



UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA
Denkleiers • Leading Minds • Dikgopolo tša Dihlalefi

A Digital Forensic Readiness Approach

for

e-Supply Chain Systems

by

Derek Jens Emeth Masvosvere

Submitted in fulfilment of the requirements for the degree

Master of Science (Computer Science)

in the

**Faculty of Engineering, Built-Environment and Information
Technology**

At the

UNIVERSITY OF PRETORIA

SUPERVISED BY

Prof. H.S VENTER

Table of Contents

Chapter 1	1
Introduction	1
1.1 Introduction.....	1
1.2 Problem Statement	3
1.3 Motivation.....	4
1.3 Objectives	4
1.5 Research Methodology	5
1.6 Dissertation Outline	5
1.7 Conclusion	8
Chapter 2	9
Digital Forensics	9
2.1 Introduction.....	9
2.2 Digital Forensics Concepts and Definitions.....	9
2.3 Digital Forensics Concurrent Processes.....	11
2.3.1 Readiness Processes Class	12
2.3.2 Initialisation Processes Class	13
2.3.3 Acquisitive Processes Class	13
2.3.4 Investigative Processes Class.....	13
2.3.5 Concurrent Processes Class	13
2.4 Digital Forensic Readiness Defined.....	14
2.5 Digital Forensic Readiness Processes	16
2.5.1 Planning Process Group	16
2.5.2 Implementation Process Group.....	18
2.5.3 Assessment Process Group	18
2.6 Digital Evidence.....	19
2.7 DFR tools.....	19
2.7.1 Incident detection systems	19
2.7.2 Security Event Management Software (SEMs)	19
2.7.3 Incident Management software.....	20
2.8 Conclusion	21
Chapter 3	22
E-Supply Chains	22



3.1 Introduction.....	22
3.2 Supply Chain.....	22
3.3 E-Supply Chain System Defined	23
3.3.1 E-supply Chain Essential Elements	24
3.3.2 E-Supply Chain Model.....	26
3.4 Conclusion	28
Chapter 4	29
DFR challenges in e-supply chains	29
4.1 Introduction.....	29
4.2 DFR in e-Supply Chains	29
4.3 Limitations of Current DFR Tools.....	30
4.3.1 Limited Throughput for Data Capturing Devices	31
4.3.2 Poor Usability	31
4.3.3 Compromised Privacy and Limited Filtering of Packets	32
4.3.4 No technical Support.....	32
4.3.5 Software Errors	33
4.4 Conclusion	33
Chapter 5	34
A model for Digital forensic readiness in eSCs	34
5.1 Introduction.....	34
5.2 Proposed Methodology for eSC-DFR.....	35
5.2.1 Planning processes group for DFR in E-supply chains.....	35
5.2.2 Implementation processes group for DFR in E-supply chains.....	38
5.2.3 Assessment of implementation processes group for DFR in E-supply chains.....	40
5.3. Proposed eSC-DFR process model.....	42
5.4 eSC-DFR Conceptual model.....	43
5.4.1 eSC-DFR planning processes leading to eSC-DFR system design.....	44
5.4.2 Concept of an eSC-DFR system	46
5.5 Scenario.....	49
5.6 Conclusion	50
Chapter 6	51
ESC-DFR system requirements.....	51
6.1 Introduction.....	51
6.2 eSC-DFR System goals.....	51
6.3 Functional Requirements	52
6.4 Non-Functional requirements	53



6.4.1 Usability	54
6.4.2 Quality of Service	Error! Bookmark not defined.
6.4.3 Security	54
6.4.4 Scalability	54
6.4.5 Availability	54
6.4.6 Accessibility.....	54
6.4.7 Follow existing standards and practices.....	55
6.5 Conclusion	55
Chapter 7	56
ESC-DFR system Design	56
7.1 Introduction.....	56
7.2 Architecture overview.....	56
7.2.1 eSC network component.....	57
7.2.2 eSC-DFR component.....	57
7.2.3 Description of a typical eSC network environment.....	58
7.2.4 eSC hypothetical incident scenario.....	59
7.3 The eSC-DFR system components	60
7.3.1 Logging modules for PDE collection.....	61
7.3.2 eSC-DFR system PDE handling component.....	63
7.4 eSC-DFR system Central Data Repository component	65
7.4.1 Log Daemon in eSC-DFR component.....	67
7.4.2 eSC-DFR application server modules.....	68
7.4.3 The eSC-DFR web server	71
7.5 Detailed eSC-DFR system architecture model	71
7.6 Conclusion	73
Chapter 8	74
ESC-DFR System Prototype	74
8.1 Introduction.....	74
8.2 Use case for the eSC-DFR system prototype.....	74
8.2.1 eSC-DFR component actors.....	75
8.3 The eSC network.....	76
8.3.1 Supplier eSC network web application user interface	78
8.3.2 Retailer eSC network web application user interface	80
8.4 The eSC-DFR component of the prototype	86
8.4.1 Potential Attacks tab	87
8.4.2 Login Flags tab	90



8.4.3 System Flags tab	91
8.4.5 System Users tab.....	94
8.4.6 Products Tab	95
8.5 Conclusion	98
Chapter 9	99
Critical Evaluation	99
9.1 Introduction.....	99
9.2 Primary Benefits of the Research.....	99
9.2.1 An eSC-DFR process model based on standardised principles	100
9.2.2 An implementation of the eSC-DFR process model.....	100
9.2.3 Usability of eSC-DFR component	100
9.2.4 PDE preservation by eSC-DFR component.....	101
9.2.5 PDE Pre-analysis by eSC-DFR component	101
9.3 Secondary End-user benefits.....	102
9.4 Shortcomings of Research	103
9.4.1 Inconsistent judicial laws on electronic evidence	104
9.4.2 Privacy Issues.....	104
9.4.3 Different platform requirements	104
9.5 Conclusion	105
Chapter 10	106
Related Work	106
10.1 Introduction.....	106
10.2 Related work on the eSC-DFR process.....	106
10.3 Related work on DFR tools.....	108
10.4 Related work on DFR tool requirements specifications	110
10.5 Conclusion	111
Chapter 11	113
Conclusion	113
11.1 Introduction.....	113
11.2 Summary of Dissertation	113
11.3 Recap of the Problem Statement.....	114
11.4 Future Work	115
11.5 Conclusion	117
Bibliography	118
Appendix: Publications	124

List of Tables

Table 6.1 Functional Requirements of eSC-DFR system.....	64
Table 6.2 Non-Functional Requirements of eSC-DFR system	64
Table 9.1: Summary of Benefits and shortcomings.....	117

List of Figures

Figure 1. 1 Dissertation Layout.....	7
Chapter 2	
Figure 2. 1 Comprehensive harmonised digital forensic investigation process model[18]	12
Figure 2. 2 Readiness processes groups.....	15
Chapter 3	
Figure 3. 1 E-supply chain Structure	27
Chapter 5	
Figure 5. 1 eSC-DFR planning processes group.....	36
Figure 5. 2 eSC-DFR implementation processes	38
Figure 5. 3 Assessment of implementation eSC-DFR processes group.....	40
Figure 5. 4 eSC-DFR process model	42
Figure 5. 5 eSC-DFR conceptual model	44
Figure 5. 6 eSC-DFR planning processes in eSC network diagram	45
Figure 5. 7 eSC-DFR system functional model	47
Figure 5. 8 A small eSC network.....	49
Chapter 7	
Figure 7. 1 High level eSC-DFR systems Architecture	57
Figure 7. 2 eSC network	58
Figure 7. 3 Sample typical web server log file	60
Figure 7. 4 Component diagram for PDE collection process.....	62
Figure 7. 5 PDE handling process in eSC-DFR system.....	64
Figure 7. 6 PDE capturing to PDE storage process	66
Figure 7. 7 eSC-DFR database.....	67
Figure 7. 8 eSC-DFR application server components.....	69
Figure 7. 9 eSC-DFR system design model.....	72

Chapter 8

Figure 8.1 eSC-DFR component use-case diagram	75
Figure 8.2 programming languages used in eSC network web application frontend and backend	77
Figure 8.3 eSC network application Login/Register Page	78
Figure 8.4 eSC network application User New Account page.....	79
Figure 8.5 Supplier Dashboard upon successful Login	80
Figure 8.6 Supplier statistics.....	80
Figure 8.7 A retailer's eSC app user interface dashboard.....	81
Figure 8.8 A retailer purchasing cars from a supplier.....	81
Figure 8.9 The retailers' webstore where they can change inventory pricing.	82
Figure 8.10 Generated retailer invoices from supplier.....	82
Figure 8. 11 PDF Generated retailer invoice from supplier.....	83
Figure 8.12 Retailer inventory data.....	83
Figure 8.13 Customer Dashboard	84
Figure 8.14 Customer adding vehicles to cart.....	84
Figure 8.15 Customer purchasing vehicles from cart.	85
Figure 8.16 Generated customer invoice in PDF format	86
Figure 8. 17 eSC-DFR component authentication page.....	86
Figure 8. 18 DFI Dashboard in eSC-DFR component.....	87
Figure 8. 19 Potential flagged attacks Tab.....	88
Figure 8. 20 Cross-Site Scripting attack flagged by the eSC-DFR component	89
Figure 8. 21 eSC app web server response to injected script.....	89
Figure 8. 22 URL tampering flag.....	90
Figure 8. 23 Login flags tab.....	91
Figure 8. 24 System flags tab.....	91
Figure 8. 25 flagPriceChange function	92
Figure 8. 26 eSC Generated invoices.....	93
Figure 8. 27 invoice manipulation check function.....	93
Figure 8. 28 System users tab	94
Figure 8. 29 System users tab and price change chart	95
Figure 8. 30 Chart generating function	95
Figure 8. 31 Chart generating function	96
Figure 8. 32 Products tab and price change chart	96
Figure 8. 33 eSC-DFR component Products PDE	97
Figure 8. 34 A graphical representation of the vehicle price changes	97



Declaration

I declare that this dissertation, which I submit in fulfilment of the requirements for the degree of Master of Science in Computer Science at the University of Pretoria, is entirely my own work and has not been submitted elsewhere for the award of a degree or otherwise. One national and one international peer reviewed conference papers were published from this dissertation. One journal article was published in a national peer-reviewed scientific journal. Any errors in thinking or delivery as well as any omissions are entirely my own responsibility.

I, Derek Jens Emeth Masvosvere, declare that this dissertation entitled, “A Digital Forensic Readiness Approach for e-Supply Chain Systems” and the work presented in it is my own.

Author Signature Date Signed

Acknowledgements

I am sincerely thankful to my supervisor, Prof. Hein S. Venter, for embarking on this journey with me and believing in me even when I felt defeated at times. I could have never asked for a more suited supervisor to mentor me, keep me focused (take out the whip) and supervise my work throughout this entire process.

I am more than grateful to the Computer Science Department's staff, and the University of Pretoria as a whole for giving me this priceless opportunity to conduct this research and gain the knowledge that I have today. Without the financial support from the University completing this research would not have been possible.

I would also like to thank my fellow colleagues from the ICSA group for sharing their knowledge and friendship, making the research process enjoyable.

Last but not least I would like to thank my family for giving me encouragement and support throughout the course of my studies. I cannot thank you enough, family.

Abstract

The internet has had a major impact on how information is shared within supply chains, and in commerce in general. This has resulted in the establishment of information systems such as e-supply chains (eSCs) amongst others which integrate the internet and other information and communications technology (ICT) with traditional business processes for the swift transmission of information between trading partners. Many organisations have reaped the benefits that come from adopting the eSC model, but have also faced the challenges with which it comes. One such major challenge is information security. With the current state of cybercrime, system developers are challenged with the task of developing cutting-edge digital forensic readiness (DFR) systems that can keep up with current technological advancements, such as eSCs. Hence, the research highlights the lack of a well-formulated eSC-DFR approach that can assist system developers in the development of e-supply chain digital forensic readiness systems. The main objective of such a system is that it must be able to provide law enforcement/digital forensic investigators that operate on eSC platforms with forensically sound and readily available potential digital evidence that can expedite and support digital forensics incident-response processes. This approach, if implemented can also prepare trading partners for security incidents that might take place, if not prevent them from occurring. Therefore, the work presented in this research is aimed at providing a procedural approach that is based on digital forensic principles for eSC system architects and eSC network service providers to follow in the design of eSC-DFR tools. The author proposes an eSC-DFR process model and eSC-DFR system architectural design that was implemented as part of this research illustrating the concepts of evidence collection, evidence pre-analysis, evidence preservation, system usability alongside other digital forensic principles and techniques. It is the view of the authors that the conclusions drawn from this research can spearhead the development of cutting-edge eSC-DFR systems that are intelligent, effective, user friendly and compliant with international standards.

Chapter 1

Introduction

1.1 Introduction

In this digital age, collaborative commerce is the key to running a successful business. Organisations have come to realise that it is important to establish and manage relationships that are mutually beneficial, as this is central to corporate survival and growth [1]. As a result, most organisations have made adjustments to their traditional trade patterns to stay competitive. A supply chain supports the co-ordination of a number of business processes that include order taking, order generation and order fulfilment/distribution of products, services, or information. These processes cover the flow of goods and services from suppliers to consumers through manufacturing and distribution chains. Over the years supply chains have become more automated, allowing for increased collaboration between trading partners [2]. This has positively impacted on the quality of service, lowering of cost and the increase of value along the supply chain.

According to Bellefeuille and Lynn [3], information is often considered to be as important as the value of physical assets. Hence safeguarding the integrity, confidentiality, accuracy and accessibility of company information is critical to a trading partner's ability to operate in today's supply chains. Technology has played a pivotal role in making it possible for organisations within a supply chain to share useful information and resources with the objective of producing results. It has also been observed that with a great deal of advancement in technology, supply chains have become more efficient and more complex [4]. It is also undeniable that sharing information with trading partners provides many exceptional benefits but also leaves the supply chain vulnerable to an array of threats. Examining the risk that information security incidents can pose to the supply chain is critical not only from an operational perspective, but in order to comply with regulations such as the Electronic Communications and Transactions (ECT) Act of 2012. The application of e-commerce to the management of a supply chain creates a new term that is e-supply chain management. This refers to the management of electronic supply chains. E-commerce delivers all the above mentioned benefits, but it also introduces vulnerabilities that if exploited could be detrimental to the supply chain.

Digital forensics provides an approach to prepare the supply chain for threats, identify, analyse and treat the supply chain for the vulnerabilities identified. Threats to supply chains vary from network breaches, hacking, and cybercrime just to mention a few. It is quite feasible to assume that not everyone that makes use of technology is using it for the right reasons. That being the case, criminals are beginning

to realise that unlike using old tactics to commit crime such as robbing a store, it might be safer and more rewarding to commit crime from a laptop somewhere in a basement. It is important to note that e-supply chains highly rely on the flow of information; hence the surge of cybercrime poses serious threats to supply chain continuity [5]. Hence a Digital Forensic Readiness Process to identify vulnerabilities across the supply chain would help mitigate the many risks posed by the advanced use of technology in today's supply chains.

In recent years systematic cyber-attacks on financial institutions have been increasing and corporations are finding it tougher to obtain insurance coverage paying higher premiums, while financial reforms are putting pressure on banks to tighten the terms of trade finance [6]. This requires an updated framework for evaluating and responding to security threats. A company might risk losing large amounts of money if it does not monitor and assess the relationships that it has with other trading partners. As a point of reference, there are company policies and controls that if implemented can be the first line of defence to trading partners within an e-supply chain environment. Hence implementing systems that can expose vulnerabilities is something that is necessary in order for steps to be taken to provide tighter security measures.

For a long time, individual corporations have been conscious of the need to implement in-house risk assessment and risk management systems. Now with the globalisation of industries, companies today are restructuring themselves to function on a global scale and take advantage of the benefits that come with e-collaboration. This has resulted in companies working more closely together, resulting in a lot more information sharing between trading partners over the internet and a lot more criminal activity over the internet. Considering that an increased amount of criminal activity is taking place over the internet costing businesses millions of rands, there is a need for law enforcement to get more involved with the organisations that work in this environment to deal with the challenges they are facing more effectively. There is need for a security approach that can benefit both investigators and trading partners to assess the risk associated with companies sharing sensitive information with their trading partners across the internet (e-collaboration). Mentzer [7] acknowledges a great deal of literature on the security challenges associated with complex supply chains. However, there is a gap that exists between the current model for security implemented by most organisations conducting business over the internet and what is actually required from a digital forensics standpoint to provide a more secure environment.

To fulfil the aims of this research, key problems are identified in section 1.2. Research limitations are listed in section 1.3. In section 1.4 a motivation behind the reason why the stated problems are applicable is stated. Section 1.5 covers the objectives of this dissertation, outlining the tactics employed to solve the identified problems. Section 1.6 details the methodology that is implemented to meet the objectives of this research. Lastly, section 1.7 the overall layout of this dissertation is presented in section 1.7.

1.2 Problem Statement

Over the years supply chains have evolved alongside technological evolution, becoming more complex and vulnerable [4]. The complexity and vulnerability comes as a result of adopting of the internet and its infrastructure in the supply chain environment (e-supply chain), which exposes the supply chain to numerous threats. The implementation of weak non-versatile security systems that cannot meet the required amount of vigilance required in this fast-paced environment leads to many unidentified vulnerabilities and ineffective counter measures that affect both trading partners and digital forensic investigators [9]. Therefore, the *problem* that this dissertation addresses is that the complexity of e-supply chain network environments leaves trading partners vulnerable to security threats such as network breaches, asset failure and cyber-attacks. With insufficient digital forensic readiness measures in place security incidents become costly for trading partners and gathering sufficient digital evidence for analysis in a forensically sound manner becomes challenging and time consuming for digital forensic investigators. The list below outlines the sub problems that this research addresses:

- One sub-problem this research addresses is the lack of a standardised approach to digital forensic readiness (DFR) in e-supply chains. Organisations within a supply chain do not have DFR systems in place to prepare them for security incidents that might occur as a result of sharing information with other trading partners. There are so many sources where useful information can be collected, whether it is for a digital forensic investigation or for a risk analysis operation. An agreed-upon method to collect this information in a forensically sound manner and monitor the supply chain is lacking [132].
- Another sub-problem is that there is no clear security procedure to identify and combat threats across the supply chain e.g. between customer and supplier relationships and supplier's supplier relationships. Through e-collaboration trading partners within a supply chain share resources and services in the supply chain network. For big organisations, some responsibilities are outsourced to third parties, creating room for intruders to find their way into the supply chain network. According to de Crespigny, an Australian company “40 percent of the data-security breaches experienced by organizations arise from attacks on their suppliers”. Criminals are increasingly realising that this is a channel they can attack [9].
- The last sub-problem addressed in this research is the usability aspect of e-SC DFR tools. Most tools do not cater for a user-friendly interface for end-users to quickly scan through a visual timeline of an event, deeply interrogate the activity, and understand the context associated with each object [8]. Large amounts of unfiltered data are collected from different network access points and represented in a form that is too sophisticated for an ordinary person to understand; creating a need to improve the GUI, data search and filtering capabilities in DFR tools. Considering that an eSC is a distributed system, there is a need for DFR tools that can capture

potential digital evidence at different parts of the supply chain and store it in a central place, where collected data can be retrieved by digital forensic investigators or law enforcement, which would be readily available in the case of an enquiry.

1.3 Motivation

The field of e-supply chain risk assessment is relatively new, with not much attention being placed on the forensic readiness aspect. Several studies have indicated that an organisation can immensely improve its performance through online collaboration. It is believed that Dell could obtain \$43 million in potential annual savings through its "e-commerce and manufacturing initiatives" that would lower inventory held by their suppliers at Dell manufacturing facilities [10]. Which in many ways is certainly in the best interest of companies, but the level of risk that comes with online collaboration to a company has to be considered so that necessary extenuation strategies can be implemented. E-supply chain collaboration requires the exchange of all kinds of data between entities, some of it highly sensitive about customers and trading partners. With an increase in online collaboration within the supply chain environment, comes the potential aftermath of attacks that might result in data theft, compromised trading partner relationships and eventually financial loss. For an e-Supply chain network service provider, potentially losing a trading partner as a result of data corruption would have a negative impact on the service provider. Hence, it is important to identify and deal with the risks that come with this type of collaboration accordingly.

Compliance with regulations is also making the need to evaluate information security within firms a priority. Digital forensic readiness is a proactive process in digital forensics to monitor and collect potential digital evidence [11]. With that in mind, an integration of this process into the risk assessment approach creates an assessment process that can be supported in a court of law as it yields evidence. It is important to consider that risk assessment and forensic readiness can provide the supply chain with useful information that can be used to analyse and manage risk.

1.4 Objectives

The primary *objective* of this dissertation is to provide a risk mitigation approach that would be beneficial to both trading partners and digital forensic investigators. A proactive approach is required that can be implemented across an e-supply chain, to manage the risk caused by sharing information between trading partners. It has been indicated by Kunnathur and Vaithianathan [8] that a great deal of research has been conducted on different approaches to secure information within an organisation, but little attention has been placed upon the assessment of risk created by sharing information with trading partners within a supply chain. The main focus of this dissertation is to create an e-supply chain digital forensic readiness system (ESCDFRS) that identifies vulnerabilities in the supply chain, so that organisations are more prepared for any security risks associated the sharing of information in their eSC

environments. The ESCDFR system makes use of forensic readiness methods and techniques to identify information assets. Upon asset identification, useful information is collected that is used in the management of risk.

Such a system can be integrated within the eSC system to monitor the supply chain for threats, collect useful information that would aid the assessment process.

The proposed objectives of this research are:

- To examine relevant literature on digital forensic readiness and e-supply chains and laws regarding monitoring the supply chain.
- Develop an eSC-DFR process model.
- Develop a conceptual model of the ESCDFR system.
- Develop a proof of concept prototype of the ESCDFR system.
- Make use of a case study to determine the accuracy or usability of the ESCDFR system in a supply-chain environment.

1.5 Research Methodology

Research methodology is a way to systematically solve the research problem [12]. There are a few issues this dissertation addresses. The first issue is the lack of digital forensic readiness in the risk assessment process across an e-supply chain network. The second issue involves the large amounts of data to be analysed during the risk assessment process.

To address the above-mentioned issues, the following method is used. Extensively explore current literature on digital forensic readiness process models, some which include standardised models from ISO/IEC 27043 and ISO/IEC 27002 standards [71]. This is to review and identify fundamental concepts of the forensic readiness process derived from conceptual models. This is crucial in the development of an integrated e-supply chain digital forensic readiness process model.

- Develop a model based on the fundamental factors identified in the literature study to illustrate the e-supply chain digital forensic readiness system. A case scenario is used alongside activity models.
- Develop a prototype to prove the concept using applicable software development tools.

1.6 Dissertation Outline

Outlining a dissertation involves two main features, a summary of what is covered in the dissertation and a diagram that supports the summary.

In this dissertation, Chapter 1 starts off with an introduction that sets the scene, stating the main problem and sub problems that are addressed in this dissertation. After the problem statement has been stated, the main objectives of the research are stated. The research methodology is discussed and lastly an outline of the research is presented.

In Chapter Two, a literature review is carried out, giving some background on the digital forensics field as a whole and the role digital forensic readiness plays in the field. The techniques and tools that are used by digital forensic investigators for investigative and readiness purposes are also discussed in this chapter. Also included in this chapter are the definitions to frequently used terms such as digital forensics, digital forensic readiness, and digital evidence.

In Chapter Three, the term e-supply chain is defined, giving some insight as to the evolution of supply chains and how the internet has impacted on supply chains. Also included in this chapter is a description of the architecture and infrastructure that makes up the e-supply chain environment.

Chapter Four throws light on the challenges faced in e-supply chains regarding DFR and points out limitations to security infrastructure used in eSC network environments. In this chapter a literature review is carried out, that identifies the progress made by researchers in areas of digital forensics and the impact that digital forensics has on networked environments.

This leads to Chapter Five, where the concept of digital forensic readiness is introduced into the e-supply chain. This chapter presents the proposed standard approach for achieving DFR in eSC environments, presenting a process model that shows the processes that must be implemented to achieve DFR. A conceptual model of the ESC-DFR system is also proposed. This model outlines the architectural requirements, quality requirements and integrity of the system.

Chapter 6 gives a list of requirements that have to be met by an eSC-DFR system. Both functional and non-functional requirements are discussed.

In Chapter 7 an architectural design for an eSC-DFR system is presented and discussed. In Chapter 8 the prototype is described, followed by a demonstration of how the prototype created by the researcher works. In Chapter Nine the eSC-DFR system is critiqued, evaluated and analysed. In Chapter Ten the author takes a look at some related work and compares it with the contribution made in the current research and lastly a conclusion and summary of the entire dissertation is provided in Chapter Eleven, where future work is also addressed.

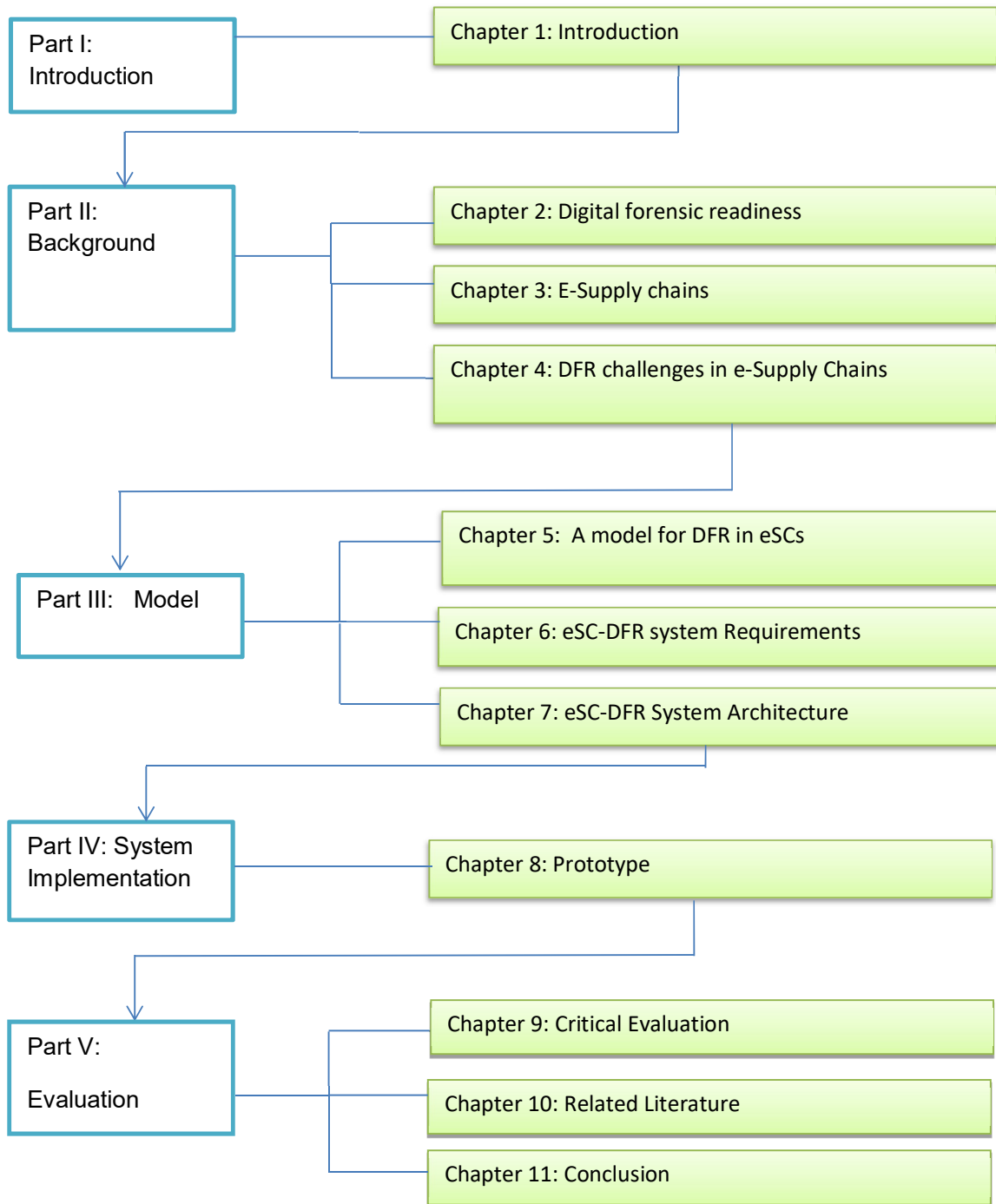


Figure 1. 1 Dissertation layout



1.7 Conclusion

In Chapter 1, the author introduced the problem and sub-problems that this research attempts to solve. Also discussed in this chapter were the motivation for conducting this research, the research objectives, the research limitations and lastly the layout of the dissertation.

Chapter 2

Digital forensics

2.1 Introduction

The field of digital forensics has grown rapidly over the years, becoming one of the leading fields in the world of information security as computer professionals and law makers attempt to keep up with the ever evolving world of computer technology. With the sudden bombardment of the market of different tools such as smart phones, tablets and mobile apps, the field of digital forensics has also had to grow and evolve. In the world of business, technology has come to the forefront providing businesses with tools and services that enable trading partners and consumers to conduct business more swiftly and quickly. Technology makes business ventures that were impossible, possible by providing services such as EFTs (electronic fund transfers), electronic mail and e-supply chains. Hence it is the role of forensic investigators to conduct the necessary investigations so as to combat crimes that might be committed in this digital environment. Digital forensic readiness (DFR) is a proactive digital forensics process that maximises the effectiveness of the reactive digital forensics processes by providing readily available potential digital evidence. Therefore, in this conducted research the main focus is on DFR. The ISO/IEC 27043 international standard [13] provides guidelines that cover idealised models for common investigation processes across many investigation scenarios which include processes for pre-incident preparation (forensic readiness). Therefore, in Chapter Two, the author discusses some of the processes. Next, the author defines digital forensics and discusses its processes, with main focus being placed on DFR.

In the following sections, the author defines digital forensics and zooms in on digital forensic readiness. Therefore the chapter gives a short review of current literature on digital forensics with much focus placed on digital forensic readiness, explaining the processes involved and some of the terms used. In the conclusion, a summary of what has been discussed here is given.

2.2 Digital Forensics Concepts and Definitions

Leigl and Krings [14] define digital forensics as the process of identifying, preserving and presenting digital evidence in a legally permissible manner. Digital forensics also referred to as computer forensics is a process that operates on clearly defined techniques to gather and preserve digital evidence from a particular digital device as supporting evidence in a court of law. The goal of this systematic process is to conduct a structured investigation that incorporates maintaining a well-documented line of digital evidence, to discover what activities were carried out on a digital device and by whom. Many notable crimes and investigations have leveraged digital forensics for key pieces of evidence. In many instances

the information provided by the digital forensics investigation was paramount to understanding key details. It is therefore, important that that standardised and formalised processes be followed for the sake of providing forensically sound evidence in a court of law. The Daubert case which took place in the United States has been an important point of reference for many countries, in which it was ruled that theories and techniques used to draw conclusions in a digital forensic case must result in positive answers to a number of questions, notably the question of whether the theories and techniques used during a digital forensic investigation are subject to standards governing their application [15]. Such a ruling indicated the need for a harmonised and standardised digital forensic process. Therefore, it is critical that standardised methods and techniques to acquire and investigate be implemented so that potential digital evidence (PDE) can be used in a court of law. PDE is defined as information and data of that might be of value to an investigation that is stored on, received or transmitted by an electronic device [25].

With the proliferation of technology in today's culture, digital evidence from computers, mobile phones, webservers, and intrusion detection technologies can provide critical evidence for an investigation of any kind. The terms digital forensics and computer forensics have been used interchangeably over the years by different authors but they basically refer to the same field, although the term digital forensics is used more regularly [16]. In order to bring some clarity as to why the term digital forensics is used more often than computer forensics (cyber forensics), it is important to recall that in the past; this type of forensic work was pretty much performed exclusively on computers, hence the term "computer forensics." As the types of devices expanded (phones, tablets, etc.), "digital forensics" became a more accurate label for the field. Therefore the term computer forensics is now called upon when referring to investigations that only have to do with computer systems that might provide digital evidence for crimes and the term digital forensics being used as the more generic term for the investigation and analysis of all digital systems [17]. As technology advances and new devices and information systems are developed the field of digital forensics also grows with new tools being built to keep up with these advances. The whole purpose of this field is to provide investigators with the best tools to combat any criminal activity executed on any new media that is developed.

Digital forensics can be defined more broadly as the analysis of information contained and created with computer systems and computing devices [18]. Typically, this occurs in the interest of four primary objectives, to determine what event took place, when an event happened, how an event happened and to possibly determine who were the parties involved. There can be wide-reaching purposes for this level of detailed analysis such as computer security incidents or to find out who is responsible for the misuse of a computer system, or perhaps who committed a crime using a computer system or against a computer system. The usage of digital forensics extends into theft of information or to provide extensive information in detailed timelines of computer activities that occurred on a computer.

This being the case digital forensic techniques and methodologies are commonly used for conducting digital investigations to determine the details of interest. In many instances, information that is gathered during a digital forensic investigation is not available or viewable by the average computer user. Examples of this kind of information would be deleted files and fragments of data that can be found in un-allocated areas of the hard drive. Therefore, unique skills and tools are needed to properly decipher this type of information for evidentiary value [19].

Digital forensics is considered the application of science to the identification, collection, examination and analysis of data whilst preserving the integrity of the information and maintaining a strict chain of custody for the data [25]. Therefore, a comprehensible forensic methodology that is repeatable and defensible is increasingly important to demonstrate conclusively the authenticity, credibility and reliability of the evidence. References of such a need were expressed in the Daubert ruling, where empirical testability, scientific falsifiability, reliability and validity of court evidence were raised [20].

The ISO/IEC 27043 standard provides established guidelines covering incident preparation and investigation, and will be discussed in the next section.

2.3 Digital forensics concurrent processes

Digital evidence can be the deciding factor in criminal, civil and corporate investigations. Technology often plays a role in data theft, employee compliance and policy violations, embezzlement, fraud and commercial disputes, just to name a few. With 98% of information created digitally, digital forensics can uncover critical pieces of information such as recovered communications and other electronic evidence[21]. It is therefore, the responsibility of forensic investigators to properly identify the relevant pieces of technology pertinent to an investigation, collect the evidence in a forensically sound manner, and ensure a proper chain of custody of evidence for admissibility into the courts and then to accurately examine and analyse the information.

The ISO/IEC 27043 standard (2015) provides processes that must be implemented for an effective DFI [7]. It is understood that some of the identified digital forensics processes are prerequisites for efficient digital investigations and if omitted, can create serious investigation delays and implementation issues. The ISO/IEC 27043 standard explains each process in detail for the benefit of law enforcement, digital forensic investigators and organisations implementing some form of IT. The digital forensics processes are discussed in the subsections that follow, showing their applicability in different types of investigations e.g. eSC environment. At a high level, all digital forensic investigation processes can be grouped into the following categories: readiness processes class, initialisation processes class, acquisition processes class, investigative processes class and concurrent processes[18] class as illustrated in Figure 2.1.

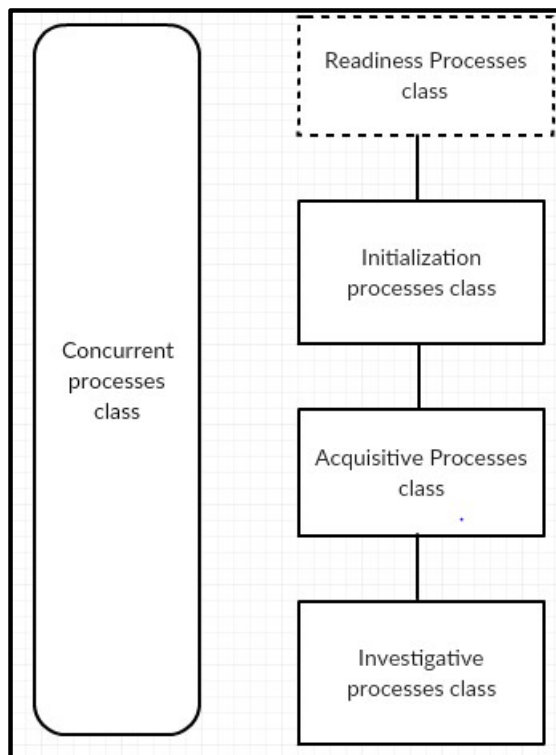


Figure 2. 1 the classes of the comprehensive harmonised digital forensic investigation process model[18].

In the subsections that follow, the author discusses the five classes of digital forensic investigation processes.

2.3.1 Readiness processes class

The readiness processes class deals with maximising an environment's ability to provide potential digital evidence. This class provides pre-incident investigation processes aimed at achieving DFI readiness within an environment [7]. Therefore, it is a proactive class of processes that handle the collection and preservation of potential digital evidence. This class of processes is critical because it also ensures that the information security aspect of potential digital evidence is taken care of i.e. securing the data with regard to its confidentiality, integrity and availability.

2.3.2 Initialisation processes class

Processes in the initialisation processes class are mainly concerned with incident detection, initial response, and lastly planning and preparation for the actual investigation[22]. This class of processes is critical to the effectiveness of an investigation.

2.3.3 Acquisition processes class

The foundation of digital forensics is to use a methodical approach to reach appropriate conclusions based on the available data or to determine that no conclusions can yet be drawn. Therefore, there has to be special attention placed on using effective methods to identify and acquire useful evidence[22]. The acquisition processes class deals with the acquisition of digital evidence which includes, incident scene documentation, digital evidence identification, digital evidence collection, transportation and storage[18]. This class of processes is very important because digital evidence is very delicate, hence special care needs to be taken to ensure that PDE is not compromised in its acquisition or is not lost in the process of acquiring it. In addition, special attention needs to be placed on identifying digital evidence to ensure that no PDE goes unnoticed. Secure transportation and storage processes are also very important in ensuring the information security aspect of the collected data is taken care of.

2.3.4 Investigative processes class

The investigative processes class deals with examining PDE to acquire digital evidence and produce a hypothesis about the events that resulted in an incident occurring. Much analysis of collected data takes place in this class and forms a train of events that would have taken place and relates those events with actual entities and events [22]. The end result is the reporting and presentation of investigation findings and investigation closure. Reporting is the phase of actually recording the results of the digital forensic analysis, which may include describing the actions used, explaining how tools and procedures were selected, or determining what other actions need to be performed. However, the primary purpose of the reporting is to provide the detailed conclusions with supporting evidence.

Once all the above-mentioned aspects are complete, the investigation is not complete until findings are properly disclosed to a client via electronic exhibits, written reports or proper verbal communication to ensure that the client has a complete understanding of the information.

2.3.5 Concurrent processes class

The concurrent processes class takes place simultaneously with all the above-mentioned classes. By definition concurrent processes are the principles that must be implemented throughout the DFI process[22]. This comes as a result of concurrent processes being applicable to many other processes within the digital forensic investigation process. These processes ensure that forensic principles are implemented in the investigative process, ensuring the effectiveness of a digital investigation.

It is important to note that there are many other processes that might make up a forensic investigation such as scene detection [23]. For the purpose of maintaining the context of this literature review only one investigation process is discussed.

The key to a successful forensic investigation is being prepared for an incident before it actually happens. This assists in the location and collection of solid digital evidence which may be presented in court during criminal proceedings[24]. Digital Forensic Readiness (DFR) is a proactive process that provides such tools that can assist in the preparation for incidents before they actually take place. By preparing for an incident, investigators are able to collect relevant information from different digital media that can be used to build a case. This concept is expounded in the next section.

2.4 Digital Forensic Readiness Defined

Due to the above-mentioned security issues and problems, there is a need to find ways to gather digital evidence in a forensically sound manner. DFR provides different techniques which can be used to address such issues.

Very often digital forensics is called upon in response to an information security incident or computer-related crime. Although that is what happens in most cases, there are many circumstances where DFR may benefit an organisation by providing the ability to gather and preserve digital evidence before an incident occurs [25]. DFR is defined as the capability of a system to efficiently collect valid digital evidence that can be used in a court of law [26]. This is an optional proactive operation in digital forensics with two main objectives, to minimise the cost of digital forensic investigations and to maximise an environment's ability to collect credible digital evidence. It is important for organisations to understand the crucial role that DFR plays in digital forensics in order to conduct successful forensic investigations. Rowlingson [25] makes it clear that the goals of forensic readiness are to gather admissible evidence legally and without interfering with business processes, to gather evidence targeting the potential crimes and disputes that may adversely impact on an organisation, to allow an investigation to proceed at a cost in proportion to the incident, to minimise interruption to the business from any investigation, and to ensure that evidence makes a positive impact on the outcome of any legal action.

DFR can provide many benefits to an organisation, such as collecting data from an organisation's information system in a network environment using log files, hence lowering investigation costs. Log files can be collected across a network's infrastructure, for instance at the servers, routers, e-mails and firewall. An organisation may therefore require access to potential evidence that will be able to support its position in the event an incident occurs. Thus many organisations have put in effect policies to ensure that digital evidence is available even before an incident occurs [25]. In a forensic readiness approach, this incident preparedness becomes a corporate goal and consists of those actions, technical and non-

technical, that maximise an organisation’s ability to use digital evidence. Any computer data may be used in a formal process and may need to be subject to forensic practices. The ability of an organisation to exploit this data is the focus of forensic readiness. Therefore DFR is the incident anticipation for an incident response.

There are many techniques to achieve DFR such as logging techniques, IDS data usage, forensic acquisition and evidence handling [26]. Most authors do not explain how these processes can be incorporated into a trading partners (TPs) security infrastructure to achieve DFR. By definition a trading partner refers to one of the two or more participants in an ongoing business relationship [19].

ISO/IEC 27043, which is an International Standard, outlines a three-step procedure to fully implement DFR [7]. The processes in this standard deal with setting up an organisation in a way that, if a digital investigation needs to be carried out, such an organisation has the ability to maximise its potential to use digital evidence; whilst minimising the time and costs incurred in an investigation.

According to ISO/IEC 27043, the three processes’ groups that make up DFR are: planning, implementation and implementation assessment as shown in Figure 2.2 below.

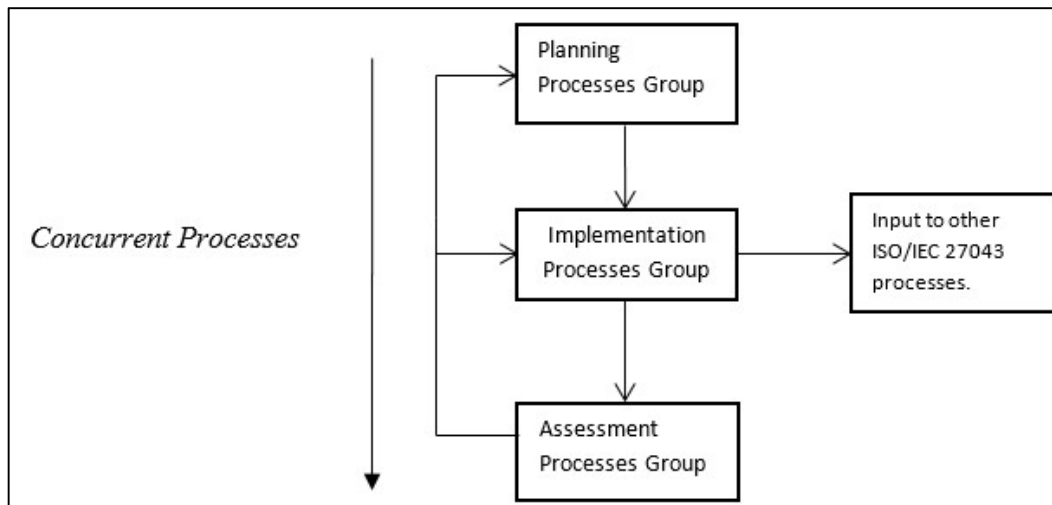


Figure 2. 2 Readiness processes groups

Figure 2.2 illustrates the order in which DFR processes take place, starting with the planning group which is concerned with the planning activities and the implementation group which includes readiness processes concerned with implementing the planned activities from the planning group. Lastly, the assessment group defines readiness processes which are concerned with the assessment of the success from the implementation process group. The processes groups are concurrent with other processes that are defined in ISO/IEC 27043 such as DFI; meaning that as DFR takes place, investigative processes

can be taking place as well. The data collected from the implementation of DFR in the e-supply chain can therefore be used as input to other processes in the ISO/IEC 27043 standard such as a DFI.

2.5 Digital Forensic Readiness Processes

According to the Oxford English Dictionary, a process is defined as “a series of actions or steps taken in order to achieve a particular end.” In digital forensics, a digital forensic readiness process consists of a number of steps or actions taken in order to maximise an environment’s ability to provide digital evidence[27]. As illustrated in Figure 2.1 the three forensic readiness processes include planning, implementation and assessment of planning and implementation processes.

2.5.1 Planning Process Group

Planning may be defined as a process of brainstorming and organising the activities required to achieve a desired outcome. In DFR, planning activities have to do with brainstorming, identifying potential data collection sources, planning data collection procedure, storing and handling of this data, planning incident detection and defining the system architecture [7].ISO/IEC 27043 (2015) mentions the key processes in the planning processes group that must be considered to ensure an effective DFR strategy, namely:

- Scenario Definition Process;
- Identification of Potential digital evidence sources process;
- Planning Pre-incident gathering, storage, and handling of data representing PDE process;
- Planning pre-incident analysis of data representing PDE process;
- Planning pre-incident detection process; and
- Defining system architecture process.

A. Scenario definition process

In the scenario definition process, all the probable scenarios where potential digital evidence might be found are examined to assess the risk that each identified scenario would pose. Such an assessment would also assist in identifying possible threats and vulnerabilities that would expose information assets. From the output of the process, one can decide on the necessary controls and systems to be implemented for DFR to be achieved.

B. Identification of potential digital evidence sources process

As the title indicates, the main objective of this process is to identify sources of potential digital evidence (PDE) e.g. access logs. For DFR to be effectively implemented, sources of PDE need to clearly be identified by the organisation. The output of this process enables the organisation to explore controls that will make the identified sources available.

C. Planning pre-incident gathering, storage, and handling of data representing the PDE process

In this process, activities for gathering, storing and handling PDE must be identified. The activities identified have to conform to digital investigation principles so as to ensure that the PDE is admissible in a court of law.

D. Planning pre-incident analysis of data representing PDE process

In this process, the procedures for pre-incident analysis of data representing potential digital evidence must be defined. These procedures assist in detecting incidents within a system. Therefore, the defined procedures must provide the exact information on how an incident is detected and what type of behaviour constitutes an incident.

E. Planning an incident detection process

In this process, actions that must be performed when an incident is detected are defined. The output from this process refers to the actions to be performed once an incident has been detected (information that must be passed on to the digital investigation process).

F. Defining system architecture process

In this process, the information system architecture that is to satisfy all the DFR requirements is defined. This refers to the organisational structure of an information system, application systems, computer equipment, communications network and related software.

All of the above-mentioned planning activities can be adopted and implemented as business requirements of an organisation. In the business world trading partners or service providers must follow the same planning activities to ensure that data is collected from the right data sources in the network environment so that it is stored in a secure manner to ensure its integrity. Rowlingson [25] mentions the different data that can be collected from a network environment such as log files, e-mails, back-up disks and network traffic records amongst others. This data can be useful in the case of forensic investigations or where it is needed as input to other processes. It is important to note that there are technical and non-technical actions, which maximise an organisation's ability to use digital evidence, for example Log-in authorisation controls. This relates to security policies and infrastructure that should be agreed upon and implemented before any communication takes place between trading partners (TPs).

The output of the planning process leads to the implementation of the planned steps. This means once the planning phase is complete, the information system of an organisation and the network architecture should be customised in a way that meets DFR requirements. This is with reference to the system architecture's ability to accommodate electronic storage and transportation of collected data.

2.5.2 Implementation Process Group

In the Implementation process, all the planned processes in the planning processes group must be implemented, including the defined system architecture [27]. This involves installation of new software, hardware and implementation of defined controls. It is therefore the responsibility of an organisation or service provider to ensure that all the planned activities are implemented accordingly. It is the role of service providers or an organisation to implement systems that support logging and storage of logged files in their information system or network environment. Logging has to do with recording of all data generated by a device such as a server, router, intrusion detection system, information hub or the data passing through a particular point in a networked computer system[28]. As part of the implementation process, security policies that support DFR are put in effect as well. This has to do with policies that govern network access and the collection of data. The DFR system architecture defined in the planning phase is implemented in this process. Data collection, storage, handling and integrity which are the main processes that enable DFR are implemented at this process.

Once DFR is fully implemented, there has to be a method to assess the effectiveness of the DFR process.

2.5.3 Assessment Process Group

An assessment is a set of processes that evaluate or estimate the nature, ability, or effectiveness of a method [7]. It is very important to be able to assess the effectiveness of the DFR process in an environment so as to be able to keep up with the ever changing ICT used in that environment. An assessment on the effectiveness of DFR enables entities to modify the DFR process, in-order to maximise its ability to capture useful information in that environment. It is also important to note that there are costs incurred in implementing DFR, therefore companies/service providers must plan strategically on how to implement DFR across the e-supply chain to achieve the best results from the process. ISO/IEC 27043 [27] indicates that to ensure DFR requires an assessment of the results obtained from the implementation process and comparing them to the aims for achieving DFR. The information collected from the assessment processes can be used to identify vulnerabilities within an information system and calculate risk. To ensure DFR across any environment, an assessment of the results from the implementation process should be performed to determine if the results meet the aims of achieving DFR. During this process recommendations are made on certain changes that might need to be made on the previous processes. Here entities decide on whether to go back to the planning process or implementation process, depending on the conclusions of the assessment process.

The three DFR processes outlined above make up the DFR process. For these processes to be impactful, it is necessary for those organisations to identify any forms of evidence that may be of value in a court of law. Therefore, in the next section the author elaborates further on digital evidence.

2.6 Digital Evidence

The use of computers to commit crime has resulted in plenty of digital evidence that can be used to apprehend and prosecute criminals. Therefore, it is basically up to an organisation to take advantage of the opportunities that DFR provides to gather such evidence. Digital evidence has been defined as any data that is stored or transmitted using a computer that support or oppose a theory of how an incident occurred [11]. Digital evidence is used to answer questions that have to do with what, who, where, how and when a crime took place. Therefore it comes in different forms e.g. timestamps, log files, data files, audio files, video files electronic documents. When it is broken down, digital evidence is just a sequence of binary values called bits. These bits if extracted correctly can provide insight into the activity of a criminal, whether it is on a local computer or on a network such as an e-supply chain. Therefore, it is highly critical that the integrity of such evidence not be compromised and presented in a logical comprehensible manner in a court of law.

Digital forensic evidence can be derived from many sources such as routers, firewalls, servers, monitoring software and logs just to name a few [25].

In the next section the author discusses current tools used for DFR purposes.

2.7 DFR tools

From reviewing the literature on DFR tools, it became apparent that there were no tools or software dedicated exclusively to the management of DFR. Therefore in this section the author discusses software or tools that are related to, but not dedicated to, the management of DFR. There are three types of software and systems that are directly related to the management of DFR, namely security event management software, intrusion detection systems and incident management software [18]. Therefore, each one of them is discussed below.

2.7.1 Incident Detection Systems

Incident detection systems (IDSs) enable the monitoring of events on computers and networks[29]. The main functions that an intrusion detection system provides are to monitor and analyse the events occurring in a computer system or network and raise an alarm if an intrusion is presumed to have occurred.

In the next section the author discusses security event managers.

2.7.2 Security Information and Event Management Software (SEIMs)

SIEMs also referred to as *security information and event managers* were developed due to the inability of intrusion detection systems (IDSs) to effectively filter real threats from false alarms [30]. Like IDSs,

SEIMs monitor events or data from multiple sources; however they also perform additional tasks. Reddy [18] lists the four main functions that all SEMs perform:

- *Log Consolidation*, which refers to the centralisation of logged data from different sources.
- *Threat Correlation*, in which artificial intelligence techniques are applied to sort through multiple logs and log entries in order to identify attackers or threats.
- *Incident Management*. This is where workflows are defined and stored to determine what happens once a threat is identified. Each workflow is a suggested path from the initial identification of a threat to the threat's containment or eradication.
- *Reporting*. Reports on the effectiveness and efficiency of the SEIMs have to be produced, as well as reports tailored for regulatory compliance and forensic investigations.

IDSs are different to SEIMs as they do not typically perform all the tasks listed by Swift above, SEIMs may in fact make use of IDSs to perform specific functions [30]. The real focus of SIEM systems is to provide real-time detection of threats created by network hardware and applications with examples such as Qradar by IBM and ArchSight that have been providing network security, preventing external threats and helping secure networked platforms from various threats [132].

In the next section the author discusses incident management software.

2.7.3 Incident Management Software

Within the information security (IS) domain, an incident may be defined as an identified occurrence of a system, service or network state indicating a possible breach of IS policy or failure of safeguards, or a previously unknown situation that may be relevant to security [16]. Incident management software facilitates the incident management process within an organisation, which amongst other things consists of, incident detection, classification, analysis/diagnosis and finally repair and recovery [18]. It does this by controlling the workflow involved in the incident management process. In order to do this the software also contains “incident records, escalation rules, information about customers and end users, and information about configuration items”[17]. Since both SEMs and incident management software suggest some or all of the workflow in the incident management process, there is an overlap of functionality between the two. SEMs, however, only deal with IS incidents while most dedicated incident management software deals with IT incidents in general. It is of course up to the organisation itself to determine whether they prefer to deal with IS incidents separately or whether they prefer to adopt a more unified approach.

2.8 Conclusion

In Chapter Two the author discussed the background on DFR. In it he defines the terms digital forensics and digital forensic readiness that are used numerous times in this dissertation. In this chapter the author also elaborates on the processes and techniques that make up the digital forensic readiness domain and discusses some technologies that are used in DFR. The next chapter, Chapter Three provides background information on the e-supply chain environment.

The main objective of this research is to apply DFR within an e-supply chain environment. Hence, the next chapter focuses on defining the e-supply chain network environment.

Chapter 3

E-Supply Chains

3.1 Introduction

The use of IT has impacted on business processes within a supply chain in a big way. Companies around the world have begun to appreciate the many benefits that come from using electronic technologies to collaborate and accomplish different tasks [31]. Collaborative business mandates that each entity within a supply chain must share both the gains and losses equitably and every entity must be able to share information with trading partners and customers in real-time [32]. Such networks are based on mutual trust, shared risk and shared rewards that would not be achieved if organisations operated independently. As technology advances, businesses are becoming heavily reliant on the internet for communication and collaboration. This has resulted in the development of multiple web-based solutions that facilitate interactions between businesses, one of them being the e-supply chain. Since this research is dedicated to addressing various issues surrounding the e-supply chain in relation to digital forensic readiness, the author has devoted this chapter to defining e-supply chains and discussing how they function, their processes and components

In this chapter the author provides background on the e-supply chain environment, starting off by defining the supply chain in section 3.2, followed by a discussion of essential e-supply chain design elements and the e-supply chain model in section 3.3. Lastly, the chapter is summarised in section 3.4.

3.2 Supply Chain

A supply chain is a system that comprises of various activities that are vital for the delivery of goods and services to customers. The globalisation of markets and advances in ICT has influenced new patterns of cooperation between companies in various industries to respond to e-business demands [19]. Activities range from product design to receiving orders, procuring product materials, receiving payment, marketing of products, manufacturing, logistics and customer service, just to name a few [1]. By definition, a supply chain is a system of organisations, people, technology, activities, information and resources involved in the design and movement of a product or service from supplier to customer [33].

The ability to manage this chain of interaction to optimise decisions is fast becoming a crucial competitive factor within a supply chain network. As a result, supply chains are increasingly becoming global and sophisticated in nature, allowing trading partners to share responsibilities [26]. Organisations have awakened to the many benefits that come from focusing on their main competencies and collaborating with other entities that have complementary strengths, resulting in an integrated supply

chain network. Some of the most noticeable benefits of such interactions have shortened transaction time, lowered costs for suppliers and provided better customer service for consumers [19]. Technology plays a crucial role in automating many supply chain processes and enabling such transactions and interactions between different trading partners within the supply chain environment to happen efficiently. Proof of this is seen in the development of web-based platforms for collaboration such as the e-supply chain. An e-supply chain is a web-based system made up of individual entities, often located in different geographical locations that form a strategic relation for the purpose of designing, manufacturing, and delivering quality products and services to customers efficiently [34]. Such relations are typically facilitated by web technologies for the smooth sailing of information between entities.

In the next section the author provides a more elaborate definition of an e-Supply chain.

3.3 E-Supply Chain system defined

E-supply chains have created a new trend for organisations to conduct business and interact, by digitally connecting organisations in different sectors of industry into supply chain networks of different sizes[35]. This interaction is facilitated by information and communications technology such as the internet and other web technology. E-supply chains (eSCs) are typically found in the energy, automobile, computer, food and apparel industry sectors, just to name a few. In such global industries, components may be fetched from one country, assembled in another country, and distributed to customers all over the world.

By definition, e-SCs are defined as an advancement of supply chains, with additional building blocks such as web technologies that contribute to an improved supply-chain relationship[36]. The internet overcomes the gap that has been there for business systems to be connected, providing a means to connect businesses all over the world. This success has out rightly had an impact on the manner in which businesses collaborate and compete; affording businesses the opportunity to reach new markets. Also traditional businesses have benefited from the new lease of life which is afforded by the automation of their activities and processes and also by remodelling existing supply-chain relationships into computer mediated collaboration in e-supply chains [32].

In order to improve the efficiency of partner relationships there are three elements that stand as the foundation for developing effective e-supply chains, namely visibility of information, supply-chain planning and workflow automation, all of which will be discussed in section 3.3.1. In section 3.3.2 a scenario is provided illustrating how an e-supply chain operates also discussing the e-supply chain model structure and its components.

3.3.1 E-supply chain essential elements

E-supply chains are designed through a systematic approach that considers the various levels at which ICT can be applied in a traditional supply chain environment to automate various processes [35]. This comes from the fact that over the years the internet has become a more interactive tool that allows applications not only to view data, but also to make active use of data.

Scenario: To illustrate how an e-supply chain operates, consider a supplier Jeff, who owns a massive warehouse in Johannesburg South Africa from which he sells all kinds of shoes under the brand name of Smiley Shoes. Jeff sells his shoes to many retailers across the country, a typical retailer of Jeff being John who owns Bunnylux Shoes, where he sells Jeff's shoes in the retail store and on the website. Like many retail stores, Bunnylux Shoes have limited space to sell all of Jeff's shoes, hence the Business Connect network. The Business Connect (eSC network) network in this scenario allows retailers to overcome their limited space and sell all the products available to them by their suppliers. The BusinessConnect network is a solution that automates product catalogue, transaction automation and selling tools. Using the BusinessConnect work is easy. Jeff can enter or input inventory data into the BusinessConnect included software and set the product catalogue data. Once ready, he can publish the catalogue on the BusinessConnect network. Once Jeff's catalogue is published, retailers like John can apply to sell Jeff's products on their webstores and in return Jeff can approve and set the pricing of the products. With Jeff's approval, John can download the product catalogue directly into his included kiosk in the website software and start selling Jeff's shoes. When a consumer orders Jeff's products on the Bunnylux Shoes website, the BusinessConnect network will automatically send the order to Jeff's system for fulfilment. Jeff can fulfil orders and make shipping arrangements using the connected warehouse module/ desktop software. As orders are fulfilled, shipment tracking data and invoices are automatically sent to John. This allows John's customers to track their orders online and allows Bunnylux Shoes to easily make payments to Jeff. An eSC network can automate the entire process, driving down consumption-related costs, allowing both the retailer and supplier to grow their business with minimal cost and effort.

What has been noticed over the years is that as internet tools become more interactive, business systems have also evolved from supplier-centric to customer-centric systems [37]. Supplier-centric systems require little integration between information systems within a supply chain. This is where a trading partner (T1) can go directly to the website of another trading partner (T2) and find out information about a product and purchase it from T2's website, without the T1's business system being integrated to the T2's system. In a customer-centric system, most processes are automated between partners and business systems linked for the convenience of a customer. Therefore, there is a higher level of integration between partners. For example, the supplier might supply a component that automatically updates the retailer's system whenever an order status changes allowing a retailer to deal better with

issues like inventory shortages. It is therefore very important that the information sharing activities between partners be explicitly defined to automate some of the supply-chain processes (Visibility of information) [38].

It is important to note that the purpose of incorporating ICT in supply chains is to make them more efficient. Therefore three elements for efficient e-supply chain design were defined; namely visibility, workflow automation and planning, each of which are discussed in the next section.

Visibility of information focuses on automating the communication processes between partners within a supply chain. Communication technologies such as the Internet and other technologies such as XML Java and WAP amongst others have made the sharing of information seamless [37]. The ordering and purchasing of goods is now an instantly available service between partners, which would have taken minutes or hours and even days in the past. The formation of *information hubs* in the e-supply chain environment has addressed many of the shortcomings of previous systems. This is with regard to previous systems such as electronic data interface (EDI) which require dedicated links between each supply chain trading partner (TP), relationships cannot be created dynamically with new TPs when consumer requirements demand so and are very expensive to maintain [35]. An information hub is defined as a web-based system, such as a website, which facilitates and encourages buying and selling to induce collaboration among trading partners across a selection of industries [39]. In an e-supply chain information hub, buyers and sellers gather together in a virtual environment to transact in goods, services and information through web-based search, negotiation and collaboration tools. Therefore the visibility element focuses on the identification of all e-supply chain business processes, where information is shared between partners leading to the automation of those processes.

Workflow Automation is the second essential element for e-supply chain efficiency. Work flow automation tools build upon the visibility building block in a supply chain [40]. These tools automate many of the interactions between trading partners by utilising the visibility within the e-supply chain. Examples of some workflow automation tools are the track and trace tools and electronic procurement. Track and trace services usually provided by logistics companies process the information related to the fulfilment of a particular product in order to provide the latest status report on the location and condition of the product[41]. This also includes track and trace of work in progress. As for electronic procurement, some e-supply chains automate the entire procurement process for large organisations. Electronic procurement tools incorporate electronic catalogues from different suppliers and make interaction with all of them cost effective.

Supply chain Planning enforces the automated movement of information within an e-supply chain environment[35]. Planning tools incorporate a much greater degree of efficiency in the e-supply chain through intelligent design support; hence the effectiveness of the visibility and workflow automation

elements can be fully harnessed. Supply chain visibility and workflow automation provide significant savings and tremendous opportunities to trading partners, but their true ability can only be recognised when accompanied by intelligent decision-support tools [39]; tools that optimise the automated movement of materials based on the information available from supply chain visibility. Such an automated and optimised process will lead to lower inventory levels and greater asset utilisation while meeting customer requirements. As a result these planning tools incorporate a much greater degree of efficiency in the operation of the supply chain. In terms of supply chain excellence through planning the ultimate goal is the synchronisation of all the activities right from the raw material supplier to the final delivery to the customer [42]. This is achieved through solutions, which optimise scheduling of activities on a global level.

With the above elements considered, the e-supply chain environment becomes an essential tool for many companies.

In the next section the author discusses the e-supply chain network at technical level, discussing its components as illustrated in Figure 3.

3.3.2 E-Supply chain model

With the e-supply chain building blocks defined, in this section the author focuses on the components that make up the e-supply chain network. An eSC network is achieved through integration of the information systems of all supply chain partners (distributed network) [37]. These partners can be referred to as hosts that are connected to a central point known as an information hub over the internet using middleware components. The incorporation of ICT in the supply-chain environment has caused a shift from a linear supply-chain structure to a more circular star e-supply-chain structure; where trading partners and customers share information and services through a central point known as an information hub as illustrated in Figure 3 below.

An information hub is defined as a web-based system, such as a website, which facilitates and encourages buying and selling to induce collaboration among trading partners across a selection of industries [19]. Figure 3 below shows a top level e-supply-chain model structure, where trading partners (TP) share information and services through a central point known as an information hub. E-supply chain systems make use of software, middleware and hardware infrastructure that works together to facilitate the smooth operation of business processes between trading partners. The structure of the distributed e-supply chain network is presented below in Figure 3.

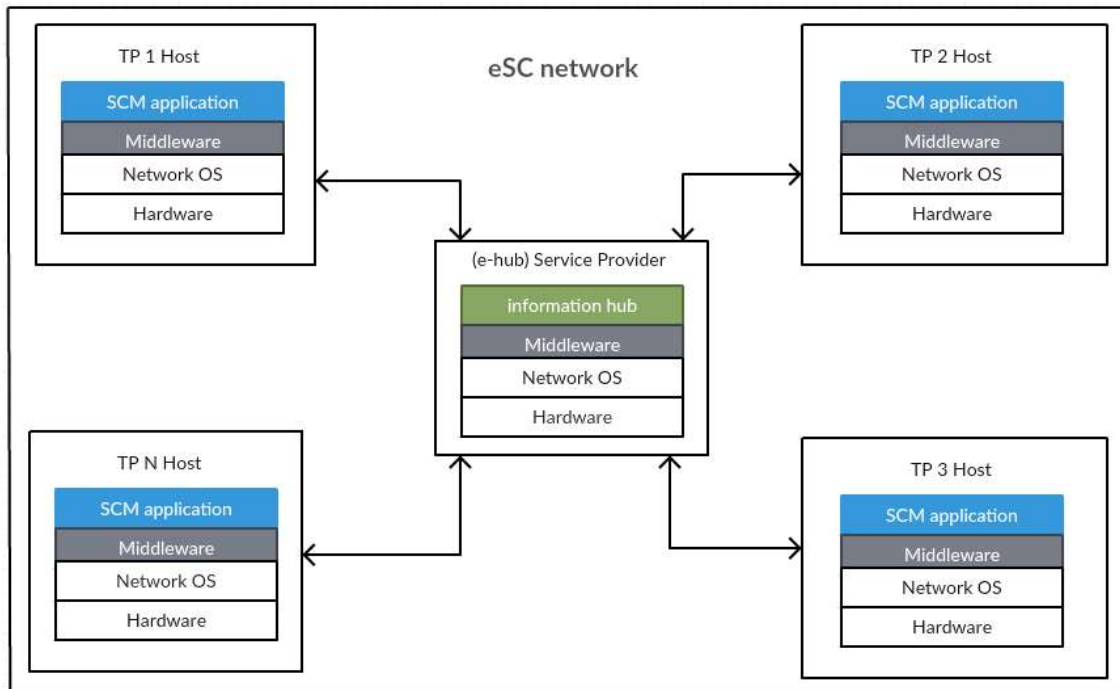


Figure 3.1 E-supply chain Structure

Software components such as Supply-chain management (SCM) applications provide both internal and external services to trading partners and an integrated view of core business processes [43]. These software components, in conjunction with the internet and web services, provide an entry point for an enterprise to access information from other trading partners. All SCM software applications are ready-made package applications usually designed to deal with specific tasks e.g. the online inventory management process between supplier and client. These ready-made software applications are mass-customised for specific markets and industries. From the data management point of view e-supply chain software can be organised into two categories: transactional and analytical software applications [42]. Transactional software applications provide services that are concerned with acquiring, processing and communicating raw data about a partner's supply chain network interactions with other partners. Analytical software applications focus on developing and applying systems for evaluating and disseminating decisions based on e-supply chain decision databases. Examples would be forecast systems or production scheduling systems, just to mention a few.

Middleware components, such as application servers and content management systems, are computer software that supports enterprise application integration (EAI). Middleware can be defined as programs that provide messaging services, which include enterprise-application integration, data integration, links between database systems and webservers in the eSC. This is systems software that resides between the applications and the operating systems, network protocol stacks and hardware [44]. The role of middleware software is to bridge the gap between applications and the lower-level hardware and

software infrastructure in order to coordinate how applications are connected and how they interact. Such middleware components if implemented properly can help to shield software developers from low-level and error prone platform details and assist in providing developer-oriented services such as logging and security services that are necessary in a network environment [37].

Hardware components create a communication link between each trading partner in the eSC for the transmission and processing of data. Examples of hardware components include PCs, mobile computers, routers, switchboards and servers just to mention a few, all of which are vulnerable to IT-specific threats. From Figure 3 above, the different components that make up an eSC environment are illustrated at a high level. The Figure illustrates the structure of an eSC and how the internal infrastructure of a trading partner (TP) interacts with the information hub that facilitates interactions with other trading partners' internal systems via internet-based protocols [12].

3.4 Conclusion

In this chapter focus has been placed on introducing the e-supply chain environment and its various components. As mentioned before, e-supply chains are built upon software, middleware and hardware components that work together to automate and facilitate supply-chain business processes. Smith [2] in an article points out that the benefits of interconnectivity of businesses are not gained without risk, as IT removes protective barriers around assets and processes. Thus, e-supply chains are better able to satisfy customer needs and yet are more vulnerable to security incidents due to an array of threats. Greater levels of collaboration expose significantly more sensitive information to potential risk, suggesting that a greater emphasis should be placed on information security. This call for increased scrutiny in the area of e-supply chain information security has been widely echoed in literature [45-47]. Therefore in the next chapter, the author discusses the security challenges faced in the e-supply chain environment.

Chapter 4

DFR challenges in e-supply chains

4.1 Introduction

It is needless to say that with advances in information technology, particularly in Internet technologies within supply chains, new avenues for crime to be committed are created. This poses a challenge for eSC service providers and digital forensic investigators to improve the information security infrastructure across e-supply chains to prevent and respond to security incidents. Many organisations have reaped the benefits of adopting the e-supply chain (eSC) model, but have also faced the challenges that it comes with. One such major challenge is information security. The integration of information systems to facilitate business processes within supply chain environment creates new avenues malicious individuals to commit crimes within such environments. Digital forensic readiness (DFR) is a relatively new exciting field which can prepare eSC trading partners from a policy standpoint as well as a technical position for cyber incidents; providing digital forensic investigators with forensically sound information if implemented strategically. With the current state of cybercrime in eSC environments, system developers and client service providers (CSPs) are challenged with the task of implementing effective security policies and digital forensic readiness solutions that can keep up with current cyber threats and technological advancements. Therefore Chapter Four is devoted to unveiling the state of DFR in the e-supply chain environment and also to discuss the limitations of current monitoring systems from a DFR perspective.

Therefore this chapter is structured as follows: Section 4.2 defines the state of DFR in eSCs by providing some background. Section 4.3 lists the limitations of current DFR tools and further elaborates on each limitation. A conclusion is presented in section 4.4.

4.2 DFR in e-Supply Chains

E-supply chain forensic readiness is concerned with the application of forensic readiness processes, techniques and security infrastructure that ensure that eSC environments are forensically ready before incidents occur, providing many benefits to law enforcement, digital forensic investigators and trading partners. Richard [48] mentions that at some point preventative measures fail, hence the need to develop strategies to collect information needed to recover from future incidents. It is important to mention that this does not mean prevention efforts should be abandoned, just complemented with readiness processes. The ISO/IEC 27043 provides a clear strategy to accomplish DFR, which is the blueprint for this research. In e-supply chains, communication networks are used to share enterprise information, maintain strong relationships with trading partners and conduct enterprise transactions through the use

of the Internet [49]. Trading partners use network infrastructure to share resources and information, these resources include servers, databases and other hardware. It is in the e-supply chain network environment where e-supply chain security is compromised with threats that include network sniffing, packet spoofing, interface intrusion, denial of service attacks, wide-scale Trojan distribution, anti-forensic techniques and a wide-scale use of worms, just to name a few trending cyber security threats [50].

Casey [11] indicates that network security breaches are both complex and costly. Part of the reason is that organisations are usually ill-prepared due to a lack of security infrastructure and processes that can prepare them for such incidents. Many researchers have conducted research on security solutions to prevent an incident from occurring such as firewalls, virus scans and intrusion detection software, amongst others. However, to date, there has been no presentation of an approach to prepare trading partners for threats and gather useful information in the e-supply chain that can be used to identify vulnerabilities across the e-supply chain. Ayers[51] indicates that current digital forensic tools are not keeping up with the increased complexity and data volumes of modern investigations and insists that the existing architecture of first-generation computer forensics tools is rapidly becoming out-dated. Developments in today's networks, which support both internal and external business processes, call for cutting edge DFR tools that can assist in the collection, storage and retrieval of potential evidence in a forensically sound manner. By means of thorough research on DFR tools, what has been noticed is that there are no DFR tools that are designed to support eSCs specifically.

With all the technological advancements that have occurred over the years in eSCs, there has been very little focus on the implementation of digital forensic readiness within this environment. The EnCase forensic tool and the Forensic Tool Kit (FTK) application, which are the two industry-standard digital forensic analysis tools for digital forensic investigations, do not incorporate digital forensic readiness properties in their specifications[52]. Therefore, the role of a DFR tool in an eSC environment would be to gather such evidence from the eSC network environment and store it in a forensically-sound manner. A digital forensic investigator may therefore require access to potential evidence that will be able to support its position, in the event that an incident occurs. Unfortunately, the current variety of DFR tools does not support forensic readiness processes that maximise the eSC's ability to provide digital forensic evidence. Therefore, in the next section, the author reviews some limitations that such tools exhibit.

4.3 Limitations of current DFR tools

A considerable amount of research has been conducted on the adoption of DFR processes in different network environments. Unfortunately there has not been adequate attention given towards the

development of eSC-DFR tools. It is in this chapter that the author identified a number of limitations concerning DFR tools in the eSC category. Limitations include:

- Limited throughput for data capturing devices.
- Poor Usability.
- Compromised Privacy and limited filtering of packets.
- No technical support.
- Centralising the storage of data captured in a distributed network for data retrieval.
- Software errors.

Each of these limitations is elaborated upon in the sections to follow.

4.3.1 Limited throughput for data capturing devices

Due to a tremendous increase in network traffic over the years, current DFR tools are struggling to keep pace with network traffic speeds. These tools cannot capture 100% of network traffic data at higher speeds. Tscheper [60] gives an illustration of the problem, stating that two end-users reaching maximum throughput, talking at gigabit (1000Mbps) speed in full duplex mode (i.e. they can send and receive data at the same time) will generate an aggregate throughput of close to 2000Mbps. The data capturing device would most likely be limited to 1000Mbps, causing a loss of half the data to be monitored if full throughput is occurring. In a typical data transmission scenario, the endpoints are only concerned with packets that are associated with their conversation. Other packets sharing the same connection are simply filtered out. It is the view of the author that in a data capturing scenario on the other hand, interest is in the ability of a DFR system to capture all the packets traversing the point being logged. For an investigation to be successful, every packet needs to be captured. This means that packet loss is unacceptable because a missing packet could be the key to solving a digital forensic investigation.

4.3.2 Poor Usability

Most DFR tools do not provide a user-friendly interface for end-users to quickly scan through a visual timeline of an event, deeply interrogate the activity, and understand the context associated with each object [53]. Large amounts of unfiltered data are collected from different network access points and represented in a form that is too sophisticated for an ordinary person to understand; creating a need to improve the GUI, data search and filtering capabilities in DFR tools. Due to a significant escalation in digital crime, law enforcement agents, trading partners and forensic investigators need swift access to potential digital forensic evidence, presented to them in a structure that is easy to comprehend. Most DFR tools struggle to provide an interface that enables users to quickly and efficiently scan through a visual timeline of an event, deeply interrogate the activity, and understand the context associated with each object. Therefore there is a need to improve user-interface, data search and filtering capabilities in

DFR tools. Considering that an eSC is a distributed system, there is a need for DFR tools that can capture potential digital evidence at different parts of the supply chain and store it in a central place, where collected data can be retrieved by digital forensic investigators or law enforcement, which would be readily available in the case of an enquiry.

4.3.3 Compromised Privacy and limited filtering of packets

Packet sniffing and filtering has its drawbacks [54]. Firstly, only limited filtering on packets received is carried out, resulting in massive post processing. Secondly, no filtering is done based on the packet payload content (which is the critical data that is carried within a packet or other transmission unit). Lastly, as the entire data is dumped into a central database, the privacy of innocent individuals who may be communicating during the time of monitoring may be violated. Therefore, access to captured eSC data is not restricted to relevant potential evidence and relevant parties. In this information society, privacy of digital evidence is critical. Most DF tools do not provide adequate security measures to ensure strictly controlled access to potential evidence, therefore leading to compromised digital evidence [55]. For log data to be considered as evidence it must meet a number of legal requirements that have to do with the architecture and the cryptographic operations used to gather and secure log data. Whilst much attention is placed on mechanisms to collect log data, not much attention is placed on protecting the log data [56]. As a result, system engineers are often confused by the jargon used to define the legal requirements for evidence admissibility. Moreover, since requirements are not completely clear, there is a mismatch between what has to be offered and what a particular logging protocol in fact fulfils. Such a mismatch has a fatal implication: more often than not, digital evidence gained from log data loses on probative force or it is not admissible in the first place [57].

4.3.4 No technical support

Commercial Digital forensics tools that offer technical support are generally costly, making it difficult for small- to medium-sized enterprises (SMEs) to purchase them [51]. On the other hand, open-source network monitoring tools are very often difficult to use as they do not provide technical support and the ability to gain insight into their inner workings. The validity and trustworthiness of digital evidence is an essential part of digital forensics. This calls for the validity of a DFR tool to verify that tools meet the requirements of a digital forensics tool. Guo [58] mentions that the growth of the digital forensics field has created a need for new tools with increased functionality and a means to verify that the tools meet the requirements of a digital forensics tool. Unfortunately DFR tools rarely provide detailed logging or debugging information that would allow investigators to validate the operation of a tool with respect to data collected [51]. This is critical because without collected data being validated as evidence in court, it cannot be used to acquit or condemn an individual or organisation.

4.3.5 Software errors

Software errors continue to pose a challenge for tool developers. Ayers[51] mentions that analysts and other digital forensics tool users are often faced with the problem of unexplained crashes that lead to disruption and often loss of data. These seem to be caused by a combination of factors such as, design errors in tools, a lack of high integrity software development practices within the tool developers and a desire driven by commercial imperatives to deliver new features to market as quickly as possible. Carrier[59] also mentions that there have been incidents where forensic tools have malfunctioned, capturing or interpreting evidential data incorrectly. Such situations could cost organisations millions of dollars. Hence such software crashes continue to be a significant concern for analysts and improvements to the robustness of forensic tools are crucial for this reason alone.

This chapter seeks to introduce the DFR concerns that are faced in eSC environments and provide insight into possible implications of the limitations of current DFR tools. As mentioned in the problem statement DFR is a fairly new concept that many different network platforms are slowly getting familiar with and as a result there is much work needed in implementing its processes efficiently, following the ISO/IEC 27043 standard.

4.4 Conclusion

Existing general purpose DFR tools are rapidly becoming inadequate for modern commercial network systems (eSCs). The out-dated architecture of such tools limits their ability to scale and adopt the current and future eSC forensic readiness processes. In the recent past, researchers have cited the need for more capable DFR tools that can support digital forensic investigations in the event an incident occurs. As much as these are steps in the right direction, implementing security policies and processes alone does not ensure that the eSC environment is fully forensically ready. Chapter Four briefly highlighted some of the limitations of current DFR tools in the eSC environment and the repercussions of such limitations.

These concerns need to be kept in mind when in the next chapter requirements for an eSC-DFR system are proposed that ensure that DFR is implemented in an eSC according to the processes and methods defined in the ISO/IEC 27043 standard.

Chapter 5

A model for Digital forensic readiness in eSCs

5.1 Introduction

Up to this point, the preceding chapters have presented background information on the issues faced in the e-supply chain (eSC) environment with regard to digital forensic readiness (DFR), especially regarding a lack of digital forensic readiness tools that are specifically designed for the eSC environment. DFR tools that can capture forensically sound potential digital evidence (PDE) from across an eSC environment and store it in a secure centralised data repository where authenticated users such as law enforcement (LE) agents and digital forensic investigators (DFI) can retrieve this potential digital evidence (PDE) for analysis. This chapter shows how DFR can be implemented in the eSC environment by adopting processes and techniques provided by the ISO/IEC 27043 standard that can enhance the ability of an eSC environment to provide readily available PDE (DFR). Many researchers have conducted research on security solutions to prevent incidents from occurring such as firewalls, virus scans and intrusion detection software, amongst others. However, to date there has been no presentation of an approach to prepare e-supply chain trading partners for security threats and to gather useful information in the eSC that can be used by authorised parties to identify vulnerabilities across the supply chain.

Digital forensic readiness offers a data collection framework that has vast capabilities to obtain potentially useful information that can be used for many purposes including Digital forensic investigations (DFIs). Hence in the next section the author discusses the methodology for achieving DFR in the eSC environment which follows a number of identified DFR processes that are separated into three respective groups as proposed by ISO/IEC 27043 in Chapter Two. Sections 5.2.1, 5.2.2 and 5.2.3 discuss the processes identified for each process group respectively in more detail to give the reader a clear understanding of the processes involved to achieve DFR in the eSC environment; these will be followed in this dissertation. In section 5.3, a process model which encompasses all the identified eSC-DFR processes is presented and discussed. Section 5.4 introduces a conceptual model that supports the proposed eSC-DFR process model, showing where the identified processes from the process model take place in the eSC network. To support the concept, a scenario is also included in section 5.5 to illustrate how such a system can have an impact within an eSC network. The chapter is summarised in section 5.6.

5.2 Proposed Methodology for eSC-DFR

In this section the methodology that is used to achieve DFR is discussed. As mentioned earlier in Chapter Two, DFR provides processes and techniques that if adopted can ensure that an environment is forensically ready providing readily available potential digital evidence (PDE) [60]. Therefore, for the purpose of this dissertation, the researcher follows the ISO/IEC 27043 DFR process model as a blueprint for the development of an eSC-DFR process model, which splits the forensic readiness processes into three groups; namely the planning processes group, implementation processes group and assessment of implementation processes group. It is in the author's opinion that the splitting of DFR processes into three categories as illustrated in Chapter Two indeed helps to identify processes that are relevant for achieving DFR in the eSC environment and clearly defines the order in which processes must be executed. Therefore this dissertation follows the order of events which are proposed in ISO/IEC 27043 in the following chapters to plan, implement and assess a proposed eSC-DFR solution. The identified processes must be utilised in three ways as indicated by the grouping of processes.

The first process group, i.e. the planning processes group, involves the planning and designing of an eSC DFR system architecture for this environment [48]. The second process group, i.e. the implementation processes group, targets the implementation of eSC-DFR system architecture in the eSC environment to achieve forensic readiness. The last group, i.e. the assessment of implementation processes group basically focuses on the assessment/evaluation of the effectiveness of the implemented solution/system to identify adjustments that need to be made in the implemented architecture for maximum performance. In the following sub-sections the author elaborates on each of these process groups, discussing the identified processes that are applicable to the eSC-DFR process and how they relate to the eSC-DFR conceptual model.

5.2.1 Planning processes group for DFR in E-supply chains

Planning may be defined as a process of brainstorming and organising the activities required to achieve a desired outcome [61]. In the eSC-DFR process model, the planning processes group presents the critical processes required to achieve DFR in the eSC environment. Figure 5.1 presents the critical DFR planning processes identified by the researcher for the eSC environment.

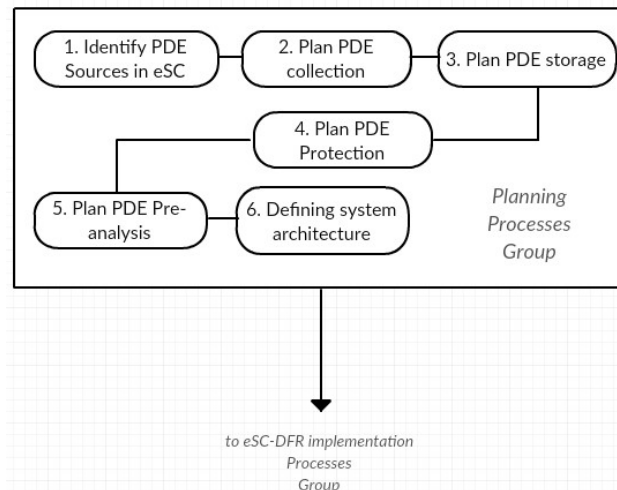


Figure 5. 1 eSC-DFR planning processes group

As indicated in Figure 5.1, planning activities have to do with identifying potential data collection sources, planning PDE collection, storage, protection, pre-analysis and lastly defining the system architecture for an eSC-DFR solution. The following sub-sections elaborate on each eSC-DFR planning process.

5.2.1.1 Identify PDE sources

Identifying sources of potential evidence is a crucial step in the DFR process. Rowlingson [9] mentions that the purpose of this process is to identify what evidence is available across an entire system or application for collection. For the purpose of this research the role of process no. 1 is to identify the different types of potential digital evidence that may be available across an e-supply chain network and where it may be located. Examples of data sources in an eSC system include servers, firewalls and application software [62].

5.2.1.2 Planning data collection

After identifying PDE sources, it is up to the eSC service provider to decide which of the identified sources of PDE is worth pursuing to collect PDE and which methods will be considered to gather this evidence. There are a number of issues that must be considered during this process, such as how to acquire digital evidence without interfering with business processes, the legality behind collecting this data, size of collected data, and the costs involved [9]. All which have an impact of the effectiveness of the DFR process in an eSC.

5.2.1.3 Plan PDE storage

Upon collecting PDE, the next issue of concern is the storage of the collected PDE. It is the author's opinion that there are a number of issues that arise when considering the storage of gathered digital evidence, such as the security factor and the size of storage factor. An eSC handles sensitive company

data such as client records, business transactions and other sensitive trading partner information hence it is important to ensure that gathered information is kept secure from unauthorised parties. Also it is important to consider efficient ways of storing large amounts of PDE that is captured across the eSC.

5.2.1.4 Plan PDE Protection

This process's main focus is ensuring that the integrity of captured PDE is not compromised. The eSC is a web-based system hence there are many ways for intruders to try to access and either steal or corrupt PDE. Therefore, it important to consider methods of protecting captured data from potential threats through the deployment of certain security measures such as encryption and password protection. It is necessary to ensure that once data is collected or stored in a data repository, its integrity is maintained and it can be used in a useful way. This also involves considering measures to assess the authenticity of captured data to ensure that at all times there is proof that the PDE has not been tampered with e.g hashing. Therefore content management policies and systems have to be looked into to identify specific policy measures that can be implemented in the eSC to ensure captured data is secure and can be used in a useful manner.

5.2.1.5 Plan PDE pre-analysis

Once data is collected and stored in a secure database, there are elements that have to be considered to identify what can be done with the collected data, such as presenting it in a manner that makes it easy to trace events for law enforcement and forensic investigators. Therefore within the design of eSC-DFR tools that operate within the eSC environment, developers should consider all the scenarios in which collected data could be useful and design systems that can perform certain pre-analysis functions, such as categorising different types of PDR.

5.2.1.6 Defining system architecture

With all the above-mentioned factors considered, process number 6 has to do with designing a system that incorporates all the planned DFR processes, from the security aspect to the usability aspect of an eSC-DFR system. This has to do with defining the architecture and behaviour of a system that implements the DFR solutions that come from all the above-mentioned planning processes [63].

Trading partners (TPs) or service providers must follow the same planning activities to ensure that forensically sound data is collected from the right data sources in the eSC network environment and certain legal aspects are considered. This data can be useful in the case of forensic investigations or where it is needed as input to other processes.

An outcome of the planning process group must be the defined system architecture for an e-supply chain DFR system. This means once the planning phase is complete, e-supply chain system architecture should be customised in a way that meets DFR requirements. This is with reference to the system

architecture’s ability to meet judicial requirements, accommodating data collection across the network, meeting security requirements, and finally, transportation and electronic storage of collected data within the e-supply chain.

5.2.2 Implementation processes group for DFR in E-supply chains

In the Implementation processes group, defined system architecture is implemented. This involves the incorporation identified DFR policies and DFR infrastructure i.e. software, middleware and hardware. It is the responsibility of each enterprise in the e-supply chain or eSC service provider to ensure that all planned DFR activities are implemented across the e-supply chain. It is in the implementation processes group where the eSC-DFR tools/systems are developed and implemented. E-supply chain service providers are to develop and implement systems that support data collection and storage of collected potential digital evidence as mentioned previously.

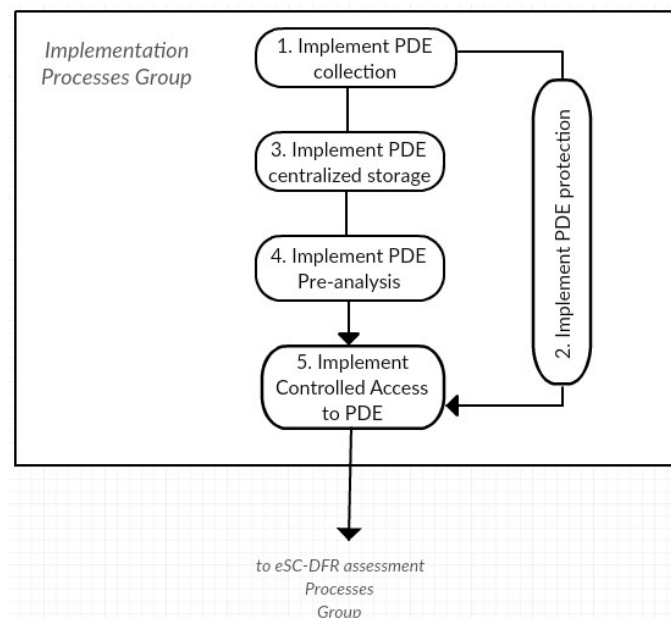


Figure 5. 2 eSC-DFR implementation processes

Figure 5.2 shows the DFR processes that must be implemented by an e-supply chain DFR system. The implementation of all planned activities takes place at this processes group. These include data collection, PDE handling, and centralised storage of collected data, security measures to protect data from criminals, incorporating some pre-analysis properties in eSC-DFR tools and monitoring access to captured information. Rowlingson [25] categorises DFR security policies that must be considered in a forensic readiness implementation, namely as security policies that assist in:

- Preserving potential digital evidence.
- Preparing for incident response.

- Training users.
- Speeding up the Investigation.
- Prohibiting anonymous activities.

The mentioned policies are to be considered in the planning processes group, as they would have an impact on the design of the implemented e-supply chain digital forensic readiness system (eSC-DFR system). The system architecture defined in the planning phase is implemented in the implementation processes group defined in the Figure 5.1. Data collection, storage, handling and integrity, which are the main processes that enable DFR must be implemented across the e-supply chain at this process. The following sub-sections elaborate on each eSC-DFR implementation process.

5.2.2.1 Implement PDE collection

Through the identified sources for potential digital evidence sources in an eSC network, the specified process deploys data capturing methods such as logging and network sniffing to capture data (PDE) at specified critical points in the e-supply chain potential digital evidence. As mentioned previously in section 5.2.1.1, examples of data sources in an eSC system include servers, firewalls, application software, general logs and network logs.

5.2.2.2 Implement PDE Protection

Implementing PDE handling focuses on implementing security measures across the e-Supply chain. Making sure that from the time PDE is collected from the eSC network (process (1) refer to Figure 5.2) to the time that collected PDE is accessed by a DFI (process (5) refer to Figure 5.2) it is not compromised. Hence in this process (2), security measures such as encryption, hashing, firewall and intrusion detection systems may be deployed to protect the integrity and privacy of captured PDE.

5.2.2.3 Implement centralised storage

Upon collecting PDE, the next issue of concern is the storage of the collected PDE. The researcher believes that the centralisation of collected data is critical in a distributed network environment, let alone a business platform such as an eSC network. That is because it reduces the chances of data redundancy and replication, also making it easy to manage the collected data and have closer control of data protection [64].

5.2.2.4 Implement PDE pre-analysis

Collected data from the eSC environment must be insightful and also presented in a manner that is useful to its users; hence during this process planned data pre-analysis methods should be implemented, to provide a user friendly yet multifaceted DFR solution to the eSC environment.

5.2.2.5 Implement controlled Access

This has to do with controlling the access to the PDE. Considering that captured data is sensitive information, it is necessary that only entities that need to use the PDE to solve an investigation are granted access to it. Therefore implementing controlled access focuses on ensuring that authenticated users are the only ones that can view and use the PDE e.g. using username and password to access an eSC-DFR system. Once DFR is fully implemented across the e-supply chain, there has to be a method to assess the effectiveness of the DFR process across the e-supply chain.

5.2.3 Assessment of implementation processes group for DFR in E-supply chains

An assessment is a set of processes that evaluate or estimate the nature, ability, or effectiveness of a method [65]. It is quite critical to be able to assess the effectiveness of an implemented DFR approach e.g. eSC-DFR system. That is necessitated by the simple reason that certain adjustments might need to be made in infrastructure and policy to keep up with advancements in information and communications technology. An assessment of implementation comes after the implementation of a DFR solution in the eSC has taken place (other process groups). Figure 5.3 shows the three processes that were identified as part of the assessment processes group, namely implementation testing process, result documentation process and result evaluation process respectively.

The main role of this group is to provide processes that can lead to an improved e-supply chain DFR implementation.

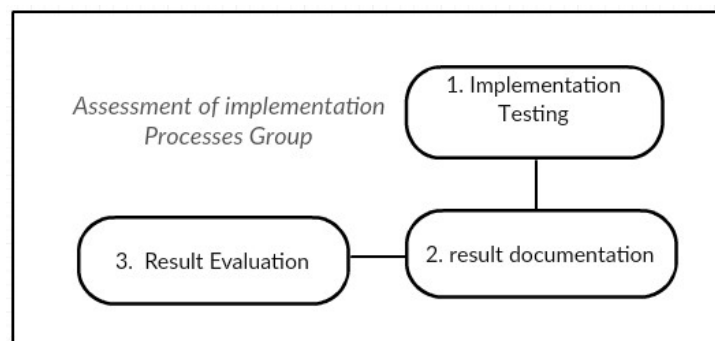


Figure 5. 3 Assessment of implementation eSC-DFR processes group

Each process is elaborated on in the following sections respectively.

5.2.3.1 Implementation Testing

As mentioned in ISO/IEC 27043 (2015), the assessment of implementation process focuses on assessing the effectiveness of an implemented DFR strategy, to determine if it meets the fundamental principles for achieving digital forensic readiness. Therefore, as illustrated in Figure 5.3, the implementation testing process is an assessment process where it is determined if the implemented DFR procedures, controls and architectures meet DFR principles.

It is also important to note that there are costs incurred in implementing DFR, therefore companies/service providers must plan strategically on how to implement DFR across the e-supply chain to achieve the best results from the process, without affecting the performance of eSC network. Another important aspect to consider is the legal aspect. The ISO/IEC 27043 suggests that it is during this process that a legal review must be carried out to determine if implemented processes conform to legal regulations and digital forensic principles. This is to ensure that all collected PDE is forensically sound and can be used in a court of law.

5.2.3.2 Result documentation process

Documentation of results obtained from the testing process is an essential part of an assessment. It is a way to keep track of all the elements that are tested in the implementation testing process and the observations made during testing process. This gives an authentic account of the testing process. Documentation of results from assessing various aspects of the implemented eSC-DFR strategy assists in the evaluation process which comes next in the assessment of implementation process group.

5.2.3.3 Result Evaluation

An evaluation is the process of analysing, summarising and making informed decisions based on results obtained during implementation testing process [66]. During this process recommendations must be made on some critical adjustments that might need to be made on identified and implemented DFR processes. An evaluation of the implemented DFR process in the e-supply chain environment enables service providers to modify the process, in-order to maximise its ability to provide useful information and its impact towards an investigation. Here trading partners decide on whether to go back to the planning process or implementation process, depending on the conclusions of the assessment process.

The three DFR process groups discussed above make up the eSC-DFR process model presented in the next section.

5.3. Proposed eSC-DFR process model

As mentioned in the previous section, the e-supply chain digital forensic readiness (eSC-DFR) process model represents the methodology used to implement DFR within the eSC-DFR environment. It is in the author’s opinion that through correct application of the eSC-DFR process model, sources of PDE in the eSC network may be identified, PDE can be collected from the eSC network and securely stored for access to authenticated parties. Therefore, figure 5.4 presents the model and the processes that belong to each DFR process group as categorised by the researcher. Each of the process groups identified in this process model are implemented in in the following chapters; where Chapter Five and Six focus on the planning of a DFR solution for the eSC environment, Chapter Seven and Eight focus on the implementation of the planned processes and lastly, Chapter Nine and Ten focus on the assessment/evaluation processes of the DFR implementation. It is important to keep in mind that Chapter Five basically gives an overview of the eSC-DFR concept and the methodology that is used to achieve forensic readiness in the eSC environment hence it falls under the planning processes.

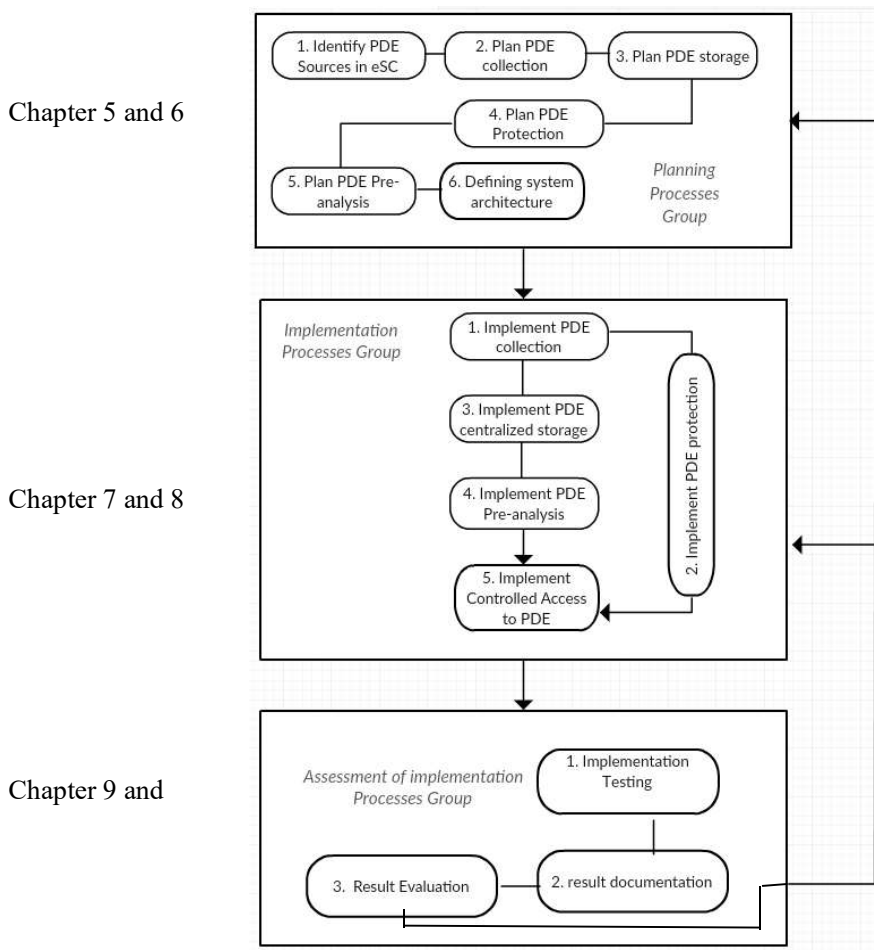


Figure 5. 4 eSC-DFR process model

It is the author's opinion that the three ISO/IEC 27043 DFR process groups adopted in the eSC-DFR process model eSC must result in the development of cutting edge eSC-DFR systems that have five main objectives:

- To capture PDE from the eSC network environment
- To protect PDE from unauthorised parties and ensure its integrity is not compromised through the PDE protection process
- To provide store secure centralised for PDE
- To present collected PDE in a useful manner
- To ensure that authenticated users can only access information that is relevant to a specific case and incident through the controlled access to PDE process.

In the next section the author presents the eSC-DFR conceptual model that illustrates how DFR is to be integrated into the eSC network environment and show where the above-mentioned DFR processes fit into the eSC network environment.

5.4 eSC-DFR Conceptual model

E-supply chains can be seen as a conglomerate which consists of organisations in a given field, say a group of car manufacturers (trading partners) that partner and develop a platform for collaboration such as a website. The information hub links all the internal systems of each car manufacturer for swift information sharing on the site. This information hub has multiple capabilities of data storage, information processing and push/pull publishing (Whang and Seungjin, 2001). Hence the DFR conceptual model for e-supply chains in Figure 5.5 illustrates the introduction of DFR across the eSC network from the trading partners' side to the information hub. As discussed in Chapter Three, the eSC network is made up of software and middleware components that facilitate information sharing between partners, and it is in this network environment that DFR processes discussed in the process model must be implemented at identified critical points. As system developers design eSC system architecture, it is important for them to incorporate the eSC-DFR planning processes in their design to come up with a DFR strategy for this environment. Figure 5.5 illustrates the proposed concept at a high level, showing the incorporation of DFR in the eSC network environment.

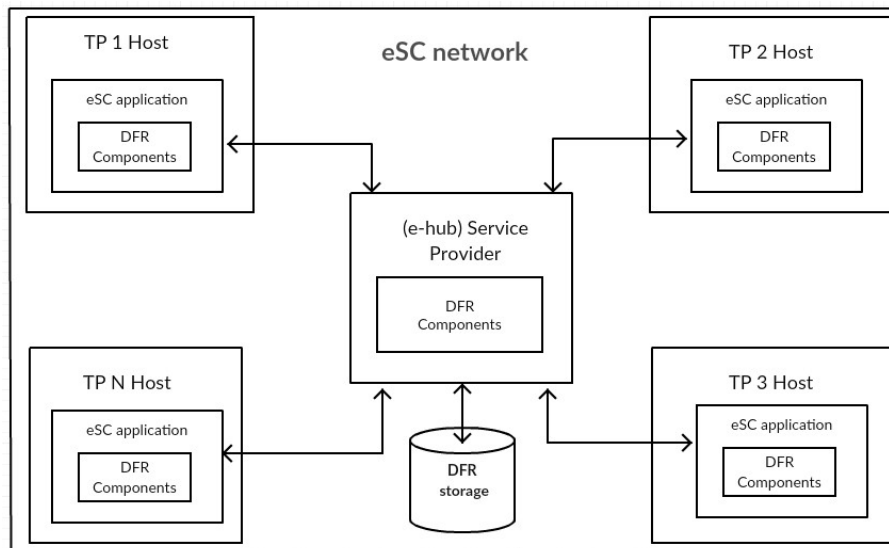


Figure 5.5 eSC-DFR conceptual model

As illustrated in the conceptual model, DFR components must be integrated across the eSC network that includes at the client side of the network (trading partner host machines) and the server side (eSC information hub), facilitating PDE collection. Other DFR infrastructure must be also included that facilitates secure transmission of collected data and secure centralized storage as illustrated in Figure 5.5. Therefore in the following sections the author illustrates and discusses where planning processes from the process model in Figure 5.4 fit into the eSC-DFR conceptual model.

5.4.1 eSC-DFR planning processes leading to eSC-DFR system design

As mentioned in section 5.3, the eSC-DFR process model helps separate DFR processes into groups, allowing processes to be identified and executed in sequential order. Hence the first group of processes identified are the planning processes which are fundamental for the design of eSC-DFR system architecture. These are processes that must be considered by any eSC system developer in order to incorporate DFR in the eSC network environment. Hence Figure 5.6 below shows where the identified planning processes as identified in Figure 3.1 must be executed in the eSC network for an effective eSC-DFR system architecture design. The numbers in Figure 5.6 represent the DFR processes from the process group in section 5.1.

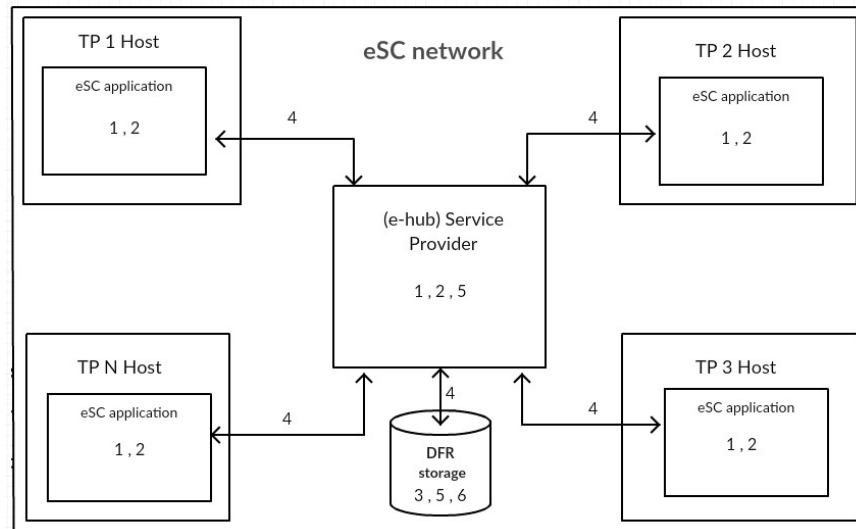


Figure 5. 6 eSC-DFR planning processes in eSC network diagram

Just as the processes are numbered in Figure 5.4, it can be seen where the planning processes take place in the eSC network environment starting with process 1 and 2.

Process 1 and 2: As mentioned in the eSC-DFR process model, process 1 and 2 refer to the identification of PDE sources and planning of a PDE collection strategy. Considering that the eSC environment is vast with many potential sources of information it is up to the system developer to consider the most relevant sources in an eSC network where PDE can be captured for collection both at an application and middleware level. This applies to both client side (Trading partner) and server side the (information hub) as both are key information sources. With PDE sources identified, the next important step to consider is how PDE capturing will be implemented. The use of data capturing agents such as logging modules is proposed, which capture data at critical points in the eSC network as shown in Figure 5.6 and send it to DFR storage. But before PDE capturing is considered there has to be a strategy in place that ensures that captured PDE is not compromised in the process of collection and transmission to storage.

Process 4 and 5: Process 4 and 5 represent the security measures that are put in place to ensure that captured PDE is secure as it is transmitted from different parts of the eSC network as well as when it is stored in PDE storage. Measures such as encryption and hashing must be considered during these two processes to keep PDE secure from unauthorised access and verify its authenticity. The use of secure communication protocols such as SSL and Https must also be considered for the transmission of PDE across the eSC network to the DFR storage.

Process 3: With PDE sources identified and methods for PDE collection defined, PDE protection considered, it is important to decide where and how PDE will be stored. The use of a centralised storage repository is proposed as it provides better control over PDE and its maintenance, solving issues of data

redundancy amongst others, which result in increased PDE quality and accuracy. This PDE storage is where authenticated users such as law enforcement and digital forensic investigators can access this PDE.

Process 6: This process refers to the process of ensuring that access to PDE is strictly given to law enforcement agents and forensic investigators who are the main users of such a system. This process also identifies ways in which to monitor what information is accessible to such users considering that the eSC network environment consists of very sensitive information e.g. when accessing the eSC-DFR system, a law enforcement agent should only be able to PDE what is relevant to a reported incident. From the above-mentioned processes, eSC-DFR system architecture must be defined that comprises of all the elements discussed in the previous processes. The concept of such a system is discussed in the next section.

5.4.2 Concept of an eSC-DFR system

As previously mentioned in Chapter Four, organisations that conduct business processes within collaborative environments such as eSC networks are usually ill-prepared for network security incidents, due to a lack of awareness concerning potential threats and a lack of security infrastructure to prepare them for such incidents. This refers to forensically ready systems that can effectively predict security concerns and address them before they prime, or reduce their impact if they eventually take place. Rowlingson [25] indicates that an investigation of digital evidence is commonly employed as a post-event response to an information security incident; whereas there are numerous instances where an organisation may benefit from an ability to gather and preserve digital evidence prior to the occurrence of an incident. In addition, from a digital forensic investigator's standpoint the process of gathering admissible DFR evidence within a distributed network environment such as an eSC can be challenging with no forensic readiness strategy in place.

Therefore, from the implementation processes group of the eSC-DFR process model, it can be derived that there are five key DFR processes that must be executed by an eSC-DFR system namely: continuous PDE collection, PDE protection, PDE centralised storage, PDE pre-analysis and controlled access to PDE. Each eSC-DFR system that is developed must be able to execute these key processes. Therefore Figure 5.7 below shows the abovementioned processes that an eSC-DFR system must satisfy in relation to the eSC-DFR process model.

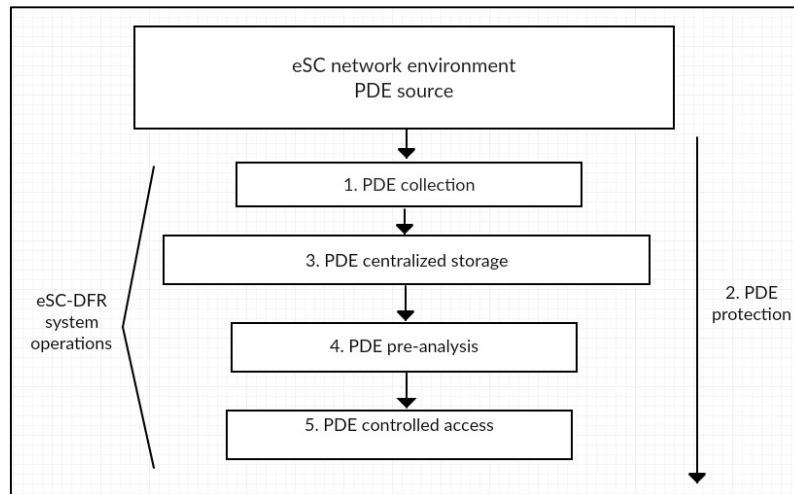


Figure 5. 7 eSC-DFR system functional model

Hence in the following sections the author elaborates on the operations illustrated in the functional model above that an eSC-DFR system must be able to execute.

5.4.2.1 Potential Digital Evidence collection

Developments in technology have a major influence on the way in which companies create, store and share information, this creates many avenues for crime to be committed. Therefore, it is crucial for an eSC-DFR system to be able to collect continuous data that pertains to events taking place across the eSC network. In such an environment there is a lot of sensitive information that is transmitted and shared between trading partners such as electronic payments through transaction processing tools, shipping information, consumer information, intellectual property and other trading partner information. Therefore, it is crucial to be able to collect as much information about events executed in this environment, through data collection techniques such as logging and sniffing; that can assist to trace all the events taking place in the eSC. It is through the implementation of data collection methods that are identified in the eSC-DFR process model, that data systems that can collect PDE must be implemented.

5.4.2.2 Potential Digital evidence protection and storage

Data collection alone does not satisfy key requirements for eSC-DFR to be achieved within the e-supply chain, but a clear data collection and data preservation solution ensures that PDE across the eSC is captured and securely stored for retrieval. With the e-supply chain being a distributed network, it is important to ensure that the integrity of captured PDE is not compromised at any point. This calls for measures that prevent the deletion and modification of PDE to be incorporated in an eSC-DFR system, ensuring that PDE is preserved and presented in a "read only" state to authenticated users. It is also through the usage of security methods such as encryption and hashing that PDE can be preserved. Another key aspect of the eSC-DFR concept is the centralisation of captured potential digital evidence.

Meaning that data that is captured from across the e-supply chain environment must be stored in a central database repository to reduce redundancies and make it easier to manage and secure. Therefore an eSC-DFR system must be able to collect data from across the eSC network environment and store in in a centralised database.

5.4.2.3 Potential Digital Evidence pre-analysis

Having unstructured PDE in storage alone is not enough. With PDE sources already identified, it is crucial to classify the different data that is captured making it easier to extract meaning out of it. Logothetis [67] mentions the importance of deploying specialised frameworks that assist in the process of harnessing multiple commodity machines to process enormous data sets from logged data across an e-commerce distributed environment. Therefore, it is important to keep in mind that there is much activity that takes place within an eSC network, with much important data that can be captured as PDE. That being the case, it is important to implement a DFR strategy that can present captured data in a usable manner. It is also through the pre-analysis process that captured events in the eSC might be highlighted according to their threat level. Meaning there are certain captured events that might have higher priority than others and must be highlighted as high risk events making the PDE analysis process a lot less time-consuming.

5.4.2.4 Controlled access to PDE

With sensitive data being captured through the eSC-DFR process it is important to consider the legal factors involved with PDE gathering, use and preservation. Rajamaki [68] indicates that there is need for a consistent approach to which PDE is captured, stored and retrieved. This is to ensure that potential evidence is admissible in a court of law. Therefore, there are judicial laws that must be followed that govern the usage of gathered PDE and the collection thereof. The reason behind controlled access to PDE is to restrict access to authenticated users such as law enforcement agents and digital forensic investigators (DFIs), who are governed by judicial law on how they are to handle PDE. Such laws differ from country to country and it is a service provider's responsibility to identify the laws that apply to that particular jurisdiction and apply them to the eSC-DFR strategy. Depending on the jurisdiction that an eSC system service provider falls under, it is important to consider certain legal requirements guarding the protection of personal information such as the Protection of Personal information (POPI) act [54] or Electronic Communications Privacy Act (ECPA) [55], which discusses the intercepting of digital evidence and communication records to facilitate prosecution [48].

The next section puts the above-mentioned concept of a system into perspective by providing a practical scenario illustrating the applicability of the eSC-DFR system and its processes.

5.5 Scenario

To illustrate the provided scenario, consider Figure 5.8 that shows some trading partners retailers, logistics and suppliers all connected in an eSC network. (Note: ‘Approach’ w/s below in circle)

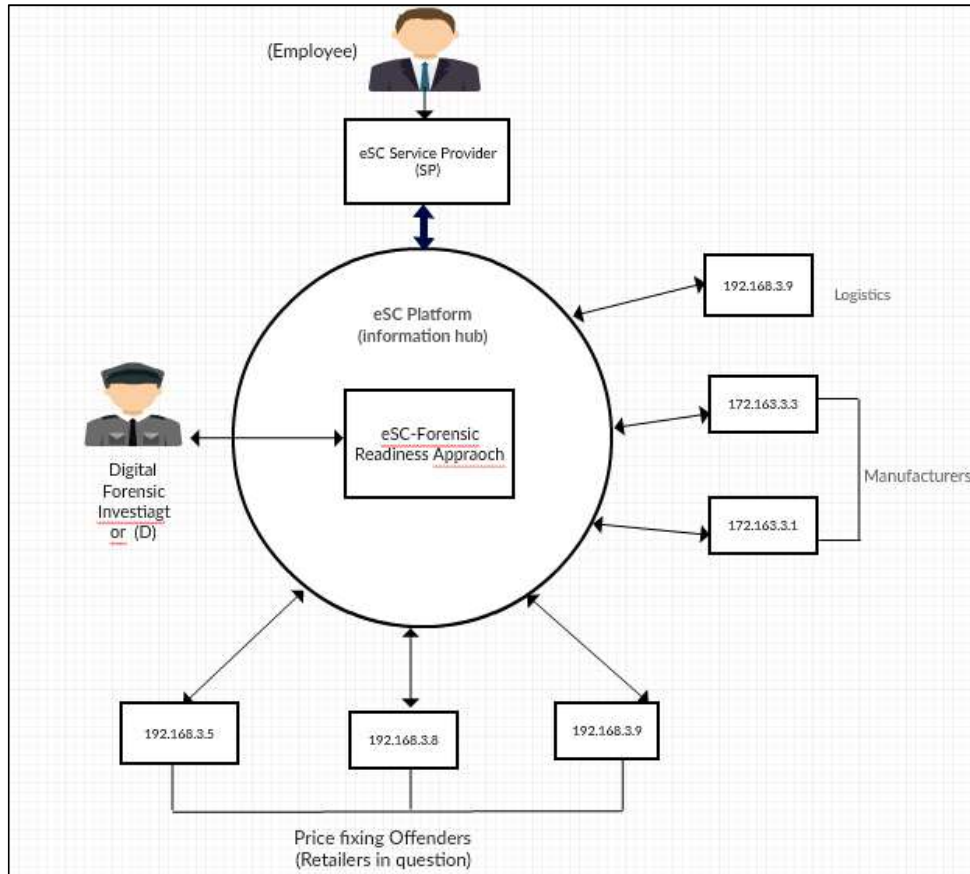


Figure 5. 8 A small eSC network

In the provided scenario, SP is an e-Supply Chain network service provider, offering trading services to a chain of trading partners (which include manufacturing M, logistics L and retail companies R) also referred to as suppliers. The eSC system also provides a network that connects suppliers to their consumers, ensuring a demand-driven supply chain. Furthermore, SP has enforced digital forensic readiness approaches in its system as shown in the Figure. Now consider a disgruntled employee who works at SP has been bribed by a group of retailers (r) to fix the prices of their related services/goods on the eSC platform. This employee was paid to add a computer code that instructs the pricing algorithm in the eSC application to set prices in conformity with their agreement, coordinating changes to their respective prices. A bunch of customers decide to launch a complaint to SP suspecting a price-fixing scandal on the part of SP’s clients.

With the e-supply chain network integrated with the eSC-DFR system (that extracts PDE and log information across the eSC network), records of all the events executed in the eSC network should be collected and securely stored in a centralised data repository. An authenticated forensic investigator should be able to retrieve readily available digital evidence pertaining to the incident. The captured PDE which includes timestamps, system logs and transaction logs could lead directly to the relevant conclusion, showing the installation of the code and the changes made by the malicious code on the eSC-DFR system, the time of events and maybe who was logged in at the time of incident. Through the pre-analysis feature of the eSC-DFR system, the investigator must be able to narrow down from all the captured data to the specific events related to the incident.

As illustrated in Figure 5.5 an eSC-DFR system must be designed and integrated with the e-supply chain environment enabling data collection across the network. This is to maximise the environment's ability to collect usable data.

Service providers that design and manage the data network environment should ensure that DFR requirements are met as discussed in the previous section. The incorporation of log monitoring and management systems such as logging probes across the e-supply chain, for instance TPs internal systems, servers, routers, databases and other network architecture is essential before any information transmission takes place. This ensures that there are retrievable records of events that take place in the entire e-supply chain. Implementing DFR in the e-supply chain environment can be achieved by establishing a standard to which all TPs that use the e-supply chain have to comply with.

This standard should consist of basic requirements and security policies that have to be met for DFR to be fully implemented, which will be discussed in the next chapter. In the next section a hypothetical scenario to illustrate how an eSC-DFR system could benefit both trading partners and digital forensic investigators is provided.

5.6 Conclusion

The concept of DFR in eSCs was discussed in this chapter, along with the methodology proposed to achieve it. The methodology was proposed using a process model to illustrate the DFR processes that are applicable to the eSC environment and a conceptual model showing how and where DFR is to be implemented across an eSC environment. It was explained how the DFR processes stated in the ISO/IEC 27043 standard can be incorporated in an eSC to design and develop next generation eSC DFR solutions, from the planning processes group to the assessment of implementation processes group.

The following chapter provides a list of functional and non-functional requirements that must be considered in the development of an eSC-DFR system.

Chapter 6

ESC-DFR system requirements

6.1 Introduction

This chapter presents the requirements that an eSC-DFR system must fulfil. The requirements discussed in this chapter are based on the research problem given in Chapter 1 and the identified eSC challenges highlighted in Chapter Four. Chapter Six clearly identifies the stakeholders and uses cases that will assist in identifying the functional and non-functional requirements that lay a foundation of eSC-DFR systems.

Functional requirements define functions that a system and its components must perform which include calculations, technical details, data manipulation and processing and other specific functionality that define what a system is supposed to accomplish [69]. Non-functional requirements specify the criteria that can be used to judge the operation of a system, rather than the specific operations that a system must execute. Therefore, the plan for implementing functional requirements is detailed in the system design, whereas the plan for implementing non-functional requirements is detailed in the system architecture.

In this chapter the system goals that an eSC-DFR system must satisfy are elaborated on in section 6.2, whilst the functional and non-functional requirements are discussed in sections 6.3 and 6.4. Section 6.5 concludes the chapter by giving a summary of what was discussed in the chapter and introduces Chapter Six. Both the functional and non-functional requirements presented in this chapter support the system architecture and design of an eSC-DFR system that is presented in Chapter Seven.

6.2 eSC-DFR System goals

Crimes that take place in eSC environments take two generic forms that determine the entities that would use an eSC-DFR tool. The first form is a crime committed internally by an entity in the eSC environment such as a company employee or an external source such as a hacker. The second form is a crime committed against an innocent eSC user who has to cooperate in an investigation. In both cases law enforcement, the eSC user (victim) and to a lesser extent the eSC service provider will use the eSC system. In both cases the idea is to minimise interaction with the eSC service provider (SP). From the above assumption, the SP must deploy the eSC-DFR system and have no other responsibilities. The main goal of this dissertation is provide a framework for the design and implementation of DFR in eSC environments that can simplify the work of eSC SPs, law enforcement agents (LEAs) and digital forensic investigators (DFIs).

Dykstra *et al* mention that there is no sole, authoritative source for requirements development of new digital forensic tools [70]. The proposed solution this research provides is informed by accepted practices and teachings. This dissertation incorporates DFR processes and principles from the ISO/IEC 27043 standard [71] along with other respected bodies such as the Scientific Working Group on Digital Evidence (SWGDE) [72] and the National Institute for Standards and Technology [73], which prescribe accepted *PDE collection*, *PDE storage*, and handling activities that incorporate *data integrity* and *data completeness*. Furthermore, the research is intended to provide a blueprint to the design of useful eSC-DFR systems that are cutting edge, not only collecting unstructured PDE from the e-supply chain and storing it for retrieval but also presenting it in a manner that provides insight to incidents for authenticated law enforcement and forensic investigators. Therefore the use of an eSC-DFR system to law enforcement and judiciary systems dictates the functional requirements of such a system and the eSC network environment itself dictates the non-functional requirements.

From the above-mentioned goals it may be seen that certain requirements must be met, both functional and non-functional. Hence section 6.3 and 6.4 are dedicated to discussing these requirements.

6.3 Functional Requirements

In the instance of an eSC-DFR system, at a high level such a system has three main functions, to collect PDE from the eSC environment, to preserve collected PDE in storage and provide access to collected PDE. Below is a list of the functional requirements that the eSC DFR system must meet. Such requirements comply with the ISO/IEC 27043 standard to deal with minimising the cost of digital forensic investigations, maximising the potential use of digital evidence and preventing generic information security threats that might target collected PDE.

Table 6.1 is an important reference to the proposed system because it relates the proposed requirements to the DFR process discussed in ISO/IEC 27043. For example requirement 1, complies with the ISO/IEC 27043 DFR process for collecting pre-incident PDE for the purpose of minimising the cost of an investigation. Another example would be Requirement 2, which is in accordance with the PDE protection process that aims at preventing generic information security threats mentioned by Pfleeger and Pfleeger [133].

In Table 6.1 each requirement is motivated by ISO/IEC 27043 and the eSC-DFR process model.

Table 6.1. Functional Requirements in order to achieve Digital Forensic Readiness in an eSC environment

<i>Requirement</i>	<i>Description</i>	<i>ISO/IEC 27043 DFR Implementation group</i>	<i>Motivation</i>
1.	Real-time capturing of data from identified PDE sources in the eSC network. E.g logs	Pre-incident PDE collection	Minimise cost of a digital forensic investigation.
2.	Centralised storage of collected PDE	PDE storage	Reduce redundancies, provide better control over PDE and its maintenance [64].
3.	Implement PDE validation techniques such as hashing.	PDE protection	To ensure that collected PDE is admissible as sound evidence.
4.	Capture timestamps of collected data	PDE pre-analysis	For easier event traceability and data analysis.
5.	Compatible with existing forensic formats	PDE storage	To maximise the potential use of PDE in the data analysis process.
6.	Produce informative PDE reports.	PDE pre-analysis	To maximise the potential use of collected digital evidence

In the next section the author lists the identified non-functional requirements

6.4 Non-Functional requirements

Non-functional requirements are those related to the operation, quality and constraints of a system[74]. Therefore, in this section the requirements that ensure the effectiveness of the system being proposed are listed in Table 6.2 and explained. Processes adopted from the ISO/IEC 27043 standard are indicated in the Table

Table 6.2. Non-Functional Requirements to achieve Digital Forensic Readiness in an eSC environment

<i>Requirement</i>	<i>Description</i>	<i>ISO/IEC 27043 DFR Implementation group</i>
1.	Usability	PDE pre-analysis
2.	Quality of Service	X
3.	Security	PDE protection
4.	Scalability	X
5.	Availability	X
6.	Accessibility	PDE controlled access

6.4.1 Usability

It is most crucial that an eSC-DFR system be user-friendly, displaying data to trading partners and law enforcement in such a manner that it is easy to deduce and trace the events recorded. Hence, the usability aspect of such a tool is crucial in its design. The graphical user interface (GUI) of such a tool must provide users with enough flexibility to either view, download, search categorically and filter captured data.

6.4.2 Security

Considering that the eSC-DFR system handles highly sensitive information, intensive measures should be taken to ensure that the system is secure and protected from external and internal threats. Captured PDE must be protected at all times. The use of secure communication protocols that incorporate encryption and hashing is mandatory. In addition, once the captured data is stored in the central data repository it must be encrypted to maintain its integrity. The encryption method selected should be fast and efficient not affecting the performance of the overall system.

6.4.3 Scalability

The system should be able to support increasing amounts of data collected from the eSC, without its performance being affected.

6.4.4 Availability

A digital forensic investigator must be able to sign up, login and navigate through captured data effortlessly. Hence, the availability aspect of such a tool is crucial in its design. The system must be able to perform all its designated functions that include providing forensically sound captured data to users upon demand. It is therefore, crucial that availability tests be conducted to ensure that the system meets its intended functions. Ensuring that the system is reliable is also of utmost importance, especially considering that this is a system that operates within a distributed network environment. Hence, the proposed system has to be carefully designed and implemented to ensure that the system is highly robust. The use of modern software engineering techniques have to be considered to ensure that the system is as secure, robust and versatile; able to handle any unforeseen software errors while minimising the risk of data loss.

6.4.5 Accessibility

Since an eSC is a web-based system, an eSC-DFR system must also be web-based, providing services to law enforcement agents and digital forensic investigators from this platform. ESC network developers must integrate the eSC-DFR system with the eSC system, giving the tool access to the systems that are in the e-supply chain network (trading partner systems) for data capturing purposes.

The system must direct all captured data to a central eSC-DFR system repository server where it is securely stored. Any system errors or alarms raised by a trading partner's internal system must also be captured by the eSC-DFR system and stored in the repository server, where records can be retrieved once a user logs in to the eSC-DFR system.

6.4.6 Follow existing standards and practices

Dykstra *et al* [70] mention the importance of following the existing practices and standards when developing digital forensic tools therefore in the same manner it is important to consider possible standard forensic practices. The forensic data that is provided in the proposed solution must adhere to accepted practices that can be ingested by standard forensic tools such as Guidance EnCase.

For collected data to be accepted in a court of law, a transparent system that describes a process used to produce a result must be used, showing that the process produces an accurate result [58]. Therefore, in the case of data collected from the eSC network the reliability of this the eSC system can be established by showing that law enforcement and forensic investigators actually do rely on it on a regular basis for useful PDE. To that effect, the solution proposed in this research uses ordinary data generated in an eSC network, that includes system logs and firewall logs.

6.5 Conclusion

This chapter has presented the functional and non-functional requirements to be considered in the development of an eSC-DFR solution. These requirements serve as guidelines for the design and implementation of the system presented in the following chapters. This research intends to allow service providers to retrieve forensic logs and metadata directly from the online-management console. In addition, investigators need a solution to preserve evidence and prevent the loss of forensic evidence when cloud resources are released. This research lays a foundation and path to enable digital forensic investigators to take effective initial steps in the forensic investigation of eSC crimes. Therefore in Chapter Seven the proposed eSC-DFR system design is presented and elaborated, providing eSC-DFR system developers with information that can make the development process of eSC-DFR systems easier.

Chapter 7

ESC-DFR system Design

7.1 Introduction

The preceding chapters have discussed the concept of an eSC digital forensic readiness (DFR) solution that is designed to take care of this problem, defining key processes and requirements that need to be considered when developing a DFR solution for the eSC environment. This information is critical because it equips one with the knowledge that is needed in order to define the generic architecture of such a solution.

Chapter Seven discusses the proposed eSC-DFR system design that builds on the eSC-DFR process model presented in Chapter Five. This design comprises of key components that perform different functions in an eSC-DFR system. Such functions refer to the processes listed in the implementation processes group of the eSC-DFR process model in Figure 5.4, from PDE collection (process number 1) to controlled PDE access (process number 5). The proposed system provides DFR capabilities built directly into an eSC network and applies DFR principles discussed in Chapter Two to provide DFIs and law enforcement agents (LEAs) with readily available PDE. The forensic extensions allow for efficient, trustworthy, and user-driven incident response and forensic evidence acquisition in an eSC environment.

The work presented in this chapter applies practical tools on the theoretical foundations that were established in Chapters 4 and 5. The system proposed in this research is called an eSC-DFR system that collects PDE from the eSC network at the middleware and application level and stores it in an isolated central database repository, where it can be accessed by authenticated users on the web.

Therefore, in order to clearly present the architecture of such a system, Chapter Seven is structured as follows: Section 7.2 discusses the architecture overview of the eSC-DFR system at a high level alongside a practical scenario, followed by a discussion on the components that make up the system in sections 7.3 and 7.4. A detailed model of the eSC-DFR system, which comprises of the components discussed in section 7.3 and 7.4 is presented and discussed in section 7.5. Section 7.6 concludes the chapter, summarising the discussed architecture.

7.2 Architecture overview

A system architecture is defined as the structure of a system, that comprises of special components, the visible properties of those components, and the relationships among them [75]. Therefore, using the above stated definition, the eSC-DFR system consists of two key components: the *eSC network component* and the *eSC-DFR component* as shown in Figure 7.1. The eSC network component is the

business environment that provides PDE and the eSC-DFR component is an integrated part of the eSC network that collects the PDE, processes it and provides authenticated users with access to it.

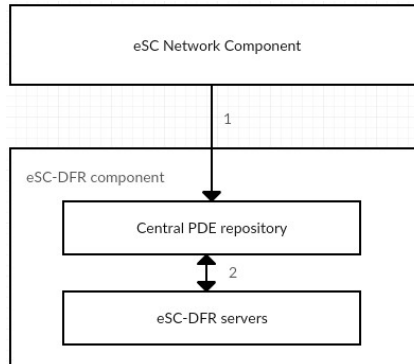


Figure 7.1 High level eSC-DFR systems Architecture

In Figure 7.1 the relationship between the eSC network component and the eSC-DFR component is illustrated at a high level. The Figure shows the relationship between the two components mentioned and direction that captured PDE moves from the eSC network component to the eSC-DFR component (1). Also illustrated is access to PDE in the central PDE repository (2) by authenticated users through eSC-DFR servers. This chapter focuses on the DFR components allocated at both components indicated in Figure 7.1 starting from the eSC network component to the eSC-DFR servers in the eSC-DFR component. The eSC-DFR system architecture proposed in this chapter is built on the eSC-DFR process proposed in Chapter Five that lists five key eSC-DFR implementation processes, namely PDE collection, PDE preservation, PDE storage, PDE pre-analysis and PDE controlled access. Therefore, in the following section the two components are briefly discussed.

7.2.1 eSC network component

The eSC network component, also referred to as the eSC network environment, is an important factor in the architectural design of the eSC-DFR system because it is the environment where PDE is collected from, hosting infrastructural components that are PDE sources. As different events take place in the eSC network environment at a software or middleware level, there are eSC-DFR modules in the eSC network environment that must capture these events (PDE collection process from Figure 5.4) and send them to the eSC-DFR component; which will be discussed in the following sections.

7.2.2 eSC-DFR component

The eSC-DFR component provides DFR services to DFIs and law enforcement agents (LEAs), hosting the sub-components that are crucial for PDE storage, PDE pre-analysis, and PDE retrieval. These sub-components are integrated with the eSC network infrastructure enabling data transmission between the eSC network component and the eSC-DFR component. Hence, communication between the eSC-DFR component and the eSC network component through web protocols and IT infrastructure is a key part

of the eSC DFR system architecture as illustrated in Figure 7.1. This allows PDE to be captured in the eSC network and securely stored in the eSC-DFR system. In order to get a clear understanding of the role that the proposed eSC-DFR system is supposed to play the author presents a practical eSC network environment and eSC hypothetical incident scenario in the next section.

7.2.3 Description of a typical eSC network environment

Consider an eSC network that connects three groups of trading partners namely *Suppliers*, *Shipping companies*, and *Retailers*. The network automates the process of buying, selling and shipment of goods to the available retail stores where the goods are sold to consumers through the eSC system. This eSC network allows a group of retailers to purchase goods from multiple suppliers to sell in their stores, and in order for the goods to reach the retailer a shipping company has to transport the goods; hence, their role in the eSC network. All three groups are connected through an eSC information hub that provides services such as, *user management*, *transaction processing*, *inventory management*, goods and services *pricing management* and *shipment tracking*, as is illustrated in Figure 7.2

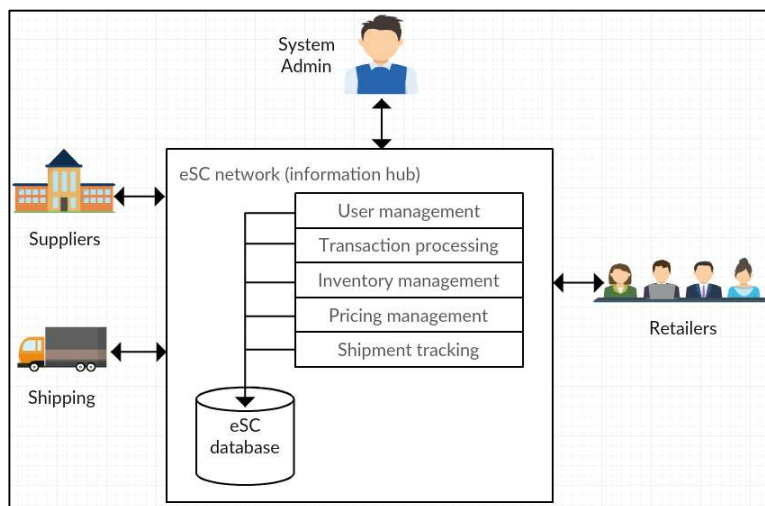


Figure 7. 2 eSC network

The *transaction processing* component is an important information processing system for electronic transactions between trading partners e.g. if a retailer purchases goods from a supplier the transaction processing component ensures that payment is made from the retailer’s bank account to the supplier’s bank account and a record of the transaction is created. The *inventory management* component handles retailer and supplier inventory information such as inventory levels, orders, sales and deliveries. The *pricing management* component handles the pricing of goods and services, also ensuring a supply and demand environment e.g. the Uber pricing algorithm that manages the pricing of Uber fares. When there is high demand for Uber cabs the Uber application, through the pricing component, systematically increases the fare of Uber cabs according to the demand until the demand drops down to a specific range of figures and the number of available Uber cabs increases [76]. The *shipment tracking*

component keeps track of the processes that the goods pass through from supplier to retailer, e.g. notifications that goods have left the warehouse. Therefore, these four components, with the help of the Internet, work together to ensure information is shared seamlessly between the different entities of the eSC. The eSC network is managed by an eSC system administrator who maintains and monitors the eSC system from a security and operational standpoint.

With a description of a typical eSC network environment discussed in this section, the author introduces a hypothetical incident scenario that will be used to illustrate the concepts discussed in the chapter.

7.2.4 eSC hypothetical incident scenario

From Figure 7.2 consider that a group of retailers through an employee of the eSC service provider have conspired to manipulate the prices of their goods (price fixing) by manipulating the pricing algorithm in the pricing management component of the eSC system. Price fixing [64] is a conspiracy between business competitors to set their prices to buy or sell, which is a federal offence [77] in countries such as the United States of America and many European Countries including the United Kingdom. Instead of applying the supply and demand concept, the system now systematically increases the pricing on goods sold by the retailers uniformly. A group of enraged consumers decide to lodge an enquiry on the gradual increase in uncompetitive prices that the retailers are receiving.

Therefore, with the eSC-DFR component integrated with eSC network component, collected PDE such as system records, executed transaction records, inventory records, shipment pricing records and product pricing records must be retrievable and presented in a way that makes the analysis process easy. This allows for an authenticated Digital forensic investigator to have readily available evidence if an investigation needs to be carried out about a price-fixing or data-manipulation incident amongst many other potential incidents that could have taken place in the eSC environment.

Therefore, as indicated in the eSC-DFR process model in Chapter Five, identifying PDE sources is the first most crucial process in planning an eSC-DFR solution. In the proposed system architecture, the author identifies the PDE sources as, the transaction processing component, user management component, inventory management component, goods and services pricing component and the shipment tracking component. It is important to point out that eSC PDE sources are not limited to the ones mentioned here due to the fact that eSC environments differ from environment to environment, e.g. corporate supply that only has transaction processing and user management. For the sake of this research the author uses a consumer-retail supply chain with the mentioned components as PDE sources.

In the next section, the components that facilitate this integration are presented and discussed. It is important for the reader to understand the relationship that exists between the processes listed in the implementation processes group of the eSC-DFR process model and the architecture that is presented

in this chapter. This is due to the fact that the components discussed in this chapter are designed to satisfy the requirements that come from the eSC-DFR process model.

Therefore in the sections that follow, the researcher discusses the eSC-DFR system components that execute the implementation processes group processes, starting with the components deployed in the eSC network.

7.3 The eSC-DFR system components

As discussed previously, the eSC-DFR system architecture comprises of two key components: the eSC network component that provides PDE sources and the eSC-DFR component that collects PDE from eSC network and preserves PDE for access by law enforcement agents and DFIs. In this section the author discusses the eSC-DFR system components that conduct PDE collection (process 1) and PDE protection (process 2) as illustrated in the eSC-DFR process model in Chapter Five.

Whilst trading partners across the eSC network component execute transactions, a non-interfering PDE collection process has to take place. This process can be facilitated by the logging of events, which refers to a process of capturing records of different events executed in the eSC environment [78]. In most cases logging is used to only identify system errors and breaches, but in actuality can be used in many different scenarios, the eSC-DFR system being one of them. Therefore, the logging of events (PDE collection process) is adopted in the eSC network environment for DFR purposes and should be incorporated in the architecture of the eSC-DFR solution. The author would like to point out that as discussed in chapter five, part of the planning process is to identify PDE sources hence log data is just one source of PDE which used for the purpose of this research.

Figure 7.3 illustrates a log file from an eSC network transaction executed, showing some sample fields that are critical to most log files. Each entry in the log file could become an individual database “record” with information about the user’s unique identification; the date when events were executed, and other useful data.

id	supplier	consumer	prod_id	prod_name	event	ip_address	user_agent	date_time
11	admin	Daniel	12	Gallery05	sale	196.248.127.32	Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML	2016-02-08 01:31:04
10	admin	Daniel	10	Gallery03	sale	196.248.127.32	Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML	2016-02-08 01:29:57

Figure 7. 3 Sample typical web server log file

As illustrated in Figure 7.3 the following data about a transaction can be logged such as the ID of a transaction, the name of supplier/consumer, product ID and name, IP address of consumer, user agent used to access eSC, and the date/time, respectively.

The above data illustrates the type of data that can be captured, stored and used as PDE to determine who bought what in the eSC network, from whom, at what time and from which computer. It is important to mention that collected PDE is not limited to data illustrated in Figure 7.3. As users execute programs at the front end, the eSC-DFR system must be able to invisibly build a vault of useful information (log entries) for forensic investigators through what are referred to as *logging modules*.

7.3.1 Logging modules for PDE collection

In this section the author discusses the logging module and how it passes the captured data to an eSC-DFR component which stores all captured data for retrieval by authenticated parties (law enforcement agents and digital forensic investigators).

The logging module incorporated in the code of an eSC system is designed to let a program produce messages of interest to other processes. The ability to obtain useful records of events taking place across the distributed eSC network is one of the main functional requirements of the eSC-DFR system. Therefore, having a sound logging strategy is critical. Logging modules also facilitate event aggregation, which has to do with consolidating similar event entries into a single entry, containing the number of occurrences of that particular event [64]

The eSC system must contain *logging modules* that are essential for the data collection process discussed in the eSC-DFR process model e.g. when a retailer issues a purchase order to a supplier through the transaction processing component, a record of that purchase order must be logged.

Logging gives software developers much flexibility in determining what data is captured and where. Through the use of standardised logging frameworks such as log4J, Java Logging API and SLF4J [78-80] (which are data logging packages for different platforms), PDE can be captured at predefined critical points in the eSC network, recording specific events such as user login/logout operations, user transactions, system errors and updates amongst other events. Ravens [81] mentions that the use of standardised logging frameworks is highly recommended as it provides a standard information set of logs and log formats in which captured data can be stored [81]. It is also critical that in the data collection process which is defined in the eSC-DFR process model, adequate research is done to identify the most suitable logging framework to deploy. This is due to the fact that these standard frameworks operate differently, with others being more difficult to configure and some not being as robust as others [81].

Logging modules are integrated with the eSC system to capture useful data from different parts of the eSC network component (e.g. the PDE sources identified in section 7.2.3) about interactions between trading partners, also ensuring that security measures are implemented on captured data before it is transmitted to the eSC-DFR component. Host machines represent the trading partners being monitored within the eSC network environment. These can be classified as client or server systems, with trading partner (TP) host machines being the client systems and the server system representing the eSC

information hub. As eSC retailers or suppliers run instances of the eSC distributed web application in their stores or warehouses, the eSC-DFR logging modules record all the events executed through a number of modules illustrated in Figure 7.4.

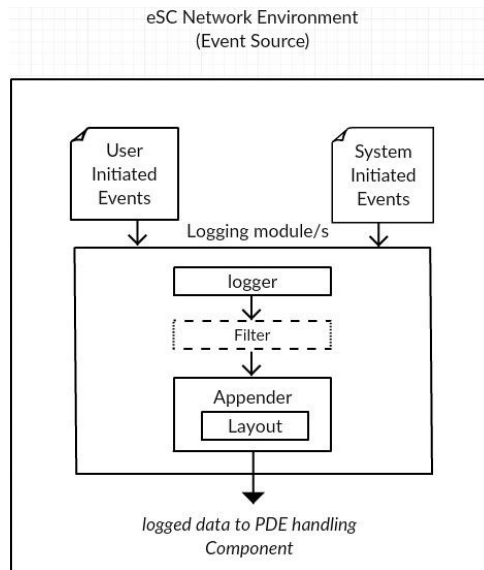


Figure 7. 4 Component diagram for PDE collection process

Figure 7.4 illustrates the fundamental modules that facilitate the data collection process in an instance of the eSC application. As mentioned previously, the eSC network must be integrated with the logging module at critical points in the system. This module has three fundamental elements: the logger, the appender and the layout [79].

- A **logger** is a central class that captures data over time from a specific application such as the inventory management component and passes it to the appropriate appender [78]. In the eSC application, there are many log messages that need to be captured from different parts of the system such as invoice entry data at the transaction processing component or user authentication data at the user management component. Therefore, it is the *logger* class that enables capturing of different events executed across the eSC application.
- A **Filter** receives the logged events from the logger, blocking or allowing a log entry to proceed to an appender based on a number of features such as level of severity or according to what is specified by the developer as critical or non-critical data. This is an *optional mechanism* used to configure more precisely which logging events are logged by an appender and which events must be ignored, more especially the system initiated events [7]. Considering that the eSC-DFR system's main objective is to provide as much PDE as possible, a log filter must filter out log entries as minimally as possible; as long as it does not affect the overall performance of the eSC-DFR system. This again can be decided in the planning processes group. Once captured

log data is filtered, it must be sent to the appender where it is directed to output. To illustrate, consider we only want to capture failed login authentication requests. To do this we can set the filter to only forward a log message to the appender when a user has failed to login to the platform.

- **Appendors** also known as *handlers* [8] are components that listen for log messages that have been captured by the *logger* and forward them in a specific format to the eSC DFR database at the eSC-DFR component. Considering that the eSC is a distributed network, the *appender* must direct captured logs to a network socket that sends the log data to the eSC-DFR component for storage. For example, with a logging module added to the transaction processing component, any captured data that passes through the transaction processing component, such as invoice data, purchase order data or timestamps, must be directed to the eSC-DFR component by the Appender. *Appendors* use *layouts* to format events before sending them to an output.
- **Layouts**, also known as *formatters*, are responsible for converting the contents of a log entry from one data type into another. Logging frameworks provide *Layouts* for plaintext, HTML, syslog, XML and other logs. *Layouts* determine how the data looks when it appears in a log entry. For example, when a log message about an invoice generated by the transaction processing component is captured, the *Layout* element breaks down the invoice log message and presents it according to a specified layout configuration for either plaintext or HTML file formats.

In summary, when a Logger records an event, it forwards it to the appropriate Appender. The Appender then formats the log entry using a Layout before sending it to the eSC-DFR component for storage.

With the data capturing components defined, comes the issue of maintaining the integrity of captured logs (PDE) which is of utmost importance when it comes to digital forensics, referred to as the PDE protection process in the eSC-DFR process model. The issue of the reliability/accuracy of digital evidence is an area that is of great importance requiring attention when designing an eSC-DFR system. Hence it must be incorporated in the system architecture. This is discussed in the next section.

7.3.2 eSC-DFR system PDE handling component

PDE protection as mentioned in Chapter Five is the process of ensuring that the integrity of captured PDE is not compromised. Beddoe *et al.* [82] mention the importance of identifying security vulnerabilities within a system and ensuring that security measures are put in place to protect sensitive information. DFR evidence relies on the ability to prove its accuracy, therefore within eSC-DFR system architecture, it is important to incorporate a PDE component that ensures that the integrity of captured PDE from across the eSC network is not compromised. Therefore, it is in the author's opinion that ensuring the integrity of captured data is reliant on adopting security infrastructure, which ensures that data privacy and data integrity between the eSC network component and the eSC-DFR component are

not compromised. The proposed architecture requires that logs captured across the eSC network environment must be *encrypted* and *hashed*, ensuring that from the time PDE is captured by the logging modules to the time it is accessed by DFIs the integrity of captured data is not compromised.

The PDE handling component comprises of two processes that ensure that the integrity of captured data is not compromised from when it is captured to when it is stored in the eSC-DFR component. These processes are encryption and hashing as illustrated in Figure 7.5.

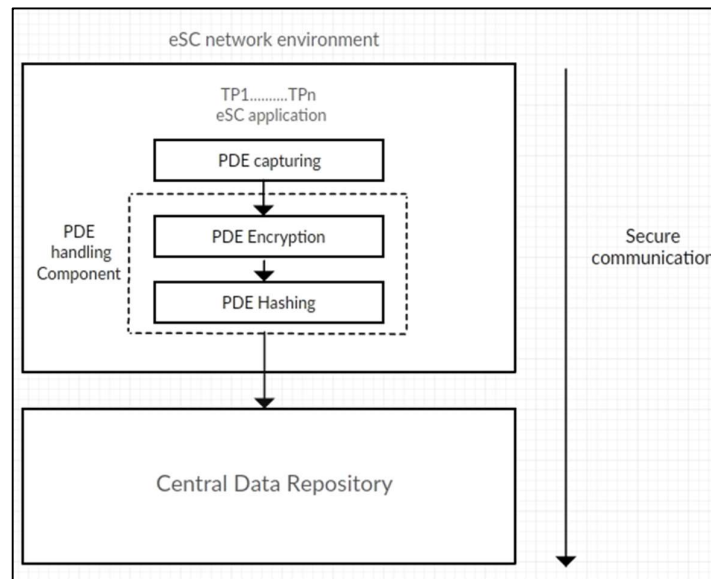


Figure 7. 5 PDE handling process in eSC-DFR system

Encryption over the years has been seen as a secure way of sharing information; ensuring that information is only accessible to authenticated parties. Therefore, in the proposed eSC-DFR system architecture encryption is used to prevent eavesdropping and tampering of captured PDE.

Figure 7.5 illustrates the order of events from the time PDE is captured by a logging module to the time logged PDE is encrypted including the hash value and sent to the central data repository. The use of secure communication protocols is proposed, such as the secure sockets layer protocol (SSL) and transport layer protocol (TLS) which make use of symmetric cryptography to secure data. Therefore the eSC-DFR system architecture has a PDE handling component that ensures that as soon as log data (PDE) is captured at different parts of the eSC network using the logging module, it must be encrypted and transmitted as encrypted data to the eSC-DFR component where it is stored and managed. Protocols such as the SSL/TLS protocol allow for the eSC system and eSC-DFR component to communicate across the internet in a secure manner. It is therefore critical that eSC-DFR system developers ensure that the transmission of PDE between the eSC network and the eSC-DFR component is through a secure communication protocol connection.

Dierks and Tim [10] suggest that the best way to establish encrypted communication is making use of a different port number for secure communication protocol connections e.g. port 443 for HTTPS. It is through the use of the defined secure communication protocols that measures to ensure the integrity of captured data are implemented. Another very important process in the PDE handling component is the hashing process. Many researchers have stressed the importance of providing a means to verify the integrity of transmitted information or stored information in an unreliable medium [83]. Therefore, in the eSC-DFR system hashing is proposed as a solution for verify that the integrity of captured PDE is not compromised. By definition hashing is the process of converting captured data into a fixed value that represents the original data [83, 84]. As soon as an event is captured by a logging module, the hashing process must be carried out. Log data that is captured at different critical points in the eSC network must have a hash value attached to it that is used to verify the authenticity of captured data when it arrives to the forensic database for storage in the eSC-DFR component. As trading partners execute certain transactions e.g. conduct a purchase order with a supplier, all PDE about the purchase order transaction must be captured by the logging module and directed to the PDE handling component that makes use of *encryption* to convert PDE to ciphertext and then create a hash of the encrypted data using the *hash function* to get a hash value of the captured data and the PDE before transmission over a secure connection to the central data repository. This ensures that captured data is not compromised. Also with the hashing of captured PDE, the integrity of PDE can be verified through the hash values that are provided through the use of hash functions.

As is shown in Figure 7.5 captured PDE from trading partner eSC applications must be stored in a central data repository (eSC-DFR database), which is part of the eSC-DFR component. Centralised storage as mentioned in previous chapters is a very crucial part of the eSC-DFR system, considering that the eSC system is a distributed system. Hence in the next section, the author discusses sub-components that are located in the eSC-DFR component that handle PDE storage.

7.4 eSC-DFR system Central Data Repository component

There are very few DFIs who enjoy poring through potential evidence by hand to identify evidence in a network environment because it is like finding a needle in a haystack but fortunately there is a way around this; implementing centralised storage of PDE. In the past, logs were mostly useful as a troubleshooting method, but more recently they have become a very important asset for system performance optimisation, capturing user behaviour and providing helpful PDE for investigating suspicious activity [16]. The information extracted from these logs provides a DFI with information necessary for early warnings about incidents before they spiral out of control or PDE that can be used in a court of law.

Once PDE is collected from the eSC network component it must be securely stored in an eSC-DFR database. As is illustrated in Figure 7.6, with the eSC-DFR component integrated with the eSC network component, PDE collected from the eSC network component must be stored in the eSC-DFR database. An example could be data from the pricing management component about product prices set by retailers and suppliers which must be captured and stored accordingly in the eSC-DFR database (central data repository). As indicated in the previous section, for logged data to be transmitted to the eSC-DFR database, it is important to establish a secure connection between the eSC network environment and the eSC-DFR component that receives log data (PDE) from the identified PDE sources in the eSC network environment. The PDE is transferred to the eSC-DFR database in real-time or close to real-time based on the amount of data that needs to be transferred.

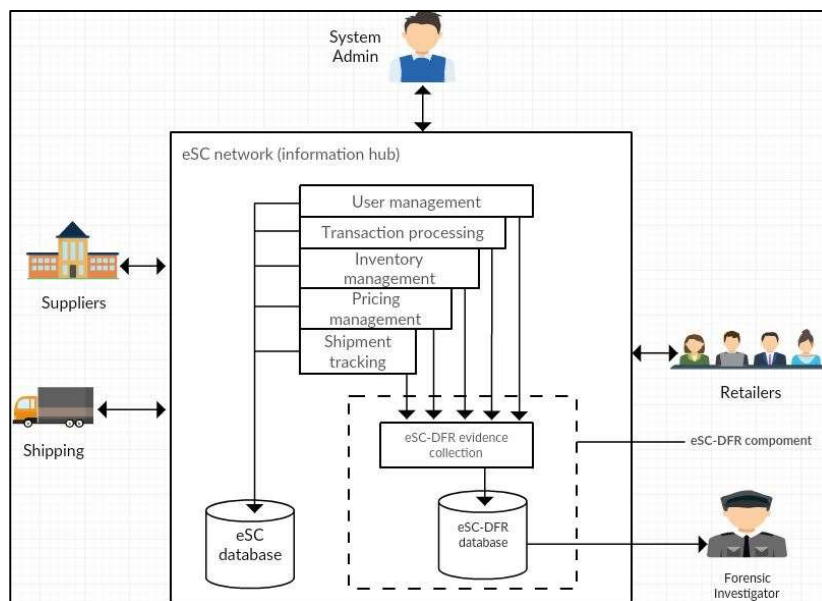


Figure 7. 6 PDE capturing to PDE storage process

Figure 7.6 illustrates the integration of the eSC-DFR component into the eSC network environment, where PDE is collected from identified PDE sources and stored in the eSC-DFR database for access by Digital Forensic investigators. Consider the hypothetical scenario presented in section 7.2.4. Due to the eSC-DFR component being integrated with the eSC network environment, any changes made to the eSC system, such as added code to manipulate prices of goods using a pricing algorithm, must be captured by the logging module and securely stored within the eSC-DFR database. This could be information that includes timestamps, type of events executed, who updated the system, which part of the eSC system was modified, which companies were involved and which goods were affected. With all the above-mentioned PDE stored and readily available, a DFI can go directly to the eSC-DFR database, get authentication and retrieve the above-mentioned records of events. The eSC-DFR database (central data repository) is where captured data from different parts of the eSC network component is

stored, including eSC-DFR system files, metadata and user profiles. A central data repository can be defined as a central place where data is stored and maintained or a place where data is obtained for distribution across a network [85]. When information is transmitted across the eSC network or actions are executed on a trading partner host machine e.g. when an invoice is transmitted from a supplier to a retailer, deployed eSC-DFR system infrastructure will capture as much data pertaining to the transaction, hash it and encrypt it before sending it to the eSC-DFR database through a module referred to as a *log daemon* that processes received PDE from eSC network environment (eSC network component).

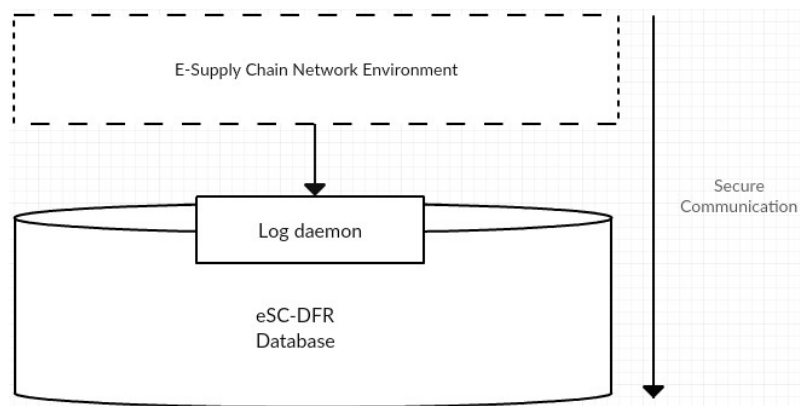


Figure 7. 7 eSC-DFR database

It is the author's view that an eSC-DFR system might require large volumes of storage, resulting in the clustering of database servers, depending on the size of the e-supply chain and considering the amount of data collected from different parts of the eSC network.

Therefore, the eSC-DFR database might differ in complexity and structure [86]. With the simplest arrangement being a single eSC-DFR database server that handles all log storage and pre-analysis functions. Other arrangements deploy the use of multiple servers performing different roles such database cluster servers and eSC-DFR application servers that perform the logic functions of the system. Taking that into consideration, what is proposed is a generic architecture that can be applied to different system arrangements.

In the following sections the author discusses the Log Daemon at the eSC-DFR database server.

7.4.1 Log Daemon in eSC-DFR component

A log daemon is a server program that provides a message logging facility for application and system processes. Log daemons have been used in many distributed systems over the years to gather log data from across a network and store it in a central location using a centralised system log host [87]. Therefore the use of such programs is proposed in the eSC-DFR system architecture. The log daemon

must run on an eSC-DFR database server accepting log data on an appropriate port from logging modules in the eSC network and process the received data before storing it in the eSC-DFR database.

Therefore the processes that the Log daemon must execute are:

- *PDE retention* - which is the archiving of all captured PDE as part of the eSC-DFR system's standard operational activities. Considering that the main objective of the eSC-DFR system is to provide forensically sound records of eSC network activity, it very critical for all captured PDE to be retained in the eSC-DFR database.
- *PDE compression* - which is the process of storing PDE in a way that reduces the amount of storage space needed for retaining the PDE without altering it. This is a process that requires special attention to ensure that the credibility of the stored PDE is not compromised in the process, calling for the usage of hash functions.
- *Log conversion* – which is the process of parsing a log in one format and storing its entries in a second format [86]. Considering that log data is captured from a distributed eSC network environment for forensics purposes, it is important to be able to take that data and convert it to a standard forensics file format (e.g generic forensic zip (gfwzip) file format, (.E01) format for Encase) that facilitate other forensic tools such as Encase and FTK. If a forensic investigator would like to examine and analyse the collected PDE in another application for investigation purposes, they should be able to do so.
- *PDE integrity checking* is a process that involves calculating a message digest for each log file and storing the message digest securely to ensure that any changes made to the archived PDE can be detected. By definition a message digest is a digital signature that uniquely identifies data and has the property that ensures that a slight change to data as small as a single bit will cause an entirely different message digest to be generated [88]. The most common message digest algorithms used today are the Secure Hash Algorithm (SHA-1) and MD5 [56]. Stored PDE should be protected from alteration through the usage of approved encryption algorithms, storage on read-only media, or other suitable means.

With PDE securely stored in the eSC-DFR database and above-mentioned functions handled, the next group of components are responsible for handling the eSC-DFR system business logic and presentation aspects of the eSC-DFR system for users to be able to access the eSC-DFR system content with relative ease. These are discussed in the next section.

7.4.2 eSC-DFR application server modules

An application server by definition provides the business logic for a web-based system, running different processes in the middleware tier [26]. Hence an eSC-DFR application server executes a number of operations which are critical for enforcing some important eSC-DFR system requirements e.g. usability, authentication, maintenance and access to PDE. There are a number of modules that

execute the mentioned requirements which are represented in Figure 7.8, namely the pre-analysis module, data access agent, personalisation manager and user manager.

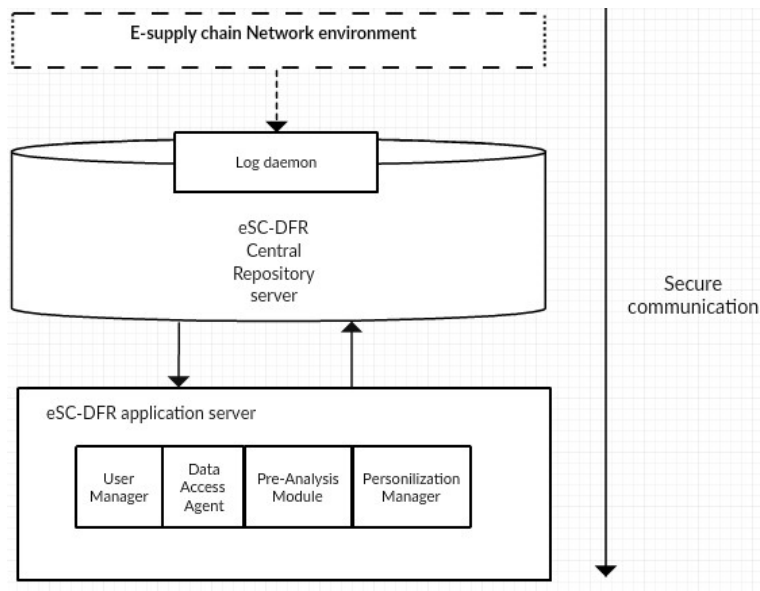


Figure 7. 8 eSC-DFR application server components

In the sections that follow, each of the above-mentioned components are discussed in detail explaining the functions executed by each component.

7.4.2.1 PDE data access module

The data access agent is the module that processes the user requests from the web server to access PDE and with the help of a pre-analysis module; the system can provide meaningful data to law enforcement agents and digital forensic investigators. When choosing a data access technology, one must consider the type of data that is being accessed and how that data is to be manipulated within the system. The next component is discussed is the pre-analysis module.

7.4.2.2 PDE pre-analysis module

The pre-analysis module is designed to make the DFI's PDE analysis process more effective by ensuring that stored data is presented in a comprehensive manner to the user, allowing the user to search for specific events, narrow down the search and trace events. It is therefore the responsibility of the system developer to ensure that the following pre-analysis functions are executed.

- **Log viewing** – which is the displaying of log entries in a human-readable format. Usability is an important aspect of the eSC-DFR system, therefore it is important to be able to view captured

logs in manner that LE agents and DFIs can comprehend and make sense of the events recorded, filtering out irrelevant events and also aggregating certain events [86].

- **Event correlation** – which is the process of finding relationships between two or more log entries. The most common form of event correlation is rule-based correlation, which matches multiple log entries from a single source or multiple sources based on logged values, such as timestamps, IP addresses, and event types. Event correlation can also be performed in other ways, such as using statistical methods or visualisation tools e.g. in the case of the hypothetical scenario provided, collected PDE that could assist in proving that a price-fixing incident took place could be the records from the pricing component. Such records could show that the retailers selling price of certain goods was gradually increasing regardless of the suppliers selling price and the shipping companies' costs. If correlation is performed through automated methods, generally the result of successful correlation is a new log entry that brings together the pieces of information into a single place. With the help of graphs and Tables it would be easier to execute a form of pre-analysis as to what transpired. Depending on the nature of that information, the infrastructure might also generate an alert to indicate that the identified event needs further investigation.
- **PDE reporting** - is the gathering of PDE from a search and presenting it in a summarised, structured and comprehensive document that can be used for further analysis or in a court of law. Log reporting is often performed to summarise significant activity over a particular period of time or to record detailed information related to a particular event or series of events. Therefore it is a critical function that must be implemented in an eSC-DFR system.

The next module discussed is the user manager.

7.4.2.3 User manager module for controlled access to PDE

The user manager module handles the administrative functions of the eSC-DFR system that include system maintenance and managing user profiles.

- System maintenance is a critical process for keeping systems running smoothly. In the eSC-DFR system it is the term used to describe the maintenance required to keep the eSC-DFR system running properly, meaning that the system and its servers are being updated, changed, or repaired.
- Managing user profiles is the function that an eSC-DFR system uses to create user accounts for law enforcement agents and digital forensic investigators, granting them access to certain functions of the system that include downloading PDE reports, accessing certain PDE that is relevant to a particular case and restricting access to irrelevant data.

7.4.2.4 Personalisation manager module

The personalisation manager module of the eSC-DFR system handles the customisation aspect of the system to provide users with a user-friendly system. The personalisation manager attempts to satisfy the usability requirements of the eSC-DFR system, making it an interactive system. The functions that this module provides are to improve the users' experience in using the system. These may include, users being able to share reports with other users within a jurisdiction, being able to view graphs and charts that represent the PDE for analytics purposes, provide a platform for users to interact with the system to address queries and recommend system improvements. Other components that might be critical for improving the systems performance and capability can be proposed and suggested through the personalisation manager module.

In the next section the author discusses the key component that processes user requests and interacts with the user directly.

7.4.3 The eSC-DFR web server

The eSC-DFR webservice processes user requests via HTTP/S. This server attends to requests to access the eSC-DFR system by authenticated users. For example, a forensic investigator may request to login to the eSC-DFR system through a user agent such a web browser. The web browser should initiate communication with the web server by making a request for specific confirmation in the eSC-DFR application server and the web-server will either respond with the successful login response or an error message.

All the above components make up the eSC-DFR system architecture design model presented in the following section.

7.5 Detailed eSC-DFR system architecture model

The previous sections discussed and illustrated how the proposed system architecture will implement each of the processes defined in the implementation processes group of the eSC-DFR process model presented in Chapter Five. In this section a unified view of the system is presented in Figure 7.8, showing where the PDE collection process, PDE handling process, PDE storage process, PDE pre-analysis process and the controlled access process take place.

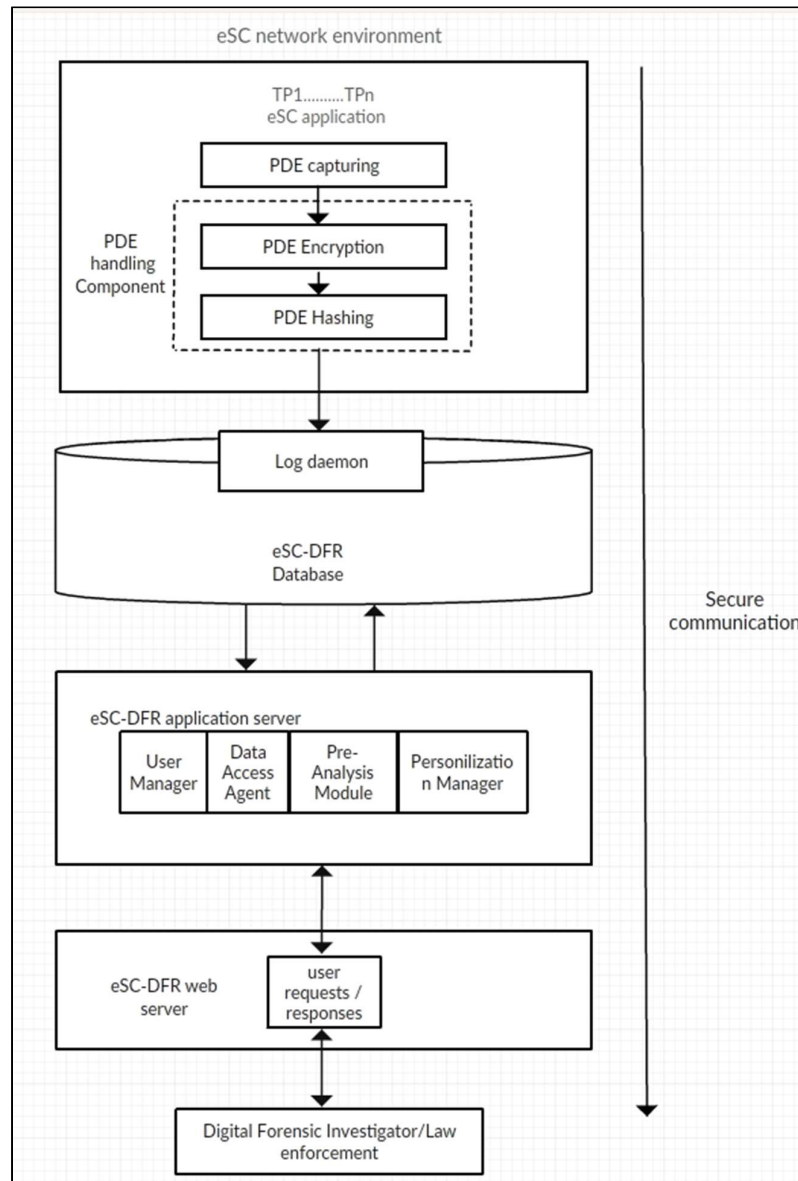


Figure 7. 9 eSC-DFR system design model

As mentioned previously there are two key components in the proposed architecture. One is the eSC network component (eSC network environment) and second is the eSC-DFR component. The eSC network component is the environment where PDE is collected from through eSC-DFR system logging modules, that capture specified log data at critical points in the eSC application and sending it for storage in the eSC-DFR component. The eSC-DFR component is the part of the eSC-DFR system that collects PDE from the eSC network component and stores it in the eSC-DFR database, providing access to collected PDE to authorised DFIs and LEAs. Both the eSC network component and eSC-DFR component are to utilise secure protocols such as the SSL protocol to transmit data over the web; from the eSC network to the eSC-DFR component.

A DFI can go directly to the eSC service provider, get authentication through the user manager module, login to the eSC-DFR system, and retrieve records of events through the data access module in the eSC-DFR component of the system. For example, through the pre-analysis module, an agent can trace and identify when the prices of goods were modified and which companies were involved, which entities were affected by the crime committed, when the eSC system was updated and by whom. Once a DFI has found useful data that can be helpful in solving the case, he/she can put together and download a report that can be used as PDE.

7.6 Conclusion

A solution for achieving DFR in the eSC environment was proposed in this chapter. This solution involved the implementation of an eSC-DFR system architecture that was presented in this chapter. The architecture illustrated how the eSC-DFR process model in Chapter 5 can be implemented; showing how processes identified in the implementation processes group of the model can be executed in an eSC-DFR system. The architecture showed the components that make up the system, from the components that are involved in PDE capturing process in the eSC network to the components that provide controlled access to the eSC-DFR system. The proposed system design calls for the integration of eSC-DFR system infrastructure with the eSC network infrastructure, ensuring that all the requirements discussed in Chapter 6 are met.

This chapter introduced eSC-DFR system architecture, showing the general details of how different components of the system will work together to achieve DFR. The chapter illustrated the design of the eSC-DFR system through the use of diagrams that show the relationship and interaction between components. Chapter 8 discusses the formal specifications of the system and shows the dynamic aspect of the eSC-DFR system, displaying steps a user needs to follow to acquire PDE as well as how the various system components interact with a user.

Chapter 8

ESC-DFR System Prototype

8.1 Introduction

In this chapter an implementation of the eSC-DFR system architecture discussed in Chapter Seven is presented. The author presents an eSC-DFR system prototype as a proof of concept of how the eSC-DFR process model can be implemented in an eSC network. The main objective of the eSC-DFR system prototype is to reduce the time it takes an investigator to collect and examine potential digital evidence from a distributed environment such as an eSC network environment, while preserving the integrity of the collected PDE. Included in this chapter is an illustration of how users such as law enforcement and DFIs can interact with the eSC-DFR component of the eSC-DFR system. The eSC-DFR component, which for the purpose of this research is the contribution, is designed in Chapter Six and Seven, incorporating processes from the planning processes group of the eSC-DFR process model. Chapter 8 focuses on an implementation of the eSC-DFR component and the processes which it executes in relation to the implementation processes group of the eSC-DFR process model. The processes referred to are from the eSC-DFR model in Chapter Five namely PDE collection, PDE Protection, centralised storage of PDE, PDE pre-analysis and controlled Access to PDE.

From the prototype an investigator has readily available evidence about who did what and when, which files were modified and at what point in time. By definition, the eSC-DFR component is a PDE vault used to extract data from across the eSC network, store it, analyse it and present it in a manner in which meaning can be derived from the collected data. The eSC-DFR component deals with large volumes of PDE by breaking it down into datasets of events and providing visualisation of events in a user friendly manner which will be illustrated in this chapter.

The remainder of this chapter is constructed as follows. A use case for the eSC-DFR prototype is presented and explained in section 8.2, followed by technical platform specifications of the eSC-DFR prototype discussed in section 8.3. In section 8.4 the interface design of the eSC network component and its interactions with the various trading partners is explained. The interface design of the eSC-DFR component from the prototype is discussed in section 8.5, showing how a DFI can navigate through the various functionalities that it provides, with reference to Chapter Seven.

8.2 Use case for the eSC-DFR system prototype

A use case diagram is widely used to capture the dynamic aspect of a system, displaying steps a user needs to follow to reach a goal as well as how the various elements interact with a user [89]. In this

section the author makes use of a use-case diagram in Figure 8.1 to show the high-level view of an eSC-DFR component and the interactions between actors of the system with the system itself. Remember that the eSC-DFR component is a component situated within the greater e-supply chain as shown in Chapter Five in Figure 5.8.

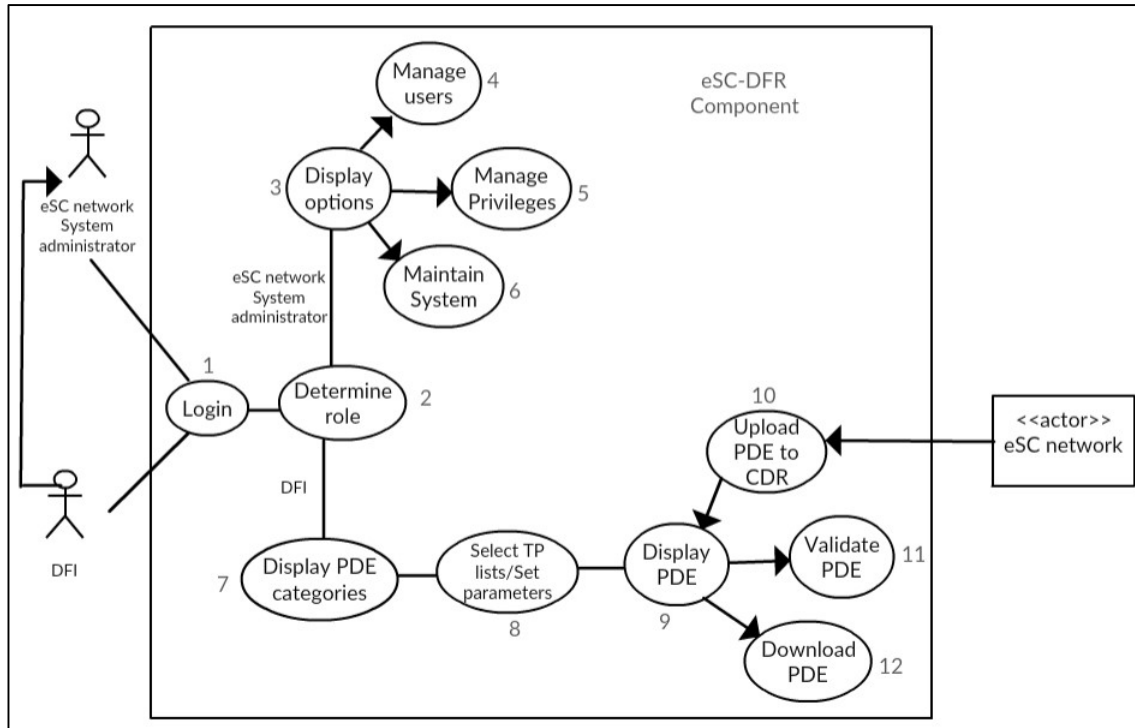


Figure 8.1 eSC-DFR component use-case diagram

8.2.1 eSC-DFR component actors

The author identified three main actors i.e. eSC network, eSC network System administrator and DFI, depicted in the use-case diagram in Figure 8.1. An actor refers to an external system or person that interacts with the eSC-DFR component [89]. A stick man represents a human actor and a square box with <<actor>> in it represents a system actor (i.e. non-human actor) as is illustrated in Figure 8.1. Each of the three actors are discussed next.

eSC network System administrator - In Figure 8.1 the eSC network system administrator (system admin) represents the person responsible for handling the administrative aspect of the eSC-DFR component. It is the role of a system admin to manage user accounts, manage user privileges and maintain the eSC-DFR component upon validation at login. The system admin is also authorised to administer any updates to the eSC-DFR component of the eSC-DFR system such as install new updates to the eSC-DFR component that add new features and resolve bugs. To better illustrate how a user would navigate the eSC-DFR component the author uses numbers indicated in brackets in Figure 8.1

Consider from Figure 8.1, a user logs into the eSC-DFR component as a system admin (1). The eSC-DFR component determines if the user is indeed a system admin or not (2). If validated, the system admin is directed to the display options page (3) where three functions are available for the administrator to execute, namely to manage other user accounts (create, delete) (4), manage privileges (allow users to view, download and share files) (5) or maintain the system (install eSC-DFR component updates) (6).

DFI (digital forensic investigator) - As is illustrated in Figure 8.1, a DFI is the main actor of the eSC-DFR component, getting access to all the collected data stored in the eSC-DFR component, with the ability to analyse vast amounts of PDE and selecting collected data from specific trading partners for a better forensic data analysis experience. Consider from Figure 8.1 that a DFI logs into the eSC-DFR component (1). Upon logging in, the eSC-DFR component determines whether the user is indeed a DFI (2). Once it has been determined that the user is a DFI the eSC-DFR component displays the PDE categories that a DFI can choose from (7). Once the PDE category is selected, the eSC-DFR component allows a DFI to narrow down the search for specific PDE using different parameters such as date, eSC trading partner name or location (8). With the parameters selected, the eSC-DFR component displays the PDE (9) for selected parameters and allows a DFI to download displayed PDE (12) or validate PDE (11).

The eSC network supports multiple trading partners that interact with each other through an information hub, sharing information and services [2]. Therefore, collected PDE from the eSC network has to be uploaded to the eSC-DFR component where it is stored and processed for DFIs to access it (10). Captured data might be, amongst other forms, in the form of information requests and responses sent between trading partners through the information hub, transaction records such as invoices generated and eSC network modifications. The eSC network may be accessed through an internet browser for users to access the system. In the next section the author discusses the eSC network in more detail, to give the reader a deeper understanding of the system that is being monitored by the eSC-DFR component. Thereafter the eSC-DFR component will be discussed. For that reason the author had to develop a prototype of an eSC network first before incorporating the eSC-DFR component to it. The eSC system administrator and DFI are human actors and, therefore, they are not the main focus of this research. Only the eSC network component is discussed next.

8.3 The eSC network

In-order for a proof of concept to be achieved, the author developed an eSC network web application, that serves as this proof of concept (prototype) where the web application acts as a simulation of the eSC network. It is important to point out that the developed eSC network web application developed does not fully define the capabilities that an eSC network application can provide. An eSC network environment can be vast and quite complex in its design, with different capabilities for different

customer requirements e.g integration with different components such as enterprise resource planning or Customer Relationship Management solutions. For the sake of this research the author built a basic eSC web application that is integrated with the eSC-DFR component providing simple test data as PDE for proof of concept. The application allows transactions to be executed between trading partners such as suppliers, retailers and customers and provides PDE to the eSC-DFR component. The eSC network web-application front-end (eSC app) for the prototype was developed using HTML, CSS and JavaScript. The eSC network web application back-end (eSC app) was developed in PHP, which provides libraries that support the extraction of data from selected critical points in the eSC network. To ensure the integrity of transported data is not compromised from a logging module in the eSC app to the eSC-DFR component, AES encryption was used to encrypt logged data before transmission. The eSC app was tested on a Linux platform.

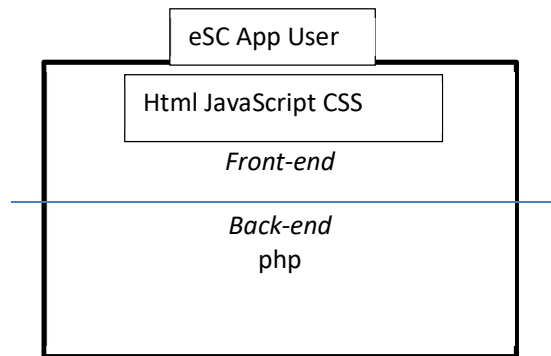


Figure 8.2 programming languages used in eSC network web application frontend and backend

To see how such an application would work practically , consider the following hypothetical scenario. Consider Suppliers S1, S2 and S3 specialising in car manufacturing and having warehouses across the country. They decide to improve their business by joining an eSC network web application to interact more closely with their clients, i.e. the dealerships (retailers). In turn, retailers R1, R2 and R3 decide to sign up on the eSC App to interact more effectively with their business partners, i.e. suppliers S1, S2 and S3, for the purchasing of cars. Retailers R1, R2 and R3 also make use of the eSC App to be able to sell their cars on the internet. For the sake of this scenaio we consider customers C1, C2 and C3. Customers C1, C2 and C3 sign up on the eSC App through a browser interface to create user accounts that can be used to purchase cars that retailers R1, R2 and R3 are selling. Now, considering that the vehicle warehouses are scattered across the country, a logistics company is needed to pick up and drop vehicles either from the supplier warehouse to the retailer dealership, or from the retailer dealership to the customer's doorstep.

In the next section the author discusses the eSC network web application that was developed as the prototype described in the scenario above. For the sake of the prototype, the stakeholders created for

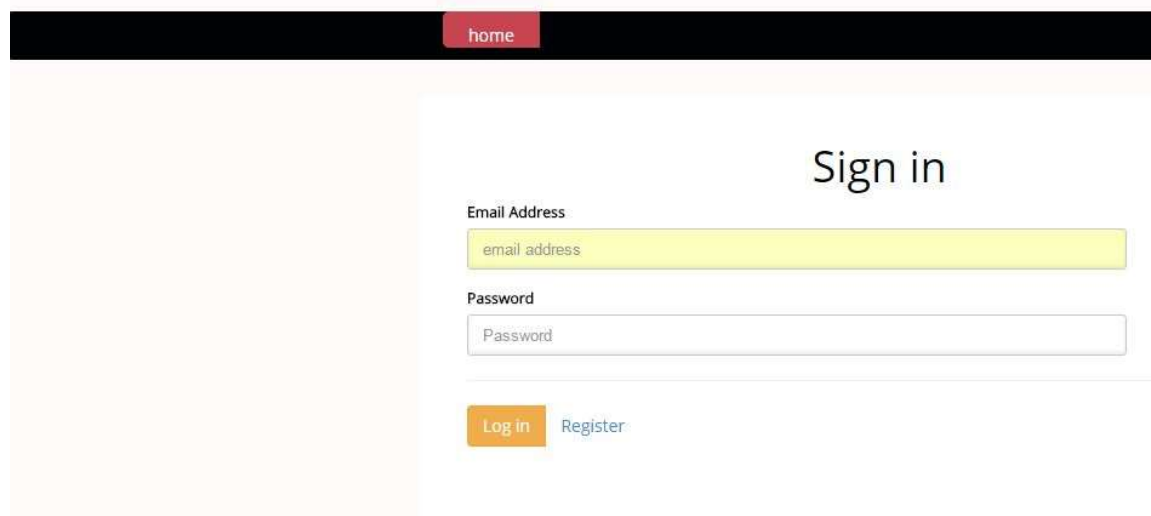
the eSC network web application are suppliers, retailers and customers which are discussed respectively, next.

8.3.1 Supplier eSC network web application user interface

A new supplier can access the eSC network web application from the web browser to Login/Register an account as either a customer, retailer or supplier shown in Figure 8.2 and Figure 8.3. The SHA-256 hashing algorithm is used in the access control process to check password hashes for users that access both the eSC network web application and the eSC-DFR component. The SHA-256 hashing algorithm was chosen for it being a secure hashing algorithm with a very low collision rate [90]. Upon logging into the platform the supplier is presented with the main dashboard indicated in Figure 8.4 and is able to upload inventory catalogue data about cars being sold. This information is essential to retailers and customers that will be purchasing goods on the eSC platform. From the supplier dashboard a supplier can update/remove inventory items using the change price function or the remove product button From the supply statistics option, a supplier can track the number of goods sold as illustrated in Figure 8.5.

To differentiate between a supplier, retailer and customer user interface upon signing in, the colours red, blue and green are used respectively in the top left corner of the user dashboard. In Figure 8.2 and 8.3 the sign in and new applicant pages of the eSC network web application are indicated, where a user is requested to login or register an account.

ESC Service Provider



The screenshot shows the 'Sign in' page of the eSC network application. At the top, there is a navigation bar with a 'home' button. The main content area is titled 'Sign in' and contains two input fields: 'Email Address' and 'Password'. Below these fields are two buttons: 'Log in' and 'Register'.

Figure 8.3 eSC network application Login/Register Page

As illustrated in Figure 8.3, when a user visits the eSC network web application, the first page that opens is the sign-in page where a new user can **Register** or **Log In** as a supplier, retailer or consumer

as illustrated in Figure 8.3 and 8.4. If the user is an existing client, then from the Sign in page the user can enter credentials and login to the eSC network.

ESC Service Provider

home

New Account

Which user are you?

Retailer

Company Name:

Executive cars

Company Registration Number:

12344311234

Phone Number:

+27849736181

Email Address:

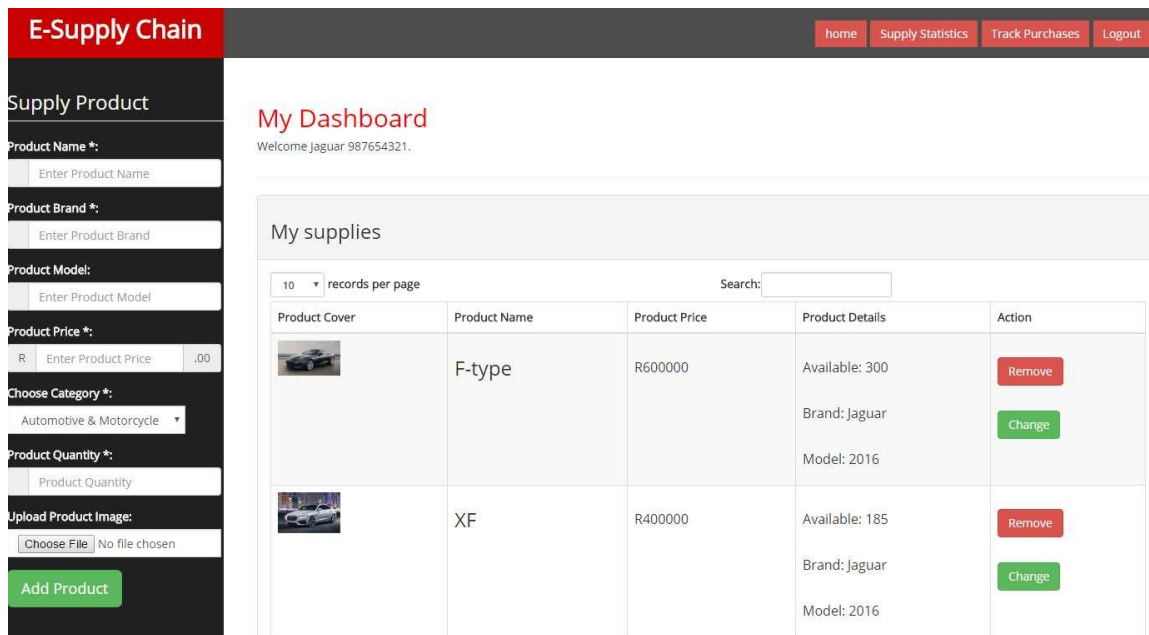
derek@executivecars.co.za

Address:

1003 Burnett villa Hatfield Pretoria south africa

Figure 8.4 eSC network application User New Account page

When an existing supplier logs into the eSC Network web application (eSC app), the dashboard appears as illustrated below in Figure 8.5 with the top left corner of the dashboard coloured red. From the dashboard a supplier can add new inventory for sale, view supply statistics (Figure 8.6), track purchases and update inventory.



E-Supply Chain | home | Supply Statistics | Track Purchases | Logout

Supply Product

Product Name *:

Product Brand *:

Product Model:

Product Price *: R .00

Choose Category *:

Product Quantity *:

Upload Product Image: No file chosen

My Dashboard
Welcome Jaguar 987654321.

My supplies

10 records per page | Search:



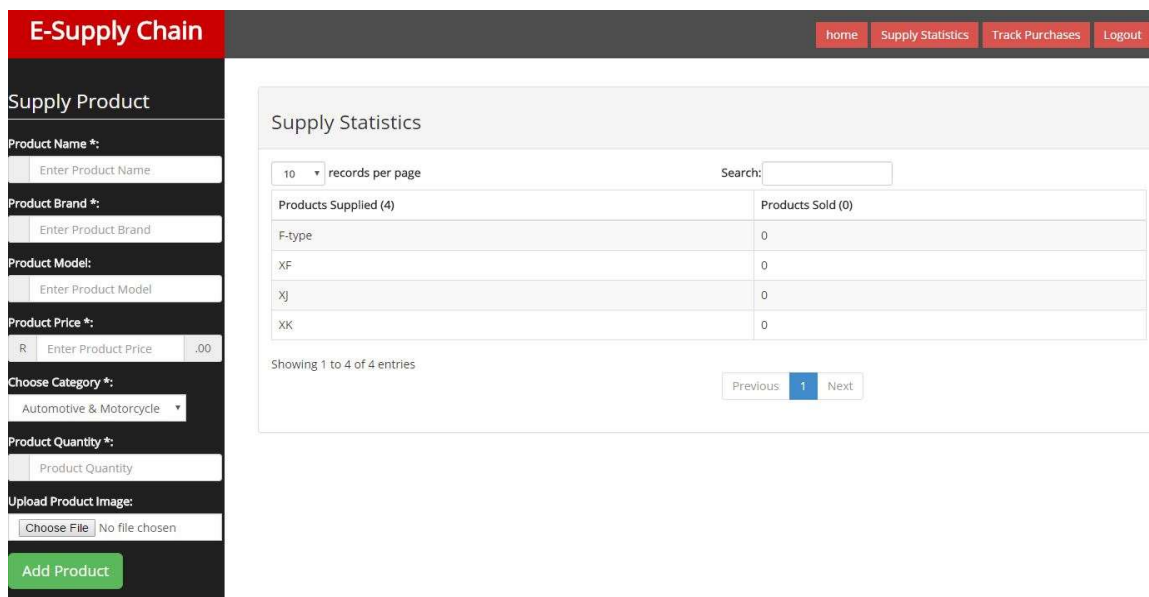
Product Cover	Product Name	Product Price	Product Details	Action
	F-type	R600000	Available: 300 Brand: Jaguar Model: 2016	<input type="button" value="Remove"/> <input type="button" value="Change"/>
	XF	R400000	Available: 185 Brand: Jaguar Model: 2016	<input type="button" value="Remove"/> <input type="button" value="Change"/>

Figure 8.5 Supplier Dashboard upon successful Login



E-Supply Chain | home | Supply Statistics | Track Purchases | Logout

Supply Product

Product Name *:

Product Brand *:

Product Model:

Product Price *: R .00

Choose Category *:

Product Quantity *:

Upload Product Image: No file chosen

Supply Statistics

10 records per page | Search:

Products Supplied (4)	Products Sold (0)
F-type	0
XF	0
Xj	0
XK	0

Showing 1 to 4 of 4 entries

Figure 8.6 Supplier statistics

The basics of the supplier interface have been discussed here. In the next section the author discusses the retailers user interface.

8.3.2 Retailer eSC network web application user interface

When an existing retailer logs into the eSC Network web application (eSC app), the dashboard appears as illustrated in Figure 8.7 with the top left corner of the dashboard coloured blue. With supplier product catalogue data loaded onto the eSC app, a registered retailer can login to the platform and view a

supplier’s product catalogue from the dashboard. From the dashboard a retailer has the option of choosing the category of products they would like to sell in their webstore using the grey tabs on the left of the retailer dashboard. For example if a retailer is interested in selling cars, they can select the *Automotive & Motorcycle* tab and view the vehicles/motorcycles catalog data uploaded by the different suppliers as illustrated in figure 8.7.

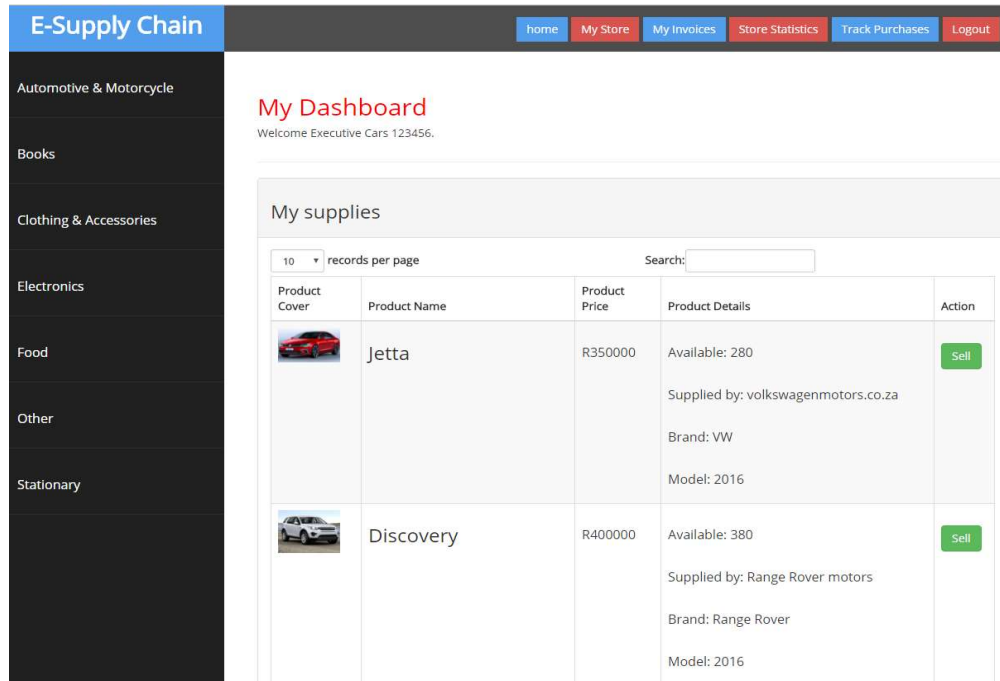


Figure 8.7 A retailer’s eSC app user interface dashboard.

If the retailer finds a vehicle that they would like to sell in their webstore, they can click the *Sell* button on the right upon which a Product Quantity pop up box appears and they can choose the quantity of vehicles they would like to purchase from a supplier (Figure 8.8). Once the requested number of cars is entered the retailer can choose to click on the purchase products button to complete purchase between retailer and supplier.

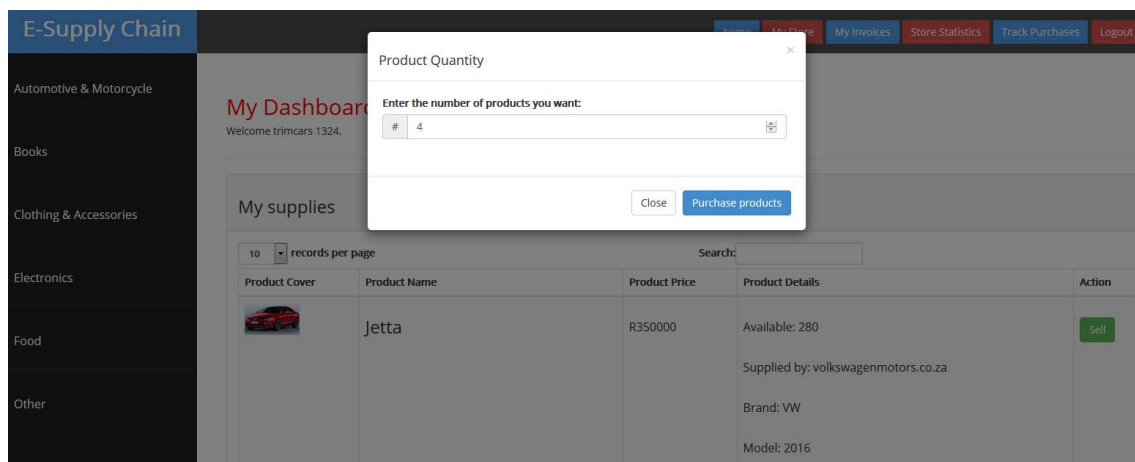


Figure 8.8 A retailer purchasing cars from a supplier

Once a retailer has purchased cars from the supplier (Figure 8.7) they can adjust the price of the cars by clicking the **My Store** button and **Change Price** button illustrated in Figure 8.9.

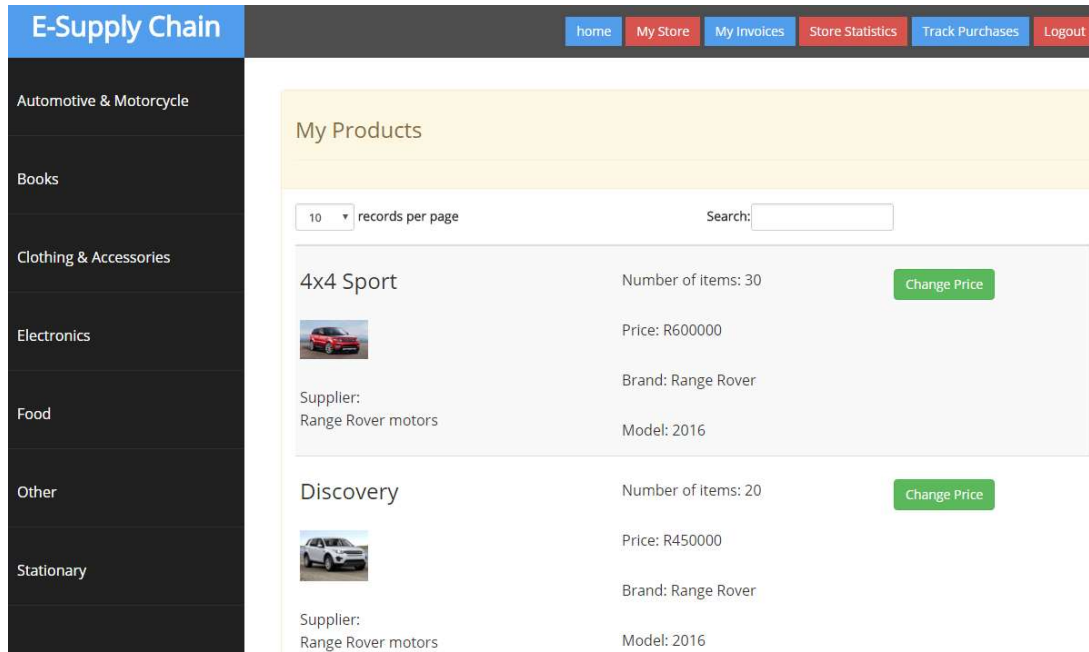


Figure 8.9 The retailers' webstore where they can change inventory pricing.

When a retailer purchases cars from supplier, an invoice is generated that showcases the particulars of a purchase as is illustrated in Figure 8.9 and Figure 8.10 with the option to download a generated invoice.

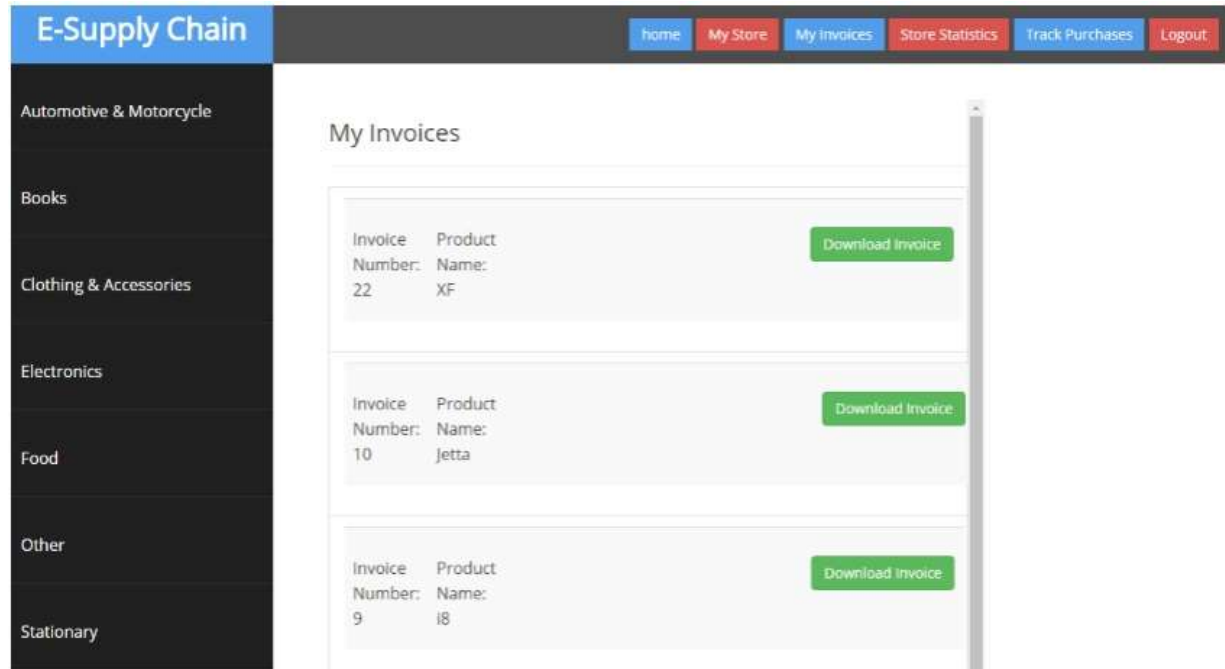
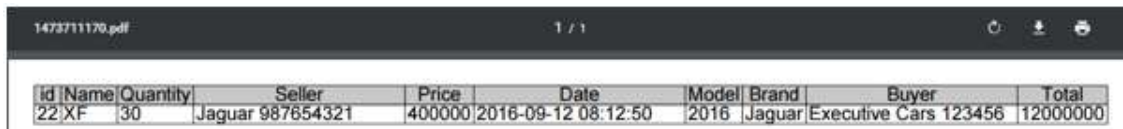


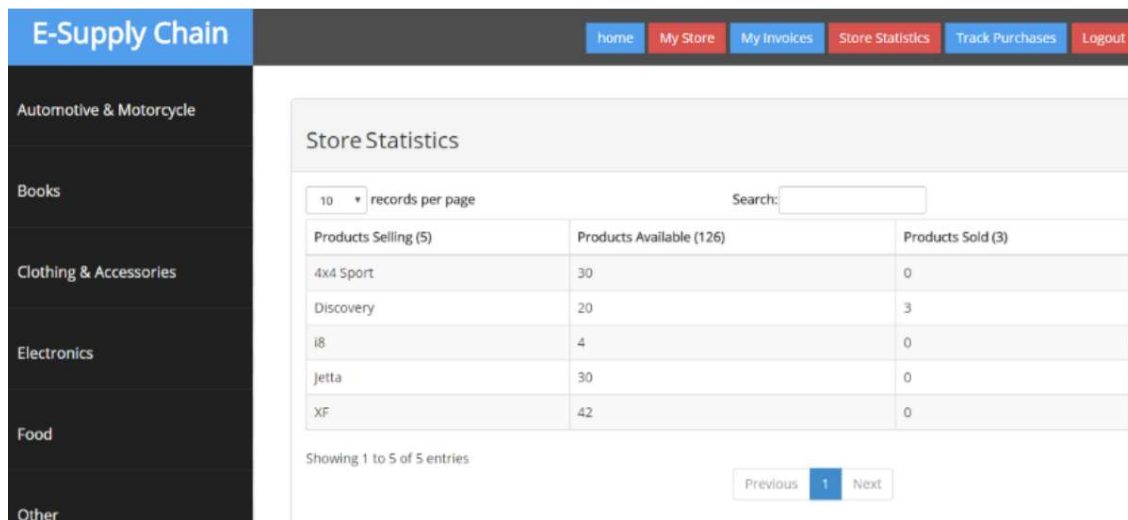
Figure 8.10 Generated retailer invoices from supplier



id	Name	Quantity	Seller	Price	Date	Model	Brand	Buyer	Total
22	XF	30	Jaguar 987654321	400000	2016-09-12 08:12:50	2016	Jaguar	Executive Cars 123456	12000000

Figure 8.11 PDF Generated retailer invoice from supplier

To keep track of inventory levels and sold goods, the retailer using the **Store Statistics** button is able to view inventory data as is illustrated in Figure 8.12.



Products Selling (5)	Products Available (126)	Products Sold (3)
4x4 Sport	30	0
Discovery	20	3
i8	4	0
Jetta	30	0
XF	42	0

Figure 8.12 Retailer inventory data

With a retailer having purchased vehicles from different suppliers and loaded the inventory data onto the retailer’s webstore in the eSC app, customers can login to the eSC app view the retailer’s inventory for purchase. This process is illustrated in the next section.

8.3.3 Customer eSC network web application user interface

The customer eSC network web application user interface is for product consumers that prefer to shop online for goods with a wide variety of products and brands to pick from. Through the eSC app customers can view products being sold by retailers from the customer dashboard once they login as customers. Illustrated in Figure 8.13 on the far left are the product categories and the description of products on the left. A customer is able to view who the retailer is that is selling a product, the product information and pricing.

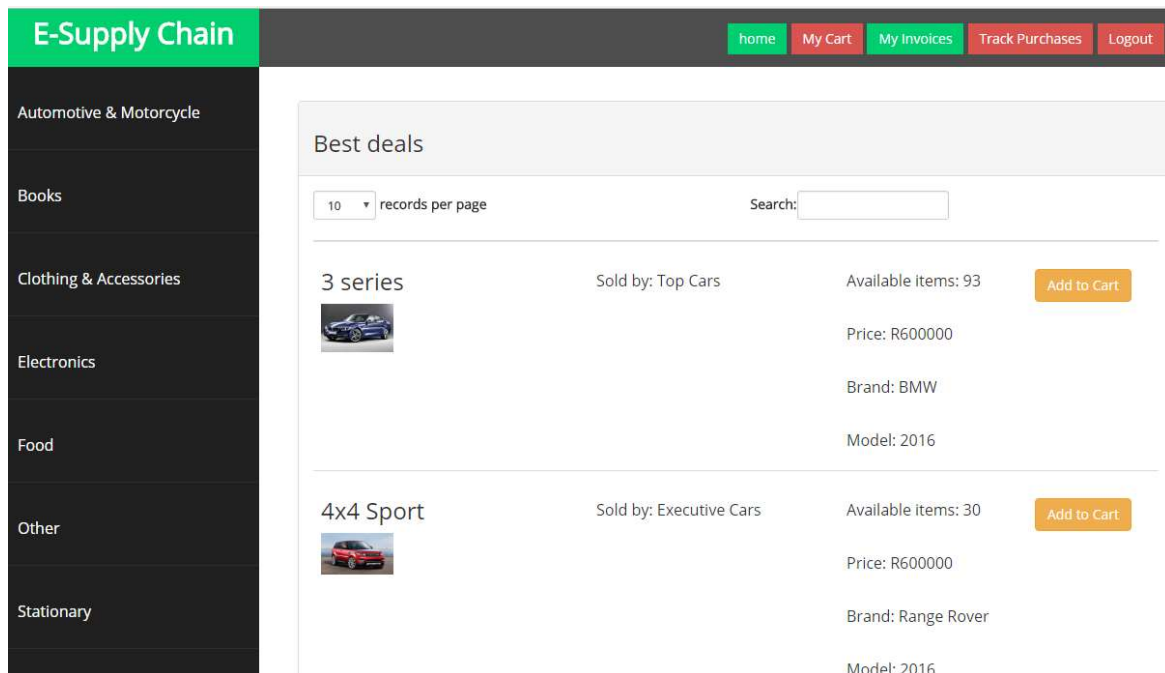


Figure 8.13 Customer Dashboard

If interested in purchasing a vehicle as is illustrated in Figure 8.13, a customer must add the vehicle to their cart by clicking the **Add to Cart** button. With the vehicle added to the cart, a customer can select the quantity they want to purchase from the Product Cart pop up box illustrated in Figure 8.14 and click the **Add Products** button as illustrated in Figure 8.15 to update cart.

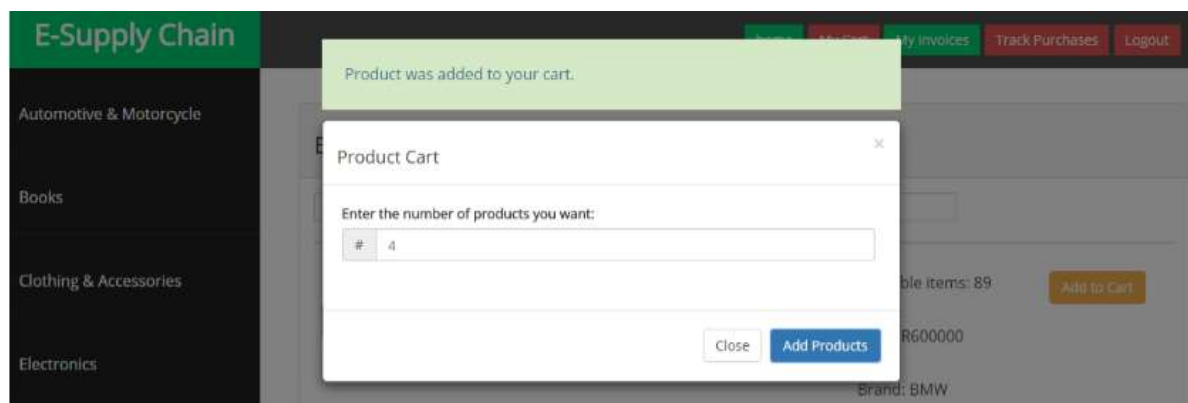


Figure 8.14 Customer adding vehicles to cart

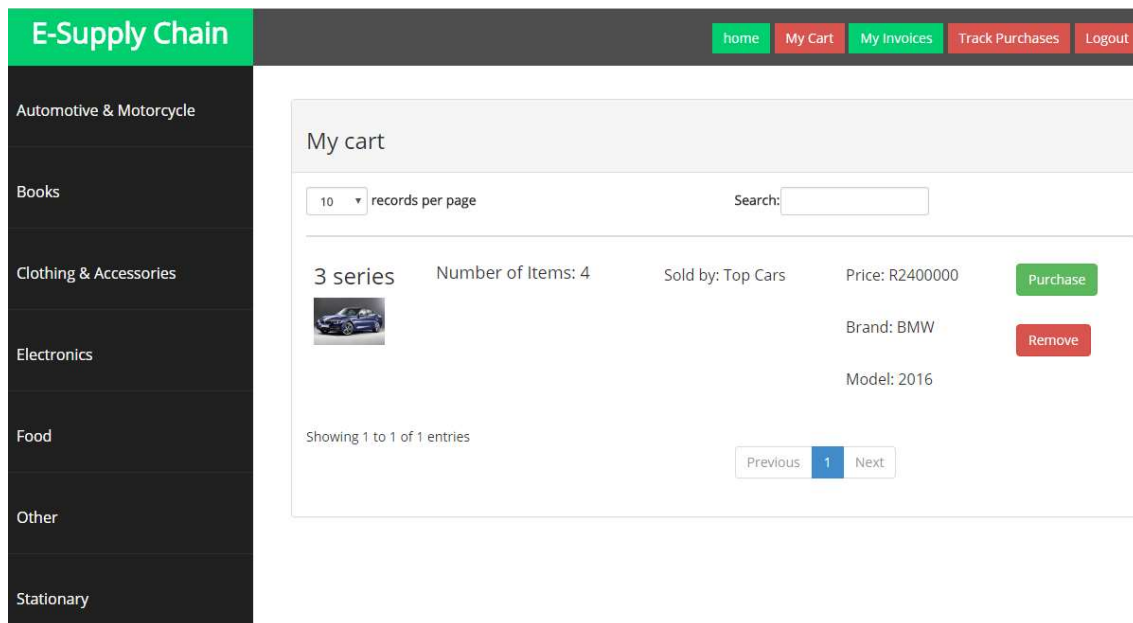


Figure 8.15 Customer purchasing vehicles from cart.

Once the cart is updated with the quantity of vehicles being purchased by the customer, the customer must click on the **Purchase** button to complete the purchase (Figure 8.14). When the transaction is complete an invoice is generated and the purchase information, including the address of the customer and the address of the supplier are provided to the logistics company for pick up and drop off vehicles. To view invoices for past transactions a customer must click on the **My Invoices** button, upon which a list is generated as is indicated in Figure 8.15. When a customer clicks on the **Download Invoice** button to download an invoice, XML to PDF conversion is executed for the invoice to be generated and downloaded in PDF format.

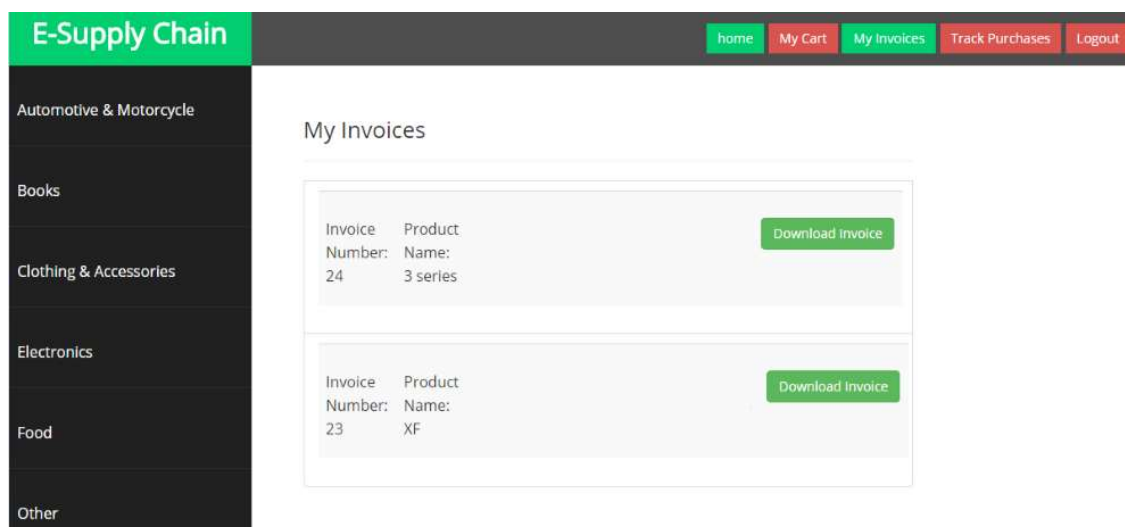
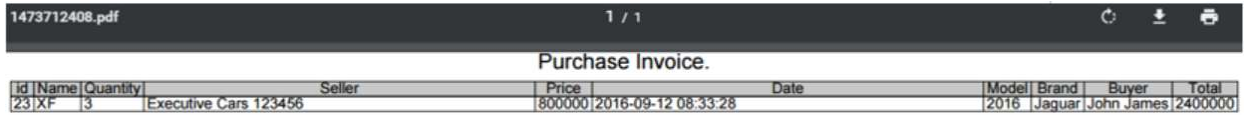


Figure 8.15 Generated Customer invoices

In Figure 8.16 the customer invoice layout is illustrated, showing the name of seller, name of buyer, timestamp, quantity of purchased goods and information about the goods purchased.



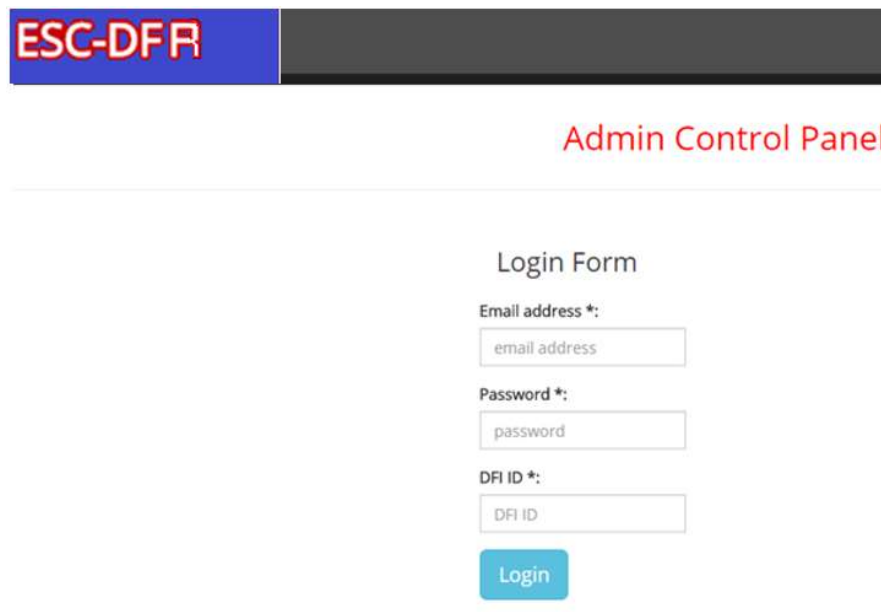
Purchase Invoice.										
ID	Name	Quantity	Seller		Price	Date	Model	Brand	Buyer	Total
231XF		3	Executive Cars 123456		800000	2016-09-12 08:33:28	2016	Jaguar	John James	2400000

Figure 8.16 Generated customer invoice in PDF format

With the functional elements of the eSC app discussed and how users interact with the platform, in the next section the user interface of the eSC-DFR component is explained and the functional elements of the component discussed.

8.4 The eSC-DFR component of the prototype

With the eSC app discussed in previous sections, section 8.4 introduces the eSC-DFR component built for the eSC app and discusses its functional elements. Figure 8.17 shows the login page of the eSC-DFR component that was developed using HTML, CSS and JavaScript and can temporarily be accessed via a web browser with url address http://dfr.esctrade.co.za/_admin.php. On the login page of the eSC-DFR component a DFI is given 3 fields to fill in namely username, password and DFI id number for authentication.



ESC-DFR

Admin Control Panel

Login Form

Email address *:

Password *:

DFI ID *:

Figure 8. 17 eSC-DFR component authentication page

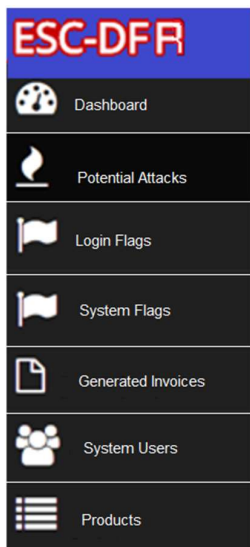


Figure 8. 18 DFI Dashboard in eSC-DFR component

The eSC-DFR component is designed to conduct some pre-analysis to collected PDE in-order to assist investigators with useful information for an investigation.

The home page of a logged in DFI has seven tabs to select from (Figure 8.18). The first tab is the main dashboard of the eSC-DFR component, which highlights a summary of collected PDE. The other six tabs are associated with the different categories of PDE that the eSC-DFR component provides. The tabs allow an investigator to categorically search through all collected PDE and in the following sections the author addresses what each tab provides.

8.4.1 Potential Attacks tab

The *Potential Attacks* tab lists flagged system attacks targeted at the eSC app to bypass the access control component of the eSC app. Examples of attacks include Cross-Site Scripting attacks, Brutefore attack and URL tampering attacks. Cross-Site Scripting and URL tampering are the two main system attacks addressed by the author and used as proof of concept. By definition, Cross-Site Scripting [91] is a security vulnerability typically found in web applications. This type of vulnerability enables attackers to inject client-side scripts into web pages to bypass access controls and manipulate the operations of a web application. URL (Uniform Resource Locator) tampering [92] is a web-based attack which is based on the manipulation of parameters in the web address exchanged between client and server in order to access web pages or modify application data, such as user credentials and permissions, price and quantity of products.

The author chose to address two major attacks that are very prevalent and common in eSC environments. According to the 2017 Year- End Report from Risk-Based Security, Cross-Site Scripting was the most encountered security bug (28.9%) in 2017 [93]. Another source reported that Cross-site Scripting and URL tampering were amongst the top ten website threats in 2017 with effects that vary

in range from petty nuisance to significant security risk [92]. For the above- mentioned reasons the author chose to focus on these two attacks. It is important to point out that there are other tools that are able to detect the above-mentioned attacks, but what separates the eSC-DFR component from other tools is the quality of forensic evidence that it provides and the forensic processes that it follows and complies with in the collection, preservation and presentation of collected evidence. When a DFI clicks on the **Potential Attacks** tab, the following PDE about Cross-Site Scripting and URL tampering attacks is displayed as is illustrated in figure 8.19.

Potential flagged attacks

Export Report

10 records per page Search:

Attack Name	Date/Time Occurred	Source IP	Source Location	RAW DATA
cross-site scripting	2016-08-29 14:45:33	137.215.6.50	{Country: South Africa,ZA;City: Pretoria,Gauteng;Location: -25.7069,28.2294}	<pre><script>alert(1);<script></pre>
URL Tampering	2016-09-12 20:57:30	137.215.6.53	{Country: South Africa,ZA;City: Pretoria,Gauteng;Location: -25.7069,28.2294}	<pre>http://esctrade.co.za/mycart.php</pre>
URL Tampering	2016-09-12 20:50:35	137.215.6.53	{Country: South Africa,ZA;City: Pretoria,Gauteng;Location: -25.7069,28.2294}	<pre>http://esctrade.co.za/mycart.php</pre>
URL Tampering	2016-09-12 20:49:13	137.215.6.53	{Country: South Africa,ZA;City: Pretoria,Gauteng;Location: -25.7069,28.2294}	<pre>http://esctrade.co.za/mycart.php</pre>

Figure 8. 19 Potential flagged attacks Tab

When a DFI clicks the **Potential Attacks** tab there are five columns that are presented with information about a potential attack namely, the attack name, date/time of attack, the source IP of the perpetrator, the location where the attack was executed from and the script/command (raw data) injected by the perpetrator. Below, the author gives examples of how the eSC-DFR component detects Cross-Site Scripting attacks and URL tampering attacks

Cross-Site Scripting – consider a malicious individual X with source IP (137.215.6.50), tries to hack the eSC app by attacking the access control component using a Cross-Site Scripting attack. In this scenario X decides to inject a simple script (raw data) indicated in Figure 8.20 in the username input box of the eSC app login page to verify whether the eSC app web server will respond to requests containing malicious scripts upon which further scripts can be used to manipulate the operations of the eSC app web server.

Attack Name	Date/Time Occurred	Source IP	Source Location	RAW DATA
cross-site scripting	2016-08-29 14:45:33	137.215.6.50	{Country: South Africa,ZA;City: Pretoria,Gauteng;Location: -25.7069,28.2294}	<pre><script>alert(1);<script></pre>

Executed script:
 <Script>alert(1);<script

Figure 8. 20 Cross-Site Scripting attack flagged by the eSC-DFR component

In this instance when the script is executed on the eSC app web server to return an alert pop-up message with the number 1 illustrated in Figure 8.21, the eSC-DFR component analyses the injected raw data to determine if it is a script. If the injected raw data is indeed a script, a Cross-Site Scripting vulnerability incident is flagged by the eSC-DFR component and more data about the incident is logged such as the date/time that the script was injected.

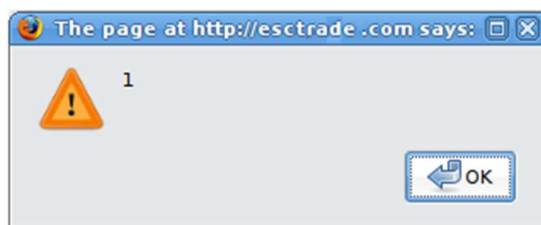


Figure 8. 21 eSC app web server response to injected script

The eSC-DFR component detects scripts that are targeted at the authentication component by analysing the text used in the login and password filled areas. In order for the eSC-DFR component to detect Cross-Site Scripting attacks the author used the php *strip_tags* method. The *strip_tags* method determines whether a string of text contains tags “<>”, in the case of the eSC-DFR component, when a perpetrator injects a script into the username field of the eSC app login page, the *strip_tags* method detects the tags in the inserted text and flags a potential Cross Site Script attack illustrated in Figure 8.20.

The eSC-DFR component detects a script-structured message and therefore immediately captures the IP address of the machine used to inject the script, the time that the event took place using a timestamp function and the source location using an IP address location API. To provide the location of X, the *FreeGeoIp API* is used that provides IP address location. *FreeGeoIp API* is a PHP source location API that provides the exact geolocation of IP addresses from where requests or events are executed. It uses a database of IP addresses that are associated to cities along with other relevant information like time zone, latitude and longitude. In order to identify the geographical location of a request the eSC-DFR component captures the IP address of the user using the server array and sends it to the *FreeGeoIp API* which processes the request providing the location where the request came from, which is then stored in the eSC-DFR component.

URL tampering – assume X would like to delete the webpage *mycart.php* from the eSC app web server so that other users cannot access it when ordering goods. In an attempt to achieve this X tampers with the URL parameters, more specifically the *status* variable used to perform unique functions on web pages within eSC app server such as to read or delete a page. For example to read the *mycart.php* page the URL address is as indicated below:

```
http://www.esctrade.co.za/mycart.php?nr=147&status=read
```

By modifying the *status* variable for the *mycart.php* page from *read* to *del* as illustrated below, the user of a non-protected eSC app website is able to delete the *mycart.php* page from the eSC app web server.

```
http://esctrade.co.za/mycart.php?nr=147&status=del
```

With the eSC-DFR component integrated with the eSC app, all high priority requests to the eSC app web server such as *delete*, *update* and *duplicate* are flagged. Therefore, when the request to delete the *mycart.php* page is sent from the URL to the eSC app web server it is flagged as is illustrated in Figure 8.22.

| Attack Name | Date/Time Occurred | Source IP | Source Location | RAW DATA |
|---------------|---------------------|--------------|--|--|
| URL Tampering | 2016-09-12 20:57:30 | 137.215.6.53 | (Country: South Africa,ZA;City: Pretoria,Gauteng;Location: -25.7069,28.2294) | http://esctrade.co.za/mycart.php?nr=147&status=del |

Figure 8. 22 URL tampering flag

With the potential attacks tab explained and the information that it provides to a DFI indicated, the next tab that the author discusses is the **Login Flags** tab.

8.4.2 Login Flags tab

Login flags tab provides a DFI with logs about successful and failed login attempts by users of the eSC app; information which may be critical to a DFI as it allows a DFI to trace who was using the eSC app, at what time and from where.

Flagged login information

Export Report

10 records per page Search:

| Attempted Email | Date/Time Occurred | Source IP | Source Location | Attempt Flag |
|----------------------------|---------------------|----------------|--|--------------------|
| <script>alert(1);</script> | 2016-08-29 14:45:33 | 137.215.6.50 | {Country: South Africa,ZA;City: Pretoria,Gauteng;Location: -25.7069,28.2294} | failed attempt |
| 1 | 2016-08-31 09:11:22 | 82.145.222.174 | unknown | failed attempt |
| 1 | 2016-08-31 09:11:05 | 82.145.222.174 | unknown | failed attempt |
| bmwmotors.co.za | 2016-09-12 22:55:27 | 137.215.6.53 | {Country: South Africa,ZA;City: Pretoria,Gauteng;Location: -25.7069,28.2294} | successful attempt |
| bmwmotors.co.za | 2016-08-29 22:09:30 | 137.215.6.53 | {Country: South Africa,ZA;City: Pretoria,Gauteng;Location: -25.7069,28.2294} | successful attempt |

Figure 8. 23 Login flags tab

Figure 8.23 shows some logs collected from the authentication component. When a user attempts to login to the eSC network as a supplier, retailer or customer, the eSC-DFR component will capture data about the request as illustrated above. Using the *FreeGeoIp API*, the eSC-DFR component provides the country, city and latitude where the user request came from. as illustrated in Figure 8.23. In the next section the author discusses the **System Flags** tab that lists flagged irregular activities in the eSC app such as price fixing incidents and price overcharge incidents.

8.4.3 System Flags tab

System flags refer to supply chain specific incidents such as price fixing, price overcharge incidents and other malicious operational activities by users. The **System Flags** tab illustrated in Figure 8.24 shows how price overcharge incidents are flagged by the eSC-DFR component.

User ID	Seller	Action	Date	IP Address	Location	Operation
9	Top Cars 126472394	Price Overcharge	2016-08-29 22:59:43	137.215.6.53	{Country: South Africa,ZA;City: Pretoria,Gauteng;Location: -25.7069,28.2294}	The new price: 800000 is more than 50% of supplier product {id=2,Original price=500000}
9	Top Cars 126472394	update_product_info	2016-08-29 22:59:28	137.215.6.53	{Country: South Africa,ZA;City: Pretoria,Gauteng;Location: -25.7069,28.2294}	Product was successfully updated.
9	Top Cars 126472394	Price Overcharge	2016-08-29 22:59:27	137.215.6.53	{Country: South Africa,ZA;City: Pretoria,Gauteng;Location: -25.7069,28.2294}	The new price: 800000 is more than 50% of supplier product {id=2,Original price=500000}
9	Top Cars 126472394	update_product_info	2016-08-29 22:58:52	137.215.6.53	{Country: South Africa,ZA;City: Pretoria,Gauteng;Location: -25.7069,28.2294}	Product was successfully updated.
9	Top Cars 126472394	Price Overcharge	2016-08-29 22:58:52	137.215.6.53	{Country: South Africa,ZA;City: Pretoria,Gauteng;Location: -25.7069,28.2294}	The new price: 700000 is more than 50% of supplier product {id=5,Original price=400000}

Figure 8. 24 System flags tab

Using the product price set by a supplier and the product price set by a retailer, the eSC-DFR component is able to compare between retailer price and supplier price to determine whether the price margin is more than what is prescribed as reasonable by law. To achieve this, a *flagPriceChange* function is used as illustrated in Figure 8.25. In the *flagPriceChange* function used, the eSC-DFR component compares prices and flags a price overcharge incident if the retailer price is more than 50% of supplier price. The flagged profit margin value depends on the laws of a particular country, therefore 50% used is for illustration purposes.

```
private function flagPriceChange($pid,$price,$stprice)
{
    □
    $cprice = $stprice+($stprice*(50/100));
    //Flag if new price is more than 50% of supplier price
    if($price > $cprice)
    {
        //Call logData function and freeGeoIp API and send logged data to
        eSC-DFR database
    }
}
```

Figure 8. 25 *flagPriceChange* function

As a hypothetical scenario, consider that in South Africa the law limits profit margins on sales to 50% on vehicles. If a retailer, Top Cars referred to in Figure 8.24 purchases a vehicle from a supplier at R300 000 to sell vehicle at R800 000, the eSC-DFR through the *flagPriceChange* function will flag the price change as a price overcharge incident as indicated in Figure 8.24.

For all the transactions that are conducted by different users of the eSC app, invoices are generated which are captured by the DFR component and presented in the Generated Invoices tab. In the next section the author discusses the *Generated invoices* tab.

8.4.4 Generated Invoices Tab

The *Generated Invoices* tab provides the DFI with records of all the invoices generated by retailers and customers across the eSC app. As part of the *Generated Invoices* tab, checksum functionality of generated invoices is provided to identify manipulated invoices using the eSC-DFR component generated invoice and its hash value and an external invoice and its hash value. The MD5 Hash Function is used to check for file corruption or file differences of PDE. The MD5 hash function was chosen for its ability to hash files fast without requiring a lot of processing power [94].

Invoices Generated				
10 records per page		Search: <input type="text"/>		
Invoice Number #	User	Filename	Invoice Checksum	Verify Checksum
1	#10 FirstClass vehicles 12487927592	Download Invoice	8c2b032f10586f84b02562697c3c7462	Upload Invoice
2	#10 FirstClass vehicles 12487927592	Download Invoice	8e918deec8eac925a571f21b4cd0de3d	Upload Invoice
3	#10 FirstClass vehicles 12487927592	Download Invoice	a37f6869a0fa6bc30309c0e120bf0e1d	Upload Invoice
4	#10 FirstClass vehicles 12487927592	Download Invoice	cf84cd3c9ccc664dab0f9443a1611af0	Upload Invoice
5	#8 Executive Cars 123456	Download Invoice	7c5a3690ffd217e6f832c25e79f048ed	Upload Invoice

Figure 8. 26 eSC Generated invoices

As is illustrated in Figure 8.26, the eSC-DFR component keeps track of all the generated invoices from the eSC app e.g. when suppliers sell to retailers and retailers sell to customers. When an invoice is generated for a transaction, it can be downloaded as a PDF by the end-user or viewed on the browser. On the eSC-DFR component side, it is stored in the eSC-DFR database as a pdf file including the name and hash of file. Therefore, when a DFI needs to verify the particulars of a transaction they can download the invoice. If they want to verify if the file generated for the end-user was not tampered with by a third party they can upload the file in question and verify using a checksum function, that compares the hash values of both files. If an invoice is manipulated by a malicious individual attempting fraud, a DFI can upload the malicious invoice to compare with the original one that was stored in the server as illustrated in Figure 8.27.

Verify PDF Invoice Checksum

Your invoice file:

wisa09p1.pdf

Original Checksum:
8c2b032f10586f84b02562697c3c7462

Uploaded Checksum:
e6860e4212621a773ad47ad3cc5fc0bb

Figure 8. 27 invoice manipulation check function

If the hash values do not match, that means the uploaded file has been manipulated or is not the correct file, which could suggest a file manipulation incident by a perpetrator e.g. changing the number of vehicles purchased or shipping dates for transporting vehicles. In-order to achieve this the author created a filecheck function that determines if the hash value from an uploaded invoice pdf file matches the hash value of the invoice pdf file logged by the eSC-DFR from eSC app.

For example, consider a retailer has sold a vehicle on the eSC app to a customer. In order to complete the transaction an invoice is generated. Upon reconsideration the customer decides they wanted another vehicle instead of the one purchased. Because it is against the retailer’s company policy to undo an already concluded transaction, the customer decides to manipulate the data in the generated invoice to match those of the vehicle they want and accuse the retailer of shipping the wrong vehicle. With the eSC-DFR system in place the DFI goes straight to the checksum function of the eSC-DFR component to compare the customer’s invoice and the eSC-DFR system generated invoice. From the **Generated Invoices** tab, the DFI can search for the transaction between the retailer and customer. If the hash values of the invoices match, that means the customer is correct and the retailer is in the wrong. If hashes do not match that clearly means the customer is in the wrong and further action can be taken.

In the next section the author discusses the **System Users** tab and the PDE it provides.

8.4.5 System Users tab

The **System Users** tab allows an investigator to have a list of all the eSC stakeholders and their information e.g. name, address and company registration number and a chart that shows all the price changes that they have executed in the eSC app (for suppliers and retailers).

9	Top Cars 126472394	Contact: +27117438472 1224 Hatfield	Retailer	View Graph
---	--------------------	--	----------	----------------------------

Figure 8. 28 System users tab

As illustrated in Figure 28, the **System Users** tab shows the name of eSC stakeholder, contact number and address of stakeholder, type of stakeholder and the option to view the graph that represents the stakeholder’s pricing history. From the list, a DFI can view the price change chart of retailer Top Cars indicated in Figure 8.29. This chart shows the price set by a supplier for a vehicle with product id 14 (red) and the price that the retailer Top Cars changed it to for sale (blue). As the DFI moves across the chart, he should be able to view the pricing for different products. This information can be very useful to a DFI to catch a price overcharge incident referred to in the **System flags** tab in a matter of seconds. For example if retailer Top Cars bought a vehicle with product id 14 as is illustrated in Figure 8.30 at R450 000 and raised the selling price to R600 000, the graph will indicate that price change. If for instance the retailer changed the selling price to more than 50% of buying price, the graph will clearly indicate that price overchange, making it easy for a DFI to detect such an incident.

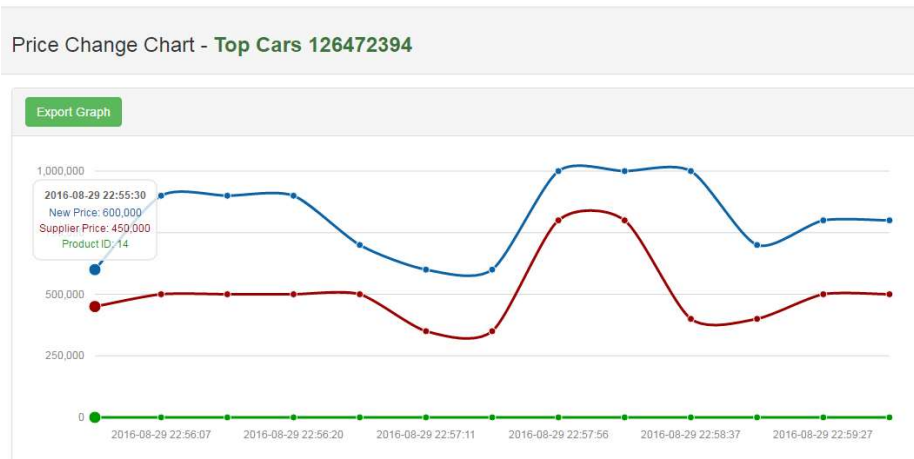


Figure 8. 29 System users tab and price change chart

In-order to generate the graph the author used the Morris javascript library which gets data from the eSC-DFR database based on the product id and encodes it to a JSON object and parses it as a parameter to the Morris javascript library as illustrated by the getPChart function below in Figure 8.31.

```

public function getPChart($id)
{
    $data = $this->getGraphByProduct($id); //gets product data
    $_SESSION['for'] = $this->getProductByID($id); //get product name
    $_SESSION['view'] = ($data != FALSE)? //generates graph
    openssl_encrypt(
        ('<script>Morris.Line({element: "morris-line-chart", data:
        ', json_encode($data).' , xkey:
        "g_date", ykeys: ["g_value", "g_original_value", "g_user"], labels:
        ["New Price", "Supplier Price", "User ID"], linecolors:
        ["#0b62a4", "#9a0000", "#009a00"], parseTime: false, smooth: true, resize:
        true});</script>')
        , EALGO, EPASS) : openssl_encrypt('<p>No graph data available.</p>', EALGO, EPASS);
}
  
```

Figure 8. 30 Chart generating function

In the next section the author discusses the **Products** tab and the PDE it provides.

8.4.6 Products Tab

The **Products Tab** illustrated in figure 8.32 provides a DFI with all the information about all the products that were in the eSC app and the supplier pricing history for each product, which is provided in the form of a chart as illustrated in Figure 8.33.

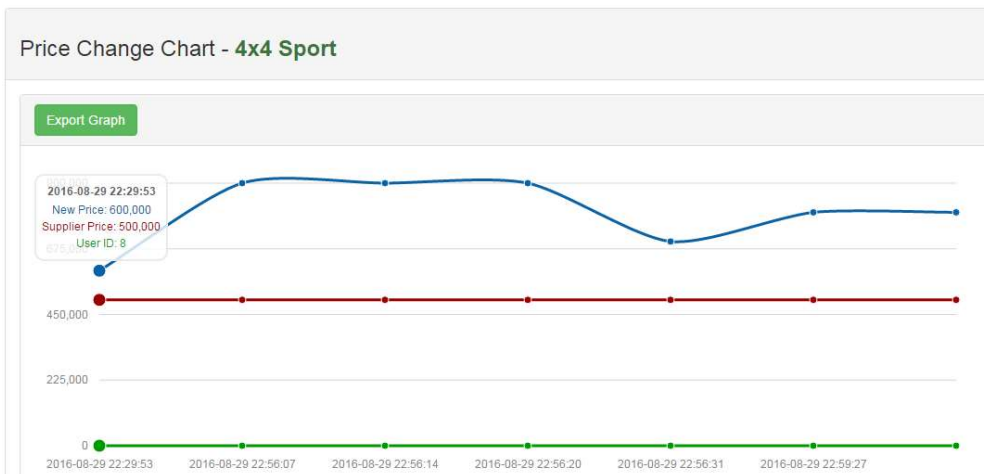


Figure 8. 31 Chart generating function

ID#	Product Name	Supplier/Manufacture	Action
1	Sneaker X	Matome Suppliers AdXds12/2016	View Graph
2	4x4 Sport	Range Rover motors 12345678	View Graph
3	Discovery	Range Rover motors 12345678	View Graph
4	Luxury SUV	Range Rover motors 12345678	View Graph
5	Evoque Convertible	Range Rover motors 12345678	View Graph
6	XF	Jaguar 987654321	View Graph
7	F-type	Jaguar 987654321	View Graph
8	XK	Jaguar 987654321	View Graph
9	XJ	Jaguar 987654321	View Graph
10	Jetta	volkswagenmotors.co.za 135790	View Graph

Figure 8. 32 Products tab and price change chart

PDE in the **Products Tab** makes it easier for a DFI to identify the pricing history of all the products sold by suppliers. As a hypothetical scenario consider a simple price gouging incident where retailers decide to manipulate the prices of the products they are selling to customers. Such an incident would need reliable digital evidence to support such a serious allegation against a group of retailers. Without a DFR in place to prepare the eSC network environment for such incidents, the investigative process would be cumbersome and time consuming for a DFI. Without a standardised and traceable approach for collecting potential evidence it would be highly unlikely that collected PDE would be admissible in a court of law. With an eSC-DFR component in place that has its architecture based on the eSC-DFR process model and ISO/IEC 27043 [13], the accuracy of collected PDE can be validated. In the scenario provided there are a few easy steps that a DFI needs to follow to access PDE, namely:

- Obtain a search warrant to present to the eSC service provider.
- Obtain access credentials to the eSC-DFR component from a system administrator.
- Login to the eSC-DFR component as DFI using DFI id number and system generated password.
- From Dashboard of the eSC-DFR component the DFI can click on the **Products Tab**.
- Search for the specific product that is reportedly being overpriced.
- Access a graphical representation of the price changes of the product over time which includes the dates when the price was changed. This gives the DFI a clear indication of the pricing pattern of a retailer and clear visibility as to whether there was a price gouging incident.

With that information a DFI through the eSC-DFR component is able to export the graph and transaction history of the accused retailers to generate a report that is reliable for investigative purposes. This is illustrated in Figure 8.34 and Figure 8.35 with the example of a 4x4 sport vehicle sold by Range Rover motors where the pricing history of the vehicle is clearly visible through a graph and the supplier of the vehicle can be identified.

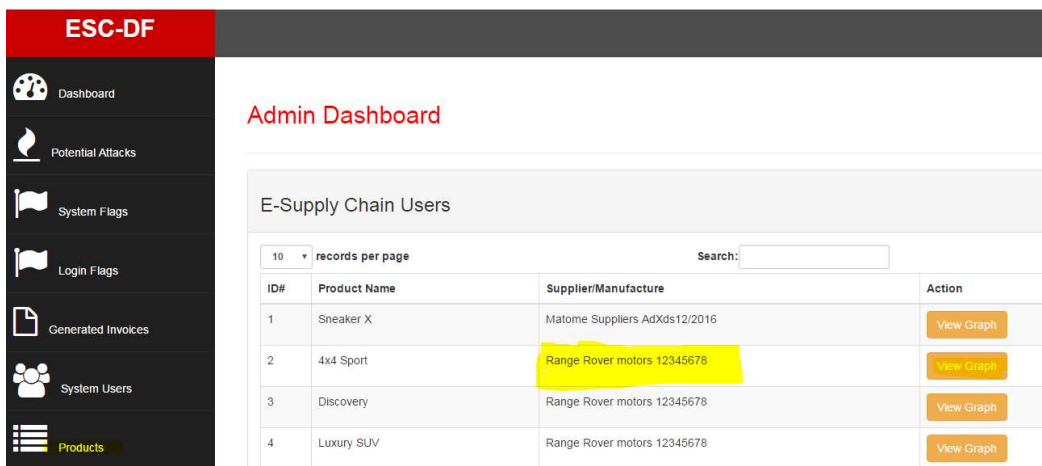


Figure 8. 33 eSC-DFR component Products PDE

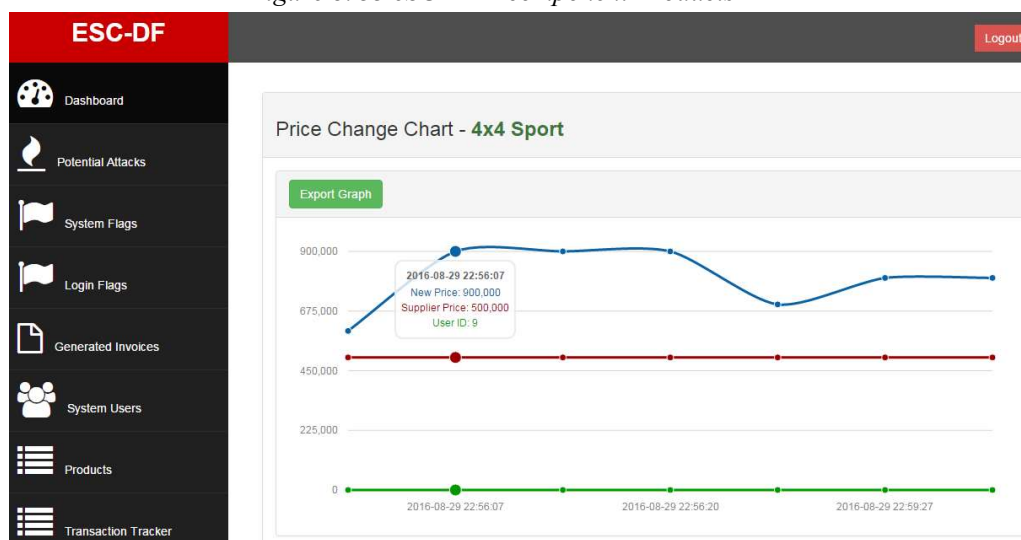


Figure 8. 34 A graphical representation of the vehicle price changes

From Figures 8.34 and 8.35, one can clearly see that Retailer (User ID 9) overpriced the Range Rover 4x4 sport from 500 thousand rand (supplier price) to 900 thousand rand which can be identified as price gouging and an offence in some countries [95]. From the Price Change Chart in Figure 8.35 a DFI can identify User ID 9 as the user that changed the selling price of the vehicle. Using the System user tab in Figure 8.30 a DFI can identify User ID 9 as retailer Top cars. In the next section the author discusses a price fixing incident and how the eSC-DFR component could assist law enforcement in identifying such an incident.

8.5 Conclusion

The eSC-DFR system prototype serves only as a proof of concept and is not in itself the contribution. The focus of the dissertation was on the DFR process model and architecture design for eSC environments. The processes identified were seen as processes which are not included currently in eSC forensic tools. Before implementing the eSC-DFR process model and system design, various shortcomings of current eSC forensic tools were identified especially in relation to forensic readiness. For the sake of this research forensic readiness processes were examined, with ISO/IEC 27043 standard being the closest model of choice that the eSC-DFR process model was built on, discussed in Chapter Five. The eSC-DFR system prototype was discussed with the functional requirements from Chapter Six being the focus of the discussion. The eSC-DFR process model processes that are supported by the prototype were also illustrated and discussed briefly. The aim of the eSC-DFR system prototype is not to be a complete solution to the eSC digital forensics framework. This leaves scope for further development on a number of the eSC digital forensics processes. The aim of the eSC-DFR system prototype was to draw attention to address to what can be achieved by taking a proactive approach to forensics in eSC networks.

Chapter 9

Critical Evaluation

9.1 Introduction

This chapter evaluates various aspects of this research. It analyses how the research conducted addresses the objectives set out in Chapter 1 and the shortcomings that were realised whilst conducting the research. The chapter begins with an overview of the purpose of this research, which is to propose a proactive forensic approach for the management of risk caused by sharing information between trading partners in eSC environments. This is with reference to the design of an eSC-DFR process and system that will provide DFI and law enforcement with readily available PDE. The research was motivated by a lack of digital forensic readiness tools tailored for eSC network environments and the use of non-standardised tools for the collection of PDE in eSC environments resulting in inadmissible PDE which would not stand up in court. What is proposed by the author is an eSC-DFR process model which complies with ISO/IEC 27043 and ISO/IEC 27002 [17] to provide a framework for the design and development of a forensically ready eSC environment referred to as an eSC-DFR system. By incorporating eSC-DFR components in eSC environments that collect, store and maintain collected PDE, DFIs and law enforcement agents can have readily-available and sound evidence to address or mitigate security risks within eSC environments.

The remainder of this chapter is structured as follows. Section 9.2 discusses the benefits of this research. In section 9.3 the author discusses some shortcomings that were realised during the research. The chapter is concluded in section 9.4.

9.2 Primary Benefits of the Research

The eSC-DFR system developed is a web-based application that generates PDE about any activity within an eSC network environment. The PDE collected by the eSC-DFR component may be used by DFIs to uncover malicious behaviour across the eSC network environment by intruders or by non-compliant eSC trading partners. Seeing that the eSC-DFR component enables DFIs and law enforcement agents to effectively manage security incidents within eSC network environments, the following primary benefits were identified as result of this research namely:

- The eSC-DFR process model based on standardised principles;
- Implementation of the eSC-DFR process model
- Usability requirements of eSC-DFR component defined;
- PDE preservation by eSC-DFR component; and
- PDE pre-analysis by eSC-DFR component.

9.2.1 An eSC-DFR process model based on standardised principles

The research conducted provides a systematic approach to the incorporation of digital forensic readiness in eSC network environments. Due to the complexity of eSC infrastructure as compared to the traditional supply chains, it is necessary to rethink the security methods used to secure information and prepare for new threats that come as a result of ICT. Therefore, the problem this research aimed to address was the lack of a well-formulated approach for eSC network environments to prepare for security incidents that might occur due to the use of ICT. This research proposed the incorporation of a DFR process across the eSC network environment as a solution to the problem. The reason for this is that DFR prepares trading partners for information security threats, helps them identify vulnerabilities and provides data that can be used to conduct risk assessments and forensic investigations. In this research the DFR process model from ISO/IEC 27043 was adopted and integrated into the eSC model to create the eSC-DFR process model. This model suggests that data can be collected from the eSC network environment, validated and securely stored for analysis using techniques such as logging, encryption and hashing amongst others. The eSC-DFR process model defines processes that are to be followed in the development of eSC-DFR systems that are based on standardised principles; the focus being on processes that provide measures to reduce crime and generate forensically sound potential evidence.

9.2.2 An implementation of the eSC-DFR process model

This research started by introducing an eSC-DFR process model upon which eSC-DFR tools must be built. The research proposed that strategic PDE locations in eSC network environments must be identified for PDE collection and that collected PDE must be stored in a secure central data repository for PDE pre-analysis and PDE retrieval by DFIs and law enforcement agents. The research went further to illustrate the eSC-DFR process model in action by following the eSC-DFR process model in the design and development of a working eSC-DFR system prototype. It went a step further to present real-life case studies for its illustrations. The eSC-DFR system prototype comprises of the eSC network web application and the eSC-DFR component. The eSC network web application is a platform that allows for trade between trading partners and the eSC-DFR component is used to store PDE, retrieve PDE by authorised users and maintain PDE. Each of the authorised users maintain a level of access as allocated by the system administrator.

9.2.3 Usability of eSC-DFR component

One of the problems that this research addresses is the lack DFR tools that are designed to support eSCs specifically. The literature review conducted at the beginning of this research indicated that at present there are general-purpose monitoring tools that have forensic readiness functionality, but none are

specifically designed to serve eSC network environments in relation to criminal activity such as price fixing, data manipulation and price gouging. It is the view of the author that the conclusions drawn from this research can spearhead the development of cutting-edge eSC-DFR tools that do not only address information security threats but also help regulate compliance to trade policies. The difference between an eSC-DFR component and an intrusion detection monitoring tool is that the eSC-DFR component is focused on capturing and providing PDE that can help law enforcement agents and DFIs in crime investigations related to criminal activity conducted on eSC platforms.

The eSC-DFR component ensures the preservation of PDE from the time it is collected to its usage in a court of law. The author took into account that the usability aspect of an eSC-DFR tool is of utmost importance. Most monitoring tools are not easy to navigate, making it difficult for users to identify incidents when they occur or to monitor traffic. On the other hand, the developed eSC-DFR component displays collect PDE in such a manner that it is easy to deduce and trace events recorded. The user interface of the tool provides DFIs and law enforcement with enough flexibility to either view, download, search categorically and filter captured data. A DFI is able to sign up, login and navigate through collected PDE.

9.2.4 PDE preservation by eSC-DFR component

Another benefit that emerged from the research conducted is that it indicated how the dedicated central data repository for PDE ensures the preservation of forensic evidence by complying with ISO/IEC 27043 [17]. This standard is designed to guide information security policies for information systems to enhance digital evidence admissibility. The eSC-DFR central data repository serves as the first point of reference for DFIs and law enforcement in the case of an incident in the eSC network environment. The eSC-DFR central data repository employs digital forensic requirements such as PDE preservation rules, by employing security measures such as encryption and hashing of collected data from the time data is captured to the time it is retrieved for download by a DFI. Such processes were incorporated in the design of the eSC-DFR system in Chapter 7 and illustrated in this the prototype developed in Chapter Eight. The process followed in the design of the eSC-DFR system (illustrated in Chapter Seven) ensures a clear chain of custody from the time that PDE is collected, stored in the eSC-DFR central data repository and downloaded by a DFI for the purpose of an investigation. Applying this audit trail process ensures that collected PDE holds evidential weight in the judiciary.

9.2.5 PDE Pre-analysis by eSC-DFR component

PDE pre-analysis is a crucial step in the eSC-DFR process model because it allows for the generation of insight and context to collected data by providing services such as flagging security attacks, grouping related PDE, flagging non-compliant users and analysing data for graphical representation (which is illustrated in Chapter Eight). One of the objectives of this research was to simplify the data collection

and PDE analysis process a DFI has to conduct in a forensic investigation by presenting collected PDE in a manner that makes for easier PDE analysis and threat detection. Therefore, PDE pre-analysis serves as a process that aims to simplify the role that a DFI has to play in examining collected PDE when conducting an investigation. Such pre-analysis services should be defined in the planning processes group of the eSC-DFR process model, hence the services listed in this research are strictly for the proof of concept.

In the next section the author highlights the secondary benefits to the primary benefits of this research. Such benefits would be experienced by end-users of an eSC-DFR system, such as DFIs, law enforcement agents, and trading partners (TPs).

9.3 Secondary End-user benefits

It is the view of the author that implementing the eSC-DFR process model across an eSC network provides a number of benefits to trading partners, DFIs and law enforcement, such as:

- Time efficiency.
- Cost reduction.
- Credible evidence.
- Available data.
- An Improved trading partner relationship.

Time efficiency refers to the time it takes to conduct an investigation in the case of an incident occurring in the eSC network. With collected data readily available in the eSC-DFR component, trading partners, DFIs and service providers can save a lot on the time required to gather information for different processes such as forensic investigations or risk assessments. A reduction in the time it takes to conduct an investigation and identify vulnerabilities in the eSC network is a major benefit to trading partners as disruptions to business processes can be resolved quickly.

Cost reduction is a direct result of time efficiency and refers to the costs incurred during a forensic investigation or risk assessment, to gather credible evidence and information. It is the authors' opinion that with a DFR system spread across the eSC network, useful information and credible evidence are readily available in the eSC-DFR component for DFIs to use, hence cutting down the costs required to conduct an investigation and risk assessments.

Credible evidence refers to information that can be used as evidence in a court of law. An implementation of DFR provides the eSC networks with potentially useful information that can be used

by DFIs. With timestamps on the collected data and proof that the integrity of the collected data has not been compromised, for instance through hashing, the collected data may can be used as evidence in a court of law to solve cases that may arise in the eSC environment.

Available data is an extension to the previous point in that DFR provides entities in the eSC network not only with data for DFIs, but for any other process that requires information about eSC network activity. The data collected across the eSC network environment is available from the central data repository for TPs to conduct analysis on the security status of the eSC network and can be used for other processes that do not necessarily have to do with information security such as updates on network infrastructure.

An improved partner relationship refers to the impact of implementing DFR in the eSC. It is the authors' opinion that by implementing DFR in the eSC, trust between trading partners can be established to a greater extent. TPs can share information more freely and cautiously with the assurance that all the activities taking place in the eSC are recorded and stored securely. This allows TPs to collaborate on a larger scale with their business partners with the surety that their information is safe and all the interactions taking place in the eSC are traceable.

Section 9.2 and 9.3 highlighted the many benefits of the eSC-DFR process model and its implementation which resulted in a eSC-DFR system. However, there are some shortcomings that are yet to be overcome. These are presented in the next section.

9.4 Shortcomings of Research

Eradicating digital crime in eSC environments and becoming forensically ready can be a challenging task for eSC service providers due to the complexity of different eSC environments and the many security risks that should be considered in the planning stages of the eSC-DFR process. Therefore, some shortcomings were identified as this research was being conducted for example, this research assumes that the eSC network is centralised, making for easier architecture modification to incorporate the eSC-DFR component; where in some cases eSC network environments might be decentralised and incorporating the eSC-DFR component might be a complex task for system architects. Other limitations of research are as follows:

- Inconsistent judicial laws on electronic evidence;
- Privacy Issues; and
- Different Platform requirements.
- Scalability

The author discusses each shortcoming in greater detail in the sections that follow.

9.4.1 Inconsistent judicial laws on electronic evidence

eSc network environments in some cases span across borders and jurisdictions, which creates an inconsistent view on the weight of digital evidence. When cross-border wrongs are committed they may lead to transnational litigation. Due to the inconsistent treatment of electronic evidence in different jurisdictions, some collected PDE may be deemed unusable for an investigation. In an article by the International Trademark Association [96], it is highlighted that various courts and tribunals are inconsistent in their treatment of websites and other electronic evidence.

9.4.2 Privacy Issues

Trading partner privacy and consumer privacy is an important concern for most users of an eSC network environment, hence fears of compromising that privacy may create hesitation on the part of many users to want a centralised repository of all their sensitive information. Also some companies and users are very particular about the geolocation where their information is stored, this is with reference to cloud hosting of eSC platforms. With the technical details of how a user's privacy is protected not easily presented to the users at the forefront, this may create an unwillingness to operate on such a platform. In an attempt to protect the privacy of eSC-DFR system users, this research used information security techniques and technologies both at the front-end and back-end of the eSC-DFR system and assumed that the eSC network application is hosted locally.

9.4.3 Different platform requirements

Another shortfall to the research conducted is that this research does not factor other platforms such as mobile applications and other digital devices used in eSC environments meaning malicious activity conducted on other digital devices might go unnoticed by the eSC-DFR component. Although a case study of applying the eSC-DFR process to mobile application devices and other digital devices was out of scope for this research, it is the view of the author that the framework used in the design of eSC-DFR systems would still apply.

9.4.4 Scalability

An implementation shortfall of the research conducted is that it does not place attention on the factors related to the collection/analysis of collected PDE from various data points across an eSC network which would most likely result in large volumes of data. Large volumes of data that would need processing. This could have tremendous impacts on the efficiency of the eSC-DFR system. Therefore, this could warrant future work for this research in the direction of big data intelligence/scalability of eSC-DFR systems.

9.5 Conclusion

In conclusion to this chapter and to highlight the benefits and shortcomings identified in this research the author created Table 9.1 below.

Table 9.1: Summary of Benefits and shortcomings

No.	Primary benefits	Secondary benefits
1	Introduction to the eSC-DFR process model based on standardised principles	Time efficiency.
2	Implementation of the eSC-DFR process model	Cost reduction.
3	Usability of eSC-DFR component	Credible evidence.
4	PDE preservation	Available data.
5	PDE pre-analysis	An Improved trading partner relationship.
	Shortcomings	
1	Inconsistent laws on electronic evidence based on jurisdiction	
2	Privacy Issues	
3	Different platform requirements	

This chapter highlighted the benefits and shortcomings of this research. It is hoped that the eSC-DFR system can be extended to more platforms and incorporate more digital devices such as IOT and mobile devices. There is clearly a need for a proactive approach to forensics to eradicate and manage crime in this fast growing and evolving digital commerce environment through the use of proactive digital forensics techniques and systems. The successful implementation and application of the eSC-DFR process model should not only reduce crime and provide for better co-operation between law enforcement agents and eSC network service providers but also help to build trust between eSC network users.

The next chapter presents some related literature to shed light on the contributions made by this study.

Chapter 10

Related Work

10.1 Introduction

Over the years organisations have become heavily dependent on computers and the internet. The comprehensive use of computers and the internet for the exchange of information and services has also had tremendous ramifications on the escalation of crime [97]. As a result, monitoring and managing eSC networks has become a mission-critical job for IT. Developments in today's eSC environments which support both internal and external business processes call for cutting edge DFR tools that can assist in the collection, storage and retrieval of PDE in a forensically sound manner. Digital forensic readiness provides processes and tools that enable DFIs and other stakeholders to acquire critical-sensitive data about events in a forensically sound manner. Therefore, this research aimed at defining a standardised approach to the implementation of DFR in eSC environments and the design of eSC-DFR tools for the collection and analysis of PDE. The author during the course of this research published two conference papers focusing the eSC-DFR conceptual model and the design of next generation DFR tools (refer to appendix). Chapter Ten reviews related literature on DFR that has had an impact on this research. The literature reviewed is split into three sections starting with section 10.2 that discusses related work to the eSC-DFR process model and its sub-processes. In section 10.3 the author looks at what other researchers have proposed regarding DFR tools and how far they have been able to go in their research. Lastly, in section 10.4 literature related to requirements specifications of DFR tools is reviewed before the chapter is concluded in section 10.5.

10.2 Related work on the eSC-DFR process

The review starts by referring to the work of Pilli *et al.* [98], who focused on defining a generic framework for network forensics. In their research, Pilli *et al.* [98] studied different network environments to propose a generic network forensics framework comprising of DFR phases and incident response phases. There is a relationship between the DFR phases defined in the network forensics framework and the processes defined in the eSC-DFR process model in that both frameworks highlight the importance of planning for PDE collection, collection of PDE and the preservation of PDE for analysis. The difference is that the concept of network forensics as described by Pilli *et al.* [98] deals mainly with the data found across a network connection. In their research Pilli *et al.* [98] limited their research to analysing traffic data logged through firewalls, intrusion detection systems and routers. The network forensics framework does not attempt to address the usability aspect of eSC-DFR tools or the collection and analysis of transactional data collected in eSC networks about malicious behaviour by users or user non-compliance to eSC network policies. In their proposed framework Pilli *et al.* [98]

specifically focus on security threats related to cyber-attacks and in their model do not make reference to other types of threats more specifically to eSC network environments.

In a quest to develop an eSC-DFR process model that complies with global standards, the ISO/IEC 27043 DFR model was used as a guideline for the development of the eSC-DFR process model. ISO/IEC 27043 clearly groups processes according to where they lie in the DFR process such as the planning processes group, implementation processes group and assessment of implementation processes group. This allowed the author to identify processes in each process group that would apply to the eSC network environment. Also considered was the iterative nature in which the DFR model is structured which allows for constant improvement and refinement of a DFR process implementation.

Another researcher, Endicott-Popovsky [99] in her research contends that changing the implementation of DFR from reactive to proactive necessitates new investment in the way networks are managed. In her research Endicott-Popovsky [99] urges organisations to devote new resources to fund procedures and technology that will allow for the collection of forensically sound digital evidence. In her research Endicott-Popovsky points out three research questions that must be considered when attempting to reduce inefficiencies in conducting digital forensic investigations namely:

- What are the challenges faced by entities when conducting forensic investigations?
- How can forensic investigation inefficiencies be reduced?
- How can DFR be implemented in an enterprise to address inefficiencies?

The current research addresses the questions highlighted by Endicott-Popovsky [99] by looking at the security challenges faced in eSC networks in relation to forensic evidence and the cost associated with such inefficiencies. By highlighting the challenges faced in eSC networks, processes and techniques to reduce inefficiencies were identified and incorporated in the eSC-DFR process model such as PDE source identification, PDE collection techniques and PDE preservation. A roadmap to the implementation of an eSC-DFR system was established partly by addressing the research questions posed by Endicott-Popovsky [99].

According to Pooe [100], there are four critical components that form part of the DFR conceptual model comprising of people, process, policy and technology. In his research, Pooe [100] acknowledged the need for a consolidated framework that can help to address the present security threats facing information systems. He stresses that the sophistication of present security threats necessitates the need for a DFR model to aid organisations in aligning efforts that ensure that credible evidence can be retained during normal business operations. Pooe [100] mentions that people play a pivotal role in ensuring that DFR is properly implemented and refers to acquiring the right skills to manage forensic operations in an organisation. He also highlights the need for organisations to follow a standard forensic readiness approach that ensures no contamination of digital evidence and provides the organisation with

a guide to meeting the requirements set by regulatory framework and organisational policies. Some of the key processes that form part of the DFR process model have to do with securing evidence without contamination, acquiring digital evidence without altering or damaging the original, authenticating that the recovered evidence is the same as the original seized data and analysing the evidence without modifying it.

In the present research the eSC-DFR process model employs encryption, hashing and user authentication as measures to ensure that PDE is preserved. According to Poee [100], policy formulation and implementation is another element that is critical for an organisation to achieve forensic readiness. He refers to six categories of forensic readiness processes proposed by Rowlingson [25] to govern the retaining of information, facilitate the planning process for incident response, policies for the training of staff, policies that address operational aspects of an investigation and policies that address the handling and protection of evidence. The eSC-DFR process model adopts key policies/controls from ISO/IEC 27043 that reinforce the importance of maintaining a chain of custody of PDE and ensuring that the integrity of PDE is preserved at all times. Although the conceptual model proposed by Poee [100] provides a holistic view of how organisations should view DFR, it is very generic in nature and is not targeted to a specific stakeholder's environment such as the eSC-DFR model which is for the eSC environment.

In the next section the author reviews related literature on digital forensic evidence integrity and admissibility.

10.3 Related work on DFR tools

The cloud is rapidly becoming the destination for hosting enterprise systems, including eSC networks. In 2013 Dystra [101] proposed a cloud forensic tool (FROST) for the OpenStack cloud platform. The implementation for the OpenStack cloud platform was developed to support an Infrastructure-as-a-Service (IaaS) cloud and provide trustworthy forensic acquisition of virtual disks, API logs, and guest firewall logs. Unlike traditional acquisition tools, Dystra [101] designed FROST to work at the cloud management plane rather than interacting with the operating system or SaaS level inside the guest virtual machines, thereby requiring no trust in the guest machine. On the other hand the eSC-DFR system is not limited to system logs but rather is designed to provide PDE that spans from system logs to user operation logs. According to Dystra [101], FROST uses encryption and hash functions for evidence validation and preservation which the eSC-DFR system does as well. Part of the motive to develop FROST was that Dystra [101] wanted to enable forensic investigators to obtain forensically sound data from OpenStack clouds independent of service provider interaction. Part of the motive to develop the eSC-DFR system was to enable forensic investigators to obtain forensically sound data eSC network environments with limited service provider interaction. The eSC-DFR system attempts to minimise the

interaction between DFIs and service providers by providing an independent eSC-DFR component/dashboard for authorised DFIs to access and collect PDE without service provider supervision.

In another research study, Stephens *et al.*, [102] acknowledge that methods of threat detection that rely on system log auditing and rule breaking are inadequate and lack user attribution and as such are incapable of detecting threats caused by users that operate within their privileges. On the other hand, Stephens *et al.*, [102] also acknowledge that threat detection methods based on focused user-observation tools are only effective once the subject of the threat has been identified. Therefore, both types of methods lack the “smart” analysis capabilities required to analyse and categorise large volumes of generated data, which tends to be the norm in a large organisation network. The eSC-DFR system applies the same “smart” analysis concept referred to as the DFR pre-analysis process for the extraction of insight on captured data. Stephens explored the concept of an insider threat detection system that detects when trusted insiders misuse information in a manner consistent with espionage.

Furthermore, the insider threat detection system that was proposed exploits subtle differences between legitimate and malicious behaviour by leveraging contextual information about users and the information with which they interact. The eSC-DFR system proposed in this dissertation contextualises the concept presented by Stephens and his colleagues by focusing specifically on the eSC network environment and the malicious behaviour conducted by eSC network insiders as well as external users. The research by Stephens *et al.*, [102] focused specifically on information espionage by malicious individuals inside an organisation’s network. On the other hand, the eSC-DFR system aims to address a larger scope of security threats and malicious behaviour specific to eSC network environments such as information espionage, price gouging and price fixing.

Angeles [103] in 2015 conducted research on an event tracking system (ETS) for web-based applications that tracks client server communication over http and ftp protocols to detect any malicious behaviour by users over the internet. Angeles [103] indicated that the tracking of user behaviour over web sites for malicious behaviour in relation to e-commerce transactions, credit card transactions and user account creation is usually captured as system logs, leaving out a lot of critical information that is crucial from a legal standpoint. Therefore, in his research Angeles [103] proposes an ETS system that reports on many different types of known online activity and data including but not limited to purchases from the sale of goods and services online, online shopping cart abandonment, airline ticket reservations, credit card type usage and user account creation. The concept proposed by Angeles is aimed at providing the investigator with as much data as possible for analysis purposes. The eSC-DFR system also follows the same concept of collecting as much PDE from the eSC network environment at a network and browser level ensuring that DFIs have much PDE for analysis. Angeles [103], however, does not indicate or suggest the use of any forensic procedure in the acquiring and storage of logged

information, whereas the eSC-DFR system follows a strict eSC-DFR process based on standardised digital forensic principles to ensure that collected evidence is admissible in a court of law.

In the next section the author looks at related literature on requirement specifications of digital forensics tools.

10.4 Related work on DFR tool requirements specifications

Richard [104] in his research was concerned with the state of digital forensics and highlighted that investigators have access to a wide variety of tools, both commercial and open source, which assist in the preservation and analysis of digital evidence. He also pointed out that unfortunately, most digital forensic tools fall short in that they are unable to cope with the ever-increasing storage capacity of target devices. Furthermore, the research highlighted the need for high-performance computing and more sophisticated analysis techniques, such as automated categorisation of data to handle huge amounts of captured data in our current sophisticated network environments. Richard's also stressed the importance of more sophisticated evidence discovery and analysis techniques, and better collaborative functions are necessary to allow digital forensic investigators to perform investigations much more efficiently than they do today.

Ayers [51] introduced fundamental requirements for second generation computer forensic tools by first highlighting to shortcomings of what he refers to as first generation computer forensic tools. Ayers [51] stated to five limitations that industry standard tools have such as slow processing speed, limited auditability, poor support for planning of investigative tasks, software errors (unexplained crashes of forensic tools), limited support for task automation, and data abstraction. He also highlighted how first generation computer forensic tools struggle to keep pace with modern analysis workloads and do not provide much insight into their inner workings to determine the accuracy of how PDE has been interpreted. Ayers [51] also indicated that first-generation tools provide poor support for detailed planning of investigative tasks and recording the detailed results of investigative processes, leaving it to DFIs who end up using nonconventional methods of planning their investigation, skipping crucial steps. He therefore, recommended the incorporation of four key requirements for second-generation computer forensic tools namely parallel processing using computational resources of many separate processors, scalable data storage for forensic evidence, exceptional accuracy and reliability metrics in all validation tests and auditability of forensic tool- source code for independent review. There are key elements in Ayers' research that the eSC-DFR system incorporates in its architecture design such as the parallel processing, data validation, auditability of code and scalability of data storage which are highly critical to ensure excellent performance and accuracy of the eSC-DFR system.

Garfinkel et al.,[105] stressed that DFIs need tools that can detect, prevent, reconstruct and analyse forensic evidence. The author noted that there is a need for the auditability of digital forensic tools in

order to generate accurate results. Furthermore, the authors highlighted the need for reproducible techniques and results including the use of a standardised forensic process in the designing of digital forensic tools.

Grispos *et al.*, [106] indicate in their research that the majority of organisations commence investigation with determining the events that led to an incident. Unfortunately in most cases the necessary data to draw any conclusions is lost due to a range of reasons. The authors emphasised against implementing a reactive digital forensic process and recommended adopting a proactive approach to forensics. The authors called for the need to implement DFR processes that ensure that systems are forensically ready, providing readily available evidence with the benefits of minimising costs associated with conducting an investigation. In their research the authors went on to use a survey to identify at what point in time do organisations tend to consider digital forensics requirements, whether it is at the beginning of a digital forensic design or post-delivery of a digital forensic system. The research findings show that organisations consider requirements for forensics during various stages in the development process especially at post-delivery. Grispos *et al.*, [106] recommend integrating the DFR process in the digital forensic tool design at the beginning of a digital forensic tool design to ensure that the needs of PDE that may arise when an incident occurs are taken care of.

The eSC-DFR process model ensures that DFR requirements are defined at the beginning stage of an eSC-DFR system as presented in this dissertation. The author follows a systematic, repeatable process that ensures that the same results are achieved repeatedly as a result of applying a transparent standardised process to the development of an eSC-DFR system. Literature on requirements engineering for DFR system design is at a minimum at the time this research was conducted.

Having presented some selected literature, the next section summarises the literature and identifies the contribution of this research in comparison to the related literature presented here.

10.5 Conclusion

In this chapter the author examined related work of other researchers who conducted research in the area of digital forensics in networked environments. From the related work reviewed, it is evident that numerous researchers in their work defined processes and steps to achieve DFR in networked environments. It is also evident that other researchers designed and developed network monitoring tools that collect and analyse data for the prevention and detection of threats in different web-based environments including eSC network environments. However, little to no attention has been focused on incorporating DFR principles or techniques in the design of such tools to ensure that such tools comply with DFR standards and controls. DFR puts emphasis on maximising an environment's ability to provide readily available PDE and ensuring that the forensic soundness of all collected PDE is effected.

Therefore, in this research the author provided a framework for the design of eSC-DFR tools that proactively perform crime prevention and detection functions using standardised DFR principles. The research also illustrated the critical role an eSC-DFR system could play in assisting DFIs in conducting an investigation by providing them with forensically sound potential PDE; and not only that, but also to assist them in identifying threats and malicious conduct by performing pre-analysis on collected PDE. It is also evident from the reviewed literature that there does not yet exist a comprehensive model that enables eSC network environments to generate forensically sound evidence that can be used in a court of law against security incidents and malicious activity. This research therefore focused on closing that gap by looking at numerous security incident scenarios in eSC environments and proposed an eSC-DFR process model based on standardised principles that provides processes, techniques and controls that should be incorporated in the design of eSC-DFR systems in order to achieve DFR eSC network environments.

The next chapter concludes this research by taking a broader look at the problem statement discussed in Chapter 1 and determining to what extent the problems were addressed.

Chapter 11

Conclusion

11.1 Introduction

The internet over the last few years has revolutionised how companies conduct business across the globe. The sharing of information between trading partners and consumers over the internet through specialised networks such as eSC environments has allowed for companies to experience tremendous growth and allowed for closer collaboration between them. It is needless to say that this has also left trading partners and consumers vulnerable to new threats that are inherent to the internet. This research takes advantage of the information that is generated in an eSC network environment and uses it to proactively prepare trading partners for incidents and provide DFIs with the necessary forensically sound information in the event of an investigation. Chapter Eleven gives a summary of this research, starting with revisiting the problem statement and concluding with the contribution presented in this dissertation. Therefore, the remainder of this chapter is broken down into the following sections. Section 11.2 gives a brief summary of all the chapters in this dissertation, section 11.3 revisits the problem statement, section 11.4 points to future work, section 11.5 presents a Table showing the contribution of this research and lastly section 11.6 provides some final concluding remarks about this research.

11.2 Summary of Dissertation

In this section the author gives a brief summary of each chapter of the research in order for the reader to understand the purpose of each chapter and follow the structure of the entire dissertation.

- Chapter 1 was an introductory chapter to the research focusing on the problem statement. The chapter also outlined the objectives and methodology used to address the identified research problems.
- Chapter 2 provided background literature on digital forensics and its processes. It further introduced the terms used in digital forensics throughout this dissertation. The chapter also went further to provide literature on digital forensic readiness and detailed the techniques and processes used to achieve digital forensic readiness.
- Chapter 3 provided background on eSC networks, describing the technical elements and architecture that make up eSC networks.
- Chapter 4 introduced the DFR challenges facing eSC network environments in relation to other researchers' literature. The chapter summarises the DFR challenges faced in eSC network environments that this research aims to address.

- Chapter 5 introduced the eSC-DFR process model proposed for the design and development of eSC-DFR systems. The chapter concentrated on the DFR process that entities should follow in order to achieve forensic readiness in eSC environments and presented a high level conceptual model of an eSC-DFR process implementation.
- Chapter 6 focused on the requirements that an eSC-DFR system must fulfil. The requirements discussed in Chapter Six were based on the research problem given in Chapter 1 and the identified eSC challenges highlighted in Chapter Four. Therefore the functional and non-functional requirements of an eSC-DFR system implementation were defined in Chapter Six.
- Chapter 7 designed the eSC-DFR system using the eSC-DFR process model in Chapter Five and the requirements described in Chapter Six as a reference. The design comprises of key components that perform different functions in an eSC-DFR system.
- Chapter 8 presented the prototype of the eSC-DFR system, where the DFR components in Chapter Seven were developed as a web application termed the eSC-DFR component.
- Chapter 9 focused on evaluating this prototype and focused on its benefits and shortcomings.
- Chapter 10 reviewed related literature and examined similar work conducted by other researchers/authors and their contribution to the field of digital forensic readiness.
- Lastly, Chapter 11 provides a summary of this research, to what extent the problem has been addressed and points to future work.

The next section revisits the problem statement stated in Chapter 1 and shows to what extent the problems stated were achieved.

11.3 Recap of the Problem Statement

This research set out to address the lack of a standard approach to mitigate risk associated with cyber threats and malicious conduct in eSC network environments. The inconsistent process used to design eSC-DFR tools and acquire digital evidence leaves eSC environments vulnerable to many threats that result in tremendous losses for eSC trading partners and a strenuous investigation process for DFIs. The research set out to address three key sub problems affecting eSC networks in relation to DFR. The extent to which the sub-problems were addressed is discussed below:

- One sub-problem this research addresses is the lack of a standardised approach to digital forensic readiness (DFR) in e-supply chains. Organisations within a supply chain do not have DFR systems in place to prepare them for security incidents that might occur as a result of sharing information with other trading partners. This research, therefore, addresses this problem by proposing an eSC-DFR process model that is based on standardised principles applied from ISO/IEC 27043 [107]. The eSC-DFR process model takes the eSC network service provider on

a journey of eSC-DFR system planning, eSC-DFR system implementation and eSC-DFR system assessment as are illustrated in this research.

- Another sub-problem identified in this research is the lack of standard procedure that is reliable and dedicated to identify and mitigate security threats or malicious conduct in an eSC network. In most cases more than one tool is used for securing eSC transaction logs and for intrusion detection making PDE preservation and PDE consolidation a difficult task. The problem was addressed by incorporating threat detection and PDE preservation in the eSC-DFR process model. This is to ensure that PDE is not only collected and stored for download by the eSC-DFR component but through the pre-analysis process defined in the eSC-DFR process model PDE system logs and transaction logs are captured by the eSC-DFR system and consolidated through an automated process for threat detection and malicious conduct flagging. The inclusion of threat detection and PDE preservation in the eSC-DFR process simplifies the digital evidence examination process a DFI has to conduct when conducting an investigation, reducing the time and cost associated with conducting a forensic investigation.
- The last sub-problem addressed in this research is the pre-analysis aspect of e-SC DFR tools. Most DFR tools do not cater for data intelligence to address eSC specific threats such as insider/compliance issues related to price fixing or price gouging threats. The design and development of the eSC-DFR system requires that a lot of attention be placed on planning for these types of incidents as much as the external cyber threats. The research addresses this problem by proposing two key components that satisfy the pre-analysis and robustness requirement of an eSC-DFR system: a pre-analysis module and a personalisation manager module. The personalisation manager module plays a crucial role in making the eSC-DFR system an interactive system. This module is designed to make the DFI's PDE analysis process more effective by ensuring that stored data is presented in a comprehensive manner. In the prototype that was developed, users were able to query collected PDE from the eSC-DFR component and view graphs and charts that represent collected PDE for analysis purposes. The pre-analysis module introduced data intelligence by acquiring insights on collected data allowing for event correlation, PDE categorisation and PDE reporting.

11.4 Future Work

The implementation of the eSC-DFR process model is hoped to assist the fight against eSC malpractices and cybercrime. However, during the research process some new areas falling outside the scope of the current research were discovered and these can be considered for future work. Future work will aim:

- To extend the eSC-DFR system to accommodate more complex eSC platforms such as cloud-based eSC platforms and mobile applications.

- To build big data intelligence into the design of eSC-DFR tools for the analysis of big data collected in bigger and more complex eSC network environments. This will support DFIs and law enforcement agents with more efficient analysis of big data collected as PDE.
- To investigate on how the eSC-DFR component can address more security threats such as Brute Force attacks that target the user authentication component of the eSC-DFR system or Distributed Denial of Service attacks that overload the eSC-DFR system with malicious traffic. The eSC-DFR component should be able to detect and flag more security threats and user malpractices, making it a more useful tool for eSC service providers. The eSC-DFR component must conduct all key DFR processes such PDE generation, incident detection and prevention, allowing for DFIs to use one tool for PDE evidence collection and incident prevention. This will also ensure that there is consistency to the process followed in acquiring PDE and confidence regarding the soundness of collected PDE.
- To model the approach for improving usability in eSC-DFR tools. This is an area that needs substantial further research. Standardisation is critical in ensuring that there is correlation in terms of the usability requirements for DFR tools. This research identified key requirements for improving a DFI's interaction with the eSC-DFR system, but to ensure consistency and further improvements in this area, further research is still required to apply standard methodologies such as Design Thinking to model an approach for defining the usability requirements of eSC-DFR tools. By definition Design Thinking is defined as a mind-set, process, and toolbox. As a mind-set, Design Thinking is characterised by several key principles, a combination of divergent and convergent thinking, a strong orientation to both obvious and hidden needs of customers and users, and prototyping. As a process, Design Thinking is seen as an iterative process which seeks to understand the user, challenge assumptions, and redefine problems in an attempt to identify alternative strategies and solutions that might not be instantly apparent with an initial level of understanding. As a toolbox, Design Thinking refers to the application of numerous methods and techniques from various disciplines such as design, engineering, informatics and psychology [108].
- To extend the eSC-DFR component to accommodate more complex eSC network architectures such as decentralised eSC networks that have more than one central information hub. The eSC model as proposed in Chapter Five currently only follows a centralised approach.

In the next section the author provides some final concluding remarks.

11.5 Conclusion

The eSC-DFR process model and eSC-DFR component demonstrate a means to acquire PDE from an eSC network environment and at the same time ensure that forensic soundness of digital evidence is maintained. The forensic soundness of digital evidence is maintained by the use of cryptographic hash functions, encryption, timestamps and other metadata that can be generated from eSC environments. These security measures were put in place to strengthen the soundness of PDE and ensure adequate protection of collected PDE. The eSC-DFR system was designed using the eSC-DFR process model in order to provide a detailed illustration of how an eSC-DFR system, that was designed for the purpose of addressing cybercrime or malpractice in eSC environments, was created. The eSC-DFR process was created by the author to design eSC-DFR systems. One of the benefits of using the eSC-DFR process model is that it can be extended to allow for future developments as technology advances or crime patterns change. Therefore this research serves as the foundation for the development of next generation eSC-DFR tools.

In this era where user experience is a critical component to the attractiveness of tools, the author aimed to shed focus on the need for advancement of the usability metrics used in the development of digital forensics tools by inserting usability as part of the eSC-DFR process. With advancements in technology and areas such as business intelligence rapidly growing, DFR tools must incorporate data intelligence in their architecture in order to acquire as much insight from data and present it in a manner that is simplified for users. Therefore, the eSC-DFR component attempts to achieve this by providing additional functionality such as event correlation, PDE categorisation and data visualisation. It is needless to say that more usability elements can be incorporated to provide a more advanced user experience for DFIs and law enforcement agents. Therefore, this research does not exhaust all the elements that can be added.

With e-commerce crime on the rise and eSC networks becoming essential platforms for conducting business, the role of DFR is fast becoming greater. Therefore, eSC network service providers and trading partners have to invest in DFR infrastructure and adhere to DFR policies and standards that ensure DFR against security threats. With eSC-DFR systems that are able to detect cyber threats and flag malpractices by trading partners, criminals will be deterred from committing crime on eSC platforms as chances of escaping conviction will be lowered due to the availability of credible digital evidence for prosecution.

Bibliography

1. Paulraj, A. and I.J. Chen, *Environmental uncertainty and strategic supply management: a resource dependence perspective and performance implications*. Journal of Supply Chain Management, 2007. **43**(3): p. 29-42.
2. Smith, G., et al., *A critical balance: collaboration and security in the IT-enabled supply chain*. International journal of production research, 2007. **45**(11): p. 2595-2613.
3. Bellefeuille, C.L., *Quantifying and managing the risk of information security breaches participants in a supply chain*. 2005, Massachusetts Institute of Technology.
4. Jüttner, U., H. Peck, and M. Christopher, *Supply chain risk management: outlining an agenda for future research*. International Journal of Logistics: Research and Applications, 2003. **6**(4): p. 197-210.
5. J.Wright. *New Threats to Supply Chains Call for New Approaches to Risk Management*. . 2013 [cited 2014 17 Septeber 2014]; Available from: <http://www.industryweek.com/supplier-relationships/new-threats-supply-chains-call-new-approaches-risk-management?page=2>.
6. McGarvey, R. *DDoS Hacker Attacks on Banks Escalating*. 2012 [cited 2014 17 September 14]; Available from: <http://www.cutimes.com/2012/09/28/ddos-hacker-attacks-on-banks-escalating>.
7. Manuj, I. and J.T. Mentzer, *Global supply chain risk management strategies*. International Journal of Physical Distribution & Logistics Management, 2008. **38**(3): p. 192-223.
8. Kunnathur, A.S. and S. Vaithainathan. *Information security issues in global supply chain*. in *IMR Conference*. 2008.
9. Burnson, P. *State of Cargo Security: Higher stakes in the risk vs. reward scenario*. 2013 [cited 2014; Available from: http://www.logisticsmgmt.com/article/state_of_cargo_security_higher_stakes_in_the_risk_vs_reward_scenario.
10. Kapuscinski, R., et al., *Inventory decisions in Dell's supply chain*. Interfaces, 2004. **34**(3): p. 191-205.
11. Casey, E., *Digital evidence and computer crime: Forensic science, computers, and the internet*. 2011: Academic press.
12. HAMID, K.T. *Research Methodology in Accounting*. 2012 05 September 14]; Available from: http://www.academia.edu/2003378/Research_Methodology_in_Accounting.
13. Grant, T., E.v. Eijk, and H. Venter. *Assessing the Feasibility of Conducting the Digital Forensic Process in Real Time*. in *International Conference on Cyber Warfare and Security-ICCWS2016*. 2016.
14. Leigland, R. and A.W. Krings, *A formalization of digital forensics*. International Journal of Digital Evidence, 2004. **3**(2): p. 1-32.
15. Fradella, H.F., L. O'Neill, and A. Fogary, *The impact of Daubert on forensic science*. Pepp. L. Rev., 2003. **31**: p. 323.
16. Kostina, A., N. Miloslavskaya, and A. Tolstoy. *Information security incident management process*. in *Proceedings of the 2nd international conference on Security of information and networks*. 2009. ACM.
17. Jäntti, M. *Defining requirements for an incident management system: A case study*. in *Systems, 2009. ICONS'09. Fourth International Conference on*. 2009. IEEE.
18. Reddy, K. and H.S. Venter, *The architecture of a digital forensic readiness management system*. Computers & Security, 2013. **32**: p. 73-89.
19. Richard III, G.G. and V. Roussev, *Digital forensics tools: the next generation*. Digital crime and forensic science in cyberspace, 2006: p. 76-91.
20. Fradella, H.F., L. O'Neill, and A. Fogary, *Impact of Daubert on Forensic Science, The*. Pepp. L. Rev., 2003. **31**: p. 323.

21. Lankshear, C. and M. Knobel, *Digital literacies: Concepts, policies and practices*. Vol. 30. 2008: Peter Lang.
22. Valjarevic, A. and H.S. Venter, *Introduction of concurrent processes into the digital forensic investigation process*. Australian Journal of Forensic Sciences, 2015(ahead-of-print): p. 1-19.
23. Reith, M., C. Carr, and G. Gunsch, *An examination of digital forensic models*. International Journal of Digital Evidence, 2002. **1**(3): p. 1-12.
24. Mabuto, E.K. and H.S. Venter. *State of the Art of Digital Forensic Techniques*. in ISSA. 2011.
25. Rowlingson, R., *A ten step process for forensic readiness*. International Journal of Digital Evidence, 2004. **2**(3): p. 1-28.
26. Endicott-Popovsky, B., D.A. Frincke, and C.A. Taylor, *A theoretical framework for organizational network forensic readiness*. Journal of Computers, 2007. **2**(3): p. 1-11.
27. Valjarevic, A. and H.S. Venter. *Harmonised digital forensic investigation process model*. in *Information Security for South Africa (ISSA), 2012*. 2012. IEEE.
28. Wolf, J.B., et al., *Collecting and reporting monitoring data from remote network probes*. 2001, Google Patents.
29. Thomas, N., *Multi-state and multi-sensor incident detection systems for arterial streets*. Transportation Research Part C: Emerging Technologies, 1998. **6**(5): p. 337-357.
30. Mehdizadeh, Y., *Security event management*. The ISSA Journal, 2005: p. 18-21.
31. Kock, N., *A Basic Definition of E-Collaboration and its Underlying Concepts*. E-Collaboration: Concepts, Methodologies, Tools, and Applications: Concepts, Methodologies, Tools, and Applications, 2009: p. 1.
32. Manthou, V., M. Vlachopoulou, and D. Folinas, *Virtual e-Chain (VeC) model for supply chain collaboration*. International Journal of Production Economics, 2004. **87**(3): p. 241-250.
33. Rostami, M., et al. *Hardware security: Threat models and metrics*. in *Proceedings of the International Conference on Computer-Aided Design*. 2013. IEEE Press.
34. Kadavearamath, R.S., et al., *Application of particle swarm intelligence algorithms in supply chain network architecture optimization*. Expert Systems with Applications, 2012. **39**(11): p. 10160-10176.
35. Viswanadham, N. and R. Gaonkar, *Understanding E-Supply Chains*. Design and Future Trends, the Logistics Institute-Asia, Research paper, No: TLIAP/02/01, 2001: p. 3-7.
36. Pulevska-Ivanovska, L. and N. Kaleshovska, *Implementation of e-Supply Chain Management*.
37. Handfield, R.B. and E.L. Nichols, *Supply chain redesign: Transforming supply chains into integrated value systems*. 2002: FT Press.
38. Gunasekaran, A. and E.W. Ngai, *Virtual supply-chain management*. Production Planning & Control, 2004. **15**(6): p. 584-595.
39. Chong, A.Y., F.T. Chan, and K.B. Ooi. *Collaborative commerce technologies adoption for supply chain collaboration and service innovation: A conceptual model*. in *Proceedings of the 2011 International Conference on Industrial Engineering and Operations Management*. 2011.
40. Kaplan, S. and M. Sawhney, *E-hubs: the new B2B marketplaces*. Harvard business review, 2000. **78**(3): p. 97-106.
41. Stohr, E.A. and J.L. Zhao, *Workflow automation: Overview and research issues*. Information Systems Frontiers, 2001. **3**(3): p. 281-296.
42. Helo, P. and B. Szekely, *Logistics information systems: an analysis of software solutions for supply chain co-ordination*. Industrial Management & Data Systems, 2005. **105**(1): p. 5-18.
43. Cheng, H. *An integration framework of erm, scm, crm*. in *Management and Service Science, 2009. MASS'09. International Conference on*. 2009. IEEE.
44. Schantz, R.E. and D.C. Schmidt, *Middleware for distributed systems: Evolving the common structure for network-centric applications*. Encyclopedia of Software Engineering, 2002. **1**.
45. Lee, H.L. and S. Whang, *Information sharing in a supply chain*. International Journal of Manufacturing Technology and Management, 2000. **1**(1): p. 79-93.

46. Kolluru, R. and P.H. Meredith, *Security and trust management in supply chains*. Information Management & Computer Security, 2001. **9**(5): p. 233-236.
47. Finch, P., *Supply chain risk management*. Supply Chain Management: An International Journal, 2004. **9**(2): p. 183-196.
48. Bejtlich, R., *The Tao of network security monitoring: beyond intrusion detection*. 2004: Pearson Education.
49. Liao, C.-J., Y. Lin, and S.C. Shih, *Vehicle routing with cross-docking in the supply chain*. Expert Systems with Applications, 2010. **37**(10): p. 6868-6873.
50. Lord, W.T., *USAF Cyberspace Command: To Fly and Fight in Cyberspace*. 2008, DTIC Document.
51. Ayers, D., *A second generation computer forensic analysis system*. digital investigation, 2009. **6**: p. S34-S42.
52. Manson, D., et al. *Is the open way a better way? Digital forensics using open source tools*. in *System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference on*. 2007. IEEE.
53. Clegg, R.G., et al., *Challenges in the capture and dissemination of measurements from high-speed networks*. arXiv preprint arXiv:1303.6908, 2013.
54. Pande, B., et al. *The Network Monitoring Tool-PickPacket*. in *Information Technology and Applications, 2005. ICITA 2005. Third International Conference on*. 2005. IEEE.
55. Accorsi, R. *Safe-keeping digital evidence with secure logging protocols: State of the art and challenges*. in *IT Security Incident Management and IT Forensics, 2009. IMF'09. Fifth International Conference on*. 2009. IEEE.
56. Kent, K., *Guide to Computer Security Log Management*. 2007.
57. Cohen, F., *Challenges to digital forensic evidence*. 2008: Fred Cohen and Associates.
58. Guo, Y., J. Slay, and J. Beckett, *Validation and verification of computer forensic software tools—Searching Function*. digital investigation, 2009. **6**: p. S12-S22.
59. Carrier, B., *Open source digital forensics tools: The legal argument*. 2002, stake.
60. Kemande, V.R. and H.S. Venter. *A Cloud Forensic Readiness Model Using a Botnet as a Service*. in *The International Conference on Digital Security and Forensics (DigitalSec2014)*. 2014. The Society of Digital Information and Wireless Communication.
61. Owen, A.M., *Cognitive planning in humans: neuropsychological, neuroanatomical and neuropharmacological perspectives*. Progress in neurobiology, 1997. **53**(4): p. 431-450.
62. Casey, E., *Handbook of digital forensics and investigation*. 2009: Academic Press.
63. Jaakkola, H. and B. Thalheim. *Architecture-Driven Modelling Methodologies*. in *EJC*. 2010.
64. Turner, A., et al., *Method and system for acquisition and centralized storage of event logs from disparate systems*. 2005, Google Patents.
65. Prybutok, V.R., L.A. Kappelman, and B.L. Myers, *A comprehensive model for assessing the quality and productivity of the information systems function: toward a theory for information systems assessment*. Information Resources Management Journal, 1997. **10**(1): p. 6-26.
66. Wiggins, G.P., *Educative assessment: Designing assessments to inform and improve student performance*. Vol. 1. 1998: Jossey-Bass San Francisco, CA.
67. Logothetis, D., et al. *In-situ MapReduce for log processing*. in *2011 USENIX Annual Technical Conference (USENIX ATC'11)*. 2011.
68. Rajamaki, J. and J. Knuuttila. *Law Enforcement Authorities' Legal Digital Evidence Gathering: Legal, Integrity and Chain-of-Custody Requirement*. in *Intelligence and Security Informatics Conference (EISIC), 2013 European*. 2013. IEEE.
69. Roman, G.-C., *A taxonomy of current issues in requirements engineering*. Computer, 1985. **18**(4): p. 14-23.
70. Dykstra, J.A.B.S., *Digital forensics for infrastructure-as-a-service cloud computing*. 2013: University of Maryland at Baltimore County.
71. ISO/IEC-27043, *Information Technology-Security techniques- Assurance for digital evidence investigation process*. 2015, ISO/IEC

72. De Marco, L., F. Ferrucci, and T. Kechadi. *A Cloud Forensic Readiness Model for Service Level Agreements Management*. in *Proceedings of the 14th European Conference on Cyber Warfare and Security 2015: ECCWS 2015*. 2015. Academic Conferences Limited.
73. Simmons, M. and H. Chi. *Designing and implementing cloud-based digital forensics hands-on labs*. in *Proceedings of the 2012 Information Security Curriculum Development Conference*. 2012. ACM.
74. Glinz, M. *On non-functional requirements*. in *Requirements Engineering Conference, 2007. RE'07. 15th IEEE International*. 2007. IEEE.
75. Clements, P.C. and L.M. Northrop, *Software Architecture: An Executive Overview*. 1996, DTIC Document.
76. Dolgui, A. and J.-M. Proth, *Dynamic Pricing Models*. *Supply Chain Engineering: Useful Methods and Techniques*, 2010: p. 41-76.
77. Garrity, E., *A New Chapter in Antitrust Law: The Second Circuit's Decision in United States v. Apple Determines Hub-and-Spoke Conspiracy Per Se Illegal*. *Boston College Law Review*, 2016. **57**(6): p. 84.
78. Gupta, S., *Logging in Java with the JDK 1.4 Logging API and Apache log4j*. 2003: Springer.
79. Gulcu, C., *Short introduction to log4j*. 2002.
80. Jordan, G., *Extending Neo4j*, in *Practical Neo4j*. 2014, Springer. p. 59-68.
81. Rc.Ravens, *Application Logging – Effectively use a logging framework*. 2009.
82. Beddoe, M.A. and S.C. McClure, *System and method of network endpoint security*. 2010, Google Patents.
83. Krawczyk, H., R. Canetti, and M. Bellare, *HMAC: Keyed-hashing for message authentication*. 1997.
84. Baier, H. and F. Breitingner. *Security aspects of piecewise hashing in computer forensics*. in *IT Security Incident Management and IT Forensics (IMF), 2011 Sixth International Conference on*. 2011. IEEE.
85. Steele, N., et al., *Single sign-on for access to a central data repository*. 2006, Google Patents.
86. Kent, K. and M. Souppaya, *Guide to Computer Security Log Management*. *National Institute of Standards and Technology (NIST) Publication 800-92*. 2006.
87. Prewett, J.E. *Analyzing cluster log files using logsurfer*. in *Proceedings of the 4th Annual Conference on Linux Clusters*. 2003. Citeseer.
88. Turner, S. and L. Chen, *Updated Security Considerations for the MD5 Message-Digest and the HMAC-MD5 Algorithms*. 2011.
89. Dori, D., *SysML: Use Case, Block, and State Machine Diagrams*, in *Model-Based Systems Engineering with OPM and SysML*. 2016, Springer. p. 29-35.
90. Ferguson, N., B. Schneier, and T. Kohno, *Hash Functions*. *Cryptography Engineering: Design Principles and Practical Applications*, 2015: p. 77-88.
91. Gupta, S. and B.B. Gupta, *Cross-Site Scripting (XSS) attacks and defense mechanisms: classification and state-of-the-art*. *International Journal of System Assurance Engineering and Management*, 2017. **8**(1): p. 512-530.
92. Smith, R., *Information security-a critical business function*. *Journal of GXP Compliance*, 2009. **13**(4): p. 62.
93. Arghire, I. *Record-Breaking Number of Vulnerabilities Disclosed in 2017: Report*. 19 February 2018 [15 June 2017]; Available from: <https://www.securityweek.com/record-breaking-number-vulnerabilities-disclosed-2017-report>.
94. Bellare, M., R. Canetti, and H. Krawczyk. *Keying hash functions for message authentication*. in *Annual International Cryptology Conference*. 1996. Springer.
95. Snyder, J., *What's the matter with price gouging?* *Business Ethics Quarterly*, 2009. **19**(2): p. 275-293.
96. Bidgoli, H., *Handbook of Information Security, Information Warfare, Social, Legal, and International Issues and Security Foundations*. Vol. 2. 2006: John Wiley & Sons.

97. Pande, B., et al. *The Network Monitoring Tool—PickPacket*. in *Information Technology and Applications, 2005. ICITA 2005. Third International Conference on*. 2005. IEEE.
98. Pilli, E.S., R. Joshi, and R. Niyogi, *A generic framework for network forensics*. International Journal of Computer Applications, 2010. **1**(11).
99. Endicott-Popovsky, B., D.A. Frincke, and C.A. Taylor, *A Theoretical Framework for Organizational Network Forensic Readiness*. JCP, 2007. **2**(3): p. 1-11.
100. Poee, A. and L. Labuschagne. *A conceptual model for digital forensic readiness*. in *Information Security for South Africa (ISSA), 2012*. 2012. IEEE.
101. Dykstra, J. and A.T. Sherman, *Design and implementation of FROST: Digital forensic tools for the OpenStack cloud computing platform*. Digital Investigation, 2013. **10**: p. S87-S95.
102. Stephens, G.D. and M.A. Maloof, *Insider threat detection*. 2014, Google Patents.
103. Angeles, P., *System and method for detecting and reporting online activity using real-time content-based network monitoring*. 2015, Google Patents.
104. Richard, I. and V. Roussev, *Digital Forensic Tools: The Next Generation*, in *Digital crime and forensic science in cyberspace*. 2006, IGI Global. p. 75-90.
105. Garfinkel, S., et al., *Bringing science to digital forensics with standardized forensic corpora*. digital investigation, 2009. **6**: p. S2-S11.
106. Grispos, G., T. Storer, and W.B. Glisson, *A comparison of forensic evidence recovery techniques for a windows mobile smart phone*. Digital Investigation, 2011. **8**(1): p. 23-36.
107. Ab Rahman, N.H., et al., *Forensic-by-design framework for cyber-physical cloud systems*. IEEE Cloud Computing, 2016. **3**(1): p. 50-59.
108. Brenner, W., F. Uebernickel, and T. Abrell, *Design thinking as mindset, process, and toolbox*, in *Design Thinking for Innovation*. 2016, Springer. p. 3-21.
109. Lin, H.-J., M.-M. Wen, and W.T. Lin, *The relationships between information technology, e-commerce, and e-finance in the financial institutions: evidence from the insurance industry*, in *Intelligent Information and Database Systems*. 2012, Springer. p. 194-206.
110. Derek, M. and V. Hein, *A Conceptual Model for Digital Forensic Readiness in E-supply Chains*, in *European Conference on Cyber Warfare (ECCWS) 2015*. 2015.
111. Mouton, F. and H. Venter. *A prototype for achieving digital forensic readiness on wireless sensor networks*. in *AFRICON, 2011*. 2011. IEEE.
112. Derek, M.H., Venter, *An approach for the Design of next generation e-supply chain tools*, in *ISSA*. 2015, IEEE: Johannesburg South Africa.
113. Poirier, C.C. and M.J. Bauer, *E-supply chain: using the Internet to revolutionize your business: how market leaders focus their entire organization on driving value to customers*. 2000: Berrett-Koehler Publishers.
114. Brown, M., *Event logging system and method for logging events in a network system*. 1999, Google Patents.
115. Samoriski, J.H., J.L. Huffman, and D.M. Trauth, *Electronic mail, privacy, and the Electronic Communications Privacy Act of 1986: Technology in search of law*. Journal of Broadcasting & Electronic Media, 1996. **40**(1): p. 60-76.
116. Patel, S.K., V. Rathod, and S. Parikh. *Joomla, Drupal and WordPress—a statistical comparison of open source CMS*. in *Trendz in Information Sciences and Computing (TISC), 2011 3rd International Conference on*. 2011. IEEE.
117. Tatroe, K., P. MacIntyre, and R. Lerdorf, *Programming Php*. 2013: " O'Reilly Media, Inc."
118. Barske, D., A. Stander, and J. Jordaan. *A Digital Forensic Readiness framework for South African SME's*. in *Information Security for South Africa (ISSA), 2010*. 2010. IEEE.
119. Disterer, G., *Iso/iec 27000, 27001 and 27002 for information security management*. 2013.
120. Zabala, L., et al., *Modelling a Network Traffic Probe Over a Multiprocessor Architecture*. Edited by Jesús Hamilton Ortiz, 2012: p. 303.

121. Pathak, S.D., D.M. Dilts, and G. Biswas. *Next generation modeling III-agents: a multi-paradigm simulator for simulating complex adaptive supply chain networks*. in *Proceedings of the 35th conference on Winter simulation: driving innovation*. 2003. Winter Simulation Conference.
122. McKemmish, R., *When is digital evidence forensically sound?* 2008: Springer.
123. KEBANDE, V. and H. VENTER. *A Functional Architecture for Cloud Forensic Readiness Large-scale Potential Digital Evidence Analysis*. in *Proceedings of the 14th European Conference on Cyber Warfare and Security 2015: ECCWS 2015*. 2015. Academic Conferences Limited.
124. Omeleze, S. and H.S. Venter. *Testing the harmonised digital forensic investigation process model-using an Android mobile phone*. in *Information Security for South Africa, 2013*. 2013. IEEE.
125. Grobler, M., *The Need for Digital Evidence Standardisation*. Emerging Digital Forensics Applications for Crime Detection, Prevention, and Security, 2013: p. 234.
126. Ingels, M., A. Valjarevic, and H.S. Venter. *Evaluation and analysis of a software prototype for guidance and implementation of a standardized digital forensic investigation process*. in *Information Security for South Africa (ISSA), 2015*. 2015. IEEE.
127. Ajjola, A., P. Zavarsky, and R. Ruhl. *A review and comparative evaluation of forensics guidelines of NIST SP 800-101 Rev. 1: 2014 and ISO/IEC 27037: 2012*. in *Internet Security (WorldCIS), 2014 World Congress on*. 2014. IEEE.
128. Trenwith, P.M. and H.S. Venter. *Digital forensic readiness in the cloud*. in *Information Security for South Africa, 2013*. 2013. IEEE.
129. 27043, I.I., *Information Technology-Security techniques- Assurance for digital evidence investigation process*. 2015, ISO/IEC
130. Sinz, E.J., B. Knobloch, and S. Mantel, *Web-Application-Server*. Wirtschaftsinformatik, 2000. **42(6)**: p. 550-552.
131. Ryan, D.J. and G. Shpantzer. *Legal aspects of digital forensics*. in *Proceedings: Forensics Workshop*. 2002.
132. Kailash, K., Balaiah, C.P., Pangen, S., Sinha, A., Crank, S.J., Apte, M. and Narasimhan, S., Zscaler Inc, 2018. *Systems and methods for integrating cloud services with information management systems*. U.S. Patent 9,912,638.
133. Pfleeger, C. and Pfleeger, S., 2016. *Security In Computing* (4th Edition, 2006).

Appendix: Publications

1. Masvosvere, D. and H. Venter. *A Conceptual Model for Digital Forensic Readiness in e-Supply Chains*. in *ECCWS2015-Proceedings of the 14th European Conference on Cyber Warfare and Security 2015: ECCWS 2015*. 2015. Academic Conferences Limited.
2. Masvosvere, D. and H.S. Venter. *A model for the design of next generation e-supply chain digital forensic readiness tools*. in *Information Security for South Africa (ISSA), 2015*. 2015. IEEE.
3. Masvosvere, D. and H. Venter, *Using a standard approach to the design of next generation e-Supply Chain Digital Forensic Readiness systems*. SAIEE AFRICA RESEARCH JOURNAL, 2016. **107**(2): p. 104-119.

A Prototype for Achieving Digital Forensic Readiness in e-Supply Chain environments

Derek .J.E Masvosvere, H.S Venter

Department of Computer Science, University of Pretoria, Pretoria, South Africa

dkmasvo911@yahoo.com

hventer@cs.up.ac.za

Abstract: The internet has transformed the way information is shared upstream and downstream in a supply chain environment. This has resulted in the development of electronic supply chain platforms referred to as e-supply chains, which make use of additional building blocks such as information and communications technology to share information between trading partners. These new platforms provide many benefits to both suppliers and consumers that include improved service delivery to consumers and lowered costs to suppliers, just to name a few. Unfortunately, they also come with high information security risks that leave them vulnerable to a number of security threats. As a result Digital forensic investigators and Law enforcement agents are often challenged with the task of gathering forensically sound potential digital evidence from these distributed eSC environments when security incidents occur. This turns out to be an enormous challenge with no digital forensic readiness system in place to instantly collect and provide that potential digital evidence. Therefore this paper examines how one can integrate a digital forensic readiness component into an e-supply chain network environment to capture potential digital evidence and make it readily available to Law enforcement agents and digital forensic investigators (DFIs) when needed. This takes into account all the fundamental DFR principles and legal issues of concern. This paper also provides demonstrations of a working prototype to show that a digital forensic readiness component can be added indeed to an existing eSC network. This is done by performing several demonstrations which resemble real world e-Supply Chain environment scenarios in order to illustrate that the prototype indeed adds a DFR component to the eSC environment.

Keywords: Digital Forensic Investigator (DFI), Law Enforcement Agent (LEA), Digital Forensic Readiness (DFR), Trading Partner (TP), E –Supply Chain (eSC), Potential Digital Evidence (PDE).

1. Introduction

Technology is at the heart of every business today, big or small. This can be noticed through the development of e-commerce platforms such as e-supply chains, (eSCs) that improve the way companies share information and services with their partners or consumers [109]. Unfortunately with such advancements come some security risks such as information espionage, brute force attacks and other malicious attacks, just to name a few. The implementation of effective security measures in the eSC environment is still an area that requires much attention, and even more so, the digital forensic readiness (DFR) aspect of security within this environment [110]. This has led to the problem that is tackled in this paper, that there exists only a list of requirements and processes for achieving (DFR) in eSC environments, which have not yet been tested by means of a prototype using real world eSC scenarios. The aim of this paper is to implement the key processes and requirements that have been identified in previous work and to test if they are sufficient in order to achieve DFR in an eSC environment. The paper also sheds light on the design of a prototype that implements the listed requirements and processes in order to show the applicability of the listed requirements and processes.

The remainder of the paper is structured as follows: Section II gives a comprehensive background on the e-Supply Chain environment and the concept of DFR is defined. Section III and IV discuss the concept behind e-supply chain DFR, presenting the DFR processes and prototype requirements for achieving DFR in eSC environments. Section V demonstrates the prototype which was implemented taking all the requirements and processes presented in Section III into account. Lastly, Section VI concludes the paper with a summary of the work covered in this paper and proposed future work.

2. Background

This section provides the background on the eSC environment and DFR. The authors present a brief background discussion on the e-Supply Chain (eSC) environment because the prototype proposed in this paper is created to serve the eSC environment. DFR is also considered an essential aspect of this paper because it is the component that is being integrated with the eSC environment to collect potential digital evidence (PDE) from the eSC and serve law enforcement agents (LEAs) and digital forensic investigators (DFIs). In the next section the authors discuss the eSC network and the components that make up its environment.

2.1 E-supply Chains

The internet overcomes the gap that has been there for business systems within a supply chain to share information. This success has had a direct impact on the manner in which businesses collaborate and compete; affording businesses the opportunity to reach new markets. By definition, an eSC is defined as an advancement of a supply chain, having additional building blocks such as web technologies that contribute to an improved supply-chain relationship [3]. An eSC network is achieved through the integration of trading partners' information systems, allowing for information sharing between partners which supports close collaboration [39]. These trading partners can be referred to as hosts that are connected to a central point known as an information hub over the internet using middleware components. The incorporation of ICT in the supply-chain environment has also caused a shift from a linear supply-chain structure to a more circular star eSC structure; where trading partners and customers share information and services through the information hub. An information hub is defined as a web-based system, such as a website, which facilitates and encourages buying and selling to induce collaboration among trading partners across a selection of industries [32].

It is important to mention that eSC networks are built on hardware, middleware and software components that work together to facilitate the smooth operation of business processes between trading partners; the key components being software and middleware [110]. Software components such as Supply-chain management (SCM) applications provide both internal and external services to trading partners and an integrated view of core business processes [43]. These software components, in conjunction with the internet and web services, provide an entry point for an enterprise to access information from other trading partners.

Middleware components such as application servers and content management systems are computer software that supports enterprise application integration (EAI). This is systems' software that resides between applications and the operating system, network protocol stacks and hardware [7]. The role of middleware software is to bridge the gap between applications and the lower-level hardware and

software infrastructure in order to coordinate how applications are connected and how they interact [37]. Hardware components create a communication link between each trading partner in the eSC for the transmission and processing of data. Examples of hardware components include PCs, mobile computers, routers, switchboards and servers just to mention a few, all of which are vulnerable to IT-specific threats.

A graphical representation of an e-supply chain network is provided in Figure 1 below that shows the different components that make up an eSC environment at a high level and also illustrates the sharing of information and services between trading partners through the information hub [2, 32, 35].

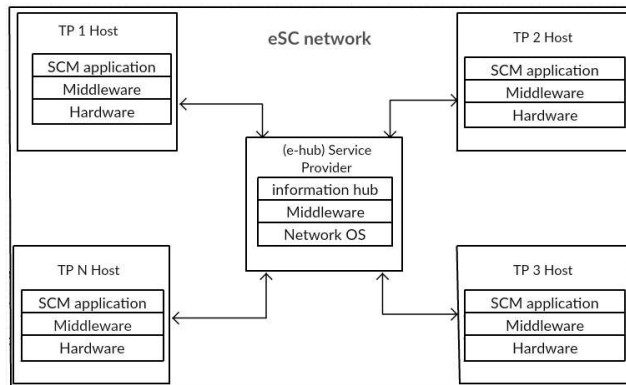


Figure 1 - A graphical representation of an e-Supply Chain network

Figure 1 illustrates the structure of an eSC and how the internal infrastructure of a trading partner (TP) interacts with the information hub that facilitates interactions with other hosts via internet-based protocols [9]. Although there are many security features that can be applied within e-Supply Chains to ensure information security, still lacking is a proactive process to support digital forensics investigators and law enforcement agents in the process of collecting forensically sound PDE from across the eSC environment in case those security features fail. Therefore digital forensic readiness provides techniques and processes that can ensure that the eSC environment is forensically ready and is discussed in the next section.

2.2 Digital Forensic Readiness

In order to come up with a strategic DFR solution for any environment, one has to establish an acceptable definition for it. By definition digital forensic readiness (DFR) is the capability of a system to efficiently collect valid digital evidence that can be used in a court of law [26]. This process has two main goals, to minimise the cost of a digital forensic investigation and maximise an environment's ability to collect credible digital evidence. ISO/IEC 27043 (2015), which is an international standard, presents a DFR process model that outlines the processes that must be followed to fully implement DFR [110]. The processes outlined in this model deal with setting up an organisation in a way that, if a digital forensic investigation needs to be carried out, such an organisation is able to reduce the time period that it takes to conduct a digital forensic investigation, cut down the cost incurred during an investigation and ensure the ability to gather digital evidence without disrupting the environment being monitored [111]. In the DFR process model, the processes are grouped into three process groups

namely, the planning processes group, the implementation processes group and the assessment of implementation processes group as illustrated in figure 2.

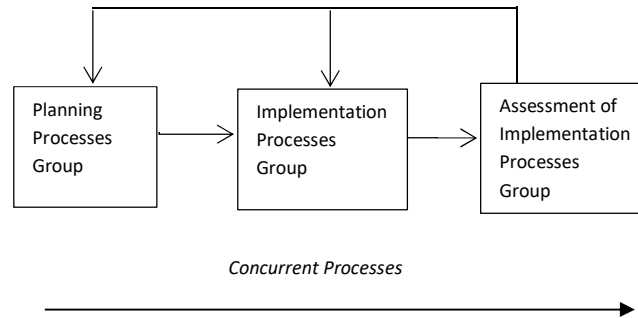


Figure 2 - Readiness processes groups

As illustrated in Figure 2, the DFR process starts at the *planning processes group* which is concerned with the brainstorming of a DFR solution, which must result in the architectural design of a DFR solution. The *implementation processes group*, which is the main focus of this paper, is concerned with processes that must be executed by a DFR system. Such processes must have been defined in the planning processes group and incorporated in the architectural design. Lastly, the *implementation assessment processes group* defines readiness processes that are concerned with the assessment of the success from the implementation process group, which focuses on evaluating the performance of an implemented system. The processes groups are concurrent with other processes that are defined in ISO/IEC 27043 such as DFI; meaning that as DFR takes place, investigative processes can be taking place as well [110]. It is through the implementation of the above standard DFR process that the requirements for a DFR system can be effectively identified and implemented in the eSC environment and in this paper it is this same process that is followed to design and implement an eSC-DFR system prototype.

Unfortunately, tools used in the eSC do not incorporate forensic readiness processes that maximise the eSC’s ability to provide digital forensic evidence, let alone use the ISO/IEC 27043 standard in their design. Therefore in the next section, the DFR processes that are used to identify eSC-DFR system requirements are discussed.

3. DFR in e-Supply Chains

In a previous paper by Masvosvere and Venter, an eSC-DFR process model was presented that was adopted from the DFR process model presented in ISO/IEC 27043 [112]. The model presented in that paper defines the entire process for achieving DFR in the eSC environment, from the planning processes to the assessment processes [112]. Considering the scope of this paper, focus is placed on the implementation processes group, due to the fact that the processes that are identified in this group are solely the processes that an eSC-DFR system must implement. As illustrated in Figure 3, the implementation processes group indicates five key processes that must be implemented in the eSC environment by an eSC-DFR system, namely continuous PDE collection, PDE protection, PDE centralised storage, PDE pre-analysis and controlled access to PDE, respectively. It is through the implementation of DFR processes from the implementation processes group in Figure 3 that the requirements for an eSC-DFR system are identified.

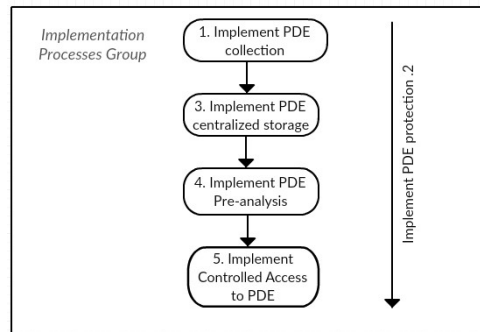


Figure 3 - Implementation processes group of eSC-DFR process model

3.1 PDE collection

Therefore, it is crucial for an eSC-DFR system to be able to collect continuous data that pertains to events taking place across the eSC network. In such an environment there is much sensitive information that is transmitted and shared between trading partners such as electronic payments through transaction processing tools, shipping information, consumer information, intellectual property and other trading partner information [113]. Therefore, it is crucial to be able collect as much data about events executed in this environment, through data collection techniques such as logging that can assist to trace all the events taking place in the eSC [114].

3. PDE protection

Data collection alone does not satisfy key requirements for eSC-DFR to be achieved within the e-supply chain, but a clear data collection and data preservation solution ensures that PDE across the eSC is captured and securely stored for retrieval. With the eSC being a distributed network, it is important to ensure that the integrity of captured PDE is not compromised at any point, from the time it is collected to the time it is accessed by authenticated parties. This calls for measures that prevent the deletion and modification of PDE to be incorporated in an eSC-DFR system, ensuring that PDE integrity is preserved.

3.3 PDE storage

With PDE sources identified, methods for PDE collection defined and PDE protection considered, it is important to decide where and how PDE will be stored. Another key aspect of the eSC-DFR concept is the centralisation of captured potential digital evidence. This means that data captured from across the eSC environment must be stored in a central database repository to reduce redundancies, provide better control over PDE and its maintenance, resulting in increased PDE quality and accuracy. Therefore, an eSC-DFR system must be able to collect data from across the eSC network environment and store it in a centralised database. This PDE storage is where authenticated users such as law enforcement and digital forensic investigators can access this PDE.

3.4 PDE pre-analysis

Having unstructured PDE in storage alone is not enough. With PDE sources already identified, it is necessary to classify the different data captured making it easier to extract meaning out of it. Logothetis mentions the importance of deploying specialised frameworks that assist in the process of

harnessing multiple commodity machines to process enormous data sets from logged data across a distributed environment [67]. Therefore, it is important to keep in mind that much activity takes place within an eSC network, with much important data that can be captured as PDE. That being the case, the implementation of a DFR strategy that can present captured data in a usable and insightful manner is critical.

3.5 Controlled access to PDE

With sensitive data being captured through the eSC-DFR process and securely stored in a centralised database repository, it is necessary to consider the legal factors involved with PDE gathering, use and preservation. This is to ensure that potential evidence is admissible in a court of law. Therefore, there are judicial laws that must be followed that govern the usage of gathered PDE and the collection thereof. The reason behind controlled access to PDE is to restrict access to authenticated users such as law enforcement agents and digital forensic investigators (DFIs), who are governed by judicial law on how they are to handle PDE. Such laws differ from country to country and it is a service provider’s responsibility to identify the laws that apply to that particular jurisdiction and apply them to the eSC-DFR strategy. Depending on the jurisdiction that an eSC system service provider falls under, it is important to consider certain legal requirements guarding the protection of personal information such as the Protection of Personal information (POPI) Act or Electronic Communications Privacy Act (ECPA) [115], which discusses the intercepting of digital evidence and communication records to facilitate prosecution.

From the above mentioned DFR processes, requirements that an eSC-DFR system must satisfy are identified. The next section puts the above mentioned eSC-DFR system processes into perspective, providing a formal list of functional and non-functional requirements that must be met by an eSC-DFR system according to the implementation processes group.

4. Requirements In order to achieve DFR in an eSC environment

This section presents a table of requirements that are needed for a prototype in order to achieve DFR in an eSC network environment. Table 1 below which contains the requirements is an important reference point to the prototype in order to implement DFR in an eSC network.

Table 1 Requirements in order to achieve DFR in an eSC network

<i>Requirement</i>	<i>Description</i>
1.	Real-time capturing of logs from identified sources in the eSC network.
2.	Ensure captured data is protected at all times through secure methods such as encryption.
3.	System must require log in authentication for DFIs and law-enforcement agents that make use of the system.
4.	The system shall accommodate large amounts of captured data in its CDR, due to the amount of PDE data will be collected from across the eSC network.
5.	When successfully logged into the system, the eSC-DFR system shall retrieve and display eSC PDE that the system has in its possession.
6.	The authenticity and integrity of all captured data should be able to be verified in case a digital investigation takes place through integrity validation methods.
7.	The eSC-DFR system shall allow a system administrator to add a new user (law enforcement or digital forensic investigator), edit or delete an existing user profile.
8.	The eSC-DFR system shall allow a system administrator to maintain the system; allowing him/her to install updates and fix bugs.
9.	The system must capture timestamps of events from the eSC network.
10.	The eSC-DFR system must provide a means for the user to view PDE in a meaningful manner through a pre-analysis module, for easier event traceability and data analysis.

11.	The eSC-DFR system shall provide a way for a DFI and LEA to download PDE reports according to the specified restrictions for their convenience.
12.	Captured PDE at critical point in the eSC network shall be transmitted to a secure database by means of a secure communication protocol.
13.	Once PDE is in storage it must be classified accordingly, by means of various tables.

Having provided this list of requirements, the following section will demonstrate a working eSC-DFR system, which takes into account all the above-listed requirements in order to achieve DFR in an eSC network environment.

5. eSC-DFR Prototype Implementation overview

In this section, the authors discuss how the concept of achieving DFR using the eSC-DFR process model and eSC-DFR requirements has been realized and has been described in sections 3 and 4. The authors first describe how the digital evidence is extracted based on the processes including user authentication, disk usage, RAM and IP addresses. Then the authors explain the components that have been implemented to support the eSC-DFR solution towards achieving DFR. The need for the implementation of this prototype as mentioned in the introduction has been motivated by the rise of cybercrime incidents, hence, the prototype serves as a proof of concept as a way of support for achieving DFR based on the ISO/IEC 27043 standard guidelines on forensic readiness.

5.1 Technical Goals

In order to find potential evidence that can link a suspect to a crime in the eSC environment, intruders' footprints are basically examined based on the system content and log files which is relatively manual forensic analysis. Furthermore, with the existence of big data, this proposition might be impossible when it comes to tracking the source of potential attacks because while filtering logs using manual forensics you might remove what you are looking for without noticing. In fact since these processes are implemented separately it might be tedious to reconstruct the sequence of events in order to create a hypothesis that can be used in a court of law for digital investigations.

The above mentioned limitation can be overcome using the prototype that the authors have developed. The prototype focuses on the following technical goals: monitors activities in the eSC environment using a distributed eSC-DFR solution that captures PDE at identified critical points within the eSC environment. Next, the digital information gathered in this process is digitally preserved then transmitted to a central database repository for secure analysis. These processes are able to monitor disk usage in case a malware is utilizing the memory allocating to the eSC environment as well as the RAM processes and user activity with respective timestamps. Lastly, events are reconstructed in the eSC-DFR database repository for easy detection of any potential security incident.

5.2 Potential Digital evidence collecting prototype

PDE collecting probes are represented as an agent based logging probes that act as a sniffing tools with modified functionality and operate in a non-malicious manner. These components are able to monitor activities by recognizing the disk usage periodically, RAM usage and processes executed by eSC users in the eSC environment. This digital data collection process has been developed to assist the eSC to be forensically prepared. It is worth noting that these processes comply with forensic readiness processes that have been highlighted in the ISO/IEC 27043 standard. The PDE collecting probes will

monitor events in the eSC environment and give reports periodically that show respective timestamps. The reporting process is invoked by an authenticated forensic investigator at any time that an incident is reported or a potential threat is detected from the collected log data. All collected activities. The proposed DFR prototype adheres to the requirements which have been set and presented in the previous section. The implementation of the prototype was done using the Joomla supply chain management platform. Joomla is an advanced content management system, which is used to create highly interactive websites, like online communities, portals and e-commerce applications; under which e-Supply Chains fall [116]. This platform provided the eSC application needed to implement the prototype. The eSC application allows suppliers and retailers to sign up, create online stores and interact directly from the buying and selling of goods. It is in this environment that sensitive information is shared between trading partners. All the coding for the eSC application and the eSC-DFR system was done using the php scripting language [117] and the MySQL relational database management system for the storing and accessing of captured PDE.

For the purpose of proving the concept, demonstrations were done to show that it is possible to implement DFR in the eSC environment whilst adhering to the eSC-DFR process model. To demonstrate this, a sample eSC system was created using the Joomla platform. The front end the eSC website allows suppliers to sign up as companies and upload their product catalogue data for the purpose of selling goods to retailers; that can sign up and interact with different suppliers for the purchase of goods. At the back-end, the eSC web application is managed by an authenticated system administrator who has access to the system files of the eSC application. It is in the eSC application code where logging scripts that capture potentially useful information at critical points within the eSC network are added, securely sending the captured log data to the eSC-DFR storage server, where law enforcement agents and digital forensic investigators can access it. Figure 4 is presented below to illustrate how the eSC network and the eSC-DFR component were set up.

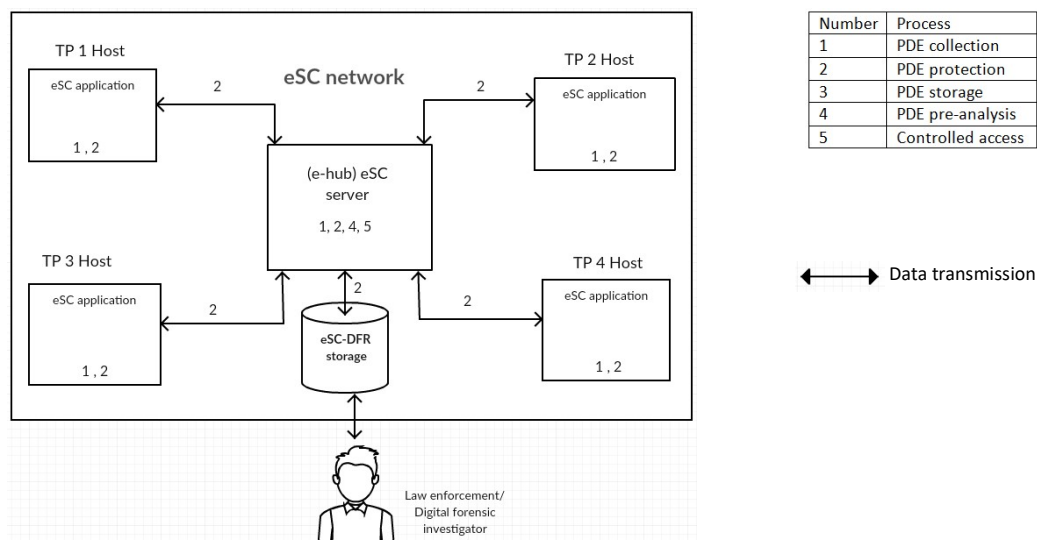


Figure 4 - A graphical representation of the eSC-DFR network layout for demonstration

Figure 4 shows where in the eSC network the eSC-DFR processes are implemented. As different users interact through the eSC server, information about each event is logged through a logging component (php script) from the time they log in and try to access the eSC server. The logging component hashes

the captured data and encrypts it before sending it to the eSC-DFR database server where it is decrypted and stored. In the eSC-DFR database, the captured data is stored either as transaction data, system data and log in data. It is on the eSC-DFR side that a law enforcement agent or digital forensic investigator can access stored PDE from the front-end of the eSC-DFR server. The scale of this demonstration is limited to the critical points that were identified as PDE sources in the presented eSC scenario. This means that PDE sources are not limited to the ones presented in the prototype.

In figure 5 it can be seen how the prototype displays log data which has been generated from the eSC-DFR central database repository. All columns presented have been given names to make it easier to recognise which data is being displayed in the figure.

id	supplier	consumer	prod_id	prod_name	tax	book_fee	event	action	ip_address	user_agent	hash	date_time
5	admin	admin	16	I am Kalam	0	0	sale	purchase	41.146.67.40	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML	like Gecko) Chrome/47.0.2526.106 Safari/537.36	2016-01-17 02:03:06

Figure 5 - Demonstration to show how transaction log data is handled

It important to mention that for the purpose of ensuring readability of the snapshots, captured log data was grouped into three separate tables, transaction logs, system logs and log in logs. Transaction logs presented in figure 5 provide data about each transaction that is carried out by different buyers and sellers of the eSC network. The “ID” column in Figure 5 simply indicates a line number, making it easier to discuss specific lines from the figure. The “Supplier id” column represents the entity that is initiating a transaction with another entity represented in the “Consumer ID” column. The “prod ID” column represents the product that is being purchased by the consumer admin, with this type of event represented in the “event” column as a sale. Also included in this transaction log table is the IP address of each consumer represented in the “IP address” column, which may be very useful in a digital forensic investigation. The “user agent” column represents the browser agent that was used to access the eSC system and for purposes of validating the authenticity of captured log data, each event is allocated a hash value represented in the “hash” column. A “date” column is also included as a timestamp to represent the time that each transaction was executed. This might be very useful data in a digital forensic investigation. Thus if this information were to be used in a digital forensic investigation, there would be no doubt as to the authenticity and integrity of the captured data.

Other captured data that can be used to support and validate each transaction is data from the login table presented in Figure 6. This table represents all successful and failed log in attempts by users at the front-end and back-end of the eSC-network. This information might provide insight as to the potential threats that come from malicious individuals trying to access the eSC, or to prove who was logged into the eSC application when certain incidents took place.

id	type	message	username	ip_address	hash	date
12	frontend	login_failed	MarilynKaw	151.249.196.132	42937930085816ed0edef29cddb458de	2016-01-22 22:45:50
13	frontend	login_failed	uwabarirolokus	91.200.12.106	2a10c88f30c9caa08945785f0c73bfb	2016-01-25 10:06:57
14	frontend	login_failed	upesedevoid	91.200.12.106	0f53f2aacd998e648927b56e8eb124f7	2016-01-25 10:21:20
15	frontend	login_failed	izocisuuzige	91.200.12.141	2b13507994088cd2aa6bc22fafd48dc	2016-01-25 10:35:18
16	frontend	login_failed	ekefolujeba	91.200.12.143	f85887163b2c8981c0fc22a04511f808	2016-01-25 10:37:16
17	frontend	login_success	admin	196.249.3.96	082325fb47fe87e246032318f9134e3	2016-01-25 10:48:54
18	backend	login_failed	admin	189.219.167.107	b6f89d5aaff4065a14d053b36eca086d	2016-01-25 18:36:08
19	backend	login_failed	admin	189.219.167.107	b6f89d5aaff4065a14d053b36eca086d	2016-01-25 20:00:01
20	frontend	login_failed	dkmasvo911@yahoo.com	137.215.6.53	437c413de93298ca9d58a42bfb789719	2016-01-27 04:09:01
21	frontend	login_failed	dkmasvosvere	137.215.6.53	fd74ddcbf5aa86795c8602f7c0cac2fa	2016-01-27 04:09:31
22	frontend	login_failed	dkmasvo911@yahoo.com	137.215.6.53	437c413de93298ca9d58a42bfb789719	2016-01-27 04:09:47

Figure 6 - demonstrations of captured logs for successful and failed logins

As illustrated in Figure 6, this table is made up of a number of columns; an “ID” column just like the one represented in the transaction log table, a login “type” column that represents whether a user was trying to access the eSC from the front-end or back-end. Also represented in Figure 6 is the “message” column that indicates whether a login was successful or not. A hash value column, an IP address column, user column and a date column are also included in this log table to provide credible insight as to who, where and when an event was executed. The purpose of collecting this data is to show how versatile and useful the eSC-DFR system can be, providing data can be useful in different scenarios.

In Figure 7 below, focus was placed on illustrating that with the eSC-DFR component, eSC system logs can also be captured. Such logs could be useful in trouble shooting the eSC server/s or identifying different attacks on the eSC server. System logs contain events that are logged by the eSC server such as server Uptime, disk usage and RAM usage.

id	uptime	load	disk	ram	processes	datetime
3	294	2	58%	20%	340818	2015-12-17 23:43:25
4	294	2	58%	18%	347092	2015-12-17 23:45:56
5	294	1	58%	18%	370728 371080 371104	2015-12-17 23:55:29
6	294	3	58%	19%	370728 391736 391746	2015-12-18 00:03:38
7	294	2	58%	19%	370728 424735 424817	2015-12-18 00:16:52
8	294	1	58%	19%	370728 424982 425283 435785 435918	2015-12-18 00:21:18
9	294	2	58%	19%	458916 458930	2015-12-18 00:30:20
10	294	2	58%	19%	464552 496917 496925	2015-12-18 00:45:38

Figure 7 - Server logs for eSC system

Each of the columns presented in the figure represent some potentially useful evidence. The uptime column represents the time that the eSC server was functional in minutes. The load column expresses the number of processes that are in the queue to access the processor and the smaller the number of processes the more in performance you can will get from the server. The server disk column represents the percentage of disk space used in the eSC server. The ram column shows the amount of ram used in the eSC server. The processes column indicates the number of processes running in the eSC server at the time represented in the date time column.

This shows that adding DFR to an existing eSC environment can provide numerous benefits, which include providing readily available forensically sound PDE to law enforcement and forensic investigators for analysis purposes and providing system administrators with useful information for trouble shooting faults and preventing potential incidents from taking place. The next section concludes the paper by discussing the strength of the implementation and how it has provided digital forensic readiness to an existing network.

6. Conclusion

The eSC network is a fairly new concept which has acquired much attention in the e-commerce sphere, with numerous incidents taking place over the course of its establishment. This has resulted in some attention being placed on the security issues that affect e-Supply Chain-users but unfortunately not much attention has been placed on the challenges that law enforcement and digital forensic investigators face when trying to acquire and analyse potential evidence from the eSC environment. This paper proposed a DFR prototype implementation which can be integrated with the eSC system to provide a layer of DFR which can only be accessed by authenticated users such as law enforcement

agents and digital forensic investigators in the case of an incident. This paper focused mainly on being able to add a DFR component to any existing eSC system. The problem that this paper addressed was that currently there exists only a list of requirements and a process model in order to achieve digital forensic readiness in an eSC environment, and these requirements have not yet been tested by means of a prototype and with real world eSC network scenarios. This paper has shown that following the eSC-DFR process model in order to design a prototype is beneficial in identifying the list of requirements that are essential for the development process. This paper showed that the prototype was able to successfully incorporate a DFR component that is based on DFR principles presented in the ISO/IEC 27043 standard. As this is only a prototype implementation it has only been demonstrated by the use of a small eSC network. In future research this can be expanded to a larger network with more users and not limited to the supplier-consumer relationship presented. Researchers may also identify other potential digital evidence that may be collected from this environment that might be useful in identifying other forms of attacks such as flooding attacks and malicious software.

A Model for the Design of Next Generation e-supply Chain Digital Forensic Readiness Tools

D.J.E. Masvosvere
Department of Computer Science
University of Pretoria
Pretoria, South Africa
dkmasvo911@yahoo.com

H.S. Venter
Department of Computer Science
University of Pretoria
Pretoria, South Africa

Abstract— The internet has had a major impact on how information is shared within supply chains, and in commerce in general. This has resulted in the establishment of information systems such as e-supply chains amongst others which integrate the internet and other information and communications technology (ICT) with traditional business processes for the swift transmission of information between trading partners. Many organisations have reaped the benefits of adopting the eSC model, but have also faced the challenges with which it comes. One such major challenge is information security. Digital forensic readiness is a relatively new exciting field which can prepare and prevent incidents from occurring within an eSC environment if implemented strategically. With the current state of cybercrime, tool developers are challenged with the task of developing cutting edge digital forensic readiness tools that can keep up with the current technological advancements, such as (eSCs), in the business world. Therefore, the problem addressed in this paper is that there are no DFR tools that are designed to support eSCs specifically. There are some general-purpose monitoring tools that have forensic readiness functionality, but currently there are no tools specifically designed to serve the eSC environment. Therefore, this paper discusses the limitations of current digital forensic readiness tools for the eSC environment and an architectural design for next-generation eSC DFR systems is proposed, along with the system requirements that such systems must satisfy. It is the view of the authors that the conclusions drawn from this paper can spearhead the development of cutting-edge next-generation digital forensic readiness tools, and bring attention to some of the shortcomings of current tools.

Keywords— *Network forensics, e-Supply Chains (eSCs), Digital forensic readiness (DFR), Cyber-Crime, Monitoring tools, Digital forensic data analysis tools, Forensics domains, Digital forensic Investigation (DFI).*

I. INTRODUCTION

In the recent past, organisations have become heavily dependent on their computers and networks. Needless to say, the comprehensive use of computers and networks for the exchange of information and services has had a major impact on the escalation of crime through their use [1]. As a result, monitoring such networks has become a mission-critical task.

E-supply chains (eSCs) are becoming an increasingly adopted model for organisations to conduct business. This model encourages organisations to share information and resources in order to achieve improved customer service, speed up business operations and reduce costs. Despite the many benefits that eSCs provide, they also create new avenues for fraudsters. Ayers indicates that current digital forensic tools are not keeping up with the increased complexity and data volumes of modern investigations and insists that the existing architecture of first-generation computer forensics tools is rapidly becoming out-dated [51]. Developments in today's networks, which support both internal and external business processes, call for cutting edge DFR tools that can assist in the collection, storage and retrieval of potential evidence in a forensically-sound manner.

The problem pursued in this paper is that there are no DFR tools that are designed to support eSCs specifically. With all the technological advancements that have occurred over the years in eSCs, there has been very little focus on the implementation of digital forensic readiness within this environment. The EnCase forensic tool and the Forensic Tool Kit (FTK) application, which are the two industry-standard digital forensic analysis tools for digital forensic investigations do not incorporate digital forensic readiness properties in their specifications. Therefore, in this paper, the authors provide an architectural design and blueprint for next-generation eSC-DFR systems along with the system requirements.

The remainder of this paper is structured as follows: section II provides background on eSCs and digital forensic readiness. Section III sheds light on the limitations of current digital forensic readiness tools. Section IV defines the next generation DFR tools; setting out a series of requirements that such tools must meet. In section V the design of the eSC-DFR is introduced, showing the dynamic aspect of the system through the use of a use-case diagram. In

section VI the proposed architectural design of the next generation eSC-DFR system is presented and discussed to illustrate how the requirements set out in the previous section may be implemented and to demonstrate the benefits of doing so. Finally, the last section concludes with a discussion about the proposed system and future work.

II. BACKGROUND

In this section, a background on eSCs and Digital forensic readiness is conducted. eSCs form an integral part of this paper because they provide an environment that supports the transmission of information and services between trading partners and customers. DFR provides ways to capture critical data in the eSC environment—data that is crucial for DFIs and information risk assessments in the eSC.

A. E-supply chains

A conventional supply chain comprises of a system of firms, activities, people, information and resources that harmoniously facilitate in the moving of services or products from supplier to customer [3]. An eSC is an advancement of a conventional supply chain, meaning it has additional building blocks, such as web technologies, that contribute to an improved and integrated supply-chain relationship. This relationship is facilitated by web technology solutions that effect information exchange between trading partners and consumers over a distributed network environment. In the next section a more detailed description of the components that make up the eSC environment is given.

B. E-supply chain Architecture

E-supply chains are built on hardware, middleware and software components that work together to facilitate the smooth operation of business processes between trading partners. Software components such as Supply-chain management (SCM) systems and Customer-relationship management (CRM) systems provide both internal and external services to trading partners and an integrated view of core business processes. These software components, in conjunction with the internet and web services, provide an entry point for an enterprise to access information from other trading partners. Middleware components, such as application servers and content management systems, are computer software that support enterprise application integration (EAI). Middleware can be defined as programs that provide messaging services, which include enterprise-application integration, data integration, links between database systems and web servers in the eSC. Hardware components create a communication link between each trading partner in the eSC for the

transmission and processing of data. Examples of hardware components include PCs, mobile computers, routers, switchboards and servers just to mention a few, all of which are vulnerable to IT-specific threats. From figure 1 below, the different components that make up an eSC environment are illustrated at a high level. The figure illustrates the structure of an eSC and how the internal infrastructure of a trading partner (TP) interacts with the information hub that supports interactions with other trading partners' internal systems via internet-based protocols [12].

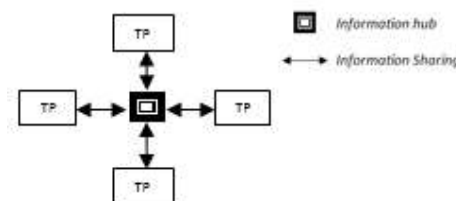


Figure 1. eSC Structure

The eSC network environment is full of potential evidence data that can be used when an incident occurs; that is if data is collected in a forensically sound manner. Therefore, it is the authors' view that a digital forensic readiness system can provide such critical data.

C. Digital Forensic Readiness

Due to the above-mentioned security issues and problems, there is a need for ways to gather digital evidence in a forensically-sound manner. DFR provides different techniques which can be used to address such issues [118]. Rodney McKemmish [4] defines “forensically sound” as a term used in the digital forensics community to qualify and justify the use of a particular forensic method or technology. Very often digital forensics is called upon in response to an information security incident or computer-related crime. Although this happens in most cases, there are many situations where DFR may benefit an organisation before an incident occurs, providing the ability to gather and preserve potential digital evidence [25]. By definition DFR is the capability of a system to efficiently collect valid digital evidence that can be used in a court of law [26]. It is important for organisations to understand the crucial role that DFR plays as a proactive process in digital forensics and the impact a DFR system could have in a DFI. In an article Rowlingson [6] mentions a number of goals that are essential to DFR. These goals include gathering admissible evidence legally without interfering with business processes, gathering evidence targeting the potential crimes and disputes that may adversely impact an organisation and to minimise interruption to the business from any investigation.

Therefore, the role of a DFR tool in an eSC environment would be to gather such evidence from the eSC network environment and store it in a forensically-sound manner. A digital forensic investigator may therefore require access to potential evidence that will be able to support its position, in the event that an incident occurs. Unfortunately, the current variety of DFR tools do not support forensic readiness processes that maximise the eSC's ability to provide digital forensic evidence. Therefore, in the next section, the authors review some limitations that such tools exhibit.

III. LIMITATIONS OF CURRENT DFR TOOLS

A considerable amount of research has been conducted on the adoption of DFR processes in different network environments. Unfortunately there has not been adequate attention given towards the development of eSC-DFR tools. It is in this paper that the authors identified a number of limitations concerning DFR tools in the eSC category. Limitations include:

- Limited throughput for data capturing devices.
- Poor Usability.
- Compromised Privacy and limited filtering of packets.
- No technical support.
- Centralising the storage of data captured in a distributed network for data retrieval.
- Software errors.

Each of these limitations are elaborated upon in the sections to follow.

A. Limited throughput for data capturing devices

Due to a tremendous increase in network traffic over the years, current DFR tools are struggling to keep pace with network traffic speeds. These tools cannot capture 100 percent of network traffic data at higher speeds [36]. For an investigation to be successful, especially in the DFR arena, as much data as possible needs to be captured.

B. Poor Usability

Most DFR tools do not provide a user-friendly interface for end-users to quickly scan through a visual timeline of an event, deeply interrogate the activity, and understand the context associated with each object [53]. Large amounts of unfiltered data are collected from different network access points and represented in a form that is too sophisticated for an ordinary person to understand; creating a need to improve the GUI, data search and filtering capabilities in DFR tools. Considering that an eSC is a distributed system, there is a need for DFR tools

and store it in a central place, where collected data can be retrieved by digital forensic investigators or law enforcement, which would be readily available in the case of an enquiry.

C. Compromised Privacy and limited filtering of packets

Packet sniffing and filtering has its drawbacks [54]. Firstly, only limited filtering on packets received is carried out, resulting in massive post processing. Secondly, no filtering is done based on the packet payload content (which is the critical data that is carried within a packet or other transmission unit). Lastly, as the entire data is dumped into a central database, the privacy of innocent individuals who may be communicating during the time of monitoring may be violated. Therefore, access to captured eSC data is not restricted to relevant potential evidence and relevant parties.

D. No technical support

Commercial Digital forensics tools that offer technical support are generally costly, making it difficult for small to medium-sized enterprises (SMEs) to purchase them [51]. On the other hand, open-source network monitoring tools are very often difficult to use as they do not provide technical support and the ability to gain insight into their inner workings [51]. The validity and trustworthiness of digital evidence is an essential part of digital forensics. This calls the validity of DFR tool to verify that tools meet the requirements of a digital forensics tool.

E. Software errors

Software errors continue to pose a challenge for tool developers. Analysts and other digital forensic tool users are often faced with the problem of unexplained crashes that lead to disruption and often to loss of data [51]. These seem to be caused by a combination of factors, such as design errors in tools and a lack of high-integrity software development practices within the tool. Therefore, software crashes continue to be a significant concern for analysts and improvements to the robustness of forensic tools are crucial for this reason alone.

The authors, in the next section identify some crucial requirements that next-generation eSC DFR tools must incorporate for optimum results.

IV. REQUIREMENTS FOR NEXT GENERATION DFR TOOLS IN E-SUPPLY CHAINS

The ability of an organisation to gather potential digital evidence from its network environment before an incident occurs is the focus of digital forensic readiness. Therefore the functional requirements of a DFR eSC tool, basically define the services that such a tool must provide; which are

that can capture potential digital evidence at different parts of the supply chain

- Monitor and capture all network traffic from the eSC.
- Ensure confidentiality of captured data.
- Exceptional Usability and Availability.
- Provide accessibility to the system.
- Ensure access control to system.

Therefore, the proposed requirements are elaborated in the sub-sections that follow.

A. Monitor and Capture Data from E-supply Chain

The main function of a DFR tool is to provide forensically-sound records of events before an incident occurs [119]. Therefore an eSC-DFR tool should give the user a holistic view of the events transpiring in the eSC. The use of probes and other data capturing techniques ensure that all the events that take place within an eSC are recorded in a forensically-sound manner and incidents are identified. An eSC DFR tool must therefore, have a monitoring component, which is able to monitor and capture (logging) all the events that take place across the IT infrastructure of an eSC communication network. Once the system captures data, it should ensure the safe-keeping of this data in order to ensure that the integrity is not compromised.

B. Confidentiality, integrity and privacy of collected Data

One of the biggest concerns of many organisations is the privacy of their users' sensitive data. An eSC-DFR system must ensure that users' privacy is not compromised. The authors stress that logging facilities and log information which refers to captured data from different parts of the eSC, must be protected against tampering and unauthorised access. An eSC is a highly-targeted environment; therefore it is safe to assume that an eSC-DFR system will also be a target for hackers and criminals [2]. For that reason it is highly critical that such a system be able to provide as much security as possible by employing security measures such as confidentiality, integrity, access control and privacy.

C. Improved Usability and Availability

The usability of an eSC-DFR tool is of utmost importance. Most monitoring tools are not easy to navigate, making it difficult for users to identify incidents when they occur or to just monitor traffic [51]. It is very crucial that an eSC-DFR system be user-friendly, displaying data to trading partners and law enforcement in a manner that is easy to deduce and trace events recorded. The graphic user interface (GUI) of such a tool must provide users with enough flexibility to either view, download, search categorically and filter captured data. A digital

forensic investigator must be able to sign up, login and navigate through captured data effortlessly. Hence, the availability aspect of such a tool is crucial in its design. A DFR tool must be able to perform all its designated functions that include providing forensically sound captured data to users upon demand. It is therefore crucial that usability and availability tests be conducted to ensure that the system meets its intended functions.

D. Having an accessible system

Since an eSC is a web-based system, an eSC-DFR system must also be web-based, providing services to law enforcement agents and digital forensic investigators from this platform. eSC network developers must integrate the eSC-DFR system with the eSC system, giving the tool access to the systems that are in the e-supply chain network (trading partner systems) for data capturing purposes. The system must direct all captured data to a central eSC-DFR system repository server where it is securely stored. Any system errors or alarms raised by a trading partner's internal system must also be captured by the eSC-DFR system and stored in the repository server, where records can be retrieved once a user logs in to the eSC-DFR system.

E. Access control of Data retrieval

Considering that eSC DFR tools have to be web-based, strict authentication and access control measures must be implemented. Different entities must be allocated different roles within a DFR tool. Therefore, it is proposed that an eSC-DFR system limit the access rights of different users as a privacy and confidentiality measure, in order to ensure that users only access relevant potential digital evidence from the eSC-DFR system. This requires that the system be able to store meta-data about different users, which include the system administrator, trading partners, digital forensic investigators and law enforcement agents.

In the next section the authors present a high level use-case diagram to show an outside view of the proposed eSC-DFR system and show how such a system interacts with its users and other software.

V. ESC-DFR SYSTEM USE-CASE DIAGRAM

A use case diagram is widely used to capture the dynamic aspect of a system, displaying steps a user needs to follow to reach the goal as well as how the various components interact with a user. In this section the authors make use of a use-case diagram to show the high-level view of an eSC-DFR system and the interactions between actors of the system with the system itself. The authors identified three main actors i.e. eSC trading partner systems, system administrator and law enforcement agents/Forensic

Investigators, depicted in the use-case diagram in Figure 2. Each actor is discussed in the sections that follow and an illustration of the roles that each user executes are also depicted in the figure.

For the system to work effectively, there are conditions that must be met. Namely, each user must have an account with the system as a system administrator, law enforcement agent or digital forensic investigator. Furthermore, the eSC network must incorporate the eSC-DFR system.

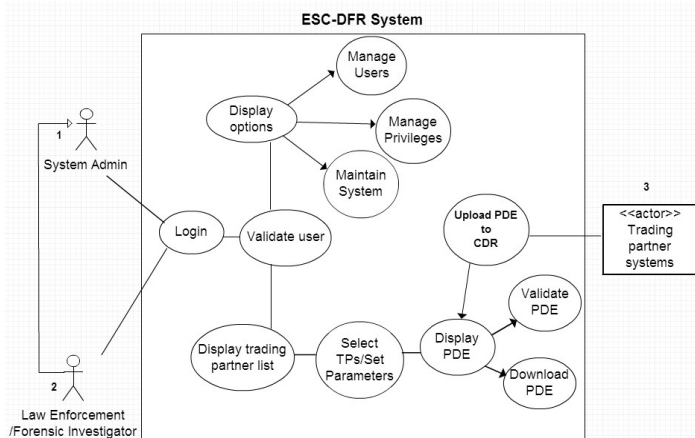


Figure 2. ESC-DFR System use-case diagram

In the sections that follow, each actor is defined, illustrating the role that each user of the system executes.

A. System Administrator

The system administrator (actor number 1 in Figure 2) represents the person responsible for maintaining the eSC-DFR system. This user must have full access rights to the administrative aspects of the system, ensuring that the system is configured correctly. It is the role of a system administrator to manage user accounts, manage user privileges and maintain the system. It is the role of the system administrator to implement any updates to the system that add new features and resolve bugs. It is important to note, that all other users in the system are dependent on the system administrator as illustrated in the use-case diagram in Figure 2.

B. Law-enforcement agent/Digital forensic investigator

Actor number 2 represents a law enforcement agent or digital forensic investigator, responsible for downloading, analysing and validating collected potential digital evidence (PDE) from the eSC-DFR system. This actor is granted access to the system to view, download and validate the potential digital evidence captured from the eSC. The regulation of access to captured data is critical within an eSC business environment as organisations might want to maintain a level of privacy concerning their business operations. Therefore, strict authentication measures ensure that a user is validated and granted access to relevant data only.

C. Trading Partners Systems

An eSC is a distributed business network environment; made up of multiple web-based trading partner systems that interact with each other through an information hub, sharing information and services [11]. Therefore, a DFR tool that operates in this environment has to be integrated with the information hub and trading partners' web-based systems (actor 3) to capture data coming in and out of these systems and upload it to the eSC-DFR system. Captured data might be in the form of information requests and responses sent between trading partners through the information hub, eSC system modifications on trading partner systems or other system data such as alarm system data. The eSC-DFR system may use an internet browser for users to access the system, considering that it is a web-based application. Furthermore multiple web servers may be involved in performing different functions such as secure storage, run applications and so forth.

In the next section the design of a next generation eSC DFR system is presented, showing the system's components and how the system operates.

VI. THE DESIGN OF PROPOSED E-SUPPLY CHAIN DFR SYSTEM

In this section the authors propose a model for the design of an eSC-DFR system. The model is illustrated with two significant views; a high-level structure in figure 5 and a more detailed logical view of the design in figure 6. In figure 4 an activity diagram illustrates the services provided by the system to its users (digital forensic investigators).

Section A provides a hypothetical scenario to illustrate how the eSC-DFR system could benefit both trading partners and digital forensic investigators.

A. Hypothetical Scenario

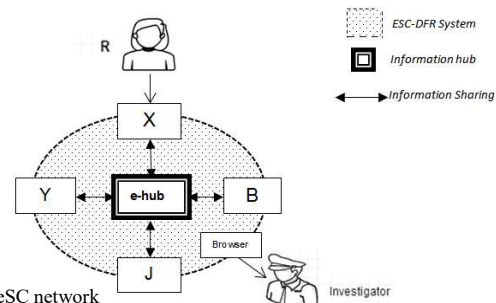


Figure 3. A small eSC network

In the provided scenario, e-hub is a service provider (information hub) that connects suppliers, retailers and consumers in real time. It allows retailers to sell supplier products that they do not keep in stock on their webstores; connecting Product Catalog Data, using Selling and Fulfilment Tools and lastly making use of Transaction Processing. X is a web store that is connected to the e-hub network, selling Y and J's products. Both Y and J are suppliers

running massive warehouses. A malicious employee R who works for X decides to install a malicious code on X's web server that infiltrates the e-hub network, attacking other trading partners Y, J and B's web-based systems. After J, Y and B realise that their systems are being attacked they decide to call upon a digital forensic investigator to assist them with the investigation. With the e-hub network integrated with the eSC-DFR system (that extracts PDE and log information on each trading partner's web system) that is connected to the e-hub network. The forensic investigator should be able to retrieve readily-available digital evidence pertaining to the incident. The evidence captured could lead directly to trading partner X's webstore, showing the installation of a malicious code and the changes made by the malicious code on trading partner X's web-based system, the time of events and maybe who was logged in at the time of incident. Through the user-friendly eSC-DFR system, the investigator must be able to narrow down from all the captured data to the specific events related to the incident.

Figure 4 illustrates the behaviour of the system when a forensic investigator logs into the eSC-DFR system.

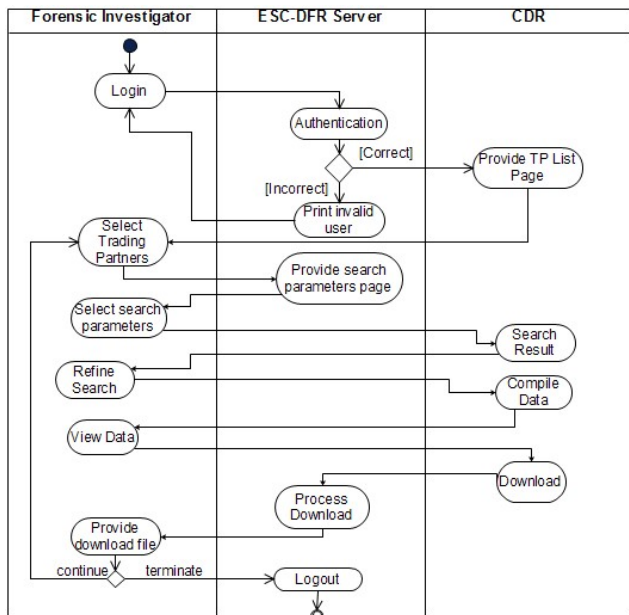


Figure 4. Digital forensic investigator and law enforcement interacting with ESC-DFR system.

The eSC-DFR system will request that the user enters username and password. If invalid, the system will output an error message and return to the login page. If username and password are valid, the system will retrieve the list of trading partners (TPs) from the central data repository (CDR) and present it to the user through a GUI. From the list, the digital forensic investigator can select the trading partners being investigated. The system will return a search parameter page for the user to search for specific data that is relevant to the selected TPs. The user can then

narrow down the search to specific data types, specific time period and send request to database. The CDR compiles the selected trading partners' logged data and allowing the user to view the PDE, download the data, logout or return to the trading partner list page. Thereafter the forensic investigator with the PDE can commence the investigative processes.

In the next section, the authors present and discuss the high level eSC-DFR system architecture.

B. High Level ESC-DFR System architecture

There are two essential elements to the discussion of the eSC-DFR system, namely the eSC network and the eSC-DFR component. These elements combined provide a platform for DFR to be achieved across the eSC. The eSC network is an important aspect in the architectural design of the eSC-DFR system because it is the environment where PDE is extracted, with infrastructural components that are critical to the implementation of DFR in the eSC. Some of the components are discussed in the following sections.

The eSC-DFR component provides DFR services to DFI's and law enforcement. Such services include eSC PDE capturing, PDE storage, eSC incident prevention and eSC PDE retrieval. The DFR components that are intergrated with the eSC network infrastructure enable data capturing in the eSC network. Hence, communication between the eSC-DFR component and the eSC network through web protocols and IT infrastructure is a key part of the eSC DFR system architecture as illustrated in Figure 5. This allows PDE to be captured in the eSC network and securely stored in the CDR.

Figure 5 illustrates the integration between the eSC network and the eSC-DFR component, showing the transporting of captured data to the CDR (1) and the requesting/retrieval of PDE at the eSC-DFR component (2).

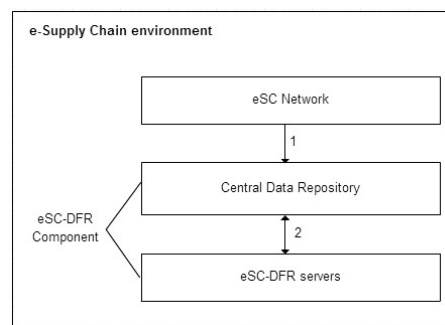


Figure 5. High level architecture of eSC-DFR system

In the next section a more detailed model of the eSC-DFR system is presented and some critical components of the system are discussed.

VII. MODEL OF THE ESC-DFR SYSTEM ARCHITECTURE

Figure 6 illustrates a more detailed model of the eSC-DFR system and its key elements. It must be noted that with further research, more components might be added to the proposed model.

As mentioned previously there are two key components in the proposed architecture. One is the eSC network and second is the eSC-DFR component. Both components utilise secure protocols such as the SSL protocol to transmit data over the web; from the eSC network to the eSC-DFR component. There are elements that are critical to both the eSC-DFR component and the eSC network. Such elements include the eSC host servers and deployed logging probes; which are located in the eSC network shown in Figure 6.

In the eSC-DFR component there are 4 key components, the CDR, database management system, eSC-DFR server and a content management system which interacts with the database management system located in the CDR shown in Figure 6 below.

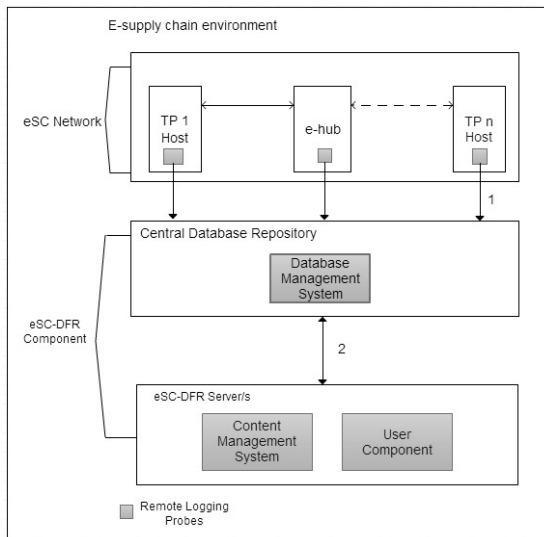


Figure 6. Architecture of the ESC-DFR System

As mentioned in section B, PDE is captured in the eSC network by the deployed probes and sent through to the CDR; where it is processed by the database management system (DBS) and stored. In an event that an incident occurs, digital forensic investigators and law enforcement agents can retrieve captured PDE from their work stations through the user component that connects them to the content management system. In the sub-sections that follow, the authors take a deeper look into the role that each element illustrated in Figure 6 performs in the eSC-DFR system.

A. Remote logging probes

Remote probes generally offer a number of different functions for different scenarios. In this scenario, the main function of such probes is to

extract critical information about the eSC network from the host machines, compute digital signatures and initiate the transmission of captured data from the eSC network across the web to the eSC-DFR component. PDE might include firewall data, system log files, erased files, temp files and sniffed packets depending on the configuration of the probes. Considering that the eSC network and the eSC-DFR system are integrated, the logging module has to be incorporated in the code of the eSC System application. Once the eSC system is installed onto a trading partners host machine, the probe must start capturing system activity and initiate communication with the eSC-DFR component.

For such communication to take place, it is important to establish a connection between the eSC network and the CDR server. This might require that all the necessary ports in the eSC-DFR component firewall be opened. To ensure the security of transmitted data, the remote probes must send the captured data through secure channels such as the SSL protocol. This is to ensure that data sent back and forth from different parts of the eSC-DFR system is not visible to intruders.

The logging probes collectively must be able to record the entire procedure leading to an incident. They must be able to identify, where requests and responses in the eSC network are coming from, the time when requests are sent and received, protocols being used and type of data being transmitted between entities in the eSC. For improved performance a number of remote probes can be deployed. This number is based on the number of eSC hosts being monitored and the eSC network traffic throughput.

B. E-supply chain DFR server

The eSC-DFR server resides in the middleware tier discussed in section II. This component provides middleware services that include system security, system maintenance, content management, system configuration and user management. The server ensures that all the DFR processes are systematically executed in the eSC, also providing authenticated user access to the system's functions. It is important to mention that the eSC-DFR system might incorporate a server cluster. This means that the functions that an eSC-DFR server executes might be spread over a cluster of servers, running simultaneously and working together to provide increased scalability. The main functions of a content management system (CMS) are to send requests to the CDR and retrieve data from the CDR, organise them in the eSC-DFR server and provide controlled access to data[11]. The eSC-DFR server can be presented using the layered approach, with a presentation layer, services layer, business logic layer and data layer that all perform different roles.

C. Database server (4)

The central database repository (CDR) is where captured data from different parts of the eSC network is stored, including eSC-DFR system files, metadata

and user profiles. The CDR can be defined as a central place where data is stored and maintained or a place where data is obtained for distribution across a network. When information is transmitted across the eSC or actions are executed on trading partner systems, deployed eSC-DFR system infrastructure will capture as much data pertaining to the those events and send that data to the CDR. Where the captured data is processed by a database management system (DBMS). A DBMS can be defined as a program or collection of programs that manage incoming data, organise the data, and provide ways for that data to be retrieved by users or other programs. It is the view of the authors that an eSC-DFR system might require large volumes of storage, depending on the size of the e-supply chain and considering the amount of data collected from different parts of the ESC network. Hence, issues of big data might arise but are not discussed in this paper. The database management module handles the structuring of PDE and retrieval of stored data. With the help of the (CMS) in the eSC-DFR server, users can access the eSC-DFR system content with relative ease.

VIII. ARCHITECTURAL ASPECTS

Considering that the key functions of a eSC-DFR system are to capture PDE and to securely store the captured PDE for retrieval, it is safe to assume that the most critical elements of such a system are data capturing, secure storage and system reliability. Therefore, in this section the authors elaborate further on the design of the remote probes as indicated in Figure 6 and key factors to consider for system reliability and secure storage.

A. Design of Remote Probes

A remote probe in general can be seen as an object used for data extraction. Data includes system log files, Intrusion detection system log files, system configure files, temp files and network packets [11]. Within an eSC environment, this capturing module would be installed within each trading partner’s host machine where it can capture data concerning the eSC system and send captured data to the CDR, where all captured data is stored [120]. In Figure 7 the authors display the adapted architecture of the remote probes.

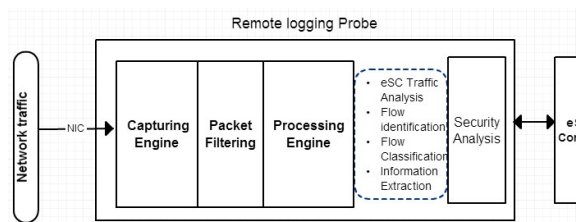


Figure. 7. Remote probes

In an eSC environment information is shared and transmitted at fast rate; many transactions are conducted by different trading partners. It is for that reason that a probe capturing PDE in this

environment needs to be able to handle the rate at which data is transmitted.

As stated in section III, current limitations in DFR tools include limited throughput. Hence, as a measure to ensure that the eSC-DFR system is able to cope with the high-speed traffic, the authors propose the use of a kernel-level multi-processor traffic probe that captures and analyses network traffic in high speed networks [120]. This solution is based on execution threads that are designed to take advantage of multiprocessor architectures. The network interface cards (NIC) within the eSC host machines direct the network traffic to the probes where it is captured by the capturing engine. In the eSC-DFR system the probes as illustrated in Figure 7 are responsible for capturing eSC network traffic, filtering through captured traffic (based on their protocol or IP address), capturing system data related to the eSC network on host machines and processing/analysing captured traffic before it is sent to the CDR for storage.

B. Evidence storage and system reliability

It is no secret that digital forensic workloads are characterised by large volumes of data and the need for high data throughput is in fact real. Therefore, it is in the authors’ opinion that improvements to data capturing rates and data transfer rates will definitely improve the performance of an eSC-DFR system. A suggested solution would be to use clustered or parallel file systems where a user reading data from the eSC-DFR system is actually receiving data from multiple physical servers at once. This would mean that a user’s read rate can exceed the maximum network I/O bandwidth of a single server. This supports the idea that was stated by Ayers that the performance of clustered file systems is greatly increased when servers and clients use teamed network adapters to increase bandwidth [51]. The eSC-DFR system will incorporate a module for managing the capturing of potential evidence and maintaining a detailed record of all tasks executed users by the system.

Making sure that the system is reliable is also of utmost importance, especially considering that this system must provide services to businesses of all sizes. Hence, the proposed system has to be carefully designed and implemented to ensure that the system is highly robust. The use of modern software engineering techniques has to be considered to ensure that the system is as secure, robust and versatile; able to handle any unforeseen software errors while minimising the risk of data loss.

While there is room for more thorough optimisation of the eSC-DFR system, it is in the authors’ opinion that the core elements that are included in the proposed design validate this approach.

IX. DISCUSSIONS

The primary objective of this research was to design a high level architecture of an eSC-DFR system that can provide useful data to digital forensic investigators and law enforcement agents to aid in digital forensic investigations and other processes that might require such data. From the limitations identified in current DRF tools. The proposed architecture is designed to cater to the security needs of an eSC environment specifically, ensuring that the eSC is forensically ready. It comprises of a secure eSC-DFR system web server, remote logging probes that are strategically deployed in the eSC network, a central repository database for storage of PDE and a user component that provides users with controlled access to the system. The authors identified the need for next generation DFR tools that:

- Can handle high throughput that passes through eSC information networks.
- Are robust and can meet DFR toll requirements.
- Can present captured PDE in a comprehensible manner.
- Are able to maintain a level of privacy for trading partners.
- Provide users with uncompromised forensically sound data.
- Collect data on supplier's supplier relationships.

Considering that an eSC environment may comprise of many entities, the proposed architecture was designed to handle large amounts of potential evidence data. It is in the authors' opinion that software developers must ensure that the capturing and storage components of such a system can capture data at high speeds and accommodate large volumes of data. Also considering that an eSC is a distributed network environment connecting retailers to suppliers and suppliers to more suppliers. The architecture of the eSC-DFR system is designed to cater to those kinds of relationships. The deployment of remote probes as data capturing modules onto host systems in the eSC network ensure that potential digital evidence is captured across the eSC.

As mentioned earlier in the paper, a major requirement of a DFR tool is that it must ensure that the integrity of captured PDE is not compromised, thereby meeting digital forensics standards. Therefore, the use of secure communication protocols and remote probes is incorporated in the proposed architecture. The use of encryption and digital signatures amongst other methods are suggested to maintain the integrity of captured data. Also a specialised probe design was incorporated to ensure that the capturing of high speed traffic is accomplished [120].

It has been strongly emphasised by the authors that ease of use that a DFR system provides and its

ability to present captured data in a comprehensible manner is of utmost importance (Usability). Therefore in this paper the authors emphasise the importance of paying close attention to the design of a usable graphic user interface; making the eSC-DFR system easy to navigate and the time taken to retrieve captured evidence and trace events is greatly reduced. Hence, developers must ensure that much attention is placed on the usability aspect of the system.

The strict authentication of users through the security component in the eSC-DFR system architecture ensures that a level of privacy for sensitive data is maintained. It is of great importance to stress the point that the eSC-DFR system is a system designed to serve law enforcement and digital forensic investigators to solve cases and monitor the eSC. Therefore, rights of access must be strictly monitored to ensure that only validated users are granted access to the system. Therefore, measures taken to control access and at the same time maintain a level of flexibility for users must be considered in the development of such a system.

It is evident, that the use of IT comes with numerous challenges that can cost organisations large sums of money. Although the effectiveness of a DFR system can only be fully comprehended through an assessment of the system, the authors believe that the proposed eSC-DFR system can help organisations avoid incidents in the eSC. Also such a system can assist law enforcement agents and digital forensic investigators by providing readily available digital evidence that can be used in the investigative processes.

X. CONCLUSION

Existing general purpose DFR tools are rapidly becoming inadequate for modern commercial network systems (eSCs). The out-dated architecture of such tools limits their ability to scale and adopt the current and future eSC forensic readiness processes. In the recent past, researchers have cited the need for more capable DFR tools that can support digital forensic investigations in the event an incident occurs. As much as these are steps in the right direction, implementing security policies and processes alone does not ensure that the eSC environment is fully forensically ready.

This paper proposes a model which can be used as a blueprint for the design of next generation eSC-DFR systems that can fully cater to the DFR requirements of such an environment. The eSC-DFR system is a useful tool for collecting data and monitoring the eSC environment. The design of the proposed system is built around improving the user experience and providing adequate forensically sound data to trading partners and law enforcement agents about all trading partner interactions. The use of kernel-level multiprocessor network probes ensures that no data is lost during the packet



capturing process. The authors also acknowledge that an eSC handles large amounts of data that are transmitted upstream and downstream the supply chain, hence the eSC-DFR system provides clustered storage to increase the performance, capacity and reliability of the system.

In this paper the authors were able to discuss the limitations to current DFR tools and requirements for next-generation eSC-DFR tools where proposed. An early high-level design for a practical next-generation eSC-DFR system was presented. The design and implementation of such a system is ongoing. The system incorporates strategies for optimising and managing potential evidence data collected from different parts of an eSC. For future work an implementation of the eSC-DFR system is necessary, also providing a look into the performance of the proposed system. This would assist in verifying whether the proposed system accomplishes what it is intended to accomplish.

Using a standard approach to the design of next generation e-Supply Chain Digital Forensic Readiness systems

D.J.E. Masvosvere and H.S. Venter***

** ICSA Research Group, Department of Computer Science, Corner of University Road and Lynnwood*

Road, University of Pretoria, Pretoria 0002, South Africa E-mail: dkmasvo911@yahoo.com

*** Department of Computer Science, Corner of University Road and Lynnwood Road, University of*

Pretoria, Pretoria 0002, South Africa E-mail: hventer@cs.up.ac.za

Abstract: The internet has had a major impact on how information is shared within supply chains, and in commerce in general. This has resulted in the establishment of information systems such as e-supply chains (eSCs) amongst others which integrate the internet and other information and communications technology (ICT) with traditional business processes for the swift transmission of information between trading partners. Many organisations have reaped the benefits that come from adopting the eSC model, but have also faced the challenges with which it comes. One such major challenge is information security. With the current state of cybercrime, system developers are challenged with the task of developing cutting edge digital forensic readiness (DFR) systems that can keep up with current technological advancements, such as (eSCs). Hence, the problem addressed in this paper is the lack of a well-formulated DFR approach that can assist system developers in the development of e-supply chain digital forensic readiness systems. The main objective of such a system being that it must be able to provide law enforcement/digital forensic investigators (DFI) with forensically sound and readily available potential digital evidence that can expedite and support digital forensics incident response processes. This approach, if implemented can also prepare trading partners for security incidents that might take place, if not prevent them from occurring. Therefore, the work presented in this paper is aimed at providing a procedural approach that is based on digital forensics principles. This paper discusses the limitations of current system monitoring tools in relation to the kind of specialised DFR systems that are needed in the eSC environment and proposes an eSC-DFR process model and architectural design model that can lead to the development of next-generation eSC DFR systems. It is the view of the authors that the conclusions drawn from this paper can spearhead the development of cutting-edge next-generation digital forensic readiness systems, and bring attention to some of the shortcomings of current system monitoring tools.

Keywords: Network forensics, e-Supply Chains (eSCs), Digital forensic readiness (DFR), Cyber-Crime, e-supply chain digital forensic (eSC-DFR) system, digital forensic data analysis tools, Forensics domains, Digital Forensic Investigation (DFI).

1. INTRODUCTION

In this digital age, collaborative commerce is the key to running a successful business. Organisations have come to realise that it is important to establish and manage relationships that are mutually beneficial, as this is central to their survival and growth [43]. In the recent past, organisations have become heavily dependent on their computers and networks. Needless to say, the comprehensive use of computers and networks for the exchange of information and services has had a major impact on the escalation of crime through their use [1]. As a result, monitoring such networks has become a mission-critical task.

E-Supply Chains (eSCs) are becoming an increasingly adopted model for organisations to

conduct business. This model encourages organisations to share information and resources in order to achieve improved customer service, speed up business operations and reduce costs. Despite the many benefits that eSCs provide, they also create new avenues for fraudsters.

Ayers [51] indicates that current digital forensics (DF) systems, of which digital forensic readiness (DFR) systems fall under are not keeping up with the increased complexity and data volumes of modern investigations and insists that the existing architecture of first-generation computer forensics tools is rapidly becoming out-dated. DF systems generally implement reactive processes that assist in the collection, preservation, analysis and reporting of digital evidence. DFR systems on the other hand are systems that implement proactive processes such as potential digital evidence (PDE) gathering and data

pre-analysis. Reddy and Venter [10] indicate that many digital forensic investigations take a long time to conclude due to a lack of sufficient forensically sound digital evidence. Therefore, developments in today's networks, which support both internal and external business processes, call for cutting edge DFR systems that can assist in the collection, storage and retrieval of PDE in a forensically sound manner.

The problem pursued in this paper is that there are no DFR systems that are designed specifically for the eSC environment and no standardised approach followed in the design and development of such tools. With all the technological advancements that have occurred over the years in eSCs, there has been very little focus on the is the implementation of digital forensic readiness (DFR) within this environment. By definition digital forensics is the use of specialised techniques for the extraction, preservation, identification, authentication, examination, analysis and documentation of digital information from any environment [60].

This procedure is often called upon in response to the occurrence of an incident and not as a proactive process that is incorporated in the design of eSC systems. Industry's standard tools such as the EnCase forensic tool and the Forensic Tool Kit (FTK) application do not incorporate DFR properties in their specifications, which is a proactive forensic process. Therefore, in this paper, the authors present an eSC-DFR process model that can be viewed as the methodology for achieving DFR in an eSC environment and a system-design model that is to be used as a blueprint for the design of next-generation eSC-DFR systems.

The remainder of this paper is structured as follows: section 2 provides background on the eSC environment and digital forensic readiness. Section 3 discusses the limitations of current digital forensic readiness systems, leading to the proposed methodology for achieving DFR in the eSC environment in section 4. Through the proposed method, eSC-DFR system requirements are identified and discussed in section 5. In section 6 and 7 the design model for eSC-DFR systems is presented, showing the dynamic aspect of the system through the use of a use-case diagram and activity diagram. Section 8 and 9 present the generic architectural model of a next generation eSC-DFR system and its components to illustrate how the requirements set out in previous sections may be implemented. In section 10 some architectural aspects regarding the proposed model are elaborated on for greater clarity; followed by the last two sections that conclude the paper and provide a critical evaluation of the proposed eSC-DFR model.

2. BACKGROUND

This section provides the background on the e-Supply Chain environment and digital forensic

readiness. The authors present a brief background discussion on e-supply Chains (eSCs) because the approach proposed in this paper is created to serve the eSC environment. The approach employs a digital forensics process, digital forensic readiness (DFR), justifying its importance in this section.

2.1 e-Supply Chains

Pathak, Dilts and Biswas mention that a conventional supply chain is a system that comprises of firms, activities, people, information and resources that work together to facilitate the movement of goods and services from supplier to customer [121]. The internet overcomes the gap that has been there for business systems to be connected, providing a means to connect businesses all over the world. An eSC is an advancement of a conventional supply chain, meaning it has additional building blocks, such as web technologies, that contribute to an improved and integrated supply-chain relationship [36]. This relationship is facilitated by web technology solutions that effect information exchange between trading partners and consumers over a distributed network environment. In the next section a more detailed description of the components that make up the eSC environment is given.

2.2 E-supply chain Architecture

E-supply chains are built on hardware, middleware and software components that work together to facilitate the smooth operation of business processes between trading partners; the key components being software and middleware.

Software components : such as Supply-chain management (SCM) systems provide both internal and external services to trading partners and an integrated view of core business processes [43]. These software components, in conjunction with the internet and web services, provide an entry point for an enterprise to access information from other trading partners. All SCM software applications are ready-made applications usually designed to deal with specific tasks e.g. online inventory management processes between suppliers and clients. These ready-made software applications are mass-customised for specific markets and industries. From a data management point of view, e-supply chain software can be organised into two categories: transactional and analytical software applications [42].

Transactional software applications are applications that provide services that are concerned with acquiring, processing and communicating raw data about a trading partner's supply chain network interactions with other partners. Analytical software applications are applications used for evaluating and disseminating decisions based on e-supply chain decision databases. Examples would be forecast

systems or production scheduling systems just to mention a few.

Middleware components: such as application servers and content management systems, are computer software that support enterprise application integration (EAI). Middleware can be defined as programs that provide messaging services, which include enterprise-application integration, data integration, links between database systems and web servers in the eSC network. This is systems software that resides between applications and the operating system, network protocol stacks and hardware [44].

The role of middleware software is to bridge the gap between applications and the lower-level hardware and software infrastructure in order to coordinate how applications are connected and how they interact. Such middleware components if implemented properly can help to shield software developers from low-level and error-prone platform details and assist in providing developer oriented services such as logging and security services that are necessary in a network environment [37].

Hardware components: create a communication link between each trading partner in the eSC for the transmission and processing of data. Examples of hardware components include PCs, mobile computers, routers, switchboards and servers just to mention a few, all of which are vulnerable to IT-specific threats. From Figure 1, the different components that make up an eSC environment are illustrated at a high level. The figure illustrates the structure of an eSC and how the internal infrastructure of a trading partner (TP) interacts with the information hub that facilitates interactions with other trading partners' internal systems via internet-based protocols [29].

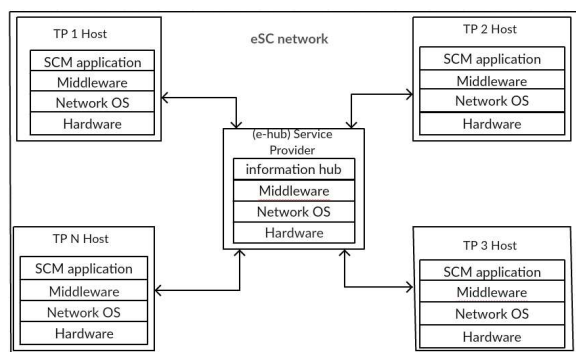


Figure 1: eSC Structure

The eSC network environment is full of potential evidence data that can be used when an incident occurs; that is if data is collected in a forensically sound manner. Therefore, it is the authors' view that a digital forensic readiness system can provide such critical data.

2.3 Digital Forensic Readiness

Due to the above-mentioned security issues and problems, there is a need for ways to gather digital evidence in a forensically sound manner. DFR provides different techniques which can be used to address such issues [18]. Rodney McKemish [122] defines "forensically sound" as a term used in the digital forensics community to qualify and justify the use of a particular forensic method or technology. Very often digital forensics is called upon in response to an information-security incident or computer-related crime. Although this happens in most cases, there are many situations where DFR may benefit an organisation before an incident occurs, providing the ability to gather and preserve potential digital evidence [19]. By definition DFR is the capability of a system to efficiently collect valid digital evidence that can be used in a court of law [21]. It is important for organisations to understand the crucial role that DFR plays as a proactive process in digital forensics and the impact a DFR system could have in a DFI. In an article Rowlingson [25] mentions a number of goals that are essential to DFR. These goals include gathering admissible evidence legally without interfering with business processes, gathering evidence targeting the potential crimes and disputes that may adversely impact on an organisation and to minimise interruption to the business from any investigation.

Therefore, the role of a DFR tool in an eSC environment would be to gather such evidence from the eSC network environment and store it in a forensically sound manner; allowing a forensic investigator to access the collected potential evidence in the event that an incident occurs.

2.4 ISO/IEC 27043

ISO/IEC 27043 (2015), which is an International Standard, outlines a three-step procedure to fully implement DFR [28]. The processes in this standard deal with setting up an organisation in a way that, if a digital investigation needs to be carried out, such an organisation has the ability to maximise its potential to use digital evidence; whilst minimising the time and costs incurred in an investigation. This standard has been tested and applied to numerous real world scenarios by different researchers, validating its importance scientifically [123-127].

According to ISO/IEC 27043 [25], the three groups of processes that make up DFR are: planning, implementation and implementation assessment as shown in figure 2 below.

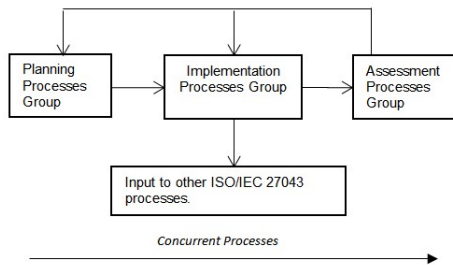


Figure 2: Readiness processes groups

Figure 2 illustrates the order in which DFR processes take place, starting with the planning group which is concerned with the planning activities, followed by the implementation group which includes readiness processes concerned with implementing the planned processes from the planning group. Lastly, the assessment group defines readiness processes which are concerned with the assessment of the success from the implementation process group.

The processes groups are concurrent with other processes that are defined in ISO/IEC 27043 such as DFI; meaning that as DFR takes place, investigative processes can be taking place as well [25]. The data collected from the implementation of DFR in the e-supply chain can therefore be used as input to other processes in the ISO/IEC 27043 standard such as a DFI.

Unfortunately, tools used in the eSC do not incorporate forensic readiness processes that maximise an eSC’s ability to provide digital forensic evidence, let alone use the ISO/IEC 27043 standard in their design.

In the next section the authors discuss the limitations of current monitoring tools, in relation to what is required of eSC-DFR systems.

3. LIMITATIONS OF CURRENT TOOLS

A considerable amount of research has been conducted on the adoption of DFR processes in different network environments [18, 60, 118, 128]. Unfortunately there has not been adequate attention given towards the development of eSC-DFR systems that are designed specifically for eSC environments. The eSC environment is a distributed web-based network hence it requires a specialised DFR strategy that is able to capture PDE from different parts of the network and ensure its integrity.

It is in this paper that the authors identified a number of DFR limitations that come from not having a standard approach to design and implementation of most monitoring systems that are in most cases used

as DFR tools and sources of PDE. Limitations include:

- Limited throughput for data capturing devices.
- Poor usability.
- Compromised privacy and limited filtering of packets.
- No technical support.
- No centralised storage for collected data from a distributed network environment.
- Software errors.

Each of these limitations are elaborated upon in the sections to follow.

3.1 Limited throughput for data capturing devices

Due to a tremendous increase in network traffic over the years, current monitoring systems are struggling to keep pace with network traffic speeds. These tools cannot capture 100 per cent of network traffic data at higher speeds [36]. For an investigation to be successful, especially in the DFR arena, as much data as possible needs to be captured. Considering that the practicality of capturing all network traffic data is questionable, other strategic methods that come from implementing the ISO/IEC 27043 standard must be considered and are going to be discussed in this paper.

3.2 Poor Usability

Most monitoring systems do not provide a user-friendly interface for end users to quickly scan through a visual timeline of an event, deeply interrogate the activity, and understand the context associated with each object [53]. Large amounts of unfiltered data are collected from different network access points and represented in a form that is too sophisticated for an ordinary person to understand; creating a need to improve the GUI, data search and filtering capabilities in such systems so that DFR processes and functionality can be executed efficiently.

Considering that an eSC is a distributed system, there is a need for DFR systems that can capture potential digital evidence at different parts of the supply chain and store it in a central place, where collected data can be retrieved by digital forensic investigators or law enforcement, which would be readily available in the case of an enquiry. Through perfect planning that comes from adopting planning processes from ISO/IEC 27043, eSC-DFR systems can be designed to provide users with the best user experience and system functionality.

3.3 *Compromised privacy and limited filtering of packets*

Packet sniffing and filtering has its drawbacks [54]. Firstly, only limited filtering on packets received is carried out, resulting in massive post processing. Secondly, no filtering is done based on the packet payload content (which is the critical data that is carried within a packet or other transmission unit). Lastly, as the entire data is dumped into a central database, the privacy of innocent individuals who may be communicating during the time of monitoring may be violated. Therefore, access to captured eSC data is not restricted to relevant potential evidence and relevant parties. ISO/IEC 27043 provides processes that can be incorporated in DFR systems for PDE preservation purposes.

3.4 *No technical support*

Commercial Digital forensics tools that offer technical support are generally costly, making it difficult for small to medium-sized enterprises (SMEs) to purchase them [51]. On the other hand, open-source network monitoring tools are very often difficult to use as they do not provide technical support and the ability to gain insight into their inner workings [51]. The validity and trustworthiness of digital evidence is an essential part of digital forensics. This calls the validity of a DFR tool to verify that tools meet the requirements of a digital forensics tool.

3.5 *Software errors*

Software errors continue to pose a challenge for tool developers. Analysts and other digital forensic tool users are often faced with the problem of unexplained crashes that lead to disruption and often to loss of data [51]. These seem to be caused by a combination of factors, such as design errors in tools and a lack of high-integrity software development practices within the tool. Therefore, software crashes continue to be a significant concern for analysts and improvements to the robustness of forensic tools are crucial for this reason alone. This issue can be solved through the assessment process group in ISO/IEC 27043 which provides assessment tests to ensure that all the errors are eradicated [129].

Therefore, in the next section, the authors introduce the adoption of the ISO/IEC 27043 DFR model as a method for achieving forensic readiness in the eSC environment and countering the identified limitations. This standard provides a standard approach to the design, implementation and assessment of DFR systems.

4. DIGITAL FORENSIC READINESS IN E-SUPPLY CHAINS

In this section a discussion on how DFR can be implemented in the eSC environment by adopting the ISO/IEC 27043 DFR process model and identifying DFR processes is carried out.

4.1 *Proposed methodology for achieving DFR in eSC environment*

The ISO/IEC 27043 standard DFR model illustrated in Figure 2 provides us with three DFR process groups which are adopted in this paper and are critical to the achievement of DFR in the eSC environment. This grouping of processes helps to identify processes that are critical for achieving DFR in the eSC environment and clearly define the order in which events should take place. It is also important to mention that the proposed methodology goes beyond a mere adoption of the ISO/IEC 27043 standard DFR process and some identified processes for each DFR process group are not necessarily mentioned in the ISO/IEC 27043 standard.

It is the author's opinion that the three ISO/IEC 27043 DFR process groups adopted in the eSC-DFR process model eSC must result in the development of cutting edge eSC-DFR systems that have 5 main objectives:

- To capture PDE from the eSC network environment
- To protect PDE from unauthorized parties and ensure its integrity is not compromised through the PDE protection process
- To provider store secure centralized for PDE
- To present collected PDE in a useful manner
- To ensure that authenticated users can only access information that is relevant to a specific case and incident through the controlled access to PDE process.

Figure 3, shows an adoption of the standard DFR model by the authors to develop the eSC-DFR process model, which constitutes processes that are essential to the eSC-DFR process.

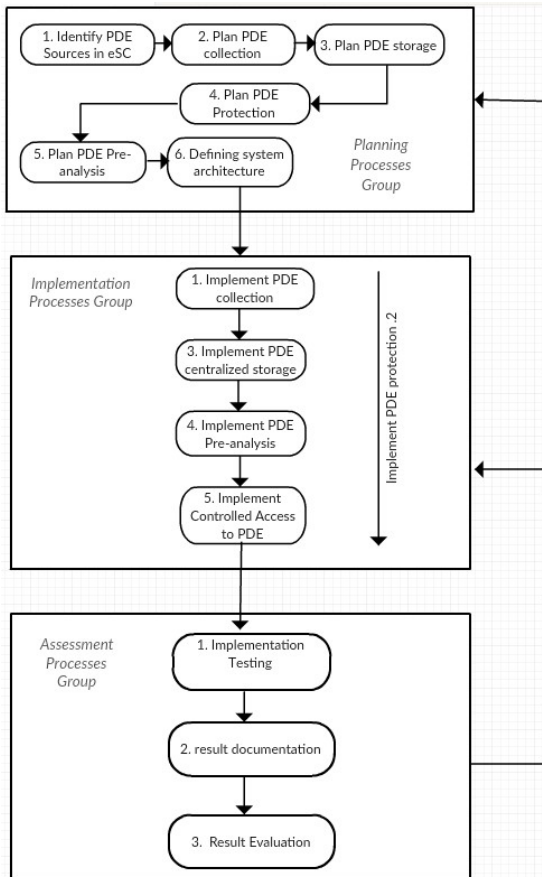


Figure 3: eSC-DFR process model

The processes shown in the figure must be utilised in three ways as indicated by the grouping of processes. The first process group is the planning process group, which involves the planning and designing of DFR solutions for this environment through the identification of policies that need to be implemented. The second process group is the implementation process group, which focuses on the implementation of solutions/systems to achieve forensic readiness in the eSC environment. The last group is the assessment of implementation process group that basically focuses on the assessment/evaluation of the effectiveness of the implemented solutions/systems in order to determine and make the necessary adjustments to achieve an effective DFR strategy. Each process group is discussed in greater detail in the following sections, starting with the planning processes group.

4.2 Planning processes group for DFR in e-supply chains

Planning may be defined as a process of brainstorming and organising the activities required to achieve a desired outcome [28]. In the eSC-DFR process model, the planning processes group

presents critical processes required to achieve DFR in the eSC environment. The following sub-sections elaborate on each eSC-DFR planning process identified.

Identify sources of PDE in e-supply chain: Identifying sources of potential evidence is a crucial step in the DFR process. Rowlingson [9] mentions that the purpose of this process is to identify what evidence is available across an entire system or application for collection. For the purpose of this research the role of process no. 1 is to identify the different types of potential digital evidence that may be available across an e-supply chain network and where it may be located. Examples of data sources in an eSC system include servers, firewalls, application software, general logs [11]. Examples of digital evidence include e-mails, transaction logs, audio files, system logs and video files.

Planning data collection: After identifying PDE sources, it is up to the eSC service provider to decide which of the identified sources of PDE is worth pursuing to collect PDE and which methods will be considered to gather this evidence. There are a number of issues that should be considered during this process, such as how to acquire digital evidence without interfering with business processes, the legality behind collecting this data, size of collected data, and the costs involved [9]. All of these have an impact on the effectiveness of the DFR process in an eSC.

Plan PDE storage: Upon collecting PDE, the next issue of concern is the storage of the collected PDE. It is the authors' opinion that there are a number of issues that arise when considering the storage of gathered digital evidence, such as the security factor and the size of storage factor. An eSC handles sensitive company data such as client records, business transactions and other sensitive trading partner information, hence it is important to ensure that gathered information in it is kept secure from unauthorised parties. In addition, it is important to consider efficient ways of storing large amounts of PDE that is captured across the eSC such as compression.

Plan PDE Protection: The main focus of this process is ensuring that the integrity of captured PDE is not compromised. The eSC is a web-based system hence there are many ways for intruders to try and access and either steal or corrupt PDE. Therefore, it important to consider methods of protecting captured data from potential threats through the deployment of certain security measures such as encryption and password protection. It is necessary to ensure that once data is collected or stored in a data repository, its integrity is maintained

and it can be used in a useful way. This also involves considering measures to assess the authenticity of captured data to ensure that at all times there is proof that the PDE has not been tampered with e.g. through hashing. Therefore content management policies and systems have to be looked into to identify specific policy measures that can be implemented in the eSC to ensure captured data is secure and can be used in a useful manner.

Plan PDE pre-analysis: Once data is collected and stored in a secure database, there are elements that have to be considered to identify what can be done with the collected data, such as presenting it in a manner that makes it easy to trace events for law enforcement and forensic investigators. Therefore within the design of eSC-DFR systems that operate within the eSC environment, developers should consider all the scenarios in which collected data could be useful and design systems that can perform certain pre-analysis functions, such as categorising different types of PDR.

Defining system architecture: With all the above-mentioned factors considered, process number 7 has to do with designing a system that incorporates all the planned DFR processes, from the security aspect to the usability aspect of an eSC-DFR system. This has to do with defining the architecture and behaviour of a system that implements the DFR solutions that come from all the above-mentioned planning processes [63].

4.3 Implementation processes group for DFR in e-supply chains

In the Implementation processes group, defined system architecture is implemented. This involves the incorporation of new DFR infrastructure that is software, middleware and hardware (eSC-DFR systems). It is therefore the responsibility of each e-supply chain service provider to ensure that such architecture is implemented across the e-supply chain. It is in the implementation processes group where next-generation eSC-DFR system architectures are realised and implemented.

E-supply chain service providers are to develop and implement systems that support data collection and storage as illustrated in Figure 3. The following subsections elaborate on each eSC-DFR implementation process.

Implement PDE collection: Through the identified sources for potential digital evidence in an eSC network, the specified process deploys data capturing methods such as logging and network sniffing to capture data (PDE) at specified critical points in the e-supply chain. As mentioned in section 3.2.2, examples of data sources in an eSC system

include servers, firewalls, application software, general system logs and network logs.

Implement centralised storage: Upon collecting PDE, the next issue of concern is the storage of the collected PDE. The centralisation of collected data is critical in a distributed network environment, let alone business platform such as an eSC network [64]. That is because it reduces the chances of data redundancy and replication, also making it easy to manage the collected data and have closer control on data protection.

Implement PDE protection: Implementing PDE handling focuses on implementing security measures across the e-supply chain. Making sure that from the time data is collected and transported across an eSC network to storage, to it being accessed by authorised parties, it is not compromised. Hence in this process, security measures such as encryption, hashing, firewall and intrusion detection systems may be deployed to protect the integrity and privacy of captured PDE.

Implement PDE pre-analysis: Collected data from the eSC environment must be insightful and presented in a manner that is useful to its users. Therefore, during this process planned pre-analysis methods should be implemented, to provide law enforcement agents and forensic investigators with a user friendly yet multifaceted DFR solution to the eSC environment.

Implement access control: Access control has to do with controlling the access to the PDE. Considering that captured data is sensitive information, it is necessary to ensure that only users that need to use the PDE to solve an investigation are granted access to it. Therefore, implementing an access control strategy focuses on ensuring that authenticated users are the only ones that can view and use the PDE e.g. using username and strong passwords to access an eSC-DFR system.

Once DFR is fully implemented across the e-supply chain, there has to be a method to assess the effectiveness of the DFR process. This calls for assessment processes which are discussed in the next section.

4.4 Assessment of implementation processes group

An assessment is a set of processes that evaluate or estimate the nature, ability, or effectiveness of a method [65]. It is quite critical to be able to assess the effectiveness of a DFR approach that is implemented in an information system such as an eSC. This is necessitated for the simple reason that certain adjustments over time need to be made in infrastructure and policy to keep up with advancements in information and communications

technology. An assessment of implementation must come after the implementation of a DFR solution in the eSC has taken place. Figure 3 shows the three processes that were identified as part of the assessment processes group, namely the implementation testing process, result documentation process and result evaluation process respectively. Each process is discussed in the following sections.

Implementation Testing: As mentioned in ISO/IEC 27043 (2015), the assessment of implementation process focuses on assessing the effectiveness of an implemented DFR strategy, to determine if it meets the aims for achieving digital investigation readiness. Therefore, as illustrated in the eSC-DFR process model, the implementation testing process is an assessment process that checks to see if the implemented DFR techniques, controls and architectures are cost-effective and meet DFR fundamentals. Another important aspect to consider is the legal aspect. The ISO/IEC 27043 suggests that it is during this process that a legal review should be carried out to determine if implemented processes conform to legal regulations and digital forensics principles. This is to ensure that all collected PDE is forensically sound and can be used in a court of law.

Result documentation process: Documenting the testing process is an essential part of an assessment. It is a way to keep track of all the elements that are assessed in the implementation testing process and the observations made during testing process. This gives an authentic account of the testing process. A documentation of assessment results assists in the evaluation process, ensuring that an accurate evaluation of results can take place, which comes next in the assessment of implementation process group.

Result Evaluation: An evaluation is a process of analysing, summarising and making informed decisions based on results obtained during the result documentation process[66]. During this process recommendations are made on certain changes that might need to be made regarding implemented processes. An evaluation of the implemented DFR process in the e-supply chain environment enables service providers to modify the DFR process, making adjustments to implemented tools. Here trading partners decide on whether to go back to the planning process or implementation process, depending on the conclusions from the assessment process.

It is the authors' opinion that the three ISO/IEC 27043 DFR process groups adopted in the eSC-DFR process model eSC should result in the design and development of cutting edge eSC-DFR solutions that have three main goals, to capture PDE from the eSC network environment, ensure its integrity and

store it in a centralised data repository for retrieval by authorised users.

In the next section, system requirements that next generation eSC-DFR systems must satisfy are listed and elaborated on.

5. REQUIREMENTS FOR NEXT-GENERATION eSC-DFR SYSTEMS

The ability of an organisation to gather potential digital evidence from its network environment before an incident occurs is the focus of digital forensic readiness. Therefore the functional requirements of a DFR eSC tool, basically defines the services that such a tool must provide; which are:

- Monitor and capture all network traffic from the eSC.
- Ensure confidentiality of captured data.
- Provide exceptional usability and availability.
- Provide accessibility to the system.
- Ensure access control to the system.

Therefore, the proposed requirements are elaborated on in the sub-sections that follow.

5.1 Monitor and Capture Data from e-supply Chain

The main function of a DFR tool is to provide forensically sound records of events before an incident occurs [129]. Therefore an eSC-DFR tool should give the user a holistic view of the events transpiring in the eSC. The use of probes and other data-capturing techniques ensure that all the events that take place within an eSC are recorded in a forensically sound manner and incidents are identified. An eSC DFR tool must therefore, have a logging component, which is able to monitor and capture all the events that take place across the IT infrastructure of an eSC communication network. Once the system captures data, it should ensure the safekeeping of this data in order to ensure that the integrity is not compromised.

5.2 Confidentiality, integrity and privacy of collected data

One of the biggest concerns of many organisations is the privacy of their users' sensitive data. An eSC-DFR system should ensure that users' privacy is not compromised. The authors stress that logging facilities and log information which refers to captured data from different parts of the eSC, should be protected against tampering and unauthorised access. An eSC is a highly targeted environment; therefore it is safe to assume that an eSC-DFR system will also be a target for hackers and criminals

[129, 130]. For that reason it is highly critical that such a system be able to provide as much security as possible by employing security measures such as confidentiality, integrity, access control and privacy.

5.3 Improved usability and availability

The usability of an eSC-DFR tool is of utmost importance. Most monitoring tools are not easy to navigate, making it difficult for users to identify incidents when they occur or to merely monitor traffic [51]. It is very crucial that an eSC-DFR system be user friendly, displaying data to trading partners and law enforcement in a manner that is easy to deduce and trace events recorded. The graphic user interface (GUI) of such a tool should provide users with enough flexibility to either view, download, search categorically and filter captured data. A digital forensic investigator should be able to sign up, login and navigate through captured data effortlessly. Hence, the availability aspect of such a tool is crucial in its design. A DFR tool should be able to perform all its designated functions that include providing forensically sound captured data to users upon demand. It is therefore, crucial that usability and availability tests be conducted to ensure that the system meets its intended functions.

5.4 Having an accessible system

Since an eSC is a web-based system, an eSC-DFR system should also be web based, providing services to law enforcement agents and digital forensic investigators from this platform. Supply Chain network developers must integrate the eSC-DFR system with the eSC system, giving the tool access to the systems that are in the e-supply chain network (trading partner systems) for data capturing purposes. The system should direct all captured data to a central eSC-DFR system repository server where it is securely stored. Any system errors or alarms raised by a trading partner's internal system should also be captured by the eSC-DFR system and stored in the repository server, where records can be retrieved once a user logs in to the eSC-DFR system.

5.5 Access control of data retrieval

Considering that eSC DFR systems have to be web based, strict authentication and access control measures should be implemented. Different entities should be allocated different roles within a DFR tool. Therefore, it is proposed that an eSC-DFR system limit the access rights of different users as a privacy and confidentiality measure, in order to ensure that users only access relevant potential digital evidence from the eSC-DFR system. This requires that the system be able to store meta-data about different users, which includes the system administrator, trading partners, digital forensic investigators and law enforcement agents.

In the next section the authors present a high-level use-case diagram to show an outside view of the proposed eSC-DFR system and show how such a system interacts with its users and other software.

6. eSC-DFR SYSTEM USE-CASE DIAGRAM

A use-case diagram is widely used to capture the dynamic aspect of a system, displaying steps a user needs to follow to reach the goal as well as how the various components interact with a user. In this section the authors make use of a use-case diagram to show the high-level view of an eSC-DFR system and the interactions between actors of the system with the system itself. The authors identified three main actors i.e. eSC trading partner systems, system administrator and law enforcement agents/Forensic Investigators, depicted in the use-case diagram in Figure 4. Each actor is discussed in the sections that follow and an illustration of the roles that each user executes are also depicted in the figure.

For the system to work effectively, there are conditions that should be met. Namely, each user should have an account with the system as a system administrator, law enforcement agent or digital forensic investigator. Furthermore, the eSC network should incorporate the eSC-DFR system.

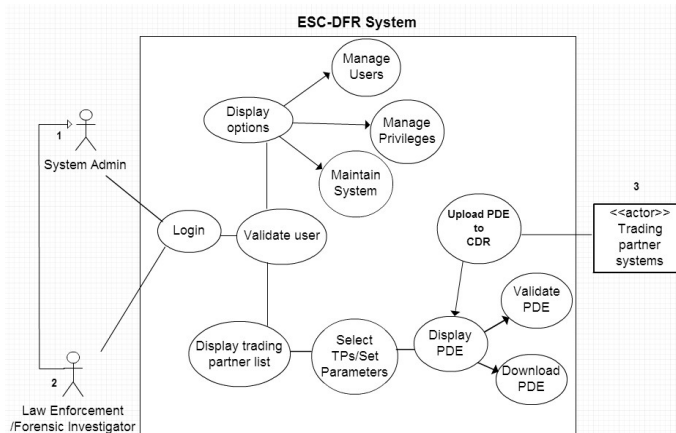


Figure 4: ESC-DFR System use-case diagram

In the sections that follow, each actor is defined, illustrating the role that each user of the system executes.

6.1 System administrator

The system administrator (actor number 1 in Figure 2) represents the person responsible for maintaining the eSC-DFR system. This user must have full access rights to the administrative aspects of the system,

ensuring that the system is configured correctly. It is the role of a system administrator to manage user accounts, manage user privileges and maintain the system. It the role of the system administrator to implement any updates to the system that add new features and resolve bugs. It is important to note, that all other users in the system are dependent on the system administrator as illustrated in the use-case diagram in Figure 4.

6.2 Law enforcement agent/Digital forensic investigator

Actor number 2 represents a law enforcement agent or digital forensic investigator, responsible for downloading, analysing and validating collected potential digital evidence (PDE) from the eSC-DFR system. This actor is granted access to the system to view, download and validate the potential digital evidence captured from the eSC. The regulation of access to captured data is critical within an eSC business environment as organisations might want to maintain a level of privacy concerning their business operations. Therefore, strict authentication measures ensure that a user is validated and granted access to relevant data only.

6.3 Trading partners' systems

An eSC is a distributed business network environment; made up of multiple web-based trading partner systems that interact with each other through an information hub, sharing information and services [11]. Therefore, a DFR tool that operates in this environment has to be integrated with the information hub and trading partners' web-based systems (actor 3) to capture data coming in and out of these systems and upload it to the eSC-DFR system. Captured data might be in the form of information requests and responses sent between trading partners through the information hub, eSC system modifications on trading partner systems or other system data such as alarm system data. The eSC-DFR system may use an internet browser for users to access the system, considering that it is a web-based application. Furthermore multiple web servers may be involved in performing different functions such as securing storage, running applications and so forth.

In the next section the design of a next generation eSC DFR system is presented, showing the system's components and how the system operates.

7. DESIGN OF PROPOSED eSC-DFR SYSTEM

In this section the authors propose a model for the design of an eSC-DFR system. The model is illustrated with two significant views; a high-level structure in Figure 7 and a more detailed logical view of the design in Figure 8. In Figure 6 an activity

diagram illustrates the services provided by the system to its users (digital forensic investigators).

Below a hypothetical scenario is provided to illustrate how the eSC-DFR system could benefit both trading partners and digital forensic investigators.

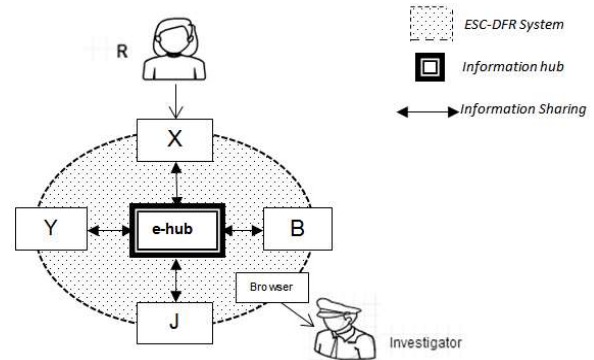


Figure: 5 A small eSC network

In the provided scenario, e-hub is a service provider (information hub) that connects suppliers, retailers and consumers in real time. E-hub allows retailers to sell supplier products that they do not keep in stock on their webstores; connecting Product Catalogue Data, using Selling and Fulfilment Tools and lastly make use of Transaction Processing. X is a web store that is connected to the e-hub network, selling Y and J's products. Both Y and J are suppliers running massive warehouses. B is a retailer just like X, selling Y and J's products. A malicious employee R who works for X decides to install a malicious code on X's web server that infiltrates the e-hub network, attacking other trading partners Y, J and B's web-based systems. After J, Y and B realise that their systems are being attacked they decide to call upon a digital forensic investigator to assist them with the investigation. The e-hub network integrated with the eSC-DFR system (that extracts PDE and log information on each trading partner's web system) is connected to the e-hub network. The forensic investigator should be able to retrieve readily available digital evidence pertaining to the incident. The evidence captured could lead directly to trading partner X's webstore, showing the installation of malicious code and the changes made by the malicious code on trading partner X's web-based system, the time of events and maybe who was logged in at the time of incident. Through the user-friendly eSC-DFR system, the investigator should be able to narrow down from all the captured data to the specific events related to the incident.

Figure 6 illustrates the behaviour of the system when a forensic investigator logs into the eSC-DFR

system, illustrating the processes that must take place at different parts of the system.

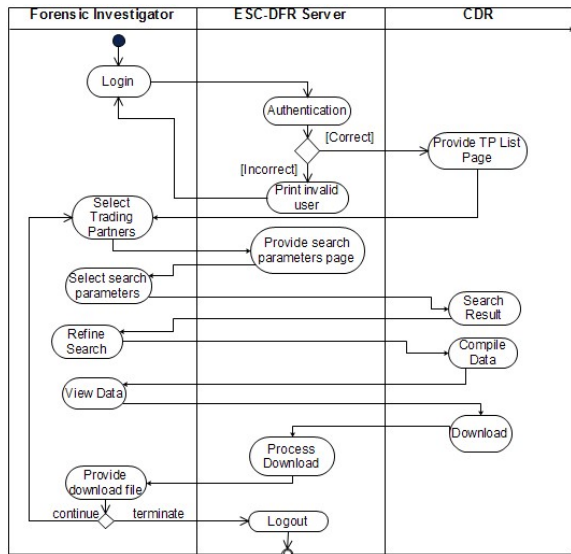


Figure 6: Digital forensic investigator and law enforcement interacting with ESC-DFR system.

In the next section, the authors present and discuss the high level eSC-DFR system architecture.

8. HIGH-LEVEL eSC-DFR SYSTEM ARCHITECTURE

There are two essential elements to the discussion of proposed eSC-DFR system, namely the eSC network and the eSC-DFR component. These elements combined provide a platform for DFR to be achieved across the eSC. The eSC network is an important aspect in the architectural design of the eSC-DFR system because it is the environment where PDE is extracted, with infrastructural components that are critical to the implementation of DFR in the eSC. Some of the components are discussed in the following sections.

The eSC-DFR component provides DFR services to DFIs and law enforcement. Such services include eSC PDE capturing, PDE storage, eSC incident prevention and eSC PDE retrieval. The DFR components that are integrated with the eSC network infrastructure enable data capturing in the eSC network. Hence, communication between the eSC-DFR component and the eSC network through web protocols and IT infrastructure is a key part of the eSC DFR system architecture as illustrated in Figure 7. This allows PDE to be captured in the eSC network and securely stored in the CDR.

Figure 7 illustrates the integration between the eSC network and the eSC-DFR component, showing the

transporting of captured data to the CDR (1) and the requesting/retrieval of PDE at the eSC-DFR component (2).

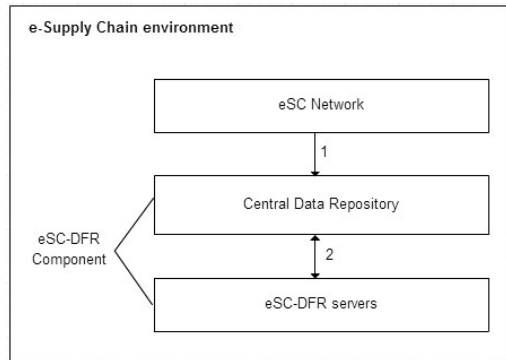


Figure: 7 High level architecture of eSC-DFR system

In the next section a more detailed model of the eSC-DFR system is presented and some critical components of the system are discussed.

9. DETAILED MODEL OF eSC-DFR SYSTEM ARCHITECTURE

Figure 8 illustrates a more detailed model of the eSC-DFR system and its key elements. It should be noted that with further research, more components might be added to the proposed model.

As mentioned previously there are two key components in the proposed architecture. One is the eSC network and second is the eSC-DFR component. Both components are to utilise secure protocols such as the SSL protocol to transmit data over the web; from the eSC network to the eSC-DFR component. There are elements that are critical to both the eSC-DFR component and the eSC network. Such elements include the eSC host servers and deployed logging probes; which are located in the eSC host machines as shown in Figure 8.

In the eSC-DFR component there are three key components, the CDR server, eSC application server, eSC-DFR web-server and a log daemon which interacts with the database located in the CDR shown in Figure 8.

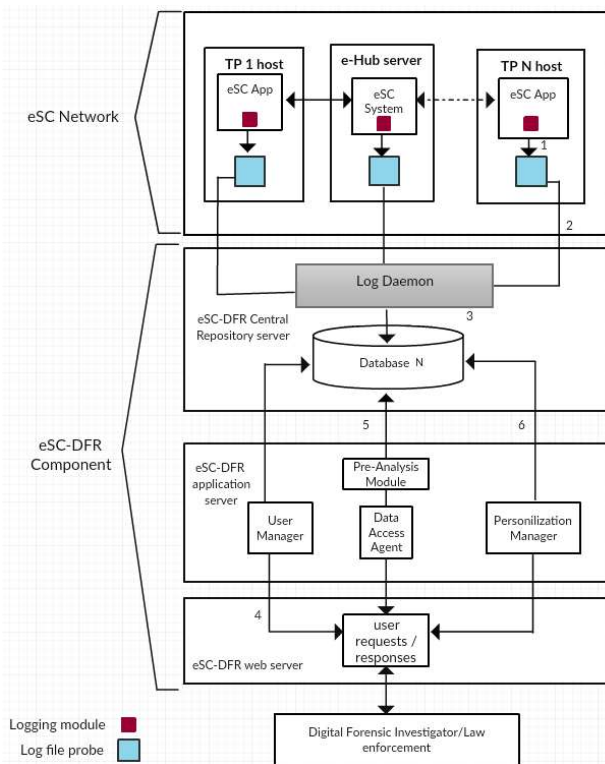


Figure: 8 Architecture of the ESC-DFR System

As mentioned in section 8, PDE is captured in the eSC network by the deployed probes and sent through to the CDR; where it is processed and stored. In the event that an incident occurs, digital forensic investigators and law enforcement agents can retrieve captured PDE from their web-browser through the eSC-DFR webserver that connects them to the CDR. In the sub-sections that follow, the authors take a deeper look at the role that each element illustrated in Figure 8 performs in the eSC-DFR system.

9.1 eSC Network

The eSC network is basically the environment that is being monitored, hence it is the source for PDE. It comprises of trading partner (TP) host machines and other eSC system infrastructure. In this network instances of the application are run by the user, whilst in communication with the eSC information hub which is the heart of the eSC allowing users to interact. The two DFR components proposed for data collection are the logging module and logging probe.

Logging module: Integrating data capturing functionality to the eSC system is the most

important aspect of an eSC-DFR system. Considering that the eSC network and the eSC-DFR system are integrated, the logging module has to be incorporated in the code of the eSC system application. Once the eSC system is installed onto a trading partner's host machine, the logging module should start capturing system activity and initiate communication with the eSC-DFR logging probe. As trading partners perform business processes using the eSC system, the eSC applications through the logging module should be able to invisibly build a vault of useful event information (log entries) for forensic investigators through the logging module. The logging module incorporated in the code of an application is designed to let a program produce messages of interest to other processes. The ability to obtain useful records of events taking place on each instance of the distributed eSC system is one of the main functional requirements of the eSC-DFR system. Therefore, having a sound logging strategy is a critical factor.

Log file probe: A log file probe is a program that runs as a background process, acquiring PDE in the form of logged events from the eSC system through the logging module, providing common formatting/filtering of log data and forwarding logs to the designated storage. Remote probes generally offer a number of different functions for different scenarios. In this scenario, the main function of such probes is to extract critical information about the eSC network from the host machines, compute digital signatures and initiate the transmission of captured data from the eSC network across the web to the eSC-DFR component. PDE might include firewall data, system log files, erased files, temp files and sniffed packets depending on the configuration of the probes. The incorporation of event logging within an instance of the eSC application is critical to the implementation of the eSC-DFR system. The distributed eSC system and other integrated eSC processes must direct log data to the log file probe using the logging module, allowing the probes to process the log data according to the log file probe's configuration. The logging file probes collectively should be able to record the entire procedure leading to an incident. They should be able to identify where requests and responses in the eSC network are coming from, the time when requests are sent and received, protocols being used and type of data being transmitted between entities in the eSC.

For improved performance a number of remote probes can be deployed. This number is based on the number of eSC hosts being monitored and the eSC network traffic throughput. Upon completion of processing the log data, the log file probe on the TP host machine should compile a log file containing the approved log events and forward it over the

internet through a secure communication channel to the central database repository server.

9.2 eSC-DFR Component

The eSC DFR component provides a number of services that include system security, system maintenance, database management, content management, and user management. The component ensures that all the DFR processes are systematically executed in the eSC, also providing authenticated user access to the system's functions. For log files to be transmitted to the eSC-DFR component, it is important to establish a connection between the eSC network and the eSC-CDR server. This might require that all the necessary ports in the eSC-DFR component firewall be opened. To ensure the security of transmitted data, the log file probes should send the captured data through secure channels such as the SSL protocol. This is to ensure that data sent back and forth from different parts of the eSC-DFR system is not visible to intruders. Once captured data is received at the eSC-CDR server, it is processed by a log daemon.

In the following sections the eSC-DFR component's sub-components are discussed.

Log daemon in eSC-DFR Repository server: A log daemon is a server process that provides a message logging facility for application and system processes. The log daemon receives data on an appropriate port from the eSC hosts and processes the received data as specified by the configuration file before sending it for storage in the central database repository database where logged events are stored.

CDR in eSC-DFR Repository server: The central database repository (CDR) is where captured data from different parts of the eSC network is stored, including eSC-DFR system files, metadata and user profiles. The CDR can be defined as a central place where data is stored and maintained or a place where data is obtained for distribution across a network. When information is transmitted across the eSC or actions are executed on trading partner systems, the deployed eSC-DFR system infrastructure will capture as much data pertaining to the those events and send that data to the CDR through the log daemon that processes received PDE from eSC network. It is the view of the authors that an eSC-DFR system might require large volumes of storage, depending on the size of the e-supply chain and considering the amount of data collected from different parts of the eSC network. Hence, issues of big data might arise but are not discussed in this paper. The database management module handles the structuring of PDE and retrieval of stored data. With

the help of the different modules at the eSC-DFR application web server that handles the logic and presentation aspects of the eSC-DFR system, users can access the eSC-DFR system content with relative ease.

eSC-DFR application server: An application server by definition provides the business logic for a web-based system, running different processes in the middleware tier [130]. Hence an eSC-DFR application server executes a number of operations which are represented in Figure 8. There are a number of modules that execute diverse critical functions, starting with the user agent.

The *user manager* handles the administrative functions of the eSC-DFR system that include system maintenance, managing user profiles, user authentication and validation.

The *data access agent* is the module that processes the user requests to access PDE and with the help of a pre-analysis module, the system can provide meaningful data to law enforcement agents and digital forensic investigators.

The *personalisation manager* module of the eSC-DFR system handles the customisation aspect of the system to provide users with a user-friendly system. The personalisation attempts to satisfy the usability requirements of the eSC-DFR system, making it an interactive system.

eSC-DFR web server: The eSC-DFR webserver is to process user requests via HTTP/S. This server attends to requests to access the eSC-DFR system by authenticated users. For example, a forensic investigator may request to login to the eSC-DFR system through a user agent such a web browser. The web browser should initiate communication with the web server by making a request for a specific for confirmation in the eSC-DFR application server and the web-server will either respond with the successful login response or an error message.

10. ARCHITECTURAL ASPECTS

Considering that the key functions of an eSC-DFR system are to capture PDE and to securely store the captured PDE for retrieval, it is safe to assume that the most critical elements of such a system are data capturing, secure storage and system reliability. Therefore, in this section the authors elaborate more on the design of the remote probes as indicated in Figure 8 and key factors to consider for system reliability and secure storage.

10.1 Design of Probes

A remote probe in general can be seen as an object used for data extraction. Data includes system log files, intrusion detection system log files, system configure files, temp files and network packets [11]. Within an eSC environment, this capturing module would be installed within each trading partner's host machine where it can capture data concerning the eSC system and send captured data to the CDR, where all captured data is stored [120]. In Figure 9 the authors display the adapted architecture of the remote probes.

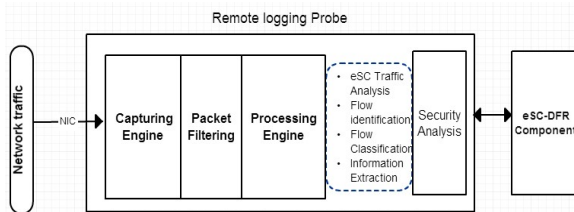


Figure: 9 Remote probes

In an eSC environment information is shared and transmitted at a fast rate; many transactions are conducted by different trading partners. It is for that reason that a probe capturing PDE in this environment needs to be able to handle the rate at which data is transmitted.

As stated in Section 3, current limitations in DFR systems include limited throughput. Hence, as a measure to ensure that the eSC-DFR system is able to cope with the high-speed traffic, the authors propose the use of a kernel-level multi-processor traffic probe that captures and analyses network traffic in high-speed networks [120]. This solution is based on execution threads that are designed to take advantage of multiprocessor architectures. The network interface cards (NIC) within the eSC host machines direct the network traffic to the probes where it is captured by the capturing engine. In the eSC-DFR system the probes as illustrated in Figure 8 are responsible for capturing eSC network traffic, filtering through captured traffic (based on their protocol or IP address), capturing system data related to the eSC network on host machines and processing/analysing captured traffic before it is sent to the CDR for storage.

10.2 Evidence storage and system reliability

It is no secret that digital forensic workloads are characterised by large volumes of data and the need for high data throughput is in fact real. Therefore, it is in the authors' opinion that improvements to data capturing rates and data transfer rates will definitely improve the performance of an eSC-DFR system. A suggested solution would be to use clustered or

parallel file systems where a user reading data from the eSC-DFR system is actually receiving data from multiple physical servers at once. This would mean that a user's read rate can exceed the maximum network I/O bandwidth of a single server. This supports the idea that was stated by Ayers that the performance of clustered file systems is greatly increased when servers and clients use teamed network adapters to increase bandwidth [51]. The eSC-DFR system will incorporate a module for managing the capturing of potential evidence and maintaining a detailed record of all tasks executed by users of the system.

Making sure that the system is reliable is also of utmost importance, especially considering that this system should provide services to businesses of all sizes. Hence, the proposed system has to be carefully designed and implemented to ensure that the system is highly robust. The use of modern software engineering techniques has to be considered to ensure that the system is as secure, robust and versatile; able to handle any unforeseen software errors while minimising the risk of data loss.

While there is room for more thorough optimisation of the eSC-DFR system, it is in the authors' opinion that the core elements that are included in the proposed design validate this approach.

11. DISCUSSION OF THE eSC-DFR PROCESS MODEL AND eSC-DFR SYSTEM ARCHITECTURE MODEL

In this section, the authors discuss the relevance of the proposed next generation eSC-DFR system design that is based on the eSC-DFR process model. The eSC-DFR process model and system architecture are a new contribution that focus on forensic planning and preparing the eSC environment for a digital forensic investigation process.

It is the authors' viewpoint that due to the ever-increasing collaboration between businesses and the incorporation of the internet in business processes, there is a need to shift from old ways of incorporating digital forensics. As suggested by the problem, digital forensics is often called upon in response to cyber incidents and not adopted as a proactive process, which creates a problem that is addressed in this paper of a lack of cutting-edge DFR systems let alone a well-formulated method for proactively collecting PDE in the eSC environment.

With the proposed method (eSC-DFR process model), there are clear procedures and processes to follow that are in line with the ISO/IEC 27043 standard in order to design and develop cutting edge eSC-DFR systems. Tools that proactively collect, store in a central data repository and maintain the integrity of PDE, only giving access to such data to

authenticated users e.g. law enforcement agents and DFIs.

The proposed system architecture in Figure 8 shows that by using the eSC-DFR process model alone, cutting edge eSC-DFR systems can be developed. The primary objective of this research was to design a high-level architecture of an eSC-DFR system that can provide useful data to digital forensic investigators and law enforcement agents to aid in digital forensic investigations and other processes that might require such data. From the limitations identified in current DFR tools the proposed eSC-DFR process model is created to assist in identifying the processes that should be followed in the design and implementation of eSC-DFR systems. The proposed eSC-DFR system architecture is designed to cater to the security needs of an eSC environment specifically, ensuring that the eSC is forensically ready. It comprises of a secure eSC-DFR system web server, remote logging probes that are strategically deployed in the eSC network, a central repository database for storage of PDE and a user component that provides users with controlled access to the system. The authors identified the need for next generation DFR systems that:

- Can handle high throughput that passes through eSC information networks.
- Are robust and can meet DFR toll requirements.
- Can present captured PDE in a comprehensible manner.
- Are able to maintain a level of privacy for trading partners.
- Provide users with uncompromised forensically sound data.
- Collect data on supplier's supplier relationships.

Considering that an eSC environment may comprise of many entities, the proposed architecture was designed to handle large amounts of potential evidence data. It is in the authors' opinion that software developers should ensure that the capturing and storage components of such a system can capture data at high speeds and accommodate large volumes of data. In addition, it should be considered that an eSC is a distributed network environment connecting retailers to suppliers and suppliers to more suppliers. The architecture of the eSC-DFR system is designed to cater to those kinds of relationships. The deployment of remote probes as data capturing modules onto host systems in the eSC network ensure that potential digital evidence is captured across the eSC.

As mentioned earlier in the paper, a major requirement of a DFR tool is that it should ensure that the integrity of captured PDE is not compromised, thereby meeting digital forensics standards. Therefore, the use of secure communication protocols and remote probes is incorporated in the proposed architecture. The use of encryption and

digital signatures amongst other methods are suggested to maintain the integrity of captured data. In addition, a specialised probe design was incorporated to ensure that the capturing of high speed traffic is accomplished [11].

It has been strongly emphasised by the authors that the ease of use that a DFR system provides and its ability to present captured data in a comprehensible manner is of utmost importance (Usability). Therefore in this paper the authors emphasise the importance of paying close attention to the design of a usable graphic user interface; making the eSC-DFR system easy to navigate, the time taken to retrieve captured evidence and trace events is greatly reduced. Hence, developers should ensure that much attention is placed on the usability aspect of the system.

The strict authentication of users through the security component in the eSC-DFR system architecture ensures that a level of privacy for sensitive data is maintained. It is of great importance to stress the point that the eSC-DFR system is a system designed to serve law enforcement and digital forensic investigators to solve cases and monitor the eSC. Therefore, right of access should be strictly monitored to ensure that only validated users are granted access to the system. Therefore, measures taken to control access and at the same time maintain a level of flexibility for users should be considered in the development of such a system.

It is evident, that the use of IT comes with numerous challenges that can cost organisations large sums of money. Although the effectiveness of a DFR system can only be fully comprehended through an assessment of the system, the authors believe that the proposed eSC-DFR system can help organisations to avoid incidents in the eSC. Also such a system can assist law enforcement agents and digital forensic investigators by providing readily available digital evidence that can be used in the investigative processes.

Considering that collected PDE is for prosecution purposes and law enforcement purposes, there are strict measures that should be enforced to ensure that only authenticated users have access to collected data as there might be serious legal consequences if captured information ends up in the wrong hands. It is also important to mention that different jurisdiction laws make provision for information that is captured to facilitate prosecution in a judicial system [60, 68, 131].

12. CONCLUSION

Existing general purpose DFR systems are rapidly becoming inadequate for modern commercial network systems (eSCs). The out-dated architecture of such tools limits their ability to scale and adopt the current and future eSC forensic readiness processes. In the recent past, researchers have cited the need for more capable DFR systems that can support digital

forensic investigations in the event an incident occurs. As much as these are steps in the right direction, implementing security policies and processes alone does not ensure that the eSC environment is fully forensically ready.

This paper proposes a process model which can be used as a blueprint for the design of next generation eSC-DFR systems that can fully cater to the DFR requirements of such an environment. The eSC-DFR system is a useful tool for collecting data and monitoring the eSC environment. The design of the proposed system which is illustrated in Figure 8 is built around improving the user experience and providing adequate forensically sound data to trading partners and law enforcement agents about all trading partner interactions. The use of kernel-level multiprocessor network probes ensures that no data is lost during the packet capturing process. The authors also acknowledge that an eSC handles large amounts of data that are transmitted upstream and downstream of the supply chain, hence the eSC-DFR system provides clustered storage to increase the performance, capacity and reliability of the system.

In this paper the authors were able to discuss the limitations of current DFR systems and requirements for next-generation eSC-DFR systems were proposed. A detailed eSC-DFR process model was proposed including a generic architectural design for a practical next-generation eSC-DFR system was presented. The design and implementation of such a system is ongoing. The system incorporates strategies for optimising and managing potential evidence data collected from different parts of an eSC. For future work an implementation of the eSC-DFR system is necessary, also providing a look into the performance of the proposed system. This would assist in verifying whether the proposed system accomplishes what it is intended to accomplish.