensics, a pioneering approach that enhances digital investigations by capturing volatile evidence, complementing both reactive and real-time investigative efforts. Process forensics harnesses the power of checkpoint technology, which allows for the preservation and analysis of a running process's state (Foster & Wilson, 2004).

A process's complete address space—which includes both user and kernel space—is saved into a file during the checkpointing procedure, which entails briefly stopping the task's execution. The process continues executing from the point where it was stopped after this capture. Crucially, setting up a checkpoint requires safe storage space but does not change the process that is now executing. There are two different kinds of checkpointing: final and progressive. While termination checkpointing is carried out immediately prior to an operation and any associated processes ending, incremental checkpointing creates images at regular intervals throughout a process's operation.

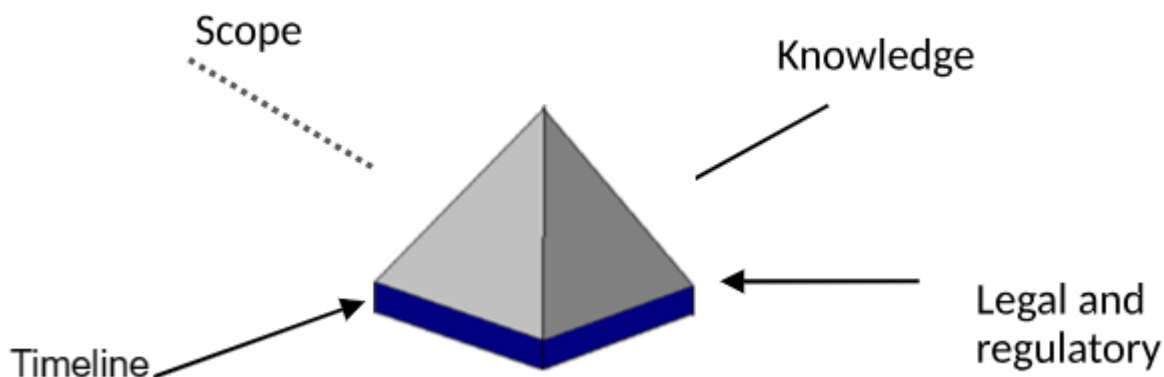
A process is any program or action that is carried out on a digital device. Important details about ongoing operations are contained in these procedures. A unique workstation-specific Process Identifier number is issued to each process. Additionally, the PID can be associated with "child" or "sibling" processes and is tied to a Parent PID. Interestingly, In the log files, the relationships among PIDs and PPIDs are not recorded. Additionally, the method's address area maintains information about peripheral elements, such open files, pipelines, socket relationships, and possible clues to the intentions of an intruder, like attempts to cover up trails or restrict damage.

Crucially, timing plays a pivotal role in the creation of checkpoints. When an intrusion detection system (IDS) triggers an alert, the immediate response of a system administrator may involve terminating all related processes. However, this action results in the loss of invaluable volatile evidence, which is essential for a successful investigation. It also alerts the attacker to the discovery of their activities. Therefore, a more strategic approach involves collecting evidence, particularly process forensic data, through the use of incremental checkpoints.

A few broad guidelines should be followed by milestone files in order to preserve the authenticity of a hierarchy of ownership and proof. This may be accomplished by using common formats and keeping them in safe places like encrypted files.

IDS systems should not only alert administrators to incidents but also trigger the activation of checkpointing applications. This dual functionality empowers IDS systems to focus on detection while ensuring that vital forensic evidence is systematically preserved.

The multidimensional Liforac framework for actual forensic training was proposed by Grobler. It consists of connected components and elements. The legal and controlling, the extent, the schedule, and understanding are some of the aspects.



The legal and regulation component serves as the model's basis, as forensic examinations must examine the incident's and investigation's legal and judicial environments. The main dimension is subdivided into four different sub-dimensions:

- 1: Commonly used criminal legislation against virtual crime

2: Specific legislation pertaining to cyberspace

3: Cases and judgments in the courts

4: Definition of admissibility in court.

#### Dimension 2: Timeline

The sequence of events view, which shows the tasks that the analyst should perform in the correct order, is the methodological view of the framework. For the time dimension, the Liforac approach included the following components:

Specific procedures, such as how to maintain the integrity of evidence, are examples of typical implied processes. These procedures will have no direct influence on a successful schedule.

The obvious processes are those that have an immediate effect on the effective completion of this dimensions, such as awareness, authorization, planning, notification, evidence search and proof of identity, inspection, theory, and information propagation (according to O' Ciardhuain's framework).

The first section looks at identifying every possible course of action before the acquisition starts, which frequently involves preparation, permission, and knowledge. Assessing the subject of the investigation's device's energy state (on or off), choosing a search technique, determining whether to safeguard or separate the device under investigation, and gathering evidence online or offline are some of the parts.

All potential operations throughout the purchase process must be identified. Coordination between announcement, search and proof of identity, and inspection is necessary. During the purchasing process, every possible operation has to be recognized. Typically, tasks such as notification, search and identification, and inspection should be undertaken.

Include comprehensive coverage of all conceivable post-acquisition actions, such as controls, information dissemination, and hypotheses. Maintaining the chain of authority, safeguarding the proof, transporting and storing this proof, and assessing the proof are among the duties using forensic software applications, and composing a report.

The understanding aspect denotes the investigators' various levels of comprehension and awareness. This dimension includes the conditions that investigators must fulfill, such as who needs to be engaged and what abilities are necessary. If they lacked the necessary abilities, they should be given appropriate training. The seven recognized components are as follows:

1. To grasp the background, implications, and scope of a given event, investigators must have a solid IT knowledge foundation.
2. Knowledge of the latest developments in cybercrime as well as how to counteract the most recent offences will keep the investigator up to speed.
3. Data is transformed into meaningful information via information systems, which are collections of techniques, algorithms, and procedures. An grasp of computer systems will aid the investigator in locating data or information to use as possible proof.
4. Social understanding of science can help the investigator construct an

outline of the cybercriminal.

5. Forensic science is an established field with firm foundations. The person conducting the investigation must be able to apply core forensic concepts to DF.
6. DF and law constitute two subjects that are inextricably linked. Legal and ethical understanding is required of investigators.
7. DF queries will be impacted by new technologies. The investigators need to ensure that they are knowledgeable about the latest software and technological advancements.

The nature of the aspect addresses common issues that investigators would encounter during actual investigations. The five parts are as follows:

1. To acquire entry to the targeted equipment, the investigator must first identify the legal criteria. To get a password or encryption keys obtaining an arrest warrant or a person of interest's cooperation may be required.
2. Every OS and forensic procedure has a unique interaction.
3. Procedures alter data while capture, resulting in live proof that is unacceptable under legal standards.
4. Proof must be verified in order to demonstrate that the proof given in court is the real evidence obtained.
5. Decide what is necessary to guarantee that the evidence obtained fulfills legal standards.

Certain requirements must be met by the proof acquired during real inquiries: it must be complete, require enough time to collect, be substantial, case-dependent, fair, verified, intact, precise, consistent, and have a particular sequence of variation. When choosing data, take into account completeness, time required, significance, and case dependence leads. Crucially, the data should be arranged according to variance so that you can assess if it could be applicable. The data collection technique reference order is shown in Figure 6-5 (below).

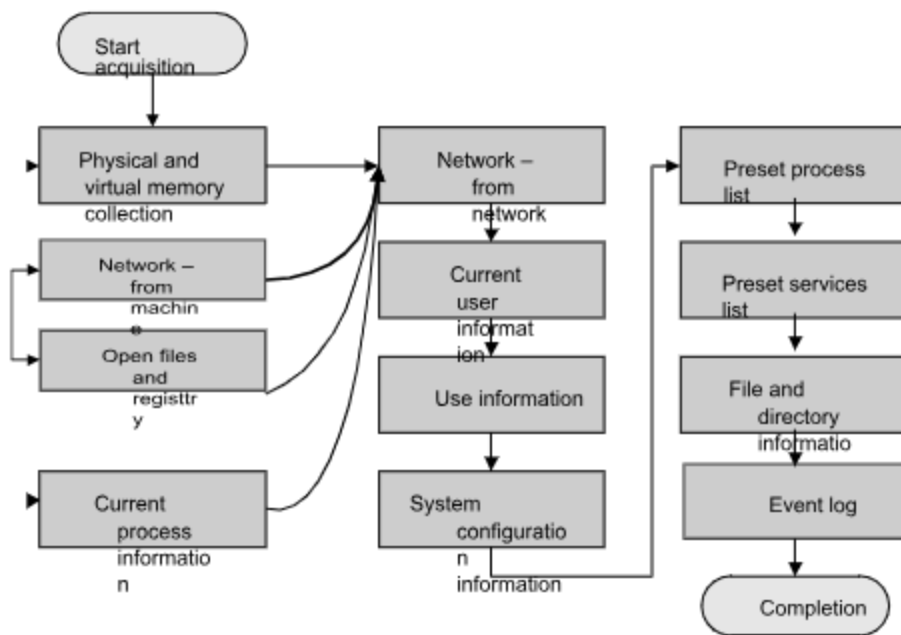


Figure 6-5: Data collecting procedure order in real forensic cases (leong & Leung, 2007).3

Unrelated to any live proof investigative tools or procedures offer a theoretical architecture for active inquiries. Table 6.1's layers 1 and 2 reveal that it does in fact imply some linkages to ReDF research, but it does not provide any ties to ProDF (below). Legal and judicial, administrative, procedural, policy, human, and technological aspects of DF will be interconnected through the use of the following questions: who, what, where, why, and how.

## ActDF definition

In Chapter 2, we adopt the suggested description for the ActDF part.

**Active DF is the ability of an organisation to gather (identify, collect and preserve) Comprehensive Digital Evidence in a live environment to facilitate a successful investigation.**

## Objectives for ActDF

We provide a set of broad goals to provide an extensive framework for the ActDF component. Based on the phases that are indicated in Chapter 3 and the levels and kinds of questions that are outlined in Table 6-1:

There is an evident need for a structure that can offer direction to investigators working on active cases (leong & Leung, 2007). The ReDF approach (Grobler & von Solms, 2009) outlines the legal obligations that must be completely taken into account while providing clear instructions for obtaining the extra necessary CDE during an ongoing event. This structure should be a vital part of our the company's CDF capability's ActDF component.



The ActDF structure need to comprise an array of rules and processes intended to direct choices and actions if it is determined that gathering live evidence is necessary. The company's continuity of operations, recovery from emergencies, conventional incident handling, and intrusion detection systems should all function in harmony with this architecture. When it comes to gathering evidence and making the attacker's profile easier to understand, the IDS may be quite important. Specific instructions for handling the event, keeping track of evidence, and choosing when and how to launch an inquiry should be provided by the company's IRP and BCP.

The company's risk management should finally make the crucial choice of whether to put an end to the incident and the impacted systems or limit it to an isolated setting. Numerous factors, including the expense of the inquiry, the seriousness of the occurrence, and concerns about the organization's reputation, may have an impact on this choice. Experts in data safety and digital forensics should be included in the selection procedure so that the management may make well-informed choices about handling incidents.

Maintaining that the authenticity of the proof is maintained by this framework's persistent adherence to the fundamentals of the hierarchy of custody and the trail of proof is crucial. Therefore, it is essential to promote a culture of thorough recording of all actions over the course of the active inquiry.

Most active investigations take place across a network. Although there are a number of systems available for real-time research, they mostly use communication records from the IDS and the network OS.

## ActDF protocol

We suggest you go through the four stages, each with its own set of steps:

Add these ActDF criteria to the ReDF element as specified in :

Examine the logic of the procedure. The case's specifics will determine the operation's priority since they must pinpoint the exact moment the incident happened.

Along with determining if the target computer's power is on or off, researchers must also decide whether to use a covert or overt investigative technique, secure or separate the machine being investigated, and gather data on site or virtually.

Allow the occurrence to persist in a monitored setting until the enterprise's control plan is activated. The goal is to lessen the event's detrimental consequences on the existing system.

- Step 1: Identification of Vital Clues

Start the process by identifying the live proof that is essential to a thorough inquiry of the occurrence. Make wise choices on what proof to collect based on the incident's character. Consider both particular to the system variable data and incident-specific volatile data when weighing the proof's robustness and instability. Consider any temporal

limits that may impact non-volatile data as well.

Recognize that determining the required proof depends in large part on the operating system selection. Examine the limitations of the suggested live evidence collecting process, taking into account the intended device's location, the task's anticipated duration, and any possible effects on other distant systems.

- **Step 2: Collection of Proof**

Using the appropriate instruments, methods, or apps needed to create a threat profile and gather the relevant evidence, move on with gathering any more missing proof .

As quickly as feasible, streamline the methods, applications, or tools required for obtaining proof; better still, start them as soon as an emergency alert that is sparked by a particular event is sent out.

Adhere to an established procedure while gathering actual proof. Respect the subsequent foundation for data collecting, as outlined by (leong & Leung; 2007):

1. **Minimize User Involvement:** Keep user involvement to a minimum.
2. **Essential and Discreet Steps:** Make sure that every action you perform is necessary and won't create too much trouble.
3. **Minimal Modification of Static Digital Proof:** Refrain from making substantial alterations to digital evidence that is static.
4. **Degree of Instability and Urgency:** Gather information based on the digital proof collecting priority and order of instability.
5. **Obtain Non-Priority or Unstable Proof using conventional Techniques:** Save traditional approaches for the gathering of non-priority or unstable evidence.
6. **Copy or Extract Data Only When Original Data and Timestamps Remain Unaltered:** Ensure that data copying or extraction does not affect the original data or its timestamps

Determine if the requisite live proof has been obtained using the outcomes of the ActDF investigation phase. If further live proof is required, the ActDF investigative phase must be repeated to obtain more live evidence. Several considerations can influence whether the inquiry can be continued; for example, the organization's risk management framework may state that the impact on company operations or the expense is too great.

Prepare case documents for the proactive investigative unit to carry out their examination.

In the initial stage, Phase 1 aligns with Objective 2, aimed at mitigating the repercussions of an ongoing situation. Subsequently, Phases 2 and 3 correspond to Objective 1, which focuses on leveraging the right technology tools to gather and analyze relevant actual time digital proof in an operating or live system. In conclusion, Phase 4 is associated with Goal 3 and aims to set the foundation for a reactive inquiry while adhering to the the company's existing risk management structure.

The ReDF element or the ActDF element alone may activate the ActDF element when immediate style proof is needed to look into an incident. You can see an illustration of the stages that make up the ActDF part of our CDF capabilities here. After the required proof is obtained, the ReDF team regains command to continue the investigation.

ActDF is chiefly concerned with a preliminary assessment of the incident and doesn't delve

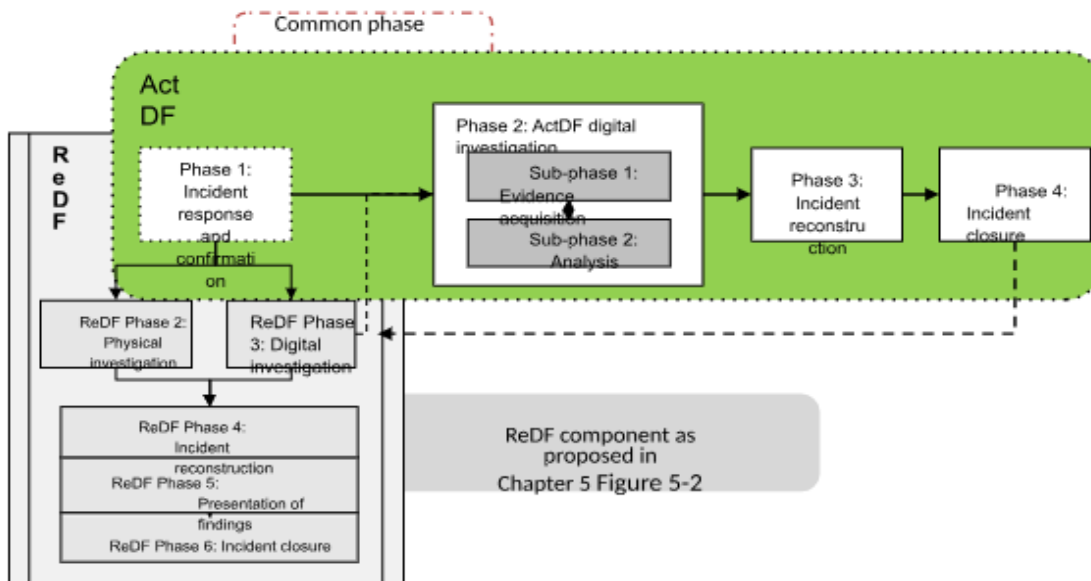


Figure 6-6. ActDF Component 4

deedply into reconstruction. Its primary aim is to ascertain if the essential real-time evidence for a successful investigation has been successfully gathered.

## CHATER 7: COMPREHENSIVE DF CAPABILITY

In light of our exploration and analysis thus far, the imperative for our Comprehensive Digital Forensics (CDF) capability has been recognized. This capacity will cover the whole range of preparatory actions, incorporating the use of digital forensic tools, the gathering of live proof, and the emergency trial that follows, incorporating post-investigation tasks. The author's illustrated description of the three essential components of the CDF competence is based on our earlier chapters, which were devoted to the examination and contrast of various DF concepts and views.

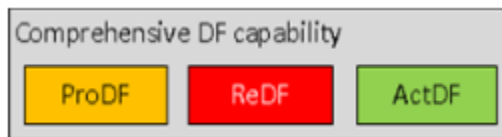


Figure 7.1 CDF capability

The principle that "prevention is more effective than intervention" is highly pertinent to modern organizations facing an escalating need for digital evidence. The idea behind a proactive digital forensics capacity is to set up an organization such that digital investigations may be completed quickly and affordably with the least amount of disturbance to regular company activities. Its main goal is to provide easily available, complete digital proof and robust forensic processes, whether they are required for inquiries or to prove due diligence in corporate governance cases during regular business operations.

Upon examining the existing body of literature, it is evident that many contemporary Digital Forensics models incorporate a "preparation" or "DF readiness" phase. In Chapter 4, we introduced a preliminary definition for ProDF, which we now seek to refine:

*DF readiness is the ability of an organisation to maximise its potential to use comprehensive digital evidence whilst minimising the costs of an investigation.*

*ProDF is the forensic preparation of an organisation to ensure successful, cost-effective investigations, with minimal disruption to business activities, and the use of DF to establish and manage governance programmes.*

We previously put forth two distinct objectives for ProDF:

1: Achieving DF readiness.

2: Enacting and overseeing DF to enhance governance initiatives.

ProDF

ProDF goal 1: Become DF-ready				ProDF goal 2: Implement and manage DF to improve governance programmes	
Sub-goal 1:	Sub-goal 2:	Sub-goal 3:	Sub-goal 4:	Sub-goal 1:	Sub-goal 2:
Prepared infrastructure	Maximize CDE availability	Prepare responsible, competent employees	Ensure a cost-effective investigation	Establish a DF management capability	Apply DF to provide reasonable assurance regarding the achievement of organizational objectives

Table 7.3 visual representation of the ProDF.

DF preparedness is an organization's capacity to maximize its ability to apply CDE while minimizing investigative expenses. Four sub-goals promote DF preparedness:

1. Establish a ready infrastructure.
2. Increase CDE availability.
3. Develop an accountable, capable workforce ability by the creation of a DF awareness, training, and education plan and accompanying programs.
4. Ensure an affordable inquiry.

The following part will elaborate on and explain the four smaller objectives of DF preparedness.

The functional and DF analysis infrastructure is part of the given architecture. It is vital to ascertain the regulatory and legal prerequisites for technology acquisition, configuration, and administration. The configuration of the hardware or software required to guarantee the legitimacy of the proof produced by the system in question is one of those criteria. Learning investigative methods and instruments suitable for the permissible and administrative domains is equally vital. In order to ensure that ready architecture is available, organizations need to have appropriate management procedures in place, and infrastructure needs to be controlled. We will now determine the necessary steps to establish our operational architecture.

In the pursuit of digital preparedness, organizations must embark on a comprehensive assessment of their operational landscape, seeking out areas ripe for transformation to facilitate Digital Forensics (DF) integration. This endeavor encompasses the identification of business processes, applications, and infrastructure earmarked for the transition to a state of DF readiness. Such an initiative extends beyond the confines of Information Security and Information Technology systems. To illustrate, consider the following measures:

1. When creating new apps or networks, take into account the forensic process and digital proof within the entire phase of the development cycle.
2. The methodical planning, setting up, carrying out, and overseeing of functional architecture, supported by pertinent guidelines and protocols, with the general goals of:
  - Thwarting anti-forensic activities.
  - Curtailing anonymous actions.
  - Establishing the ability to systematically gather possible proof by

- turning on extensive logging features.
  - Using standards, such as file system discrimination, to create forensic-friendly file structures.
  - Using profiling methods in conjunction with recurring inspection processes to identify and track down attackers or assaults.
  - Making use of virtual fingerprinting methods to protect confidential information.
  - The development of the capacity to collect dynamic, real-time evidence, particularly through offsite logging.
3. The synchronization of temporal data across all pertinent devices and systems to facilitate the chronological organization of events during any subsequent investigative processes.
  4. Implementation and configuration of an Intrusion Detection System (IDS) to expedite the early detection of security incidents, ensuring prompt response measures are initiated.

## **DF Investigation Infrastructure**

Effective management must establish and designate a secure and dedicated facility, referred to as a Digital Forensic Investigation (DFI) laboratory. This laboratory is intended to serve as a safeguarded repository for all case-related documents and evidence, ensuring their integrity and confidentiality.

In addition to committing to strong analytical skills, companies should make sure that a comprehensive investigation environment is in place. An isolated network, forensic servers (with both temporary and permanent storage), and other necessary tools and equipment are all included in this system. Disc duplicators, video cameras, mobile kits, and networking equipment are some examples of these items. Additionally, a wide range of legally acceptable forensic gear and software should be available for use in the DFI lab. These instruments ought to be able to gather, examine, assess, and display digital proof, including live, unchanging, past, and post-investigation information.

A thorough policy and procedure structure must be established in order to run the DFI laboratory. The system will control who is granted entry to the establishment, how the laboratory is used, and how instruments are used responsibly. Implementing access logbooks to regulate entry and keep track of authorized individuals is one example of such a policy.

## **To-do list**

1. Determine which laws and guidelines are applicable to the structures used for operations and investigation. Take into account the technical and analytical architecture setup, the legality of the investigations tools, the criteria for proof, and the methodologies.
2. Establish the organizational frameworks required to guarantee that the tools, hardware, software, and facilities needed for a fruitful investigation are available.
3. When formulating policies and guidelines to govern the configuration, use, and upkeep of the functional and analytical architecture, only consider the procurement and implementation of appropriate and legitimate forensic techniques, equipment, and techniques.

## Strategy for Proof Handling

Identifying and managing digital proof requires the implementation of controls and mechanisms in the field of corporate digital oversight. Within the scope of Proactive Digital Forensics, we provide the idea of a Proof Handling strategy, based on the observations made by Beebe and Clark in 2005, which emphasize the importance of a data preservation strategy.

The EMP, structured around four key steps, serves as a robust foundation for the identification and effective management of digital evidence:

### 1. Proactive Identification:

This initial step involves the proactive identification of potential Comprehensive Digital Evidence (CDE) tailored to specific risk scenarios or scenarios of concern. It is critical to identify all conceivable business circumstances that would need the use of digital evidence. Several writers (Beebe & Clark, 2005; Louwrens et al., 2006b; Rowlingson, 2004) advocate finding possible evidence throughout the risk assessment process.

A danger or assault profile is frequently created by companies as part of the company's effect study. The danger profile includes general details about the risk that has been identified, including its description or metrics, the controls that have been employed, and the policies linked to the threat (Whitman & Mattord, 2009).

### 2. Organizational Framework:

In the second step, an organizational framework is established by creating an evidence index. This index was designed using the author's innovative network proof map as well as inspiration from Casey's proof map. The same bits of proof are unavoidably needed for different situations or hazards. According to (Casey, 2007), a virtual proof connecting should be created that would include all pertinent details about the proof, such as its categorization, location, length of preservation, and methods for acquiring and accessing it.

After locating and organizing all available evidence, we need to add to the the company's information structure and evaluate how the additional evidence could affect the layout.

We recommend that the organization use its network diagram to map the evidence items. The risk profile will next be completed by analyzing the CDE grade for every risk or situation.

### 3. Evidence Assessment:

The third step entails a critical assessment of the current state of the evidence with regard to known evaluated risks or scenarios. Assessing the thoroughness of the CDE set linked to each unique risk or scenario is the main goal of this evaluation. The author has created a fresh assessment system. We recommend using the Upgrader matrix, which was first proposed by Arthur, Olivier, and Venter in 2007. This matrix is the basis for determining the Complete digital proof rating and giving an evidence set designated as [E1, E2,..., En], connected to a particular risk or situation, a matching CDE flag colour.

Within an organization, it falls under the purview of the risk management department to

establish precise combinations of certainty ratings for evidence set that are deemed acceptable.

#### 4. Policy Enhancement:

The fourth and final step of the EMP revolves around the development and enhancement of evidence-related policies and procedures. The purpose of these regulations is to guarantee that proof sets obtain the best feasible CDE rating. This CDE grade is a useful tool for evaluating how thorough the proof collection is for a particular risk or situation. Common policies and practices to take into account are:

The process of creating and refining rules and regulations serves as the foundation for directing behaviour and activities inside a company. These directives are instrumental in establishing a framework for effective evidence management. The following categories encompass some of the typical policies and procedures worthy of consideration:

1. Proof managing include specifying the procedures for digital proof from static, live, and legacy sources, including proof of identity, acquiring it, dealing with, safeguarding, authorization, transport, and safe keeping.
2. Post-Investigation Methods: In this case, the emphasis is on managing proof after the inquiry is over, including choices about the proof's preservation, exchange, or digitization.
3. Risk Control and Emergency Preparation: Procedures and regulations must be in line with these broad frameworks in order to support conventional risk management techniques and contingency plans. This involves incorporating digital forensics into the disaster healing, company continuity, and crisis management plans. Particular focus areas include incident identification, verification, containment, escalation, and cleanup. These rules must recognize the need of identifying and preserving Comprehensive Digital Evidence and place a strong focus on forensically sound practices. Additionally, maintaining the authenticity of a chain of custody and the trail of proof should be a top priority for all rules and processes.
4. Quarantine plan: Another crucial component that calls for supplementary regulations and processes is the creation of a strong confinement plan that takes into account actual systems. This ensures that organizations can effectively manage and mitigate digital incidents, reducing potential risks.

It's essential to know that this list is not exhaustive but serves as an illustrative reference, provide a foundation for thinking about the fundamental guidelines and practices required for the thorough administration of digital proof and safety.

#### **To-do list**

1. Organizations should develop an EMP to handle proof, as well as discover evidence for possible hazards or situations.
2. Determine the needs for digital and physical proof in terms of technology, law, and regulation.
3. Evaluate the entirety of an evidence collection linked with a potential danger or



- scenario.
4. develop rules and processes for managing both physical and digital evidence.
  5. Add rules and regulations that support the company's plans for emergencies and hazard managing approach by including evidence and procedural requirements.

## **Establishing Pervasive Culture**

The overarching objective of this strategic initiative is to instill a pervasive culture of preservation within the organization, encompassing the conservation of both digital and non-digital evidence. This strategic framework aims to uphold the fundamental principle of conducting activities correctly and ethically.

The Digital Forensics (DF) training and awareness strategy assumes a comprehensive scope, encompassing educational, training, and awareness programs tailored for the entire organization. These programs are designed to address multifaceted dimensions, including technical proficiencies, legal comprehension, judicial nuances, and regulatory compliance, all of which are essential facets in today's dynamic landscape. A central component of this strategy involves the creation of a dedicated DF awareness program. This program serves to enlighten employees about DF requirements, emphasizing the paramount significance of evidence in the organization's operations.

This technique is based on the creation of a policy and accompanying operational standards for DF instruction, instruction, and awareness. These guidelines are intended to provide a road map for the creation, management, and supervision of projects related to instruction, instruction, and understanding.

A successful understanding program is poised to empower employees with a deep appreciation for the value of evidence and a commitment to adhering to the prescribed protocols and standard operating procedures. It's worth noting that awareness programs should be targeted, recognizing that distinct roles within the organization necessitate varying levels of awareness. A computer system administrator's knowledge requirements will be different from that of an information capture, for example. The main goal is to foster an environment in which maintaining of proof is a routine activity.

To ensure the quality and standard of the training programs, it is advisable to seek accreditation from recognized authorities, such as the South African Qualifications Authority or other relevant certifying organizations. Accreditation provides a measure of assurance regarding the content's quality and alignment with industry standards. Facilitating opportunities for employees to attain industry certifications serves a dual purpose. It not only elevates their professional qualifications but also fortifies the credibility of evidence collected during investigations led by qualified practitioners, thereby reducing the likelihood of challenges to procedural integrity in legal contexts.

1. **Technical Proficiency Development:** Empower individuals within the organization with the technical acumen needed to navigate the digital forensic landscape. This entails cultivating an in-house Digital Forensic Investigation (DFI) capability, should the need arise. Training courses include the use of paid and freemium forensic tools for the collection and examination of digital proof on live, unchanging, and legacy systems. The

effective retention and recovery of evidence from antiquated OSeS, specialized hardware, outdated software programs, and mismatched disc drives is given particular attention. The training modules integrate real-life case studies, fostering a practical dimension that assesses participants' competency.

2. **Training for First Responders:** This section of the program is designed to provide a group of first responders with the skills necessary to safely gather, store, manage, and retrieve Complete Digital Proof. Clearly defined rules and processes must be established in order to instruct employees on the "what," "when," and "how" of reacting to event notifications.
3. **General User Education:** Beyond a broad awareness campaign, the organization extends training to its general and managerial users on a need-to-know basis. This training extends to the appreciation of the importance of evidence, an understanding of procedural workflows, and insight into the legal ramifications associated with actions carried out at different organizational levels. These training programs are tailored to align with Digital Forensic (DF) requirements commensurate with various roles and positions.
4. **Expert Witness Preparation:** This specialized training endeavor is designed to equip individuals with the expertise required to serve as credible expert witnesses in legal proceedings. The goal is to ensure that their testimony adheres to admissibility standards, bolstering the integrity and efficacy of their contributions within the legal domain.
5. **Establish an awareness programme:** Organizations, like the DF programs for learning and training, will be forced to establish awareness programs based on current situations. These will guarantee that personnel are aware of critical concerns and understand what is expected of them in specific scenarios. It is usually concerns with keeping evidence during event response.
6. **Establish a code of conduct for using DF tools and techniques.** A collection of criteria for various roles must be created due to the sensitive characteristics of DF products and processes in order to guarantee that the breakthroughs and approaches are used ethically.

## **To-do list**

Organizations are tasked with a series of vital steps to fortify their digital resilience:

1. **All-inclusive Plan:** Create a plan for Digital Forensics knowledge, instruction, and training that will provide employees in the company with the necessary abilities.
2. **Framework for Policy and Procedure:** Provide a logical set of rules and procedures to direct the development, execution, and supervision of projects related to awareness, education, and training.
3. **Certification and Recognition:** Establish what exact acceptable, judiciary, technical, and regulatory requirements must be met in order to certify employees as experts and approve training and educational programs.
4. **Customized Courses:** Create specialized understanding, training, and instruction courses to meet a range of demands and specifications.
5. **Role-Based Education:** Create a policy outlining the training requirements associated

with particular organizational responsibilities. This guarantees that any evidence used in a proceeding of law complies with the strictest admissible requirements.

6. Create a rules of ethics outlining how the company should use DF in a manner that is responsible and ethical.

## Cost Effective Measure Integration

The investigated DF frameworks do not indicate how to conduct a cost-effective study. To correct this deficiency, we integrated the following parts.

1. Make sure there is a DF inquiry methodology in place that has been verified and thoroughly documented. Create a DF inquiry process and compare it to industry standards. Supporting policies and procedures provide the framework for the procedure, ensuring that all employees are aware of the what, why, when, where, and how they are expected to perform.
2. Create a process to guarantee that occurrence's impact and investigative costs are reasonable. According to Whitman and Mattord (2008), the methodology has to include crucial components in order to determine the cost of an investigation. The elements include the anticipated number of man hours required, the potential financial loss from an interruption in service, and the importance of any sensitive data (CERT@ Coordination Centre, 2004). It is necessary to create a system that contrasts event cost with investigating cost in order to clarify the expense of inquiring preparation.

If the foundations is ready, proof and procedures are available when an inquiry or proof of compliance is necessary. The proof will be accessible and can be obtained with little disruption to the organization's everyday activities. It is essential to complement and incorporate risk management, company continuity plans, and supplementary plans, regulations, and processes in order to guarantee that DF proof and process requirements are satisfied. To reduce the effect of the event, a well-defined containment plan must be developed.

## To-do list

Organizations must adhere to a set of pivotal actions:

1. **Structured DFI Protocol:** Create and verify a thorough process for digital forensic inquiry that includes both proactive and reactive investigative techniques. This guarantees that inquiries are carried out in a logical and structured way.
2. **Policy and Procedure Alignment:** Guarantee the presence of all requisite policies and procedures essential to the effective execution of the Reactive Digital Forensic (ReDF) and Active Digital Forensic (ActDF) protocols, which are pivotal for a successful investigation.
3. **Holistic Risk Management:** Improve the company's relevant policies and processes, handling of incidents, company continuity and recovery from disasters plans, and manage risks and continuity of operations strategies. This is enhanced to include criteria for digital forensic proof and processes. It also entails putting into practice a Digital Forensics friendly confinement plan and related plan, which are designed to

minimize the effects of an event while optimizing the availability of crucial evidence.

4. **Cost Management Framework:** Ensure the presence of policies and procedures that are dedicated to managing the costs associated with investigations and incident response activities.

## Utilization of DF Resources

This plan will specify how and when DF resources and innovations may be used within the organization (four components):

1. Element 1: the hierarchical framework must be changed by management in order to accommodate DF.
2. Element 2: The roles and duties of the data security, CERT, risk management, and DF teams should all be well defined.
3. Element 3: A well-established outsourcing plan and processes are necessary when delegating a DF inquiry. Examining proof and procedure criteria is essential when creating agreements on service levels.
4. Element 4: Make sure a review of the law is in order so that appropriate action may be taken given the situation.

Establishing procedures and rules to control the use of Digital Forensics devices and instruments is necessary to give a fair level of assurance for the accomplishment of corporate objectives in the five categories below:

1. Asset protection for the firm (including information) Organizations must guarantee that information integrity is maintained. Every paper's integrity should be guaranteed by the board of members. It is possible to demonstrate that the information is in its original state using DF tools and processes. To look into allegations of corporate resource exploitation and technology misuse, DF procedures and methods can be used to obtain evidence. Creating a plan for reporting corruption is also crucial (Patzakis & Limongelli, 2004). To produce audit records that are more accurate, the Information Security team should integrate DF techniques into auditing IT processes.
2. Enabling company sustainability in both normal and unfavourable operating situations. Organizations leverage DF tools during penetration tests, a practice aimed at uncovering vulnerabilities within their systems (as emphasized by Richardson in 2008). Evaluating the potential hazards associated with emerging technologies is a requisite task. This assessment extends to determining the adequacy of existing DF tools for potential incident investigations. Vigilant monitoring and control measures are implemented for the use of removable or portable devices, with the aim of mitigating or preventing cybercrimes. Notably, new technologies like smartphones may serve as conduits for acquiring organization-specific information, including sensitive intellectual property. When DF tools are used wisely, they may improve a company's overall technology use and efficacy. These methods and technologies have many uses; they can help recover data from hard drives that have failed, safely wipe hard drives before disposing of equipment, and make it easier to find forgotten passwords. By using these technologies, company operations are disrupted as little as possible, allowing for a quick restart of operations. It is critical that DF requirements be taken into account while

creating IT governance rules, procedures, and controls. A thorough framework to traverse DF problems has been provided by the suggestion of an assortment of CobiT rules that have been the result of a thorough investigation.

A proactive strategy entails strengthening backup plans, guidelines, and protocols when unfavourable circumstances arise, especially when it comes to handling incidents, catastrophe recovery, and continuity of operations. These improvements are intended to lessen the possible impact on the company's regular operations, in line with the goals outlined in the DF preparedness sub-goal 1.

3. Reporting Reliability mechanism in Organizations are compelled to furnish trustworthy reports, underpinned by Comprehensive Digital Evidence (CDE), to fulfill the mandate laid out in the requirement, as articulated by von Solms and von Solms in 2009. According to this criterion, the committee is in charge of making sure that a methodical, thoroughly documented evaluation of the procedures and results related to key risks is carried out every year. Furthermore, it necessitates the ability to issue a public statement concerning risk management.

In the event of an incident, upon the culmination of an investigation, the organization is mandated to present a detailed report delineating the incident's nature, its repercussions, and a comprehensive review. The strategic infusion of CDE into audit trails paves the way for a continuous stream of precise audit outcomes and compliance assessments. Likewise, the integration of Digital Forensic (DF) techniques into auditing procedures augments the credibility of audit results.

To bolster informed decision-making and risk management, it becomes imperative for management to receive regular, up-to-date reports on the organization's risk management processes and ongoing investigations. This transparency is crucial in maintaining a proactive and vigilant stance in the dynamic landscape of organizational governance.

4. Element 5: Conducting oneself properly toward each stakeholder (King, 2003). Organizations must exercise due care when it comes to effective governance. Managers will be ready to produce written evaluations to demonstrate that frequent inspections were carried out. To clarify the impact on the company, it is essential to show stakeholders that you are accountable and transparent, its underlying cause, and the investigation's conclusion. ProDF covers the need for companies to be DF-ready so as to have the necessary digital evidence on hand for DF inquiries and to be ready for them. It also addresses the ethical utilization of DF technologies and methodologies to help companies create and sustain regulatory frameworks.

## **To-do list**

Organizations must:

1. Develop a DF plan for handling DF application in an organization.
2. Create regulations and processes that reinforce the DF plan and make sure the organization has clear guidelines for managing DF for investigative and non-investigative

reasons. Policies for establishing a DF capacity in the organization must be mentioned.

## **REACTIVE DF (REDF) COMPONENT**

No organization can ever be fully equipped to handle every potential crisis that may arise. The concept of ReDF, as outlined in this research, is primarily focused on the conventional investigation process, known as "dead forensics," which takes place after an incident has been identified and verified. To proactively prepare for potential incidents, it is imperative to establish a well-defined and proven digital forensics investigation protocol, as outlined by ProDF, dictating how investigations should be conducted.

The following is the formal definition of ReDF, and it will serve as our foundation:

*A ReDF component is application of analytical and investigative techniques for the preservation, identification, extraction, documentation, analysis, and interpretation of digital media, for evidentiary, and/or root cause analysis and the presentation of comprehensive digital evidence derived from digital sources for the purpose of facilitation or furthering the reconstruction of incidents; (Kruse & Heiser, 2004; Palmer, 2001; Reith, Carr & Gunsch, 2002; Rowlingson,*

We defined two primary objectives for ReDF in Chapter 5, as discussed:

### **1: Thorough Investigation of Incidents**

Obtaining the essential Cyber Digital Evidence (CDE) to determine the incident's cause, link the offender to the crime, and build a strong case is critical to achieving this objective.

### **2: Reducing the Effects of Incidents**

A thorough ReDF structure with several stages and related procedures, differentiating between digital and physical inspections, was presented in Chapter 5. Following the following definitions it is crucial to establish both physical and digital crime scenes.

The actual location where artifacts connected to an event or crime might be discovered is called a physical crime scene. In the context of a virtual crime or event, the digital space made by software and hardware is known as a digital crime scene.

## **Key Digital Forensic Phases**

For phase 1, we have specified 10 stages. To reduce phase 1 to eight processes, we consolidated certain steps and added that satisfy the forensic methods of keeping proof secure and paperwork.

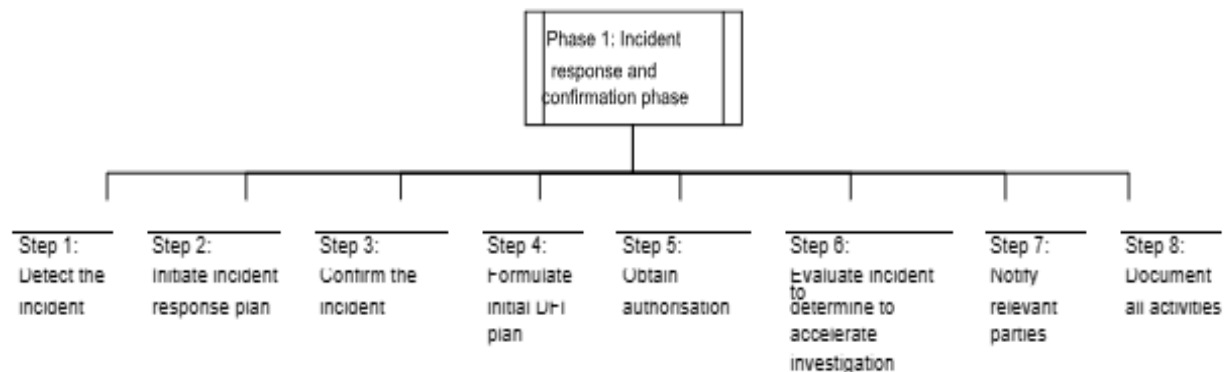


Figure 7.6 Phase 1 ReDF protocol

Phase 1: Shows reaction and verification in the ReDF part (eight phases) is depicted in

Step 1 is to identify the occurrence, which includes steps 2 and 3. States that the IDS will notify any potential incident after detecting anomalous behavior. Upon detection of an incident, the ActDF component will be carried out in response to certain incident notifications, allowing for the collection of the required live proof.

## 2. Start IRP.

Work together with the CERT and IRP to create a mitigation plan that will lessen the effect of the event. The IRP and containment plan must take into account the objectives and issues of the business reasons, legal, complicated, and political domains (par. 5.5.1.6). It is the job of the detective to make sure that forensic regulations are strictly followed and that evidence is preserved.

### Verify the occurrence

After the occurrence has been recognized, the next step is to determine its worth. Verifying the occurrence, assessing the incident's possible impact, and confirming the incidence are all necessary steps for organizations.

Someone has to decide to look into it. Considerations such as the nature of the investigation (official vs. informal) and its applicability must be carefully considered. One of two outcomes is likely to occur: If it says "NO issue," then nothing further has to be done. If it says "CONFIRMED event," then either keep looking into it or disregard it.

Step 4: Create a preliminary Digital Forensics Investigation plan for gathering and analyzing data

In the event that the company lacks sufficient internal assets, the DFI plan will organize all the resources required to complete the inquiry and indicate if the company should outsource all or only a portion of it.

The fifth stage is to get the necessary authorization, either from inside the company or from outside sources, to carry on with the inquiry.

Sixth Step: Assess the situation to see if the inquiry needs to be expedited

### Section 7: Inform Appropriate Parties of the Investigation

Step 8: Keep detailed records of all IR and confirmation phase actions (using the author's own words, following the Beebe & Clark, 2005 documentation concept).

This step will be skipped if an actual crime scene is not accessible. In order to meet the forensic standards of evidence and evidence conservation, we took note of the seven methods mentioned in Chapter 5 and added some of them. This stage of the ReDF component is shown in Figure 7-7 (below) (eight phases).

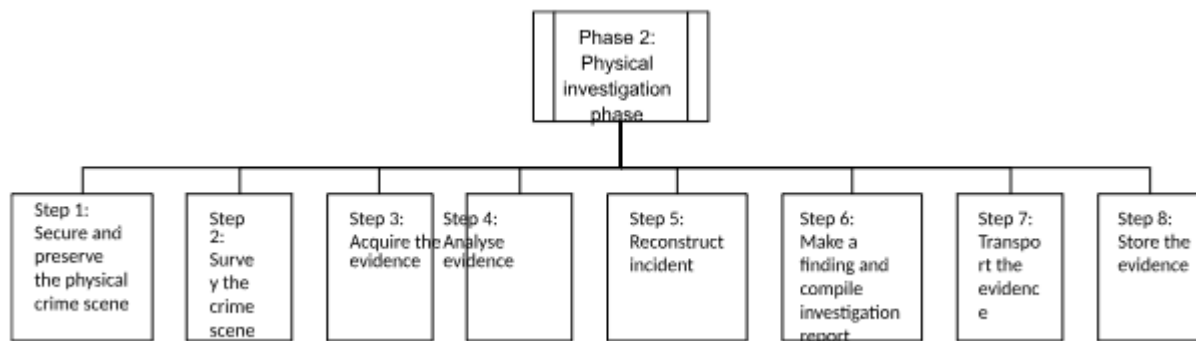


Figure 7.7 Phase 2 ReDF protocol

The investigator travels around the scene of the crime to inspect it and verify prospective proof; this includes photographing, sketching, and filming the crime scene as well as identifying both physical and digital evidence.

To get prospective evidence, follow an authorized approach. Individual evidence pieces are often photographed, bagged, labelled, and documented. Preserve the chain of custody by documenting all actions.

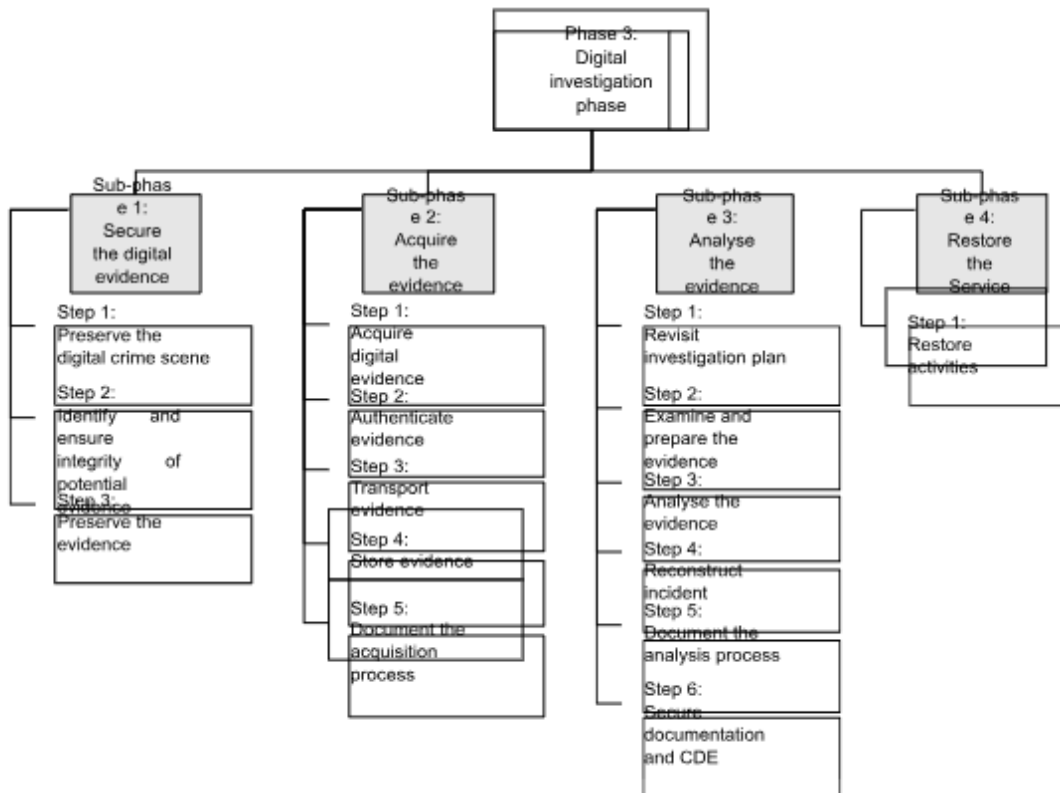
To guarantee that the proof is analyzed by the appropriate forensic laboratory, the person investigating must identify distinct forms of evidence, such as fingerprints or digital evidence.

The person conducting the investigation will utilize the physical evidence available to recreate the occurrence in order to assess if the evidence fits the initial theory.

The person conducting the investigation will make an initial conclusion based on the available evidence and construct an investigative case file that includes all supporting paperwork. The paperwork will provide the case with a chain of proof and possession.

Store the material in a secure custody room and make sure access to the proof and custody room is restricted.





This stage is divided into four sub-phases:

we found four phases for sub-phase 1 and condensed them into three to offer attention to the steps.

Sub-phase 1 consists of three steps: **Securing the digital evidence.**

First you must take steps to save the virtual crime scene. Make sure the virtual crime of the scene is preserved so proof can be found. Follow all guidelines for managing evidence as you clean up the crime scene.

**Second find and save any digital evidence that may be relevant.**

Analyze the risk profiles and CDE rating to ascertain what proof is needed to investigate the incident. Start the ActDF function to obtain instantaneous proof.

The investigator must adhere to the guidelines set forth by the DF. To preserve the evidence, be careful to write-protect any media, separate or deactivate critical systems, or shut them off completely. Forensic analysis requires an identical duplicate of the potential evidence.

If handling tangible data—such as a hard drive—is required in order obtain digital proof, record the whole process in order to save the chain of proof before and after making a forensic recording of the related virtual proof.

### **Third stage, record all actions.**

It is essential that only qualified individuals engage with the media so as to produce a trustworthy audit. This record must include all processes performed on digital evidence before it can be used in court.

Phase 2: Gather Evidence.

Gather digital proof as a first step

To collect evidence, use the ideas of recovering, harvesting, and reducing. When an investigator practices recovery, they increase the likelihood that they will recover all evidence, including evidence that has been hidden or deleted. Data and information pertaining to incidents will be gathered through harvesting. This part involves checking the evidence to determine if it backs up the theory. In a reduction analysis, all evidence that isn't pertinent to the argument will be eliminated.

Make use of relevant DF tools to unearth meta-data and files that have been buried, destroyed, swapped, or damaged. Collect evidence from hosts and networks in addition to evidence from removable media. Make use of digital evidence bags (DEB) for storing evidence (Turner, 2007). Any type of digital evidence can be stored in a DEB format.

Second Step: Verify All Evidence The person investigating will validate the copy of the collected material using a hashing procedure. Lastly, be sure you digitally stamp any copies of authorised proof.

Thirdly, transfer of evidence

Ensure that the proof's chain of custody is preserved during its transit to the DF inquiry lab if it was obtained outside of the DFI laboratory.

"Storage of Evidence," instructs you to place all collected evidence in a secure location. Restricting access to the secure custody room and implementing steps to safeguard the chain of custody in storage are both necessary.

Step 5: Record the steps used for acquisition

Stage below Step three is to examine the evidence.

Initial Step: Update the investigative strategy.

Your original plan for the inquiry will need to change once you start looking into the evidence. In order to determine if your theory is still applicable, you should review all of the available information about the event, evaluate your abilities and analytical DF tools.

You must examine and prepare the evidence.

To determine the suspect's skill level, run a preliminary data survey. To get the evidence ready, you may do things like make sure the material is understandable by humans or break down massive volumes of data into smaller parts. Encrypted data can be analysed with this guarantee.

Third, examine the proof.

A thorough evaluation of the evidence found in the previous step is what the examination phase is all about. Make use of state-of-the-art data extraction technologies to carefully examine the available information.

## Development of Chronology

In order to piece together what happened and when, the investigator will start developing a chronology. Included in the analysis should be the following components:

1. **Evaluation** (content and context): This is crucial for understanding the subject's motivations, possibilities, and skills; it needs to be presented in a way that laypeople can grasp.
2. **Exploration**: Conduct thorough investigation using a variety of tools and methodologies.
3. **Integrating and correlating data**: In many cases, many pieces of evidence must be combined to provide relevant leads, as individual pieces of evidence may not always be enough to solve the crime. It is critical to lay out the timeline and show how different pieces of information relate to one another.
4. **Confirmation**: Follow the best evidence rule standards and confirm the analysis's results to make sure they may be accepted and used in court.
5. Real proof must meet certain standards.
6. Make sure to document the analytical procedure thoroughly.

Part 4: Analyse What Happened: Applying the established criteria and previously established facts, reassemble the events in a way that allows you to test the hypothesis. Reconfirm the findings of the analysis.

The fifth step is to keep track of everything you do while you do the analysis.

Record findings and include evidence from the analytical sub-phase to ensure evidence chain and custody.

A case file containing the case information, a log file including every analysis operations, and any relevant CDE will be created by the data analysis program. Getting paperwork and CDE safe is step six. Always be sure to back up your case file and keep it in a secure location. This includes all of the related CDE and analytic tools.

Step 4 of the sub-phase is to restore the service.

Return to the usual practice first. Work together with the company's interruption team to quickly restore operations to minimize interruptions.

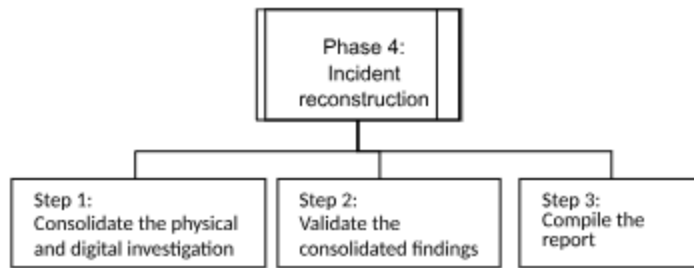


Figure 7-9 Phase 4 ReDF protocol 5

Give any conclusions together with the CDE that supports them so that the investigation procedure and findings are clearly visible. Add up all of the actions and methods that were employed to locate crucial evidence and to confiscate, gather, store, retrieve, and rebuild.

### ReDF Presentation of findings phase.

There are four steps in this stage. To provide for an appeals procedure, we have extended the procedures by adding a third phase. The ReDF methodology's phase five is shown in Figure 7-10.

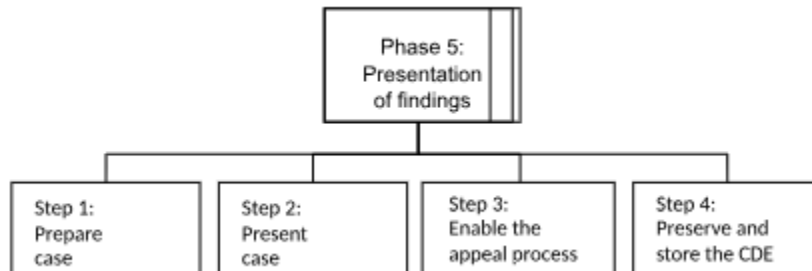


Figure 7.10 Phase 5 of ReDF

#### Step 1: Prepare the case

Before you start putting up an appearance, decide who your audience of choice is. Various tools and software should be employed in order to provide a presentation that is relevant for the intended audience. Prepare all of the artifacts and gather all the proof required for the presentation. Prepare the expert witness if their testimony is needed to provide evidence. During this phase, keep the chain of ownership intact at all instances.

#### Step 2: Present the case

Communicate the results to a variety of groups, including technical staff, managing risks, legal representatives, direction, and data safety, using the proper format. Display the proof in a rational way to show its importance to the argument. To help understand complicated concepts, provide visual or physically representations. Additionally, make sure a DF professional is on hand to assist in providing expert testimony.

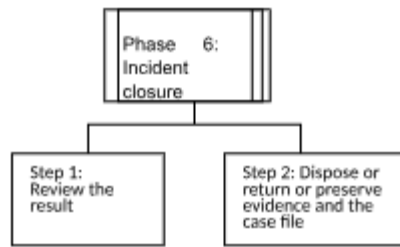


Figure 7.11 Phase 6 ReDF protocol 6

Examine the results to discover areas for improvement. As a result, new or revised policies or processes, as well as extra training, may be implemented.

The record of the case and accompanying evidence should be processed and saved for future reference. Regulatory restrictions, such as the amount of time required for keeping proof, must be taken into account while creating a post-investigation proof management strategy.

The outlined stages and processes can be seen as a sequential progression of events, however so as to end up at a more comprehensive research conclusion, it might be required to go back and complete some earlier steps in need to gather additional proof or conduct extra data analysis. The result of one stage, however, will be utilized as input towards the following phase. Organizations must take the following actions:

- Using the specified ReDF methodology, manage and carry out the reactive DF investigation. To guarantee a successful inquiry, follow all of the rules and regulations outlined in the ReDF process.
- Determine legal and judicial criteria for the particular situation.

## Live Forensic of Real-time Evidence

The demand for real-time evidence is on the rise, driven by the limitations of conventional digital forensics investigation methods, tools, and techniques, which struggle to handle the dynamic and volatile nature of such evidence.

A company's security system for intrusion detection is crucial to identifying incidents since it sets off an emergency reaction procedure. However, in order to guarantee the availability of relevant and legally acceptable live digital proof, should it be required for investigations, it is becoming more and more important to smoothly combine live forensic analysis procedures with the IR methodology. The vital components of proof verification, gathering, and live data retention are frequently missed by the conventional IR techniques.

Conventional a digital forensic analysis techniques are good at making sure the obtained material and proof don't change. On the other hand, software tools used by live investigators invariably contribute modifications to the information during gathering. Forensic criteria must be followed while documenting the live investigative procedure to preserve the chain of custody and ensure that the proof gathered is acceptable in a court.

These days, virtual forensic archiving and acquisition systems like EnCase® Enterprise Edition and ProDiscover® are used for live forensic investigations. These instruments make use of

programs and live methods of analysis that are already installed on the system during the time period being examined. The goal of virtual forensic investigations is to modify conventional criminal investigation procedures for use in real-world operating settings.

In order to integrate these approaches into the Proactive Virtual Forensics framework, we have investigated modern approaches for live, isolated, and actual time virtual investigations in the course of our study.

ActDF involves the collection of relevant live digital evidence, including volatile data, within a active system or producing environment using proper tools.

**Active DF is the ability of an organisation to gather (identify, collect and preserve) Comprehensive Digital Evidence in a live environment to facilitate a successful investigation.**

- Efficiently gather pertinent live digital evidence, including volatile data, in a live system or production environment, utilizing suitable tools and technologies.
- Minimize the impact of an ongoing incident.
- Establish a meaningful starting point for reactive investigations within the organization's risk management framework.

These aims serve as the foundation for the efficient gathering of active proof, and our ActDF procedure is made to support and conform to these objectives. We have suggested four stages and corresponding actions for the ActDF procedure in Chapter 6:

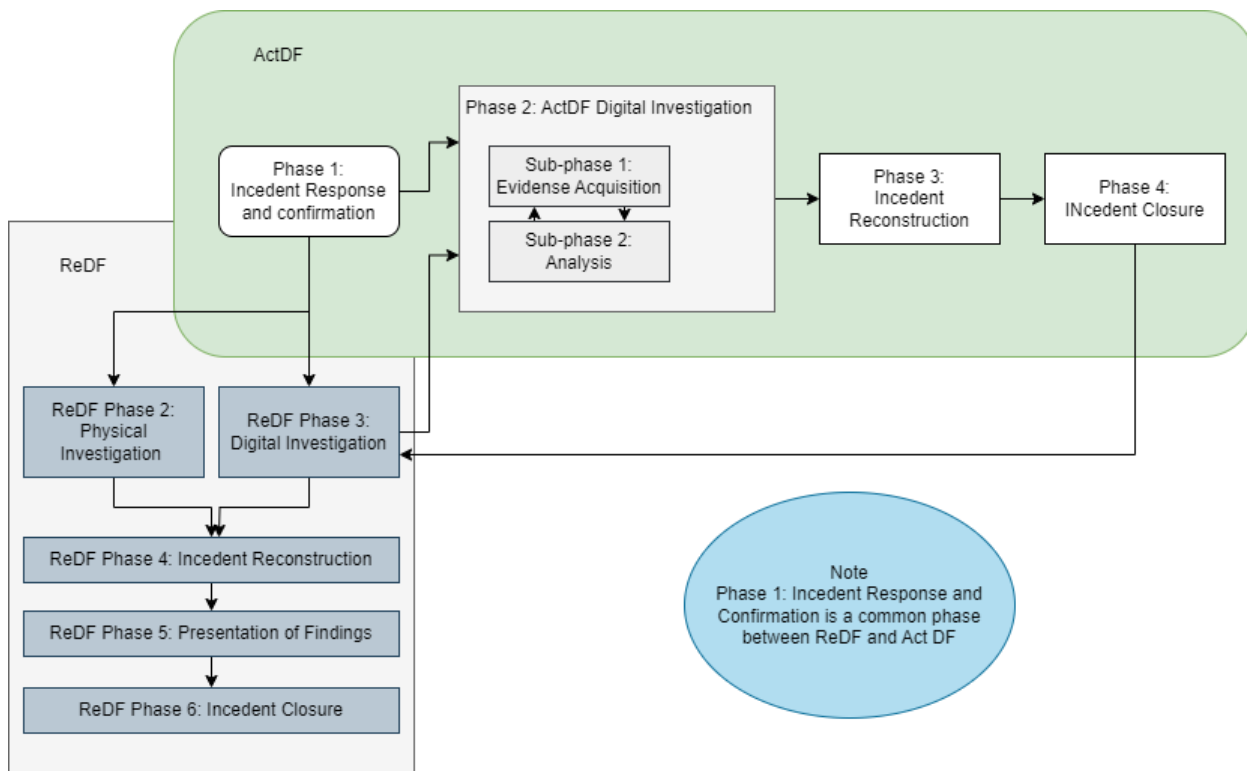


Figure 7.12 Visuals of ActDF method

## ActDF Phase 1: Phase of event reaction and verification

In Chapter 6 we identified two phases. ReDF and ActDF procedures have the same incident reaction and confirmation phases. It is critical, however, to integrate ActDF-specific criteria in the separate phases. For phase 1 of the ReDF procedure, we employed the same eight phases.

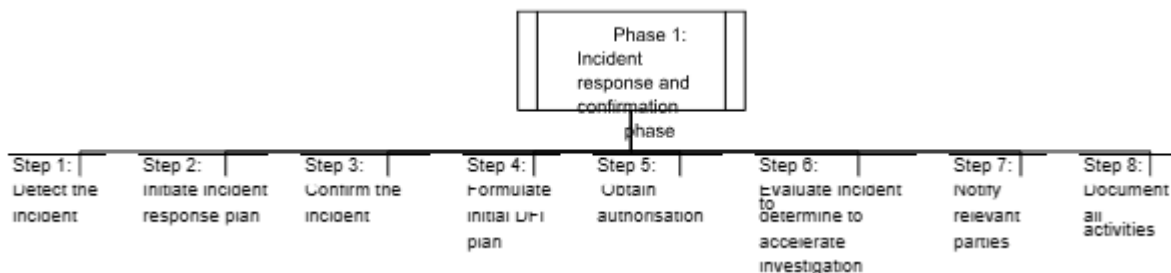
The IDS will spot questionable activity and notify the relevant person of a potential problem. Certain event alerts will initiate an event that activates the ActDF component as soon as the occurrence is detected, in order to get the required live evidence.

Notify the CERT and get valid internal and/or outside authorization to carry out further research. In order to respond to and confine the specific event and reduce its impact, activate an emergency response strategy and a plan to contain it. In accordance with the policy, let the occurrence continue but confine it to a specific location to lessen its effects. Reducing the incident's negative effects on current operations and infrastructures is the aim.

Economic, legal, scientific, and social objectives and considerations must be included into the plan of containment and IRP. At all times, detectives need to preserve the chain of possession and adhere to appropriate forensic procedures.

Once the occurrence has been identified, we must determine the value. The occurrence must be validated, assessed for possible harm or impact, and confirmed by the organization. It is necessary to decide whether to conduct an investigation. The relevance and character of the research must be determined.

During this phase of the ActDF component, investigators embark on the creation of a comprehensive investigative strategy. We propose the development of an ActDF Investigation (ActDFI) plan, a pivotal step in orchestrating all available resources for live investigations (Section 5.5.1.7). Additionally, the plan recognizes that when internal



resources are insufficient, certain parts of the investigation or the entire process may need to be outsourced.

The IRP and control strategy must take into account goals and factors related to the

economy, law, science, and society. Investigators must always follow the proper forensic protocols and maintain the chain of ownership.

Furthermore, researchers need to make critical decisions regarding the target machine's power status (whether it is turned on or off), the chosen investigation mode (whether to conduct it overtly or covertly), the need for target machine isolation or security measures, and, finally, the method for acquiring evidence, whether through local or remote means.

## ActDF Phase 2: ActDF inquiry stage

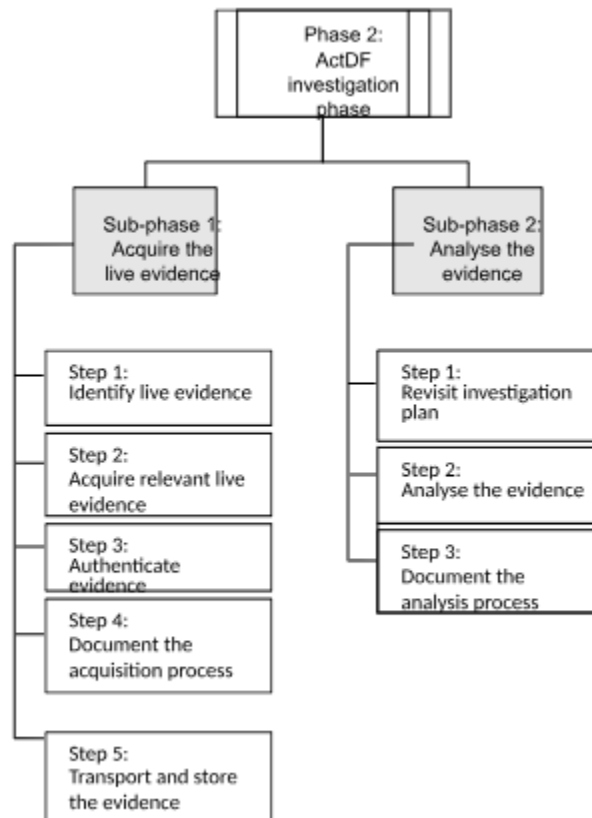


Figure 7.4 Phase 2 *Minimize User Involvement 7*

To find out which live proof has to be collected in order to examine the incident, consult the threat evaluation and digital evidence index. What evidence is acquired will depend on the nature of the incident. Think about the sensitivity and volatility of the evidence. It is important to take into account additional volatile evidence relevant to the system, specifically induced unexpected information, and temporal constraints placed on stable information.

The proof's discovery will depend on the type of operating system. Determine the boundaries of the intended live collecting method, the approximate time needed for the procedure to finish, the position of the goal device, and perhaps the operation will affect any other distant equipment.

### **Acquire relevant live evidence**

Obtain real-time evidence by employing suitable tools, technologies, or



applications essential for attacker profiling and evidence acquisition. An essential aspect is the automation of these evidence collection tools, technologies, or applications, ensuring they are promptly activated—either upon the issuance of an incident alert or initiation triggered by an event.

Adhere to an accepted live proof gaining methods, following the information gaining baseline:

1. **Minimize User Intervention:** Keep user involvement to a minimum, ensuring that the collection process is as unobtrusive as possible.
2. **Necessity and Non-intrusiveness:** Ensure that every action performed is necessary for the investigation and as non-intrusive as feasible.
3. **Minimal Modification:** Limit modifications to static digital evidence, making sure that any alterations are kept to a minimum.
4. **Ordering of Instability and Importance:** Comply with the uncertainty hierarchy and give the gathering of digital proof the highest importance based on its importance.
5. **Conventional Proof for Non-Priority or Variable Data:** Use conventional techniques for gathering evidence when working with non-priority or volatile information.
6. **Copy or Extract Data with Minimal Impact:** Only conduct data copying or extraction when it has no effect on the original data and its timestamp.

**Authenticate evidence**

Since live proof is dynamic, it is essential to utilize a cryptographic technique as soon as possible to preserve and validate all the information gathered. Make a forensic duplicate of the gathered data prior to beginning any examination.

When gathering live proof, record every action to guarantee the accuracy of all the proof and procedures. When the evidence is collected, move it and, if needed, store it in a safe place. In order to demonstrate the validity of the data and methodology, it is imperative that all actions made throughout the process of collecting data are documented. The documentation will display the custody and evidence path.

**ActDF Phase 3: Phase of restricted event rebuilding**

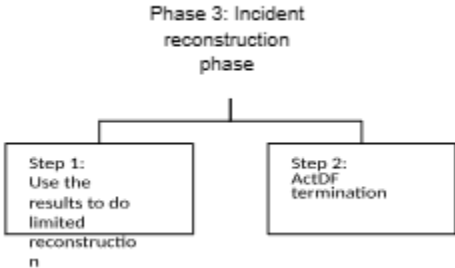


Figure 7.15 Phase 3 ActDF Method

Step 1: Create a condensed restoration of the event using the analysis step's findings.

Determining if the necessary missing or live proof has been gathered is the aim. Determining whether or when the ReDF requirements have been met is essential. The ActDF investigation phase must be continued in order to gather more live proof if more is needed.

Whether the research may proceed depends on a number of factors. For instance, the company's risk management system may indicate if the expense or effect on business operations are excessively high.

Step 2: ActDF termination

Determine whether or not the ActDF protocol should be terminated. The Risk Management Framework will dictate the termination circumstances, such as cost being too high; sufficient CDE; and the impact of continuing acquisition being reviewed. If live proof is still absent, repeat phase 2.

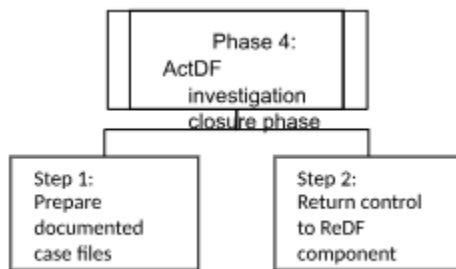


Figure 7.16 Phase 4 ActDF method 8

## To-do list

Organizations must take the following actions:

1. Coordinate and complete an ongoing or live DF inquiry using the prescribed ActDF process. Adhere to every rule and regulation specified in the ActDF approach to ensure an effective investigation.
2. Establish the legal standards applicable to the specific circumstance.

The preceding explanation has revealed some interplay between the three parts of our CDF capability. The connection between the components will be discussed briefly in the next section.

The interdependence of ProDF, ReDF, and ActDF becomes evident when considering their respective definitions and objectives. ProDF serves as the foundational component, equipping organizations with the necessary tools and technologies for the effective application of digital forensics. ActDF and ReDF rely on dependable patterns being available, established digital forensics investigation methods (both proactive and reactive), related rules and procedures, competent analysts and staff, and excellent and easily available Cyber Digital Evidence. The ProDF component's output, the accessibility of appropriate devices, technologies, and structures, is essential to the continued existence of the whole digital investigation environment.

In real time proof becomes essential in the event reaction and confirmation phase as well as the digital inquiry phase, especially when it comes to the ReDF component's proof collecting. On the other hand, ActDF is in charge of locating, obtaining, analyzing, and preparing live evidence so that the ReDF component of the thorough investigation process may use it. These results highlight how the many parts of our Cyber Digital Forensics expertise are interrelated.

A high-level visual illustration of the interactions between all three parts is shown in Figure 7-17, which reinforces their complimentary character.

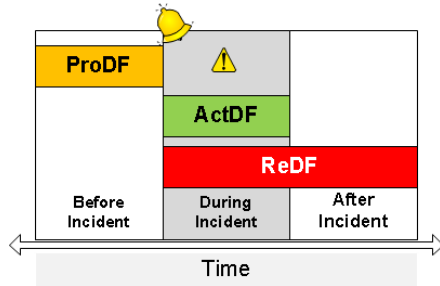


Figure 7.17 Relationship between components

These procedures offer succinct guidelines for the stages and actions that companies need to take in the event that a problem is discovered and has to be thoroughly investigated.

## **CHAPTER 8: Building a Quantified Data Managerial Architecture**

In the forthcoming chapter, we will leverage the task list as a foundational resource to propose a comprehensive Digital Forensics (DF) framework for the implementation and management of the Cyber Digital Forensics (CDF) capability. This framework will be designed to ensure the efficient and effective integration of the CDF capability into the organization's operations, addressing all critical aspects including policies, strategies, processes, training, technology, and infrastructure.

The previous chapter has established our Cyber Digital Forensics (CDF) capability, comprising distinct yet interdependent components. For organizations seeking to implement this capability, a structured approach is crucial.

The ReDF and ActDF elements serve as the fundamental investigative components, providing researchers with well-defined processes for event handling. Organizations must, however, set up policies, processes, training courses, and guarantee that the required infrastructure, technologies, and tools are available in order to be ready for the implementation of these protocols.

In contrast, the ProDF component provides firms with assistance on how to set up organizational structures, create policies and procedures, set up infrastructure, and use technology and tools while taking regulatory and legal constraints into account. The fact that these tasks frequently depend on each other makes an organized to-do list essential. The proof of identity, formulation, and execution of the required tasks are made easier by this organized list.

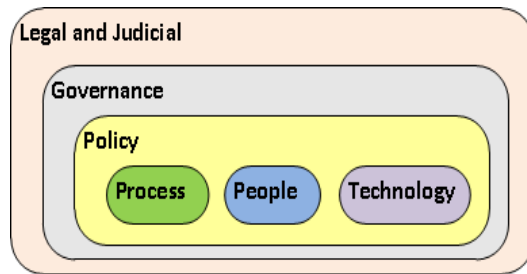
All actions inside the business are supported by its legal circumstances, and procedures, rules, and procedures are shaped by the creation of policies, which is fueled by organizational and managerial architectures. The efficient management of digital forensics technology and tools depends on the professional use of appropriate tools and technologies by experienced and competent individuals.

Although the to-do list provides a general outline, it does not specify legal or judicial requirements or specify the exact tactics, guidelines, or protocols that must be developed. None of the Digital Forensics frameworks that have been mentioned before provide the precise components required to create a CDF capability. The next stage is to determine the precise deliverables that companies need to implement by using the tasks on the agenda. The outputs are observable results that businesses may use, such training courses, rules, and processes. These items will be grouped according to the DF parameters, and they will serve as the cornerstone of our high-level scheme for DF execution and oversight.

### **CATEGORIZE THE AGENDA**

The basis for classifying certain activities and results will be the six main elements of our framework: legal and judicial, leadership and management, regulations, procedure, people, and tech.

The legal and administrative aspect provides the overall framework for all other parameters, which are interwoven and reliant on one another. A country's or a business context's regulatory, legal, and administrative constraints have an impact on all aspects of a company's operations.



The legal and administrative framework surrounds the management dimension, which is further enhanced by the policy dimension. The aspects of people, procedure, and technology are subordinate to the policy. The use of our structure in a work environment is characterized by a continuous interaction of individuals, procedures, and tech.

The relationships between these dimensions underpin the structure of deliverable categories. The graphical representation in Figure 8-2 visualizes these relationships.

To facilitate the development of our Digital Forensics Management Framework (DFMF), we have systematically categorized and reordered the specific actions outlined in Section 7.7 (Table 7.2). The operation amount and the "i" match. In the upcoming table, possible outputs that are essential for execution will be bolded.

To establish precise objectives for using our CDF abilities, we will make use of the items on the list of things to do. Hierarchical organization of the activities is another option. For example, the main DF policy is supported by many sub-policies, such as those concerning training and teaching, incident management and utilizing, and proof administration and processing. First level actions will be used to describe the fundamental DF policy, and subsequent actions will be used to describe the auxiliary sub-policies.

Although it is not covered in this thesis, the development of a fully functional DFMF will be looked at and worked on in the future.

In order to create our DFMF, we will evaluate the list of due activities to determine specific deliverables. The construction will be done in phases, starting with the judicial and legal aspects and moving on to governance, policy, process, personnel, and technology. The legal and administrative elements will be examined in the part that follows.

The legal and administrative concerns component makes sure that companies carefully determine and follow the relevant legal, regulatory, and administrative obligations that are unique to their business. We have defined legal and administrative objectives within this category, as shown.

1. This group includes the criteria for both tangible and post-investigation evidence, as well as the thorough requirements for digital proof, encompassing static, operate, and historical data.
2. The complex components of the investigative process—in particular, incident handling and the creation of Standard Operating Procedures in organizations—are covered in this area. It is important to make sure that the ReDF, ActDF, and SOP procedures are followed, mainly because this affects the legality of proof in a court of law.
3. The legislative and judicial requirements for a strong operative and investigation framework are the main topic of this section. It also emphasizes how crucial it is to confirm that digital forensics

technologies and tools are appropriate in order to guarantee the legality of collected evidence in court.

- This category includes a variety of standards, including those set forth by the South African Qualifications Authority concerning personnel certification and program accreditation. The acceptance of proof in a court of law is also significantly influenced by the technical proficiency of the investigators.

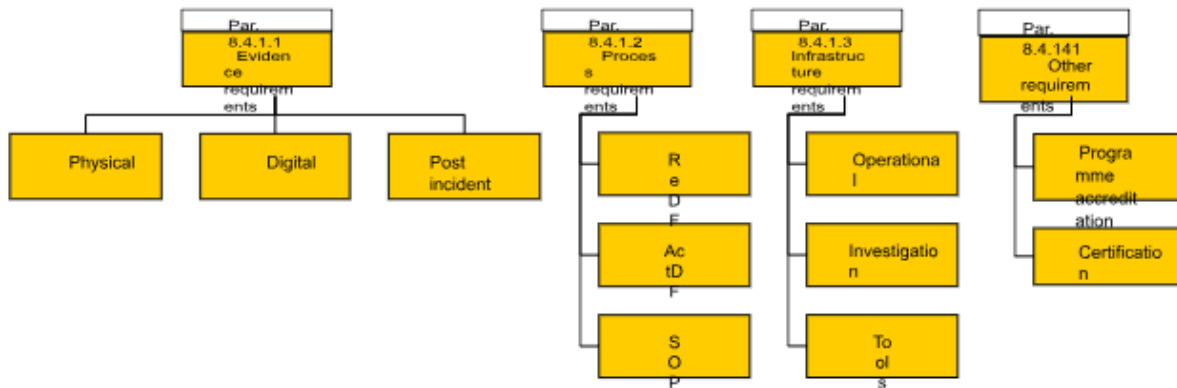


Figure first two levels of the legal and administrative deliverables

To find these legal and administrative criteria, organizations need to carefully examine a number of sources, including statutes, agreements, standards of excellence, regulating instructions, administrative conditions, and other regulatory agencies like certification authority. In cases where organizations operate internationally, compliance with the diverse legal and judicial requirements of different countries becomes imperative.

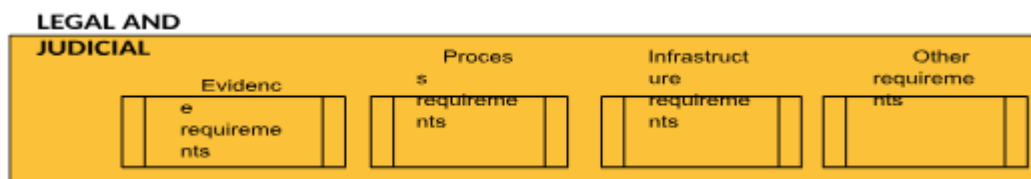


Figure 8.4 the initial step in constructing our Digital Forensics Management Framework 9

The subsequent step involves the consolidation of the governance dimension.

Within the governance dimension, the focus shifts to the management aspects, ensuring that organizations holistically address the importance and effective maintenance of Digital Forensics (DF) within their operations. Our approach involves identifying three distinct groups of deliverables:

- The DF strategy plays a pivotal role in providing a clear direction for the utilization and integration of DF within an organization. It addresses three critical groups of activities:
  - Management of the Cyber Digital Forensics ability
  - Efficient management of DF inquiries

2. Establish an Evidence Management Plan (G2): This component emphasizes the importance of having a well-defined plan for managing evidence effectively.
3. Create an approach for DF outreach, instruction, and knowledge(G4): In this category, the focus is on creating a comprehensive strategy that includes supportive policies and programs for educating, training, and raising awareness regarding Digital Forensics.

## Strengthening the Disaster Preparedness and Risk Management framework:

When it comes to risk management and backup plans, the governance component is just as influential. To properly manage risks and prepare for emergencies, it is necessary to include DF needs. To do this, it is necessary to include evidence and process needs into the organization's risk management and backup plans. Plans from organizations may include elements like company impact evaluations, incident handling strategies, continuity of operations plans, and catastrophe restoration plans. Forensic investigations are another area that this group takes into account when evaluating the effects of new technology in risk assessment.

1. Manage Infrastructure (G1): This area deals with the administration of the operating infrastructure, which includes hardware and software, as well as the investigative lab.

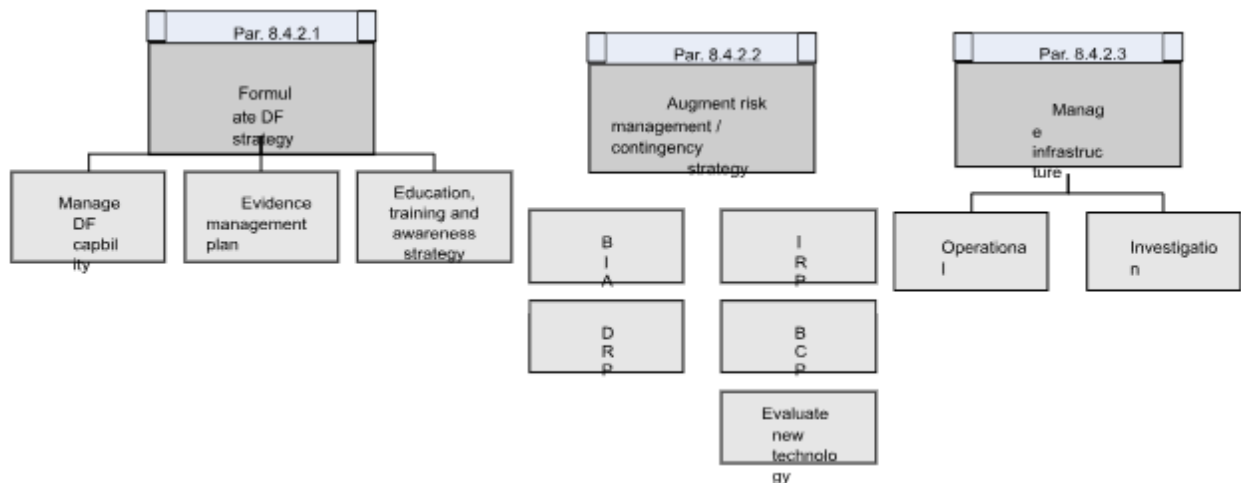


Figure 8.5 typical deliverables within the governance category. 10

The legal and administrative dimensions are closely linked to the governance component. The current Digital Forensics Management Framework will be integrated with the first tier of oversight output groups, as depicted in Figure 8-6.

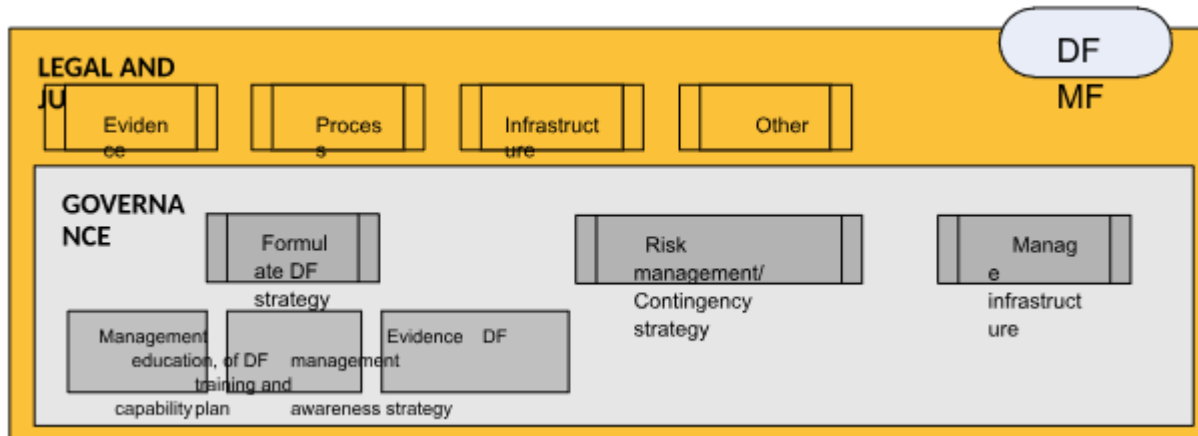


Figure 8-6 Digital Forensics Management Framework (DFMF) 11

The subsequent step in our framework construction involves consolidating the policy dimension.

### Policies

1. Policy for managing incidents (written by the author)
  - Give standards for the various types of occurrences and parameters for whether or to what extent (internal or formal) an investigation should be conducted. Incorporate investigation and occasion spending control.
2. ReDF inquiry policy and associated policies
  - IR regulations. Assist the company's IR policy for physically inquiries to incorporate the ActDF activating requirements.
  - Guidelines for case presenting are provided by the case presenting policy.
  - Guidelines for ending a case and the dissemination of inquiry findings are outlined in the case closing rule.
3. ActDF inquiry policy will now incorporate:
  - IR guidelines. Incorporate the company's IR policy with the ActDF activation criteria.
  - This regulation is derived from the company's ActDF termination standards, live proof collecting, analysis, and restricted rebuilding emergency plans. ActDF ending its policies.

### Improve organizational risk administration and contingency planning.

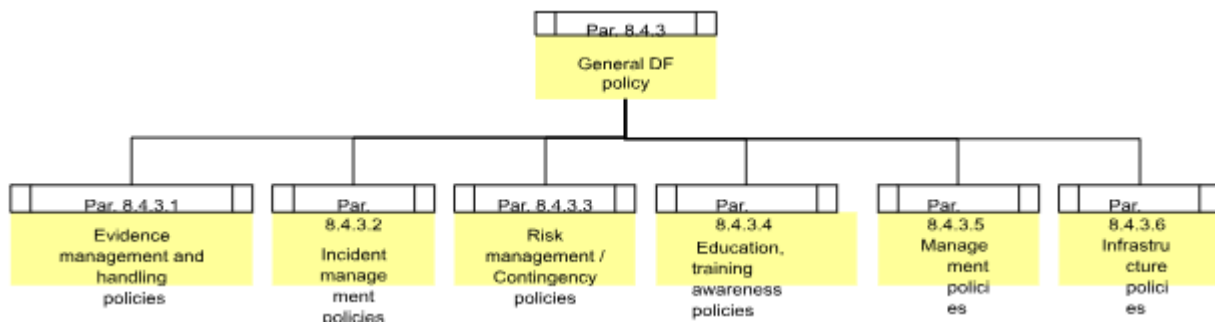
Add DF requirements to the organization's risk administration and contingency procedures. Typical policies include:

1. Change the danger profile to a risk assessment of the business impact analysis policy.
2. IR rules ActDF and ReDF's IR rules ought to align with this rule. To limit accidents and lessen their impact on the company, a prevention policy is essential and must be in place. Incorporate incident speed parameters within the guidelines.
3. Procedures for company continuity and catastrophe restoration.
4. Policy for instruction, instruction, and knowledge
5. Architecture policies
  - Network, detection of intrusions, and other architecture configuration



- A surveillance policy that delineates precise protocols for methodical evidence gathering and targeted monitoring.
  - A policy that ensures that DF concepts are integrated into the app and system planning, execution, and development life cycle (SDLC) to produce systems that are favourable to DF.
  - Anti-forensic activity prevention policy
  - Anonymous action prohibition policy
  - New technology and process evaluation policy.
6. DF laboratory policies
- Plan for acquiring and maintaining DF technologies and instruments
  - Guidelines for controlling lab access.
  - Guidelines for Using DF Labs
  - Regulation of safe storage spaces
  - Guidelines for backups
  - Verify that the DF lab has established policies and a defined backup and recovery plan. It is crucial to consider the tools and tool versions in addition to the proof, which consists of information and data.

Figure 8-7 below depicts the first two levels of policy deliverables graphically.



One aspect of political leadership is policies. The initial phase of policy outputs will be incorporated into the current DFMF version. We include the additional layer of policy execution categories because we believe policies are essential (below):

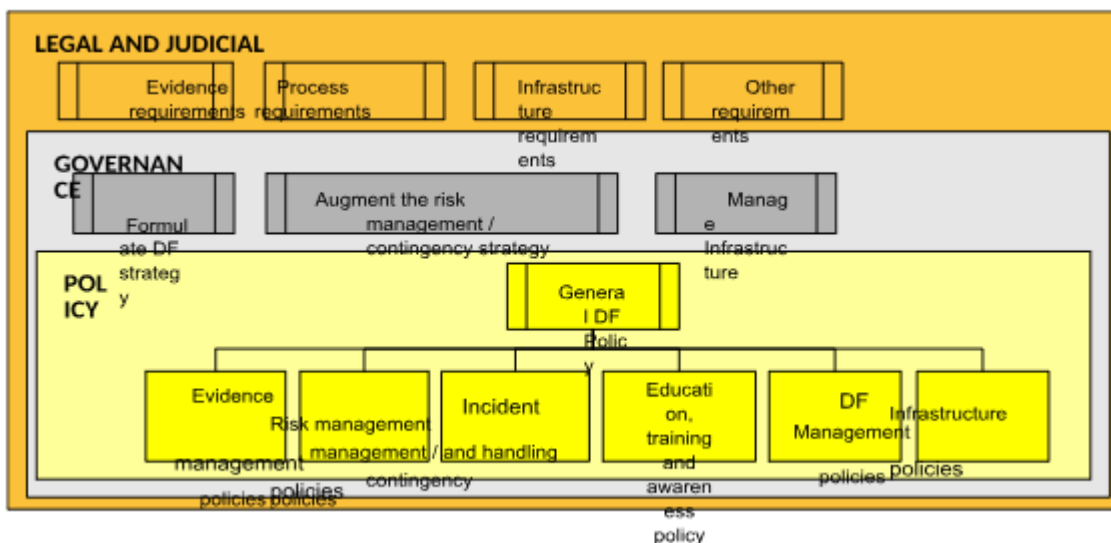


Figure 8.8 construction of our DFMF 12

## Process dimension

A company's internal DF control needs to be based on legally solid processes and concepts that are well established. The methodologies employed in a study or assessment will ultimately impact the acceptance of the information acquired and the probe's effectiveness. To supplement the relevant policy delivery kinds, we suggest the following list of six sets of procedural outcomes:

### Group 1: Rules for managing and processing proof

1. Protocols for managing evidence
  - Procedure for giving directions on how to build the proof list, compute the CDE score or a proof set associated with a risk, and generate and manage the threat profile.
2. Rules for processing digital evidence
  - Handling of static digital evidence
    - Stationary proof management procedures should include identification, gathering, acquiring, guaranteeing integrity, authenticating, conserving, storing, and transporting digital proof.
  - Protocols for handling live evidence
    - The live evidence handling processes are as follows: recognition; collection (which must be done according to the sequence of volatility); evidence integrity management; live proof purchase; live evidence authentication; live proof transport; and actual proof storage (which is done in the same manner as static evidence).
  - Protocol for handling archival material
3. Procedures for managing physical evidence:
  - Physical proof handling procedures include proof of identity, collecting (search and gather), documentation, storage, and transport.
4. Case records and proof handling and management processes following an investigation:
  - Any proof should be disposed of, returned, and archived in accordance with the protocols. Include case file and evidence presentation, storage, and transportation. Consider the legal implications of evidence storage.

### Group 2: Incident-management procedures

Organizations must establish extensive DFI processes for ActDF and ReDF that follow to acknowledged investigative best practices, including documentation and reporting requirements. The ReDF and ActDF comprehensive procedures were presented in Chapter 7. Procedures and guidelines will be used to support the protocols. we identified the following process deliverables:

1. ReDF procedures
  - we developed a ReDF study process with stages and steps. The following are typical ReDF procedures and guidelines that would go along with the ReDF investigative protocol:
  - Procedures for incident identification and confirmation (from contingency planning - IRP)

- The incident detection, containment, investigation acceleration, notification of the investigation processes, incident confirmation and authorization, internal and external authorization, This method, or a number of processes, should comprise the setting up of the ActDF element to gather live proof, event alert, and investigative process.
- There are auxiliary activities that go along with the physical investigation approach. Gathering and examining physical evidence is a common procedure, as is protecting the actual crime scene.
- There are supporting activities in addition to the digital investigative method. Add procedures for preserving digital crime scenes, gathering and analyzing evidence, and restoring services.
- Reconstruction process for an occurrence.
- How things are presented.

## 2. ActDF processes

we presented an ActDF investigation procedure with stages and related steps. The following are examples of typical protocol deliverables:

- Protocol for identifying and verifying incidents while protecting the ongoing inquiry and containment process at the crime site
- ActDF investigation procedures that use actual evidence collection and evaluation methods as well as a limited event recreation methodology
- The ActDF investigative procedure has been terminated.
- 

Group 3: Enhanced emergency planning and risk management To handle forensic evidence and procedure demands, it is imperative that the company's current emergency processes—such as risk administration and data security—be enhanced and modified. Take into account the procedures or rules listed below:

1. IR processes
2. These processes should be the same as the ActDF and ReDF detecting and proof procedures. strategies for recovering from disasters
3. Protocols for company continuity
4. Add a method for assessing novel technology.
5. Determine the risk element in the investigative scenario.

Group 4: DF Management procedures

1. Protocols for general DF administration
  - Fundamental methods of management, such whether and how to hire out DF services, should be supported by procedures and policies.
  - Process for reporting violations through leaks use DF strategies to safeguard the company's assets
  - Determine the probe's cost and ensure that it is appropriate for the investigations extent..
2. The control over the application of DF for non-forensic operations are:
  - Technique and suggestions for DF integration into processes and systems
  - Incorporate the DF process, proof requirements, and other organizational aspects when creating business processes. Modify the standard operating protocols of critical business processes for conformity reporting, inspections of quality,

handling changes, and other purposes. Additionally, ensure that a method for gauging the effectiveness and effectiveness of safeguards within frameworks is there.

- Approach to the non-investigative application of technology and techniques from DF Provide instructions on how to use DF tools for tasks like disc cleaning, password recovery, and information restoration.
- Method for utilizing DF instruments and protocols to safeguard the business's resources
- How to use DF to gather proof for continuing audits and quality control.

Group 5: Infrastructure procedures

The responsible utilization of DF tools is paramount, given their potential for misuse. Consequently, the establishment of precise protocols and guidelines is imperative to govern their usage, as delineated in applicable sections.

For organizations harboring an internal DF team, the provision of a dedicated DF laboratory is crucial. Within this laboratory, meticulous access regulations and procedural controls must be instituted to oversee activities. Additionally, measures for data backup pertaining to proof and associated technology must be rigorously enforced.

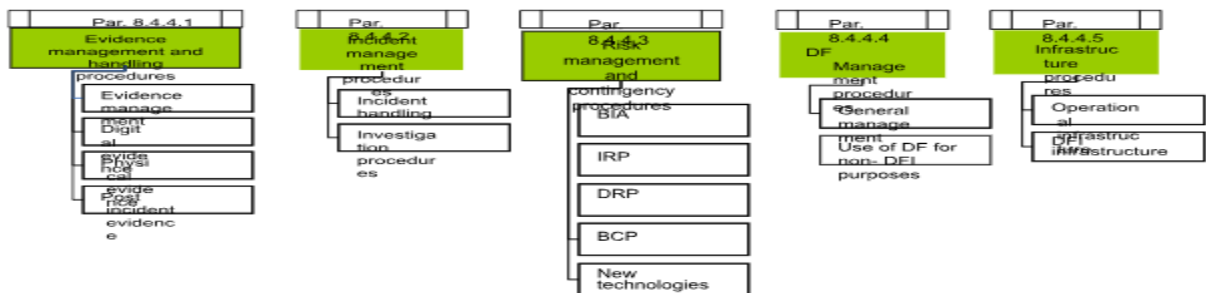
It is crucial to guarantee that evidence generated using DF tools and procedures is admissible in a court of law. As such, a concerted effort is needed to ensure that courts and the legal system appropriately acknowledge the chosen instruments as forensically reliable. The acquisition of DF tools and approaches should be governed by clear guidelines that prioritize the adoption of ActDF products and technologies that are recognized as having constitutional validity in court. Physical investigations, for instance, should involve the deployment of specific equipment such as evidence containment units, cameras, and meticulously maintained records.

Group 6: Inquiry laboratory procedure

The physical laboratory method will involve the following steps: procedures for setting up and managing the actual investigation equipment.

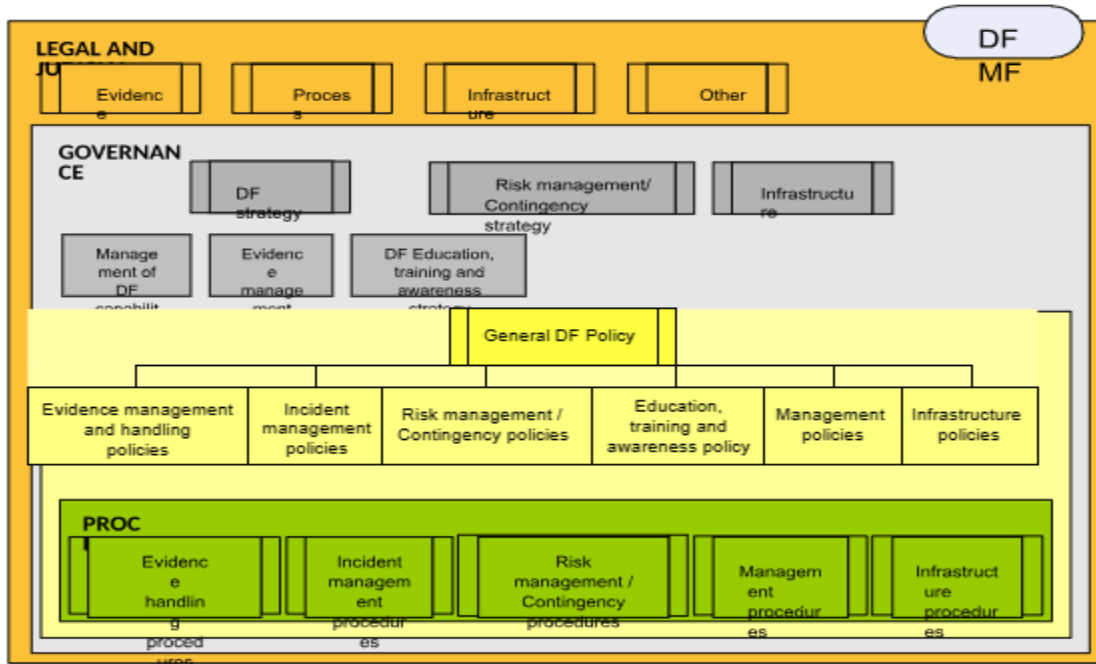
- a clear backup and restoration plan for the strength room and DFI lab.
- A backup strategy should incorporate tools, case proof, and proof
- As well as a process for DF tool acquiring it, availability, control of versions, and maintenance.

Figure 8-9 depicts the first two layers of process deliverables graphically.



The strategy dimensions represents a portion of the procedure dimension. Figure 8-10 (below) now includes the process outputs from the present version of DFMF:

Figure 8.9 13



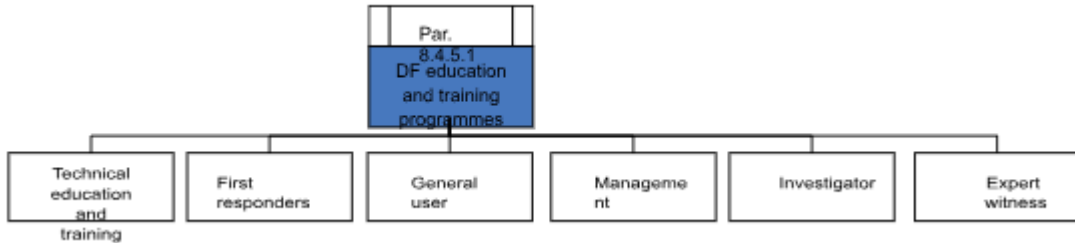
## People dimension

When it comes to managing people in a company, there is no category more unpredictable and risky than humans. Effective education and awareness programs have the potential to impact employee behaviour. Although not all employees may necessitate the same level of training, it is critical that all employees comprehend the purpose and use of DF. One goal of the governance is to make sure that DFs are well-informed and educated (par.7.3.1.6). Three distinct kinds of person deliverables have been identified:

1. It is imperative that groups to provide information, instruction, and educational programs. To address the varied functions within the organization, a number of training, awareness-raising, and education activities will be required. Training and education programs for first responders, general customers, managers, investigators, and expert witness preparations are typical examples.
2. A qualifying body, like SAQA, or another certifying body, such an En-Case® qualified investigator, must accredit internal training programs. This will ensure that the courts and the DF community's demands are met by the training. Since it is believed that a competent (certified) investigator have the requisite skills to carry out the investigation properly, courts would prefer to accept proof gathered by this type of investigator. Workers at different levels might be qualified to ensure successful criminal prosecutions and positive investigation results.

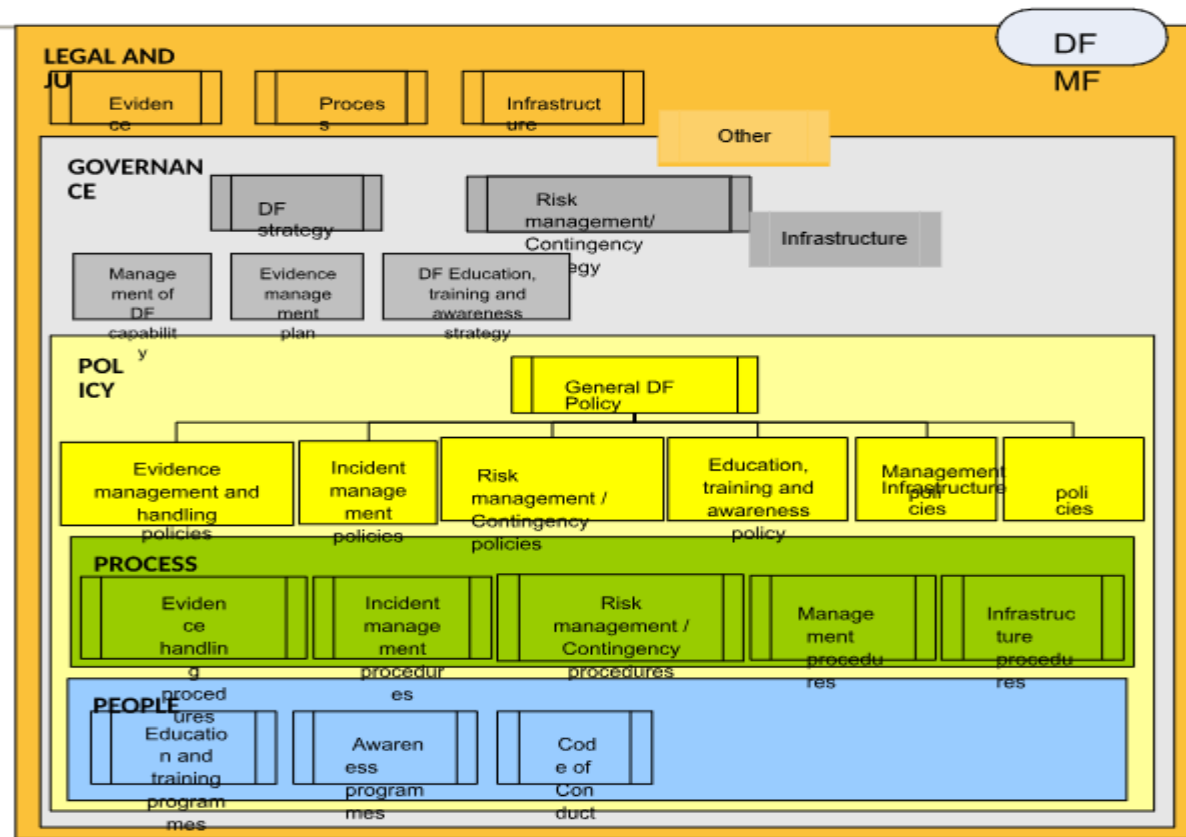
3. An investigation's outcome may be impacted by an expert witness's level of competence. Expert witnesses need to be ready for everything. The people deliverables are visually shown in Figure. A few examples of technical education courses are offered.

4. Upholding ethical values is crucial for the education and understanding plan to support the company's moral culture. Given the sensitivity of DF technology and machines, the firm must apply ethical DF



practices. Companies must create an ethical code for their utilization of DF assets and procedures.

Figure 8. the people deliverables 14



The policy aspect a sub part of the human parameters. In Figure 8-12 (below), we will now add those objectives to the existing version of DFMF:

## Technology dimension

In calculating the technical element, all requirements for operating facilities and DFI infrastructure will be included.

DFI tools and procedures are essential since not all collection and administration techniques are accepted in court. As a result, companies have to invest in case-management software to guarantee that all required documentation is centralized and can furnish the evidence and accountability required by the legal system. In order to convey the case, the investigator will also require presenting software. The technical deliverables are categorized as follows by us:

1. The operational apparatus a firewall should be set up.
2. Construct the ability to systematically collect evidence.
3. Construct the ability to keep track of actions.
4. Physical DF investigation (DFI) infrastructure. DFI-specific hardware, including a separate system, forensic PCs, and both temporary and permanent servers, must be readily available.
5. DFI tools and procedures are essential since not all collection and administration techniques are accepted in court. As a result, companies have to invest in case-management software to guarantee that all required documentation is centralized and can furnish the evidence and accountability required by the legal system. In order to convey the case, the detective will also require presenting software. The technical deliverables are categorized as follows by us.
6. A backup facility, networking devices, jump bags, and cameras are all instances of general equipment.
7. Software
  - Software for doing research, like EnCase® or Forensic Toolkit®, and software for analysing live evidence, like EnCase® Enterprise Legacy or earlier versions of the author's toolkits
  - Software for managing cases, also developed by the author
  - Software for creating presentations
  - Data backup software.
8. Things of several types Items like bags, gloves, and blank storage are essential for every investigation.

The initial two tiers of technical deliverables or specifications are illustrated in Figure 8-13 (below):

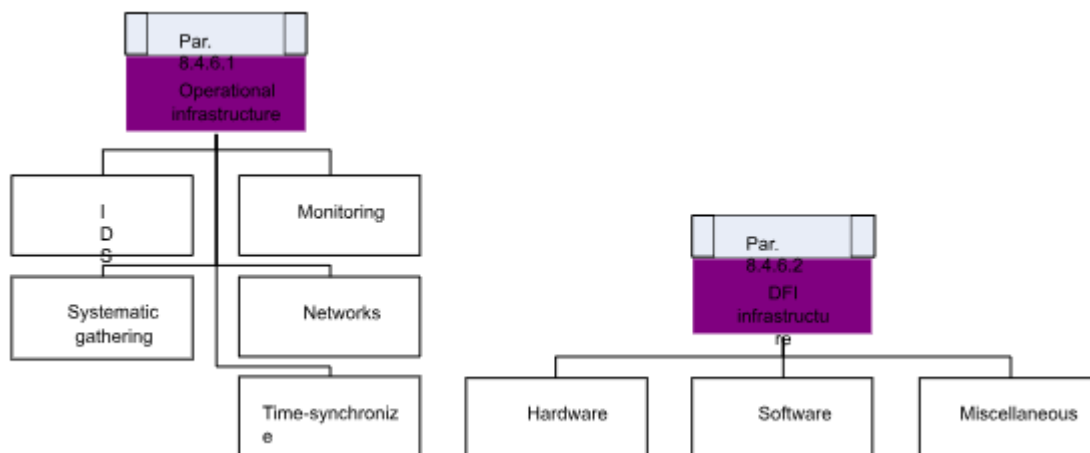


Figure 8-13 first two levels of the technology deliverables

A portion of the technical dimension is referred to as the policy dimension. The following technical dimension will be presented for the current DFMF construction in Figure 8-14 (below): other

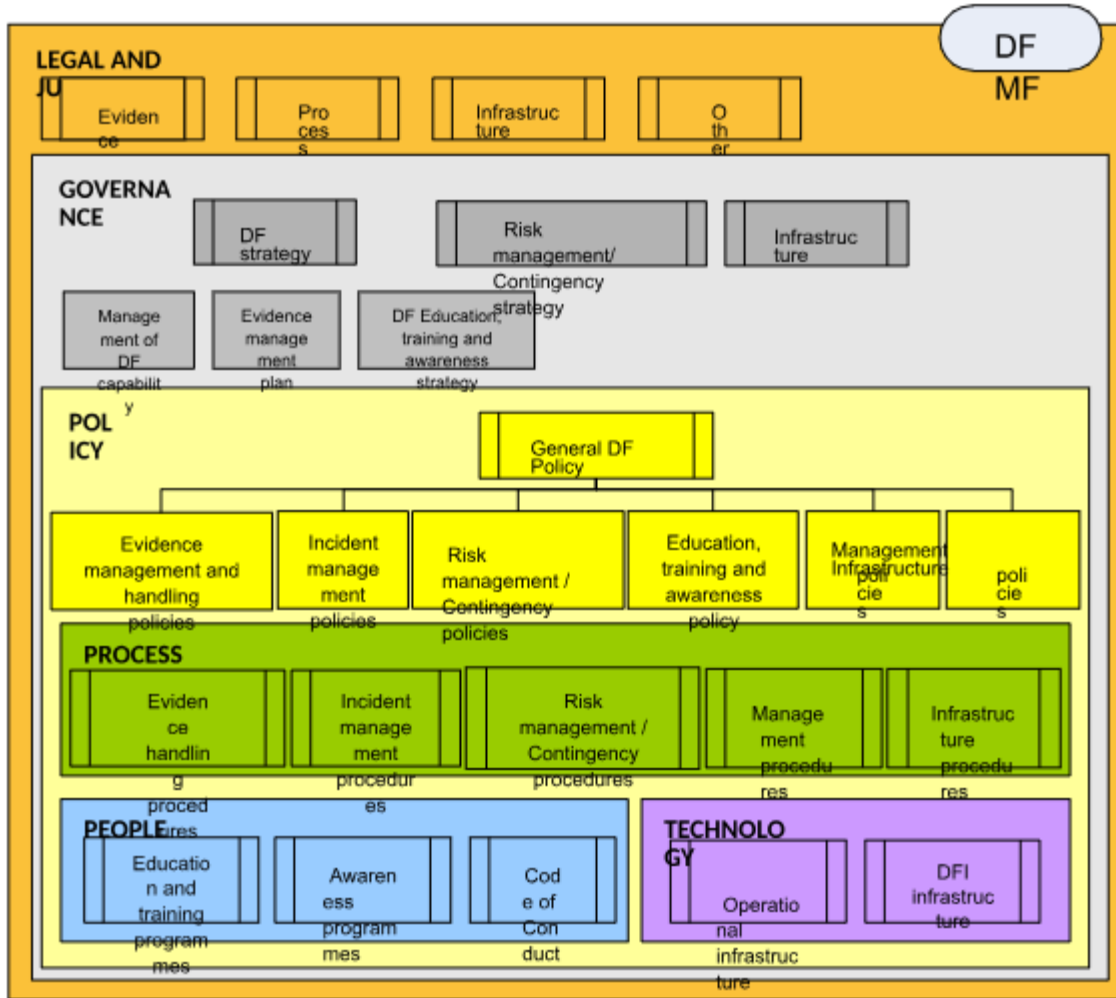


Figure 8.14 the construction of our DFMF

## A COMPLETE PERSPECTIVE OF OUR DFMF

We meticulously constructed the DF application and monitoring architecture, or DFMF, in the chapter's preceding part. Our DFMF currently consists of many delivery levels. There are a lot of significant relationships between deliverables in the fields of regulation and policy. The principal DF policy will serve as the organization's strategic guide for other auxiliary policies. The DF strategy, which outlines how the organization should use DF, will be supported by a DF capacity management plan, a proof management approach, and a DF awareness, method for education and instruction (Figure 8-5). In Figure 8-15, we have modified many output groups to ensure our DFMF is displayed beneath:



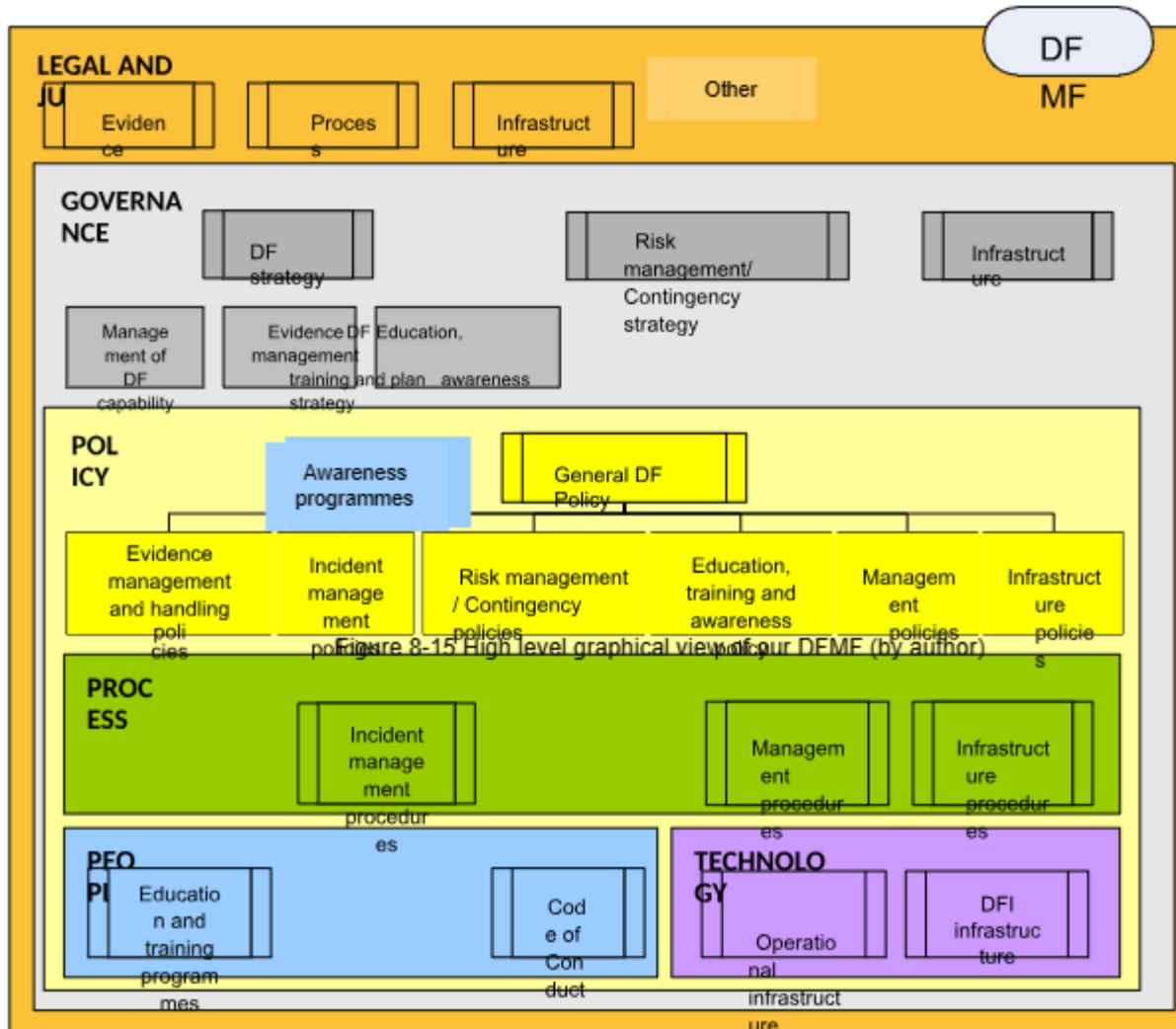


Figure 8.15 15

Management may utilize the framework to put a CDF capability into practice. Using the DFMF, the CDF capability may be developed by starting with the external legal and administrative aspects and working your way progressively inside. The framework encapsulates the interplay among the deliverables necessary for the effective implementation of the CDF.

# CHAPTER 9: CONCLUSION

## INTRODUCTION

The surge in virtual crime and fraud, coupled with corporate demands, necessitates substantial evidentiary support, known as 'Conclusive Digital Evidence' (CDE). Organizations increasingly require robust evidence for legal compliance and governance structure evaluation. Digital forensics (DF) is crucial for gathering compelling evidence, but challenges in preparation can hinder its benefits.

DF, traditionally reactive, systematically explores processes related to digital evidence retrieval, safeguarding, and scrutiny. Existing DF frameworks focus on preparatory aspects, often lacking specific guidelines for real-time evidence acquisition. Comprehensive Conclusive Digital Forensics (CDF) capability is essential, addressing preparation, live evidence acquisition, and reactive investigation.

Organizations face challenges in practical DF tool utilization, resulting in unsuccessful investigations due to inadequate evidence or contamination. Proper infrastructure configuration is necessary for effective DF application. The lack of holistic DF frameworks for implementation and management within organizations is evident in existing literature.

This thesis aims to fill this gap by developing a comprehensive Digital Forensics Management Framework (DFMF) for efficient implementation and management. The three main segments include:

1. Setting the Stage for Digital Forensics
2. Crafting the DFMF
3. The Way Forward and Conclusion.

The opening section of this dissertation delved deeply into the domain of Digital Forensics (DF), providing comprehensive definitions and a thoughtful exploration of its internal and external catalysts. The objective was to uncover the common motivations driving its application within organizational contexts. For instance, these tools are utilized to dissect cybercrimes and unearth digital evidence, a topic that has been exhaustively examined. However, it's crucial to note that not all evidence is created equal, making it imperative to discern its defining attributes. In order to tackle these complex issues, we put forth a full Digital Forensics capability that includes elements for proactive, reactive, and activity (Active DF - ActDF) evidence gathering as well as a clear characterization of digital evidence. To emphasize the distinctive characteristics of digital evidence, a brand-new phrase called Comprehensive Digital Evidence (CDE) was created.

Process-based and role-based systems are the two categories into which DF architecture fall. In Chapter 3, a number of process-oriented DF structures were carefully identified, talked about, and compared, including those by leong. The majority of DF frameworks that have been studied recognize the importance of three main regions or components:

However, all three aspects have not been adequately addressed by any of the current DF systems. we created an early version of our CDF capability by comparing and contrasting several frameworks and their methodologies. A representation of our scholarly contribution, this CDF capacity is comprised of three interconnected parts: ProDF, ActDF, and ReDF.

When it comes to DF tools and technology, the ProDF component is all about getting organisations ready to perform at their best. On the other hand, the ReDF and ActDF parts are concerned with incident investigations; the former deals with conventional investigations conducted after an event has occurred, while the latter focuses on gathering evidence in real-time while an incident escalates.

In order to define the goals and elements of DF preparedness, we drew inspiration from Rowlingson and Garcia's ideas when developing the ProDF component. DF preparedness is a subset of ProDF, as shown by a comparison between the DF readiness outlined in Chapter 4 and the typical motivations for companies to get ready for DF. This paved the way for the creation of the ProDF component and a.

We unified the ReDF element in Chapter 5, outlining its rules, establishing objectives, and providing a thorough ReDF research process consisting of six phases, each with associated sub-phases and actions.

For the all-encompassing ActDF component, we conducted an extensive examination and comparison of different live investigation frameworks, such as those proposed by Payer, Ren, Foster, Grobler, and leong. This research culminated in the definition of ActDF, identification of its goals, and the formulation of our ActDF protocol, consisting of four stages, with corresponding sub-phases and procedures for gathering live proof while the event is still happening in each stage. The vital need for an ActDF protocol was also emphasized.

To enrich the BOK in DF, we introduced precise definitions:

Data recorded or communicated via digital devices that supports or refutes a fact was defined as digital evidence (Chawki, 2004). In order to prove a crime has been committed, this data must be accurate and provide evidence that either supports or disproves a theory (Casey, 2004).

Digital evidence that may be used to show or deny a fact and has the weight of evidence in a court of law is called Comprehensive Digital Evidence (CDE).

- An integrated framework that includes components of proactive (ProDF), active (ActDF), and reactive (ReDF) inquiry has evolved as a Comprehensive DF (CDF) capacity.

It is the CDF capabilities that we have added most significantly to the DF BOK. By dissecting the ProDF, ReDF, and ActDF components and talking about how they work together, Chapter 7 outlined our CDF capabilities.

## ProDF component

The existing literature does not contain information on the ProDF aspect that the present paper describes. We assess the organization's suitability to employ DF for both non-investigative and criminal investigations. By establishing ProDF, goals, smaller objectives, and related factors, we were able to develop our ProDF section.

We are confident that companies will reap the whole rewards of DF tool execution with the successful installation of the ProDF elements.

## General ProDF

- Definition of ProDF
- The ProDF part includes objectives, sub-objectives, and components (Figure 7-3).

ProDF goal 1: Become DF-ready				ProDF goal 2: Implement and manage DF to improve governance programmes	
Sub-goal 1:	Sub-goal 2:	Sub-goal 3:	Sub-goal 4:	Sub-goal 1:	Sub-goal 2:
Prepared infrastructure	Maximise CDE availability	Prepare responsible, competent employees	Ensure a cost-effective investigation	Establish a DF management capability	Apply DF to provide reasonable assurance regarding the achievement of organisational objectives

Figure 9.1 ProDF component 16

### ProDF goal 1: Become DF-ready

We cover both operational and analytical aspects within the context of a ready infrastructure. Building strong SOPs for digital forensics, setting up infrastructure to support effective use of DF abilities, and integrating DF specifications into the development of new programs and networks are all covered by the method of operation provisions. Software and equipment, as well as authorized tools and technologies, make up the digital forensic infrastructure. Putting a backup strategy and process in place in a Digital Forensics and Investigations lab is essential.

We present the idea of an evidential Oversight Strategy in an effort to maximize the availability of Critical Digital Evidence and proactively identify evidential components pertaining to certain dangers or scenarios. Our proposal is to create a risk assessment that surpasses the conventional assault profile by integrating disparate data sets and assessing the extent of gathering proof for a particular threat or circumstance. The found evidence has been methodically categorized into a proof catalogue. The evidence-based standards and procedures (EOS) include administrative, legal, and technological requirements pertaining to the proof that has been found.

The EOS is a ground-breaking invention that enables companies to assess the breadth and availability of the available evidence in relation to identified risks in cases. To prepare competent and responsible personnel, we support the creation of an all-encompassing plan for awareness, education, and training in Digital Forensics supported by recognized programs. We concentrate on how important it is to accredit training courses and certify staff members in order to enhance the legitimacy of investigations and their conclusions. Furthermore, we support the creation of an ethical code of ethics that regulates the use and deployment of DF technology and tools.

We suggest defining clearly appropriate inquiry processes and carefully weighing the expense of an investigation against the incident's cost in order to guarantee a prudent approach to inquiries. Integrating of DF needs into the company's risk control and emergency preparedness tactics, and policies is essential.

**Goal 2** of ProDF explores the effects of DF methods and tools for non-research goals. The following crucial actions are included in a well-designed execution and oversight strategy for this objective:

1. Developing a DF Strategy: Formulating a comprehensive strategy that outlines the strategic use of Digital Forensics within the organizational context.
2. Creating DF Management Competence: Defining how to integrate DF into organizational structures, thereby establishing a competence framework for the effective management of Digital Forensics.
3. Including DF in Emergency and Risk Administration: Describes how the organization's plans, procedures, guidelines, and strategies for disaster and risk control take into account the DF requirements. This guarantees the availability and acceptability of the proof in the event that an investigation is required.
4. Clearly Outlining Suggestions for DF Technologies and Processes: giving clear advice on how to apply digital forensics techniques and tools to give a fair level of confidence regarding the accomplishment of company objectives, having an emphasis on DF's non-investigative uses.

The concentration on leveraging DF for non-investigative reasons underscores the versatility and strategic value of Digital Forensics beyond traditional investigative purposes.

The ReDF element has been extensively explored and refined within existing research literature. We've discerned two distinctive DF frameworks, one grounded in processes and the other in roles. Our formulation of the ReDF component involved a rigorous definition of ReDF, the establishment of clear-cut objectives, and the construction of a ReDF protocol featuring six distinct phases along with their associated sub-objectives and steps. Our ReDF protocol stands as a dynamic process framework, where each phase feeds into the subsequent one, although we acknowledge the potential need to revert to a prior phase under specific circumstances.

Our confidence in the comprehensiveness of our ReDF protocol surpasses that of the DF frameworks expounded in Chapter 3. In crafting our protocol, we've not only encompassed all feasible activities from a spectrum of frameworks but also integrated unique steps.

Contributions to the BOK:

We present our proposed ReDF protocol comprising 6 aspects and their associated steps.

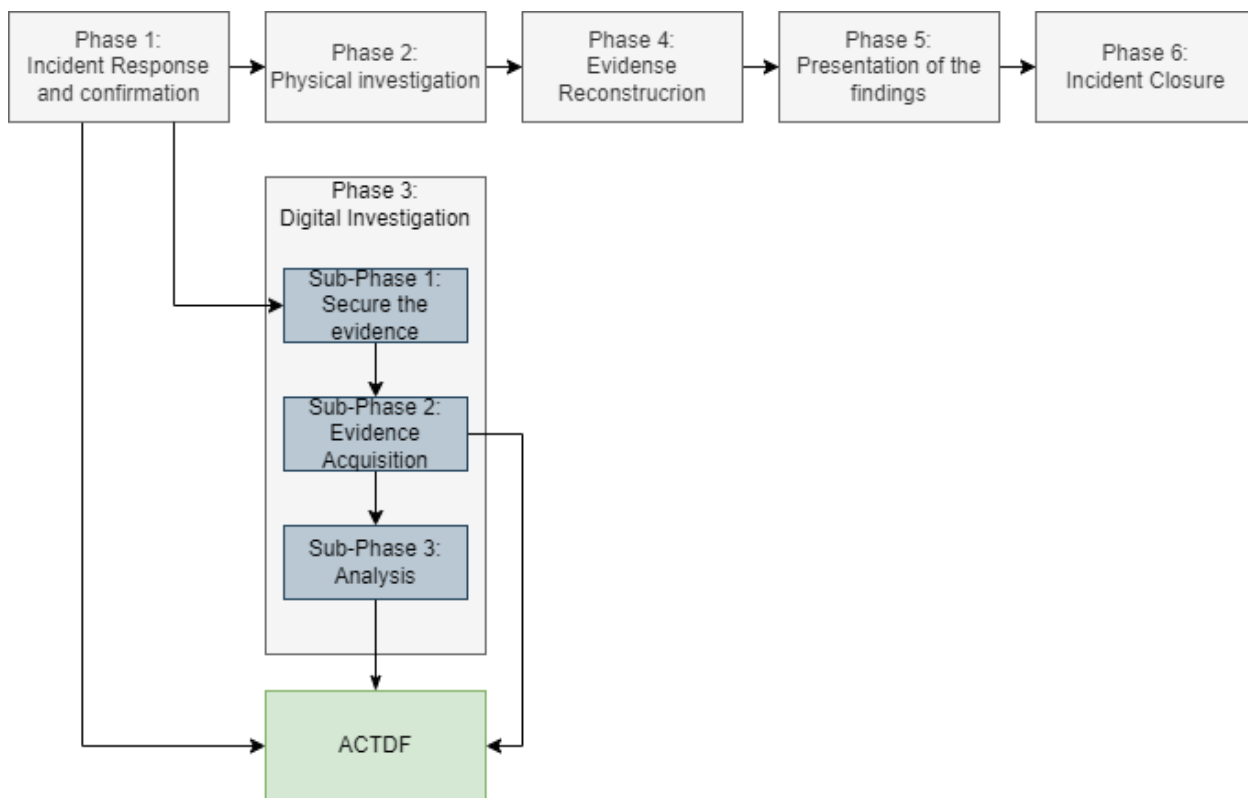


Figure 9.2: ReDF Protocol 17

A company's response to incidents strategy must include both event reaction and verification. It is recommended that organizations improve their plans by adding certain DF rules, processes, and actions.

The procedure clearly indicates that the ActDF element has been activated in order to get actual time proof.

## ActDF component

It has been recognized that an ActDF structure that is independent of technology is essential. We have presented the ActDF protocol, which expands on the framework of our ReDF protocol. The ActDF element has undergone a complex development process that began with a clear description of ActDF, goal definitions, and an ActDF protocol consisting of four stages, each with their own set of sub-goals and processes.

Remarkably, the first phase of the ActDF and ReDF procedures is the same. The ActDF protocol is only triggered in response to a specific request for real-time evidence.

Make an addition to the BOK (Body of Knowledge). Our study outlines the concept and goals of ActDF, which we have contributed to.

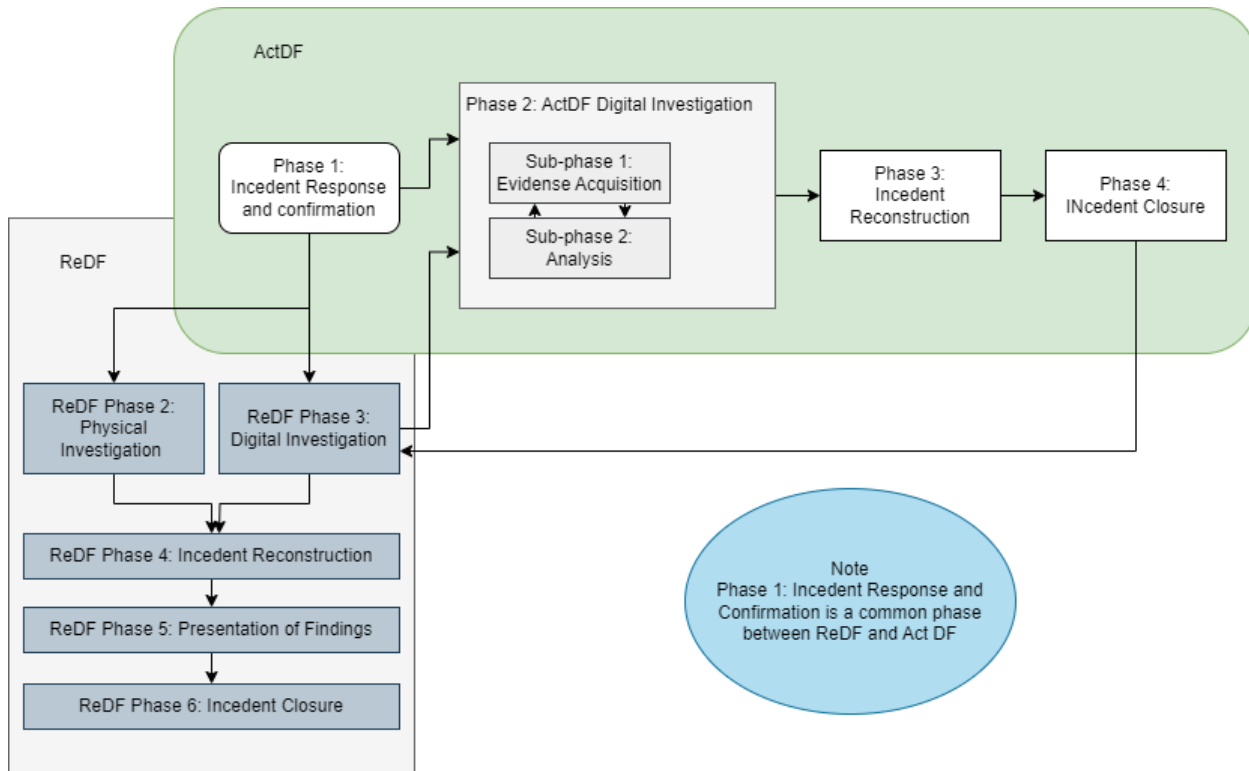


Figure 9.3 ActDF protocol 18

We present a distinctive ActDF protocol, comprising four phases along with their associated steps.

When there is a need for actual time proof, the ReDF method triggers the ActDF protocol, or it may be activated by certain specified situations.

Phase 4 is particularly noteworthy since it denotes the Event Closing stage, which entails compiling the real-time information gathered and giving the ReDF element authority to carry out the inquiry moving forward.

## Construction of our DFMF

In our pursuit of implementing the Comprehensive Digital Forensics (CDF) capability within an organization, it becomes crucial to outline precise actions. In order to help companies create plans, tactics, rules, and processes, as well as an infrastructure for operations and investigation and an effective capacity for human resources, we have methodically identified a set of tasks that can be implemented after each element of the CDF ability, as explained in Chapter 7. Interestingly, no other Digital Forensics framework that has been published in the literature offers this degree of thorough instruction or specificity to help with the deployment or administration of DF inside a company.

We carefully classified the combined list of tasks to be performed from Chapter 7 in Chapter 8. These were divided into groups based on several DF factors, including as administrative and legal factors, administration, policy making, procedure elements, human resources, and technology features. We developed the idea of a Digital Forensics Deployment and Governance Framework by utilizing the linkages that are naturally present between various DF components. It is essential to emphasize that

there is presently no DF architecture in use in the research community that offers the degree of precision required for the successful establishment and management of a CDF capability within a company.

When combined with the related DFMF, our CDF ability offers businesses a full manual. Companies may effectively get ready, control, and deploy DF for both analytical and non-investigative reasons with the help of this guidance. The end result is that businesses will be prepared to use DF methods and technologies to:

1. Examine occurrences, fraud, or staff conduct.
2. Make sure trustworthy and acceptable digital proof is available.
3. Evaluate the efficiency and usefulness of the processes and controls.
4. Assess adherence to laws and regulations.
5. Make non-investigative use of DF tools to increase the efficiency and oversight structures of IT and data security.

Contributing to the Body of Knowledge (BOK):

1. The DFMF idea was introduced, offering an organized method for putting our CDF capacity into practice and maintaining it.
2. The delivery of comprehensive output lists that cover administration, policy, operational elements, technology, personnel, and constitutional and judicial issues.
3. By capturing the connections among these outcomes, the DFMF promotes an all-encompassing strategy for the execution and administration of DF.

## **POSSIBLE DIFFICULTIES IN USING OUR DFMF AND CDF ABILITY**

Ideas like our DFMF and CDF abilities have not yet been validated in real-world scenarios. We use Casey's specifications for a DF architecture to assess DFMF and CDF abilities:

Here are some possible areas of research that we have identified:

- Make use of our CDF skills to evaluate the DF readiness of Pakistan organizations.
- Take a look at the ProDF component to find out how well organizations are prepared for DF.
- Examine how thorough the proof collection was in order to expand the proof technique and add more characteristics to the system.
- Find out how the use of digital forensics tools and techniques relates to digital finding.
- We should be able to control our CDF abilities by utilizing quantifiable qualities in the outputs.
- It will need further research and DFMF improvement to provide a complete architecture for the use and management of our CDF capabilities.
- Provide a DFMF monitoring app that is simple for management to utilize.

## **SUCCESS OF THE THESIS'S GOAL**

By creating a thorough, conceptual DF Management Framework for creating and sustaining an efficient CDF capability in a business, we were able to achieve the aim.



In summary, this thesis has confronted a critical challenge: the lack of a comprehensive framework for the effective management and implementation of Digital Forensics (DF) capabilities in organizational settings. The introduction of the Comprehensive Digital Forensics (CDF) capability and the Digital Forensics Management Framework (DFMF) marks a significant breakthrough in resolving this issue. Upon a thorough examination of the sub-objectives outlined in this thesis, it is clear that each one has been successfully addressed. Thus, the main goal of this thesis was successfully accomplished, leading to the creation of a comprehensive and theoretical DF administration Framework (DFMF), which is intended to facilitate the administration and use of CDF capabilities in organizational settings.

We continue to be confident in the significant addition to the Body of Knowledge in the area of digital forensics. Organizations may fully utilize DF by implementing our CDF capabilities, which will enable them to get reliable evidence, build sturdy procedures, and carry out effective investigations. This not only exhibits professionalism but also is essential to improving the company's general governance structures and good governance practices.

# BIBLIOGRAPHY

- ADELSTEIN, F. (2006). Live Forensics: Diagnosing your system without killing it first. *Communications of the ACM*, 49(2) 63-6. (Accessed May 5, 2008).
- ALLEN, W. (2005). Computer Forensics. *IEEE: Security and Privacy* 3(4) 59-62. Available from: <http://0-ieeeexplore.ieee.org.raulib.rau.ac.za/iel5/8013/32072/01492345.pdf?tp=&arnumber=1492345&isnumber=32072> (Accessed August 6, 2009).
- ARTHUR, K., VENTER, H. & OLIVIER, M. (2007). Applying the BIBA integrity model within a forensic evidence management system. In: *IFIP International Federation for Information Processing. Advances in Digital Forensics III*. Edited by CRAIZER, P. & SHENOI, S.: Springer.
- BABU, M. & PARISHAT, M. (2004). What is cybercrime? , *Star Of Mysore Online*. Available from: <http://www.crime-research.org/analytics/702/> (Accessed 1 September 2010).
- BARAYUMUREEBA, V. & TUSHABE, F. (2004). *The enhanced digital investigation process model*. Conference proceedings of the Fourth Annual Digital Forensics Research Workshop held in Baltimore, Maryland. 11- 13 August 2004. Available from: [http://www.dfrws.org/2004/bios/day1/Tushabe\\_EIDIP.pdf](http://www.dfrws.org/2004/bios/day1/Tushabe_EIDIP.pdf) (Accessed 5 March 2005).
- BEEBE, N. & CLARK, J. (2005). A hierarchical, objectives-based framework for the digital investigations process *Digital Investigation Journal, Elsevier*, 2 147-67.
- BRADFORD, P., BROWN, M. & PERDUt, J. (2007). Towards Proactive Computer-Systems Forensics. Available from: [www.cs.ua.edu/~pgb/papers/proactiveForensics.pdf](http://www.cs.ua.edu/~pgb/papers/proactiveForensics.pdf) (Accessed February 2, 2007).
- CAMPIA, M. (2012). *Security+ Guide to networking security fundamentals*. Course Technology.
- CARRIER, B. (2003a). Defining digital forensic examination and analysis tools using abstraction layers. *International Journal of Digital Evidence*, 1(4).
- CARRIER, B. (2003b). Open Source Digital Forensics Tools, The Legal Argument, *@stake Research Report*. Available from: [www.digital-evidence.org/papers/opensrc\\_legal.pdf](http://www.digital-evidence.org/papers/opensrc_legal.pdf) (Accessed 26 June 2007).
- CARRIER, B. (2006). Risks of live Digital Forensic analysis. *Communications of the ACM*, 49(2) 56 - 61.
- CARRIER, B. & SPAFFORD, E. (2003). Getting physical with the digital investigation process. *International Journal of Digital Evidence*, 2(2).
- CARRIER, B. D. & GRAND, J. (2004). A Hardware-Based Memory Acquisition Procedure for Digital Investigations. *Digital Investigation Journal*, 1(1). Available from: <http://www.digital-evidence.org/papers/tribble-preprint.pdf> (Accessed 6 April 2006).
- CARRIER, B. D. & SPAFFORD, E. H. (2005). *Automated digital evidence target definition using outlier analysis and existing evidence*. Conference proceedings of the 2005 Digital Forensic Research Workshop (DFRWS) held in New Orleans. Available from: [www.dfrws.org/2005/proceedings/carrier\\_targetdefn.pdf](http://www.dfrws.org/2005/proceedings/carrier_targetdefn.pdf) (Accessed 17 April 2006).
- CASEY, E. (2004). *Digital evidence and computer crime*. Elsevier academic press.
- CASEY, E. (2007). Digital evidence maps - A sign of the times. *Digital Investigation, Elsevier*, 4( ) 1- 2.
- CASEY, E. (2011). *Digital evidence and computer crime, forensic science, computers and the Internet*. Elsevier.
- CASEY, E. & STANLEY, A. (2004). Tool review - remote forensic preservation and examination tools. *Digital Investigation Journal, Elsevier*, 1 284-97.

- CERT@\_COORDINATION\_CENTER. (2004). How the FBI investigates computer crime. Available from: [www.cert.org/tech\\_tips/FBI\\_investigates\\_crime.html](http://www.cert.org/tech_tips/FBI_investigates_crime.html) (Accessed Aug 9, 2009).
- CHAWKI, M. (2004). The Digital Evidence in the Information Era *Computer Crime Research Center*. Available from: <http://www.crime-research.org/articles/chawki1/2> (Accessed October 6, 2008).
- CLARK, A. (2006). Are you ready for Forensics? Available from: <http://www.inforenz.com/press/20060223> (Accessed October 6, 2008).
- COMMISSION ON CRIME PREVENTION AND CRIMINAL JUSTICE, T. S. (2001). Conclusions of the Study on effective measures to prevent and control high-technology and computer-related crime. No:E/CN.15/2001/4.
- Computer evidence defined* [Online]. (2008). Available from: <http://www.forensics-intl/def4.html> (Accessed July 1, 2011).
- FBI, U. D. O. J. (1999). Trace evidence recovery guidelines. *Forensic science communications*, 1 (3). Available from: <http://www.fbi.gov/hq/lab/fsc/backissu/oct1999/trace.htm> (Accessed February 5, 2009).
- FERGUSON, N. (2006). AES-CBC + Elephant di@user A Disk Encryption Algorithm for Windows Vista. Available from: <http://pdos.csail.mit.edu/6.858/2011/readings/bitlocker.pdf> (Accessed 20 February 2012).
- FORRESTER, J. & IRWIN, B. (2007). *A Digital Forensic investigative model for business organisations*. Conference proceedings of the IFIPSec 2007 held in Sandton, South Africa. 14-16 May 2007
- FOSTER, M. & WILSON, J. (2004). Process Forensics: A pilot study on the use of checkpointing technology in computer forensics. *International Journal of Digital Evidence*, 3(1).
- FRYE, M. (2005). The Coroner's Toolkit. *Linux magazine*, Tuesday, 15 March 2005.
- GARCIA, J. (2005). Proactive and Reactive Forensics. Available from: [http://rediris.es/cert/doc/reuniones/af05/proactive\\_n\\_reactive\\_forensics.pdf](http://rediris.es/cert/doc/reuniones/af05/proactive_n_reactive_forensics.pdf) (Accessed 5 September 2005).
- GARFINKEL, S. (2010). Digital forensic research: The next 10 years. *Digital Investigation, Elsevier*, 7 64-78.
- GORDON, L., LOEB, M., LUCYSHYN, W. & RICHARDSON, R. (2006). CSI/FBI Computer Crime and Security Survey.
- GROBLER, C. & LOUWRENS, C. (2006). *Digital Forensics: a multi dimensional discipline*. Conference proceedings of the 4th annual Information Security South Africa conference held in Sandton, South Africa. 5 - 7 July 2006.
- GROBLER, C. & LOUWRENS, C. (2007). *DF readiness a component of Information Security best practise*. Conference proceedings of the IFIPSec 2007 held in Sandton, South Africa. 14- 16 May 2007. Springer.
- GROBLER, C. & LOUWRENS, C. (2009). *High-level integrated overview of DF*. Conference proceedings of the Information Security of South Africa held in Johannesburg.
- GROBLER, C. & LOUWRENS, C. (2010). *Evidence Management Plan*. Conference proceedings of the Information Security South Africa held in Sandton South Africa. IEEE Express.
- GROBLER, C., LOUWRENS, C. & VON SOLMS, S. (2010a). *A framework to guide the implementation of Proactive Digital Forensics in organizations*. Conference

- proceedings of the Workshop for Digital Forensics 2010 held in Krakow, Poland. IEEE Explore.
- GROBLER, C., LOUWRENS, C. & VON SOLMS, S. (2010b). *A multi-component view of Digital Forensics*. Conference proceedings of the Workshop for Digital Forensics held in Krakow, Poland. 15-18 February 2010. IEEE Explore.
- GROBLER, M. (2009). *Liforac, a model for live forensic acquisition*. PhD Computer Science, University of Johannesburg.
- GUIDANCE\_SOFTWARE. (2005). EnCase Enterprise detailed product description. Available from: <http://www.encaseenterprise.com/support/resources.aspx> (Accessed 8/8/2009).

- GULDENTOPS, E., HARDY, G., HESCHL, J. & STROUD, R. (2005). Aligning COBIT, ITIL and ISO 17799 for Business Benefit.
- HILLEY, S. (2006). The Corporation: the non-policed state. Available from: [http://www.infosecurity-magazine.com/features/novdec04/corp\\_novdec.html](http://www.infosecurity-magazine.com/features/novdec04/corp_novdec.html).
- IEONG, R. (2006). FORZA – Digital forensics investigation framework that incorporate legal issues. *Digital Investigation* 329-36.
- IEONG, R. & LEUNG, H. (2007). *Deriving Cse-specific Live Forensics Investigation Procedures from FORZA*. Conference proceedings of the 2007 ACM symposium on Applied computing held in Seoul, Korea. 2007. ACM Press New York, NY, USA. Available from: <http://portal.acm.org/citation.cfm?id=1244049> (Accessed 11 Oct 2007).
- INSTITUTE, I. G. (2000). Control Objectives for Information and related technologies. Available from: ('Accessed').
- ISACA. (2004). IS Auditing guideline Computer forensics Document G28. Available from: [http://www.isaca.org/AMTemplate.cfm?Section=Standards,\\_Guidelines,\\_Procedures\\_for\\_IS\\_Auditing&Template=/ContentManagement/ContentDisplay.cfm&ContentID=18642](http://www.isaca.org/AMTemplate.cfm?Section=Standards,_Guidelines,_Procedures_for_IS_Auditing&Template=/ContentManagement/ContentDisplay.cfm&ContentID=18642).
- ISO/IEC17799. (2005).
- ITGI. (2000). Control Objectives for Information and related Technologies. Available from: [www.isaca.org/cobit](http://www.isaca.org/cobit) (Accessed 20 February 2007).
- KING. (2003). King II Report on Corporate Governance. Available from: <http://iodsa.co.za/lod%20draft%20king%20report.pdf> (Accessed January 2006).
- KING. (2009). King III Report on Corporate Governance. Available from: [http://www.iodsa.co.za/downloads/documents/King\\_Code\\_of\\_Governance\\_for\\_SA\\_2009.pdf](http://www.iodsa.co.za/downloads/documents/King_Code_of_Governance_for_SA_2009.pdf) (Accessed 13 October 2009).
- KRUSE, W. & HEISER, J. (2004). *Computer Forensics, Incident Response Essentials*. Addison- Wesley.
- LEE, H., PALMBACH, T. & MILLER, M. (ed.). 2001. *Henry Lee's crime scene handbook*. : San Diego: Academic Press.
- LEIGHLAND, R. & KRINGS, A. (2004). A Formalization of Digital Evidence. *International journal of Digital Evidence*, 3(2).
- LEMONS, R. (2011). Stuxnet more effective than bombs. *Info world Techwatch*, 19 January 2011.
- LOUWRENS, C. & VON SOLMS, S. (2005). Relationship between Digital Forensics, Corporate Governance, Information Technology and Information Security Governance. In: *Digital Crime and Forensic Science in Cyberspace*. Edited by KANELIS, P., KIOUNTOUZIS, E., KOLOKOTRONIS, N. & MARTAKOS, D.: National and Kapodistrian University of Athens, Greece.
- LOUWRENS, C., VON SOLMS, S. & KANNELIS (ed.). 2006a. *Digital Crime and forensic Science in Cyberspace: The relationship between Digital Forensics, Corporate Governance, IT Governance and IS Governance* Idea Group publishing, Hershey
- LOUWRENS, C., VON SOLMS, S., REECKIE, C. & GROBLER, T. (2006b). *A control Framework for Digital Forensics*. Conference proceedings of the IFIP11.9 International Conference on Digital Forensics held in Orlando Florida. Springer.
- NIKKEL, B. (2006). *The role of Digital Forensics within a corporate organization*. Conference proceedings of the IBSA Conference held in Vienna. May 2006. Available from: <http://digitalforensics.ch/nikkel06a.pdf#search=%22digital%20Forensic%20readiness%22> (Accessed November 2007).

- NIKKEL, B. J. (2005). Generalizing sources of live network evidence. *Digital Investigation Journal*, 2(3) 193-200.
- NOLAN, R., O'SULLIVAN, C., BRANSON, J. & WAITS, C. (2001). Electronic Crime Scene Investigation: A Guide for first responders. No:NIJ#: 187736. Available from: <http://www.ncjrs.org> (Accessed June 2007).

- O'CIARDHUAIN, S. (2004). An extended model of cybercrime investigations. *International journal of Digital Evidence*, 3(1).
- OREBAUGH, A. (2006). Proactive Forensics. *Journal of Digital Forensic Practice*, Volume 1 37-41.
- PALMER, G. (2001). *A Roadmap for Digital Forensics Research*. Conference proceedings of the Digital Forensic Research Workshop held in Utica, New York. 7- 8 August 2001. Available from: <http://www.dfrws.org/2001/dfrws-rm-final.pdf> (Accessed 2 February 2006).
- PARKINSON, M. & BAKER, N. (2005). IT and Enterprise Governance. *Journal of Information Systems Control*, 3 17-21.
- PATZAKIS, J. (2003). Computer Forensics as an Integral component of the Information Security Enterprise. Available from: <http://www.guidancesoftware.com/downloads/getpdf.aspx?fl=.pdf> (Accessed 10 May 2009).
- PATZAKIS, J. & LIMONGELLI, V. (2004). Internal computer investigations as a critical control activity under Sarbanes-Oxley. Available from: <http://www.guidancesoftware.com/downloads/getpdf.aspx?fl=.pdf> (Accessed 10 May 2009).
- PAYER, U. (2004). *Realtime intrusion forensics: A first prototype implementation (based on a stack-based NDIS)*. Conference proceedings of the Terena networking conference held in University of Aegean, Rhodes, Greece. 7-10 June. Terena publishing.
- PIETERSE, I. (2006). E-mail risk not managed. *ITWeb*, 11 July 2006.
- REITH, M., CARR, C. & GUNSCH, G. (2002). An examination of Forensic models. *International Journal of Digital Evidence*, 1(3).
- REN, W. & JIN, H. (2005). *Honeynet based distributed adaptive network forensics and active real-time investigation*. Conference proceedings of the ACM Symposium on Applied Computing held in Santa Fe, New Mexico, USA. 13-17 March 2005.
- RICHARDSON, R. (2007). The 12th Annual Computer Crime and Security Survey. Available from: [http://www.gocsi.com/forms/csi\\_survey\\_thanks.jhtml?\\_DARGS=/forms/csi\\_survey.jhtml](http://www.gocsi.com/forms/csi_survey_thanks.jhtml?_DARGS=/forms/csi_survey.jhtml) (Accessed 29 February 2008).
- RICHARDSON, R. (2008). The 13th CSI/FBI Computer Crime & Security Survey.
- RICHARDSON, R. (2012). 15th Annual 2010/1022 Computer crime and security survey. Available from: [www.GoCSI.com](http://www.GoCSI.com) (Accessed February 25, 2012).
- ROGERS, M. & SIEGFRIED, K. (2004). The future of computer forensics: a needs analysis survey. *Computers and Security*, 23(1) 12-6.
- ROWLINGSON, R. (2004). A ten step process for forensic readiness. *International journal of Digital Evidence, Elsevier*, 2(3). Available from: [www.ijde.org](http://www.ijde.org) (Accessed June 2006).
- RUDD, C. (ed.). 2004. *An Introductory Overview of ITIL® Version 1.0a*: ITSMF Ltd.
- SAPS. (2011). Crime Situation in South Africa Available from: [http://www.saps.gov.za/statistics/reports/crimestats/2011/crime\\_stats.htm](http://www.saps.gov.za/statistics/reports/crimestats/2011/crime_stats.htm) (Accessed 28 February 2012).
- Sarbanes-Oxley Act of 2002. (2002). USA. Available from: [http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107\\_cong\\_bills&docid=f:h3763enr.txt.pdf](http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_bills&docid=f:h3763enr.txt.pdf). (Accessed 10 November 2008).
- SHELDON, A. (2004). Forensic Auditing, The role of computer forensics in the corporate toolbox. Available from: <http://www.itsecurity.com/papers/p11.htm> (Accessed 25/3/2004).
- SHIPLEY, T. G. & REEVE, H. R. (2006). Collecting evidence from a running computer: A technical and legal primer for the justice community. Available from:

- <http://www.search.org/files/pdf/CollectEvidenceRunComputer.pdf> (Accessed Aug 8, 2009).
- SINANGIN, D. (2002). Computer forensics investigations in a corporate environment. *Computer Fraud and Security Bulletin*, 8(June) 11-4.
- SOANES, C. & HAWKER, S. (2005). Oxford Dictionary. Oxford University press. Available from: <http://www.askoxford.com/dictionaries/?view=uk>.



- SOMMER, P. (1999). Intrusion Detection Systems as Evidence. *Computer Networks: The International Journal of Computer and Telecommunications Networking* Volume 31 , (123-24 (December 1999)) 2477 - 87 Available from: [http://www.raid-symposium.org/raid98/Prog\\_RAID98/Full\\_Papers/Sommer\\_text.pdf](http://www.raid-symposium.org/raid98/Prog_RAID98/Full_Papers/Sommer_text.pdf).
- SOMMER, P. (2005). Directors and Corporate Advisors' Guide to Digital Investigations and Evidence, *Information Assurance Advisory Council*. Available from: <http://www.iaac.org.uk/Portals/0/Evidence%20of%20Cyber-Crime%20v12-rev.pdf> (Accessed June 3, 2007).
- SREMACK, J. (2005). *Investigating real-time systems forensics*. Conference proceedings of the Workshop of the 1st International Conference on Security and Privacy for Emerging Areas in Communication Networks, SecureComm 2005 held in Athens, Greece. 5-9 Sept 2005. IEEE Explore.
- STEPHENSON, P. (2002). End to End Forensics. *Computer Fraud and Security Bulletin*, 2002(9) 17- 9.
- STEPHENSON, P. (2003). Conducting incident post mortems. *Computer Fraud and Security*. Available from: [www.emich.edu/cerns/downloads/pstephen/Conducting-Incident-Post-Mortems.pdf](http://www.emich.edu/cerns/downloads/pstephen/Conducting-Incident-Post-Mortems.pdf) (Accessed January 2006).
- SWGDE & IOCE (2000). Digital Evidence: Standards and Principles. *Forensic Science Communications*, April 2000 Volume 2 (2). Available from: <http://www.fbi.gov/hq/lab/fsc/backissu/april2000/swgde.htm> (Accessed June 2008).
- TC-11, I. (2006). Digital Forensics - Fact sheet. Available from: [http://www.tc11.uni-frankfurt.de/WG/Factsheet\\_WG\\_11-9.pdf](http://www.tc11.uni-frankfurt.de/WG/Factsheet_WG_11-9.pdf) (Accessed February 3, 2007).
- TECHNET. (2009). Windows BitLocker Drive Encryption Frequently Asked Questions. Available from: [http://technet.microsoft.com/en-us/library/cc766200\(WS.10\).aspx#BKMK\\_WhatIsBitLocker](http://technet.microsoft.com/en-us/library/cc766200(WS.10).aspx#BKMK_WhatIsBitLocker) (Accessed August 6, 2009).
- THOMAS, D. (2005). Organisations need a digital evidence plan. *Computing*, 21 Sep 2005.
- TURNER, D., ENTWISLE, S. & DENESIUK, M. (2007). Symantec Internet Security Threat Report Trends for July–December 06, Volume XI. Available from: [http://eval.symantec.com/mktginfo/enterprise/white\\_papers/ent-whitepaper\\_internet\\_security\\_threat\\_report\\_xi\\_keyfindings\\_03\\_2007.en-us.pdf](http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xi_keyfindings_03_2007.en-us.pdf) (Accessed January 2008).
- TURNER, P. (2007). Applying a forensic approach to incident response, network investigation and system administration using Digital Evidence Bags. *Digital Investigation*, (4) 30-5.
- UNESCO. (1997). Definitions, *Technology and Learning portfolio*. Available from: <http://www.unesco.org/education/educprog/lwf/doc/portfolio/definitions.htm> (Accessed 8 August 2008).
- VON SOLMS, S. & VON SOLMS, R. (2009). *Information Security Governance*. Springer.
- WHITMAN, M. & MATTORD, H. (2008). *Management of Information Security*. Course Technology Cengage learning.
- WHITMAN, M. E. & MATTORD, H. J. (2009). *Principles of Information Security*. Thompson Course technology.
- WIKIPEDIA. (2008). Cybercrime. Available from: [http://en.wikipedia.org/wiki/Cyber\\_Crime](http://en.wikipedia.org/wiki/Cyber_Crime) (Accessed July 19, 2008).
- WIKIPEDIA. (2009). BitLocker Drive Encryption. Available from: [http://en.wikipedia.org/wiki/BitLocker\\_Drive\\_Encryption#Security\\_concerns](http://en.wikipedia.org/wiki/BitLocker_Drive_Encryption#Security_concerns) (Accessed January 2010).
- WIKIPEDIA. (2012a). Expert witness. Available from: [http://en.wikipedia.org/wiki/Expert\\_witness](http://en.wikipedia.org/wiki/Expert_witness) (Accessed 20 February 2012).
- WIKIPEDIA. (2012b). Statement on auditing standards. Available from: <http://>

[en.wikipedia.org/wiki/SAS\\_70](http://en.wikipedia.org/wiki/SAS_70) (Accessed February, 28 2012).