

Computer Science and Software Engineering
College of Engineering, University of Canterbury

Master's Thesis

Design of a Forensic Overlay Model for Application Development

Linlin Ke

A thesis submitted in fulfilment of the requirements for the Degree of Master of Science in Computer Science at the University of Canterbury, New Zealand

Supervisors:
Ray Hunt
Malcolm Shore

Forensics capability is becoming increasingly important for the enterprise/network environment. Therefore, businesses need to find an optimised forensics solution that suits the high level business/forensics requirements. However, most businesses are still staying with the conventional method of digital investigation, which means using forensics tools to retrieve evidential data from the target system. Many businesses lack a comprehensive model to help understand the forensics requirements on different levels. Also, businesses lack a method to integrate and manage forensics knowledge into daily operation.

In this research, a forensics overlay is being developed on an existing business framework – SABSA model. The overlay helps different business roles to understand and apply forensics knowledge into their daily tasks. With help of the overlay, businesses are able to reduce the overreliance on the third party forensics tools through developing their own forensically sound applications. To test the theory of forensically sound application development, and evaluate the usability of the overlay, a forensically sound email client is designed and developed accordingly.

Contents

List of Figures.....	IX
List of Tables.....	X
1 Introduction.....	1
1.1 Current Digital Forensics Environment.....	1
1.1.1 Law Enforcement Elements in the Previous Forensics Landscape	2
1.1.2 The Corporate Elements in the Current Forensics Landscape.....	3
1.2 Forensically Sound Applications (FSAs).....	5
1.2.1 Challenges of the Forensics Tools Development.....	6
1.2.2 Define “Forensically Sound”	6
1.3 Research Progress and Proposed Solution.....	7
1.3.1 Forensics Overlay Development Process	8
1.3.2 Forensics Overlay	9
1.3.3 Forensically Sound Email Client Development Process.....	10
1.3.4 Research Goals.....	12
1.4 Related Work	13
1.5 Outline.....	15
2 Sherwood Applied Business Security Architecture	16
2.1 What is SABSA?	16
2.1.1 Broad Strategic Objective.....	17
2.1.2 Awareness of Risks.....	18
2.1.3 Simplify Complexity.....	18
2.1.4 Measure Performance against Objectives.....	19
2.2 SABSA Model	20
2.2.1 Contextual Security Architecture.....	21
2.2.2 Conceptual Security Architecture.....	22
2.2.3 Logical Security Architecture	24
2.2.4 Physical Security Architecture	25
2.2.5 Component Security Architecture	26
2.2.6 Operational Security Architecture	27
2.3 Why Use SABSA?	27
2.3.1 Other Forensics Models	27
2.3.2 Advantages of SABSA Model.....	29
2.4 Previous Work.....	31

2.5 A New Model – The Forensics Overlay Based on SABSA	32
2.5.1 Differences between the Forensics Overlay and the SABSA Matrix.....	34
3 Forensics Industry Evolution and Forensics Knowledge.....	36
3.1 Evolution of Cybercrime and Digital Forensics Investigation	36
3.1.1 The Early Days	37
3.1.2 The Golden Age.....	38
3.1.3 The Current Crisis of Digital Forensics.....	42
3.2 Forensics Knowledge	44
3.3 Selection of Forensics Standards.....	46
3.4 Summary: The Knowledge Structure of the Forensics Overlay.....	51
4 Design of a Forensics Overlay	53
4.1 Contextual Layer	53
4.1.1 Assets	54
4.1.2 Motivation.....	56
4.1.3 Process	57
4.2 Conceptual Layer.....	59
4.2.1 Assets	59
4.2.2 Motivation.....	62
4.2.3 Process	63
4.2.4 People.....	65
4.3 Logical Layer.....	66
4.3.1 Motivation.....	66
4.3.2 Process	67
4.3.3 People.....	68
4.3.4 Location.....	69
4.4 Physical Layer.....	70
4.4.1 Motivation.....	70
4.4.2 Process	71
4.4.3 People.....	71
4.6 Operational Layer.....	73
4.7 Forensics Overlay	73
4.7.1 Layers	73
4.7.2 Cells.....	74
5 Digital Forensics in a Business Environment	76

5.1 Introduction.....	76
5.2 Static Forensics Implementation in a Business Environment.....	77
5.2.1 SF Deficiencies.....	78
5.3 Live Forensics Implementation in a Business Environment.....	79
5.3.1 LF Challenges.....	79
5.3.2 Hybrid Implementation of Both SF & LF in a Business Environment	80
5.4 Case Study [75].....	81
5.4.1 Issues.....	84
5.5 Proposed Solution.....	86
5.5.1 “Forensics-Friendly Features” are NOT “Forensics Features”	86
5.5.2 From “Forensics Requirements” to “Forensics Features”	87
5.5.3 Designing and Developing Forensically Sound Applications for Businesses	88
6 Design of a Forensically Sound Email Client with the Overlay	90
6.1 Email Client as a Testing Platform	90
6.2 Using the Overlay to Design Email Client Forensics Features.....	91
6.3 Forensics Features for an Email Client.....	93
6.4 Implementation.....	95
6.4.1 Real-Time Recording Email SENDING Event	95
6.4.2 Forensically Backing up Email SENDING Records.....	98
6.4.3 Structured Record.....	98
6.4.4 Hash Function.....	98
6.4.5 User Authentication and User Record.....	99
6.4.6 Fixed Email Account	101
6.4.7 Other Forensics Features.....	103
7 Conclusion.....	105
7.1 Summary	105
7.1.1 Results of a Forensically Sound Email Design	105
7.1.2 Result of a Forensically Sound Email Development	107
7.2 Future Works.....	109
7.2.1 Additional Development for the Forensics Overlay	109
7.2.2 A Future Development for FSFs	110
7.2.3 A Future Overlay for Cloud Computing	111
Bibliography	113

A. Forensically Sound Email Development Code	124
A.1 Login	124
A.2 Normal User's Email Activities.....	127
A.3 Investigator's Activities.....	133
A.4 Sample Code of an Additional Application that Compares the Hash Values.	139

List of Figures

Figure 1- 1 Forensics Entities.....	3
Figure 1- 2 Updated Forensics Entities.....	4
Figure 1- 3 FSAs for Corporate Environment.....	5
Figure 1- 4 Research & Proposed Solution.....	8
Figure 1- 5 SABSA Lifecycle.....	9
Figure 2- 1 SABSA Standard Business Attributes (SBAs)	23
Figure 2- 2 Traceability Sample between Logical and Physical Layer.....	25
Figure 2- 3 Forensically Sound Application Users.....	26
Figure 2- 4 Differences between Current Forensics Model and SABSA Model	30
Figure 2- 5 SNA/RAPSA Integrated with SABSA Framework.....	31
Figure 2- 6 Forensics Element Integrated with SABSA Framework	32
Figure 2- 7 Forensics Overlay for Enterprise Forensics Program/Project Development	33
Figure 2- 8 Differences between the Forensics Overlay and the SABSA Matrix.....	34
Figure 3- 1 Cybercrime Categories.....	39
Figure 3- 2 Conventional Forensics Lifecycle.....	40
Figure 3- 3 Digital Forensics Standardisation.....	41
Figure 3- 4 Business Considerations.....	51
Figure 3- 5 Framework of SABSA Matrix.....	51
Figure 3- 6 Knowledge Structure of the Forensics Overlay.....	52
Figure 4- 1 Factors to Consider for Developing Forensics Capability.....	59
Figure 4- 2 Threats to Digital Evidence.....	62
Figure 4- 3 Enterprise Forensics Procedure (EFP).....	64
Figure 4- 4 Traceability of the Forensics Process between Overlay Levels.....	68
Figure 4- 5 Trusted Evidence Transferring.....	69
Figure 4- 6 Forensics Policy Domain Map	70
Figure 4- 7 Design of a Forensics Overlay.....	75
Figure 5- 1 Enterprise Forensics Action Flow Chart.....	83
Figure 5- 2 FCT and FMT in Microsoft Office Documents.....	87
Figure 5- 3 Design Process of a Forensically Sound Application	88
Figure 5- 4 High Level Design of Business Forensically Sound Application.....	89
Figure 6- 1 Forensics Overlay Tractability.....	92
Figure 6- 2 Mapping the Overlay Layers with SDLC.....	93
Figure 6- 3 User Authentication Interface	100
Figure 6- 4 Search Warrant Information Enter	101
Figure 6- 5 Fixed Email User Account	102
Figure 6- 6 Host Information Interface	103

List of Tables

Table 1- 1 Criterion for Forensically Sound.....	7
Table 1- 2 Enterprise Forensics Architecture	13
Table 2- 1 Sample Business Attributes Measurement Table [16].....	19
Table 2- 2 SABSA Model: Stakeholders' Views [14].....	20
Table 2- 3 SABSA Matrix Structure	21
Table 2- 4 Business and Forensics Definition of the Term “Inform”	31
Table 3- 1 Forensics Knowledge and Forensic Challenges	46
Table 3- 2 Selected Forensics Standards	50
Table 4- 1 Business/Forensics Drivers for Contextual Asset	56
Table 4- 2 Threats against Potential Digital Evidence	57
Table 4- 3 Sample Attributes Extracted from WD27037	61
Table 4- 4 Define Attributes in Terms of Forensics.....	61
Table 4- 5 Sample Attributes of Rules of Evidence	63
Table 4- 6 RACIW Table.....	65
Table 4- 7 Forensics Policy Matrix.....	67
Table 4- 8 DO and DONOT List	71
Table 4- 9 Overlay Layers.....	74
Table 5- 1 Issues of an Enterprise Forensics Action	85
Table 6- 1 Forensics Design Process in Details.....	94
Table 6- 2 Sample Code 1 - Regular Email Sending Event	96
Table 6- 3 Sample Code 2 - Forensically Sound Email Sending.....	98
Table 6- 4 Sample Code 3 - Hash Function	99
Table 6- 5 Sample Code 4 - SHA1 Hash	100
Table 6- 6 Sample Code 5 - Host Information.....	104

1 Introduction

This project analyses the deficiencies of current forensics models. To overcome these deficiencies, a new forensics model is built for enhancing digital investigation capability in a business environment. In addition, this project also analyses the overly reliance of third party forensics tools and propose that businesses construct their own forensics application and further develop a business/forensics environment. To improve the usability of the new model and demonstrate that a business/forensics environment can be less dependent on the third party forensics tools, an email client (the most sought-after business application) is designed and developed according to current forensics standards. This project was motivated by several questions. Why a new forensics model is needed? What are the deficiencies of current forensics models? What is needed in the new forensics model? Why a daily used application such as an Email Client needs built-in forensics features? And how the new forensics model helps design forensics features? This chapter briefly explores answers to these questions. More detailed analysis is provided in later chapters.

Chapter One:

- 1.1 Describes the Current Digital Forensics Environment
- 1.2 Introduces the Concept of Forensically Sound Applications (FSAs)
- 1.3 Introduces the Current Research Progresses and Goals

1.1 Current Digital Forensics Environment

To briefly answer some of the questions raised previously, section 1.1 gives a general picture of the current forensics landscape and key forensics research objectives and also introduces the methodology that guides the development of a forensics model.

1.1.1 Law Enforcement Elements in the Previous Forensics Landscape

Emerging in the 1980s, digital forensics has evolved to become an integral part of many legal case investigations. Digital forensics evolves with new techniques, concepts, legal frameworks, and forensics regulations. In recent years, some revolutionary technological developments have shaped the forensics landscape into a new form in which digital forensics has been widely adopted in the business world.

In previous forensics landscapes, one of the most essential preconditions of digital forensics was to meet the requirements of the key stakeholder – Law Enforcement, seen in Figure 1-1. The forensics standards and legal case precedent are studied to provide forensics requirements for forensics operations. The most frequently used (or conventional) method to conduct digital investigation is to use tools that have built-in forensics features to collect, preserve and analyse evidential data. These forensics features are designed, implemented and tested in a manner according to the requirements from forensics regulation authorities so that the tools are able to extract evidence from the target system. Design and development of current forensics tools are continually being challenged by two major factors. Firstly, anti-forensics techniques and new technologies such as virtualisation, cloud computing and distributed computing [1] [2]; secondly, it is also challenged by the expanding scope of digital forensics.

This research focuses on the expanding scope of digital forensics and its impact on various levels of digital forensics activities.

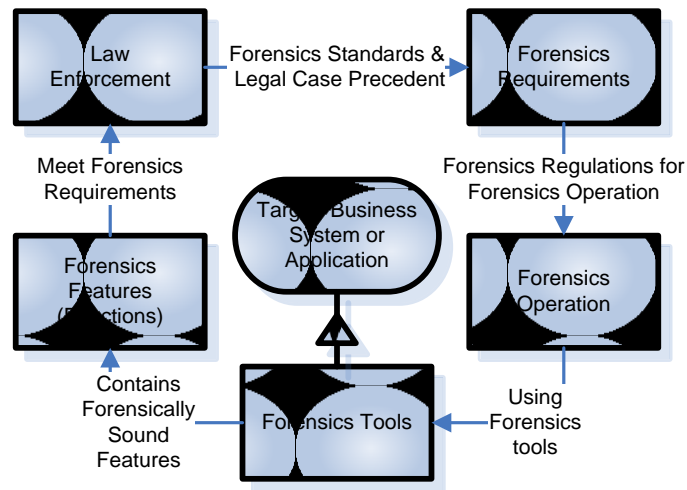


Figure 1- 1 Forensics Entities

1.1.2 The Corporate Elements in the Current Forensics Landscape

The motivation to develop a new forensics model is that the current models cannot match the expanding digital forensics scope. One of the most important additions to digital forensics scope is additional stakeholders such as corporate environments. An increasing number of enterprise digital crimes have brought corporations and government agencies, into the battlefield against cyber crimes and cyber terrorism. Therefore, organisational decisions and forensic regulations need to be considered equally in the current forensics landscape, seen in Figure 1-2. A new forensics model is needed to provide both business and forensics views for an enterprise forensics environment.

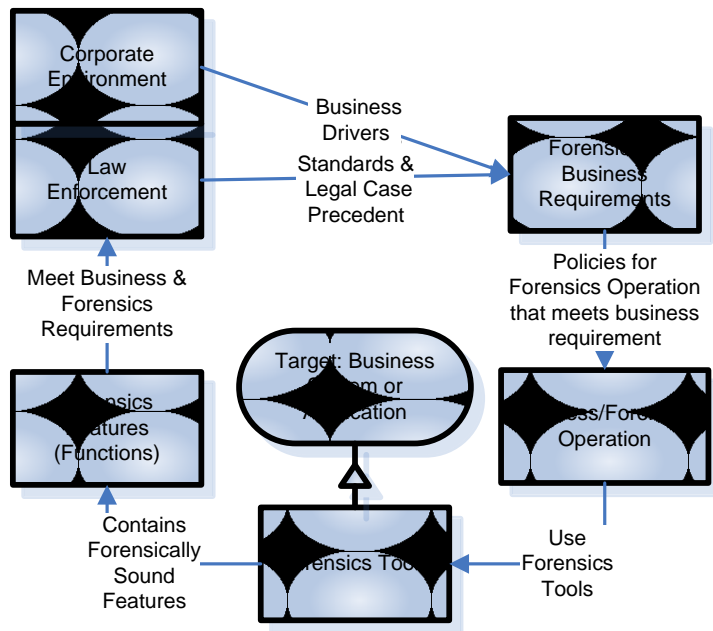


Figure 1- 2 Updated Forensics Entities

Current models have a narrow view to address forensics issues, focusing only on a technical and operational level. Technical forensics models usually focus on using tools in analysing a typical system or application. If the system or application is updated, the technical focused model may not be able to cope with the updated system. This results in businesses overly relying on forensics tools. On the other hand, operational forensics models usually focus on forensics activities phases, roles and responsibilities. It follows that businesses seeks compliance with forensics standards or business policies rather than designing a forensics solution which suits the typical problem. These are the major deficiencies of current forensics models.

The forensics community has noticed that the digital investigation capability should be initiated by high level business requirements and not by the provision of third party vendor's forensics tools. The first step to enhance an enterprise digital investigative/Electronic discovery capability is to identify business/forensics requirements from the strategic level [3]. Therefore, the new forensics model should provide an end-to-end (from business forensics requirement to physical forensics features) forensics solution to network/enterprise environments.

1.2 Forensically Sound Applications (FSAs)

To further solve the problem of overly relying on forensics tools, the second objective of this research is to test the proposed idea of designing and developing a forensically sound application using the new forensics model.

In Figure 1-2, the business systems and applications are the victims of cybercrimes while forensics tools collect the evidence from cybercrimes. The idea of FSAs aims to design the forensics features in business systems and applications so that they are not only cybercrime victims but also provide the functions of collecting evidence. In an ideal business forensics environment, shown in Figure 1-3, the business consists of various forensically sound systems, subsystems, and applications. Therefore, businesses design their own environment according to their forensics requirements.

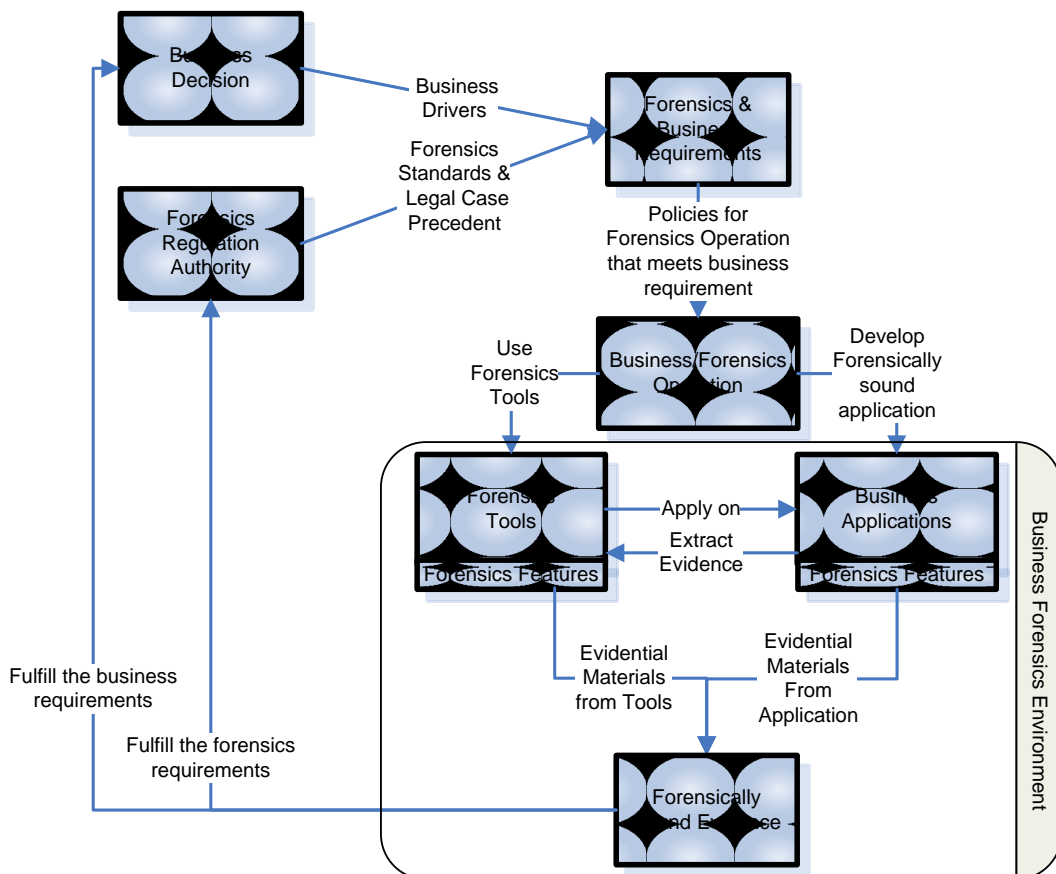


Figure 1- 3 FSAs for Corporate Environment

1.2.1 Challenges of the Forensics Tools Development

In the business component level that focuses on third party tools, recent research [4] shows that during 2005 to 2010, a significant amount of forensics suites such as EnCase and FTK have moved into the network/enterprise environment for electronic discovery purposes. It follows that the forensics tool development faces the challenges from understanding various business requirements and integrating them into software development process. Failure to fulfil the business requirement leads to the low forensics tools' compatibility. Challenged by increasingly changing business and technology environments, forensics tools are required to provide better acquisition, as well as faster and more efficient analysis [5]. Other challenges include forensics tools requiring long term testing before being ready to launch into the market and to be recognised as mainstream [6].

With all these challenges, the development of forensics tools faces tremendous amount of workload in 1) researching and gathering common corporate forensics requirements, 2) designing forensics features, 3) developing software and 4) long term testing. Most importantly, commercial forensics tools have to strictly meet overall requirements from law enforcement and businesses since commercial forensics tools serve the primary goal of prosecution, while business FSAs serve the primary goal of maintaining the business service with a secondary goal of prosecution. It is not efficient to use the same tools for different goals.

1.2.2 Define “Forensically Sound”

The entire process of designing and developing FSAs is actually to define this term in both the conceptual and physical level.

In the conceptual level, according to McKemish, R. (2008) [7] “forensically sound” means “The application of a transparent digital forensic process that preserves the original meaning of the data for production in a court of law.” There are four criteria for the term forensically sound, as shown in Table 1-1. Furthermore, the newly developed forensics model defines what “forensically sound” means in a corporate application.

In the physical level, according to the newly developed forensics model, a forensically sound email client is developed with built-in forensics features.

Criterion	Description
Meaning	Has the meaning and, therefore, the interpretation of the electronic evidence been unaffected by the digital forensic process?
Error	Have all errors been reasonably identified and satisfactorily explained so as to remove any doubt over the reliability of the evidence?
Transparency	Is the digital forensic process capable of being independently examined and verified in its entirety?
Experience	Has the digital forensic analysis been undertaken by an individual with sufficient and relevant experience?

Table 1- 1 Criterion for Forensically Sound

1.3 Research Progress and Proposed Solution

This research reviews the current landscapes of digital forensics and studies current forensics models. Learning that the current forensics models generally lack an overall view of the forensics landscape, we designed and built an end-to-end forensics model which contains different layers in the business/forensics environment. The model solves the problems of 1) lacking forensics consideration during business application development; 2) overly relying on forensics tools in a corporate environment. It further helps businesses in building forensics capabilities, dealing with corporate digital discovery issues and managing forensics related projects.

There are two outcomes for this project. The first outcome is a newly designed forensics model called the Forensics Overlay (the Overlay), which is using the SABSA (Sherwood Applied Business Security Architecture) matrix (see Section 1.4). The second outcome is (see Section 1.5) a forensically sound email client, designed and developed through the guidance of the overlay. See Figure 1-4.

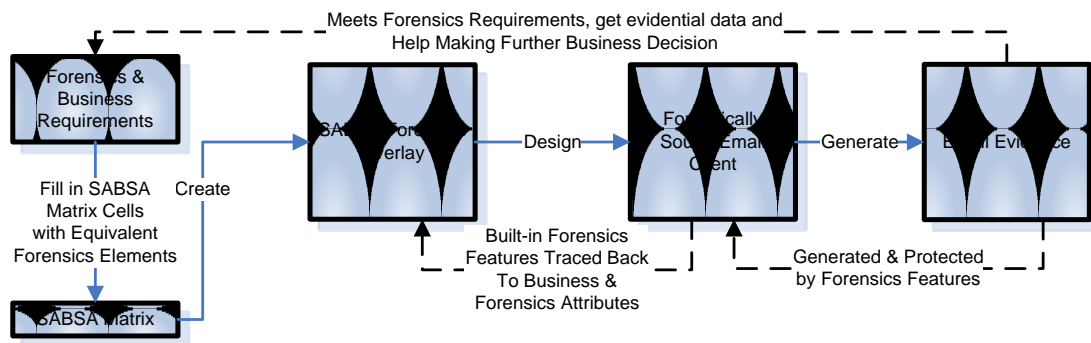


Figure 1- 4 Research & Proposed Solution

1.3.1 Forensics Overlay Development Process

The forensics overlay development is based on SABSA methodology which is elaborated in the book entitled Enterprise Security Architecture [8]. It is a business driven philosophy that has practical implications on designing security architecture.

SABSA Matrix

The core of SABSA methodology is a 6x6 SABSA matrix. The forensics overlay development process is to populate thirty six SABSA matrix cells with forensics concerns. Vertically, it contains six layers (contextual, conceptual, logical, physical, component and operational) which represent six categories of stakeholders' views on enterprise security. Horizontally, it contains six questions of "what, why, how, who, where and when". Within this matrix, each cell is one enterprise security issue presented as a question. For example conceptual asset cell presents the question of "What is your business attributes profile". This matrix has been widely used to develop solutions for other system architecture, for example, End-to-End Framework for Survivable Next Generation Networks (NGNs) [9] and SABSA cyber security solution [10].

SABSA Lifecycle

SABSA lifecycle covers all layers of the SABSA matrix. It includes Strategy & Concept, Design, Implement and Operations. See Figure 1-5.

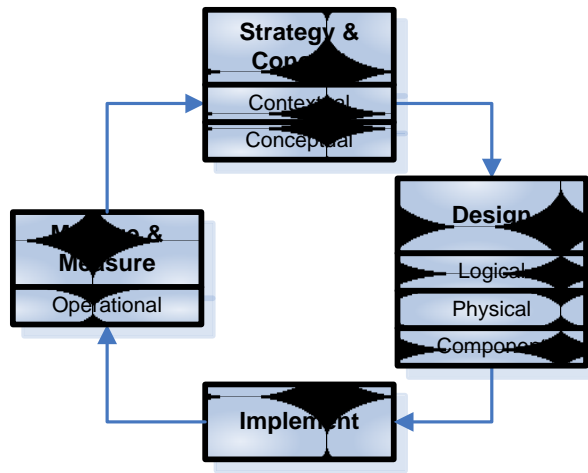


Figure 1- 5 SABSA Lifecycle

SABSA lifecycle is very similar to FSAs development lifecycle. The iterative process includes defining business drives, extracting business requirements, designing business & forensics services, implementing physical forensics features and testing these features.

1.3.2 Forensics Overlay

The overlay is the proposed new forensics model. It builds on top of the SABSA matrix. To build the overlay, not all the SABSA matrix cells are going to be populated; only those that have association with corporate forensics issues. All the issues in these associated cells are addressed and provide meaning in terms of forensics instead of security. For example, in the Contextual Layer Asset cell, the issues needing to be addressed are forensics/business drivers (not security drivers).

The forensics overlay combines the elements from the SABSA Matrix and forensics knowledge. It has the following properties that are inherited from the SABSA methodology:

- **Business Driven Approach:** SABSA methodology originally includes an entire layer to address the business issues such as business drivers, processes, business consideration of time, locations, etc. In terms of our project, the SABSA business considerations are equivalent to requirements from various forensics standards, guidelines, frameworks, methodologies etc.
- **Traceability:** the SABSA matrix originally provides the traceability to an Enterprise security architecture design. As a specific extension of it, the overlay inherits such advantage. The overlay traceability becomes very convenient, not only during the process of application development, but also when the application needs to be tested for usability and service. It also provides a clear view of how an application is designed and implemented according to forensics requirement.
- **Multiple Layered Stakeholder View:** This feature solves the problem of the lack of comprehensive stakeholder consideration during application development. With multiple stakeholders view in terms of forensics process, we are able to develop an application considering the requirements from normal business users, law enforcement, forensics experts, programmers, etc.

1.3.3 Forensically Sound Email Client Development Process

For the increasing forensics challenges, a direct solution is to develop forensics tools that provide high speed hardware and software methods for data acquisition and more efficient data triage functionality in order to find data of interest.

Besides the time and effort invested on forensics tools development, we notice that some applications provide features that might help live forensics investigation. However, the features contained in these applications are not exclusively designed and developed with the intention to help digital investigation. For example, most web service providers use cookies to personalise the customers' access to the website. A cookie contains a user's privacy and important identification which can be used to identify the user. However, the contents in the cookies can be easily changed [11] and therefore they cannot be used for digital investigation purposes.

Furthermore, these features are accessible for both investigators and suspects. That means suspects are able to delete the records in history, cookies and temp folder which leads investigators to rely on forensics tools.

Our research proposes that reliance on forensics tools is not the only solution. The application itself can be developed in a forensics manner by the guidance of the overlay. For example, Web Browsing History, Cookies, and Temporary Internet files can be designed to keep the internet browsing data in a forensics manner and thus the data that has evidential value can only be accessible to forensics investigators.

To test the overlay's ability in developing FSAs, we develop a forensically sound Email client. Email is the most sought-after and sometimes the only electronically stored information requested during digital discovery and it is defined as a business record by Federal rules [12]. During 2005 to 2010, Email has already become a major source of probative information and a forensics challenge [13]. Many corporate email software vendors have slowly added archiving and searching features that help investigators in their digital discovery needs, but most fall short. Current archiving and searching email features are designed without forensic consideration. Even though they appear to be designed to help static-forensics, they cannot provide obvious live forensics help alone since further assistance of forensics tools are still needed.

In our scenario, the email client is built according to the overlay which has its contextual layer focused on business strategy. In this case, business requirements are treated equally important as forensics requirements. Therefore, all forensics features are not randomly designed but follow the intention of the business. A forensically sound email client should at least:

- Generate email evidence on a real time bases, which means major focus on email SENDING events;
- Protect real-time evidence in a forensics manner, which means a clear presentation of the email client activities and protective mechanism for the record of these activities;
- Be role-based, which means ordinary users and forensics investigators should have individual accounts to login to use the email client.

1.3.4 Research Goals

The first part of this research aims to analyse the current forensics landscape and relevant forensics models in order to discover the models' disadvantages. Afterwards, we determine the business requirements for digital evidence and the design of mechanisms to deliver the acceptable evidence for corporate forensics environments and admissible evidence for a court of law. We also study the current forensics knowledge and examine the law enforcement requirements including rules of evidence, current forensics standards and how these requirements are applied to the new forensics model. Furthermore, we intend to combine the determined business requirements and current forensics knowledge with the SABSA matrix to build the forensics overlay.

The overlay provides an overall vision of an enterprise forensics situation and also complies with current forensics standards. It must inherit the properties from SABSA methodology and contain an end-to-end corporate forensics lifecycle. For businesses, the overlay can be use to organise corporate forensics strategy, determine formal corporate forensics requirements, design corporate forensics policies and services, help FSA development and deployment, select third party forensics tools and help handle corporate

forensics situations. For the SABSA matrix, the overlay also creates a new SABSA solution – The Enterprise Forensics Architecture. See Table 1-2.

Architecture Layers	Architecture Views
Conceptual	Enterprise and Law Enforcement's Forensics Objective
Contextual	Business and Forensics Attributes
Design	Business Forensics Policy and Service
Physical	Forensically Sound Applications (FSAs) Development
Component	Third Party Forensics Service Providers (Tool vendors)
Operational	Digital Forensics Investigation Rules and Guidelines

Table 1- 2 Enterprise Forensics Architecture

During the business application design and development, forensics issues are often overlooked. Such oversights in FSA development cause the business to overly rely on third party forensics tools which have difficulties and limitations. As a result of the second part research, we propose that the FSA development should follow the forensics overlay process. With more forensics features in business applications, corporate forensics teams spend less time and effort on extracting data for potential evidence. The evidence generated by the application should provide evidentiary value that complies with requirements from both business and law enforcement. Meanwhile, forensics tool vendors can reduce the workload on design and develop relevant features.

This project argues that the new forensics model (the overlay) helps guide the corporate forensics environment development on an overall level. Meanwhile, current forensics tools are still trusted to evaluate, collect potential evidence and organise forensics reports for computer crimes and incidents.

1.4 Related Work

In the area of design and developed forensics features, McDonald, T. (2008) [75] examines and sets forth principles of operating system (OS) designs that may significantly increase the success of (future) forensic collection efforts and also lay out several OS design attributes that synergistically enhance

forensics activities. Their research, similar to [66] shows the urge for forensics friendly operating systems but not involving forensics friendly mainstream application design.

Guo, Y. and J. Slay (2010) [82] provide a systematic description of the digital forensic discipline that is obtained by mapping its fundamental functions. The function mapping is used to construct a detailed function-oriented validation and verification framework for digital forensic tools. Their research focuses more on one single function – Data recovery for forensic tools, which has more technical focus rather than addressing the unavoidable enterprise/forensics issues.

Both researches inspire our project that the forensics elements are very similar to security elements, which need to be designed with the entire software development process to be functioning. Therefore, our project requires a business-focused model to combine with forensics elements. For this reason, we selected the SABSA matrix.

In the area of using an existing framework to design information technology solutions, the SABSA matrix was used to integrate with Survivable Network Assessment (SNA)/Risk Analysis & Probabilistic Survivability Assessment (RAPSA) and other existing approaches to deliver a coherent methodology for designing next generation networks with a business-driven level of survivability [26], more details are further explained in section 2.4. Our research utilised this previous experience to develop a forensics-related solution for mainstream application development.

1.5 Outline

This chapter includes a discussion of the current forensics environment. It shows that enterprise entity is a major element of digital forensics industry. This chapter proposes a concept of forensically sound application (FSA) development. To apply this concept into physical usage in a business, this chapter outlines two major components of this research: 1) design and develop a forensics overlay to guide and FSA design process; 2) develop an email client according to the overlay's guidance. The following chapters of this thesis are as follows:

Chapter Two introduces the foundational overlay design methodology - SABSA and its core framework - the SABSA matrix.

Chapter Three briefly describes the evolution of cybercrime and digital forensics, along with the historical timeline of forensics standardisation. Chapter 3 also proposes to combine both forensics standards with the SABSA matrix as a blueprint of the forensics overlay.

Chapter Four implements the blueprint from chapter 3 through the process of building a forensics overlay.

Chapter Five recalls the proposed concept of FSA development via further explanation of the business information management in terms of static and live forensics. This chapter then provides an Enterprise Forensics investigation case study and related issues and propose a FSA development with the overlay as a solution.

Chapter Six demonstrates a forensically sound email client design and implementation process with the overlay.

Chapter Seven concludes the thesis and gives an overview of future work in this area.

2 Sherwood Applied Business Security Architecture

To develop the forensics overlay, Sherwood Applied Business Security Architecture (SABSA) is used as the foundational tool. SABSA is a methodology originally designed for developing risk-driven information security architectures for enterprises. It delivers security infrastructure solutions that support critical business initiatives. At the heart of the SABSA methodology is a six layered model, shown in Table 2-2. It is presented as a 6x6 matrix, shown in Table 2-3. The SABSA matrix is a flexible framework that easily adopts and integrates with digital forensics knowledge. There are thirty-six compartments within the SABSA matrix which need to be addressed for corporate digital forensics. By addressing forensics issues in these cells, a forensics overlay is built. Depending on the scope of each cell SABSA provides features to help each addressing approach.

Chapter Two:

2.1 Introduces the SABSA Methodology

2.2 Analyses the Details of the SABSA Model

2.3 Explains the Benefit of SABSA Matrix for Building Forensics Overlay

2.4 Introduces Previous Works of Using the SABSA Matrix

2.5 Briefly Explains the Properties of the forensics Overlay

2.1 What is SABSA?

SABSA is an open standard, comprising a number of frameworks, models, methods and processes [14]. To build the security architecture for a business, SABSA users consider businesses as a system [15]. Therefore, a system approach can be applied to the construction of the enterprise security architecture. It separates a business system into sub-systems in order to simplify the complexity.

In the early stages of SABSA, initial activities were conducted through teamwork such as interviewing the business owner, holding workshops for documenting business requirements, extracting business drivers and peer-reviewing ideas among security experts to determine the SABSA attributes profiles. Through the entire SABSA process, the communication between

teams connects their views from different layers of expertise. The connection within all these layers help design the security mechanism that can trace back to its business driver decided in the early stage.

Using the system approach in security architecture, the SABSA methodology provides four major visions for the SABSA related projects which are 1) Broad strategic objectives, 2) Awareness of Risks, 3) Simplify complexity and 4) Measuring performance against objectives. These four visions are adopted by the forensics overlay.

2.1.1 Broad Strategic Objective

SABSA enhances business perspectives in the early stage of system architecture works. It helps solve a problem that a system architecture work usually begins from a technical perspective, looking at technologies for solutions whilst ignoring the business requirements [17].

In the SABSA model, the contextual layer, conceptual layer and logical layer optimises the business requirements collection of an application development. It also ensures business requirements are aligned with the business strategy.

In forensics overlay, Business/Forensics drivers are abstracted from business/forensics objectives. For instance, in strategic level, the senior executive team may address that the legal department should collect digital evidence in a forensics manner in cases of 1) cyber crimes, 2) highly offensive but not unlawful incidents and 3) breaches of procedure, policy or inappropriate actions. These objectives can be presented in a workshop section to extract business forensics drivers.

The law enforcement's forensics objectives are specified in forensics standards for forensics tools, technologies and methodologies compliance. The most significant objective is that the forensic evidence preservation process must meet certain conceptual, logical, technical, and operational standards. It follows that businesses must comply with these standards for the

evidence accuracy, completeness, authenticity and admissibility [19] and ensures that the business system is at all times compliant with the laws and industry sector regulations and that the system approach directly and indirectly supports legal compliance.

2.1.2 Awareness of Risks

In SABSA, focusing on environmental influences means dealing with external threats and internal vulnerabilities of businesses via risk management. The SABSA matrix contains a column of key activities that guides a top-down process for risk mitigation. These activities include setting risk management objectives, setting risk management policy, setting practical risk management processes and using risk management tools.

In terms of digital forensics for a business, the ultimate goal of a cybercrime investigation varies depending on situations, and can be influenced by business concerns, cost-benefit analysis, due diligence considerations and admissibility in court [20]. After evidential data collection and analysis, the concern of taking further legal action depends on the businesses' decision. As long as the business strategically decides "forensically sound business environment" as part of the business objective, the business should raise the risk awareness when applying "forensically sound" to the business application development. Specifically, during an application development process, the major work of risk management team needs to manage the risks that may hinder the admissibility of the evidence. Any actions that might impact the weight of evidence should be avoided.

In the forensics overlay, the risk mitigation is one of the motivations that forensically sound application is developed to protect evidential data. A risk list should be addressed in the forensics overlay.

2.1.3 Simplify Complexity

SABSA decomposes the business (system) into smaller self-contained sub-systems. This process distributes tasks to various expertises while system

architects can ensure that logically related functions are implemented together. This allows the sub-systems to be tested separately to confirm compliance with its objective. The SABSA matrix breaks down systematic problems by system stakeholders' roles and responsibilities. With each group of stakeholder, the SABSA matrix proposes six questions associated with the typical group of stakeholder's responsibilities. Such structure is presented as a 6x6 table shown in Table 2-3. This structure is later passed onto the SABSA overlay to address the forensics issues.

In terms of creating a forensics overlay based on the SABSA matrix, not all of thirty six cells of the matrix are filled. Ideally, all cells in the SABSA matrix should be able to find equivalences in the digital forensic area. However, without a specified business case, it is irrelevant to address issues such as Business Forensics Application Deployment Timetable, or Business IT Infrastructure. These blank cells are filled when a specific business starts to use the overlay to address forensics issues in its environment.

2.1.4 Measure Performance against Objectives

In the SABSA's top-down approach, business requirements are gathered to extract business drivers which are later mapped with related business attributes. SABSA provides Business Attributes Profile with a column that indicates a Suggested Measurement Approach for each business attributes. See Table 2-1 [16].

Business Attributes	Attribute Explanation	Metric Type	Suggested Measurement approach
Informed	The user should be kept fully informed about services, operating procedure, operational schedules, planner outages, and so on.	Soft	Focus groups or satisfaction surveys

Table 2- 1 Sample Business Attributes Measurement Table [16]

The business is not the only entity to make these measurements. The law enforcement also obliges forensics requirements to businesses. After all, if businesses decided to take legal actions, the law enforcement is the only party to qualify the admissibility and weight of the evidence generated by a forensically sound application.

The overall value of SABSA appears in its business focus, risk management, and built-in SABSA features that simplify system complexity and measure the business performances against business drivers.

2.2 SABSA Model

A SABSA model is a top-down approach that drives the SABSA development process. This process analyses business requirements at the outset, and creates a chain of traceability through the SABSA lifecycle phases of ‘Strategy and Planning’, ‘Design’, ‘Implement’ and ongoing ‘Manage and Measure’, shown in Figure 1-5, to ensure that the business mandate is preserved. The SABSA model is further abstractly presented as the SABSA matrix which is created from practical experience to support the whole methodology [14].

The SABSA model comprises of six layers. Each layer represents the view of different roles in building enterprise security architecture similar to the construction of a building, shown in Table 2-2.

The Business View	Contextual Security Architecture
The Architecture’s View	Conceptual Security Architecture
The Designer ‘s View	Logical Security Architecture
The Builder’s View	Physical Security Architecture
The Tradesman’s View	Component Security Architecture
The Facility Manager’s View	Operational Security Architecture

Table 2- 2 SABSA Model: Stakeholders’ Views [14]

To present the SABSA model in matrix, horizontally, SABSA matrix uses six questions “What, Why, How, Who, Where and When” to analyse six layers in detail, shown in Table 2-3.

	what	why	how	who	where	when
Contextual						
Conceptual						
Logical						
Physical						
Component						
Operational						

Table 2- 3 SABSA Matrix Structure

2.2.1 Contextual Security Architecture

One of the creative concepts of SABSA is to consider business strategy as an enabler for information security. Before an architect starts working, a business owner has to specify the business objectives which are used to extract business drivers. These processes can be done via interview or workshop, where the questions such as “What type of information system is it? Why use it? How? Who uses it and When?” are asked and answered. Understanding the business view helps to build the contextual security architecture. Contextual Security Architecture is a description of the business context in which the secure system must be designed, built and later operated. It not only solves the problem that “Technologists are traditionally not good at listening to the business owners and users”, but also solves the problem that “the business tends to consider information security is a pure technical problem” [16].

In terms of forensics overlay, the contextual layer needs to guide the business decision maker to think forensically. That means the six questions should be asked with forensics considerations. For example: What is the business attempt to achieve by designing forensics features in their information system? Why does the business need that? How does the forensically sound information system benefit the business process? Who (or which department team) are going to ensure the forensically sound business?

Another concern of forensics contextual layer is that businesses and law authorities are both high level stakeholders. Therefore, the business needs to consider forensics regulations and standards on a strategic level. That means in a cybercrime event, the business needs to enhance the ability of evidence collection, preservation, analysis and presentation according to strategic decisions.

In a forensics contextual layer (see details in Chapter 4), technical issues such as the application development are not yet addressed since an application is a part of the business system that is considered on a physical level. However, a business guided by the forensics contextual layer should consider allocating the resources and present clear requirements for a forensically sound system development.

2.2.2 Conceptual Security Architecture

The conceptual security architecture reflects architects' view of the enterprise security. It is where system architects blueprint the overall concept by which the business requirements of the enterprise may be met. It defines from higher level what kind of work needs to be done in the next layers, by engineers with specific expertise.

Similar to contextual security architecture, there are six questions applied to define: What need to be done according to the SABSA provided Business Attributes Profile (What); Provide the control objectives as the motivation for security (Why); Provide the major security strategies (How); Security entities and their trust relationship (Who); Where is the security domain and time dependence of security (When).

The key feature in contextual layer is the Taxonomy of Standard Business Attributes (SBAs), shown in Figure 2-1.

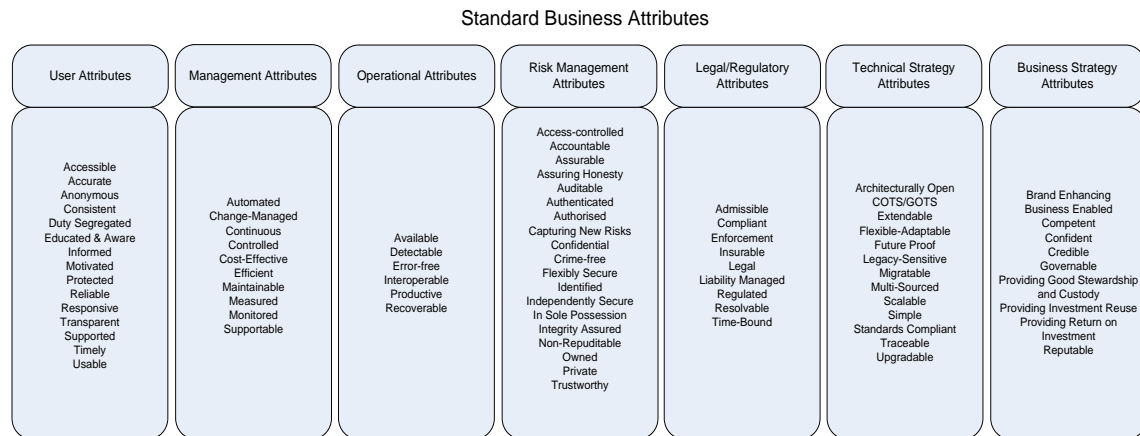


Figure 2- 1 SABSA Standard Business Attributes (SBAs)

The SBAs are the common types of high level business drivers and are seen again and again in different organisations, even in different industrial sectors. The Taxonomy is extensive which means it is encouraged to add and define new business attributes according to the specific business requirements such as corporate forensics requirements [14].

To create conceptual architecture for the forensics overlay, the most important task is to create forensics relevant Business Attributes Profile. The task involves selecting forensics relevant attributes from SBAs and adding new attributes when necessary. The relative supporting information such as suggested measurement approaches mapping to business attributes are documented during the process.

The process is conducted by the workshops to decide which attributes are relevant to business/forensics requirements. According to business/forensics requirements that are defined in the contextual layer, some of the selected attributes need to be redefined to serve a forensics purpose. The following processes abstract the forensics attributes:

- Extract Business/Forensics Drivers from collected Business/Forensics requirements;
- Select or add new forensics attributes from Standard Business Attributes according to Business/Forensics Drivers;

- Define selected or newly added attributes forensically.

Finishing the above processes helps narrow down the business attribute profile into a forensics specified attribute profile. This provides an abstract view of business/forensics requirements and can be traced back to contextual layer to map the addressed business/forensics requirements.

2.2.3 Logical Security Architecture

In the SABSA model, logical security architecture reflects the designer's view of the business in terms of a secure system. In this layer, the business information that requires protection is logically presented in form of a business policy and service. High-level security policies and logical domain policies are specified in order to guide the logical security service. The logical security service category provides a picture of overall sub-security systems in a logical level. Later on, the logical security service guides physical security architects to specify the security mechanism in physical architecture. For example, if the designers list Integrity Protection as one of the logical security services, then it should have a related security mechanism such as digital signature in the physical layer.

In the overlay, the information collected from the forensics contextual and conceptual layer helps define what "business information (NOT Business Data)" need to be protected in a forensics manner during the usage of typical applications. Relevant policies are created accordingly from both business and forensics perspectives to protect the information. Also, forensics services that need to be built into business applications are defined in this layer. For example, this layer may establish a typical business policy to protect Email information exchanged between business email client user and outside of the business. According to such a policy, the next layer defines Email data, and guides the email client development.

2.2.4 Physical Security Architecture

The physical security architecture has a strong technical focus; because this is the layer that a system builder chooses and assembles the physical elements that make the logical design come to life. Tracing back to the logical security architecture, logical security services are delivered in physical forms. Different from the logical security architecture that focus on “information”, the asset that needs to be protected in physical architecture is “data”. Developers (Builders) specify the business data model and the security related data structure (tables, messages, pointers, certificates, signatures, etc.).

In terms of the forensics overlay, the evidential data in different sub-system requires protection. The business should have a set of practical rules for each sub-system to protect the potential digital evidence. Practical rules to protect data are derived from the forensics policy that has been decided in the previous layer. Also, forensically sound applications should be developed according to forensics services that have been decided in the previous layer. Such tractability, shown in Figure 2-2, between layers can be seen often in the forensics overlay.

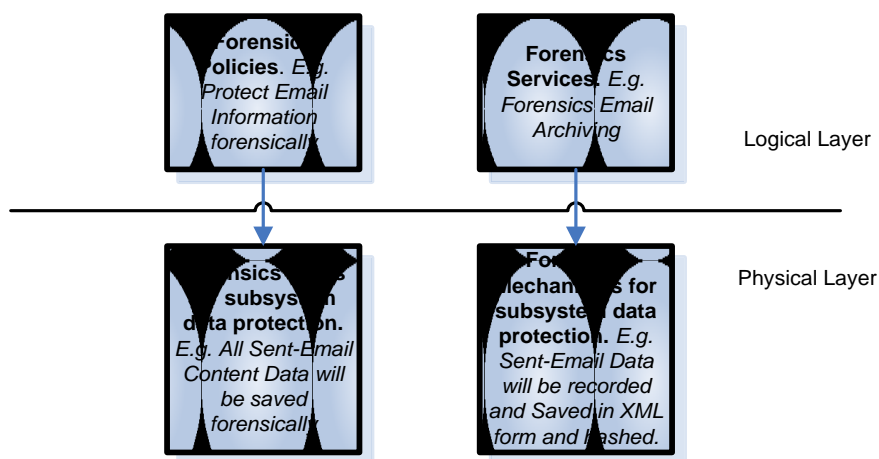


Figure 2- 2 Traceability Sample between Logical and Physical Layer

In the forensics physical layer, digital evidence integrity protection is highly prioritised since forensics overlay considers all data as potential evidence and requires protective mechanisms (e.g. Hash). Therefore, the forensics physical layer needs to be applied in an application development in order to generate the forensics mechanism.

Another concern about the forensics physical layer is that a forensically sound application usually has two contrast user (USERS) groups: offenders (OFs) who misuse the application intentionally or unintentionally; and forensics investigators (FIs) who investigate misuse cases by utilising the built-in forensics features, shown in Figure 2-3. Therefore, designing and developing authentication mechanisms are used to distinguish these different roles and are critical since forensics features require exclusive access only by FIs.

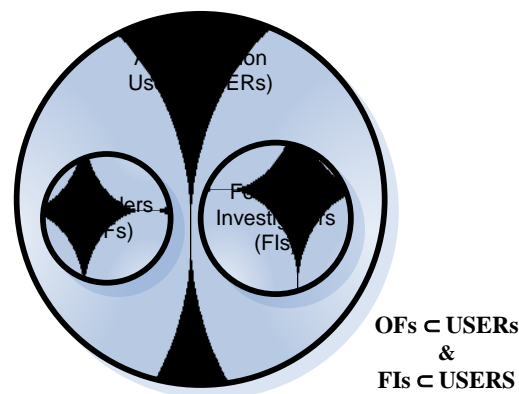


Figure 2- 3 Forensically Sound Application Users

2.2.5 Component Security Architecture

The component layer focuses on third party software and hardware tools, business partners, etc. In the concept of forensically sound software development, we attempt to reduce the overreliance of forensics tools. Therefore, we have no specific requirements on this layer.

2.2.6 Operational Security Architecture

The operational layer reflects facility-manager's view, which focuses on maintaining the security of business systems in an operational level. The operational layer further addresses the issues of using business applications according to the security policies that relate to confidentiality, integrity, availability, auditability and accountability. In terms of security, this layer involves the proper usage of security products to protect the daily business.

In terms of forensics overlay, the operational layer addresses the proper usage of forensically sound applications rather than forensics tools. Ideally, the forensically sound application has features that are sufficient for a forensics investigation. Therefore, in an operational level, the issue needed to be addressed is a chain of custody, which focuses on evidence preservation in operational level.

2.3 Why Use SABSA?

Two major reasons that SABSA overcomes other current forensics models are 1) comprehensive view on entire business/forensics environment rather than the narrow focus on Technical and Operational perspectives; 2) SABSA has an interface (contextual layer) to absorb the business requirements in the first place rather than provides "checklist liken" one for all solution.

2.3.1 Other Forensics Models

A complex cyber-forensics project requires the expertise go beyond pure technical perspective, most of current forensics models still focus on providing technical and operational solutions.

Models that Focus on Technical Forensics

Using a technical forensics model in an enterprise environment usually leads to overreliance on both vendor-based forensics tools and assistance from external forensics technical support. The tools and external supports are critical on one hand. They are insufficient in the current enterprise forensics situations, especially in case of a network/enterprise environment where the life forensics, real time monitoring and evidence collecting are needed.

Windows Vista Forensics Framework [20] is created to take advantage of new vista forensics features such as “Bitlocker, Encrypting File system (EFS), Backup and Restore” to extract data that have potential evidence value in windows vista system. The framework is more like a technical guide for forensics experts who deal with a single PC installed with the Vista system. The research successfully explained the challenges of new (year of 2008) vista system to computer forensics investigators and provided a practical solution for them.

However, the framework focuses on utilising the existing Vista features but neglects the consideration of: How these vista forensics features are high level designed to be efficient to assist the forensics process; what the forensics and business requirements are used in designing such features; How these forensics and business requirements are integrated into a software development process. Similar issues found in the researches of Mac OS X operating system forensics [21]; Windows physical memory forensics method [22] and physical memory forensics framework [23].

Models that Focus on Operational Forensics

Other researches focus on operational digital forensics perspective which is the process of Identification - Acquisition - Preservation - Examination - Analysis - Reporting lifecycle [25]. Some forensics models focus on one phase of forensics lifecycle. Such models neglect the fact that the forensics lifecycle is part of the enterprise digital investigation lifecycle. Using such models in an enterprise digital investigation, business related phases need to be added to ensure the business procedure. Sean, P., B. Matt, et al. (2007) [24] presented an overview of a forensics model for an evidence analysis phase. Even though this research attempted to reduce the focuses on technical aspects (avoid issues from technical models), it merely provides the policies and procedures during a formal forensics operation. These policies may ignore the high level business objectives and lower level business system requirements.

Another issue with operational models is that they may be out of date for current enterprise environments. The common features of forensics operation models are based on conventional forensics lifecycle which has been unchanged for decades. However, the landscape of a forensics lifecycle has begun to change, especially under the circumstance of cyber warfare and cloud computing.

2.3.2 Advantages of SABSA Model

In this section, we introduce advantages of the SABSA model. These advantages are managed to pass onto the forensics overlay, which makes the forensics overlay a new model that outgoes the previous deficiencies.

Firstly, the SABSA model provides a comprehensive view of the forensics issues. It contains six layers which represent various stakeholders' view of the system. This overcomes the problem that current forensics models have narrow focus on technical or operational issues and lack of strategically design of a forensic solution. Hence, using forensics overlay in a business helps integrate all business department efforts to devote into any forensics projects such as conducting forensics investigations, developing forensics tools, developing forensically sound software, developing business forensics plans, etc.

Secondly, recent forensics models are static, which means these models only provide informative guidance for forensics activities. These models simply organise forensics regulations and present them in form of charts, field guide, policy, checklist, cheat sheet, etc. Such phenomena results in a typical mistake that in many companies, a large portion of the forensics budget is allocated to compliance testing for industrial standards. In this case, the senior executives only assign the compliance department to deal with the seasonal compliance examination rather than be part of the business forensics strategy decision making.

The SABSA model on the other hand, has a lifecycle, which means there is an interface to intake the users' requirements, and be able to produce and measure the outcome of the physical solution, shown in Figure 2-3. In this case, the senior executives are able to enhance the influence via the input of high level requirements. This ensures the forensics/business requirements are from both regulation authorities and businesses.

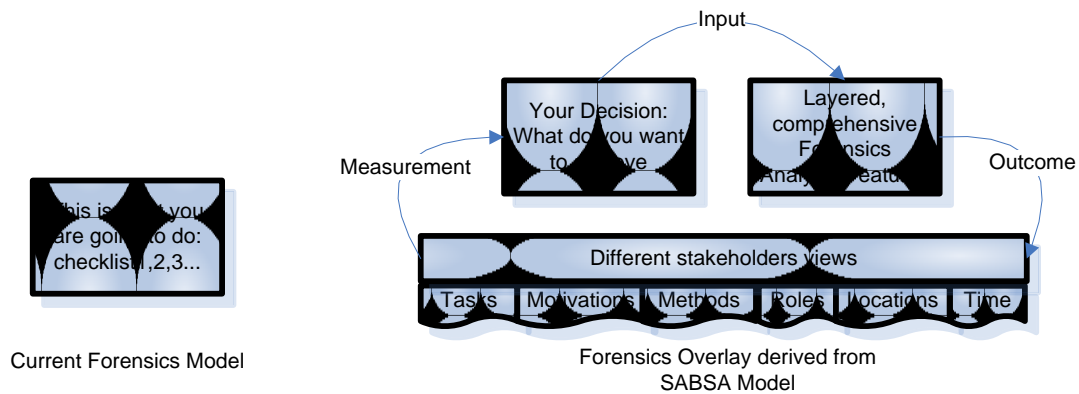


Figure 2- 4 Differences between Current Forensics Model and SABSA Model

Thirdly, due to the traceability between six layers, layers are not isolated from each other so that different system development roles work as a team. The SABSA traceability shows a clear development track that starts with high level business requirements and ends with the technical solutions. There are more details in Chapter 6 about how the SABSA traceability helps develop each forensics mechanism for an email client.

Fourthly, SABSA has existing features to help forensically address each cell. For example, in conceptual asset cell, forensics architects should create a set of forensics attributes that are extracted from forensics standards. It is not practical since attributes are highly conceptual concentrated terms. However, SABSA conveniently provides Standard Business Attributes. The forensics architects only need to select and define attributes in a forensics sense. Table 2-4 indicated how differently the SABSA Model and Forensics Overlay defined the attribute of "Informed".

SABSA Defined “Informed” [17]	Forensics Overlay defined “Informed”
The user should be kept fully informed about service, operating procedures, operational schedules, planned outage, and so on.	Forensics procedure briefing information should be documented, or DEFR should be informed to do so.

Table 2- 4 Business and Forensics Definition of the Term “Inform”

2.4 Previous Work

SABSA provides an ideal framework for integrating many traditional standards and processes from various aspects. SABSA was used to incorporate with Survivable Network Assessment (SNA)/Risk Analysis & Probabilistic Survivability Assessment (RAPSA) and other existing approaches to deliver a coherent methodology for designing next generation networks with a business-driven level of survivability [26]. Figure 2-4 shows the process to create a SABSA survivability overlay. The overlay takes the form of an additional set of activities in a number of the SABSA matrix cells, which when populated can be added to the standard SABSA assessment to provide a complementary survivability view of the enterprise’s essential services.

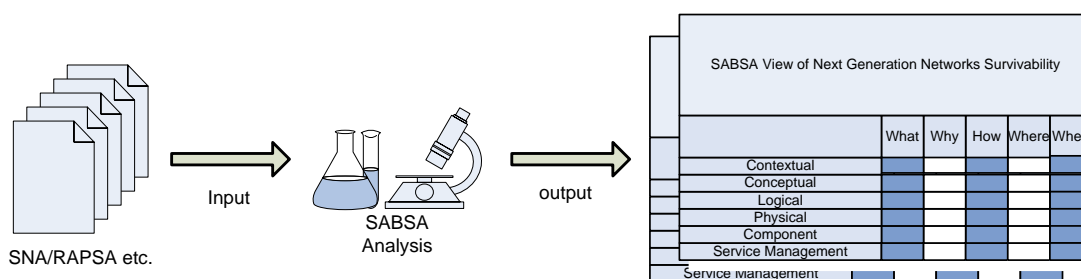


Figure 2- 5 SNA/RAPSA Integrated with SABSA Framework

In our project forensics knowledge and business forensics requirements are incorporated into the SABSA framework to deliver a forensics overlay, shown in Figure 2-5.

The Computer Forensics process requires a higher level of expertises beyond IT personals capabilities and knowledge. Improper and lack of IT staff training with formalised computer forensics methodologies may cause artefacts of potential evidentiary value to lose their overall admissibility in court or, worse yet, evidence may be destroyed altogether. In figure 2-6, forensics knowledge is one important input. SABSA is the foundation framework or analysis method. A SABSA forensics overlay is the outcome.

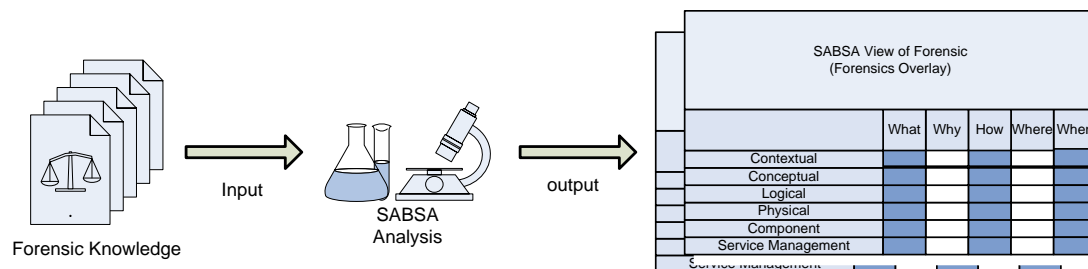


Figure 2- 6 Forensics Element Integrated with SABSA Framework

2.5 A New Model – The Forensics Overlay Based on SABSA

To sum up, increasing digital forensics activities are moving into a network/enterprise environment and existing in forms of the network and systems baseline monitoring, logs analysing, hidden and/or inappropriate files scanning, password auditing, malware investigation, incident response and forensic toolkits creating, key loggers installing/configuring and Law enforcement liaison [27]. The current models that deal with typical system data acquisitions, forensics tools and forensics operations are not comprehensive enough for current environments. A new model is needed to deal with forensics issues from the business perspective. The link between “operational, technical forensics factors” and “corporate infrastructure, enterprise content” needs to be addressed in this model. On the other hand, legal factors that represent the law enforcement’s requirements also need to be integrated into this new model. This is further explained in Chapter 3.

SABSA deals with enterprise security issues from contextual, conceptual, logical, technical and operational perspectives. Based on SABSA, the overlay should cover forensics issues in all these perspectives. Additionally, the legal considerations are needed in the overall forensics overlay, shown in Figure 2-7. These legal considerations are the forensics standards, legal precedents, laws and regulations that can be used to extract law enforcement's requirements which are explained in chapter 3.

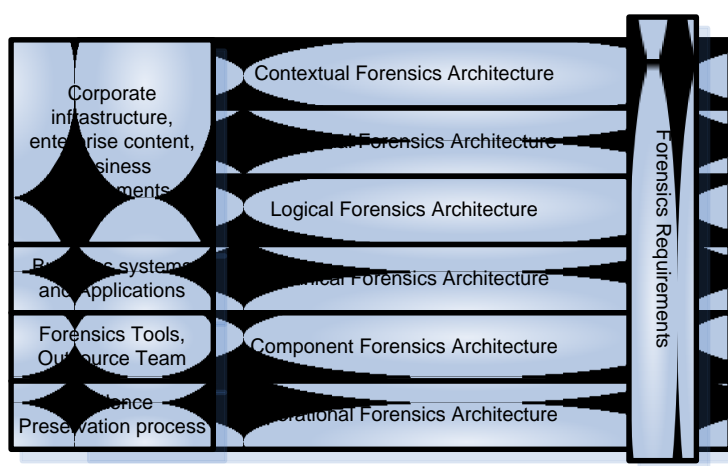


Figure 2- 7 Forensics Overlay for Enterprise Forensics Program/Project Development

For a business that plans to establish the digital forensics capability, the overlay can be used to:

- Identify the digital investigative capability requirements which include forensics goals, costs, resources, timelines, and outsources.
- Provide digital investigative capability administrative considerations, which include forensics policies and forensics investigation procedures.
- Allocate resources such as forensics tools, external teams that suit the business forensics environment.
- Guide the internal business system or application development in forensics manner.

2.5.1 Differences between the Forensics Overlay and the SABSA Matrix

On one hand the overlay is created to solve forensics issues in a corporate environment. On the other hand, the overlay is a superstructure of the SABSA matrix. In sections 2.3.2, the overlay has been introduced as it has the same properties as the SABSA model. However, they have differences in terms of scope, function, content, etc.

Firstly, the forensics overlay is a “size down” version of the SABSA model. The structure of the overlay is similar to but derived from the SABSA model. Not all cells in the SABSA model are filled to create the overlay and with the filled cell, it only addresses forensics issues.

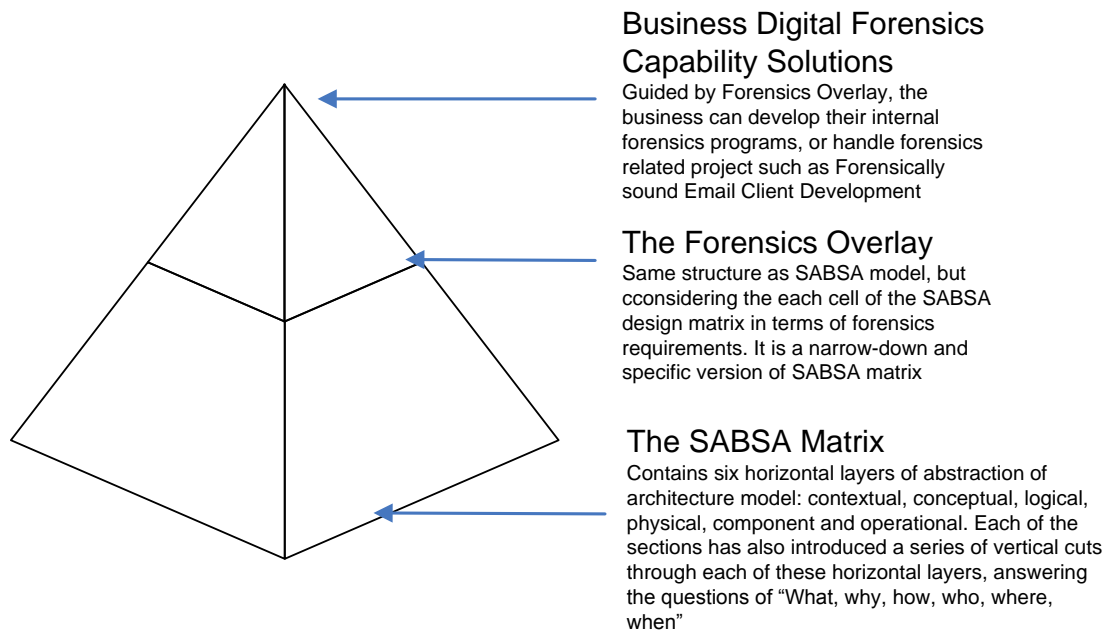


Figure 2- 8 Differences between the Forensics Overlay and the SABSA Matrix

Secondly, considering the function, the SABSA matrix deals with enterprise security issues while the overlay deals with enterprise forensics issues. The further research shows that the SABSA security model has slightly overlapped the forensics issues especially in legal part. This overlap can be observed from Taxonomy of Standard Business Attributes (SBAs) (Figure 2-1). The fifth

column of SBAs shows a category of Legal/Regulatory Attributes which already contains some forensics attributes.

Thirdly, considering the knowledge background, the contents in the overlay are extracted from forensics knowledge such as standards, legal precedents, rules of evidences, etc. The SABSA matrix is based on enterprise security knowledge. In the SABSA model, the 36 cells are all addressed with security concerns, while in overlay, some of the cells are left blank since addressing this cell may confuse the users and affect overlay's forensics emphasis.

3 Forensics Industry Evolution and Forensics Knowledge

In chapter one, issues found in current forensics models were analysed and proposed to build a forensics overlay where the “corporate infrastructure & enterprise content” is addressed. At the end of chapter one, we proposed that forensics requirements should be integrated in all layers of the overlay, shown in Figure 2-7. Forensics requirements are extracted from current forensics knowledge, mostly from forensics standards. In this chapter, we describe the evolution of cybercrime, digital forensics and how forensics knowledge is standardised during the digital forensics professionalisation. Furthermore, we explain how the current digital forensics crisis affects our extraction of forensics requirements from current forensics standards. At the end of Chapter 3, we review chapter one and two and provide a blueprint to construct the forensics overlay.

Chapter Three:

3.1 Explains the Evolution of Cybercrime and Digital Forensics

3.2 Introduces Forensics Knowledge

3.3 Introduces the Selected Forensics Standards

3.4 Sumarises the Knowledge Structure of the Forensics Overlay

3.1 Evolution of Cybercrime and Digital Forensics Investigation

The term “cybercrime” has only been used in recent years. This chapter refers to computer, system and network related crimes since the earliest cyber age. The term “digital forensics” has been mentioned for the last ten years. According to many researchers, digital forensics has been through the early days, the golden age, and the crisis time. This section explains how cybercrime and the digital forensics industry evolved with “spring up” technologies in different ages. In understanding the evolution, we explain how forensics knowledge is developed and standardised. Furthermore, study of the digital forensics crisis points out “forensics standards” as the primary component among the overall forensics knowledge.

3.1.1 The Early Days

The first hacking activities can be dated back to early 1960s when programming enthusiasts group at the Massachusetts Institute of Technology (MIT) programmed for the sheer joy of their first system – Program Data Processor (PDP) One [28]. Even though the term “hacker” is being intermingled with the term “cyber criminals” by public, in the digital world, the term “hacker” is defined as “A person who delights in having an intimate understanding of the internal workings of a system, computers and computer networks in particular” [29]. In early ages, a cybercrime that harms individuals was impossible because there was no personal computer. The mainframes were owned by cooperates or the government. There were no major arrests of cyber criminals around the 1960s, except a few cases of embezzlement, inflating company earnings, stealing trade secrets, misappropriating company data [30].

In the late 1960s and early 1970s, major cybercrimes are associated with breaking into the telecommunication system and take advantage of it, for example, “hack” and making long distance calls without the payment. The term “Phreaker” is used to describe a cyber criminal who conducts such activity. There were a few arrests during this period. John Draper designed the original blue box which could produce the 2600 Hz signal that granted access to AT&T’s long distance services. He was arrested and served time in a California minimum security prison for this infraction [28].

The 1970s is considered as the beginning of the computer era. The cyber technology had some breakthroughs such as the emergence of first affordable personal computer, early computer network, popularity of bulletin board system (BBS), etc. During this decade, illegal cyber activities started with using BBS to upload illegal material or harassed other users; however, these infractions are rarely thwarted by law enforcement but by BBS system administrators [28]. In the late 1970s, the term “hacker” was intermingled with the term “cracker” by the public and since then crackers have been using digital tools to take advantage of other computer users.

In the 1980s, the worldwide network was steadily growing. By 1989, all sources agreed that there were more than 100,000 hosts on the network. In the 1980s, the FBI made some of the first high-profile arrests of computer crackers [28].

The 1980s is referred as early stage of cybercrime and digital forensics (neither terms had been used in this stage). During this time, there was limited needs of digital forensics and few cases required analysis of digital media because there were less volume of digital media for the potential digital evidence, cybercrime investigators could find more evidence from other media such as printouts.

The 1960s to end of 1980s is the early days of cybercrime and digital forensics. Pollitt, M. (2010) referred these early days as “The Pre-history” of digital forensics [30], which means it was the least documented time in the digital forensics history. Garfinkel, S. L. (2010) marked this period by its poor documentation, heavily reliance on time-sharing and centralised computing facilities, rarely was there significant storage in the home of either users or perpetrators that required analysis and the absence of formal process, tools, and training [31]. There were no actual forensics standards. Since the early forensics professionals were mostly from law enforcement, they would work or be trained in cooperation with systems administrators [30]. Their knowledge was mostly based on the computer systems of that time.

3.1.2 The Golden Age

In the 1990s, the emergence of new technologies such as broadband Internet connectivity, wireless network, sophisticated web and email techniques, mobile computing, e-commerce and online banking, new operating system and new applications have created new vulnerabilities for crackers. On the other hand, the commercialisation of the Internet enhanced the popularity of these technologies as well as various online services. It follows that the scope of cybercrime is extended. Cybercrime evolved into two categories, shown in Figure 3-1. Firstly, crimes that must be committed through computers or

network system such as malicious code, system backdoor and network intrusion. Secondly, crimes that only finds computer as a convenient tool such as enterprise frauds, scams, and white-collar crimes.

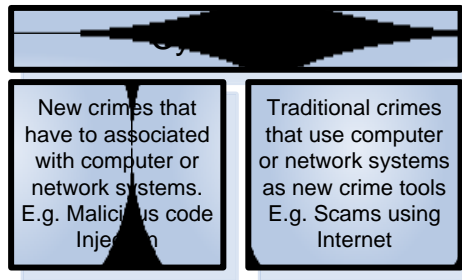


Figure 3- 1 Cybercrime Categories

Garfinkel, S. L. (2010) believes that from 1999 to 2007 is the digital forensics golden age [31]. With both categories of cybercrimes (Figure 3-1) emerging in business environments, businesses started to notice the importance of digital forensics. Forensics investigators steadily appeared in both business and law enforcement groups. Their duties in this time focused on recovering data from all sorts of digital media in a stand-alone computer, analysing aquired data, and presenting analysis results as potential evidence to the court of law if further legal actions were pursuit.

Fostered by technological developments and urged by increasing cybercrimes, the digital forensics industry accelerated its standardisation and professionalisation. The forensics golden age was characterised by the widespread use of Microsoft Windows, and specifically Windows XP; relatively few file formats of forensic interest - mostly Microsoft Office for documents, JPEG for digital photographs and AVI and WMV for video; examinations largely confined to a single computer system belonging to the subject of the investigation; storage devices equipped with standard interfaces (IDE/ ATA), attached using removable cables and connectors, and secured with removable screws; multiple vendors selling tools that were reasonably good at recovering allocated and deleted files; and a rapid growth in digital forensics research [31].

Professionalisation and Standardisation

In the “golden age”, the digital forensics industries were steadily formed due to the increasing need of tools, models and knowledge collected from digital forensics researches. The digital forensics professionalisation had adopted a “routine procedure” for investigators to conduct the forensics investigation. From time to time, this “routine procedure” has been applied and developed by investigators, verified by law enforcement, studied and analysed by forensics researchers.

These sets of routines are referred as the conventional forensics investigation lifecycle (CFL). Practically all forensics standards or studies in that time followed the CFL or phase(s) of CFL, shown in Table 3-2. The key components of CFL in order are: Identification, Preparation, Approach Strategy, Preservation, Acquisition, Examination, Analysis, Presentation and Returning Evidence [32], shown in Figure 3-2.

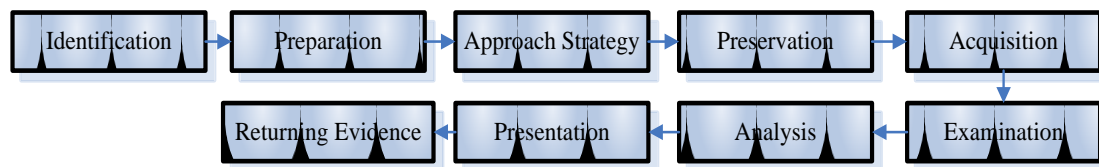


Figure 3- 2 Conventional Forensics Lifecycle

The CFL are based on the procedure of static forensics (data recovery from static data storages), lessons from legal precedents and Forensics Studies and Researches. To perform each stage in CFL, the forensics industry developed diverse forensics standards, the development approaches are introduced in [62]. These standards collect forensics requirements in technical, operational and legal perspectives, shown in Figure 3-3. These standards are created via formal and authorised organisation such as National Institute of Standards and Technology (NIST).

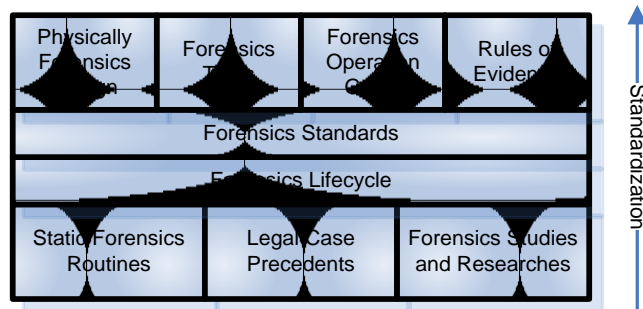


Figure 3- 3 Digital Forensics Standardisation

These standards are widely adopted by businesses that are willing to comply with the lawful regulations. For example, some businesses are required to have an adequate auditing process to ensure the compliance with forensics standards. Therefore, forensics standards are the most dominant in the industry among all categories of forensics knowledge.

In recent years forensics standards has not been able to keep up with the proliferating new technologies and cybercrimes since operational and technical standards are easily challenged and are forced to make alterations for many cases. On the other hand, legal forensics standards appear more immutable than technological and operational standards. It follows that legal elements such as “lessons from legal precedent, rules of evidence, rules of forensics operation, and chain of custody etc” are focused more in many researches. Our research focuses on determining the business and legal requirements from forensics standards, for collecting evidence and designing mechanisms to collect evidence.

3.1.3 The Current Crisis of Digital Forensics

In recent years, digital forensics has faced a crisis due to several emerging technologies. The challenges are from four areas 1) technologies forming a complex business environment in which potential evidence are more fragile and hard to collect and preserve; 2) adopting diverse technologies could mean accept more system vulnerability and business risk; 3) adopting diverse technologies makes it challenging to unify and standardise forensics activities and 4) new techniques also nourish the cybercrime incidence, details are explained with the following examples.

Digital Storage Related Technologies

The increasing data storage makes it impractical for investigators to perform a bit-by-bit copy of the entire data storage unit. The diversity of data storage (flash drivers, solid state drives, RAMs in all computer components) and data storage interface standards hinder the usage of one standardised forensics tool. Furthermore, the increasing data security awareness leads to the usage of data encryption. In addition, forensics activities are constrained since data privacy is protected by laws and regulations.

Pervasive Networks

The forensics target is not a stand-alone computer but a complex system that require analysis of multiple targets which may not geographically reside in one location. Cybercrimes are conducted with more complex tools; larger geographic domain; involve more data, etc. Moreover, virtualisation technology and cloud computing concepts are facilitated by pervasive networks, which lead user data to move to remote and discontinuous storage.

New forms of cybercrimes emerged in terms of hacktivism, cyber terrorism, cyber warfare, etc. The increasing diversity of cybercrimes raise more challenges to forensics investigation. Therefore, forensics industries require new strategy, methodology and tool for this rapid turnaround.

Diverse Operating System

The proliferation of diverse operating systems (OS) makes it challenging to unify and standardise forensics activities for investigating computers and other devices. For example, when the forensics targets OS is no longer as familiar as Windows, the digital investigator has to use different tools, procedures, and standards to deal with new OS. The aim of the investigator is to answer the questions of “What incriminating information is present in the system?” and “How did the incriminating information get there?” The answers depend in all cases on how the information of interest is stored by the operating system (i.e. the internal structure), and the analysis tools the operating system provides (i.e. the functionality) [66]. However, with different OSs, the answers are varied.

In some other cases, forensics operations have no standards to follow. For example, the proliferation of mobile operating system results in forensics investigators seeking to conduct mobile forensics under a common standard, which however, have not yet been formed. According to the NIST Guidelines on Cell Phone Forensics, when confronting a cell phone that is password-protected, forensics investigators are recommended to search Internet sites for developers, hackers, and security exploit information [31].

Over-Anticipation of Forensics Tool Development

Most forensics researchers believe a straightforward solution is to create a new operational model and develop more sophisticated forensics software. In 2006, Golden G. Richard, I. and V. Roussev (2006) foresaw the crisis and suggested that the “smart acquisition tool” should be able to cope with the larger storage problem by using built-in data reduction features to select the interesting data [33]. Garfinkel, S. L. (2010) suggested the new research direction for future forensics is to unify the forensics data image format as well as standardised the architecture for forensics software development, create alternative analysis models for data abstraction, etc. He concludes that the only solution to solve the storage volume problem is to “create more powerful abstractions that allows for the easier manipulation of data and the composition of forensics processing elements” [31].

Forensics tool vendors also foresaw this crisis and endeavoured to improve the quality of the tools based on the industrial requirements. For instance, EnCase has EnCase Enterprise (EE) and Field Intelligence Model (FIM) live investigation functions for a network/enterprise environment, because they believe “as live forensics becomes more necessary and mainstream, their value are increasingly accepted by the industry and the judiciary” [35].

However, given that “Smart and powerful acquisition tools” is a direct solution, the feasibility of such solution is still uncertain. Garfinkel, S. L. (2010) pointed out that the current dominant forensics tool vendors are relatively small but facing extraordinarily high research and development costs. Product lifetimes are short because new developments in the marketplace must be tracked and integrated into tools, or else the tools become rapidly obsolete. A few commercial players heroically struggle to keep their products up-to-date, but their coverage of the digital systems in use today is necessarily incomplete [31].

The dynamic status of the overall forensics environment (dynamic forensics targets, tools, procedure, etc) leads researchers to look for immutable (or less dynamic) elements from the current forensics knowledge.

3.2 Forensics Knowledge

Forensics knowledge was well developed and standardised in the golden age. Meanwhile, the digital forensics industry developed via the compliance with standardised forensics knowledge. Forensics knowledge is a collection of laws, industrial standards, current forensics literatures, lessons from legal cases, etc. Current forensics knowledge guides the industry in four major areas.

Firstly, in the operational area, forensics knowledge guides forensics experts to strictly follow the proper procedure of collecting digital data and presenting the data to court as evidence. For example it is the standard that forensics investigators shut down a stand-alone PC accordingly in a “pulling power cable” forensics manner rather than shut down a machine in the regular way.

Secondly, in the technical area, forensics knowledge guides the development of forensics tools. The features in forensics tools are designed and developed in a forensics manner. For example, a forensics tool must provide the data acquisition function through a bit-by-bit copying feature rather than regular copying. In this case, forensics knowledge is the software development requirement.

Thirdly, in the business area, forensics knowledge is organised as a field guide, regulation, policy, etc. These guidelines help businesses obtain and maintain current digital forensics capabilities.

Fourthly, in the legal area, forensics knowledge is integrated with current laws and regulations. In this case, the forensics knowledge includes lessons from legal precedent, rules of evidence, rules of forensics operations, chain of custody, etc.

Our study analyses these four areas in the forensics knowledge. As a result, the operational and technical areas of forensics knowledge are more vulnerable to dynamic technologies, shown in Table 3-1. That explains the constant need of updating current forensics tools. With this endless cycle of such escalation, it is challenging for authorised organisations to standardise the forensics knowledge. Therefore, forensics knowledge in technical and operational areas “does not guarantee the legal admissibility of electronic records – it is a statement of best practice... organisations are encouraged to seek both legal and other expert advices...” [29].

Forensics Knowledge	Forensics Challenges
Operational area	increase of data media volume, the diversity of data storage, the proliferation of operating system, cloud computing
Technical area	increase of data media volume, the diversity of data storage, the proliferation of operating system, encryption, cloud computing, complexity of tool development
Business area	cloud computing
Legal area	cloud computing

Table 3- 1 Forensics Knowledge and Forensic Challenges

On the other hand, the forensics knowledge in the business and legal area tend to stay immutable. Especially in legal area, the standardised rules of evidence are more dominated than other standards. For example, when email data are collected from different email clients, the data formats are different. However, the legal requirements for digital evidence are still Admissible, Authentic, Complete, Reliable and Believable. It concludes that when integrating the standards to the SABSA matrix to build the overlay, the legal and business forensics standards (especially rules of evidence) need to be focused, details of forensics standard selection is further explained in next section.

3.3 Selection of Forensics Standards

To create the forensics overlay, the SABSA matrix helps to address the link between “operational, technical forensics factors” and “corporate infrastructure, enterprise content”, while forensics standards help address the legal rules.

To extract the legal rules of forensics, a group of forensics standards, shown in Table 3-2, is selected across six organisations (NIJ, NIST, ACPO, IOCE, ISO and Australia Standards) and three countries (the States, Germany and Australia). Those standards were created from 2001 to 2010. Studying these

standards helps us to spot the rules of evidence that have steadily existed for the past decade.

Learnings from Forensics Standards

Firstly, we learn about the general forensics environment of a typical year when the forensics standard was created. For example, *Electronic Crime Scene Investigation: A guide for First Responders 1st Edition*, shows that in year 2001, computers are not frequently used to conduct crime as nowadays and also less evidence can be found within the storage due to the limited size.

Secondly, analysing forensics standards across 20 years helps to understand the development trend of the forensics industry. Initially, computer forensics are cases based on which investigators only randomly collected whatever helps to solve the case on hand. Later on, legal requirements appeared and urged the updates of forensics technique such as bit-by-bit copy. Meanwhile, the increasing digital crime cases cause the rapid forensics tool development.

Thirdly, we compare different emphasis of each standard to understand what has been changed during the past decade. The common focus of the forensics industry remains on sophisticated designed forensics tools and legal rules of evidence.

Fourthly, analysis of recent standards, we found a new trend of using built-in forensics features in daily applications to solve investigation issues. Also, new digital investigation methods such as live inspections and first responds appear in the business area.

Most importantly, the study shows that forensics standards in technical and operational areas are constantly altered. On the other hand, forensics standards in the legal area have the least alteration during the industry evolution. The legal elements contain the rules of evidence and chain of custody which have strong connection to the term “forensically sound”.

Integrate “Forensically Sound” into SABSA Matrix

Referring to the definition in chapter one, the term “forensically sound” means the application of a transparent digital forensic process that preserves the original meaning of the data for production in a court of law. The “transparent digital forensic process” is ensured by the “chain of custody”. The “original meaning of the data” is ensured by the application of the collective rules of evidence.

Therefore, to build the forensics overlay, the two most important forensics requirements that need to be integrated to the SABSA matrix are: 1) the rule of evidence, which are the rules that qualify the evidential data to be present in the court of law and 2) Chain of custody.

Name of the Standards	Publisher	Year	Major Focus							Description/Conclusion
			Collected Devices	Forensics Tools	Evidence Weight (Legal)	Crime Category	Forensics Operational Process	Digital Investigation Background	Forensics Features in Application	
Electronic Crime Scene Investigation: A guide for First Responders 1 st Edition [48]	U.S. Department of Justice; Office of Justice Programs; National Institute of Justice	2001	Devices basis investigation	General tool kits, not including forensics software	General rules of evidence collected for digital or non digital crime	General crimes such as Death Investigation, not specifically related to cybercrime.	Normal evident collection, no special operational digital collection rules			Less cybercrimes in early day, digital evidence is merely considered as a part of entire collection of evidence, no specific rules are required such as bit-by-bit copy
Guidelines for Best Practice in the Forensics Examination of Digital Technology [49]	International Organisation on Computer Evidence (IOCE)	2002			General principles applying to recover, and examining evidence		Compliant rules for managing evidence collection	Major focus on quality assurance, auditing		Provides a framework of standards, quality principles and approaches for the detection, preservation, recovery, examination; uses digital evidence for forensic purposes in compliance with the requirements of an accrediting body and or an organisation widely recognised in the digital forensic community.
Forensic Examination of Digital Evidence: A Guide for Law Enforcement [50]	U.S. Department of Justice; Office of Justice Programs; National Institute of Justice (NIJ special Report)	2004		Write protection rules required for forensics tools, but no tool vendor specified	Strong focus on rules of evidence assessment, acquisition, examination		Entire forensics procedure & Legal Forms	Policy and procedure for case Management	Forensics favoured features of physical storage mentioned	Intended for use by law enforcement officers and other members of the law enforcement community who are responsible for the examination of digital evidence.
Good Practice Guide for Computer-Based Electronic Evidence [51]	Association of Chief Police Officer	2004	What kinds of devices should be seized	Providing Guidance for Forensic Tool Use	The principles of computer-based electronic evidence.	Crime are categorised by different crime scenes or environments such as Network, Mobile phone		Major focus in the recovery of computer-based electronic evidence; but still focus on single machine		The guide revised and published as sign that digital crime are independently considered as a major crime in this society where Information Technology is ever developing, and the electronic world and the manner in which it is investigated has changed considerably.
Guide to Integrating Forensic Techniques into Incident Response [52]	National Institution of Standards and technology Administration U.S. Department of Commerce Department of Homeland Security	2006	Whatever devices seized, the storage of the devices contain the potential evidence, filesystems rules	Forensics tools have to apply to general functional and legal requirements to maintain integrity of data.	NOT only legal requirements but also forensics favoured policies for organisation.		Using the term of "Lifecycle" to describe forensics investigation or incident respond events		Major focus on forensics features of Data system, operating system, network system, and application	Definition of forensics science and the top layer requirement for digital forensics is preserving the integrity of the information and maintaining a strict chain of custody for the data which can be used later as evidence in court. Technical rules are applied to forensics tools to make it compliant with laws.

Name of the Standards	Publisher	Year	Major Focus							Description
			Devices Intro	Forensics Tools	Evidence Weight (Legal)	Crime Category	Forensics Operational Process	Digital Investigation Background	Forensics Features in Application	
Forensics Plan Guide [53]	Sesame, Audit, Networking and Security (SANS)	2006	Physical storage of any devices	<i>EnCase, and Helix and Window forensic tool</i>	Detailed evidence analysis rules		Detailed lifecycle of forensics investigation or incident respond	Management of investigation case to report	Forensics features from Unix and Windows system, and email application	A combination of a dynamic checklist and template for recording computer investigation processing steps and information. The Plan Guide is investigation case based.
HB171 – Management of IT evidence* [55]	Standards Australia	2007			Principle for the management of IT evidence			Consider the forensics lifecycle as IT evidence management lifecycle		Most evidence is collected from data storage, and there have been well-known forensics tools to extract the data. This handbook aims to provide guidance on the management of electronic records that may be used as evidence in judicial or administrative proceedings, whether as a plaintiff, defendant or referral to appropriate authorities for investigations.
Electronic Crime Scene Investigation: A guide for First Responders 2 nd Edition [56]	U. S. Department of Justice; Office of Justice Programs; National Institute of Justice (NIJ special Report)	2008	Different type of storages		Specific & detailed rules of evidence collect	Updated crime: Terrorism	Detailed procedure of evidence collection	Social network, network crime, mobile phone, cybercrime.		Digital evidence is considered as the core of digital investigation. Digital crime in business environment is considered.
Digital Evidence Field Guide: What Every Peace Officer Must Know [57]	U. S. Department of Justice; Federal Bureau of Investigation	2009			Digital crime evidence nature, rules of identify, protect and conceal the evidence, legal consideration (Search warrant)	Updated crime: Cyber terrorism, corporate espionage, phishing		Computer system is the target of a crime; it can also be an instrument of the intrusion or attack.	Cyber system as the repository of evidence	Digital evidence is not anymore an accessory of any normal crime evidence because computers can become a roadmap to a criminal's activities.
Guidelines for Identification, Collection, and/or Acquisition and Preservation of Digital Evidence Working Draft (WD 2 nd) 27037 [58]	International Organisation for Standardisation (ISO)	2010			Highly abstracted evidence requirements provide a convenient material for our project to extract forensics attributes.			Digital forensics is a mature industry but in its turnaround period due to technology development of cloud computing, network, encryption etc.	Strategically focus on network features that provide forensics value.	Includes key technical, operational and legal issues of evidence collection. Detailed fieldguide for an investigation operation.

Table 3- 2 Selected Forensics Standards

3.4 Summary: The Knowledge Structure of the Forensics Overlay

So far in this thesis, we explained in chapter one the current forensics landscape and stated that the enterprise is a significant entity in the forensics environment. It follows that a new forensics model (the overlay) should include business elements, shown in Figure 3-4.

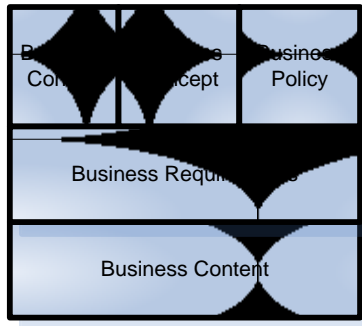


Figure 3- 4 Business Considerations

We suggest in chapter two that using the SABSA matrix, shown in Figure 3-5, as a foundation to create the overlay. With built-in features of the SABSA matrix, different perspectives of business requirements are integrated seamlessly with forensics requirements.

	what	why	how	who	where	when
Contextual						
Conceptual						
Logical						
Physical						
Component						
Operational						

Figure 3- 5 Framework of SABSA Matrix

This chapter shows that the forensics requirements are extracted from forensics knowledge. The most sought-after forensics knowledge is the forensics standard. Through studying the forensics standards created throughout the past decade, we believe the rules of evidence and chain of custody are the two elements that have the most solid connection with the term “forensically sound”. Therefore, the forensics requirements that cover all overlay layers should be the rules of digital evidence, shown in Figure 3-6.

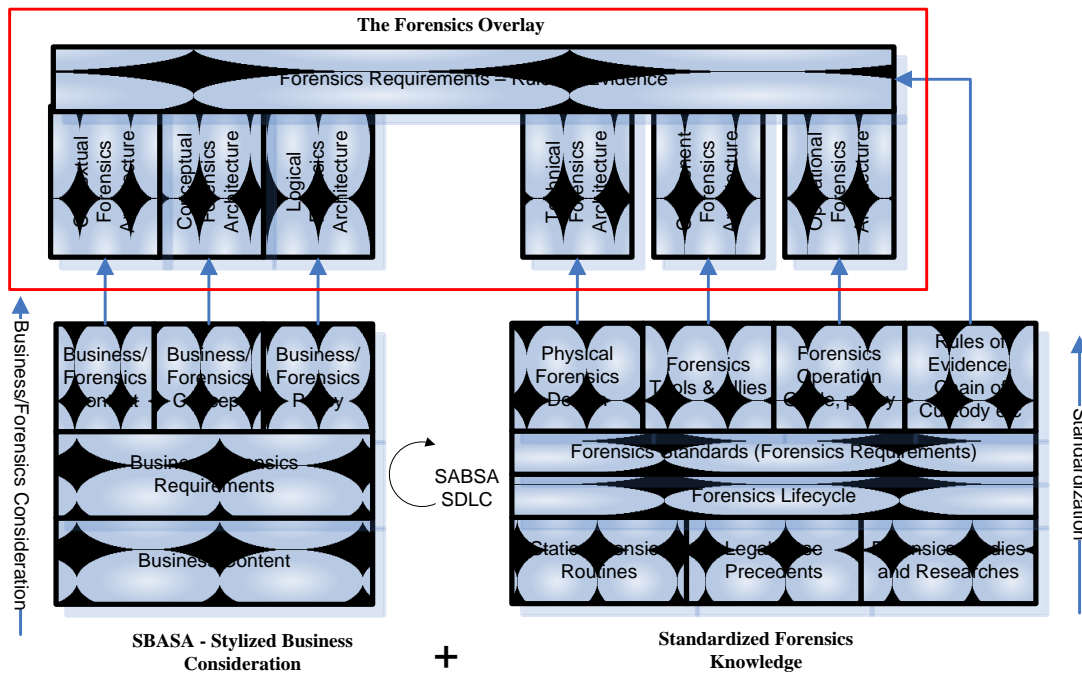


Figure 3- 6 Knowledge Structure of the Forensics Overlay

To summarise the first three chapters, figure 3-6 shows the knowledge structure of the forensics overlay. In this blueprint, business elements are addressed via application of SABSA matrix while forensics elements are addressed via application of forensics knowledge.

4 Design of a Forensics Overlay

As outlined in chapter three, a combination of the SABSA matrix and digital forensics knowledge provide a foundation for the forensics overlay, shown in Figure 3-6. In this chapter, we create the Forensics Overlay according to the previous design. The primary effort made to create the overlay includes 1) contextual layer, defining a set of forensics drivers containing business objectives 2) conceptual layer, defining a set of forensics attributes using the SABSA business attributes as a reference; 3) logical layer, creating operational policies for achieving business/forensics goals; 4) physical layer, selecting mechanism (or forensics features) to protect the evidence. The previous three layers focus on designing forensics in a business setting. The physical layer focuses on delivering practical services or mechanism to the business. Similar to the SABSA matrix, the overlay contains its own features to help the users develop solutions with each concerned cell. Furthermore, these features trigger more design and development to users' project related information. Similar to the SABSA model, the overlay is not doctrinal like a checklist or a field guide; it is dynamic and expected to suit the different business forensics cases.

Chapter Four:

4.1 Explains how to create the Contextual Layer: Forensics Drivers & Evidence Threat

4.2 Explains how to create the Conceptual Layer: Forensics Attributes Profile

4.3 Explains how to create the Logical Layer: Policy & Forensics Service

4.4 Explains how to create the Physical Layer: Design Forensics Mechanisms

4.1 Contextual Layer

The forensics contextual layer helps senior executives understand the forensics in a strategic level. This layer usually addresses the considerations for a business that start their forensics project in the early stage. For example, the contextual layer helps a business that needs to develop their forensics capabilities understanding the requirements of the program cost, resource, timeline, services, clients, etc. Same as all the following layers, forensics contextual layer has six cells: Assets (What), Motivation (Why), Process (How), People (Who), Location (Where) and Time (When). Only

contextual Assets, Motivation and Process are addressed since People, Location, and Time largely depend on the typical business cases.

4.1.1 Assets

The contextual assets cell addresses Business/Forensics (B/F) drivers that are abstracted from business goals and objectives. A B/F driver is a redefined statement of how forensics can help achieve the business goal. In the SABSA approach, each Business/Security (B/S) driver is considered as a unique sub system which needs to be designed for security from a business risk perspective. In the forensics overlay approach, each B/F driver requires defined details to understand the business forensics objectives on a strategic level. The difference between B/F and B/S is that B/S focuses more on the detection and the prevention before a cybercrime incident. The B/S drivers focus on the protection of the daily business, while the B/F drivers focus on the protection of digital evidence.

Through the study of the legal and business cases concerning the business forensics investigations, we provide forensics business drivers to present an overview of the forensics expectations from a business, shown in Table 4-1. The B/F driver table shows a short version of a business goal and objectives. These B/F drivers are basic requirements from a business which aims to conduct forensics investigation in any cyber and business conditions and pursue further prosecution when feasible and necessary. On top of these basic forensics drivers, users of the overlay may add or change any items according to their own business situations.

The Business/Forensics driver table is one of the forensics overlay features provided in our project. These basic features (including tables or models in other cells) are developed to inspire more considerations and ideas through workshops.

Driver No.	Forensics Drivers
FD1	Protecting the business reputation by ensuring a cybercrime free environment.
FD2	Ensuring that policy makers address issues of typical cybercrime from both internal and external scope in terms of cybercrime definition, legal status, victim (which sector within the business), deterrence & enforcement, coordination & cooperation plan [41] (between corporate investigators and other part of the business, also between corporate investigators and investigators from law enforcement) [36].
FD3	Maintaining the accuracy of information, especially those with potential evidential value [38].
FD4	Providing the ability to prosecute those who attempt to defraud the business [38].
FD5	Enforcing the roles and responsibilities during a cybercrime investigation.
FD6	Ensuring that information processed in the business system can be brought to a court of law as evidence in support of both criminal and civil proceedings and that the court admits the evidence, and that the evidence withstands hostile criticism by the other side's expert witness [38].
FD7	Minimising the number of incidence of cybercrime, highly offensive but not unlawful, breach of procedure, policy or inappropriate actions only.
FD8	Collecting digital evidence in forensics manner no matter the cases of cybercrime, highly offensive but not unlawful, breach of procedure, policy or inappropriate actions only [37].
FD9	Preparing and providing when required any forms of evidence that pertaining to a legal case to law enforcement party [37].
FD10	Ensuring that the business system is at all times compliant with the laws and industry sector regulations (e.g. Forensics Standards), and that the system approach directly and indirectly supports legal compliance [38].
FD11	Ensuring that transaction between parties cannot be denied that a transaction occurred [37] [38].
FD12	Detecting and forensically maintaining any records of abusing the access privileges.
FD13	Conducting investigation against any violations of enterprise policy.
FD14	Ensuring the business system provides the solution that complies as far as possible with internal and external standards and best practise, adapting forensics architecture to conduct the enterprise system design.
FD15	Ensuring that the forensics architecture is independent of any

	specific vendor or product and is capable of supporting multiple products from multiple vendors [38].
FD16	Providing a forensically sound awareness program to the employees and forensics professional training to internal investigator.
FD17	Providing a backup plan for business continuity when the system is compromised or related to cybercrime [39].

Table 4- 1 Business/Forensics Drivers for Contextual Asset

4.1.2 Motivation

The contextual motivation cell contains a list of threats that may cause the invalidation of digital evidence, shown in Table 4-2. A threat against digital evidence is an event with the potential of disclosure, modification or destruction to digital evidence contained in the business system. Threats may be non-malicious (like those caused by human error, hardware/software failures, or natural disaster) or malicious (within a range going from protests to irrational nature) [42]. The threats addressed on a higher level provide less sufficient details to typical cyber attacks, mistakes in the business and forensics operations. Therefore, the detail threats allocation depends on the actions taken in the following layers. For example, when using the forensics overlay in the business application development, these threats are mapped with forensics attributes in the conceptual layer (details explained in Section 4.2). In addition, the high level threats list addresses the link between threats and business context. Such linkage is usually ignored by many other models.

Threat No.	Digital Evidence Threats
ET1	Disclosure of digital evidence has the potential to compromise the admissibility of the evidence when the electronic stored information (ESI) is not obtained and handled by forensics investigators but by opposing party or non forensics employees [41].
ET2	Not all media that is identified and preserved need to be processed. Risks stemming from reducing the amount of ESI include: a) Excluding potential key evidence that's beneficial to your case; b) Violating e-discovery obligations resulting in sanctions, an adverse inference instruction [41].
ET3	Unauthorised deletion or modification of digital evidence data, such intentional damage to information assets that result in the loss of integrity of the assets [42].
ET4	Disruption against normal operation of forensics investigation and evidence collection, preservation, analysis and report. The reason of disruption can be malicious or simply a random power failure.
ET5	Human errors by forensics investigator, high-risk employee such as system and network administrators.
ET6	Decentralised information process may affect the forensics investigation and digital evidence collection.
ET7	Digital offenders may hide their trace by deleting the evidence. The situation may occur during organised crime, political terrorists and highly skilled hackers.

Table 4- 2 Threats against Potential Digital Evidence

4.1.3 Process

The contextual process cell addresses the factors to consider developing an enterprise forensics capability, shown in Figure 4-1. These factors can also be used when a business starts any forensics-related project, e.g. develop forensically sound application. These considerations enhance senior executives' understanding of the forensics capability. Therefore, the forensics requirements for the overall business goals are easily generated.

The “Resource” means the internal resource to develop the forensics capability. For a business that begins developing its forensics capability, its internal resources can be limited. Typically, the business may only have the IT and Legal departments to provide professional advice. Initially, the project team is formed by personnel from both departments and senior executives. The similar situation applies to the business forensics projects; the only difference is that the team should include more members who specialised in the application development. The senior executives should make it a point to have an efficient balance among resource, time and cost. It is possible to consider the consultancy from external resources including legal and technical perspectives.

The enterprise forensics capability includes both digital investigative capability and electronic discovery capability. Therefore, businesses need to consider the expense on building an incident response team that specialised in the entire enterprise-capable forensic and electronic discovery [46]. In addition, there are considerable expenses on the forensics software and hardware, unless the business decides to develop its forensically sound applications, details shown in chapter 6. All the decision should be made according to the business drivers in the contextual asset cell, which represents the overall business goals and objectives.

Cells in the overlay are connected to each other to perform common tasks in enterprise forensics related projects. Therefore, the overlay can be seen as a combination of multiple cell strings which respectively deal with different issues. These cell strings enhance the traceability of the overlay items, shown in Figure 4-4. For example, in the project of the forensically sound application development, different cells across multiple layers forms an application development lifecycle that deal with issues of application requirements, application high level design and application forensics features design, see chapter 6 for more details.

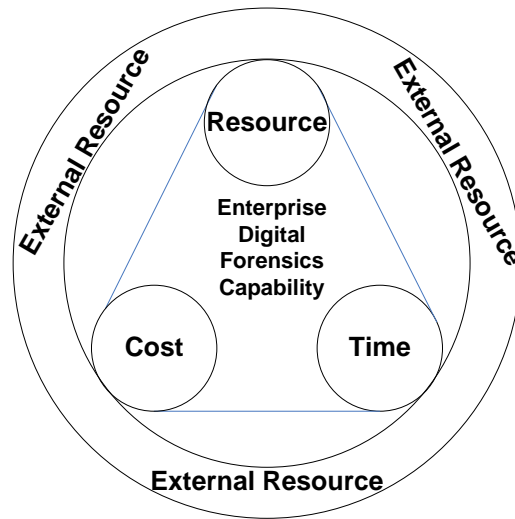


Figure 4- 1 Factors to Consider for Developing Forensics Capability

4.2 Conceptual Layer

The conceptual layer deals with how diverse forensics knowledge can be applied to support business goals. The forensics conceptual layer designs overall forensics into a business by addressing the assets, motivation, process and people.

4.2.1 Assets

Equivalent to the SABSA business attributes profile (SBAP), shown in Figure 2-1, a forensics attribute profile is presented in the conceptual assets cell. The forensics attributes are extracted from forensics standards, shown in Table 3-2. As concluded in chapter 3, the most critical requirements from current forensics standards are those related to how to maintain evidential value of the business data. Table 4-3 shows the forensics attributes samples extracted from a forensics standard: *Text for ISO/IEC 2nd WD 27037 – Guidelines for identification, collection and/or acquisition and preservation for digital evidence (WD27037)*. There are five sample attributes that are extracted; within these five attributes, “auditable”, “accountable”, and “repeatable” are quoted directly from WD27037, while “less-intrusive” and “informed” are worked out through the workshop analysis process.

During the workshop process, the attribute “informed” has been extracted from the standard *WD27037 (Section 5.4)*. It requests that “it is essential that the Digital Evidence First Responders (DEFRR) and/or Digital Evidence Specialist are adequately briefed by authorised personnel before he/she begins performing the tasks” [40]. Searching SBAP, the term “informed” is found in the USER group and refer to a situation that “The user should be kept fully informed about services, operating procedures, operational schedules, planned outage, etc” [39]. Therefore, the attribute “informed” matches the requirements from *WD27037 section 5.4*. The term “inform” is redefined in terms of forensics, see Table 4-4.

The redefining process is necessary since each selected attribute is based on forensics knowledge, while SBAP is based on security knowledge. To create the forensics attributes profile, re-definitions of each attributes are needed. Depending on each case, attributes have different definitions depending on the contextual layer and structure of the business. Only with such a re-definition, shown in Table 4-4, with each selected attribute, we add forensics implications to the overlay; otherwise, the forensics overlay is merely a subset of SABSA.

Attributes	Description
<i>* Directly Quote from Document</i>	
Auditable	Digital evidence specialist was capable of undertaking the processes and making any conclusions, with an appropriated method, technique and /or procedure were followed.
Repeatable	The same test results are produced under the following conditions: <ul style="list-style-type: none"> - Using the same measurement procedure; - Using instruments and conditions that are comparable to the original test; and - Can be repeated at any time after the original test
Defensible	The Digital Evidence First Responders (DEFRRs) should be able to justify her actions and methods used for the identification, collection, acquisition and preservation of the potential digital evidence.
<i>* Extracted from Document via Analysis</i>	
Less Intrusive	Readily verified forensics method;
Informed	Forensics procedure briefing information should be documented, or DEFRR should be informed to do so.

Table 4- 3 Sample Attributes Extracted from WD27037

SABSA Defined “Informed” [39]	Forensics Overlay defined “Informed”
The user should be kept fully informed about service, operating procedures, operational schedules, planned outage, and so on.	Forensics procedure briefing information should be documented, or DEFRR should be informed to do so.

Table 4- 4 Define Attributes in Terms of Forensics

The forensics attributes profile provides a conceptual requirement framework that is abstracted from forensics knowledge but also link with standard business requirements from SBAP. This framework guides the later design of the entire forensics environment. It connects both the business and forensics goals.

4.2.2 Motivation

The conceptual motivation cell deals with business risk management objectives. In the forensics overlay, it deals with forensics risks on a high level. The forensics risks concentrate on human, natural and environmental threats against digital evidence or the correct collection of digital evidence shown in Figure 4-2. The human issue is more focused in this research.

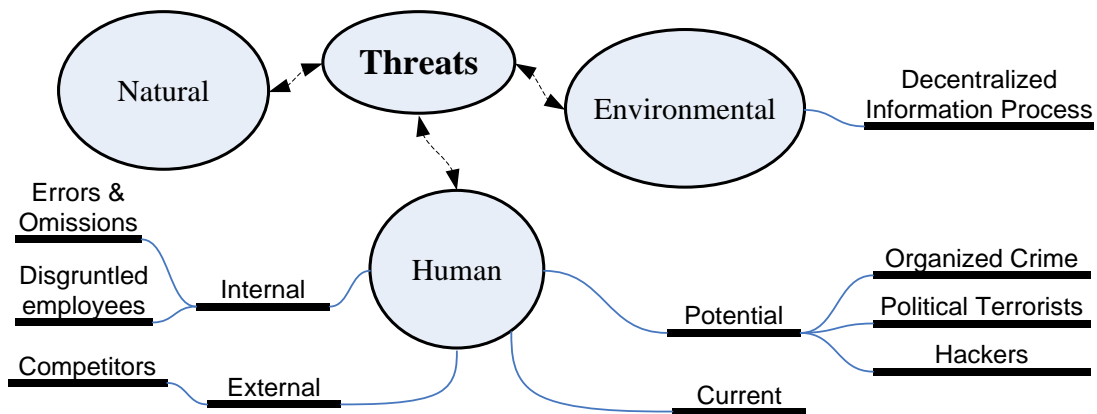


Figure 4- 2 Threats to Digital Evidence

With the overview of the threats against digital evidence, the forensics risk management team's target is to understand the rules of evidence and enhance the usability of the digital evidence in the court of law. The five rules of collecting digital evidence are Admissible, Authentic, Complete, Reliable and Believable [8]. These rules of evidence, shown in Table 4-4, are based on the practice of forensics and are a key requirement to ensure any risks to these properties are mitigated. Therefore, organisations that are willing to perform standardised forensics investigations must develop the forensics policy in the logical layer and forensics practical rules in the physical layer.

The forensics conceptual cell also relates to the forensics contextual layer presenting the evidence threat list, shown in Table 4-2. The threat list in the conceptual motivation cell focuses on the overall picture and requirements, while the other forensics conceptual cells relate to threat management.

Property	Rules of Digital Evidence
Admissible	Admissible is the most basic rule. The evidence must be able to be used in court or otherwise.
Authentic	Must be able to show that the evidence relates to the incident in a relevant way.
Complete	It is not enough to collect evidence that just shows one perspective of the incident. The collected evidence must prove the attacker's actions, also their innocence. For instance, if you can show the attacker was logged in at the time of the incident, you also need to show who else was logged in and why you think they did not do it. This is called exculpatory evidence and is an important part of proving a case.
Reliable	The evidence collection and analysis procedures must not cast doubt on the evidence's authenticity and veracity.
Believable	The collected evidence should be presented clearly understandable and believable to a jury. There is no point presenting a binary dump of process memory if the jury has no idea what it all means. Similarly, if you present them with a formatted, human understandable version, you must be able to show the relationship to the original binary, otherwise there is no way for the jury to know whether you have faked it.

Table 4- 5 Sample Attributes of Rules of Evidence

4.2.3 Process

The conceptual process cell outlines the organisational forensics process according to forensics standards and business requirements from the contextual layer. The organisational forensics process is different from the conventional forensics lifecycle. Traditionally, the forensics lifecycle includes identification, preparation, approach strategy, preservation, acquisition, examination, analysis, presentation and returning evidence, shown in Figure 3-2. However, the enterprise forensics process lifecycle contains more details to serve the forensics related project team, forensics investigators and the enterprise incident response team. The difference also lays on the fact that the

conceptual level focuses more on forensics strategies and architectural layering [47], while conventional forensics lifecycle focuses more on forensics operations.

In the conceptual level, there is more to consider during an incident in a business environment. Before actually performing the tasks in the identification phase, the business forensics process needs to conduct the following tasks: a) Address the business requirements in terms of identifying and preserving evidence; determining the method, time frame, and the scope of the compromise; perform investigations with as little disruption to the corporation as possible. b) Assess the internal/portable data storages and forensics features that are already built in a business system. c) Decide which preliminary tools would be helpful from a forensics perspective, and which parties (internal & external) may be involve in the investigation. d) Implement a plan for the preservation of logs so historical evidence is not deleted. e) Implement proper controls to keep the daily business running. As the business continues running with the investigation, the choice is made on whether to terminate the investigation. The disaster recovery plan should be launched if the decision is made to terminate the investigation.

Considering the complexity of a forensics task performed in an enterprise environment, other teams are appointed along side with the forensics investigation team. Therefore, the conceptual process cell needs to establish an overall business/forensics lifecycle rather than a conventional forensics lifecycle.

Inspired by Reyes, A. and J. Wiles's Digital investigations Standard Operating Procedures [11], we added three initial phases to the forensic lifecycle: Request for Business Forensics Process, Initial Analysis and Decision Making, shown in Figure 4-3.

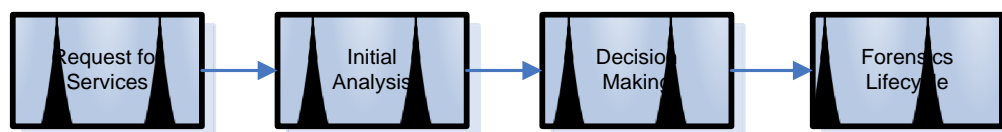


Figure 4- 3 Enterprise Forensics Procedure (EFP)

The EFP applies the principle of the business consideration and the business team cooperation. The first phase shows that a formal request is needed before any forensics process. The request must be tracked and should be used to build metrics on how many investigations are initiated, by which departments, the types of cases, and how quickly the team addresses them [46]. The request phase shows the teamwork between the applicant department and the forensics team. The initial analysis is carried on by the forensics team. The initial analysis includes documentation, planning and identification of the forensics target. The decision making phase shows the teamwork between the forensics team and senior executives. The decision making is not a simple “Yes or No” order, but the statement of investigation requirements which is based on the advices provided from the initial analysis results.

4.2.4 People

The conceptual people cell designs the forensics responsibility map according to the organisation structure. The cell represents a Responsibility Assignment Matrix table to describe how these roles participate in the cyber investigation incident. The key responsibilities are described by Responsible (R), Accountable (A), Consulted (C), Informed (I) and Witnessed (W). The following sample matrix shows several typical roles in a forensics investigation activity.

Roles	R	A	C	I	W
CTO		√			
Forensic Specialists	√				√
Legal Consultants			√	√	
IT Department Members			√		√
Normal System Users					√

Table 4- 6 RACIW Table

4.3 Logical Layer

The forensics logical layer describes and designs the forensics knowledge into the business environment. In the forensics logical layer, the asset should be the evidential information that is contained in a daily business. Without a forensics incident, the term “evidential information” is an indistinct concept; on the other hand, with forensics incident and investigation, all relevant information has the potential to be evidence. Relevant information includes data that is generated by investigators such as the crime scene pictures, notes and interview records. We decided to leave the assets cell blank so that during a typical forensics cases, logical assets can be filled. Without a typical forensics case, the logical assets cell contains all the defined enterprise information.

4.3.1 Motivation

The logical motivation cell aims to help design the organisational forensics policy to protect potential evidence. The logical policy design ensures 1) the business compliance to the evidence rules located in conceptual motivation cell and 2) the business mitigation planning against the evidence threats located in contextual motivation cell. The business may consider designing the forensics policy in five (or more) perspectives includes technical, functional, environmental, legal, and political.

Technically, the current business usually deploys the complex networking, computing and application technologies. These technologies are not traditionally designed in a forensics manner. The issue on how to design a good policy to select, deploy, and implement those technologies are challenging for a business/forensics environment. A business has to conduct its daily business through various technologies and applications. It is complicated to assure various business systems work together, it is even more complicated to assure them to work in a forensics manner when incidents occurs and the investigation follow.

Environmentally, the policies should address how to manage and obtain the knowledge of a cybercrime affected environment. Many factors are involved in this policy design, such as legal requirements, the type of the incident, the forensics tools, disk storage, network capacity and access issues.

Legally, it is the policy makers' responsibility to design an effective regulation to ensure the business compliance with industrial forensics standards.

Politically, the forensics policy involves various parties of the business such as corporate clients, business partners, the press, legal organisations, and law enforcement.

With all these five perspectives, questions that need to be asked to the architecture designers are: Which department's responsibility to protect potential evidence. What is the department responsible for, where are the forensics targets? When is the forensics supports needed and Why. A matrix is designed to assist setting up the enterprise forensics policy, shown in Table 4-6.

	Who	What	Where	When	Why
Technically					
Functionally					
Environmentally					
Legally					
Politically					
More ...					

Table 4- 7 Forensics Policy Matrix

4.3.2 Process

The logical process cell defines the forensics services for a business system. It is derived vertically from the conceptual process cell. The forensics service is abstracted from the conceptual forensics process to interpret what kind of forensics function should be performed in the business procedure. One of the most critical forensics services from

business systems is providing the evidential data when necessary. This service is later used in the physical layer to generate forensics mechanism such as system logs, configuration files, etc, shown in Figure 4-4. The other important service is to verify the business data in a forensics manner, which is later applied in the physical layer to generate forensics mechanism such as MD5 Hash.

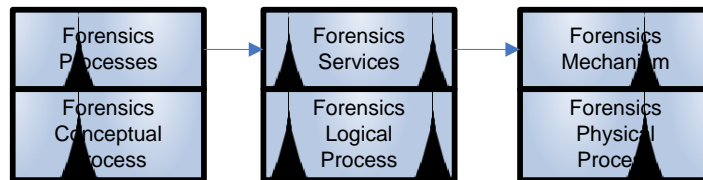


Figure 4- 4 Traceability of the Forensics Process between Overlay Levels

4.3.3 People

The people cell in the SABSA logical layer contains an entity & trust framework. Basically, it specifies how to manage the different entities such as supplier groups & customer groups to trust each other during a digital transaction.

In the case of forensics, the end-to-end evidence transactions occurs between the organisations and the court of law. The mechanism used in between can be technically a digital signature and operationally a chain of evidence. Therefore, in the forensics logical people cell, we present a forensics trust framework to help the business understand the evidential association between entities, shown in Figure 4-5.

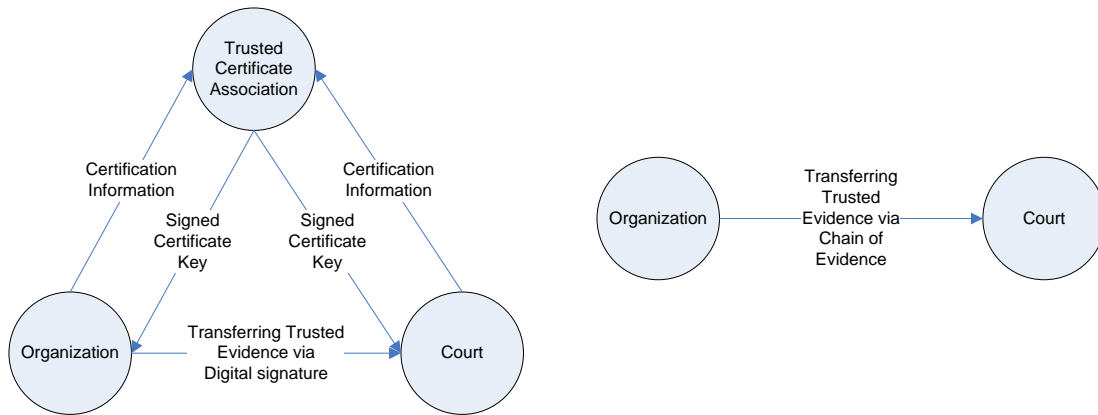


Figure 4- 5 Trusted Evidence Transferring

4.3.4 Location

According to the SASBA method, the logical location cell is originally used to define a set of security domains and associations in between. It is important to differentiate the physical domain from the logical domain. A physical domain is a location to establish the services that have been designed in a logical domain. For example, the SABSA logical domain defines the security domains and associations, while the SABSA physical domain defines the platform and network infrastructure.

Different from the SABSA logical domain (security domains and associations), the forensics logical domain has a certain hierarchy during a forensics incident, there are some regulations made by the authority (e.g. the court of law). Those regulations must be complied by the business and the related sub-domains. Furthermore, the business passes these rules to their customers, partners, etc, shown in Figure 4-5. The forensics domain association is a type of regulation enforcement but not a service. Fail to apply these rules in the evidence management leads the business in an inferior position in any further prosecutions. In the forensics logical location cell, we present a forensics policy domain sample and its regulation enforcement association. In the forensics policy domain map, the regulation authority makes the rules by law or precedent regulation. The precedent regulations include the previous issued judgement or opinions [45].

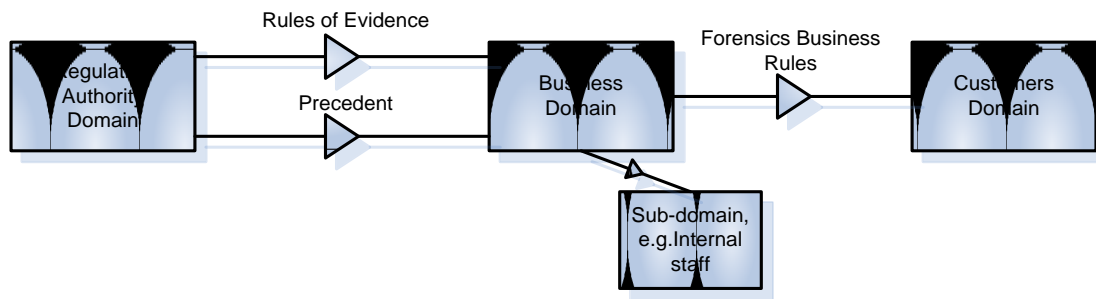


Figure 4- 6 Forensics Policy Domain Map

4.4 Physical Layer

The physical layer defines the forensics activities that different roles are performing in a business. Given different responsibilities of roles (defined in the logical layer policies), some roles such as the production manager may not perform forensics activities; while some roles such as internal forensics investigator whose daily jobs are forensics related duties. However, if a production manager does not follow the forensics related policies, the forensics investigator may fail to get evidence from the production environment. Therefore, the physical layer also focuses on raising the awareness of forensics across different roles in an enterprise environment. For example, the business application developers apply rules of evidence into the business system development.

4.4.1 Motivation

The physical motivation cell addresses a set of easily understood rules for both the forensics teams and other business teams. These rules should be derived from the Rules of Evidence in a conceptual motivation cell and an Organisational Forensics Policy in the logical motivation cell. A sample DO and DO NOT list is present in Table 4-7 [43].

Items	DO & DO NOT list
L1	Minimise handling and corruption of original data.
L2	Account for any changes and keep detailed logs of your actions.
L3	Comply with the five rules of evidence.
L4	Do not exceed your knowledge.
L5	Follow your local forensics policy.
L6	Capture as accurate image of the system as possible.
L7	Be prepared to testify.
L8	Work fast.
L9	Proceed from volatile to persistent evidence.
L10	Don't shutdown before collecting evidence.
L11	Don't run any programs on the affected system.

Table 4- 8 DO and DONOT List

The list is easily understood for those none forensically trained IT employees who are most likely summoned to draw their own conclusions in the early stage of a cyber incident. On the other hand, the business application developers also benefit from the list which is treated as one resource of the practical system development requirement.

4.4.2 Process

The process cell presents the mechanisms to protect and preserve the evidence. For example, the hashing mechanism applied to Email data of the header, body, and attachments [44]. Forensics mechanisms are varied depending on the different forensics tasks (with different business goals and requirements) planned in the contextual layer and also derived from the forensics services in the logical layer, shown in Figure 4-4.

4.4.3 People

In the forensics overlay, the physical people cell addresses the issues related to the users or user interfaces of forensics services. Since forensics services are included in an overall business service, the user includes both normal business users and forensics specialists. The specialists are qualified to use certain forensics services than other

users. For example, a forensics investigator is more eligible in collecting evidential data than an accountant. In some cases, the forensics service such as checking email user's data should be only accessible to forensics specialists. In these cases, the authentication mechanism should be applied in the users' interface or a higher level. It is critical to use an authentication method to validate all the entities involved in the crime scene—the user using the application, the system that is being used, and the application being used on the system by a user [67].

It can be ambiguous to decide the role based authentication policy if a business does not have a well structured role and responsibility framework, see Table 4-5. For example, if a business has an IT department performing the forensics functions, IT staff who has no forensics training may accidentally damage the evidential data or similarly, they are potential cyber offenders.

4.5 Component Layer

The SABSA model includes security standards in the component motivation cell since the SABSA model initialises its process by considering only the business objectives and goals to generate the business drivers. In terms of the forensics overlay, both business and forensics standards are considered to generate the Business/Forensics drivers. Forensics standards as well as forensics knowledge are not a single layer in the forensics model; instead they are a set of ubiquitous fundamental rules that guide the entire design of the forensics overlay. Therefore, the component motivation cell is left empty.

The SABSA model also includes security tools in the component process cell. However, in terms of forensics, we do not consider the forensics tools as the only solution to perform a perfect forensics operation. Sometimes the vendor tool does not work as the business requirements. For example, one tool captures volatile data but cannot display the data unless it is connected to the target system. In this case, after the incident is over, there is no way to view the volatile evidence. There are occasions on which a vendor's remote forensics tools and other tools cannot be used for network access

reasons. In terms of the forensics overlay, one of the goals is to assist developing forensics features into business systems so that the forensics mechanisms are built in the system or software. By doing so, we are able to reduce the increasing workload on designing, developing and testing forensics tools, we can also reduce the overly reliance on forensics tools. Therefore, the forensics component process cell is purposely left blank. For some businesses that decide to largely depend on third party tools, should be able to find relevant contents in the component layer.

4.6 Operational Layer

The forensics operational layer contains the chain of custody issues which has been described in detail in many relevant literatures. Therefore, we only address the chain of custody in the operational process cell.

4.7 Forensics Overlay

The SABSA methodology has a legal subset about the forensics issues. The SABSA business profile contains a set of legal attributes as the legal requirements are part of the enterprise security requirements. However, the forensics overlay, shown in Figure 4-7, is not simply using the legal contents that are already contained in SABSA. Instead, the forensics overlay considers forensics requirements as crucial as business & security requirements. That means the forensics standards are not considered as a tools on the component layer but as forensics requirements in the strategic level.

4.7.1 Layers

The forensics overlay contains five layers; each layer presents its unique focus. The tasks assigned to each layer are conducted by different roles within an organisational structure. Different layers are not isolated from each other. The hierarchy of the overlay can represent the lifecycle of a forensics project. Contextual layer is about understanding the business requirements. Conceptual layer is about analysing the business requirements. Logical layer is about designing the system with requirements. Physical layer is about implementing the actually system development. It is important to notice that the physical layer does not contain detail elements for coding and

programming since the entire forensics overlay is not only designed for software development. The forensics overlay can also be used to guide the enterprise policy making, investigations, forensics management, etc.

Forensics Layer	Description
Contextual Layer	Understanding business goals and forensics requirements
Conceptual Layer	Supporting business goals using forensics rules and standards
Logical Layer	Designing business with forensics standards
Physical Layer	Developing business system in forensic manner
Operational Layer	Relevant chain of custody issues

Table 4- 9 Overlay Layers

4.7.2 Cells

The forensics overlay contains 15 cells in total. Every cell has a unique focus depending on both the layer and the cell references, shown in Figure 4-6. The cells in the contextual layer are considered as the “root” of the following cells in the lower layer. The developments of the following cells are based on the business/forensics goals. Through the conceptual and logical design, the cells in the physical layer provide physical solutions for business forensics goals.

To deal with a typical business forensics issue, some of the cells can be connected as a string view (or tree view) structure from the contextual layer to the physical layer. Such tree view provides traceability and hierarchy of a forensics project process, detailed in forensics email client function design in chapter 6.

	ASSETS (What)	MOTIVATION (Why)	PROCESS (How)	PEOPLE (Who)	LOCATION (Where)	TIME (When)
CONTEXTUAL ARCHITECTURE	Business Decisions	Business Risk	Business Processes	Business Governance	Business Geography	Business Time Dependence
	Business/Forensics Drivers	Digital Evident Threat List	Framework of Operational Processes for Digital Investigation			
CONCEPTUAL ARCHITECTURE	Business Knowledge & Risk Strategy	Risk Management Objectives	Strategies for Process Assurance	Roles & Responsibilities	Domain Framework	Time Management Framework
	Attribute Profile Related to Forensics	Control Objective, Forensics Rules of Evidence	Forensics Process According to Standards	Forensics Responsibility Assignment Matrix		
LOGICAL ARCHITECTURE	Information Assets	Risk Management Policies	Process Maps & Services	Entity & Trust Framework	Domain Maps	Calendar & Timetable
		Organizational Forensics Policy	Forensics Service	Forensics Trusted Framework	Forensics Policy Authority Domain Map	
PHYSICAL ARCHITECTURE	Data Assets Risk	Management Practices	Process Mechanisms	Human Interface	ICT Infrastructure	Processing Schedule
		Organizational Forensics Practical Rules to Protect Digital Evidence	Mechanisms to Protect or Preserve Evidence; Design Pattern	Role Based Access Control		
COMPONENT ARCHITECTURE	ICT Components	Risk Management Tools & Standards	Process Tools & Standards	Personnel Management Tools & Standards	Locator Tools & Standards	Step Timing & Sequencing Tools
SERVICE MANAGEMENT ARCHITECTURE	Service Delivery Management	Operational Risk Management	Process Delivery Management	Personnel Management	Management of Environment	Time & Performance Management
			Chain of Custody			

Figure 4- 7 Design of a Forensics Overlay

In this thesis, we introduced the background knowledge of SABSA, the forensics knowledge, the forensics industry and the cybercrime evolution. We analysed the current forensics model and suggested that a new model is needed. We created a new forensics overlay as a new model for the enterprise forensics environment.

In the next chapter, we further analyses the current enterprise forensics environment. A case study is presented to describe forensics pros and cons in an enterprise environment. By presenting the issues in a current business forensics case, we provide one solution to build a forensics business environment using the forensics overlay.

5 Digital Forensics in a Business Environment

Section 3.1.3 illustrates how current digital forensics industries face challenges from technological perspectives and how current businesses emphasise on using forensics tools for evidence collection from limited areas. This chapter also focuses on business perspectives explaining the trends of business information management (BIM) and how digital forensics is implemented in a business environment.

Chapter Five:

5.1 Introduces the Trend of BIM in Terms of Digital Forensics

5.2 Describes the Static Forensics Implementation in Business Environments

5.3 Describes the Live Forensics Implementation and Limitations

5.4 Provides an Enterprise Forensics Investigation Case Study and Related Issues

5.5 Proposes a Forensically Sound application Development as a Solution

5.1 Introduction

Most businesses generally have a certain level of forensics capability. However, conventional forensics capability does not fulfil the current digital investigation requirements because of two reasons.

Firstly, the increasingly sophisticated cybercrime requires a higher level of forensics professionalism. Many businesses develop forensics capabilities from their IT and legal departments. Such limited forensics capabilities can only afford to solve lower level investigation cases. Evidence collection is required to serve more sophisticated cyber cases that further develop into prosecution. It follows that the business has to call for external cyber crime forensics assistances. In this case, the IT department turns into the victim that provides only informative assistance for the external forensics force. Furthermore, the information collected from the victims are generally considered as the anecdotal evidence which are less weighted than the testimonial or statistical evidence generated by the victims' computer applications [59]. Due to more focus on litigation preparation, businesses have to develop their forensics department to take charge of

using forensics tools to retrieve digital evidence; the downside of using forensics tools has been introduced in section 3.1.3.

The second challenge with conventional business forensics capabilities is that current businesses adopt a centralised information management style. This requires centralised e-discovery capabilities rather than a conventional forensics method. This trend can be demonstrated from the fact of increasing adoptions of centralised enterprise content management applications [59]. To collect evidence from these applications we need sophisticated forensics tools. That is the reason why many enterprise forensics experts desire the “perfect working together” situation among all enterprise applications, including line-of-business, applications and corporate business support systems, as well as litigation support platforms [61]. To achieve the “perfect working together” situation among all business applications, the first step is to develop the forensically sound application; details are further described in section 5.5. Despite the prediction of the “perfect situation”, more effort is still devoted to improve the current two forensics methods: static and live forensics.

5.2 Static Forensics Implementation in a Business Environment

Static forensics (SF) is a traditional and foundational acquisition approach to obtain evidential data from a halted system. The critical process of static forensics is to make a forensics image of the target storage and verify the copy with forensics mechanism such as the Hash function. SF challenges are triggered by new technologies such as Data Encryption.

Since 2007, researches started to address the issue that SF lacks “real-time” forensics capability which is critical for monitoring current network/enterprise environments and collecting evidence across various live business applications. In addition, SF’s post-mortem forensic techniques may cause significant disruption to the evidence gathering process by breaking active network connections and un-mounting encrypted disks [65].

5.2.1 SF Deficiencies

The first deficiency of SF evidence collection is that the traditional SF's pull-the-plug action sacrifices valuable potential evidence contained in the RAM. Potential evidence includes encryption secrets, running process information, active network connection information, hosts interactions, etc. Therefore, in a case when the volatile data is considered critical, a live forensics method should be applied.

The second deficiency challenge is from using data encryption, especially the Full Disk Encryption (FDE) function such as Microsoft Bitlocker, which protects the storage data from the sector level. FDE leaves three options for the forensics industry [63]. Firstly, using live forensics to analyse the target in real time may help obtain the passphrase in volatile storage; secondly, manage to obtain the passphrase in any means such as interviews or interrogations; thirdly, cooperation between forensics tool vendors and FDE function vendors to design forensics features in FDE software.

The third deficiency is that SF has trouble collecting evidence from a pervasive enterprise network; details have been introduced in section 3.1.3. The increasingly sophisticated network technology impacts the static forensics environment since there maybe data constantly written to the system from network and overwrites potential evidence in the process [64]. On the other hand, in an enterprise/network environment, forensics is more addressed on monitoring the business rather than post-mortem investigation of a cyber event. Therefore, businesses start to consider a newly forensics methodology – Network forensics, which is considered as a form of live investigation.

5.3 Live Forensics Implementation in a Business Environment

From the study of SF deficiencies, businesses and forensics industries believe Live Forensics (LF) overcomes the challenges of SF and is the next generation of the digital investigation method. Compared to static forensics which attempts to preserve all (disk) evidence in an unchanging state, LF seeks to take a snapshot of the state of the computer similar to a photograph of the scene of the crime [68]. In a narrow view, LF can be categorised as a memory forensics method. In board view, the live forensics definition is not standardised. According to [69], live forensics investigations refers to collections of dynamic and volatile data from live or production environments such as a network environment.

5.3.1 LF Challenges

The LF researches may underestimate the challenges to LF. Schwartz, E. (2010) [70] states that using specially designed tools are still the predominant method for live forensics investigators to gain a memory image as the first step in a live forensics investigation. Firstly, the overreliance on forensics tools is a significant issue, explained in chapter 3. Secondly, LF is not as simple as “gain a memory image”. It requires more sophisticated investigation methods for the complex business system.

In Carvey, H. and E. Casey’s work [71], the windows command lines are executed to gain volatile information from the Windows Operating System. To prevent a compromised Windows system forges the command line results, a live CD is used to avoid modification of the windows commands. Such implementation has one major attribute, which is using system built-in features to conduct system investigations, instead of using third party forensics tools. It has one challenge that these built-in features need to be designed and developed in a forensics manner, details are explained in later sections.

Another major live forensics type is network forensics which is applied mostly in an enterprise environment. Network forensics is mostly real-time based and “reconstructs the network events to provide definitive insight into the actions and behaviours of users,

devices, and applications” [70]. However, with the dynamic nature of an active network system, it is not feasible to collect the evidence that as consistent as by SF [72]. Network forensics may be able to “reconstruct” the network events, but it is not able to reproduce the evidence [68]. Thus, LF-collected evidence is reasonably questioned in term of Repeatability. Furthermore, according to Locard's principle that “the perpetrator(s) of a crime comes into contact with the scene, so the perpetrator(s) both bring something into the scene and leave with something from the scene” [71]. The live investigation action is a direct “contact with the (potential) crime scene”, and hence it may threaten the Integrity of the evidence.

In a business/network environment, current network forensics technology and operations focus more on incident response (case based), network real time monitoring, anti-malware and anti-virus analysis. These activities are more of a preventive and defensive solution to network crimes, while the actual purpose of the network forensics is against cybercrimes by real-time collecting admissible evidence and resorting to legal solutions. Due to short response time, the internal cyber investigators are not able to instantly respond with the external law enforcement cyber investigators [74]. Such lack of the cooperation with law enforcement may lead the business reluctant to pursue further litigation.

Even though LF overcomes some weaknesses of SF, it does not imply that LF should replace SF. Therefore, the current situation is using both methods and trying to work out the best forensics solution for the enterprise/network environment.

5.3.2 Hybrid Implementation of Both SF & LF in a Business Environment

Brown, C. L. T. (2010) [73] claims that “some investigators choose to take advantage of live forensics analysis for preview-and-cause justifications or long-term employee investigations and conduct a black bag operation to image a disk locally from a dead system based on the pre-investigation confirmation of suspicions”. This statement describes different roles of SF and LF in today's business environment.

With the real-time evidence collection, the business can make the judgment and decide the following actions. Also, with a successful LF, businesses can also identify the possible target of the following SF investigation. After all, the decision of contacting law enforcement authorities is determined by the organisation's management [74]. That means in case of an insufficient live evidence collection, the business may make the decision to turn an investigation event into a pure defensive network security event.

For instance, in a business cyber attack case, business decision makers decide whether to pursue a further legal action or simply mitigate the harm and restore the business process. Therefore, incident response is taking place, aiming to collect certain amount of initial materials to help make business decisions. These initial materials are provided through live forensics which is not required to shut down the entire business system. To make decisions is a complicated business procedure that is not concerned in this research. However, if the decision is made to take further legal action, more materials need to be collected, preserved and analysed. These further forensics actions should not affect the daily business progress. Therefore, businesses require the convenience of using forensics features in live situations. In this case, we suggest that a business should develop its own forensically sound application that contains forensics features.

To understand more about the LF/SF combination and evident collection issues, we refer *Case Study [75]* to provide a picture of a current enterprise digital crime investigation combined with “live forensics” and “static forensics”, followed by a discussion of a critical issue of current forensics investigation.

5.4 Case Study [75]

A disenchanted insider has authorised access to trade secrets. The victim organisation received notice from a business competitor that it had received communication from an unidentified individual offering information from the victim's organisation on a monthly basis in exchange for an ongoing financial stipend. The victim's organisation had all the standard protections in place to electronically monitor computer and network usage,

including network sensors that collected and analysed data transmitting throughout the environment, proxy servers to monitor Web activity, and data loss prevention products to monitor malicious behaviour on users' computers. Figure 5-1 shows the enterprise investigation action flow chart.

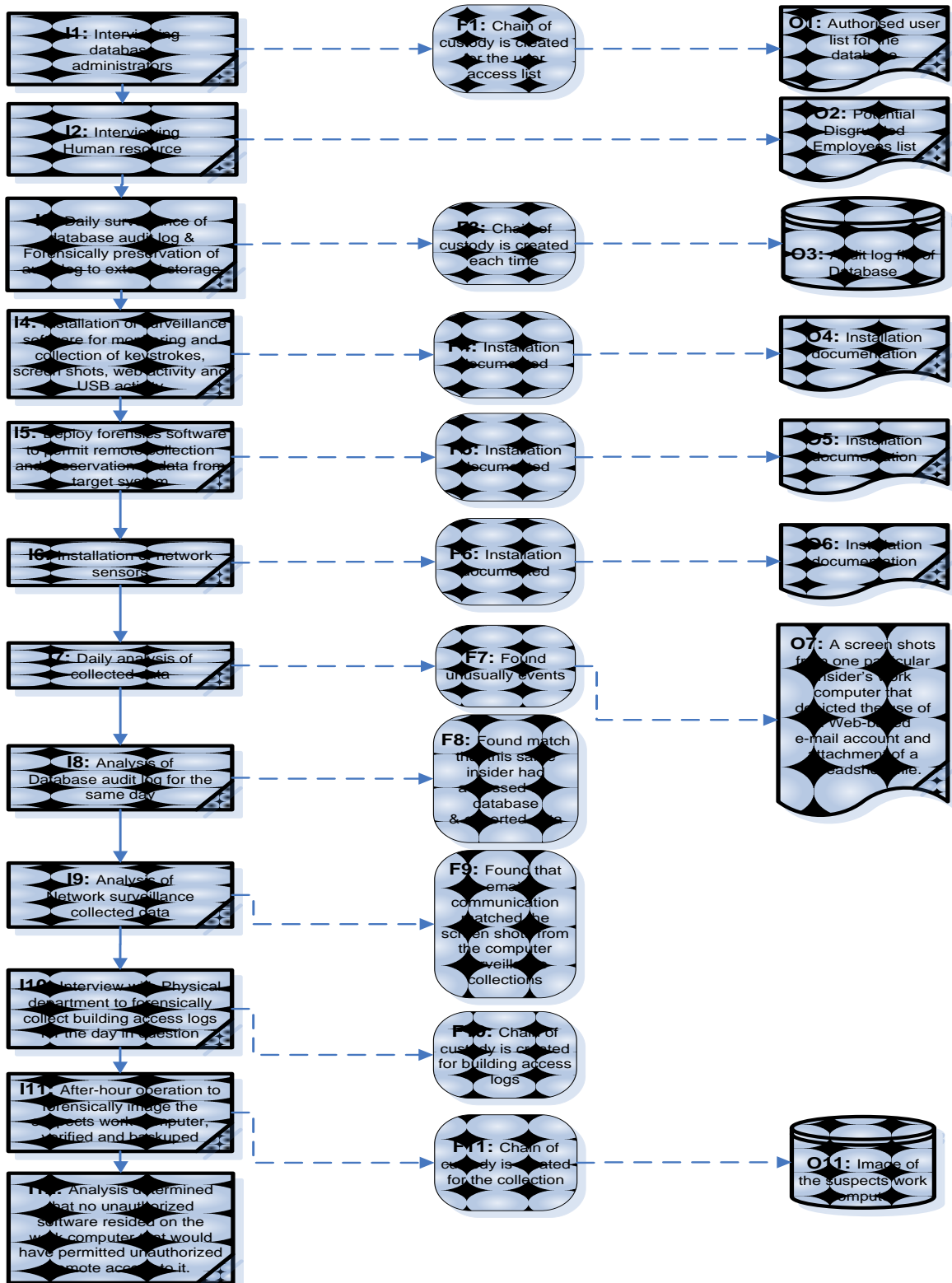


Figure 5- 1 Enterprise Forensics Action Flow Chart

This case study represents a typical corporate investigation against an inside threat. The flow chart simply shows (from the left column to right column): Investigation process (Ix), Forensics process (Fx), and the outcome of each step (Ox). From I1 to I10, are the LF processes, which involve forensics interviews, network surveillance and computer surveillance. Before I7, the investigators did not achieve much even with their daily monitoring data collection. In F7, there is an unusual event occurrence that triggers the following series of live investigation from I8 to I11. I11 is the result action taken by the likely-identification of the suspect and it is the part where SF is conducted.

The LF process has been taken in most of the investigation period to draw a possible conclusion, while the conventional SF is only taken as a final strike to get the storage evidence. However, we notice that the forensically sound processes, including four chains of custody created (F1, 3, 10, 11), have been taken since even the interview phase (starts from F1 to the end) in order to provide the admissibility of the collected outcome data (from O1 to O11). Unfortunately, process F2 is left non-existent since a “Potential Disgruntled Employees List” is not convincing enough to draw any forensics conclusions. Therefore, no action is taken except a normal documentational process for the “Disgruntled Employee List”.

5.4.1 Issues

The case study should provide seamlessly potential evidence to the court. Based on the situation, the court would accept the “potential evidence” as “court presentable evidence” by granting admissibility to them. However, from the perspective of our research, we like to address some issues from I4-F4-O4, I5-F5-O5 and I6-F6-O6, shown in Table 5-1.

Procedure & Outcomes		Issues	Forensically Sound Solution
I4	Installation of surveillance software for monitoring & collection of keystrokes, screen shots, web activity & USB activity	Only the installation process was forensically documented. Investigators fully trust that the software is developed and works in forensics manner.	Design and implementation of forensics features in daily used business applications such as email clients. Collected data required to be secured, verified and backup in a forensics manner. Chain of custody maybe provided.
F4	Installation documented		
O4	Installation documentation		
I5	Deploy forensics software to permit remote collection and preservation of data from the target system	Investigators fully trust that the software is developed and works in forensics manner.	Secure the remote control of the target in forensics manner; make sure the daily business data flow does not harm the integrity of data. Collected data required to be secured, verified and backup in forensics manner. Chain of custody must be provided.
F5	Installation documented		
O5	Installation documentation		
I6	Installation of network sensors	To some level, make change to the business network environment, network sensor need to be controlled to cause least affect on business, and forensics data.	Design and implement forensics features in network system so that it functions along side with daily business network.
F6	Installation documented		
O6	Installation documentation		

Table 5- 1 Issues of an Enterprise Forensics Action

The problems in these procedures are simply that only the “Forensics tool installation” processes are documented; the evidence of “transmitting secrets to unauthorised outsiders” is collected. However, the action is not completed in a forensics manner. Therefore, according to [75], the outcome of this investigation can only result in

termination of the employee, while “the victim organisation should choose to present the evidence to law enforcement for potential criminal action, law enforcement would be positioned to leverage forensically sound evidence that would withstand judicial scrutiny” [75].

5.5 Proposed Solution

In this chapter, we have introduced two mainstream forensics methods, and a case study of a business cybercrime situation. In this section, we propose forensically sound application (FSA) development as a new method, briefed in section 1.2.

5.5.1 “Forensics-Friendly Features” are NOT “Forensics Features”

The digital forensics targets include victim applications that relates to a cybercrime. Within these applications and systems, there are some features containing appreciable attributes that may help digital investigations. Examples of these features include: Windows built-in command in Windows Operating System [71], File Creation Time (FCT) and Modify Time (FMT) in Microsoft office documents, shown in Figure 5-2, Microsoft Windows OS built-in log file [77], history file, cookies and Temp Files in Web browsers [78] [88] and the list goes on. Providing convenience for forensics investigators, these features are referred as “Forensics-Friendly Features” [76]. However, they are not “Forensics Features”.

Forensics features are designed and developed with specific requirements from business/forensics and law enforcement. These requirements provide attributes (e.g. Tamper-Resistant) to these features that make them different from “Forensics-Friendly Features”. Currently, most of these forensics features can only be found in forensics tools, for example EnCase data acquisition implements a software write-block on all devices [64]. On the other hand, mainstream applications or operating systems are designed with other requirements in mind, for example user friendliness, performance, flexibility, expandability, and more recently security. They were not specifically designed according to forensics requirements.

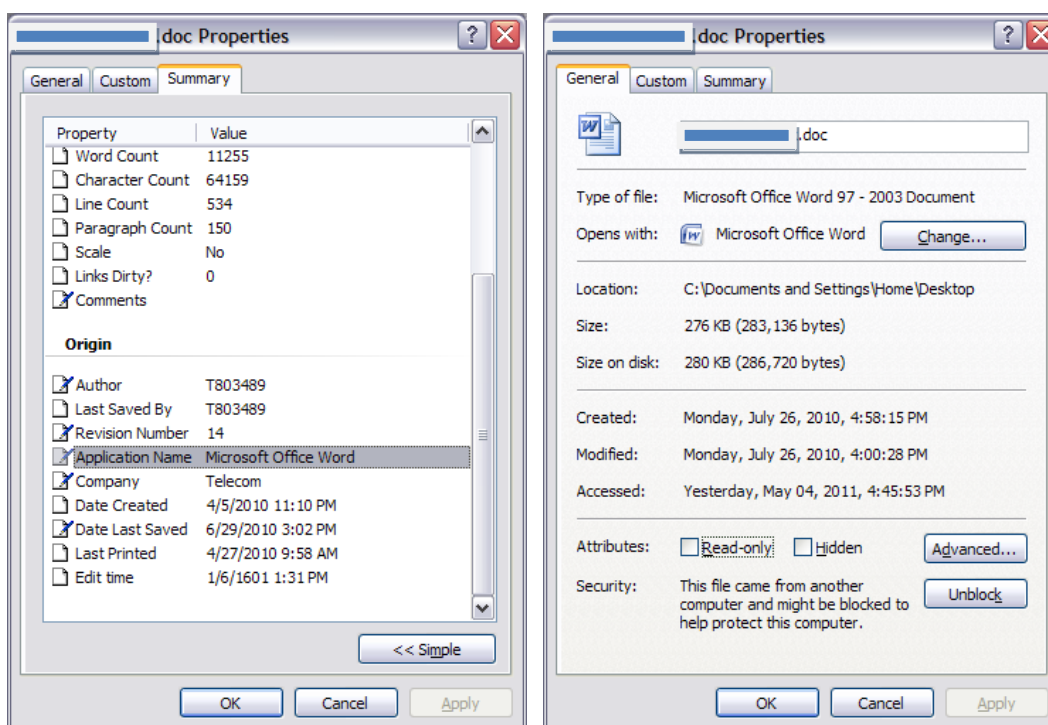


Figure 5- 2 FCT and FMT in Microsoft Office Documents

5.5.2 From “Forensics Requirements” to “Forensics Features”

An application with features that are designed with forensics requirements is a forensically sound application, which provides system-generated-material presented as evidence to stands in a court of law. Therefore, among all forensics requirements, the rules of evidence are the most critical one. The rules of evidence provide the criteria for evidential materials to be 1) qualified to be presented in the court, 2) have strong arguments. Therefore, “qualified to be presented in the court” (admissibility) is the precondition of all rules of evidence, shown in Table 4-4. To achieve admissibility, there are many attributes need to be applied. Among all attributes, Figure 5-3 uses “Integrity” as an example to show how a forensically sound application feature is developed.

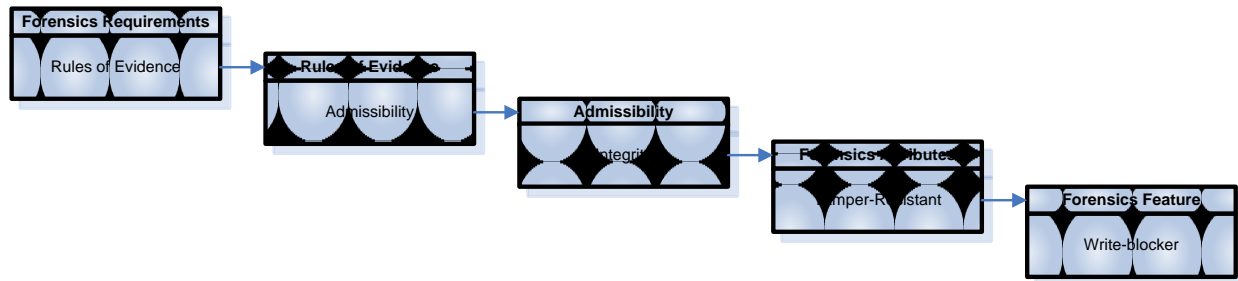


Figure 5- 3 Design Process of a Forensically Sound Application

With Figure 5-3, it is easy to explain why a Web browser is NOT a forensically sound application. Firstly, a Web browser provides the ability for all users to check the browsing history. The history features are equivalently accessible for forensics experts and other users (includes suspects). Secondly, the suspects are able to tamper with the history information that forensics experts are trying to reconstruct.

5.5.3 Designing and Developing Forensically Sound Applications for Businesses

With the change of the digital crime landscape, in the contextual layer, complying business/forensics requirements is compulsory. Designing forensics in an operational level means there should be business policies and regulations set up for enterprise investigation events which rely on forensics techniques, forensics tools and business applications with built-in forensics features.

By using the overlay, explained in chapter 4, we propose that developing a forensically sound application is equally important to using forensics investigation tools. In the requirement phase, we consider both business situations and forensics standards. In the design phase, we integrate forensics knowledge to business application design. In the implementation phase, we create forensics features according to the design.

The outcome of the entire development process is not only a piece of software, but also related documents for the business operation. These documents include Business Drive Table, Digital Evidence Attributes, Digital Evidence Threat List, and Organisational Policy to protect Digital Evidence, Forensics Services and Forensics Features (Mechanisms) to protect evidence, shown in Figure 5-4.

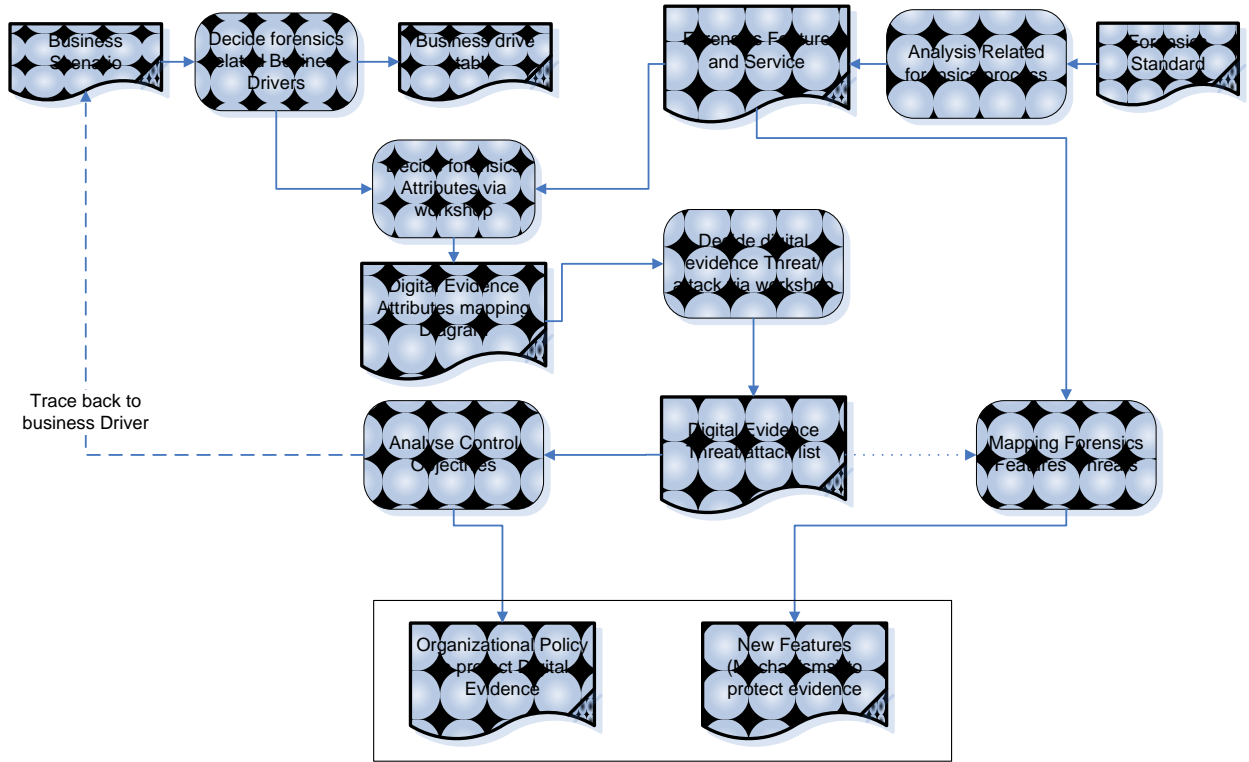


Figure 5- 4 High Level Design of Business Forensically Sound Application

To further extend the idea of forensically sound applications, we propose to build up the forensics concerns into all perspectives in an enterprise/network environment, depending on the business IT strategies, such as cloud computing or centralised content management. With raised business/forensics concerns and design, the future business should form a forensics culture and environment.

6 Design of a Forensically Sound Email Client with the Overlay

This chapter describes the implementation details of the experiments conducted for this thesis. There are two purposes of this experiment. Firstly, test the overall usability of the forensics overlay that was built based on the forensics knowledge and the SABSA matrix. Secondly, test the feasibility in developing a forensically sound email client. According to Figure 5-4, the overlay helps generate related documents for the email operation. In addition, this chapter focuses on designing forensics features for an email client.

Chapter Six:

6.1 Explains the role of the Email client as a testing platform

6.2 Describes the forensics process requirements for an email client

6.3 Demonstrates the key forensics features

6.4 Demonstrates the implementation code for a forensically sound email client

6.1 Email Client as a Testing Platform

The increasing malicious usage of email in a business environment has drawn the attention of business decision makers concerned about threats from organised crime targeting businesses' intellectual property [79]. During an electronic crime (e-crime) in business situations, the malicious business insider plays devastating roles through sending business secrets via emails. The current email system design is based on the server & client mode, performing the general function of sending and receiving forms of messages. However, as a mainstream business application, email clients are not design and developed with forensics concerns. There are limited forensics features within both client and server systems. Such situations result in forensics investigators having only two ways to gather evidence from emails. The first way is to locate the origin of an email that has been received. The second way is to gather email from an email server [80]. Both ways require great assistance through forensics tools. Also, there are no forensics mechanisms for message encryption and integrity check from the sender [81].

In a live forensics situation, it is practical for a forensics investigator to collect evidence from the suspect's email client, because it does not involve 1) demanding email evidence from an externally hosted email provider [82]; 2) accessing the company-owned servers, which has two drawbacks. Firstly, not many company-owned mail servers are designed with forensics features. That means an investigator may have to maintain the integrity of an entire mail server and prove it. Secondly, accessing mail servers against the business requirements "Minimise the impact on daily used systems during investigations", shown in Table 4-1. Thus, it is practical to initialise the investigation from the Email client's side (suspect's host) and it is critical to have forensics features built in the Email client.

6.2 Using the Overlay to Design Email Client Forensics Features

We apply the forensics overlay to design an email client that aims to facilitate a business environment free from e-crimes. The overlay outlines a software development lifecycle (SDLC) with its top-down layout. Through the process of understanding and implementing different cells in each layer, the forensics features can be listed in the Physical Process Cell. The cells that perform major tasks in SDLC are highlighted and connected to show the tractability of the forensics design, shown in Figure 6-1. With the connection of the highlighted cells, a typical forensics/business requirement should be able to find the related forensics features (controls). Figures 6-2 illustrates all highlighted cells and explains the process of mapping the overlay layers with SDLC.

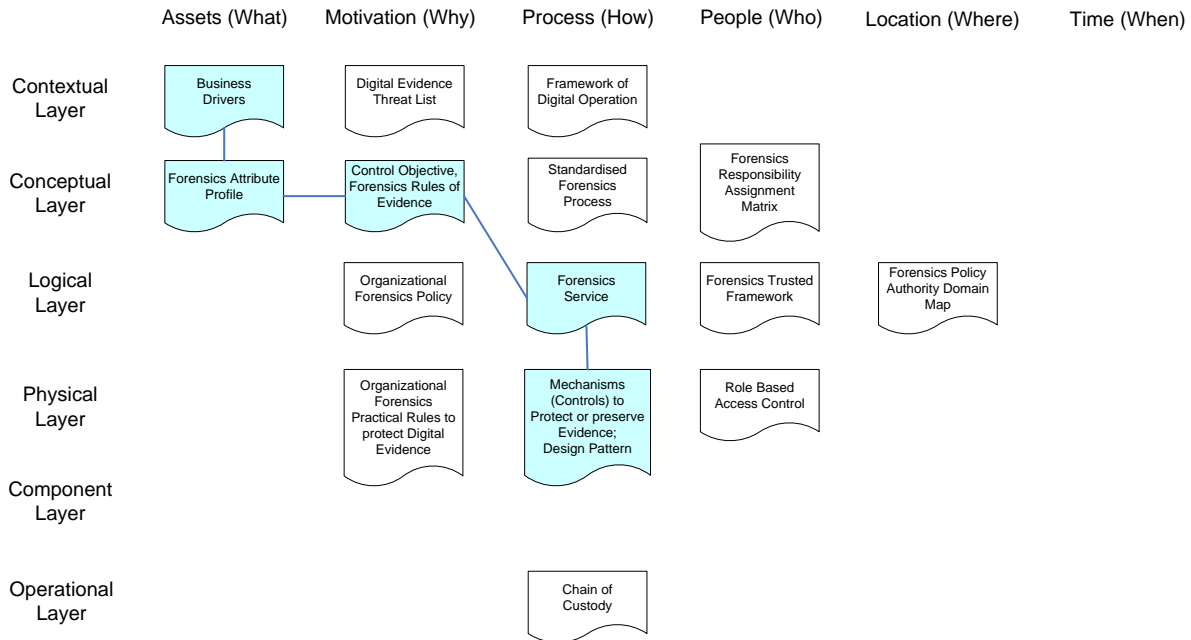


Figure 6- 1 Forensics Overlay Tractability

In Figure 6-2, business and forensics requirements are formed as a list of business drivers. The drivers (Table 4-1) are used to abstract the forensics attributes (Table 4-3 & 4-4). With the attributes, the design team is able to identify the forensics service within an enterprise environment, where business applications are widely used. Therefore, with different business applications, the forensics services should be applied. To achieve the forensics service, relevant forensics features (controls) need to be designed and implemented. Remaining cells in the overlay provide the support to the forensics management.

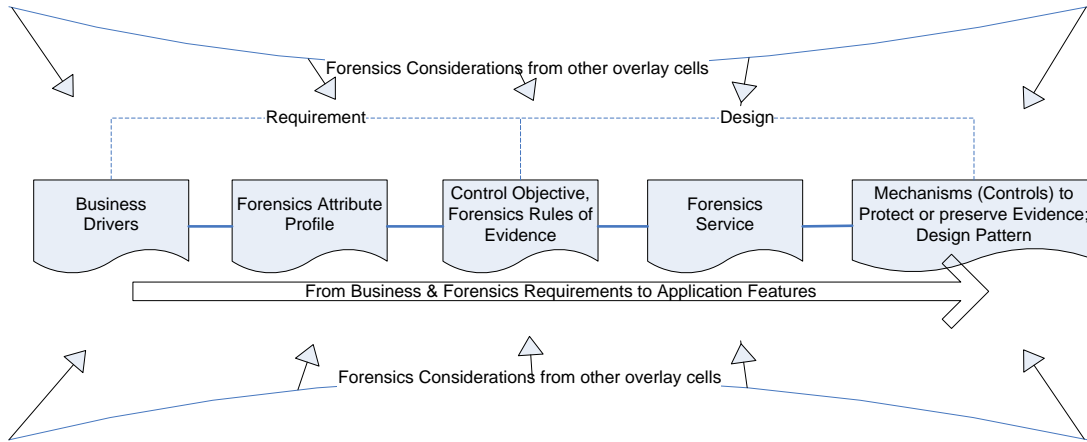


Figure 6- 2 Mapping the Overlay Layers with SDLC

6.3 Forensics Features for an Email Client

Following the process described in section 6.2; we present Table 6-1 to list all business/forensics requirements, attributes, controls, services, and features. Based on this Forensics Design Process table, all features are developed.

Business & Forensics Driver (FD)		Forensics Attributes	Objectives	Forensics Service	Forensics Control
FD15	Ensuring that the forensics architecture is independent of any specific vendor or product and is capable of supporting multiple products from multiple vendors.	Traceable	Traceability from business requirement to application forensics control	Using SABSA forensics overlay design email client for business	Physical process cell contains the consideration of forensics control contents
		Architecturally open	Using SABSA to design an email client instead of using vendor specified email client		
		Regulated	Email client designed, implemented, operated in accordance with the forensics regulations		
FD3	Maintaining the accuracy of information, especially those with potential evidential value.	Accurate	Maintaining the accuracy of sent email information	Forensics server for email client	Real time record when the Send button is clicked and HASH check for every Send button clicked
FD17	Providing a backup plan for business continuity when the system compromised or related to cybercrime.	Recoverable	Data stored in forensics server are recoverable		Forensics Back up function for the Forensics server
FD4	Providing the ability to prosecute those who attempt to defraud the business.	Admissible	Make sure the data in forensics server fulfil the requirements of admissibility	Forensics Reporting service	Hash function for sent email data forensics logs and service data storage
FD5	Enforcing the roles and responsibilities during a cybercrime investigation.	Accessible	Forensics investigators are able to access the sent email info	Forensics investigator interface	Account authentication
		Access-controlled	Accessibility needs to be controlled	Forensics investigator account	
		Accountable	Both Normal users and investigators are able to access email clients		
		Authenticated	Each party should have their identity verified		
		Authorised	Forensics investigator should be authorised by the law enforcement and the business owner		
					Forensics investigator detail record
					Search warrant detail record
FD6	Ensuring that information processed in the business system can be brought to a court of law as evidence in support of both criminal and civil proceedings and that the court admits the evidence, and that the evidence withstands hostile criticism by the other side's expert witness.	Integrity-assured	Integrity of sent email data should be protected to provide assurance of evidence admissibility.	The action of using email client is recorded and recorded data need to be hash protected	SHA1 function for forensics logs and service data storage
FD11	Ensuring that transaction between parties cannot be denied that a transaction occurred.	Non-repudiable	The sender are not able to deny the email sending action is taken by the account owner	User account locked up	Email account is bind to a locked account that cannot be changed (no from')
FD7	Minimising the number of incidence of cybercrime, highly offensive but not unlawful, breach of procedure, policy or inappropriate actions only.	Informed	Minimise the crime incidence to the lowest level by awareness of the forensics function	User Warning	Provide warning message to inform the users that the sent emails are recorded in forensics way
		Crime-free			

Table 6- 1 Forensics Design Process in Details

The major forensics features (controls) are:

- Real-Time Recording Email SENDING Event
- Forensically Backing up Email SENDING Records
- Structured Records
- Hash Function
- User Authentication and User Records
- Fixed Email Account
- Other Forensics Features

6.4 Implementation

In implementing the forensics feature development, we developed a simple email client with the basic function that sends emails through the Gmail Server. The code is constructed in C# language with the .NET platform.

6.4.1 Real-Time Recording Email SENDING Event

The email *SEND EVENT* is the initial moment of this Internet based transactions. An email sending related record is legitimately considered as a contractual acceptance by businesses and law enforcements. Therefore, strong forensically sound material of email sending provide arguable motive of the particular email sender.

Regular email client *SEND EVENT* (Table 6-2) includes 1) Setting up the host, defining client host, port number, status of using password (credential). 2) Getting Senders and receivers email addresses from the user interface. 3) Managing an Email message includes get Subject, Text Body and other relevant information. Email messages here are materials that have evidential value, if it is handled in a forensics way, and stored in a forensically sound file, or database. However, a regular *SEND EVENT* function does not protect and preserve Email messages. Meanwhile, some other evidentially valuable information such as Date & Time, Host Machine Info is not collected locally.

Table 6-3 shows a forensically sound sending event. It contains the code to keep an XML record of the email information (section 6.3.2 & 6.3.3) and hash function (section 6.3.4).

```
public void Sendmail(string sentTo, string sentFrom, string Subject,
string body)
{
    try
    {
        // Setup Host
        client.Host = "smtp.gmail.com";
        client.Port = 587;
        client.UseDefaultCredentials = false;
        client.Credentials = smtpcrds;
        client.EnableSsl = true;

        // Convert strings to Mailaddress
        MailAddress to = new MailAddress(sentTo);
        MailAddress from = new MailAddress(sentFrom);

        // Set up message settings
        msg.Subject = Subject;
        msg.Body = body;
        msg.From = from;
        msg.To.Add(to);

        // send email
        client.Send(msg);

        MessageBox.Show("Email Successfully sent from " +
        txtbxFrm.Text + " to " + txtbxTo.Text);
    }
    catch (Exception ex)
    {
        MessageBox.Show("Unable to send msg due to the
        following error: " + ex.Message);
    }
}
```

Table 6- 2 Sample Code 1 - Regular Email Sending Event

```

private void button1_Click(object sender, EventArgs e)
{
    Sendmail(txtbxTo.Text, txtbxFrm.Text, txtbxSub.Text,
    RTBoxMsg.Text);
}

private void XMLfile(string To, string From, string Subject, string
Body, string Time)
{
    XmlDocument xmldoc;
    XmlElement xmlelem;
    XmlText xto, xfrom, xsubject, xbody, xtime, xhash;
    xmldoc = new XmlDocument();
    xmldoc.Load(@"c:\logfile.xml");
    xmlelem = xmldoc.CreateElement("", "mail", "");
    XmlElement xto1 = xmldoc.CreateElement("To");
    XmlElement xfrom1 = xmldoc.CreateElement("From");
    XmlElement xsubject1 = xmldoc.CreateElement("Subject");
    XmlElement xbody1 = xmldoc.CreateElement("Body");
    XmlElement xtime1 = xmldoc.CreateElement("Time");
    XmlElement xhash1 = xmldoc.CreateElement("Hash");
    xto = xmldoc.CreateTextNode(To);
    xfrom = xmldoc.CreateTextNode(From);
    xsubject = xmldoc.CreateTextNode(Subject);
    xtime = xmldoc.CreateTextNode(Time);
    xbody = xmldoc.CreateTextNode(Body);
    string fullMessage = To + From + Subject + Body + Time;
    string hash = HashMessage(fullMessage, "internalstaff.smith1");
    xhash = xmldoc.CreateTextNode(hash);
    //xhash = xmldoc.CreateTextNode(HashMessage(To + From +
Subject + Body + Time, "mpp40"));
    xto1.AppendChild(xto);
    xfrom1.AppendChild(xfrom);
    xsubject1.AppendChild(xsubject);
    xtime1.AppendChild(xtime);
    xbody1.AppendChild(xbody);
    xhash1.AppendChild(xhash);
    xmlelem.AppendChild(xto1);
    xmlelem.AppendChild(xfrom1);
    xmlelem.AppendChild(xsubject1);
    xmlelem.AppendChild(xtime1);
    xmlelem.AppendChild(xbody1);
    xmlelem.AppendChild(xhash1);
    xmldoc.DocumentElement.AppendChild(xmlelem);
    //System.Environment.CurrentDirectory ??

```

```

try
{
xmlDoc.Save("c:\\logfile.xml"); //I've chosen the c:\ for the resulting
file pavel.xml
}
catch (Exception e)
{
Console.WriteLine(e.Message);
}
Console.ReadLine();
}

```

Table 6- 3 Sample Code 2 - Forensically Sound Email Sending

6.4.2 Forensically Backing up Email SENDING Records

The email record is kept in a XML structure and stored in C:\\logfile.xml, shown in Table 6-3. With security consideration, the records should be kept in a secure location remotely. This implementation focuses on forensics considerations; therefore, this feature only demonstrates a forensics design without security in mind. For future work, we propose that the email record should be kept in a remote storage in order to maintain the integrity of the evidence.

6.4.3 Structured Record

A structure log file is to make investigators' work easy so that normal functions such as "search" can be added later onto the XML log file. On the other hand, the forensics industry lacks a standardised evidential data format [28] [31] [32]. The XML format can be considered as a solution.

6.4.4 Hash Function

In Table 6-3, the code "*string hash = HashMessage(fullMessage, "internalstaff.smith1")*" demonstrates that the hashed function (*HashMessage*) is called to hash the full email message with the senders email account name. The *HashMessage* function code is shown in Table 6-4. The Hash function has two purposes; one is to create the hash value for full email messages for later evaluation. Second reason is the sender's email

account name is “salted” in the hash function so that the sender cannot deny that a transaction occurred if the hash values are identical.

```
private string HashMessage(string fullMessage, string username)
{
    // Add all content to one string
    string stringToConvert = username + fullMessage;
    // Convert string to data (bytes)
    var data = Encoding.ASCII.GetBytes(stringToConvert);
    // Create the hash - using SHA-256
    var hashData = new SHA256Managed().ComputeHash(data);

    // make an empty string
    var resulthash = string.Empty;

    // for each byte in the resulting hash, add to the string.
    foreach (var b in hashData)
    {
        //X2 is the Hexadecimal formatting for toString
        resulthash += b.ToString("X2");
    }

    return resulthash;
}
```

Table 6- 4 Sample Code 3 - Hash Function

6.4.5 User Authentication and User Record

The email client is used by both normal users and forensics investigators. Therefore, user authentication is required so that only investigators can access certain forensics functions, shown in Figure 6-3. Table 6-5 shows that the user account information are combined and applied with the SHA1 hash function.

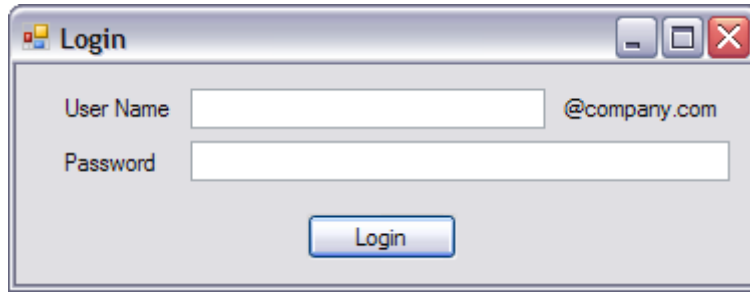


Figure 6- 3 User Authentication Interface

```
private bool checkInvestigatorCredential() // Check the Investigators  
Cred  
{  
    var PlaintextEnter = txtboxUserName.Text + txtBoxPwd.Text;  
    var InvestigatorData = Encoding.ASCII.GetBytes(PlaintextEnter);  
    var Credhash = new SHA1Managed().ComputeHash(InvestigatorData);  
    var resulthash = string.Empty;  
  
    foreach (var b in Credhash)  
    {  
        resulthash += b.ToString("X2");  
    }  
    return resulthash.Equals(investigatorCredentials);  
}  
  
private bool checkUserCredential() // Check the user's Credential  
{  
    var PlaintextEnter = txtboxUserName.Text + txtBoxPwd.Text;  
  
    var UserData = Encoding.ASCII.GetBytes(PlaintextEnter);  
    var UserDatahash = new SHA1Managed().ComputeHash(UserData);  
    var resulthash = string.Empty;  
  
    foreach (var b in UserDatahash)  
    {  
        resulthash += b.ToString("X2");  
    }  
    return resulthash.Equals(UserCredentials);  
}
```

Table 6- 5 Sample Code 4 - SHA1 Hash

The regular users have to login to use email functions. For investigators, additional information needs to be recorded; Figure 6-3 prompts an interface for investigators to enter the search warrant information. The importance of search warrants is described in [64].

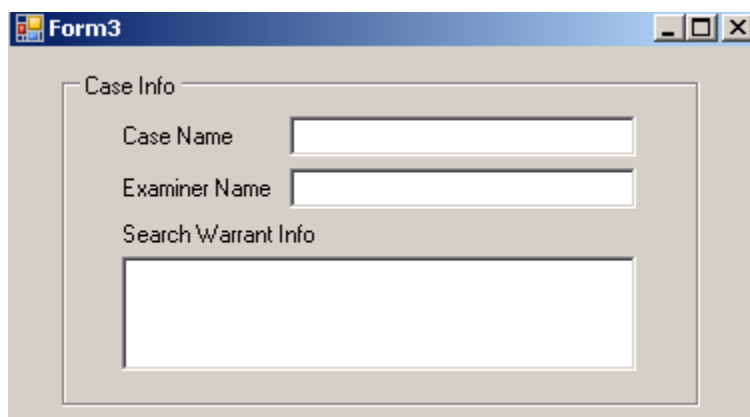
The image shows a screenshot of a Windows application window titled "Form3". The window has a standard Windows title bar with minimize, maximize, and close buttons. The main content area of the window is a form with a light gray background. The form is divided into two sections. The first section is titled "Case Info" and contains two text input fields: "Case Name" and "Examiner Name". The second section is titled "Search Warrant Info" and contains a large, empty text area for entering details.

Figure 6- 4 Search Warrant Information Enter

6.4.6 Fixed Email Account

Non-repudiation is one of the most important forensics attributes that should be maintained within an email sending process. It ensures that parties who made the email sending cannot deny that a transaction occurred. To ensure non-repudiation, the email client requires a group of features collect, maintain, and present the email sending materials in a forensics manner. In a forensically designed email client, the normal user account has already been fixed through the company policy. Therefore, the users do not need to type the sender's information. Figure 6-5 shows that the "From" tag has been greyed out for this feature.

The image shows a screenshot of a Windows-style window titled "Form2". The window has a standard title bar with minimize, maximize, and close buttons. Inside the window, there are three input fields for email headers: "To:" (empty), "From:" (containing the text "internalstaff.smith1@company.com"), and "Subject:" (empty). Below these fields is a large, empty text area labeled "Message". At the bottom center of the window is a "Send" button.

Figure 6- 5 Fixed Email User Account

6.4.7 Other Forensics Features

Other forensics features helps to provide a unique signature of the targeted computer where the evidence was collected. Figure 6-5 and Table 6-6 demonstrates the interface and sample code respectively. According to Figure 6-5, the target machine name is COSC964; Domain Name is UOCNT, etc.

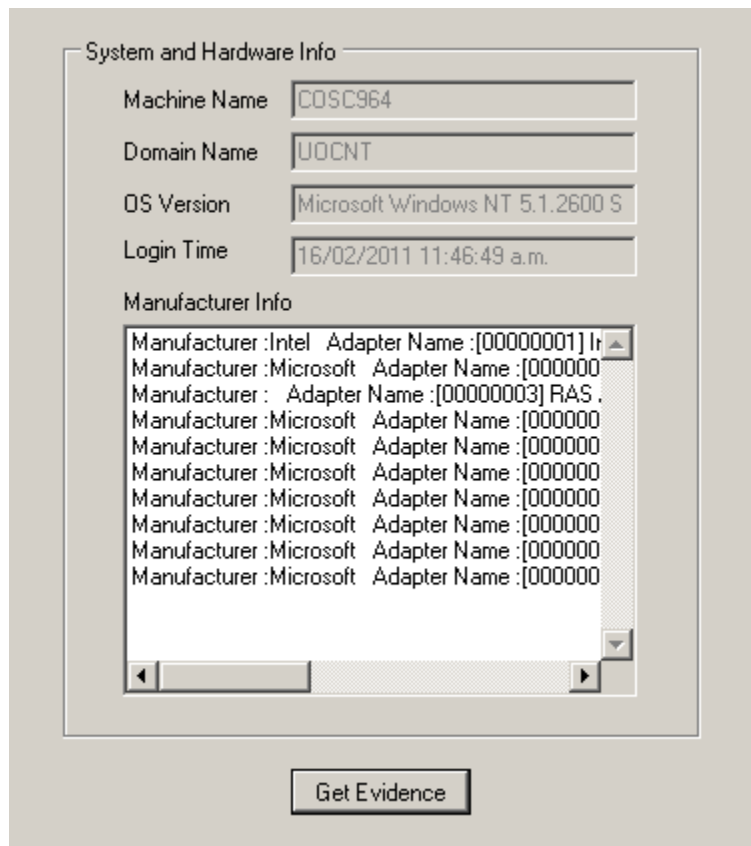


Figure 6- 6 Host Information Interface

```

private void GetSysInfo()
{
    DateTime time = DateTime.Now;
    txtboxHostname.Enabled = false;
    txtboxHostname.Text = System.Environment.MachineName;

    txtboxDomain.Enabled = false;
    txtboxDomain.Text = System.Environment.UserDomainName;

    txtboxOSversion.Enabled = false;
    txtboxOSversion.Text = System.Environment.OSVersion.ToString();

    txtboxLogintime.Enabled = false;
    txtboxLogintime.Text = time.ToString();
}

private void GetHardwareinfo()
{
    System.Management.ManagementClass ObjectiveClass = new
    System.Management.ManagementClass("Win32_NetworkAdapter");
    foreach(System.Management.ManagementObject objMgmt in
    ObjectiveClass.GetInstances())
    {
        lstBoxManuinfo.Items.Add(
        "Manufacturer :" + objMgmt["Manufacturer"] + " " +
        "Adapter Name :" + objMgmt["Caption"] + " " +
        "MAC Address :" + objMgmt["MACAddress"]);
    }
}

```

Table 6- 6 Sample Code 5 - Host Information

7 Conclusion

This chapter concludes this thesis and introduces future works. In the future works section, we focus on the improvement of the forensics overlay and the future implementation of the forensically sound application development.

Chapter Seven:

7.1 Summarises the Thesis

7.2 Describes Future Works

7.1 Summary

Current business/forensics environments require a comprehensive model that covers business/forensics decision making, processing, and enhancing capability. The new model is built through a combination of digital forensics knowledge and an enterprise security model - SABSA. This thesis describes the process of construction of the new model – The Forensics Overlay.

The thesis also describes the current digital forensics trends in an enterprise/network environment and argues that developing a forensically sound business application is a solution to deal with enterprise forensics, rather than the overreliance on forensics tools.

To test the usability of the forensics overlay, this thesis demonstrates the process of using the overlay to assist a forensically sound email design and development.

7.1.1 Results of a Forensically Sound Email Design

The result from the email client design indicates that the overlay layers are easily mapped into the system development lifecycle (SDLC). The connection between layers forms seamless traceability from business/forensics requirements to business/forensics features. The other cells in the overlay provide an overall picture for senior executives to understand the forensics projects in relevant levels.

The contents in each cell of the overlay focuses on the later software development process. Therefore, not all original SABSA cells are addressed since some have strong focus on business cases.

The design process follows the simple waterfall SDLC model. In the requirement phase, the overlay's contextual layer is used, mainly with the contextual asset cells containing the forensics/business drivers. The collection of the selected drivers helps prevent related email client cybercrimes and helps the evidence collection after a cyber incident has occurred. The overlay only provides the forensics requirements and may possibly ignore the issues of security and privacy. Therefore, further development is needed to create a practical application.

In the design phase, the overlay's conceptual, logical and physical layer is used to generate the application features according to the outcome of the contextual layer. The design phase not only determines the forensics features but also generates the related documentation of the application's forensics attributes, forensics services and forensics controls. The outcome of the forensics features are derived from the contextual layer's requirements. Therefore, these features contain functions only related to forensics. For example, the email client forensically saves the email contents in a XML structure locally, which is not as secure as saving the XML file in remote forensics data storage.

Compared with other forensics models, the overlay focuses on 1) initial business requirements; 2) traceability design; and 3) forensics concerns.

7.1.2 Result of a Forensically Sound Email Development

In a live forensics situation, the forensically sound email generates materials that fulfill the rules of evidence. Two evidence files are either available for live forensics in a crime scene or their copies can be made available for static forensics. These two evidence files are one XML file which contains all email contents, and one text file which contains the investigators information, search warrant information, the target system and hardware manufactory information. Compared with Microsoft Outlook, this email client has three major advantages. First, both files are secured by hash functions so that even with live investigation, the file integrity is maintained. Second, one of the files that contain the email contents is structured in an XML format. It is a standardised file format which is considered as the next generation evidential file format [34]. Third, this email client has separate accounts for regular users and digital investigators; this increases the authenticity and reliability of the evidence. More details about this email client are explained through the four major rules of evidence: *admissibility*, *authenticity*, *integrity*, and *reliability*.

Admissibility

Evidence is collected including the investigators' details and search warrant information. It proves that the evidence is retrieved by qualified forensics investigators. All details are hashed and kept in the local storage. When static forensics is later applied in a forensics lab, forensics tools are able to retrieve this file as additional evidence that testify the legitimacy of the investigation process.

The search warrant information is bound with the investigation case ID, investigators' name, and the email account to avoid the investigation to pass beyond the scope of its search warrant.

Authenticity

Compared with normal email clients, the forensically sound email client has two accounts: the normal user login and the investigator login. These two accounts are isolated and dedicated to different tasks. Both accounts are protected by an authentication method. In the evidence file, both accounts are bound with the full email message and the hash function is applied. Therefore, any forged data should be disclosed by comparing the hash values. The target system and hardware manufactory information are also collected as additional evidence to prove the source of the evidence.

Integrity

The evidence integrity is maintained by all hash functions. There are two major hash functions applied in the email client. Firstly, the hash function is applied to a collective message of Email Receivers, Email Senders, Email Body and Sent Time/Date. In addition, the email account name is hashed with the above collective messages. The hash value of this message is stored in one XML node. Therefore, the integrity of email contents is maintained. Secondly, evidence files which contain the target system and hardware manufactory information and investigator's information, are hashed results in recording the hash value in a local text file.

Reliability

The evidence collection features is contained in the Email Sending Event. It is a live evidence collection process by a single click of the SEND button. All records are kept in an XML form and hashed to keep intact. These records are later collected by investigators when necessary.

7.2 Future Works

Both the overlay and the concept of the forensically sound feature (FSF) need to be constantly updated with current forensics knowledge and the changing business IT environment. Future works should be carried out in the following three areas. 1) Additional development of the forensics overlay for a single forensically sound application development. 2) With businesses moving into a standardised platform for content management, the overlay development should focus on a forensically sound business environments and not a forensically sound application development. 3) Some businesses are moving into the cloud environment, therefore, the overlay development should also focus on: helping forensics-minded businesses address the cloud/forensics requirements in the service level agreement with cloud vendors; or helping forensics-minded cloud vendors to understand and design forensics features in their cloud applications.

7.2.1 Additional Development for the Forensics Overlay

Focusing on General Business/Forensics Issues

The current forensics overlay attempts to solve the issues in a forensically sound application development. Therefore, more software development issues are addressed in the existing cells. Additional development of the overlay should avoid the focus on software development issues. Instead, the future overlay should concentrate on forensics related business projects.

Populating Overlay Cells

Some cells are left blank since they provide less help on software development. The future overlay should find out the business/forensics emphasis that is related to the intention of these cells. For example, the Physical Time Cell may address the digital evidence collection order with different types of data storage. In this case, more volatile data needs to be collected earlier than those less volatile.

7.2.2 A Future Development for FSFs

FSFs for Business Content Management

Due to the urge of centralised business content management [61], businesses are gradually integrating all their diverse applications into one single standardised platform, for example, using Microsoft Sharepoint as a business content management application. Forensically sound features (FSF) design is impacted by this trend in both a negative and positive way. Negatively, the complexity is higher than designing forensics features into one small scaled application such as an Email client. On the bright side, a standardised platform reduces the time and effort of the data search and data flow since an organisation's important business data is located in a single location [84]. In this case, it is easier for FSF to perform discovery functions to a single data location in the forensics manner.

The Forensics Library for Software Development

The security library benefits our forensically sound email development. For example hash functions are coded through a simple link with using "*System.Security.Cryptography*"; email sending functions are coded via "*System.Net.Mail*"; XML file management is coded via "*System.Xml*". The future programming language and platform should have the similar library for forensics programming. These future forensics libraries may contain built-in functions such as bit-by-bit copying, evidence file management, etc.

7.2.3 A Future Overlay for Cloud Computing

The adoption of digital forensics in the emerging core business technologies such as cloud computing and virtualisation infrastructures is a popular topic around this industry [85]. It is arguable that should a business address the forensics requirements to a cloud vendor [89] (Situation One), or should a cloud vendor develop a forensically sound cloud environment for the business (Situation Two). Our discussion about future overlay focuses on situation two. However, in either situation the overlay should be updated accordingly. After all, if a business accesses their data from the cloud environment, simply performing digital investigation from the cloud client side is impractical. The cybercrime investigation requests the collaboration of both business units and the cloud vendors.

In situation one, the first three layers of the overlay are more significant since they are meant to address the Service Level agreement (SLA) between businesses and cloud vendors [86] [89]. However, the current top concern of cloud service is still security [87]. Therefore, the forensics-minded organisation may not find that the forensics services are implemented as sophisticated as security services.

Contextual, Conceptual and Logical Layers

In situation two, the cloud vendors spontaneously designs forensics features into the cloud service. In this case, the forensics overlay for the cloud need to address the clouds vendor's business/forensics requirements in the contextual, conceptual and logical layers. Researches in this area fall short.

Physical Layers

For the overlay's physical layers, some recent researches express the forensics concerns in two areas: 1) building a forensics tunnel to provide forensics as a service [89]; 2) securing the cloud data provenance [90];

Firstly, building a forensics tunnel for the cloud client opens the accessibility to gain potential evidence. This raises the challenge on how to secure the tunnel. The same security challenge of the tunnel also affects the evidence that have been collected through using the tunnel. In addition, client-side usage of the forensics tunnel increases the risk to the entire cloud environment. Researches propose that a cloud vendor should only outsource its computation ability but not outsource cloud controls [91].

Secondly, securing the provenance of the data protects the cloud evidence from the original location where evidence was generated. The research [90] discusses security mechanisms to protect the cloud data. However, the mechanisms are developed based on the requirements of confidentiality, integrity and authenticity which are conventional security requirements but not forensics requirements. This may raise the future cloud forensics researches' concerns on how to balance the forensics and security elements in a cloud environment. Some researches provide practical examples of using security mechanisms to achieve forensics services. In [92], a model is developed to protect Hospital Information System in the cloud. The model provides four functions to manage the cloud data - Authentication, Access Control, Authorisation, History and Data Logging. The first three functions are security related, but integrated well with an overall forensics purpose.

Currently, there are ongoing researches focusing on technical model and mechanisms development for cloud forensics. These researches are catergorised in the overlay's physical layer. Additional research is expected to focus on the Contextual, Conceptual and Logical Layers. These researches are vital for cloud vendors to understand forensics on a strategical level as well as designing forensics into cloud policy and provide forensics services in a logical level.

Bibliography

- [1] Barrett, D. and G. Kipper (2010). Virtualization Challenges. Virtualization and Forensics - A Digital Forensics Investigator's Guide to Virtual Environment. S. Liles. Burlington, Elsevier Inc.: p175-180.
- [2] Barrett, D. and G. Kipper (2010). Cloud Computing and the Forensics Challenges. Virtualization and Forensics - A Digital Forensics Investigator's Guide to Virtual Environment. S. Liles. Burlington, Elsevier Inc.: p197-200.
- [3] Reyes, A. and J. Wiles (2007). Developing an Enterprise Digital Investigative/Electronic Discovery Capability. The Best Damn Cybercrime and Digital Forensics Book Period. Burlington, Syngress Publishing, Inc. & Elsevier, Inc.: p83-90.
- [4] Pollitt, M. (2010). A History of Digital Forensics. Advances in Digital Forensics VI Sixth IFIP WG 11.9 International Conference on Digital Forensics, Hong Kong, China.
- [5] Golden G. Richard, I. and V. Roussev (2006). "Next-Generation Digital Forensics." Communications of the ACM **49**(2): p76-80.
- [6] Lyle, J. and S. Ballou (2003, 20/08/2003). "Computer Forensics Tool Testing Program." Retrieved 24 Oct, 2010, from www.cfft.nist.gov.
- [7] McKemmish, R. (2008). "When is Digital Evidence Forensically Sound? ." IFIP Internatinal Federation for Information Processing **285**: p3-15.
- [8] Sherwood, J., A. Clark, et al. (2005). Enterprise Security Architecture - A Business Driven Approach. San Francisco, CMPBooks.
- [9] Du, Y. and M. Shore (2010). "An End-to-End Framework For Survivable NGNs." Synthesis Journal **1**(3): p31.

- [10] Lynas, D. and M. Shore (2010). "The SABSA Cybersecurity Solution." Retrieved 3 March, 2011, from www.alctraining.com/pdf/Cybersecurity_Solution_NA.pdf.
- [11] Wu, H., W. Chen, et al. (2010). Securing Cookies with a MAC Address Encrypted Key Ring. 2010 Second International Conference on Networks Security, Wireless Communications and Trusted Computing. Wuhan, HuBei, China, IEEE. 2: p62 - 65.
- [12] Volonino, L. (2003). Computer Forensics and Electronic Evidence. Americas Conference on Information Systems (AMCIS), AIS Electronic Library (AISeL).
- [13] Iwata, E. (2002, 18 Feb). "Enron case could be largest corporate investigation." Retrieved 14 March, 2011, from <http://www.usatoday.com/tech/news/2002/02/19/detectives.htm>.
- [14] Sherwood, J., A. Clark, et al. (2009) SABSA White Paper - Enterprise Security Architecture.
- [15] Sherwood, J., A. Clark, et al. (2005). A Systems Approach. Enterprise Security Architecture - A Business Driven Approach. San Francisco, CMPBooks: p55-56.
- [16] Sherwood, J., A. Clark, et al. (2005). Measuring Return on Investment in Security Architecture. Enterprise Security Architecture - A Business Driven Approach. San Francisco, CMPBooks: p79-80.
- [17] Albert J. Marcella, J. and D. Menendez (2008). Cyber Forensics and the Law: Legal Considerations. Cyber Forensics. Boca Raton, Auerbach Publications : p267-268.
- [18] Casey, E. (2010). Electronic Discovery. Handbook of Digital Forensics and Investigation. J. O. Holley, P. H. Luehr, J. R. Smith and J. J. S. IV. Burlington, Elsevier Inc.: p85-86.

- [19] Casey, E. (2010). Intrusion Investigation. Handbook of Digital Forensics and Investigation. E. Casey, C. Daywalt and A. Johnston. Burlington, Elsevier Inc.: p179-180.
- [20] Hayes, D. R. and S. Qureshi (2008). A framework for computer forensics investigations involving Microsoft Vista. Systems, Application and Technology Conference. Farmingdale, NY IEEE: p1-8.
- [21] Joyce, R. A., J. Powersa, et al. (2008). "MEGA: A tool for Mac OS X operating system and application forensics." Digital Investigation **5**(1): p83-90.
- [22] Hejazi and S. Mahmood (2009). Analysis of Windows memory for forensic investigations, Concordia University (Canada): p124-126.
- [23] Chan, E., W. Wan, et al. A Framework for Volatile Memory Forensics. Urbana, University of Illinois.
- [24] Sean, P., B. Matt, et al. (2007). Toward Models for Forensic Analysis. Second International Workshop on Systematic Approaches to Digital Forensic Engineering Bell Harbor, WA IEEE.
- [25] Ami-Narh, J. T. and P. A. H. Williams (2008). Digital forensics and the legal system: A dilemma of our times. Australian Digital Forensics Conference. Perth, Western Australia, School of Computer and Information Science, Edith Cowan University.
- [26] Shore, M. and X. Deng (2010). Architecting Survivable Networks Using SABSA. Wireless Communications Networking and Mobile Computing (WiCOM). ChengDu, IEEE Xplore: p1-2.

[27] Crowley, E. (2007). "Corporate forensics class design with open source tools and live CDS." Computing Sciences in Colleges **22**(4): p170-172.

[28] Cross, M. (2008). The Evolution of Cybercrime. Scene of the Cybercrime Burlington, Syngress Publishing, Inc., Elsevier, Inc. : p44-48.

[29] Malkin, G. (1993). "Internet Users' Glossary." Network Working Group Request for Comments (RFC):1392. Retrieved 20 March, 2011, from <http://www.ietf.org/rfc/rfc1392.txt>.

[30] Brenner, S. W. (2010). From Mainframes to Metaverse: The Origins and Evolution of Cybercrime. Cybercrime - Criminal Threats from Cyberspace. Santa Barbara, Praeger: p9-11.

[31] Pollitt, M. (2010). A History of Digital Forensics. Advances in Digital Forensics VI Sixth IFIP WG 11.9 International Conference on Digital Forensics, Hong Kong, China.

[32] Garfinkel, S. L. (2010). "Digital Forensics Research: The Next 10 Years." Digital Investigation **Volume 7**(Supplement 1): p64-73.

[33] Reith, M., C. Carr, et al. (2002). "An Examination of Digital Forensic Models." International Journal of Digital Evidence **1**(3).

[34] Golden G. Richard, I. and V. Roussev (2006). Next-generation digital forensics. Communications of the ACM, AMC. **49**: p76-80.

[35] Bunting, S. (2008). The Official EnCE® : EnCase® Certified Examiner Study Guide Second Edition. Acquiring Digital Evidence. S. Bunting. Indianapolis, Indiana, Wiley Publishing, Inc. : p165-166.

[36] OECD (2009). Online Identity Theft. Conclusions and Recommendations, Organization for Economic Cooperation and Development: p137-138.

[37] Wright, C., B. Freedman, et al. (2008). Information Systems Legislation. The IT Regulatory and Standards Compliance Handbook: How to Survive and Information Systems Audit and Assessments. Kendall, SYNGRESS: p609-611.

[38] Sherwood, J., A. Clark, et al. (2005). Measuring Return on Investment in Security Architecture. Enterprise Security Architecture Computer Security Institution: p85-86.

[39] Casey, E. (2004). Investigating Computer Intrusions. Digital Evidence and Computer Crime: Forensics Science, Computers, and the Internet. San Diego, California, Elsevier Academic Press.

[40] Ghosh, S. and E. Turrini (2010). Spurring the Private Sector: Indirect Federal Regulation of Cybersecurity in the US. Cybercrimes: A Multidisciplinary Analysis. S. Baker and M. Schneck-Teplinsky. Berlin, Springer: p256-257.

[41] Volonino, L. and I. Redpath (2010). Processing, Filtering, and Reviewing ESI. e-Discovery for Dummies. Indianapolis, Indiana, Wiley Publishing, Inc.: p145-147.

[42] Wright, C., B. Freedman, et al. (2008). Evolution of Information Systems. The IT Regulatory and Standards Compliance Handbook: How to Survive and Information Systems Audit and Assessments. Kendall, SYNGRESS: p28-29.

[43] Vacca, J. R. (2005). Evidence Collection and Data Seizure. Computer Forensics - Computer Crime Scene Investigation. Boston, Massachusetts, CHARLES RIVER MEDIA, INC.: p220.

[44] Cardwell, K., K. O'Shea, et al. (2007). E-mail Forensics. The Best Damn Cybercrime and Digital Forensics Book Period. Burlington, MA, Syngress Publishing, Inc. & Elsevier, Inc.: p598-602.

[45] Brady, K. F., C. R. Crowley, et al. (2008). The Sedona Conference Commentary on ESI Evidence & Admissibility. Sedona Conference, The Sedona Conference Working Group.

[46] Reyes, A. and J. Wiles (2007). Developing an Enterprise Digital Investigative/Electronic Discovery Capability. The Best Damn Cybercrime and Digital Forensics Book Period. Burlington, Syngress Publishing, Inc. & Elsevier, Inc.: p83-84.

[47] Sherwood, J., A. Clark, et al. (2005). Security Architecture Model. Enterprise Security Architecture - A Business Driven Approach. San Francisco, CMPBooks: p42-50.

[48] National Institute of Justice and Office of Justice Programs (2001). Electronic Crime Scene Investigation: A Guide for First Responders. Washington, National Institute of Justice.

[49] International Organization on Computer Evidence (2002). Guidelines for Best Practice in the Forensic Examination of Digital Technology, International Organization on Computer Evidence: p1-24.

[50] Ashcroft, J., D. J. Daniels, et al. (2004). Forensic Examination of Digital Evidence: A Guide for Law Enforcement. Washington, National Institute of Justice (NIJ): p1-91.

[51] Wilkinson, S. Good Practice Guide for Computer-Based Electronic Evidence, Association of Chief Police Officers (ACPO) p1-72.

[52] Kent, K., S. Chevalier, et al. (2006). Guide to Integrating Forensic Techniques into Incident Response Recommendations of the National Institute of Standards and Technology. Gaithersburg, U.S. Department of Commerce, Technology Administration & National Institute of Standards and Technology (NIST): p1-121.

[53] King, G. L. (2006). Forensics Plan Guide, SANS Institute: p1-172.

[54] Jansen, W. and R. Ayers (2007). Guidelines on Cell Phone Forensics. Recommendations of the National Institute of Standards and Technology. Gaithersburg, Computer Security Division, Information Technology Laboratory & National Institute of Standards and Technology (NIST): p1-104.

[55] Ghosh, A. (2007). Guidelines for the Management of IT Evidence, Security and Identification Technology: p1-35.

[56] Mukasey, M. B., J. L. Sedgwick, et al. (2008). Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition. Recommendations of the National Institute of Standards and Technology. Gaithersburg, U.S. Department of Justice, National Institute of Justice (NIJ) & Office of Justice Programs: p1-121.

[57] U.S. Department of Justice, Federal Bureau of Investigation & National Program Office. (2007). Digital Evidence Field Guide: What Every Peace Officer Must Know. Quantico, Regional Computer Forensics Laboratory.

[58] International Organization for Standardization (ISO) (2010). Guidelines for Identification, Collection, and/or Acquisition and Preservation of Digital Evidence, International Organization for Standardization (ISO).

[59] Hoeken, H. (2001). "Anecdotal, Statistical, and Causal Evidence: Their Perceived and Actual Persuasiveness " Argumentation **15**(4): p425-437.

[60] Schuler, K. (2009). Managing Information and Records in An Enterprise E-discovery: Creating and Managing an Enterprisewide Program - A Technical Guide to Digital Investigation and Litigation Support. C. Peterson and E. Vincze. Burlington, Syngress Publishing, Inc. & Elsevier, Inc.: p23-37.

[61] Schuler, K. (2009). Trends in Enterprise E-discovery from the Corporate Perspective. E-discovery: Creating and Managing an Enterprisewide Program - A Technical Guide to Digital Investigation and Litigation Support. C. Peterson and E. Vincze. Burlington, Syngress Publishing, Inc. Elsevier, Inc.: p10-15.

[62] Pollitt, M. M. (1995). Principle, Practices, and Procedures: An Approach to Standards in Computer Forensics. Second International Conference on Computer Evidence. Baltimore: p1-6.

[63] Casey, E. and G. J. Stellatos (2008). "The Impact of Full Disk Encryption on Digital Forensics." ACM SIGOPS Operating Systems Review **42**(3): p93-98.

[64] Bunting, S. (2008). First Response. The Official EnCE® : EnCase® Certified Examiner Study Guide Second Edition. S. Bunting. Indianapolis, Indiana, Wiley Publishing, Inc.: p98-99.

[65] Chan, E., S. Venkataraman, et al. (2010). Forenscope: A Framework for Live Forensics. Annual Computer Security Applications Conference 2010. Austin, ACM: p6-10.

[66] Huebner, E. and F. Henskens (2008). "The Role of Operating Systems in Computer Forensics." ACM SIGOPS Operating Systems Review **42**(3): p1-3.

[67] Monteiro, S. D. S. and R. F. Erbacher (2008). "An Authentication and Validation Mechanism for Analyzing Syslogs Forensically." ACM SIGOPS Operating Systems Review **42**(3): p41-50.

[68] Adelstein, F. (2006). "Live forensics: Diagnosing Your System without Killing it First." Communications of The ACM (CACM) **49**(2): p63-66.

[69] Deriving cse-specific live forensics investigation procedures from FORZA.pdf

[70] Schwartz, E. (2010). Network Packet Forensics. CyberForensics - Understanding Information Security Investigation. J. Bayuk. Hoboken, NJ 07030, USA, Humana Press: p85-101.

[71] Carvey, H. and E. Casey (2009). Windows Forensic Analysis DVD Toolkit 2E. Burlington, MA, Syngress Publishing, Inc.

[72] Zhang, L., D. Zhang, et al. (2010). Live Digital Forensics in a Virtual Machine. Computer Application and System Modeling (ICCASM). Taiyuan, IEEE: p328-332.

[73] Brown, C. (2010). Imaging Methodologies. Computer Evidence: Collection and Preservation. Boston, MA 02210, USA, Course Technology: p287-289.

[74] Ehuan, A. (2010). Cybercrime and Law Enforcement Cooperation. CyberForensics - Understanding Information Security Investigation. J. Bayuk. Hoboken, Humana Press: p129-139.

[75] Sims, S. (2010). Insider Threat Investigations. CyberForensics - Understanding Information Security Investigation. J. Bayuk. Hoboken, Humana Press: p45-51.

[76] McDonald, T., Y. C. Kim, et al. (2008). "Software Issues in Digital Forensics." ACM SIGOPS Operating Systems Review **42**(3): p29-40.

[77] Fan, Y. and S. Wang (2010). Intrusion Investigations with Data-Hiding for Computer Log-File Forensics. 5th International Conference on Future Information Technology (FutureTech) IEEE Xplore: p1-6.

[78] David Martin, H. W., and Adil Alsaïd (2003). "Hidden Surveillance by Web Sites: Web Bugs in Contemporary Use." Communication of The ACM **46**(12): p258-264.

[79] Burgess, C. and R. Power (2008). Secrets Stolen, Fortunes Lost: Preventing Intellectual Property Theft and Economic Espionage in the 21st Century. Burlington, Syngress & Elsevier.

[80] Easttom, C. and J. Taylor (2011). Collecting Evidence From Other Sources. Computer Crime, Investigation, and the Law. Boston, Course Technology p301-316.

[81] Hadjidja, R. and M. Debbabi (2009). "Towards an Integrated E-mail Forensic Analysis Framework " Digital Investigation **5**(3-4): p124-137

[82] Philipp, A., D. Cowen, et al. (2010). Email Analysis. Hacking Exposed - Computer Forensics 2nd Edition, The McGraw-Hill Companies: p240-271.

[83] Guo, Y. and J. Slay (2010). "Data Recovery Function for Digital Forensic Tools." Advances in Digital Forensics VI **337**: p297-311.

[84] Perran, A., S. Perran, et al. (2010). Getting Started with Microsoft SharePoint Server 2010. BEGINNING SharePoint 2010: Building Business Solutions with SharePoint. Indianapolis, Wiley Publishing, Inc p37-55.

[85] Naqvi, S., G. Dallons, et al. (2010). Applying Digital Forensics in the Future Internet Enterprise Systems - European SME's Perspective. The 2010 Fifth IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering Washington, IEEE Computer Society.

[86] Biggs, S. and S. Vidalis (2009). Cloud Computing: The Impact on Digital Forensic Investigations. International Conference for Internet Technology and Secured Transactions. London, IEEE: p1-6.

[87] Barrett, D. and G. Kipper (2010). Virtualization and Forensics. Burlington, Elsevier Inc.

[88] Aggarwal, G., E. Bursztein, et al. (2010). An Analysis of Private Browsing Modes in Modern Browsers. The 19th USENIX conference on Security Berkeley, CA, USA, ACM.

[89] Grobauer, B. and T. Schreck (2010). Towards incident handling in the cloud: challenges and approaches _____ The 2010 ACM workshop on Cloud New York, NY, USA, ACM.

[90] Lu, R., X. Lin, et al. (2010). Secure provenance: the essential of bread and butter of data forensics in cloud computing. ACM Symposium on Information, Computer and Communications Security New York, NY, USA, ACM.

[91] Chow, R., P. Golle, et al. (2009). Controlling data in the cloud: outsourcing computation without outsourcing control. The 2009 ACM workshop on Cloud computing security New York, NY, USA, ACM.

[92] Ahmed, S. and M. Y. A. Raja (2010). Tackling cloud security issues and forensics model. High-Capacity Optical Networks and Enabling Technologies (HONET). Cairo IEEE: p190-195.

A. Forensically Sound Email Development Code

A.1 Login

```
using System;
using System.Collections.Generic;
using System.ComponentModel;
using System.Data;
using System.Drawing;
using System.Linq;
using System.Text;
using System.Windows.Forms;

using System.Security.Cryptography;

namespace EmailClient
{
    public partial class Form1 : Form
    {

        // User's Credential is ID plus password, which is "internalstaff.smith1" + // "password"
        private string UserCredentials =
            "4F2588A8301480FEFFFD21BE020A9FA788F25C2C";

        // Investigator's Credential is ID plus password, which is "investigator" + // "yyb5494"
        private string investigatorCredentials =
            "9C4C276806BF9539F81B4CA074C7E78EB4BFC7FD";

        // For security reason, the user credentials should be stored in a secret
        // database, we only simulate the situation by hard coded the credential in // the first
        // place

        public Form1()
        {
            InitializeComponent();
        }

        // Login Button Events

        private void btnLogin_Click(object sender, EventArgs e)
        {
            if (checkUserCredential() && (textBoxUserName.Text.Length > 0))
            {
                Form2 form2 = new Form2(textBoxUserName.Text + lblDomain.Text);
                this.Hide();
                form2.Show();
            }
        }
    }
}
```

```

}

else if (checkInvestigatorCredential() && (txtboxUserName.Text.Length > 0))
{
    Form3 form3 = new Form3();
    this.Hide();
    form3.Show();
}
else
{
    txtboxUserName.Text = "";
    txtBoxPwd.Text = "";
}
}

```

// Check the Investigators Credentials by compare the HASH value of the login // name plus password

```

private bool checkInvestigatorCredential() {
    var PlaintextEnter = txtboxUserName.Text + txtBoxPwd.Text;
    var InvestigatorData = Encoding.ASCII.GetBytes(PlaintextEnter);
    var Credhash = new SHA1Managed().ComputeHash(InvestigatorData);
    var resulthash = string.Empty;

    foreach (var b in Credhash)
    {
        resulthash += b.ToString("X2");
    }
    return resulthash.Equals(investigatorCredentials);
}

```

// Check the user's Credentials by compare the HASH value of the login // name plus password

```

private bool checkUserCredential() {
    var PlaintextEnter = txtboxUserName.Text + txtBoxPwd.Text;

    var UserData = Encoding.ASCII.GetBytes(PlaintextEnter);
    var UserDatahash = new SHA1Managed().ComputeHash(UserData);
    var resulthash = string.Empty;

    foreach (var b in UserDatahash)
    {
        resulthash += b.ToString("X2");
    }
    return resulthash.Equals(UserCredentials);
}

```


}
}
}

A.2 Normal User's Email Activities

```
using System;
using System.Collections.Generic;
using System.ComponentModel;
using System.Data;
using System.Drawing;
using System.Linq;
using System.Text;
using System.Windows.Forms;

using System.Net;
using System.Net.Mail;
using System.Xml;
using System.Security.Cryptography;

namespace EmailClient
{
    public partial class Form2 : Form
    {
        public SmtpClient client = new SmtpClient();
        public MailMessage msg = new MailMessage();

        private string username;

        // For security reason, the user's email account info should be stored in a // secret
        // database, we only simulate the situation by hard coded the
        // email account info here

        public System.Net.NetworkCredential smtpcrds =
            new System.Net.NetworkCredential("internalstaff.smith1@gmail.com",
            "sabsaforensics");

        public Form2(string user)
        {
            InitializeComponent();
            username = user;
            txtbxFrm.Text = username;
            txtbxFrm.Enabled = false;
        }

        // Email send Event, Call XMLfile function to store sent email contents in
        // forensics manner

        private void button1_Click(object sender, EventArgs e)
        {
            Sendmail(txtbxTo.Text, txtbxFrm.Text, txtbxSub.Text, RTBoxMsg.Text);
        }
    }
}
```

}

```

public void Sendmail(string sentTo, string sentFrom, string Subject, string body)
{
    try
    {

        // Setup Host
        client.Host = "smtp.gmail.com";
        client.Port = 587;
        client.UseDefaultCredentials = false;
        client.Credentials = smtpcrds;
        client.EnableSsl = true;

        // Convert strings to Mailaddress
        MailAddress to = new MailAddress(sentTo);
        MailAddress from = new MailAddress(sentFrom);

        // Set up message settings
        msg.Subject = Subject;
        msg.Body = body;
        msg.From = from;
        msg.To.Add(to);
        DateTime time = DateTime.Now;

        // Call XMLfile function
        XMLfile(msg.To.ToString(), msg.From.ToString(), msg.Subject.ToString(),
        msg.Body.ToString(), time.ToString());

        // Send email
        client.Send(msg);
        MessageBox.Show("Email Successfully sent from " + "internalstaff.smith1@gmail.com"
        + " to " + txtbxTo.Text);

    }
    catch (Exception ex)
    {
        MessageBox.Show("Unable to send msg due to the following error: " + ex.Message);
    }
}

// XMLfile function

private void XMLfile(string To, string From, string Subject, string Body, string Time)

```

```
{  
XmlDocument xmldoc;  
XmlElement xmlelem;  
XmlText xto, xfrom, xsubject, xbody, xtime, xhash;
```

```

xmldoc = new XmlDocument();
xmldoc.Load(@"C:\Evidence\logfile.xml");
xmlelem = xmldoc.CreateElement("", "mail", "");

XmlElement xto1 = xmldoc.CreateElement("To");
XmlElement xfrom1 = xmldoc.CreateElement("From");
XmlElement xsubject1 = xmldoc.CreateElement("Subject");
XmlElement xbody1 = xmldoc.CreateElement("Body");
XmlElement xtime1 = xmldoc.CreateElement("Time");
XmlElement xhash1 = xmldoc.CreateElement("Hash");

xto = xmldoc.CreateTextNode(To);
xfrom = xmldoc.CreateTextNode(From);
xsubject = xmldoc.CreateTextNode(Subject);
xtime = xmldoc.CreateTextNode(Time);
xbody = xmldoc.CreateTextNode(Body);

// Hash the full message plus the user account name
string fullMessage = To + From + Subject + Body + Time;
string hash = HashMessage(fullMessage, "internalstaff.smith1");
xhash = xmldoc.CreateTextNode(hash);

xto1.AppendChild(xto);
xfrom1.AppendChild(xfrom);
xsubject1.AppendChild(xsubject);
xtime1.AppendChild(xtime);
xbody1.AppendChild(xbody);

// the email content's Hash value, which can be used later to
// verify the integrity of the evidence
xhash1.AppendChild(xhash);

xmlelem.AppendChild(xto1);
xmlelem.AppendChild(xfrom1);
xmlelem.AppendChild(xsubject1);
xmlelem.AppendChild(xtime1);
xmlelem.AppendChild(xbody1);
xmlelem.AppendChild(xhash1);

xmldoc.DocumentElement.AppendChild(xmlelem);

try
{
// The XML file is saved locally
xmldoc.Save(@"C:\Evidence\logfile.xml");

```

```
}  
catch (Exception e)  
{  
    Console.WriteLine(e.Message);  
}  
Console.ReadLine();  
}
```

```

// Hash function

private string HashMessage(string fullMessage, string username)
{
    // Add all content to one string
    string stringToConvert = username + fullMessage;
    // Convert string to data (bytes)
    var data = Encoding.ASCII.GetBytes(stringToConvert);
    // Create the hash - using SHA-256
    var hashData = new SHA256Managed().ComputeHash(data);

    // make an empty string
    var resulthash = string.Empty;

    // for each byte in the resulting hash, add to the string.
    foreach (var b in hashData)
    {
        // X2 is the Hexadecimal formatting for toString
        resulthash += b.ToString("X2");
    }

    return resulthash;
}
}
}

```

A.3 Investigator's Activities

```

using System;
using System.Collections.Generic;
using System.ComponentModel;
using System.Data;
using System.Drawing;
using System.Linq;
using System.Text;
using System.Windows.Forms;

using System.Xml;
using System.IO;
using System.CodeDom.Compiler;

using System.Security;
using System.Security.Cryptography;
using System.Security.Cryptography.X509Certificates;

```



```
using System.Security.Cryptography.Xml;
```

```
namespace EmailClient
{
    public partial class Form3 : Form
    {
        private XmlDocument source;
        private XmlDocument copy;
        private TreeNode tree;

        private string Report_SysEnvi_MachName,
        Report_SysEnvi_DomainName,
        Report_SysEnvi_OSVersion,
        Report_SysEnvi_LoginTime,
        Report_XMLfileHashValue,
        Report_CaseName,
        Report_ExaminerName,
        Report_SearWarrantInfo;

        public Form3()
        {
            InitializeComponent();

            // The program will automatically gain sys info and hardware info
            // as a computer ID evidence

            GetSysInfo();
            GetHardwareinfo();
            source = new XmlDocument();

            // The evidence will be load into investigator's interface for live
            // forensics

            source.Load("C:\\Evidence\\logfile.xml");
            copy = null;
            tree = null;

            // Call the ShowXML function to show email sending history
            ShowXML();

            // Get the hash value of the file so that not only the file
            // content has a hash value, but also the evidence report file

```

```

// itself are hashed
Report_XMLfileHashValue = ComputeSHA1Hash("C:\\Evidence\\logfile.xml");
}

// This function collects the System info
private void GetSysInfo()
{
    DateTime time = DateTime.Now;
    txtboxHostname.Enabled = false;
    txtboxHostname.Text = System.Environment.MachineName;
    Report_SysEnvi_MachName = System.Environment.MachineName;

    txtboxDomain.Enabled = false;
    txtboxDomain.Text = System.Environment.UserDomainName;
    Report_SysEnvi_DomainName = System.Environment.UserDomainName;

    txtboxOSversion.Enabled = false;
    txtboxOSversion.Text = System.Environment.OSVersion.ToString();
    Report_SysEnvi_OSVersion = System.Environment.OSVersion.ToString();

    txtboxLogintime.Enabled = false;
    txtboxLogintime.Text = time.ToString();
    Report_SysEnvi_LoginTime = time.ToString();
}

// This function collects the computer hardware manufactory info
private void GetHardwareinfo()
{
    System.Management.ManagementClass ObjectiveClass = new
    System.Management.ManagementClass("Win32_NetworkAdapter");
    foreach(System.Management.ManagementObject objMgmt in
    ObjectiveClass.GetInstances())
    {
        lstBoxManuinfo.Items.Add(
        "Manufacturer :" + objMgmt["Manufacturer"] + " " +
        "Adapter Name :" + objMgmt["Caption"] + " " +
        "MACAddress :" + objMgmt["MACAddress"]);
    }
}

// This button click event create a txt file with collected information

private void button1_Click(object sender, EventArgs e)
{
    try

```

```

{
Report_CaseName = txtboxCaseName.Text;
Report_ExaminerName = txtboxExamName.Text;
Report_SearWarrantInfo = rtbox.Text;
StreamWriter SW;
SW = File.CreateText("C:\\Evidence\\myfile.txt");
SW.WriteLine("Case Name:" + Report_CaseName);
SW.WriteLine("Examiner's Name:" + Report_ExaminerName);
SW.WriteLine("Search Warrant Information:" + Report_SearWarrantInfo);
SW.WriteLine("Suspect's Machine Name: " + Report_SysEnvi_MachName);
SW.WriteLine("Suspect's Domain Name:" + Report_SysEnvi_DomainName);
SW.WriteLine("Suspect's OS Version:" + Report_SysEnvi_OSVersion);
SW.WriteLine("Investigator's Login Time:" + Report_SysEnvi_LoginTime);
SW.WriteLine("XMLfileHashValue:" + Report_XMLfileHashValue);
SW.Close();
}
catch (Exception ex)
{
MessageBox.Show("Report Generation Failure: " + ex.Message);
}
}

// This function shows the XMLfile contents (email sending history) in
// investigator intreface
private void ShowXML()
{
// determine if copy has been built already
if (copy != null)
return; // document already exists

// instantiate XmlDocument and TreeNode
copy = new XmlDocument();
tree = new TreeNode();

// add root node name to TreeNode and add TreeNode to TreeView control
tree.Text = source.Name; // assigns #root
treeView1.Nodes.Add(tree);

// build node and tree hierarchy
BuildTree(source, copy, tree);
}

```

```

private void BuildTree(XmlNode xmlSourceNode, XmlNode document, TreeNode
treeNode)
{
// create XmlNodeReader to access XML document
XmlNodeReader nodeReader = new XmlNodeReader(xmlSourceNode);

// represents current node in DOM tree
XmlNode currentNode = null;

// treeNode to add to existing tree
TreeNode newNode = new TreeNode();

// references modified node type for create node
XmlNodeType modifiedNodeType;

while (nodeReader.Read())
{
// get current node type
modifiedNodeType = nodeReader.NodeType;

// check for EndElement, store as Element
if (modifiedNodeType == XmlNodeType.EndElement)
modifiedNodeType = XmlNodeType.Element;

// create node copy
currentNode = copy.CreateNode(modifiedNodeType, nodeReader.Name,
nodeReader.NamespaceURI);

// build tree based on node type
switch (nodeReader.NodeType)
{
// if Text node, add its value to tree
case XmlNodeType.Text:
newNode.Text = nodeReader.Value;
treeNode.Nodes.Add(newNode);

// append Text node value to currentNode data
((XmlText)currentNode).AppendData(nodeReader.Value);
document.AppendChild(currentNode);
break;

// if EndElement, move up tree
case XmlNodeType.EndElement:
document = document.ParentNode;
treeNode = treeNode.Parent;
break;
}
}
}

```

```

// if new element, add name and traverse tree
case XmlNodeType.Element:

// determine if element contains content
if (!nodeReader.IsEmptyElement)
{
// assign node text, add newNode as child
newNode.Text = nodeReader.Name;
treeNode.Nodes.Add(newNode);

// set treeNode to last child
treeNode = newNode;
document.AppendChild(currentNode);
document = document.LastChild;
}
else // do not traverse empty elements
{
// assign NodeType string to newNode
newNode.Text = nodeReader.NodeType.ToString();
treeNode.Nodes.Add(newNode);
document.AppendChild(currentNode);
}
break;

// all other types, display node type
default:
newNode.Text = nodeReader.NodeType.ToString();
treeNode.Nodes.Add(newNode);
document.AppendChild(currentNode);
break;

} // end switch

newNode = new TreeNode();

} // end while

// update the TreeView control
treeView1.ExpandAll();
treeView1.Refresh();

} // end BuildTree

```

```

// This function calculates the hash value of the hashed Txt file
public static string ComputeSHA1Hash(string fileName)
{
return ComputeHash(fileName, new SHA1CryptoServiceProvider());
}
public static string ComputeHash(string fileName, HashAlgorithm hashAlgorithm)
{
FileStream stmcheck = File.OpenRead(fileName);
try
{
byte[] hash = hashAlgorithm.ComputeHash(stmcheck);
string computed = BitConverter.ToString(hash).Replace("-", "");
return computed;
}
finally
{
stmcheck.Close();
}
}
}
}

```

A.4 Sample Code of an Additional Application that Compares the Hash Values

```

using System;
using System.Collections.Generic;
using System.ComponentModel;
using System.Data;
using System.Drawing;
using System.Linq;
using System.Text;
using System.Windows.Forms;

using System.Security;
using System.Security.Cryptography;
using System.Security.Cryptography.X509Certificates;
using System.Security.Cryptography.Xml;
using System.Xml;
using System.IO;

```

```

// This is a the code of a sample application that developed to calculate the // hash value
of the colleted evidence file, so that the hash value can be
// compare with the one appeared in the Email Client. The identical result is // expected
to prove the integrity of the evidnce file and contents

```

```

namespace XMLfile

```

```

{
public partial class Form1 : Form
{
public Form1()
{
InitializeComponent();
}

private void button1_Click(object sender, EventArgs e)
{
textBox1.Text = ComputeSHA1Hash("C:\\Evidence\\logfile.xml");
}

public static string ComputeSHA1Hash(string fileName)
{
return ComputeHash(fileName, new SHA1CryptoServiceProvider());
}

public static string ComputeHash(string fileName, HashAlgorithm hashAlgorithm)
{
FileStream stmcheck = File.OpenRead(fileName);
try
{
byte[] hash = hashAlgorithm.ComputeHash(stmcheck);
string computed = BitConverter.ToString(hash).Replace("-", "");
return computed;
}
finally
{
stmcheck.Close();
}
}
}
}

```