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 [1]. 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 [2] 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

Based on: "A Model for the Design of Next Generation e-supply Chain Digital Forensic Readiness Tools", by D. Masvosvere and H. Venter which appeared in the Proceedings of Information Security South African (ISSA) 2015, Johannesburg, 12 & 13 August 2015.

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 [3].

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 [4]. 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 [5]. 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 [1]. 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 [6].

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 webservers in the eSC network. 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. 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 [8].

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 [9].

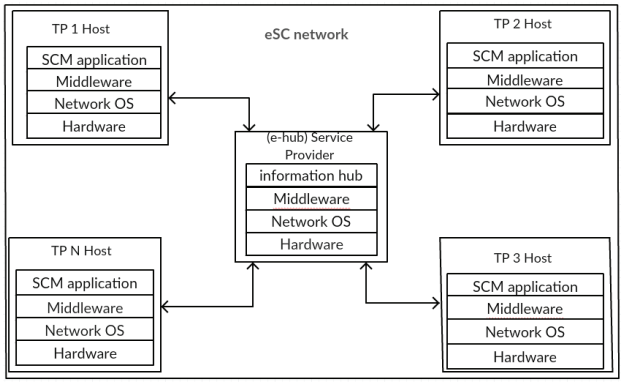

Figure 1: eSC Structure

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 [10]. Rodney McKemmish [11] 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 [12]. By definition DFR is the capability of a system to efficiently collect valid digital evidence that can be used in a court of law [13]. 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 [14] 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 [15-19].

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.

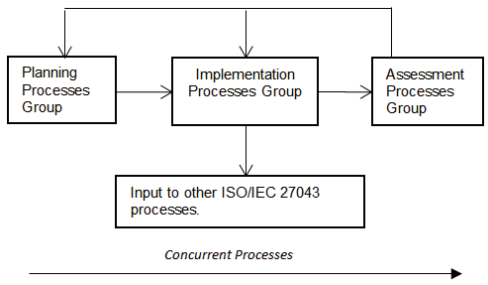

Figure 2: Readiness processes groups

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 [3, 10, 20, 21]. 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 [5]. For an investigation to be successful, especially in the DFR arena, as much data as possible needs to be captured. Considering that the practicallity 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 disussed 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 [22]. 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 experince and system functionality.

3.3 Compromised privacy and limited filtering of packets

Packet sniffing and filtering has its drawbacks [23]. 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 [2]. 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 [2]. 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 [2]. 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 [24].

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.

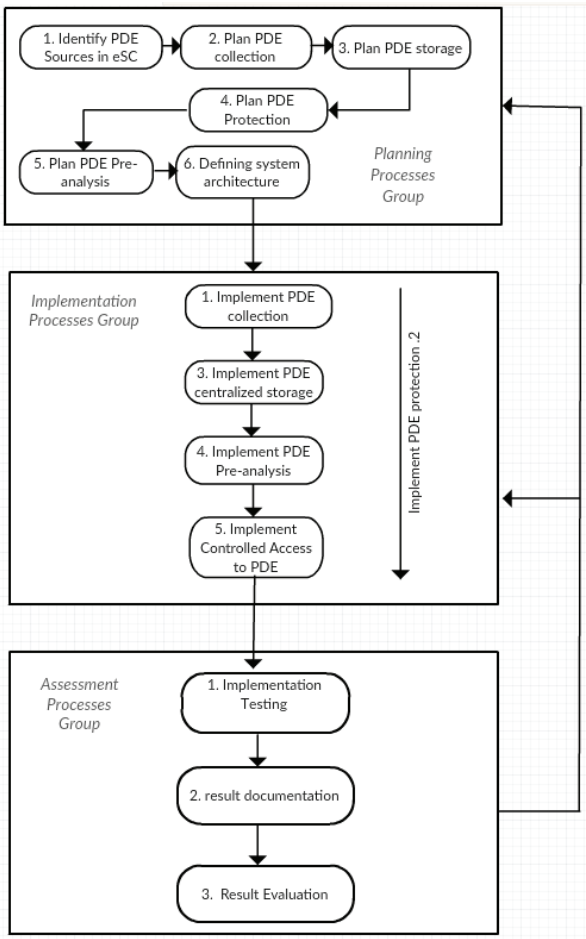

Figure 3: eSC-DFR process model

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 [25]. 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 [26].

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 sub-sections 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 [27]. 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 [28]. 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 IS0/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[29]. 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 [24]. 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 [24, 30]. 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 [2]. 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.

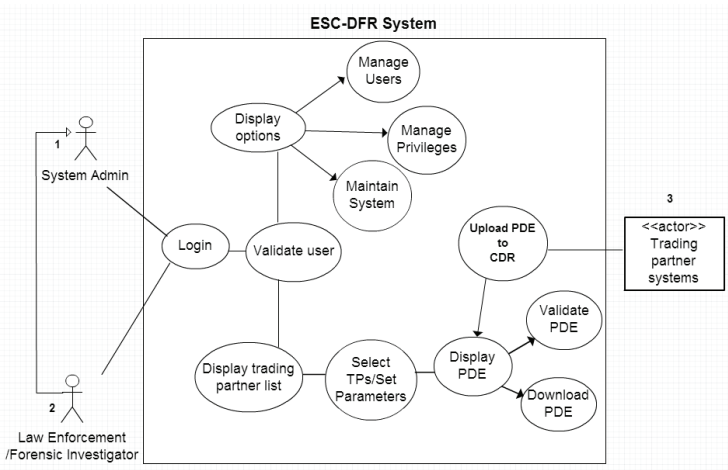

Figure 4: ESC-DFR System use-case diagram

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.

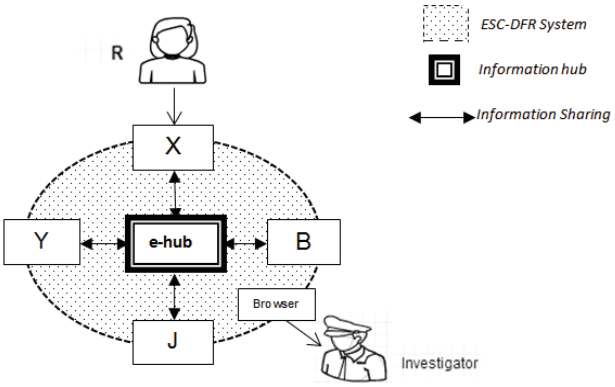

Figure: 5 A small eSC network

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.

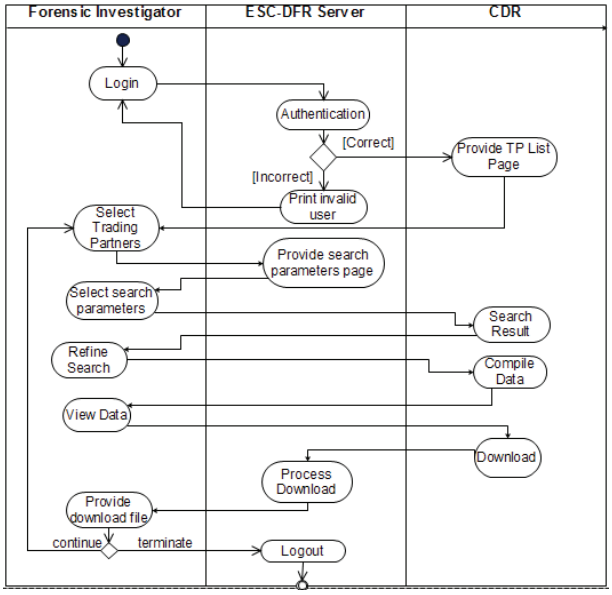

Figure 6: Digital forensic investigator and law enforcement interacting with ESC-DFR system.

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).

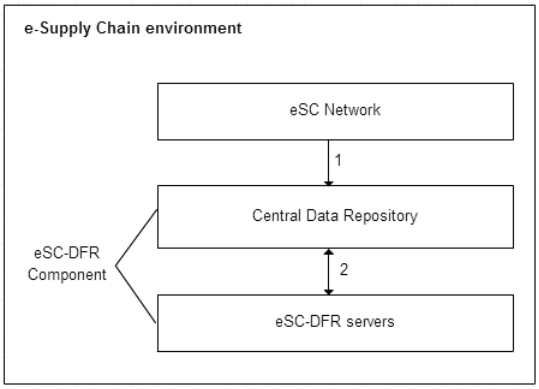

Figure: 7 High level architecture of eSC-DFR system

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 below.

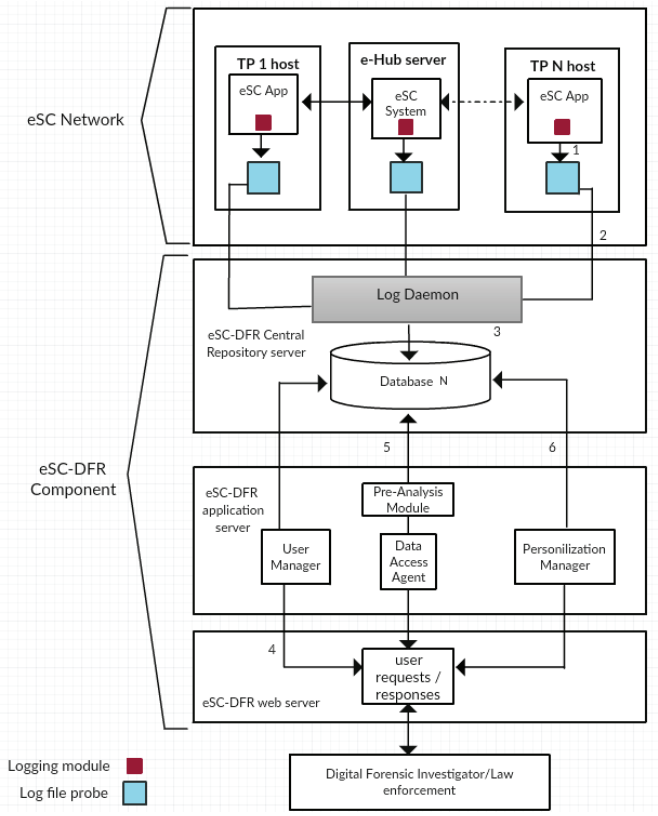

Figure: 8 Architecture of the ESC-DFR System

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 formating/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 [30]. 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 [31]. In Figure 9 the authors display the adapted architecture of the remote probes.

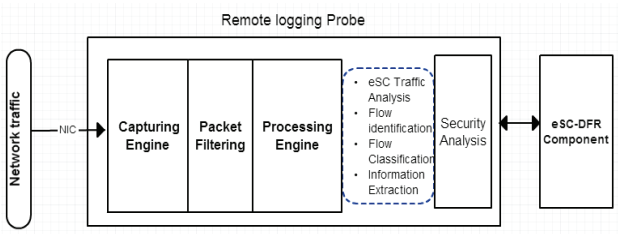

Figure: 9 Remote probes

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 [31]. 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 [2]. 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 [3, 32, 33].

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 as 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.

13. REFERENCES

[1] H. Cheng, "An integration framework of erm, scm, crm," in *Management and Service Science, 2009. MASS'09. International Conference on*, 2009, pp. 1-4.

[2] D. Ayers, "A second generation computer forensic analysis system," *digital investigation,* vol. 6, pp. S34-S42, 2009.

[3] V. R. Kebande 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, pp. 23-32.

[4] S. D. Pathak, 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, pp. 808-816.

[5] L. Pulevska-Ivanovska and N. Kaleshovska, "Implementation of e-Supply Chain Management."

[6] P. Helo and B. Szekely, "Logistics information systems: an analysis of software solutions for supply chain co-ordination," *Industrial Management & Data Systems,* vol. 105, pp. 5-18, 2005.

[7] R. E. Schantz and D. C. Schmidt, "Middleware for distributed systems: Evolving the common structure for network-centric applications," *Encyclopedia of Software Engineering,* vol. 1, 2002.

[8] R. B. Handfield and E. L. Nichols, *Supply chain redesign: Transforming supply chains into integrated value systems*: FT Press, 2002.

[9] N. Thomas, "Multi-state and multi-sensor incident detection systems for arterial streets," *Transportation Research Part C: Emerging Technologies,* vol. 6, pp. 337-357, 1998.

[10] K. Reddy and H. S. Venter, "The architecture of a digital forensic readiness management system," *Computers & Security,* vol. 32, pp. 73-89, 2013.

[11] R. McKemmish, *When is digital evidence forensically sound?*: Springer, 2008.

[12] G. G. Richard III and V. Roussev, "Digital forensics tools: the next generation," *Digital crime and forensic science in cyberspace,* pp. 76-91, 2006.

[13] C. Lankshear and M. Knobel, *Digital literacies: Concepts, policies and practices* vol. 30: Peter Lang, 2008.

[14] R. Rowlingson, "A ten-step process for forensic readiness," *International Journal of Digital Evidence,* vol. 2, pp. 1-28, 2004.

[15] V. Kebande 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, p. 373.

[16] S. Omeleze 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, pp. 1-8.

[17] M. Grobler, "The Need for Digital Evidence Standardisation," *Emerging Digital Forensics Applications for Crime Detection, Prevention, and Security,* p. 234, 2013.

[18] M. Ingels, 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, pp. 1-8.

[19] A. Ajijola, 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, pp. 66-73.

[20] D. Barske, A. Stander, and J. Jordaan, "A Digital Forensic Readiness framework for South African SME's," in *Information Security for South Africa (ISSA), 2010*, 2010, pp. 1-6.

[21] P. M. Trenwith and H. S. Venter, "Digital forensic readiness in the cloud," in *Information Security for South Africa, 2013*, 2013, pp. 1-5.

[22] R. G. Clegg, M. S. Withall, A. W. Moore, I. W. Phillips, D. J. Parish, M. Rio, *et al*., "Challenges in the capture and dissemination of measurements from high-speed networks," *arXiv preprint arXiv:1303.6908,* 2013.

[23] B. Pande, D. Gupta, D. Sanghi, and S. K. Jain, "The Network Monitoring Tool-PickPacket," in *Information Technology and Applications, 2005. ICITA 2005. Third International Conference on*, 2005, pp. 191-196.

[24] I. ISO/IEC 27043, "Information Technology-Security techniques- Assurance for digital evidence investigation process," 2015.

[25] E. Casey, *Digital evidence and computer crime: Forensic science, computers, and the internet*: Academic press, 2011.

[26] H. Jaakkola and B. Thalheim, "Architecture-Driven Modelling Methodologies," in *EJC*, 2010, pp. 97-116.

[27] A. Turner, C. Bullok, K. Irvin, J. Hayre, and K. Markham, "Method and system for acquisition

and centralized storage of event logs from disparate systems," ed: Google Patents, 2005.

[28] V. R. Prybutok, 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,* vol. 10, pp. 6-26, 1997.

[29] G. P. Wiggins, *Educative assessment: Designing assessments to inform and improve student performance* vol. 1: Jossey-Bass San Francisco, CA, 1998.

[30] E. J. Sinz, B. Knobloch, and S. Mantel, "Web-Application-Server," *Wirtschaftsinformatik,* vol. 42, pp. 550-552, 2000.

[31] L. Zabala, A. Ferro, A. Pineda, and A. Muñoz, "Modelling a Network Traffic Probe Over a Multiprocessor Architecture," *Edited by Jesús Hamilton Ortiz,* p. 303, 2012.

[32] J. Rajamaki 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, pp. 198-203.

[33] D. J. Ryan and G. Shpantzer, "Legal aspects of digital forensics," in *Proceedings: Forensics Workshop*, 2002.