



# Foreman Forensic System Analysis

May 5

# 2015

---

This report will investigate the role of Digital Forensics Case management by adopting a modified Systems Thinking approach in order to produce a set of recommendations for the developer of Foreman Forensic to include in future implementation.

James Owen  
1222060

CM3203

## **Abstract**

This project seeks to assist with the development of a simple, easy to use Open source system that is suitable for carrying out case management activities in digital Forensic investigations. Whilst conducting a simple search online it is evident that there is a plethora of case management systems providing a range of different services. However, there is currently no Open source system that is competent to meet the demands of digital forensic case management activities. The systems that can manage such activities are extremely expensive and can be very complex; the result of this is that organisations are adopting non standardised approaches such as using spreadsheets or ticketing systems designed for helpdesks.

The principal developer of Foreman Forensic is a full time digital forensic investigator at RBS, her work commitments mean that the development of this system is only completed on the weekends. Consequently, with the constant uprising of digital crimes and rumours of industrial standards being introduced, there is a dire need for a free open source system that can be distributed to organisations that do not have the financial resources to purchase such systems. Furthermore, due to the costs involved in purchasing such systems, case management aspects of digital investigations can only be taught in theory on Security and Forensic Modules at Universities. The availability of an Open source case management system that students can use for coursework purposes, will guarantee the development students hands on skills and experience that is currently not be accommodated by universities due to the significant costs involved in purchasing these systems.

This project seeks to consider the role of digital forensic case management through utilising a hybrid version of Soft System Methodology. The inclusion of additional methods within the standard approach of SSM will demonstrate how this project was able to identify areas of interest that required further analysis and research. These areas utilised many approaches such as the Making decisions in the absence of clear facts framework devised by Georgiou (2006), Neilson's Usability Heuristics (Neilsons 1995), tabular analysis and the evaluation analysis of ISO standards and other investigative frameworks. In addition this project utilised feedback from two police forces and the developer of Foreman Forensic in order to validate initial outcomes of SSM and contribute to the development of recommendations for Foreman Forensic.

## **Acknowledgements**

I would like to thank my wife for her continued support whilst I have been completing this project. Furthermore I would like to thank Mr Mike Daley for introducing me to this project and for the support he has given me throughout its completion.

I would also like to thank Dr Wendy Ivins who has provided me with specialist advice on the Soft Systems Methodology which I found very challenging at the initial stages of the project.

This project could not have been completed without the feedback that I received from South Wales Police Bridgend and Gwent Police Force so I would also like to thank them for their quick response and knowledge that they shared.

Finally, I would like to thank Sarah Holmes for her guidance and for taking the time to read and respond many of my emails whilst I was completing this project.

## **List of Abbreviations**

FF – Foreman Forensic

SSM – Soft Systems Methodology

MDACF – Making Decisions in the absence of clear facts

## **Table of Contents**

Introduction.....	5
Beneficiaries .....	5
<b>Background</b> .....	6
Locards Exchange Principles and Digital Forensic investigations .....	6
Uses of Digital Forensics .....	7
Digital evidence.....	8
Case Management .....	8
Chain of evidence.....	8
<b>Approach</b> .....	9
Soft Systems Methodology .....	9
Soft Systems Methodology Hybrid Approach.....	13
Making decisions in the absence of clear facts (MDACF) .....	15
Forza Framework .....	19
Tabular Analysis .....	21
Researching ISO standards.....	21
Heuristic Evaluation.....	21
<b>Implementation</b> .....	22
SSM Stage 1.....	22
The situation considered problematic .....	22
SSM Stage 2.....	25
Expressing the problem situation .....	25
SSM Stage 3.....	28
Formulation of the Root Definitions .....	28
SSM stage 4 .....	32
Conceptual Modelling.....	32
SSM Stage 5.....	40
Comparing Models with Real World .....	40
SSM Stage 6&7.....	47
Soft Systems Methodology Final Stages.....	47
<b>Recommendations</b> .....	48
Neilsons Heuristics evaluation.....	48
Tabular Analysis .....	50
Research of relevant ISO Standards .....	54
Comparison of Foreman Forensic and the Forza framework .....	60
<b>Evaluation of results</b> .....	65
<b>Future Work/Opportunities</b> .....	67

<b>Conclusion .....</b>	<b>68</b>
<b>Reflection .....</b>	<b>70</b>
<b>References.....</b>	<b>73</b>
<b>Appendices.....</b>	<b>75</b>
Appendix 1 Foreman Transcript .....	76
Appendix 2 Uncertainties .....	77
Appendix 3 -Complexity and Conflict.....	79
Appendix 4 Rich Picture.....	80
Appendix 5 Soft Systems Methodology (Analysis 1, 2, 3).....	81
Appendix 6 Identifying and formulating Transformations .....	84
Appendix 7 C.A.T.W.O.E. Analysis.....	85
Appendix 8 Root Definitions .....	88
Appendix 9 Comparing models with real world .....	89
Appendix 10 Correspondence from Inta Forensics .....	100
Appendix 11 FORZA – Digital forensics investigation framework.....	101
Appendix 12 Usability Evaluation Guide .....	102
Appendix 13 Correspondence –DR Alia AbdelMoty .....	106
Appendix 14 Tabular Analysis .....	107
Appendix 15 Email from SARAH Holmes (Developer) .....	113
Appendix 16 Developers Comments for Recommendations.....	115

## **Introduction**

The primary objective of this project is to provide a robust set of recommendations that can be implemented in order to assist the development of a new open source digital forensic case management system. In order to achieve this primary objective one would need to satisfy a number of sub-objectives to equip oneself with the knowledge and insight in order to produce feasible and constructive recommendations. Furthermore, in order to justify and validate ones proposed recommendations, this project will utilise many analysis techniques to examine all of the contributing factors that currently exist with the proposed system and in digital forensic case management activities.

## **Beneficiaries**

The undertaking of this project seeks to create two beneficiaries, that being oneself and the developer of FF. This project has provided oneself with the opportunity to analyse a real life system that is currently still in development. Furthermore, this project did not provide any mandatory requirements regarding how this analysis must be completed. Therefore this project has provided oneself with the freedom and flexibility to carry out and utilise any method that one deemed necessary in order to generate recommendations for this system. The project initially required additional research and the learning of a new set of skills which one believes will be beneficial in future employment as a Business Analyst. Furthermore, this project has also provided oneself with the opportunity to contribute to the development of a new open source system which one believes will be very successful once it has been completed.

Secondary, it is ones aspirations that the recommendations produced from this project will provide the developer with feasible and valuable recommendations that can be implemented to improve the current system. Furthermore, one is hopeful that this research and analysis will identify areas of interest for further investigation in the future. Conversely, one is optimistic that this project identified any unfeasible or invaluable opportunities that the developer had initially considered implementing that can now be dismissed as they have proven to be ineffective or unnecessary.

## **Background**

There appears to be a false portrayal of the concept of digital forensics, this was highlighted as many of the academic resources opening chapters choosing to immediately dispel incorrect perceptions of sunglasses, Humvees and expensive suits (Sammons 2012). Similarly the introduction to the Security and Forensics module taught by Mr Mike Daley also followed the same approach and sought to immediately dissolve false illusions of any similarities between the television program CSI and real world digital forensics.

Therefore to ensure that the reader has an accurate perception of what is involved in digital forensics; this section will briefly provide the background knowledge that is required to comprehend the objectives and scope of this project. Furthermore, this section will also attempt to eradicate any fictional Hollywood based illusions regarding what is involved in digital forensic practices.

### ***Locards Exchange Principles and Digital Forensic investigations***

These principles states that during the physical world, if a person enters or leaves a crime scene, then they will either take something with them or leave something behind such as fingerprints, DNA or fibres (Saferstein 2006, cited in Sammons 2012, p.7). Therefore in terms of a digital forensic investigation, such items left behind can be retrieved by accessing registry files and other logs.

Therefore considering the principles defined by Locard, investigators seek to apply computer science procedures in order to provide a solution for a legal problem (Sammons 20012). Furthermore according to (Marcella & Menendez 2008) digital or cyber forensics refers to the activities of locating, extracting and analysing different types of data from different types of devices in order to serve as legal evidence to prove or disprove a criminal or civil act.

## *Uses of Digital Forensics*

### Criminal investigations

According to a recent report in the telegraph the number of child pornographic web sites on the internet has doubled in the last year (Barret 2015). This subject receives a substantial amount of media attention and could be considered by some as the primary purpose of digital forensic investigations. Furthermore cases of online identify theft is another crime that is highly publicised and linked with digital forensic investigations.

However despite these being considered by many as the most prevalent reasons for the need to conduct digital investigations, Sammons (2012) states that that electronic evidence is present and sought in the majority of crimes that are taking place in society and digital forensic practices covers a wider area than the two previously discussed.

### Digital Forensics for Intelligence gathering

The use of information technology and the internet for the recruitment of terrorists has also been broadcasted in the media in recent times (Wakefield 2014). Digital Forensics currently plays an important role in identifying, spoiling and prosecuting those who are or have been engaging in terrorist activities.

### Digital Forensics for Administrative matters

Although the previously discussed uses of digital forensic are considered being criminal acts, organisations would also conduct such investigations to determine instances related to administrative issues such as employees breaching policies. Although not considered as extreme as the other methods, if an employee is engaging in ill practices this could potentially cost the company a substantial amount of money and pose a threat to their existence.



### ***Digital evidence***

According to Casey (2011) digital evidence can be sourced from three main categories, these include:

- Standard Computer systems - PC's, Laptops or other forms of devices that are considered to be traditional computers.
- Communication devices – Traditional telephones, Internet and other network devices.
- Embedded computer systems – Smart Cards, Mobile phones, GPS Systems, vehicle systems, Home appliances such as microwaves or oven which are connected to a home network.

In addition to the above, Sammons (2012) states that the emergence of new technologies such as cloud computing is another area that digital evidence can be sought.

### ***Case Management***

Case management involves the primary act of coordinating investigations from start to finish; additional activities must also be completed such as the assessing of risks, maintaining communication between those involved in the investigation and the storing and retrieval of evidence (Casey 2011). Furthermore, case management must also address and abide by the principles stated in the chain of evidence.

### ***Chain of evidence***

The term chain of evidence details the obligations of a forensic investigator to log all actions that have been performed on any of the equipment/evidence that has been submitted for analysis. Furthermore, this term also states the requirement for logging of those individuals who have had access to specific pieces of evidence/equipment. The location of this log must also be specified along with information regarding how the equipment/evidence is stored. Additionally it must also specify what precaution was used to prevent tampering or unauthorised modifications of any items/evidence (Marcella & Menendez 2008).

## **Approach**

This section will describe ones chosen approaches that this project has followed and employed throughout its lifespan. It will provide a brief description of the main principles and features of each method and discuss the reasoning of why these methods were considered the most appropriate. Furthermore it will discuss the alternative approaches that one chose not to use.

### **Soft Systems Methodology**

The decision to adopt Soft Systems Methodology for this project was due its effectiveness in structuring thought processes to manage real world complexities through the means of Systems Thinking.

System Thinking is a method of thinking where one would analyse the relationships between the individual parts of the system (activities) in order to improve the decision making processes. An illustration of the concept of Systems Thinking has been simplified by considering the example provided by Grimsley (2015).

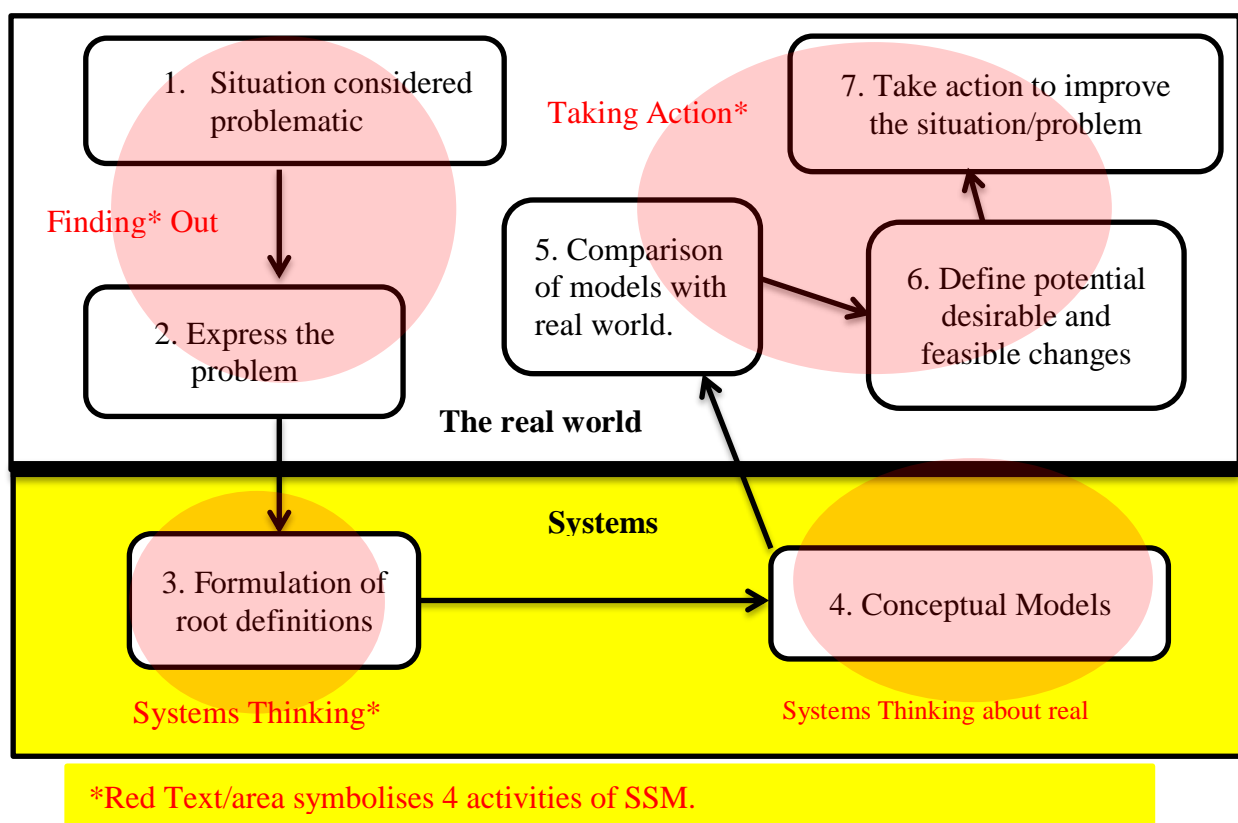
Initially one would consider and identify each part of a forest; this includes the vegetation, animals, weather and everything that exists or lives in a forest. All of these items are considered to be 'parts' of a forest, Systems Thinking is the approach that will identify the interactions and effects that each of these parts have on one and other. Therefore, each of these 'parts' construct what is considered to be a complex whole or in this case a forest system. Systems Thinking provides the framework to examine each of these interactions and influences to determine potential patterns and provide solutions that could change the behaviours that exist between these corresponding parts (Grimsley 2015).

Therefore, as one would be examining the current system and providing solutions for future improvements, it was decided that this methodology would be a suitable a fit and optimal approach to follow to achieve ones objectives.

The SSM process is considered to be a never ending cycle, once potential changes have been implemented the situation will change and further analysis can be sought. Although for the purpose of this project, only one cycle of the methodology was required.

Soft System methodology extends over two different parts, the real world and the systems world. The following diagram denotes the seven different stages that the approach follows; this approach has previously been considered as an algorithmic approach where each step is carried out in a progressive manner (Checkland 1999).

#### Traditional 7 stage Model



Traditionally Soft systems methodology was considered to be a seven stage model, although in later developments this was reduced to four main activities. This modification was implemented due to the manner that SSM was being used and it was thought that the traditional structure did not provide sufficient levels of flexibility.

However, one believes that this development would not affect the outcome of the project as they possessed many similarities. Therefore, it was decided that it was not necessary to choose or a particular process and one would consider both methods and embrace a flexible mind-set to the methodology.

Prior to concluding that this was the most suitable method of approach, one compared the use of adopting both hard and soft Systems Thinking approaches. This comparison identified that soft system thinking is considered to be suitable if the situation is complex, disorganized and susceptible to human input, particularly if there are multiple perceptions or for activities that are responsive to human behaviours (Checkland 1999). Alternatively, hard Systems Thinking would be considered more relevant in instances when a particular system already exists and the situation is deemed to be a 'straight forward' problem; this approach would then consider how the system can be engineered in order to achieve a set of objectives (Checkland 1999).

Therefore, as there is ambiguity surrounding the multiple methods that case management can be completed and that human behaviour and perceptions was a mitigating factor; one determined that Soft Systems Thinking was a better choice for this type of project.

## **Alternative methods**

### ***Systems Dynamics & iThink***

The choice between hard and soft Systems Thinking approach has previously been discussed in this section, therefore one will not reiterate ones decisions to utilise soft systems methodology.

Conversely, hard and soft Systems Thinking were not the only forms of Systems Thinking that were initially considered for this project. Whilst developing the initial plan for this project one had considered the possibility of utilising Systems Dynamics with the intention of developing a simulation model with iThink. However, throughout the completion of this project, it became apparent that the use of System Dynamics did not deliver any additional benefits and would be an unnecessary add-on.

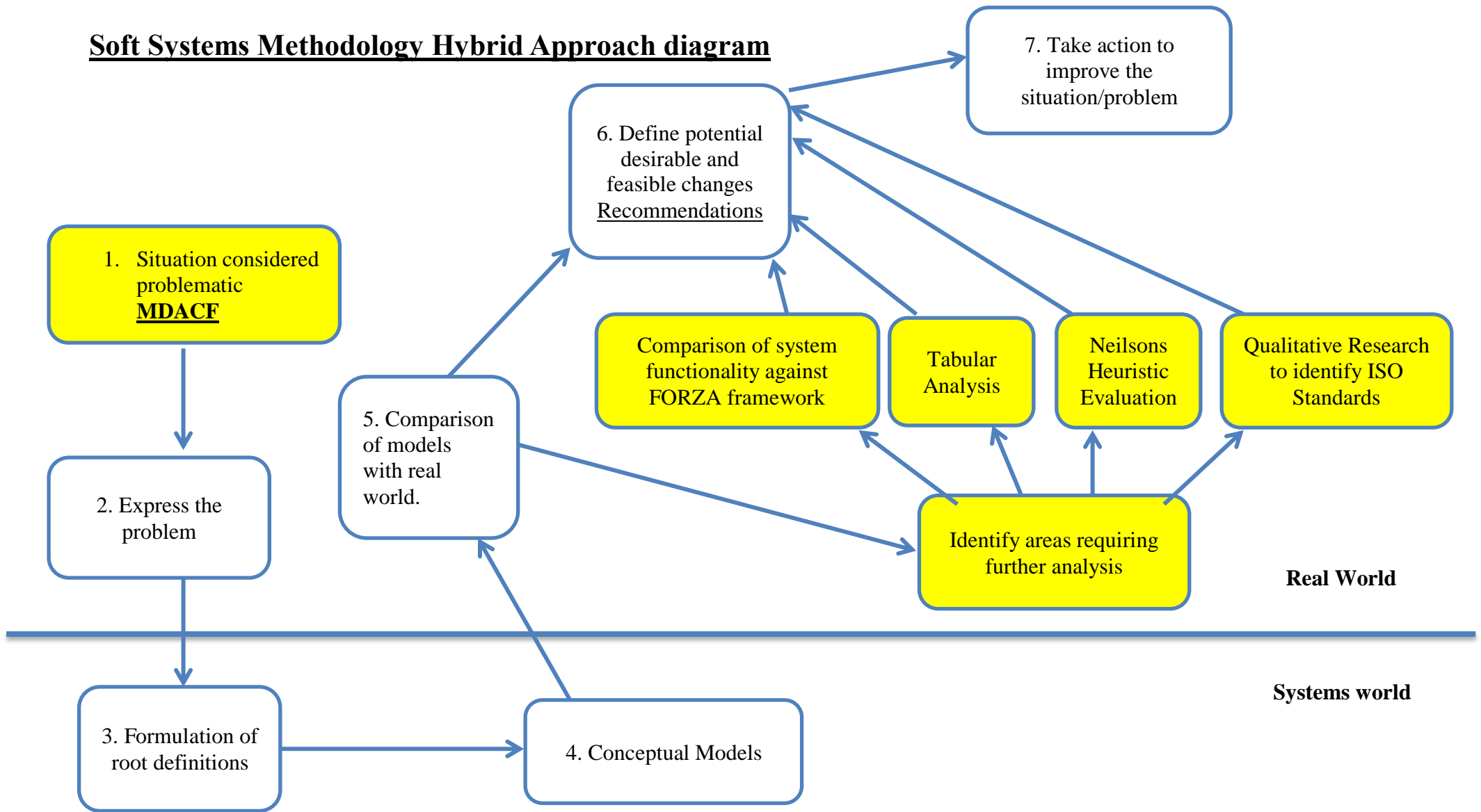
System Dynamics is a method that organises and defines problems over time, the system could then be used to predict and forecast potential changes by generating alternative outcomes based on mathematical equations. Consequently this project did not identify any aims or objectives that required the calculation and simulation of events that occurred over a proposed time scale. Furthermore, one did not require this method to validate any of one's findings as they would be validated by other means. Therefore with recommendation and guidance from Dr Wendy Ivins it was decided that Systems Dynamics would not be included in this project.

## **Soft Systems Methodology Hybrid Approach**

Although one had researched and confirmed the suitability of Checkland's SSM (1999) for achieving the objectives of this project, one had aspirations of utilising other forms of analysis methods in order to gain specific knowledge on different aspects of the system. The implementation section will discuss these methods in more depth, however the remainder of this section will introduce the methods that one utilised that would not normally be implemented with the traditional guidelines of SSM.

The following diagram displays the addition of new phases or activities that one implemented in order to conduct specific research or analysis on key areas of interest. The activities are highlighted and coloured yellow in order to distinguish the non-traditional activities.

## Soft Systems Methodology Hybrid Approach diagram



### **Making decisions in the absence of clear facts (MDACF)**

The initial plan of this project provided a clear set of objectives and desired deliverables; these stated the need to investigate the approaches to forensic case management in order to produce feasible recommendations for Foreman Forensic Case management system (FF) to implement. On initial procurement of this project, one received a transcript/abstract from the developer of FF which provided oneself with an overview of the current situation.

It was determined that for the initial stages of this project, one would prefer to adopt a structured approach to perform the necessary research; consequently one became familiar to an approach published by Georgiou (2006). This approach described a method that only considered the information that was at hand, whilst ensuring that project did not lose sight of its goals and research information that was not valuable or required.

This framework published by Georgiou (2006) considered situational characteristics that decision makers are exposed to on a regular basis; on examining these characteristics one determined that they shared similarities with this project. Furthermore, one considered that this approach could provide the foundations for building ones initial knowledge base which aligned with the initial stage of the SSM process. (Identifying the situation considered problematic)



The following table describes the characteristics that are related to decision making and provides a detailed description of how this project is relevant to each of the characteristics (Belasco et al cited in Georgiou, 2006, p.3.)

#### MDACF Characteristics

<b><i>Characteristic</i></b>	<b><i>Relevance to project</i></b>
The task is ambiguous	<p>Due to the number of different approaches being used to conduct case management, it was not clear which method was the best option and why.</p> <p>Additionally one's own knowledge of the processes involved in case management was very limited and on initial exploration of the topic revealed the absence of a silver bullet approach for case management techniques.</p>
Structure through which the task might be accomplished is loosely defined.	At present case management does not have a strict structured approach that it must follow; this was evident through different organisations using different approaches and methods.
Standard of which success is Measured remains unstable.	The success criteria stated in the transcript stated the need for a simple and easy to use system, although this may be considered as the primary focus of the system, the task of case management may require specific tasks that required complex processes. Additionally, what one person may find easy may not be easy for a different user with a different skill set.
Knowledge of organisational and wider environments remains uncertain.	This characteristic was primarily relevant to one's own knowledge, although one had gained some previous knowledge in university taught modules, one did not possess the experience and knowledge of case management in real life situations.
Opportunities for collecting more data/information/facts are constrained	<p>Due to the heightened level of competition between software vendors it became evident that retrieving information from the different competitors would be difficult. Particularly as any information that they provided could potentially be used to compete against their system.</p> <p>This issue may have been avoided if one had not being forthcoming with the intentions of the project with the software companies, however one felt that the acquisition of such information in this manner would be unethical and dishonest and was not a feasible option for this project.</p>

Georgiou (2006) utilised many concepts from different frameworks and authors which supported the development of this framework by combining different theoretical aspects and displaying the results in a table.

This approach initially considered the aspect of uncertainty and the different forms it can exist. The theoretical background for dealing with uncertainty originated in the strategic choice approach which was developed by Friend (1997), cited in Rosehead & Mingers (2001, p.117).

In this approach uncertainty is considered to exist in three different classifications;

1. The working environment
2. Guiding of values
3. Choice on related agendas.

The second areas of analysis for this framework considered the issues regarding complexity and conflict that arises in decision making.

The transcript which was provided by the developer of FF will be used as the foundation in which the analysis will initially examine. This will be completed by splitting the transcript into individual sections and each section will be examined whilst considering the issues of uncertainty, complexity and conflict in accordance with the approach specified by Georgiou (2006).

This process enabled the consideration of alternative influences that were not clearly visible on initial inspection of the transcript. An enhanced explanation of how this method was processed, combined with examples of the results it produced is provided in forthcoming Implementation section of the report.

## *Alternative Methods*

### S.W.O.T Analysis

<b><u>Strengths</u></b>	<b><u>Weaknesses</u></b>
<b><i>S.W.O.T.</i></b>	
<b><u>Opportunities</u></b>	<b><u>Threats</u></b>

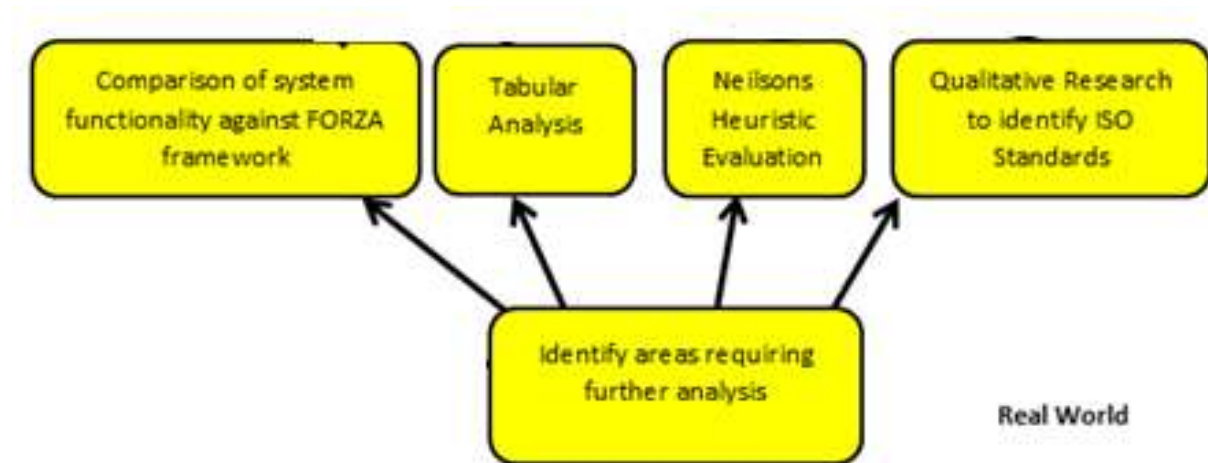
As previously discussed the MDACF framework was considered the most suitable option for this project. This analysis method was initially considered due to previous success in using this method on numerous occasions prior to this project and had produced good results.

This approach is efficient and effective at identifying Strengths, Weaknesses, Opportunities and Threats about the chosen area of interest. However the SWOT analysis is more suitable for producing information for business purposes. Furthermore, the completion of a SWOT analysis may produce a range of ideas; however it would not provide any assistance in determining which ideas are the most beneficial and provide the required information to progress (Robson 1997).

Conversely, although not all information in the MDACF approach was used and that the SWOT analysis could be adapted to suit this project, it did however provide oneself with the opportunity to learn a new technique for capturing information rather than adopting a skill that one was already competent at.

Therefore, on considering the benefits of using SWOT rather than the MDACF, one opted for the opportunity to learn a new skill that could potentially be used in future employment.

The addition of the following activities to the SSM approach provided the opportunity to exploit the feedback received from the police forces and the developer of the system. These inclusions were considered necessary once the feedback was received and analysed as it revealed the need for further examination into the different areas.

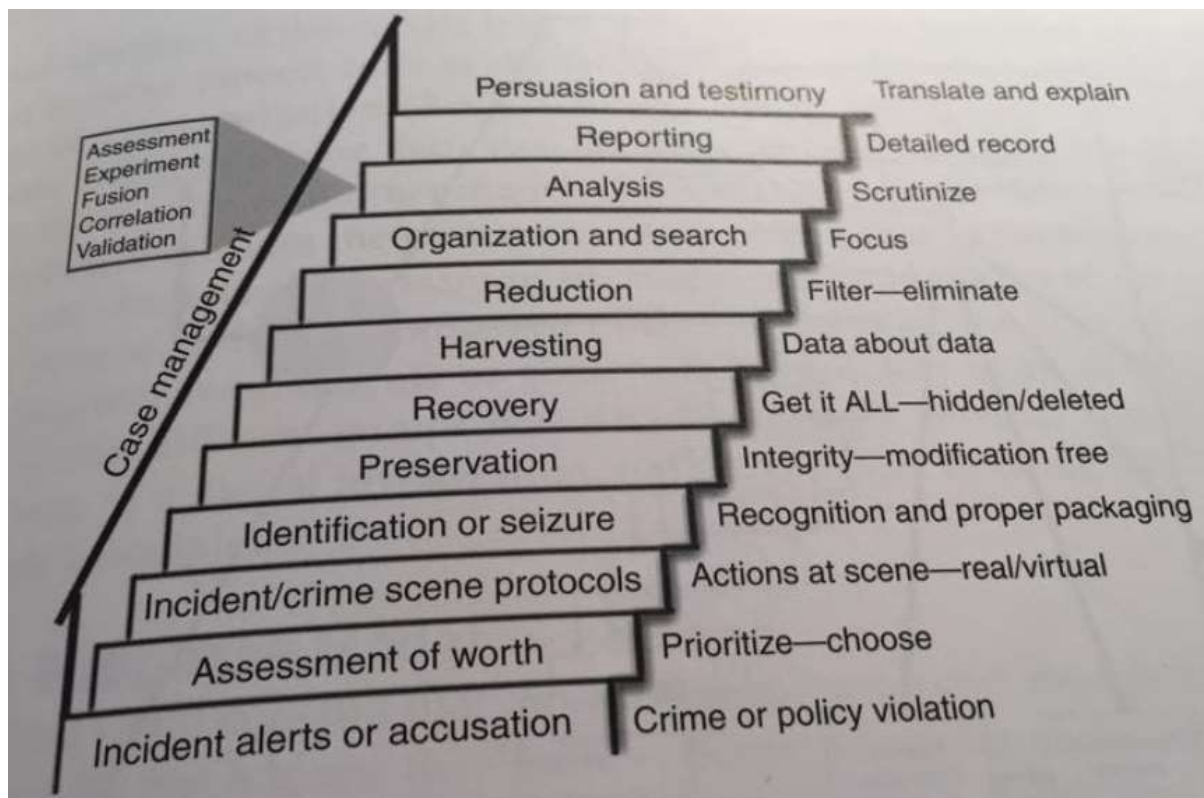


### ***Forza Framework***

The decision to analyse the Forza Framework was made due to the inclusion of legal aspects in the investigation framework Leong (2006). Furthermore the assumption that legal representatives would possess an enhanced amount of legal knowledge as opposed to digital investigators regarding what is considered to be legitimate evidence and practice. Therefore it was believed that if FF could provide the tools to improve collaboration between the legal and computer science divisions, then as a result it would improve the efficiency and effectiveness of the investigations.

As previously stated many other frameworks were considered, however several of these frameworks shared similar structures and processes to that of the ACPO guidelines. Furthermore, due to the feedback stating that ACPO guidelines had already been considered by the developer, one sought to analyse an alternative framework to avoid reanalysing content that may have already been completed by the developer,

A framework that was initially highlighted to be relevant to this project was the staircase model (Casey and Palmer 2004, cited in Casey 2011, p.192-3).



This framework above demonstrates how digital forensic investigators, examiners and legal representatives work together and progressively completing each of the proposed activities in a bottom upwards order.

This framework utilises the concept of case management as a potential handrail to ensure that all phases can be linked together to ultimately reproduce a ‘story’ once all sections have been completed (Casey and Palmer 2004 cited in Casey 2011).

Ultimately, there was no defining factor why one opted to utilise the Forza framework over the staircase model, although one did consider Forza to cover a wider range of contributing factors as it covered both roles and further analysed them with additional questions.

### ***Tabular Analysis***

In order to compare the features on different systems it was necessary to structure the results in a spreadsheet table. This was due to the ease of comparing different systems and conducting gap analysis for the different systems. Furthermore, it also ensured that each system was compared equally as each feature that was identified was included in the spreadsheet. Initially it was considered to summarise each system; however this would have made the analysis unstructured and may have missed key information when writing the summary. Furthermore, it is believed that information can be retrieved more efficiently from tables than reading multiple summaries for each independent system.

### ***Researching ISO standards***

It was determined that the most effective manner in which to identify the relevant standards was to consider which ones the competitors had adopted; in addition this was further reinforced with additional research. However, due to the substantial number of standards in circulation and the time constraints of the project, it was unachievable to complete a full comprehensive in depth analysis. Therefore, as a result only a limited number of ISO Standards were considered.

### ***Heuristic Evaluation***

This method was chosen based on the success of previous practice; this method produced valuable and effective results whilst using it to analyse user interfaces on alternative projects. This was due to it providing the necessary tools to identify potential flaws with the construction and design of user interfaces.

## **Implementation**

### ***Overview of section***

This section will discuss with further detail into the processes and methods that one employed throughout the duration of this project. This section aims to provide the reader with the deeper understanding of the methods that one adopted in order to achieve the objectives and aims of the project stipulated in the initial plan. This section will also discuss any difficulties that were experienced in implementing the chosen methodologies.

## **SSM Stage 1**

### **The situation considered problematic**

The initial stage of SSM requires the problem solver to form their initial perceptions and understandings regarding the proposed problem situation; as a result this stage can be considered to be the research or exploration phase of the methodology. As previously discussed one had considered adopting an unstructured approach in order to develop one's knowledge. However, this project included a transcript written by the developer which provided a large amount of background information regarding different aspects of the system. As the project deliverables aimed to produce recommendations for the developer of Foreman, it was decided that the transcript would be used as the basis in which to begin one's research into the proposed problem situation.

As previously discussed Georgiou (2006) wrote a journal which described in detail an approach that split sections of text into sentences, particularly in situations that were limited in terms of information. This journal described a framework that utilises as much of the available information in order to enhance the knowledge base. Although there were differences between the amount of information in one's transcript and the example, this did not pose any initial concerns. This was believed as the conventional method that this method utilises extracts information from severely sparse forms of information, whereas this transcript was particularly rich and the information was easily extractable.

The approach required the problem solver to consider three factors when evaluating the transcript which consisted of the following

- Uncertainty
- Complexity
- Conflict.

### Uncertainties

The first factor that was considered was the issue of uncertainty, the approach utilised aspects of the strategic choice approach (SCA) which describes three types of uncertainties that exist whilst dealing with non-routine decision making processes (Friend 2001, cited in Georgiou 2006, p.3). The three different types of uncertainties that exist in decision making are;

#### Uncertainties regarding the working environment (UE)

This factor refers to the particular uncertainties that exist due to the requirement of additional information. This can be managed by acquiring responses such as surveys and conducting investigations.

#### Uncertainties regarding the guiding values (UV)

This factor refers to the uncertainties that exist in guiding values and require a political response, this may occur when deciding strategic goals, choosing required policies, objectives and values. In addition this type of uncertainty also concerns matters that result from conflicting agendas and interests.

#### Uncertainties regarding the choices on related agenda (UR)

This uncertainty exists once decisions are made and there is uncertainties regarding how these decisions will impact decisions for other areas.

The implementation of this approach initially required one to separate the transcript into individual sections. The following table demonstrates how each section was analysed and includes the observations and thoughts that were developed by considering each of the three different characteristics of uncertainties. The full analysis for each section can be seen in Appendix 2.

<u>Section</u>	<u>UE</u>	<u>UV</u>	<u>UR</u>
There is a lack of simple forensics oriented case management software.	There is uncertainty with the term 'simple' as the term requires more accurate information. Do they mean simple in terms of 'having few parts and being easy to understand and use' or being classed as 'plain' and having little or no ornamentation.	Is this due to standards that forensics analysts have to adhere to which make such a 'simple' system infeasible.	Would making a Digital forensics system too easy reduce the barriers of entry into field and consequently increase competitors?



## Complexity and Conflict

The next stage in this process was to consider the issues of complexity and conflict that arise in decision making.

When considering issues of complexity, it was required to focus on instances where decisions in one part may cause consequences in other areas. Therefore complexity is considered to be established in changing and active situations where multiple problems can be created by interacting systems. Furthermore Georgiou (2006) states that complexity can be measured by calculating the number of different states it can demonstrate as it is believed that the greater number of states the more complex it will become.

Conflict focuses on human interactions, particularly in instances where relationships may become strained due to pre-existing pressures arising in present situations. These pressures could intensify minor strains due to previous volatile relationships, incompatible personalities amongst groups or individuals having different opinions on the prioritisation of a particular decision. Therefore, the identification of potential conflict areas aims to assist with the decision making process by considering such issues in order to consider feasible solutions to avoid such conflicts (Georgiou 2006).

The following table provides an example of one's observations for the issues regarding complexity and conflict. The full results can be viewed in Appendix 3.

Section	Complexity	Conflict
In today's market there is a plethora of digital forensics software available for investigators, from small scripts that do a single task to full-featured tool kits that can aid an investigation from start to finish.	Could a fully-fledged system with 'too' many features affect hinder the levels of usability and effectively become too complex for its users.	Conflict may arise from time served analysts who may have a preference for scripted systems rather than using a full featured tool kit or vice versa.

To summarise, this approach assisted by guiding ones thinking in a structured approach, it is likely that one may not have initially considered issues regarding complexity or the different forms of uncertainty. Additionally, as this approach was completed by analysing each section sequentially, this ensured that all areas of the transcript were analysed equally as opposed to only analysing the most apparent aspects of the transcript.

## **SSM Stage 2**

### **Expressing the problem situation**

The second stage of Soft Systems Methodology requires the problem solver to express the problem situation and identify areas that will be investigated further. This action must be achieved without applying any biases or making any assumptions, furthermore personality traits, emotions, experience and interests of the problem solver must not be allowed to influence this activity (Checkland 1999). Consequently, this action can be extremely difficult to implement and measure, therefore it requires a specific method to ensure that all of the pre-discussed factors are completed effectively.

Throughout the existence of SSM there have been three different methods to assist the problem solver with expressing the problem situation. These methods include the use of rich pictures, modelling or following the 'Analysis123' approach. Although this project has included a rich picture, the primary method used for generating the information for this section of the project was achieved by completing the 'Analysis123' approach.

### **Rich Picture**

A rich picture is a drawing which aims to identify all the components that are relevant to a specific problem situation. One of the primary motives why Checkland included rich pictures into soft system methodology was due to the belief that humans observe pictures are whole; consequently this would encourage holistic thinking rather than reductionist thinking. Another purpose of a rich picture is that they are effective in displaying relationships between the different features in the picture (Checkland & Scholes 1999).

However, the value of such drawings has been weakened in recent years; this is due to individuals considering that the guidelines are too abstract when capturing the energy and emotions that exist in human problematic situations (Checkland 1981, cited in Rosehead & Mingers 2001, p.45). As a brain storming exercise, one has used this method in a number of different circumstances, although the knowledge generated in this rich picture was not the primary source of research, it was still an effective method for organising initial thoughts at the beginning of the project (Appendix 3).

### ‘Analysis123’

Although Checkland (1999) has stated the many benefits of utilising rich pictures to express the problem situation, in accordance with the approach used by Georgiou (2006) it was necessary to utilise an alternative method known as ‘Analysis123’.

Analysis 1 is concerned with the intervention of the project and seeks to identify the potential occupiers involved in the systems. The analysis seeks to determine the following;

- Who is the client of the study and their potential reasons for causing the intervention to be made,
- Who is the problem solver that wishes to implement changes to the situation

The primary goal of this analysis was to identify the potential stakeholders of the system who share an interest in the subject and would usually be affected by any changes that are made to the system (Checkland 1981, cited in Rosehead & Mingers 2001, p.73).

Analysis 2 refers to the problem situation as a social system and determines what social roles are significant, what norms of behaviour are expected from these roles and what values of performance exist in these roles. (Checkland 1981, cited in Rosehead & Mingers 2001, p.73). Ultimately this analysis is concerned with the problem solver understanding the problem situation in terms of the culture that it exists.

Analysis 3 is concerned with political issues by determining the role of power in the problem situation; this is achieved by asking ‘how’ such power is expressed (Checkland 1981, cited in Rosehead & Mingers 2001, p.73).

Checkland & Scholes (1999) state that power can be expressed through different forms of commodities, such commodities of power may be role based, reputation based or intellectually based as well as many other forms. An example of how power could be expressed through a particular commodity is visible in the following example;

*‘A company was forced to reconsider its future after the death of its CEO, the company personnel were divided up into two sections based on whether they knew the CEO prior to his death. Although this was initially portrayed as a joke amongst the staff, in reality this was a very important factor which favoured those staff members who had known the CEO prior to his death ‘*

(Checkland & Scholes 1999)

Similarly to the MDACF approach, it was necessary to use the same sections from the transcript in order to conduct this analysis. This approach encourages the problem solvers creativity to enhance their knowledge in areas which may not have been clear on initial observation; also it structures the relevant material in a format that will be reused in a later stage of the SSM lifecycle (Georgiou 2006).

The following table demonstrates how the chosen method was used to generate additional information; this was achieved by considering the content from each section and considering each analysis in turn (Appendix 5).

Section	Analysis 1		Analysis 2		Analysis 3	
	Who	What	Socio Cultural Dynamics	Notes	Who/what	Power
In today's market there is a plethora of digital forensics software available for investigators, from small scripts that do a single task to full-featured tool kits that can aid an investigation from start to finish.	Users  Foreman forensic Suite.	Heightened level of availability of digital forensics software.	Plethora of digital forensics systems.	Very disorganised in the methods being adopted by its users as market consists of an excess number of systems designed for the same purpose but adopting alternative methods.	Users  Heightened level of availability of digital forensics software  Foreman	Power to impose expectations on system requirements  Power to hide/conceal Foreman forensic suite due to the number of competitors  Power to provide a system that fulfils the user's needs.

This process of knowledge elicitation combined with the previous MDACF method provided a substantial amount of information and insight into the current problematic situation. Consequently, both forms of analysis methods (MDACF, Analysis123) provided the foundations in order to acquire the required knowledge that will be utilised to complete the activities in forthcoming phases of SSM.

Although, the process of progressing to the next stage of SSM could be believed as the completion of any research, Checkland & Scholes (1999) state that these initial processes are never fully complete as new concepts and ideas will continue to surface as the project progresses.

### **SSM Stage 3**

#### ***Formulation of the Root Definitions***

A root definition is a method in which the problem solver is able to describe the aims of a proposed system through structured sentences (Checkland, 1999). The root definition aims to express the core purpose of the system by describing a particular transformation process. This transformation process initially considers the initial situation as an undesirable state and then considers the desired state. Each section of the transcript was analysed to identify these transformations, the following table demonstrates the transformation that occurred for that selected section of the transcript.

<b>Transcript Section</b>	<b>Transformation Process</b>
This results in too many companies with forensic departments using generic ticketing systems such as those intended for help desks. Others rely on a mixture of spreadsheets, documents and emails to track cases.	(T4) Uncoordinated generic approaches adopted by multiple users. ( <u>Undesirable State</u> )  →  Coordinated and inclusion of standardized approaches in case management. ( <u>Desirable State</u> )

Through observing the situation described above, it was recognised that there were too many uncoordinated generic approaches being adopted by multiple users, this is considered to be the undesirable state in which the problem solver wishes to change. Once a particular action has been implemented, it would aim to achieve the desirable state of coordinated and improved standardized approaches for case management. The transformation process does not concern itself with the ‘what’ actions; its sole purpose is to identify the conversion of a particular input into a desired output (Checkland 1999). The full list of transformations for each section of the transcript can be viewed in Appendix 6.

### ***C.A.T.W.O.E Analysis***

Once the transformations have been identified the next stage is to consider the other factors that construct a well formed root definition. There are a total of six different elements that construct a well formed root definition, the first letter of each of these elements make up the mnemonic C.A.T.W.O.E. The process of identifying knowledge on each of these elements is known as the C.A.T.W.O.E. analysis; its main purpose is to determine answers to specific questions on each of the elements.

Once the transformation has been identified, the problem solver would then progressively work through the remaining elements by considering the following questions for each element related to that specific Transformation.

- **Customers or Clients**  
who will benefit from the transformation?
- **Actor**  
who will complete this transformation?
- **Transformation**  
The stated transformation
- **Weltanschauung/Worldview**  
What reason justifies the completion of this transformation
- **Owner**  
Who can prevent or change this transformation
- **Environmental Restrictions**  
what restrictions exist for this transformation?

The final requirement of a root definition is to ensure that it has been written in a structured format, this is to ensure that the problem solver has sufficient information from the root definition to allow the problem solver to build a conceptual model from its contents. Checkland (1999) state that there are two forms of root definition known as Issue based and primary task, these root definitions are determined by how frequent the processes are.

1. Primary Based - Regular activities
2. Issue Based - one off event.

Although the structure of a root definition can change slightly, the structure should be similar to the following;

*‘A systems to do x means of y in order to do Z’*

In order to identify the information required to complete the C.A.T.W.O.E analysis, it was possible to refer to the previous results that were generated by completing ‘Analysis123’ method.

Therefore by reviewing these results and conforming to the guidelines for developing a well formed root definition, one proceeded to conduct a C.A.T.W.O.E Analysis (Appendix 7) and a root definition (Appendix8) for each section of the transcript

As previously discussed the use of the tables in the ‘Analysis123’ approach was intentional, this provided the structure in order to quickly identify the relevant components for the C.A.T.W.O.E. Analysis.

To elaborate, to determine the ‘clients’ one was able to refer to the results of Analysis 1 (Client, problem solver and problem owner) or analysis 3 (Who has the power?). Additionally, it was possible to determine the environmental restrictions and worldview by reviewing the results generated by assessing the social cultural dynamics factors addressed in analysis 2.

Analyses 1,3	Analyses 1,3		Analyses 2	Analyses 1,3	Analyses 2
Client	Actors	Transformation	Weltanschauung	Owner	Environment
<u>Users</u>	Foreman Forensic	(T1a) Plethora’s of systems adopting multiple methods. → Single system which fulfils the necessary requirements.	The requirement to lower the disorganised manner that forensic case management is being conducted.	Foreman Forensic	In an environment that has a plethora of methods.
<u>Root definition.</u>  A system to ensure forensic case management is conducted in a simplistic and organised manner by providing a single piece of software that fulfils the necessary requirements given the complex environment in which forensic case management exists					

The Weltanschauung otherwise known as the worldview expresses the outlook of why the proposed root definition is meaningful (Checkland, 1999).

It is likely that different people or users may possess different perceptions (Worldviews) of the problem; therefore in the event of this occurrence each perspective would require a root definition to represent the various 'Worldviews'. However, this project chose not to analyse multiple 'worldviews' as this wasn't considered necessary for the production of recommendations for FF. Instead, as these were personal recommendations the Weltanschauung was based on personal perceptions which will be challenged and further exploited in the forthcoming phases of the methodology.

Once all of the root definitions were formulated it was necessary to determine which ones required modelling. There were many root definitions that were not specific to case management and posed more relevance to the building of information systems, therefore it was decided that only the root definitions that were explicitly relevant to case management were to be modelled. The full list of root definitions can be viewed in Appendix 8.



## **SSM stage 4**

### ***Conceptual Modelling***

The next stage of the SSM process is to build conceptual models from the chosen root definitions. The model will include the minimum amount of activities that are necessary to fulfil the actions that were stated in the root definition. In order to identify the chosen activities and relationships, verbs from the root definition were considered to be actions and relationship were represented by linking different activities with arrowed lines (Checkland 1999).

The aim of this stage is to identify all of the required activities that must occur within that system for it to function correctly, additionally any methods (how's) which are included in the model must only be included if they exist in the root definition. Therefore conceptual model building will identify all activities from the root definitions and be presented as a model which will display any flows that exist between each activity.

Checkland & Scholes (1999) state that due to restrictions of humans short term memory, models should only include 7 plus or minus 2 activities. Although this guideline can pose restrictions on modelling, Checkland & Scholes (1999) maintain that this is the best approach as each activity can be further enhanced to display a new model that represents all the sub-activities for that initial activity.



As previously discussed the lines that flow between different activities represents the existence of a relationship between each activity. The direction that the line travels symbolises which activity is dependent on the other. Therefore, using the example above, it is clear to identify that activity B is requires or is dependent on activity A.

Finally, each model will require control mechanisms to ensure that it monitors the performance of the system. This control mechanism will ensure that the proposed system incorporates specific control measures to measure the performance of the certain factors of the systems.

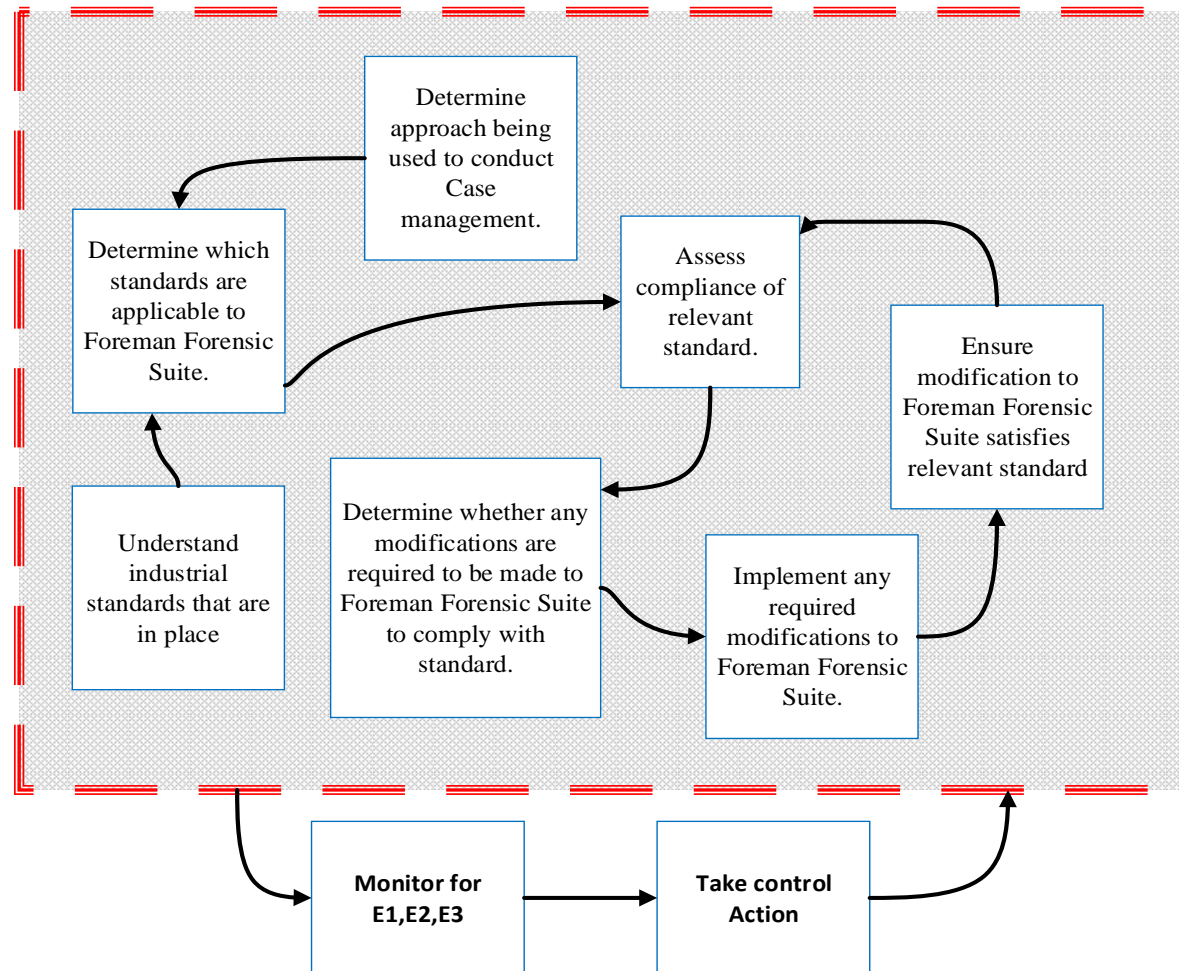
Checkland (1981) cited in Rosehead & Mingers (2001,p.81) describes the three measurements of performance as follows;

- Effectiveness – Measures whether the system has adopted the correct method to achieve the task.
- Efficacy – Measures whether the proposed method actually works.
- Efficiency – Measures how much resources are required to achieve the transformation?

As previously discussed it was decided not to model each individual root definition that was generated. Therefore, one chose three different root definitions as these were believed to identify and capture the core activities that existed in case management.

## **Conceptual Model for Root Definition 4**

The following model identifies the main activities that are required to ensure that case management adopts a co-ordinated and standardised approach by implementing industrial standards.



## Root Definition

A System owned and operated by Foreman Forensic Suite to ensure a co-ordinated and standardised approach to case management by implementing pre-defined industry standards given the constraints defined by the Forensic science Regulator in order to achieve Forensic case management for its users.

## C.A.T.W.O.E Analysis

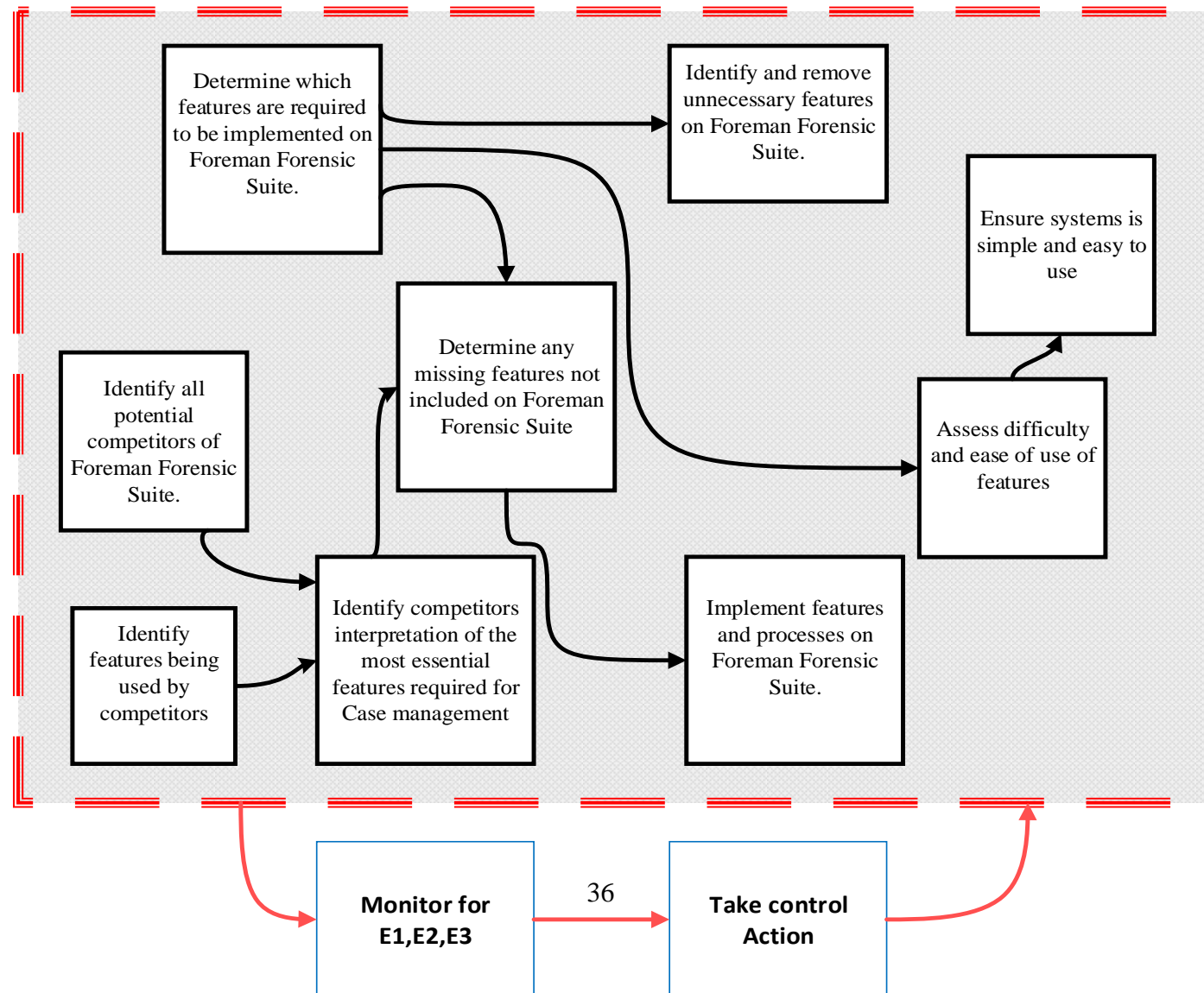
Clients	Client
Actors	Foreman Forensic
Transformation	Uncoordinated generic approaches adopted by multiple users → Coordinated and improved standardization in case management.
Weltanschauung	The belief that implementing standards will improve the methods and approaches which are currently being used to conduct case management.
Owner	Foreman Forensic
Environment	The Forensic science regulator Codes of practice.

## Performance Measures

E1	Effectiveness – Measures whether the system has adopted the correct method to achieve the task.
E2	Efficacy – Measures whether the proposed method actually works.
E3	Efficiency – Measures how much resources are required to achieve the transformation?

## Conceptual Model for Root Definition 5

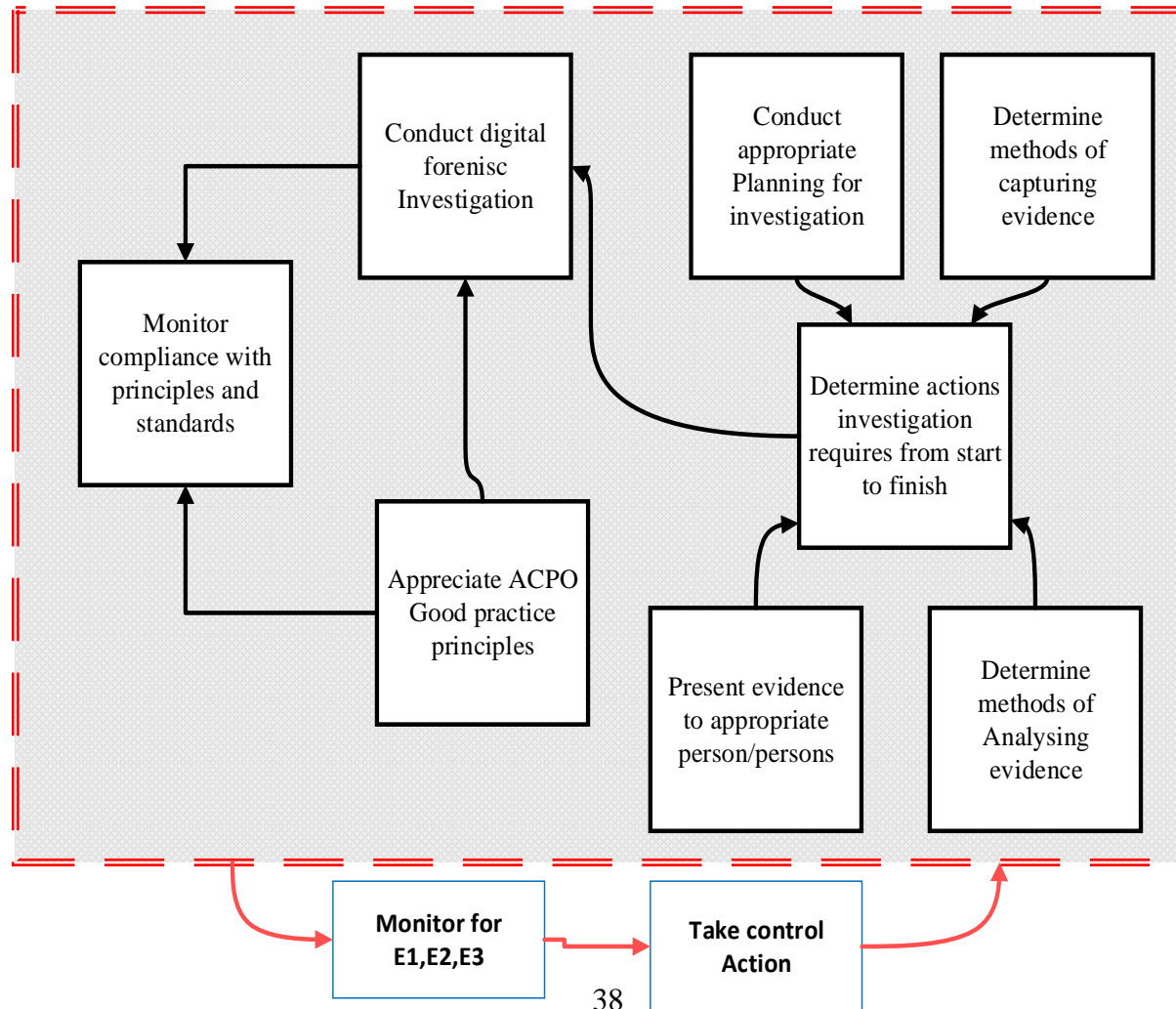
This model details the activities required to ensure that the system developed by Foreman Forensic is a simple and easy to use by identifying and implementing the required key features that may be different for different users of the system.



<b>Root Definition</b>	
A System owned and operated by Foreman Forensic to determine which features that are required in order to provide a simple, easy to use forensic case management system by identifying and implementing key features and processes given the constraints of different companies possessing different opinions on the most essential features required for Forensic case management.	
<b>C.A.T.W.O.E Analysis</b>	
Clients	Users
Actors	Foreman Forensic
Transformation	Current solutions difficult to use as they lack important features. → Identify Important features to improve systems' usability and processes.
Weltanschauung	The belief that specific features are required in order to successfully carry out case management effectively.
Owner	Foreman Forensic
Environment	Conflicting perceptions between competitors regarding the most important features a case management system must possess.
<b><u>Performance Measures</u></b>	
E1	Effectiveness – Measures whether the system has adopted the correct method to achieve the task.
E2	Efficacy – Measures whether the proposed method actually works.
E3	Efficiency – Measures how much resources are required to achieve the transformation?

## Conceptual Model For Root Definition 7

This model aims to capture the core activities that exist in digital forensic investigations whilst ensuring the investigation adheres to ACPO good practice standards and relevant industrial standards



<b>Root Definition</b>	
A System owned and operated by personnel conducting digital forensics investigations to comply with the principles of digital evidence whilst undertaking forensic analysis procedures such as the planning, capturing, analysis and presentation of digital evidence in order to aid an investigation from start to finish satisfying the constraints defined in the ACPO Good practice guide for digital evidence whilst satisfying the relevant industrial standards specified for each activity throughout the investigation process.	
<b>C.A.T.W.O.E Analysis</b>	
Clients	Personnel conducting investigation
Actors	Case management system.
Transformation	Specific and designed approaches are required to conduct digital forensics investigations. → Fulfilling this need to successful aid an investigation from start to finish.
Weltanshauung	The belief that key processes which include planning, capturing, analysing and presentation of digital evidence is required for case management to be conducted effectively.
Owner	Case management system.
Environment	Adherence to the ACPO good practice guide for digital evidence.
<b>Performance Measures</b>	
E1	Effectiveness – Measures whether the system has adopted the correct method to achieve the task.
E2	Efficacy – Measures whether the proposed method actually works.
E3	Efficiency – Measures how much resources are required to achieve the transformation?



## **SSM Stage 5**

### ***Comparing Models with Real World***

The next stage Soft Systems methodology was to compare the models with real world activities. In order to complete this analysis the intention was to conduct informal interviews with the multiple people from the digital forensic community. However, due to geographical location of the developer (Scotland) and the unavailability of the police officers, it was necessary to adopt an alternative approach. Therefore, surveys were forwarded to the personnel in order to generate further insight and validate the activities included in ones models.

As previously mentioned this stage usually utilises face to face meetings, one had many questions for the developer and police forces which would have resulted in a very large survey. Therefore, it was decided that the best method for the developer was to forward to the questions in a tabular format to allow her to quickly write her comments. However, as this project sought information from the police, it was considered necessary to develop a survey that was more presentable than a table. Therefore, one held an informal meeting with Mr Mike Daley to consider the most important questions to include prior to the creation and forwarding of the survey. Once the responses were returned, they were then summarised and a decision was made regarding whether they required any further analysis.

The traditional method for conducting further analysis according to Checkland (1991) would be to develop second tier activities from each of the activities identified in the primary model. However, one determined that one would adopt an alternative approach by utilising different techniques to gain further insight into the identified areas. This modification did not comply with the traditional methods of using SSM; however one believed that this modification was necessary in order to identify specific recommendations regarding the different areas of the models.

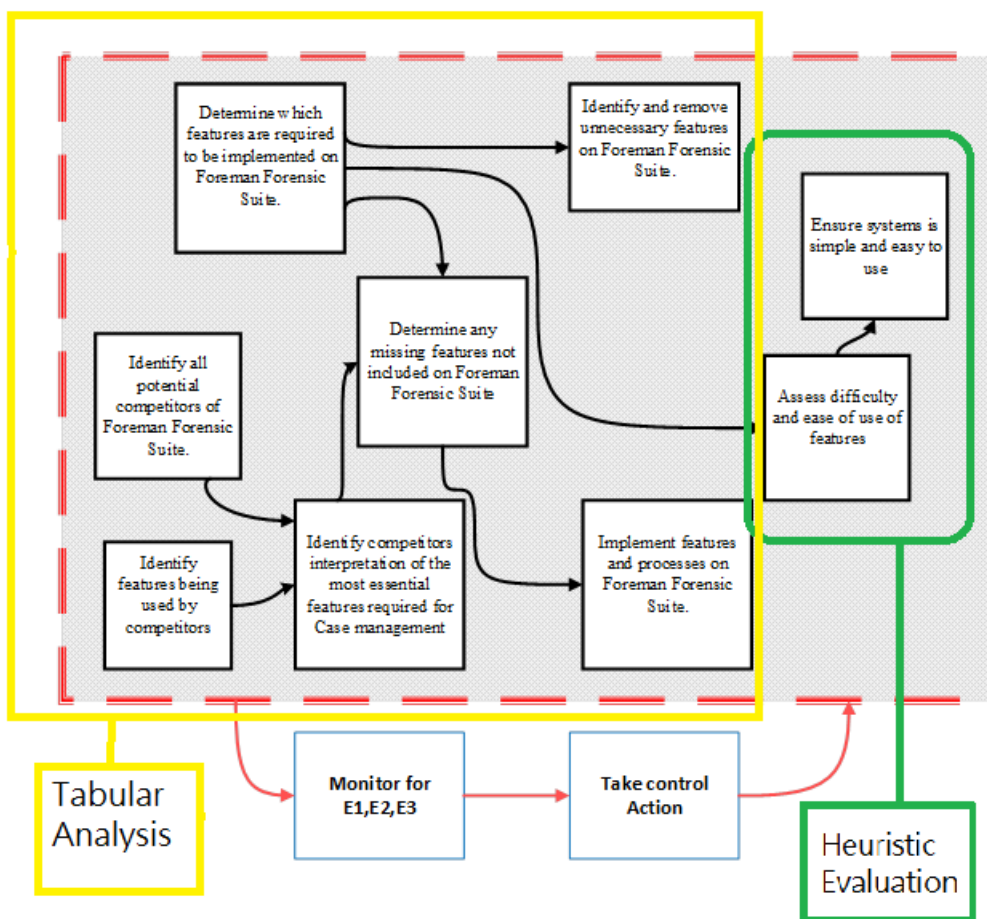
### **Conceptual Model 4 - Investigating Standards**

The feedback received from the surveys that were sent to the developer stated that FF had considered the ACPO guidelines from the initial stages of its development. The system also stated that it ensured that it followed the guidelines on audit trails, chain of custody and accountability. However, the feedback also suggested that the system had yet to consider the involvement of any ISO Standards. Therefore in order to provide the developer with further insight of the implementation of ISO standards, it was decided to investigate the key relevant ISO standards that

may be applicable for FF when further developing of the system. The results of this research will be discussed in the recommendations section of the report.

### Conceptual Model 5

On evaluation of the responses received from the developer of FF and relating them to the relevant model, it identified the need to investigate certain activities in further detail. Therefore, by considering the model and feedback one identified two sections of the model that could be divided into relevant areas of interest. The following example displays the two sections that one chose to further investigate.







**Yellow** – Determine the most popular features being deployed on leading platforms in order to recognise any missing, unnecessary features for FF.

**Green Area-** Determining how efficient and effective the user interface of the system is by conducting a heuristic evaluation.

## Tabular Analysis

This task was completed by carrying out research on each of the leading systems and consequently recording the results in a spreadsheet/table. This allowed the viewing of each of the system simultaneously to identify the most and least popular features amongst each of the systems.

APPENDIX 14 - TABULAR ANALYSIS

					Recommendations
Name of System	Foreman Forensic Suite	Case Notes	AD LAB	Lima Forensic Case Management	
Website	<a href="https://bitbucket.org/lozmanio/foreman/">https://bitbucket.org/lozmanio/foreman/</a>	<a href="http://www.blackthorn.com/case-management/">http://www.blackthorn.com/case-management/</a>	<a href="http://accessdata.com/solutions/digital-forensics/ad-lab">http://accessdata.com/solutions/digital-forensics/ad-lab</a>	<a href="http://www.intaforensics.com/software/lima-product-suite/">http://www.intaforensics.com/software/lima-product-suite/</a>	Solution in recommendations
Operating systems	Linux, Windows and IOS. Supports most browsers	Ipad, Iphone and windows pc	Microsoft Windows Server 2008 R	Windows XP,7,8 (32&64 bit systems) Supports any browser	Solution in recommendations
Database server					
Installation documentation	Provides 'wiki' with instructions for setting up system. Encountered issues regarding installation of python files which caused delays installing the system.	System can be installed by downloading app from relevant app store or website.	No installation guide online	Provides a step by step installation guide.	Solution in recommendations
Cost	Opensource therefore £0	No costs	No costs	Dependant on version	Solution in recommendations
Free trial available	Free to download	Provides 14 day free trial	No	Free trial not available	Achieved ✓
ISO Compliance	Not yet. This project seeks to identify	No information available for this system, however	No information available	ISO27001:2005 ISO 9001:2008	Discussed in further detail in

The information for this task was retrieved by visiting each competitor's website and downloading their brochures. In the initial stage of the project one had contacted each of the companies to explain and introduce this project to seek guidance and support for aspects of the project; however these attempts were unsuccessful and alternative methods were required to be implemented to acquire the relevant research.

Initially one approach that was considered was to contact the companies anonymously and impersonate a potential customer in order to acquire more information; however one considered this to be inappropriate and unethical behaviour. This was believed due to the means in which information would be acquired, as it would be obtained without consent to ultimately improve a system that may one day become a competitor.

Therefore, although it was not possible to acquire the amount of information that had been initially anticipated, it was however possible to identify many of their features by evaluating public sourced documentation provided on their websites.

## Heuristic evaluation

The initial response in the survey from the developer of the system suggested that she had acquired feedback from a range of personnel. The developer stated that she had sourced feedback from other students, Scotland Police force and digital investigators attending various conferences.

The surveys also suggested that she had received positive feedback by maintaining a simplistic, consistent design throughout and by minimising any clutter on the webpages. Therefore, due to the considerable amount of feedback that the developer had received, one determined that the likelihood of one identifying any potential flaws or improvements without adopting a structured approach would be very unlikely. Therefore, it was decided based on previous use, that it would be necessary to utilise the heuristics posed by Neilson (1995) and conduct a heuristic evaluation. At this stage it was not anticipated that there would be any significant flaws or design issues, however previous use of this method suggested that this was the most suitable and effective of finding such issues.

Prior to this decision, one had expressed an interest in conducting a heuristic evaluation on all of the leading case management systems that were identified in the transcript. However, as it was not possible to acquire copies of these systems this was not feasible. However, on further deliberation it was recognised that this process may not have been as beneficial as previously considered. The deliverables of this project stated the requirement to identify changes that can be made exclusively to FF, the process of analysing other systems may identify their methods for a particular task but this would not identify deficiencies that exist on the FF system. Furthermore, the outcomes of this task will provide FF with the necessary knowledge to make improvements to their design methods rather than attempting to replicate their competitors systems.

During the implementation of this task, it was necessary to consider how to utilise these heuristics in order to carry out a successful analysis of the system.

Therefore with the reassurance from a Dr Alia Abdelmoty, it was decided that this approach would observe the system as a whole in order to evaluate this system rather than concentrating on individual tasks (Appendix13).

Consequently, this evaluation involved the consideration of three different factors.

1. Neilsons Usability Heuristics (Appendix 12a).
2. The severity or any noncompliant heuristics (Appendix 12b).
3. The effort that would be required to fix any non-compliant heuristics (Appendix 12c).

The example below displays the structure that was used whilst conducting this analysis; the full results can be seen in Appendix 12D. Furthermore these results were then used to form recommendations which will be included in the Recommendations section of the report.

	Identified area	Problem	Violated Heuristic	Level of severity	Ease of correcting Heuristic	Proposed Solution
1	Activities that requests information from the client.	There wasn't a clear indication of which fields were mandatory.	Error prevention	1	1	Use of an asterisk to identify which data fields are mandatory for progression to the next phase.
2	Uploading Photographs	If user changes mind, there is no exit or cancel button and user is forced to upload or exit screen and re-enter information on return	Visibility of system status	3	2	Insert a cancel button so user can cancel photograph upload.
3	There is no option for choosing the relevant time zone.	If user changes mind, there is no exit or cancel button and user is forced to upload or exit screen and re-enter information on return	Error Prevention	3	1	Implement data field to select time zone  Or  Implement automated time zone capturing.
4	User has to manually enter date and time when uploading evidence.	User can input fictional time by changing the time on the computer as is installed	Error Prevention	3	2	Implement necessary features to capture time and date automatically.

### ***Conceptual Model 7- Investigation of alternative Frameworks***

The feedback received from the developer stated that FF had employed certain aspects of the ACPO guidelines; however the responses recorded in the surveys from the police forces revealed that it was not always feasible to follow these guidelines rigorously. Furthermore the police forces stated that various investigations required alternative approaches and were forced to modify the framework in order to achieve the objectives of that case.

Therefore, the purpose of this analysis was to identify and examine the activities that occur in alternative frameworks. This would then identify whether FF could implement new features in order to improve its compatibility with other investigation frameworks.

On carrying out initial research, it was noticed that there have been several attempts to define a silver bullet process model for all forms of digital investigations. However this is yet to be accomplished due to the substantial number of contributing factors that exist in digital forensics investigations. Although there are is an extensive number of process models currently in circulation, many of these models have included processes/activities that reappear frequently.

#### **Forza Framework**

On examining several different frameworks it became apparent that it would be infeasible to analyse each one individually, furthermore if this was completed it would be expected that the results would be similar for many of the frameworks due to them sharing similar activities and processes.

Therefore, it was decided to analyse the FORZA framework developed by Leong (2006) due to its consideration of legal and managerial issues that arise in digital forensic investigations. This framework considers the roles and responsibilities of all potential participants involved in an investigation, consequently this enabled oneself to examine the effectiveness of FF for each of these roles. Furthermore Leong (2006) developed a high level view of the framework which was used to compare FF with the corresponding sections specified in the framework (Appendix 15).

The proposed roles that the framework has identified for digital forensic investigations are as follows.

- Case leader
- System/business owner
- Legal advisor
- Security/system architect/auditor
- Digital forensics specialist
- Digital forensics investigator/system administrator/operator
- Digital forensics analyst
- Legal prosecutor

The secondary requirement of this framework required one to consider six questions as specified below for each of the roles described previously.

- What (the data attributes);
- Why (the motivation);
- How (the procedures);
- Who (the people);
- Where (the location), and
- When (the time).

In order to complete the necessary analysis, one referred to the diagram and progressively compared each role and question to the functionality of FF. Consequently, if FF was not equipped to complete that specific task, it could then be determined whether a modification or inclusion of a particular feature to the system was feasible. In the event that an action was feasible, a recommendation was then created to suggest a method in order to complete the desired action.

Initially, one had utilised a tabular approach to record the recommendations, however it became evident that not all areas would be relevant and the table appeared half complete. Therefore, it was decided to progressively summarise those which were identified and written as recommendations in the forthcoming section.

## **SSM Stage 6&7**

### ***Soft Systems Methodology Final Stages***

The final stage(s) of SSM specifies the necessity for the problem solver to define and implement any changes in order to improve the current situation (Checkland, 1999). The inclusion of other forms of research and analysis methods generated additional information which was used to provide recommendations.



## **Recommendations**

The primary purpose of this section is to provide the reader with an overview of one's findings and present them as recommendations for FF implement in the future; furthermore this section also aims to fulfil the requirements of the final stages of the SSM process.

FF is still in its early stages of development, therefore many of these recommendations may have already been considered by the developer but not yet been implemented.

### **Neilsons Heuristics evaluation**

As previously discussed, the developer of FF has a wealth of experience in Digital Forensics and is an experienced practitioner. The developer has also acquired feedback from multiple personnel in the digital forensic community and has utilised feedback from live demonstrations in conferences. Furthermore, the developer has also stated that she is also aware of Neilson's usability heuristics, therefore one did not expect to identify a substantial amount of violated heuristics. However by completing this evaluation, it ensured that the design of the user interface was examined by someone who may possess a different perspective to the developer of the system.

### ***Recommendations***

The following recommendations have been determined by referring to Neilson's usability Heuristics (1995) and analysing the system's user interface. Furthermore, one did appreciate that the system is not fully functional and is still in its early stages of development.

The inclusion of an asterisk on all mandatory data fields would provide the user with the knowledge of what information is required to progress to the next stage. Alternatively, if all fields are mandatory then it would also be advisable to inform the user of this requirement.

Whilst uploading images for the evidence, if the users wish to cancel the upload after selecting an image, the user will have to press the back button to cancel that process which will also cancel any recorded information. Alternatively, the user will have to choose a different file to load instead of the initially file. It is recommended that a 'cancel' process is included to provide the user with the opportunity to cancel the current task without exiting that section.

In the event that this system becomes available to users residing in different time zones particularly Europe, there is currently no feature that would allow the user to state their current time zone. Therefore, it is recommended that the system includes additional information to account for such

time zones or implement a feature that automatically determines the time zone by pairing the location with its IP address otherwise known as Geolocation.

There are currently security concerns regarding the addition of evidence. The system identifies the time and date when a user uploads evidence, however it was possible to manipulate this time by adjusting the laptop clock to a fictional time. This may contravene or degrade the reliability of the audit trail.

On inspection of a case there is currently two options available that allows the user to 'close' that case. It is recommended that this be reduced to one.

When the user visits the different sections on the system due to the number of shortcuts and quick links, the user could potentially lose track of their location within the system. This recommendation suggests that each screen provide a navigational feature to inform user of their current location. However, this has currently been achieved in some of the areas particularly in the addition of evidence as there is a notification stating that the user is at 'section 1 of 2'.

The user is only advised of their actions when they fail to comply with any necessary requirements e.g. missing data from require fields. Therefore, a recommendation for this system is to provide additional assistance without affecting its minimalistic design. A solution could be to implement a feature that displays brief snippets of information when a mouse is rolled over a particular area/text. This ensures that the design isn't affected whilst also providing the user with valuable information.

In the event that a user requires assistance or referral to documentation, the link currently listed on FF directs the user to the Bitbucket website. If the user did not have access to the internet they would not be able to retrieve the required information they desire. Therefore, it is recommended that the documentation/support be made available without having to connect to the internet.

The system has implemented warning and success screens; however these are not fully consistent throughout the whole system. This may result in users losing substantial amount of evidence if they accidentally click the backspace button on keyboard. Consequently one recommends that a warning sign be included on all key areas where the user has to input any case notes or other forms of information.

## **Tabular Analysis**

Due to the inability to acquire copies of each Case management system, it was necessary to refer to the online brochures and documentation that each company provided. This analysis has revealed that there were many similarities amongst all of the systems; however it is believed that the implementation of the following recommendations and suggestions will improve the current system.

### ***Recommendations***

The following recommendations have been formulated by researching and comparing FF and other leading digital forensic case management systems in order to identify the main features by performing tabular analysis on each system.

All three of the leading systems have a dedicated website that provides users with information. Although, the system is linked with a blog and Bitbucket it is recommended that a website specifically for FF system is constructed. This is due to the belief that a website may attract additional support from others programmers which will effectively reduce the development time and share the workload for this project.

This analysis has identified that each system is capable of being run on a Windows system; some can run on Linux and others such as Blackthorn has a mobile application that can be run on iPad's and iPhones. Mobile devices can be used in any location and would be highly valuable and convenient if the investigator was able to log their work by using such devices. Although this recommendation is not considered to be critical for the success of the current system it may be worth considering for future implementation.

The current installation for this system requires the installation of Python files. Although the installation of FF was undemanding, there were difficulties with the initial setup of Python tools. In comparison the other systems appeared to be more user friendly as they were executed in a windows environment, furthermore they provided videos and detailed installation guides. This issue could potentially be improved by;

- a. Providing additional resources such as videos with demonstrations to reduce installation technical problems.
- b. As the system is open source and users won't be charged to acquire a copy, FF could generate revenue by charging for the installation and initial setup for their future clients

Ultimately these are just suggestions; however the current process of setting up the system in Python requires more technical knowledge than the rival systems.

Throughout this project FF was not considered to be a system that required enhanced in-depth training. However, each person has different levels of skills and abilities, consequently it is recommended that some means of training is provided particularly as the leading companies have developed online videos and detailed 'How to' guides. Furthermore, Intaforensic's has developed a course that users can attend in order to use the system to its full potential. This may also be an opportunity how FF can generate additional revenue to support further development.

The leading systems have ensured that they have considered the support requirements in depth by providing several different means to provide user assistance. Currently the developer of FF has stated that this project receives minimum attention during the working week as she has employment commitments. As the system is currently not fully operational this does not cause any significant concern at present. However, once the system becomes operational FF must ensure that a support strategy is developed to ensure that their potential customers can receive support within a satisfactory timescale.

Each system has the option of exporting the data from the system into pdf, rtf, Tiff, and many other file formats. This appears to be a key feature as each system has included the tools to complete this task. FF does provide this service but it would need to install additional packages. This

recommendation suggests additional resources for those who are unsure of installing third party packages.

The logging of evidence to maintain the chain of custody is also one of the key requirements for a digital forensic case management system. FF has utilised QR codes for the logging of evidence, this feature is unique to FF as no other system currently utilises this technology. Although, hashing of evidence is included, consider implementing an onscreen notification to inform the user if any tampering or modification of evidence has occurred. This can be completed similarly to Blackthorns system by displaying a red dot if data has been changed or modified in any way.

The current setup for FF's evidence locker is that it stores evidence by date/time. This may suffice for smaller amounts of evidence; however large investigations over a long period of time may result in a substantial amount of evidence and result in the user having to scroll through a large list. The inclusion of a search feature is popular amongst the rival systems; therefore it is believed that this feature would be a valuable inclusion to the FF system.

Intaforensic's considers itself to be an end to end system that covers all aspects of Case management. There are currently two features that have been incorporated into this system which no other system has implemented; these are features that record sales and client data. Therefore, if FF wishes to be considered as an end to end system such as Intaforensic's Lima, it may need to consider additional features that are outside the scope of digital forensic operations such as these or similar management features.

The current system is believed not utilise networking technologies; therefore this would prohibit the sharing of information to different members involved in the investigation. Therefore, the system should consider implementing a network infrastructure whilst ensuring that information security principles are considered in great depth considering the sensitivity of some cases/evidence.

The photograph uploader is currently not in operation; however it is recommended that a feature that would allow other media file formats to support audio recordings and videos. Although the system is capable of uploading such files in other areas, having these options in the same location as the photograph uploader would improve the design and continuity of the system.

Intaforensic's system has also included an additional feature that monitors and 'analyses' the amount of time that is spent on different aspects of a case, this would allow the organisation to generate an enhanced understanding of the areas that may require additional support. Although, this data can be retrieved manually and may not be considered a primary concern at present, this feature could improve the efficiency of a case and reduce user's expenditures. Furthermore, the inclusion of a system that could potentially save the organisation money is a highly sought feature and highly marketable.

A potential future recommendation for FF would be to consider developing or amalgamating FF with an Open source FTK platform. Blackthorn has successfully implemented this, and as a result offers a full comprehensive digital forensic package that forensic investigators can use to conduct and manage their investigations.

## **Research of relevant ISO Standards**

In order to identify the relevant standards that may be applicable to digital forensic case management, one required in-depth knowledge of the activities that took place throughout the lifecycle of an investigation. Therefore, once this knowledge was gained regarding the investigation frameworks particularly FORZA (Leong 2006) and the ACPO guidelines (ACPO 2012), it was then possible to identify the relevant standards that would be applicable. Furthermore, it was also possible to identify some of the relevant ISO standards by referring to the results generated in the tabular analysis; these results highlighted the relevant standards that the competitor systems were utilising.

Although initial attempts of communicating with many case management companies weren't as successful as initially desired, one did receive some guidance from a director at IntaForensic regarding which standards to consider when carrying out this analysis (Appendix 10).

The next step was the acquisition of the relevant ISO standards, it was discovered that these standards are not free and purchasing several of these documents would be expensive. Fortunately it was possible to acquire copies through the University as they had copies in the library and provided access to these standards online whilst logged on to a university system.

On successfully acquiring copies of these ISO standards, it was identified that it would not be feasible within the time scales of this project to individually analyse each clause and statement within each of the standards. However, one still had aspirations of achieving the objective of identifying relevant standards for the developer of the system. Consequently, with the acceptance and guidance from the projects supervisor, it was decided that this analysis would only consider the chosen standards at a high level and only include the salient points of each standard.

In addition, currently there are approximately 19500 different ISO standards available for various aspects of business and technology (ISO1 No date). Although many of these standards may be unsuitable or irrelevant, it was decided to conduct an initial assessment on the recommended standards however only discuss the three most significant.

Finally, an ISO standard is a written document that provides a range of information on the requirements, guidelines or characteristics that are necessary to ensure the materials, products or services are sufficiently met to achieve its purpose (ISO1 No Date). These documents can be accessed and purchased online by visiting the International standards website.

## **ISO 9001 – Quality management systems**

The ISO 9001 Standard is currently under review; however it belongs to the group of standards whose purpose is to consider issues relating the management of quality. The standard aims to provide guidance and the necessary tools for companies and organisations to ensure that their products or services are satisfying their customers' needs. Furthermore this standard ensures that they engage in ongoing improvement to maintain levels of quality in their products or services, this is then measured on an ongoing basis by conducting audits and inspections.

The standard is built on eight quality management principles that it must consider in order for it to achieve the objectives of the standard. These principles consist of the following (BSI1 2000)

1. Customer focus
2. Leadership
3. Involvement of people
4. Process approach
5. System approach to management
6. Continual improvement
7. Factual approach to decision making
8. Mutually beneficial supplier relationships

The standard has been created to be applicable across multiple organisations and is not specific to industry or organisation size. This is achieved by describing a quality management system which provides the requirements for that organisation to engage and complete certain documented procedures (BSI1 2000).

In addition these procedures must adhere to specific requirements that are included in each of these clauses

- Clause 4.2.3 Control of documents
- Clause 4.2.4 Control of records
- Clause 8.2.2 Internal audit
- Clause 8.3 Control of nonconforming product
- Clause 8.5.2 Corrective action
- Clause 8.5.3 Preventative action

(BSI1 2000)



In addition, this standard states the requirement for the organisation to produce a quality policy and manual prior to considering becoming accredited.

According to the ISO standard website (ISO No date), the main objective of this standard is to ensure that the system is functioning in the correct manner. Therefore, it is ones belief, that even if the developer does not wish to proceed and gain accreditation for this standard, the identification of any factors that violate the quality of the system still needs to be identified and resolved. Therefore, if the developer chooses not to proceed with accreditation, it is recommended that a strategy is still implemented to acquire feedback relating to the functionality and quality of the system. This can be achieved by requesting feedback from users of the system or by engaging in an analysis similar to ones heuristic evaluation completed previously

## **ISO17025 - General requirements for the competence of testing and calibration laboratories**

This standard was developed for any organisation that is required to perform testing or sampling during its daily activities. This standard does not state a minimum and maximum number of personnel that are required to be engaging in laboratory activities and does not state to what extent such activities must achieve. Therefore, the primary purpose of this standard is to assist laboratories in the managing and maintaining quality, administrative and technical operations (BSI2 2006).

The following describes the prominent clauses stated in the ISO 17025 that are specific to the different activities and processes that occur during a digital forensic investigation (ACPO 2012).

### **Clause 4.13 Control of Records**

This clause states the requirement of ensuring that a record of all seized evidence is completed, this may consist of the recording of all items that have been seized according to their bag number. Additionally an audit trail must always be completed to monitor the activities that take place throughout the lifespan of the investigation (BSI2 2006 & ACPO 2012).

### **Clause 5.4.2- Selection of methods**

This clause ensures that the best methods are used to conduct the investigation by considering the needs of the customer and the investigation itself. In the event that the customer does not state a desired method, then the investigator must make the decision based on the knowledge he/she possesses. This may involve decisions on what items are required to be seized based on that specific type of case they are investigating (BSI2 2006 & ACPO 2012).

### **Clause 5.8 – Handling of test and calibration items**

This clause ensures that the integrity of the evidence is not violated; it details those procedures that must be followed to ensure that the evidence does not get compromised during the different stages of the investigation. Furthermore this clause also specifies the requirements of how the evidence is to be transported, packaged and sealed. The clause further describes the requirements for the protection of evidence whilst transporting from unauthorised personnel and environmental factors such as shock and heat damage (BSI2 2006 & ACPO 2012).

To summarise, one believes that FF must ensure that it can support those who are conducting the investigations as much as reasonably practicable. Furthermore, each of these activities discussed should be completed if a system is to be considered a case management system specifically for digital forensics. However despite reports in ones feedback that this standard may become

mandatory in the near future, one believes that a digital forensic case management system should be proficient in supporting laboratories by supporting these activities regardless. Therefore, it is recommended that once the system has been completed, that the developer considers the requirements of this standard previously discussed in finer detail and make the required modifications to the system should they be required.

### **ISO/IEC 27001 - Information security management**

It was determined that this standard is particularly important and relevant to case management systems. The primary objective of this standard is to assist organisations with the management of sensitive information. This aspect is particularly relevant for FF as it is likely that this system will be used to store sensitive images or documents. This standard utilises an information security management system (ISMS) in order to ensure that a system remains up to date with ever changing external threats. This standard is not industry, size or technology specific; therefore it covers a substantial amount of information to ensure it is relevant on a wider scale (BSI3 2013).

Certification for this standard can be acquired but it is also not mandatory, although becoming certified could demonstrate that a company uses best practices to ensure the safety of its data/information. Furthermore if a system has not considered the requirements included in this standard, it is likely that their information system is not appropriately protected. Conversely just becoming accredited to this ISO standard doesn't guarantee the safety of the system either, once accredited FF would be responsible for maintaining and ensuring their system is kept up to date and protected against emerging threats.

On initial analysis of the system it is believed that the system does not possess networking facilities; as a result one would recommend the developer of FF to consider this standard in greater depth prior to enabling any networking features.

## **Overview of ISO standards**

To summarise ones findings of this analysis, it was determined that although the standards represent the best practice methods, FF should endeavour to implement and support these requirements regardless. Furthermore, FF may experience difficulties in justifying the costs of accreditation due to it being open source software and still being in its early stages of development. Therefore, it is recommended that FF utilise specific aspects from each ISO standard that has previously been discussed and concentrate on building the system prior to acquiring accreditation for any of these standards. This will ensure that FF captures some of the criteria for these standards, and the remaining can be included at a later stage if accreditation becomes mandatory or if the developer chooses.

## **Comparison of Foreman Forensic and the Forza framework**

The following section will discuss the proposed recommendations generated from analysing the current system alongside the Forza Framework designed by Leong (2006). The recommendations will be structured in order of their roles previously discussed in the Implementation section.

### ***Case Leader***

According to Leong (2006) the case leader is considered to be the person who plans and orchestrates the entire digital investigation process. This person will be responsible for making the decisions on whether the case has scope for further progression or whether it should be discontinued.

On examining the case leader/manager section it is recommended that the developer implements a feature that records the key personnel that have an involvement in the case. This could include the suspects, witnesses, system owner, victim and the reporting person. The possession of this information could save significant amount of time when other members of the team require knowledge on the involved parties. Furthermore, this information can be used to identify any relationships between the personnel involved in the case e.g. did the owner report the case or was it someone else.

The framework recommends that the case manager should acquire specific timings related to the case. These timings should include the time that the incident occurred, the time it was reported, the start time and time that the activity finished (if relevant). Although this can be inserted manually into the 'case background' section, it is believed that this is important information and it should have its own section in order to retrieve the information more efficiently.

There is currently no feature on FF that requests geographical positions/locations where the crime/incidents took place. The inclusion of this information could be beneficial to identify whether there are any particular patterns emerging particularly if there are a large number of incidents/crimes involved in a single case located in a specific area of a company.

### ***System or business owner***

Leong (2006) considers the system or business owner to be the victim or sponsor of the case, alternatively depending on the type of case, this person can also be considered as the main suspect of the investigation.

Therefore this phase of the investigation would require the case leader to develop his or hers understanding of the situation that they are required to investigate. This can be completed by carrying out initial interviews with the system/business owner or their representative (Leong 2006).

It was not possible to determine any missing or potential features that FF could include to improve this phase of the framework. This is due to the belief that the case manager does not need to follow a rigid framework in order to develop a basic understanding.

### ***Legal Advisor***

Leong (2006) states that once the background of the case has been determined, the next step in the FORZA investigation framework would be for the case leader/case manager to determine the legal requirements of that particular investigation/incident.

A legal advisor is considered to be the initial advisor who provides the case manager with legal assistance in order to determine the course of the case/investigation (Leong 2006). Therefore, on examining the proposed activities that this phase of the framework entails, the following recommendations have been generated.

Foreman Forensic already possesses an option that allows the systems administrator to create user profiles and assign role based permissions. However, it is recommended that a 'signing off' feature is implemented that would enable law practitioners to approve or decline different aspects relevant to the case/investigation e.g. is capturing a specific piece of evidence worthwhile?

Currently, the role 'authoriser' is primarily used to respond to 'requesters' at the very initial stages of an investigation. This modification would assist and improve the efficiency and quality of evidence retrieval as it will improve the communication between the IT and legal divisions of an investigation/case. Furthermore, this could also reduce the time that is spent processing ineffective evidence or leads as any evidence that possess no legal value can be disregarded earlier in the investigation.

According to Leong (2006), in order for the legal advisor to provide a recommendation whether to proceed, he/she will need to consider a substantial amount of legal constraints about the case/investigation. The required information is as follows;

- Identify the objectives of the investigations i.e. have a crime been committed?
- Identify the legal background and preliminary issues that have arisen i.e. what information should be collected, determine information regarding the relevant law
- Identification of what procedures the investigation must follow i.e. require warrants, injections
- Identify participants of the investigation.
- Identify the maximum and minimum timeframe of the investigation

(Leong 2006)

Once this information has been acquired, the case manager would be able to determine the next steps in order to satisfy the legal aspects of the case.

Therefore, it is believed that FF should create a feature that could record or install a process that ensures that all of the above factors are considered in order to ensure all required information regarding the legal aspects of the case is secured earlier in the investigation. This information should then be accessible on the system so that the case manager can ensure that the correct procedures can be deployed. Although this feature is not an essential requirement, this feature would evolve the current system as it would be incorporating the legal aspects into the system. Furthermore, this addition would also assist FF becoming a more comprehensive 'end-to-end' case management system.

### ***Security/system Architect/Auditor***

The next step in the FORZA investigation framework is to examine and explore the involved system in greater detail (Leong 2006). This process would seek to identify information regarding the design of the system that is being investigated. This could be considered as the stage in the framework that is responsible for acquiring specific technical information from the victims or from the technical staff employed by the business/system owner.

Whilst considering the number of potential offences and the substantial amount of relevant information that would need to be captured, it is likely that the case manager may not capture each fact regarding the case. Therefore, in order to assist with the retrieval of information, the system could propose an automated list of questions which can be accessed by the investigator. The results can then be uploaded to the system and accessed by all personnel involved in the case/investigation.

### ***Technical Presentation Level and Data acquisition layer***

Once the relevant information is captured from the previous phase, the next two steps are related to the planning and execution of the procedures required carrying out the case/investigation (Leong 2006).

The FF system currently allows the case manager to assign principal and secondary forensic investigators for specific tasks. In addition the investigator is able to upload notes that will be hashed on submission and relevant files in support of the investigation/case.

Although the current system is able to log the required events/evidence, it may not be as suitable as rival competitor's mobile applications. Therefore in order to improve the functionality of the system whilst in the field, one recommends implementing a system that can be used on mobile devices similar to Blackthorns Case Notes mobile app. Furthermore, this is not an essential requirement as the system can be used effectively on a laptop. Although this recommendation may not be feasible for implementation at present, it is believed that this feature should be considered for future implementation. Furthermore; the developers of the system should begin considering some of the background functions that may be required to host a mobile application.



### ***Data analysis layer***

This stage of the framework requires the evidence that has been transported to the lab to be further analysed and reviewed to determine its relevance and importance to the case. The current system has successfully provided the means to document and record such evidence. One of the key features of this phase in the FORZA framework (2006) is the ability for the investigators to identify the chain of custody and timeline of the proposed incident. During examination of FF system, it was noticed that there is not option to include the date or time for the addition of evidence. It is believed that if the system was able to generate graphical timelines for the addition of evidence in the reports section of the system, this feature would assist all those involved in the investigation as it would organise the events in a manner than can be easily understood.

### ***Legal presentation layer***

The final phase of the FORZA framework is to reevaluate the full details of the incident/event from a legal perspective and determine whether there is a requirement for further evidence or investigation. The current system has a feature which supports this requirement as it provides a Quality assurance feature. The purpose of this feature is to determine whether the case has achieved the required objectives. Alternatively if the quality assurance is not passed this investigation will return to the previous stage and the process will be repeated until a pass is achieved. As discussed previously user profiles can be created in the administrator section of this system, therefore it is feasible that user profiles for legal teams to be manually created and achieve the requirements of this phase.

## **Evaluation of results**

In order to determine the effectiveness and suitability of my proposed recommendations I decided to send them to the developer to get her opinion. The following text is the feedback received for the proposed recommendations that was forwarded to the developer of FF (Appendix 15).

*Hi James,*

*You've done a really great job and come up with some excellent suggestions. Many of which are on my to-do list, and some are new ideas which I will add onto the list! I have tried to add a comment for each recommendation I've found. Let me know if they don't make sense or you need any further clarification.*

*Thanks,  
Sarah*

(Sarah Foreman- Developer of Foreman Forensic)

Overall, I am pleased with the feedback that my recommendations received particularly as this project identified some areas that previously been considered and those that had not.

The full comprehensive list of recommendations complete with the comments can be seen in Appendix 16. Instead, this section will now provide a brief description of the most salient comments that was received from the developer of FF.

I was particularly pleased that my project identified features that the developer had already considered. The developer is significantly more experienced and knowledgeable than I am at digital forensics processes; therefore I was pleased that my approach produced results that she had previously considered as this in effect proves the accuracy of my approach.

This was verified in the recommendations to include hover over help or providing a feature to cancel the upload of a photograph. The developer had already identified these issues and had assembled a plan for the inclusion of JavaScript to rectify these issues.

Additionally, I was particularly pleased with some of the proposals I suggested that had not been previously considered by the developer. To highlight a few, the developer was pleased with the suggestions of;

1. Implementing a feature for the user to select a time zone.
2. Improving the security requirements regarding a user manually changing the time of the local machine.

This factor verifies that my chosen approach has the capacity for identifying factors that an experienced and knowledgeable practitioner did not foresee in the initial stages of development.

Finally, although many of my proposed recommendations were considered to be positive and feasible, I did produce a small number of recommendations that were incorrect or unfeasible.

I mistakenly misjudged the system's ability to be used on a network; therefore I suggested the implementation of features that were already in existence. However, in my defence there is currently no written documentation/manual available and I was only informed of this feature once I had received feedback for my recommendations. Additionally, I believe that had I been able to conduct an in depth conversation/interview with the developer I may have been able to identify this earlier in the project.

Secondly, I had presumed that the developer of this system had the intention of developing a system that would potentially be used to compete with other systems. However, the comments also stated that she had no intention of the system generating any form of financial benefit or competing on a larger scale. Consequently this currently cancels any recommendations that I suggested for the growth of FF in terms of it rivalling other competitors.

To summarise, I was satisfied that my recommendations covered a wide range of areas whilst satisfying the developer of the system. I strongly believe that situations can change quickly, although the system may not have the aspirations for generating revenue at the present this may change in the future. I hope that my recommendations have provided the developer with the knowledge should she ever consider evolving the system further.

Finally, it is also hoped that my suggestions have identified some key features or required additions to encourage organisations such as Universities to use this system for case management purposes on digital forensics courses.

## **Future Work/Opportunities**

As previously discussed earlier in the report SSM can be considered to be a never ending cycle, therefore if this project was to continue it could be restarted from the initial stage of the methodology. This would mean that once the proposed recommendations have been implemented, the problem solver would complete each of the specified stages again. However, this project initially utilised a transcript and adopted the a MDACF (Georgiou 2006) framework, alternatively the second cycle would not be required to adopt this approach as the problem solver would already possess an enhanced amount of background knowledge regarding this problem situation.

The 'Analysis123' results not included in this project allows the opportunity for further analysis, furthermore the modelling of other worldviews and transformations could also be used to identify whether there are any other conflicting or different perceptions between different stakeholders involved with case management activities.

In the event that this project is re-commissioned, once the problem solver arrives at stage 5 where he/she is required to conduct a comparison between real and systems worlds, it is likely that alternative methods may be required rather than the ones utilised in this cycle. This was due to the responses that one received from the surveys and the decisions that were made to identify specific areas from the models. Therefore, it is likely that an alternative approach may be required to accomplish another specific requirement.

Furthermore, there are opportunities for future work in analysing other ISO standards that this project did not consider; also the analysis of the staircase model for digital investigations also provides scope for future work.

Finally, this process could be recycled on a continual basis as part of routine maintenance to ensure that the system is kept up to date and is achieving its targets.

## **Conclusion**

This section aims to summarise my conclusions in respect to the achievement of each aim identified at the initial stage of the project.

**Aim:** Identify main stakeholders of case management processes and determine whether there are any conflicting opinions on what case management represents.

**Conclusion:** This Aim was partially achieved, the choice of implementing SSM lead to the identification and analysis of the FORZA framework which considered multiple roles involved in digital investigations. However, I did not acquire any knowledge from the different perspectives of these stakeholders. This was due to my decision of only analysing one perspective due to the time constraints associated with this project.

**Aim:** Identify leading forensic case management systems and determine the key features of each platform.

**Conclusion:** The completion of tabular analysis achieved the primary objective of this aim, although this was completed by utilising public and online documentation as ones attempts to communicate with relevant companies/communities proved to be ineffective.

**Aim:** Measure usability, efficiency, and effectiveness of the interface of each system identified in previous aim.

**Conclusion:** The employment of Neilson's heuristics in this project ensured that this aim was completed through a structured and highly effective approach. Furthermore, the comparison of the features included on FF and leading digital forensic case management systems achieved by conducting tabular analysis determined how effective FF was at completing certain tasks.

**Aim:** Successfully extract both Tacit and Explicit knowledge from users of Case management systems in both the private and public sectors of industry.

**Conclusion:** The retrieval of explicit knowledge was achieved by means of the surveys that were sent to the police forces and developer. However, it was not possible to acquire any tacit knowledge from these persons as I was unable to meet or conduct face to face interviews with the relevant parties. Although, the completion of this project has developed my own levels of tacit knowledge particularly in terms of generating an understating of how a successful case management system operates.

This project attempted to complete the previously mentioned aims as far as reasonably practicable. Unfortunately it became very difficult in acquiring any feedback or support from those external to the University and I was forced to utilise the contacts that I did have. Fortunately, Mr Mike Daley knew two police officers from two local police forces that would complete my surveys. In the event that these officers were not available, the outcome of this project may have been very different.

Although, I am very appreciative for the contribution from the police and developer of FF, I believe that had I been given the opportunity to meet these people in person I may have potentially obtained richer information which could have improved the quality of my recommendations.

In future projects, I would take more care to ensure that I have the resources or contacts in place prior to developing specific project aims particularly if they are dependent on third persons. However, I also understand that issues such as this may be beyond my control and that the success of the project would be based on how effective my response is to such instances.

In conclusion, I am very pleased with my decisions to adopt the approaches and methodologies used in this project, particularly as this was my first attempt of mixing multiple approaches in order to analyse a system and due to the positive feedback that my recommendations received.

## **Reflection**

This project has been one of the most challenging yet one of the most interesting and most enjoyable I have completed whilst at University.

Prior to accepting this project I initially proposed my own idea; unfortunately I could not find a lecturer who would accept my project due to the lack of knowledge in the chosen area. I had recently completed the Security and Forensics module with Mr Mike Daley and it was on an informal conversation with him that I first heard about this project.

I was immediately attracted and interested in pursuing this project and although I was not able to complete my own project, this project shared many similarities in a subject that I had a strong interest in.

The initial concern I faced was ensuring that this project included a technical background as opposed to writing a generic list of recommendations. Although I have used Systems Thinking previously, I was not confident in my ability to use this method especially in my final year project.

However, having considered all the options available and having brief discussions with Mrs Catherine Teehan, I decided that I would use Systems Thinking in this project. It was at this stage where Mrs Catherine Teehan had introduced me to the MDACF paper.

Prior to this project I had only used Brian Wilsons' version of Soft Systems Methodology, the MDACF journal utilised Checkland's method which I believed to be slightly easier to understand. The main difference I found was the restriction on the number of activities that the conceptual model required, that being seven plus or minus two activities for Checkland's version.

Initially I found the paper very difficult to understand, this was due to my lack of experience of reading academic papers and due to my restricted knowledge of the approaches that were in the paper. I recall spending a large amount of time converting words and concepts that were in the paper into a format that I could understand.

However, as the project progressed so did my confidence. As a result I am no longer intimidated by the thought of reading advanced academic papers and will continue to do so in future, specifically as I found these more informative than my traditional sources of information.

The MDACF framework was undoubtedly the hardest task for this project, although it did provide me with an initial insight that I used to progress, I am still undecided whether I would reuse this approach in future. Alternatively, although it is primarily used in the business contexts, I would be very tempted to use a SWOT analysis in its place. However, I was very impressed by the amount of information that this framework retrieved by only utilising a small sections of information.

I believe that a valid explanation of the reason why I found MDACF framework so difficult was due to it being the initial stage of the project. As I have mentioned my confidence grew as the project progressed and I believe that similar tasks were being completed more efficiently and effectively once my confidence in my own abilities were improved

Prior to this project, although I had previously formulated root definitions and developed conceptual models, these were for problems that shared no similarities with this particular situation. The proposed paper demonstrated the use of 'Analysis 123' method which I found to be extremely effective and helpful, particularly for building the root definitions. Alternatively I could have only used a rich picture; however I believe that should I ever be required to use SSM in future, I would develop a rich picture as a brainstorming exercise and then convert its contents into the 'Analysis 123' method. This is due to the manner in which it is structured and the ease of using the information in the building of root definitions.

As I have previously mentioned I have been very apprehensive and unsure about the quality of the work that I have been producing, I believe that this was due to my lack of knowledge and experience regarding the chosen approaches. Unfortunately Mr Mike Daley has very limited knowledge in Soft Systems Methodology and could not provide a substantial amount of support. Although, prior to starting this project Mr Daley did inform me that my decision to proceed with the inclusion of Systems Thinking was done so at my own risk.

Dr Wendy Ivins agreed to provide me with some unofficial guidance for the implementation of SSM, although I always felt reluctant to approach her too often as she had her own dissertation students and projects. However, she was able to validate my models and ensure that I was utilising the approach in the correct manner.



In reflection, although Mr Daley may not have possessed a substantial amount of knowledge for SSM, he is an expert in digital forensics. Consequently, I was able to share some of my ideas with him and he was able to validate them from a digital forensic perspective. Conversely, if I was allocated a supervisor who had SSM knowledge, they may not have had the digital forensics knowledge which I also required. Therefore, I don't believe that this has restricted the outcomes of my project in any way.

Overall, I am pleased with the management of time throughout the whole project. The feedback received for the initial plan warned of the dangers involved in acquiring responses from external parties and due to the substantial amount of work that I had proposed. Consequently, I ensured that all relevant feedback was returned prior to the beginning of the Easter recess, this ensured that I was able to communicate with my supervisor and ensure that I had a sufficient amount of time to complete the project. At the initial stage I did not consider sending the results to the developer for her feedback, fortunately as I kept to a strict timescale I was able to do so which I feel has further validated my recommendations.

During the completion of this report I had to ensure that my methods were explained in a manner that was understandable for a reader with limited knowledge. The process of writing the report also removed many of my own insecurities. I believe that if I was required to use this approach for a similar project in future the learning curve would be significantly less time consuming.

The requirement to write this report using third person narrative initially consumed a great deal of time. I found it challenging maintaining consistency throughout the whole project and was required to rewrite several sections of the report on numerous occasions. However, it became more natural and required less effort as the report progressed. As a mature student who went to a Welsh school, I have also felt that my English writing skills was inferior to someone who attended a predominantly English speaking school, however I am pleased with the delivery and style that I have used to write this report

Finally, I am pleased with the outcome of this project. I have recently secured a job as a Business Analyst and Project manager in a Cardiff based company. I believe that the completion of this project has equipped me with the analytical way of thinking that is needed to become a valuable member of a team at my prospective position. I hope that I will get the opportunity to utilise the skills I have learnt in future projects and that FF will make the required changes and become the preferred system for conducting case management within Universities and smaller organisations

## References

- Access Data. 2015. *ADLAB* [Online]. Available at: <http://accessdata.com/solutions/digital-forensics/ad-lab/capabilities>
- ACPO. 2012. *ACPO Good Practice guide for digital evidence*. [Online]. Available at: [http://www.7safe.com/electronic\\_evidence/#](http://www.7safe.com/electronic_evidence/#) [Accessed 20/04/15]
- Barret, D. *Child pornography cases double as paedophiles pursue vile profit from abuse* [online]. Available at: <http://www.telegraph.co.uk/news/uknews/crime/11533252/Child-pornography-cases-double-as-paedophiles-pursue-vile-profit-from-abuse.html> [Accessed: 15/04/15].
- Blackthorn. No Date. *Blackthorn Case Notes*. [Online]. Available at: [http://assets-production.govstore.service.gov.uk/Giii%20Attachments/QCC%20Information%20Security/Bids/Archive2/CaseNotes\\_v1%200.pdf](http://assets-production.govstore.service.gov.uk/Giii%20Attachments/QCC%20Information%20Security/Bids/Archive2/CaseNotes_v1%200.pdf)
- BSI1. 2000. *ISO 9001 – Quality management systems*. UK: BSI
- BSI2. 2006. *ISO17025 General Requirements for the competence of testing and calibration laboratories*. UK: BSI
- BSI3. 2013. *ISO 27001 - Information security management*. UK: BSI
- Casey, E. 2011. *Digital Evidence and computer crime*. London: Academic Press
- Checkland, P. 1999. *Systems Thinking, Systems Practice*. England: Wiley
- Checkland, P & Scholes, J. 1999. *Soft Systems Methodology in action*. England: Wiley,
- Foreman Forensic. 2007. *ReadMe* [Online]. Available at: <https://bitbucket.org/lowmanio/foreman/>
- Georgiou, I. 2006. *Making decisions in the absence of clear facts*. European journal of operational research
- Grimsley, S. 2015. *Systems Thinking in Management: Definition, Theory & Model*. [online]. Available at: <http://study.com/academy/lesson/systems-thinking-in-management-definition-theory-model.html> [Accessed: 29/03/15].
- IntaForensics2 2015. *Lima Enterprise* [Online]. Available at: [www.intaforensics.com/index.php/download\\_file/view/223/214/](http://www.intaforensics.com/index.php/download_file/view/223/214/)
- IntaForensic. 2015. *Lima Product* [Online]. Available at: <http://www.intaforensics.com/software/lima-product-suite/standard/>

ISO. *Standards* [Online] Available at: <http://www.iso.org/iso/home/standards.html> [Accessed: 20/04/15].

Marcella, A. & Menendez, D. 2008. *Cyber Forensics- A field manual for collecting, examining and preserving evidence of computer crimes*. USA :Auerbach Publications

Neilson, J. 1995. 10 Usability Heuristics for User Interface Design. [online]. Available at: <http://www.nngroup.com/articles/ten-usability-heuristics/> [Accessed: 26/03/15]

Robson, W. 1997. *Strategic Management and Information systems*. England: Prentice Hall

Rosehead, J & Mingers, J. 2001. *Rational analysis for a problematic world revisited*. England: Wiley and Sons Ltd

Sammons, J. 2012. *The basics of digital forensics- The primer for getting started in digital forensics*. USA :Syngress

SC Magazine. 2013. [Online]. Available at: <http://www.scmagazine.com/intaforensics-lima-forensic-case-management-software/review/3874/>

Wakefield, J. 2014. *GCHQ, terrorists, and the internet: What are the issues?* [Online]. Available at: <http://www.bbc.co.uk/news/technology-29897196> [Accessed: 15/04/15].

# **Appendices**

## **Appendix 1 Foreman Transcript**

Foreman is a new open source forensic case management system. In today's market there is a plethora of digital forensics software available for investigators, from small scripts that do a single task to full-featured toolkits that can aid an investigation from start to finish. However, there is a lack of simple forensics oriented case management software. Whilst there are enterprise products such as Intaforensic's Lima and Blackthorn's Casenote, there is nothing available that is free, simple and open source.

This results in too many companies with forensic departments using generic ticketing systems such as those intended for helpdesks. Others rely on a mixture of spreadsheets, documents and emails to track cases. These solutions are inherently difficult to work with as they lack many features that are important to forensic case management. Often this leads to the various parts of a case being scattered over different systems, making it difficult to see everything related to a case in a simple, cohesive format. The intention of this project is to study a range of different digital forensic companies, departments and police forces on how they perform case management and determine how Foreman compares.

## Appendix 2 Uncertainties

Uncertainties			
	<a href="#">Uncertainties applicable to the working Environment.</a>	<a href="#">Uncertainties applicable to guiding values</a>	<a href="#">Uncertainties applicable to structural relations between decision junctures (points in time)</a>
<u>Section</u>	<u>UE</u>	<u>UV</u>	<u>UR</u>
Foreman is a new open source forensic case management system	Who will this system be created for? Who will be its potential users as a potential open source system?	What are the true objectives and values of the system?	
In today's market there is a plethora of digital forensics software available for investigators, from small scripts that do a single task to full-featured tool kits that can aid an investigation from start to finish.	Uncertainties regarding whether a full featured tool kit is more beneficial and preferred over a smaller scripted system.	Do companies want to have a fully-fledged system to portray an image of superiority against their competitors?	
there is a lack of simple forensics oriented case management software	There is uncertainty with the term 'simple' as the term requires more accurate information. Do they mean simple in terms of 'having few parts and being easy to understand and use' or being classed as 'plain' and having little or no ornamentation.	Is this due to standards that forensics analysts have to adhere to which make such a 'simple' system infeasible.	Would making a case management system too easy reduce the barriers of entry into field and consequently increase competitors?
Whilst there are enterprise products such as Intaforensic's Lima and Blackthorn's Casenote, there is nothing available that is free, simple and open source.	<p>Uncertainly regarding the reasons behind why there is such a small number of companies providing free, open source systems.</p> <p>Uncertainty why foreman would use open source code rather than traditional closed code?</p>	<p>Affected interests from these companies' interests and from the users of such systems.</p> <p>Companies want to make profits whereas users want to save money.</p>	Can such a system be manufactured as open source and still be as functional and effective as a system that has large financial backing?

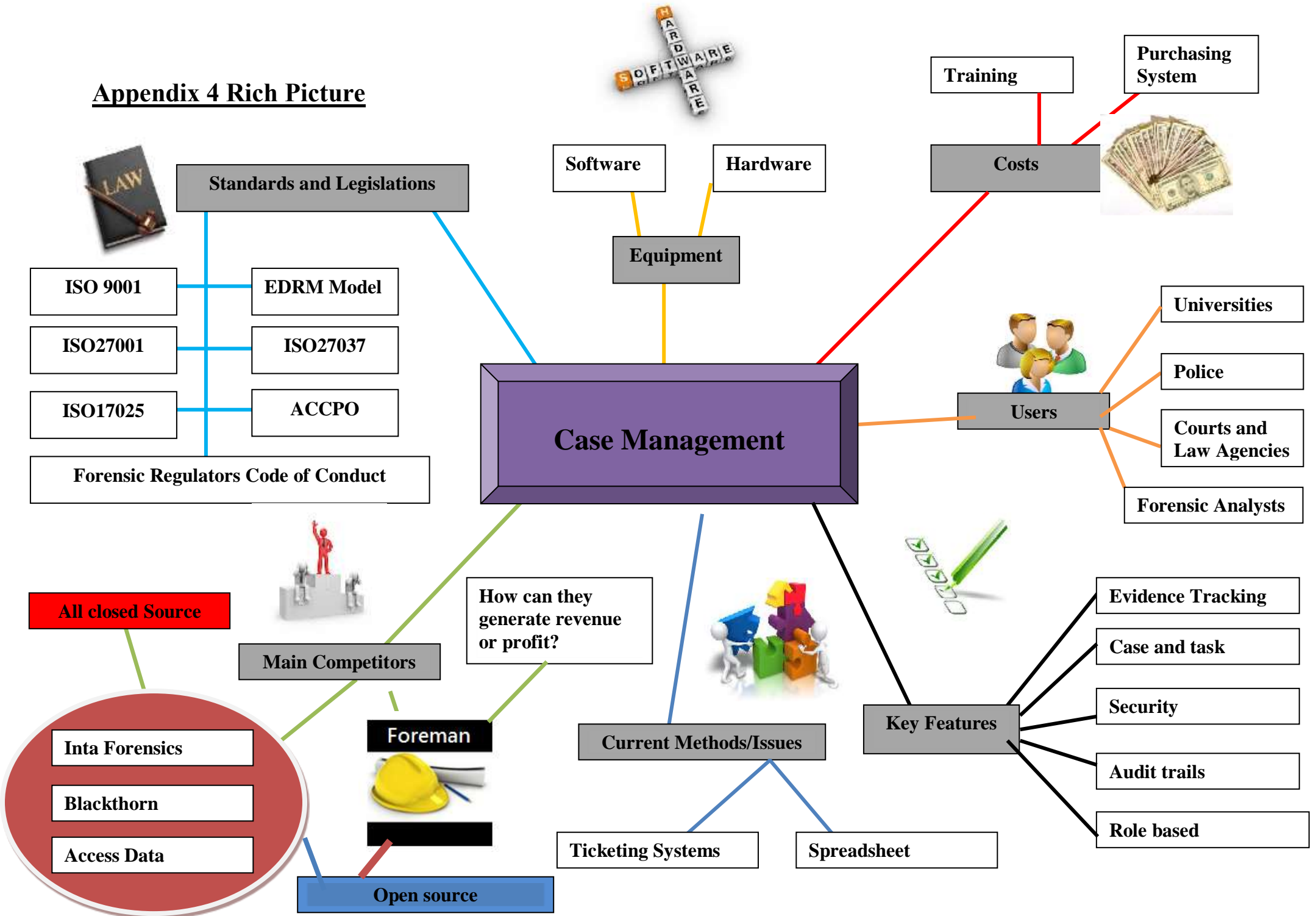
This results in too many companies with forensic departments using generic ticketing systems such as those intended for help desks. Others rely on a mixture of spreadsheets, documents and emails to track cases.	Uncertainty in regards to why generic ticketing systems and spreadsheet, documents and emails may not be sufficient methods?		Would having a single system increase security/access concerns?
These solutions are inherently difficult to work with as they lack many features that are important to forensic case management.	Term difficult may not mean the same for every user.  What features are required to complete the task in hand?	Case management guidelines follow best practices, some forensics analysts may consider one to be more important than the other	Could having too many features remove the requirement for a 'simple' approach?  “Too many cooks spoil the broth”
Often this leads to the various parts of a case being scattered over different systems, making it difficult to see everything related to a case in a simple, cohesive format.	Term difficult may not mean the same for every user.	Uncertainties regarding security policies may not be agreed	Uncertainly stemming from complexity involved in reasons

### **Appendix 3 -Complexity and Conflict**

Sections	Complexity	Conflict
Foreman is a new open source forensic case management system		Conflict may arise in ownership of pieces of code.
In today's market there is a plethora of digital forensics software available for investigators, from small scripts that do a single task to full-featured tool kits that can aid an investigation from start to finish.	Could a fully-fledged system with 'too' many features affect hinder the levels of usability and effectively become too complex for its users.	Conflict may arise from time served analysts who may have a preference for scripted systems rather than using a full featured tool kit or vice versa.
there is a lack of simple forensics oriented case management software		
Whilst there are enterprise products such as Intaforensic's Lima and Blackthorn's Casenote, there is nothing available that is free, simple and open source.	Appears to be filled with complexity as can one system fulfil all its requirements and be free, simple and open source.	Conflict may arise in ownership of pieces of code.
This results in too many companies with forensic departments using generic ticketing systems such as those intended for help desks. Others rely on a mixture of spreadsheets, documents and emails to track cases.	Due to the unavailability of such systems can lead to the rise of unacceptable conditions such as the case information and evidence being scattered across multiple platforms.	Conflict may arise in the event of the loss of evidence or information.
These solutions are inherently difficult to work with as they lack many features that are important to forensic case management.		Conflict may occur if a particular feature may not be available on a system that produces specific information which may be desired by a third party.
Often this leads to the various parts of a case being scattered over different systems, making it difficult to see everything related to a case in a simple, cohesive format.	Can conveying large quantities of information in a simple format be achievable? Significant amounts of information may induce information overload and increase levels of complexity.	



## Appendix 4 Rich Picture



## **Appendix 5 Soft Systems Methodology (Analysis 1, 2, 3)**

Case study segments	Analysis 1		Analysis 2		Analysis 3	
	Who	What	Socio Cultural Dynamics	Notes	Who/what	Power
Foreman is a new open source forensic case management system	Foreman	Open source forensic case management system	Open source	Desire to use code that would be available to the general public for use and/or modification from its original design free of charge.	Foreman/  Open source forensic case management system	<p>Potential to influence people to convert to this system.</p> <p>Power to change system properties to the expectations of the intended users.</p>

Case study segments	Who	What	Socio Cultural Dynamics	Notes	Who/what	Power
In today's market there is a plethora of digital forensics software available for investigators, from small scripts that do a single task to full-featured tool kits that can aid an investigation from start to finish.	Users  Foreman forensic Suite	Heightened level of availability of digital forensics software	Plethora of digital forensics systems	Very disorganised in the methods being adopted by its users as market consists of an excess number of systems designed for the same purpose but adopting alternative methods	Users  Heightened level of availability of digital forensics software  Foreman	Power to impose expectations on system requirements  Power to hide/conceal Foreman forensic suite due to the number of competitors Power to provide a system that fulfils the user's needs.
There is a lack of simple forensics oriented case management software	Users  Foreman forensic Suite	Case management software	Unknown culture as system does not currently exist	Goal culture and innovative culture – desire to achieve a new form of case management.	Users  Foreman forensic Suite	Power to force change Power to become very competitive as no other open source competitors on the market.
Whilst there are enterprise products such as Intaforensic's Lima and Blackthorn's Casenote, there is nothing available that is free, simple and open source.	Competitors	Do not provide any Free, simple and open source software	Conservative culture	Potential conservative culture as nobody previously attempted to develop an open source system for case management before.	Enterprise products  Free, simple and open source software	Market leaders will have power over the market as they are likely to have more resources to impose barrier of entry.

	Who	What	Socio Cultural Dynamics	Notes	Who/what	Power
This results in too many companies with forensic departments using generic ticketing systems such as those intended for help desks. Others rely on a mixture of spreadsheets, documents and emails to track cases.	Companies Users	The use of unsuitable systems and methods	Dependant on the use of generic systems.  Resistance to change.	Current Users are dependent on old type systems which may not be the most suitable and reliable.  Resistance to Change. Users may not be interested in change	Companies Users  The use of unsuitable systems and methods	Forensic science regulator - Code of practice and conduct
These solutions are inherently difficult to work with as they lack many features that are important to forensic case management.	Users of the systems	System features	Different manufacturers likely to have conflicting perceptions on the most important features		Users of the systems  System features	
Often this leads to the various parts of a case being scattered over different systems, making it difficult to see everything related to a case in a simple, cohesive format.	Users of the system	Case evidence	Different types of information may require specific methods or security measures due to the level of sensitivity or confidentiality.		Users of the system  Case evidence	

## **Appendix 6 - Identifying and formulating Transformations**

Case Study Segments	Transformation
Foreman is a new open source forensic case management system	No Transformation specified
In today's market there is a plethora of digital forensics software available for investigators, from small scripts that do a single task to full-featured tool kits that can aid an investigation from start to finish.	<p>Plethora's of systems adopting multiple methods. → Single system which fulfils the necessary requirements.</p> <p>Plethora of different software and approaches being used for investigators → Comprehensive piece of software capable of successfully aiding an investigation from start to finish</p>
there is a lack of simple forensics oriented case management software	<p>Lack of simple forensics oriented case management software → Fulfil the lack of simple forensics oriented case management systems</p>
Whilst there are enterprise products such as Intaforensic's Lima and Blackthorn's Casenote, there is nothing available that is free, simple and open source.	<p>No current system that is free, simple and open source → Successfully developing and delivering such system.</p>
This results in too many companies with forensic departments using generic ticketing systems such as those intended for help desks. Others rely on a mixture of spreadsheets, documents and emails to track cases.	<p>Uncoordinated generic approaches adopted by multiple users → Coordinated and improved standardization in case management.</p>
These solutions are inherently difficult to work with as they lack many features that are important to forensic case management.	<p>Current solutions difficult to use as they lack important features. → Identify Important features to improve systems' usability and processes.</p>
Often this leads to the various parts of a case being scattered over different systems, making it difficult to see everything related to a case in a simple, cohesive format.	<p>Solutions scattered across multiple systems resulting in information retrieval and formatting issues. → Information/evidence structured in a cohesive and easily accessible format.</p>

## Appendix 7 – C.A.T.W.O.E. Analysis

Analyses 1,3	Analyses 1,3		Analyses 2	Analyses 1,3	Analyses 2	
Client	Actors	Transformation	Weltanshauung	Owner	Environment	Root Definition
Users	Foreman Forensic	(T1a) Plethora's of systems adopting multiple methods. → Single system which fulfils the necessary requirements.	The requirement to lower the disorganised manner that forensic case management is being conducted.	Foreman Forensic	In an environment that has a plethora of methods.	A system to ensure forensic case management is conducted in a simplistic and organised manner by providing a single piece of software that fulfils the necessary requirements given the complex environment in which forensic case management exists

Analyses 1,3	Analyses 1,3		Analyses 2	Analyses 1,3	Analyses 2	
Client	Actors	Transformation	Weltanshauung	Owner	Environment	Root Definition
Personnel conducting investigation	Case management system.	(T1b) Plethora of different software and approaches being used for investigators → Comprehensive piece of software capable of successfully aiding an investigation from start to finish	The requirement of key processes which include the planning, capturing, analysing and presentation of digital evidence is conducted effectively.	Case management system.	Adherence to the ACPO good practice guide for digital evidence and the relevant British standard to that specific activity.	A System owned and operated by personnel conducting digital forensics investigations to comply with the principles of digital evidence whilst undertaking forensic analysis procedures such as the planning, capturing, analysis and presentation of digital evidence in order to aid an investigation from start to finish satisfying the constraints defined in the ACPO Good practice guide for digital evidence whilst satisfying the relevant industrial standards specified for each activity throughout the investigation process
Users	Foreman Forensic	(T2) Lack of simple forensics oriented case management software → Fulfil the lack of simple forensics oriented case management systems	a system is required to alleviate the current lack of simple forensics oriented case management software	Foreman Forensic	In a market that has currently been unable to produce such a system	A system to ensure forensic case management is conducted in a simplistic and organised manner by providing a single piece of software that fulfils the necessary requirements given the complex environment in which forensic case management exists

Analyses 1,3	Analyses 1,3		Analyses 2	Analyses 1,3	Analyses 2	
Client	Actors	Transformation	Weltanshauung	Owner	Environment	Root Definition
Users	Foreman Forensic	<p>(T5) Current solutions difficult to use as they lack important features. → Identify Important features to improve systems' usability and processes.</p>	Specific features are required in order to successfully carry out case management effectively.	Foreman Forensic	Different manufacturers likely to have conflicting perceptions on the most important features	A System owned and operated by Foreman Forensic to Specify features that are required in order to provide simple, easy to use forensic case management software by identifying and implementing specific key features and processes given the constraints of different companies possessing different opinions on the most essential features to achieve Forensic case management for its users.
Users	Foreman Forensic	<p>(T6) Solutions scattered across multiple systems resulting in information retrieval and formatting issues. → Information/evidence structured in a cohesive and easily accessible format.</p>	Information should be stored in a single location which is easy to retrieve and access.	Foreman Forensic.	Different types of information may require specific methods or security measures due to the level of sensitivity or confidentiality.	A System owned and operated by Foreman Forensic to further enhance a current system that allows its users to retrieve and access information from a single location by means of organising the information in a structured, cohesive, easily accessible format given the constraints of the compulsory security measures involved in different types of evidence to achieve Forensic case management for its users.



## **Appendix 8 - Root Definitions**

Root Definition	Notes
A system to ensure forensic case management is conducted in a simplistic and organised manner by providing a single piece of software that fulfils the necessary requirements given the complex environment in which forensic case management exists.	Not specific to Case management activities so will not model this root definition.
A System owned and operated by Foreman Forensic Suite to address the current requirements for a free, simple, open source system that is currently not being met by means of successfully developing and delivering such system given the constraints of constraints of a competitive environment creating barriers of entry in order to achieve Forensic case management for its users.	Not specific to Case management activities so will not model this root definition.
A System owned and operated by Foreman Forensic Suite to ensure a co-ordinated and Standardised approach to case management by implementing pre-defined industry standards given the constraints defined by the Forensic science Regulator in order to achieve Forensic case management for its users.	
A System owned and operated by Foreman Forensic to determine which features that are required in order to provide a simple, easy to use forensic case management system by identifying and implementing key features and processes given the constraints of different companies possessing different opinions on the most essential features required for Forensic case management.	
A System owned and operated by Foreman Forensic to provide a system that allows its users to retrieve and access information from a single location by means of organising the information in a structured, cohesive, easily accessible format given the constraints of the security procedures involved in using a variety of evidence to achieve Forensic case management for its users.	Not specific to Case management activities so will not model this root definition.
A System owned and operated by personnel conducting digital forensics investigations to comply with the principles of digital evidence whilst undertaking forensic analysis procedures such as the planning, capturing, analysis and presentation of digital evidence in order to aid an investigation from start to finish satisfying the constraints defined in the ACPO Good practice guide for digital evidence whilst satisfying the relevant industrial standards specified for each activity throughout the investigation process	

## **Appendix 9 – Comparing models with real world**

### **Forensic Investigation Survey**

#### ***Appendix 9a Feedback from South Wales Police – Bridgend***

Please complete the following questions to assist with the validation of ones models. If a question is not applicable then please type N/A and progress to the next question.

Do you use different frameworks for conducting forensic investigations? E.g. Oscar  
If so, how do you measure whether it is effective framework?

The underpinning framework adopted by Police for investigations involving Digital Media Investigations would be the 'ACPO Good Practice Guide for Digital Evidence'.

Specifically this would incorporate the following phases:

- Plan
- Capture
- Analyse
- Present

Measurement of the framework would be based around debrief sessions held during and post investigation, coupled with feedback / experiences received from the CPS and the relevant Court who heard the case.

The framework provides an overview to our processes, but the specific tactics and methodologies used are constantly changing and evolving to meet the requirements of current technologies and approaches that are used by subjects.

How do you ensure you follow the ACPO guidelines?

The ACPO guidelines and specifically the 4 principles of digital evidence underpin all actions carried out by law enforcement.

The principles are incorporated and fundamental in initial training by officers directly involved in the Digital Media field.

The principles have now been built into a mainstream cyber crime course which is delivered to Detective and Beat Officers to ensure they have a firm grasp of how to preserve and maintain best digital evidence.

Within the Regional Cyber Crime Unit the principles were used as a foundation to create the Standard Operating Procedures that are followed day-to-day.

Do you monitor compliance of investigation processes against ISO standards?

Presently ISO standards are not used directly to monitor compliance of investigation processes.  
However, preparations are currently underway to seek ISO 17025 accreditation for our Units Forensic Lab and processes ready for 2016. At this point investigation processes will be mapped against the compliance matrix of ISO 17025.

Do you agree that there are 4 main stages of an investigation being planning, capturing, analysing and presenting evidence?

I would agree with this statement, as mentioned previously these are the phases documented within the ACPO Good Practice Guide for Digital Evidence.

Do you conduct initial planning for different forms/types of investigations?  
If so, how do you measure whether the planning was effective for that investigation?

Every investigation will be different in terms of the planning requirements. There are always basic functions that will always be carried out, such as conducting police system intelligence checks. Typically open source research will be carried out on all aspects of the investigation.  
Depending on the subject, the offence and the background will determine what further planning will be required.  
Every investigation carried out thus far has provided valuable lessons about what could have been done differently. Most importantly we have learnt that you cannot plan for every eventuality, but what you can have is systems and contacts in place to detail with issues or problems that are encountered.  
The reflection portion of the investigation has been very important in identifying learning points going forward.

Do you use different methods for capturing evidence?

If so, please provide an example and state how you would measure its effectiveness?

Within our unit we use a number of methods to capture evidence.

This will fall into two main categories –

- live / volatile data acquisition
- ‘dead box’ data acquisition

Within each category we have a number of different methods and tools to acquire evidence. This is to ensure there is no single point of failure.

Effectiveness is tested by first and foremost ensuring that Hash values for acquired data match between source and exhibit. This would be viewed as a success.

Multiple tools / approaches are also used to ensure that we are able to repeat our own processes with the same results.

Do you use different methods for analysing different forms of evidence?

If so, please provide an example and state how you would measure its effectiveness?

Our unit has a number of tools to conduct a forensic analysis of evidence. Each forensic tool would have a specific purpose within an investigation.

EnCase – is used as base forensic analysis tool for windows based systems.

BlackLight – is used as base forensic analysis tool for Mac based systems.

IEF – is used to parse internet artefacts within exhibits.

These three tools are used as the main forensic analysis tools. A number of other products are used to validate results; this will depend on the examiners preference.

Validation of results is used by the examiner to measure effectiveness. This is also combined with peer review of an exhibit.

Do you consider using different methods for presenting different forms of evidence?  
If so, please provide an example and state how you would measure its effectiveness?

I can only answer this question from a perspective of what we intend to do. The unit is newly formed and as yet we have not been required to present evidence in court. This is likely to change in the very near future.

Ultimately as law enforcement our main responsibility is not to present evidence as anything more than what it was when it first came into police possession.

What we are able to do is present evidence in a format that can be understood and interpreted by the court / jury. This will be achieved through physical presentation of evidence in an easy to understand manner or using user-friendly jury bundles.

The effectiveness will be assessed through direct feedback of the court, as opposed to the result of the trial.

Thank You for taking the time to complete the survey, your contribution and time is appreciated.

James Owen

# Forensic Investigation Survey

## *Appendix 9b Feedback from Gwent Police*

Please complete the following questions to assist with the validation of ones models. If a question is not applicable then please type N/A and progress to the next question.

Do you use different frameworks for conducting forensic investigations? E.g. Oscar  
If so, how do you measure whether it is effective framework?

Not using any frameworks at this time. However, we are looking at some changes with policies and procedures in the near future and it is possible that a framework of some sort may be brought into use, either for triaging or for cases where numerous exhibits have been seized.

How do you ensure you follow the ACPO guidelines?

The guidelines have not changed vastly in the 10 years I have conducted computer forensic investigations, so they have become pretty much ingrained. We do keep a set of the most recent guidelines to refer to if need be, but most of the time it is just a natural part of the investigation.  
I did look at them a few weeks ago when I had to image an iPod. It wasn't behaving as a normal device and required a certain amount of hands on use of the physical device. I did a recheck on the guidelines to ensure that this kind of dirty forensics was still catered for when all else has failed.

Do you monitor compliance of investigation processes against ISO standards?

N/A

Do you agree that there are 4 main stages of an investigation being planning, capturing, analysing and presenting evidence?

Yes, totally. It is simple and effective and I believe in the KISS principles of it. I also find that the first 3 stages are often repeated in large multiple exhibit cases where I don't initially decide to examine all items. i.e. look at main computer, if there is little or no evidence on that machine, then plan and capture, analyse the next viable piece of equipment.

Do you conduct initial planning for different forms/types of investigations?  
If so, how do you measure whether the planning was effective for that investigation?

To a degree I do. Different jobs are looking for different types of evidence, but most of what I deal with is illegal images of children and therefore they are tackled in much the same way. The plan changes more when the evidence being sought is more specific, especially for fraud investigations. They tend to vary quite widely as to what is sought.

Do you use different methods for capturing evidence?  
If so, please provide an example and state how you would measure its effectiveness?

I use a range of different tools. The main one is Encase, but I also use ASR SMART, FTK imager, XRY, Oxygen Forensics. For obscure captures, I just use whatever I think will get me the best copy. I have been working on a damaged Apple iPod which I cannot acquire using Encase, Oxygen or XRY, so I created a device backup using iTunes and imported this into Encase 7. Another occasion with a troublesome tablet was a drag and drop from windows explorer. Crude, but it was the best evidence under the circumstances. In terms of their effectiveness; the main stream tools for capturing standard drives are pretty much all the same with slight differences in speed, but the end result is the same. I wouldn't like to commit myself to saying one was better than another.

Do you use different methods for analysing different forms of evidence?  
If so, please provide an example and state how you would measure its effectiveness?

Yes. Depending on what the data artefact is. Encase 6/7 is the main analysis and carving tool, but there are many others I use and too many to list here. I pretty much figure this out as I go along. Often I will carve elements out of a case for analysis in a more specialised piece of software. With the recent explosion of tablets I am finding that the evidence is tied up in SQLite databases. As such I have to switch to more database related tools and create my own raw queries.

In terms of effectiveness, some of the tools I use I am quite happy to say that what I am seeing is an accurate interpretation. For those I don't use as often or give odd results I will analyse the particular artefact in another program and compare results.

Do you consider using different methods for presenting different forms of evidence?  
If so, please provide an example and state how you would measure its effectiveness?

I present my evidence in a partial template word document that I aim to keep as clear and simple as possible. On occasions I will paste in a screen shot or chat log etc. If the information is too much, then I offer it in electronic format with some sample entries in the court file. The effectiveness is whether or not I have to give further explanations to court.

Thank You for taking the time to complete the survey, your contribution and time is appreciated.

James Owen



# Foreman Forensic Survey

## *Appendix 9C Feedback From Foreman Forensic Developer*

Please complete the following table/questions to assist with the validation of ones models. If a question is not applicable then please type N/A and progress to the next row.

### Root Definition

A System owned and operated by Foreman Forensic Suite to ensure a co-ordinated and standardised approach to case management by implementing pre-defined industry standards given the constraints defined by the Forensic science Regulator in order to achieve Forensic case management for its users.

<u>Activity</u>	<u>Does this activity exist?</u>	<u>How do/did you do it?</u>
<b>Notes</b>	<b>Yes/No</b>	<b>Please provide as much detail as possible</b>
Determine variety of approaches being used to conduct Case management.  Example- ticketing, spreadsheets etc.	Yes	From previous experience and talking to lots of other forensic investigators I know the different ways to conduct case management. I wanted to make sure foreman had the cleanest and easiest way to manage cases that is reliable and forensically sound.
Understand industrial standards that are in place Example –Quality management and other ISO standards	Yes	The ACPO Good Practice Guide for Digital Evidence guidelines on audit trails, chain of custody and accountability.  There is also NIST Computer Forensics Tool Testing (CFTT).  ISO27001 and 9001, information security standards
Determine which standards are applicable to Foreman Forensic Suite.	Yes	ACPO guidelines very important and followed. CFTT is applicable once the tool is completed. ISO standards not so much, but I may

		look into the standards later
Assess compliance of relevant standard.	yes	ACPO guidelines followed. I will consider CFTT testing on completion. No idea about ISOs as not looked into them yet.
Determine whether any modifications are required to be made to Foreman Forensic Suite to comply with standard.	Yes	I may need to modify the tool for CFTT, not looked in enough detail just yet.
Implement any required modifications to Foreman Forensic Suite.	yes	As above. ACPO guidelines followed and implemented from the start
Ensure modification to Foreman Forensic Suite satisfies relevant standards	yes	Yes for ACPO guidelines.

Thank You for taking the time to complete the survey, your contribution and time is appreciated.

James Owen

# Foreman Forensic Survey

## *Appendix 9c Feedback From Foreman Forensic Developer*

Please complete the following table/questions to assist with the validation of ones models. If a question is not applicable then please type N/A and progress to the next row.

### Root Definition

A System owned and operated by Foreman Forensic to determine which features that are required in order to provide a simple, easy to use forensic case management system by identifying and implementing key features and processes given the constraints of different companies possessing different opinions on the most essential features required for Forensic case management

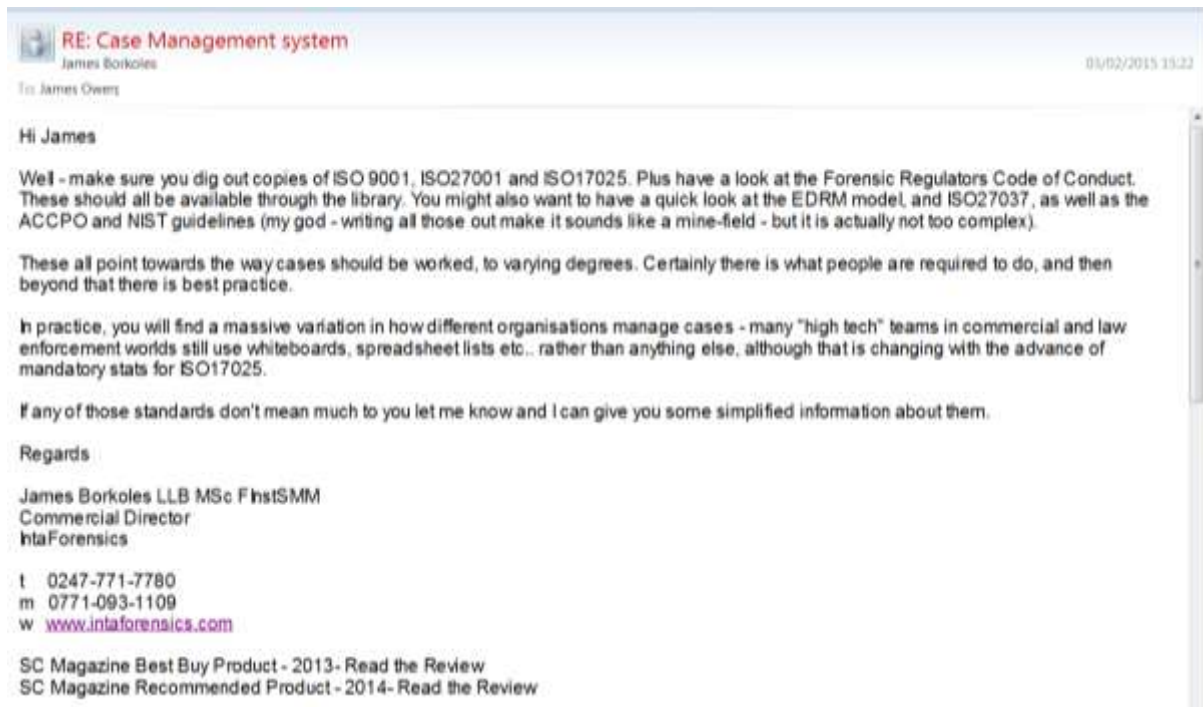
Activity	Does this activity exist?	How do/did you do it?
Notes	Yes/No	Please provide as much detail as possible
Determine which features are required to be implemented on Foreman Forensic Suite.  <b>Example – audit trails, case workflow management etc.</b>	Yes	Experience from my two previous forensics jobs meant I knew what a ‘prefect’ case management system would look like. Wrote down all the features required and then made a priority order of them to go through
Identify and removal of unnecessary features on Foreman Forensic Suite.	To an extent yes	As foreman is still in development I am still adding what I think are the necessary features; however if I get feedback saying otherwise I will reconsider the features

Determine any missing features not included on Foreman Forensic Suite.	Yes	When I presented the basic application to a conference there were many questions on additional features which were missing. These will all be considered for dismissal or implementation
Identify all potential competitors of Foreman Forensic Suite.	Yes	Currently I believe there to be no other forensics case management tool that is free and open source. I regularly check if there any. I do not have the budget to buy any commercial alternatives
Identify competitors interpretation of the most essential features required for Case management	No	As above, all alternatives are commercial and require money which I do not have a budget for
Identify features being used by competitors?	No	As above
Assess difficulty and ease of use of implemented features	Yes	I have gone through the tool with a number of students and people at a conference as well as Police Scotland. Their feedback has helped me make the features easier to use
Implement features and processes on Foreman Forensic Suite.	Yes	I update foreman as often as I can which tends to be at weekends
Ensure systems is simple and easy to use	Yes	Used simple design with no clutter on the web pages. Consistent design used throughout

Thank You for taking the time to complete the survey, your contribution and time is appreciated.

James Owen

## Appendix 10 Correspondence from IntaForensics



Hi James

Well - make sure you dig out copies of ISO 9001, ISO27001 and ISO17025. Plus have a look at the Forensic Regulators Code of Conduct. These should all be available through the library. You might also want to have a quick look at the EDRM model, and ISO27037, as well as the ACCPO and NIST guidelines (my god - writing all those out make it sounds like a mine-field - but it is actually not too complex).

These all point towards the way cases should be worked, to varying degrees. Certainly there is what people are required to do, and then beyond that there is best practice.

In practice, you will find a massive variation in how different organisations manage cases - many "high tech" teams in commercial and law enforcement worlds still use whiteboards, spreadsheet lists etc.. rather than anything else, although that is changing with the advance of mandatory stats for ISO17025.

If any of those standards don't mean much to you let me know and I can give you some simplified information about them.

Regards

James Borkoles LLB MSc FInstSMM  
Commercial Director  
IntaForensics

## Appendix 11

### FORZA – Digital forensics investigation framework

**Table 2 – A high-level view of the FORZA framework**

	Why (motivation)	What (data)	How (function)	Where (network)	Who (people)	When (time)
Case leader (contextual investigation layer)	Investigation objectives	Event nature	Requested initial investigation	Investigation geography	Initial participants	Investigation timeline
System owner (if any) (contextual layer)	Business objectives	Business and event nature	Business and system process model	Business geography	Organization and participants relationship	Business and incident timeline
Legal advisor (legal advisory layer)	Legal objectives	Legal background and preliminary issues	Legal procedures for further investigation	Legal geography	Legal entities and participants	Legal timeframe
Security/system architect/auditor (conceptual security layer)	System/Security control objectives	System information and security control model	Security mechanisms	Security domain and network infrastructure	Users and security entity model	Security timing and sequencing
Digital forensics specialists (technical preparation layer)	Forensics investigation strategy objectives	Forensics data model	Forensics strategy design	Forensics data geography	Forensics entity model	Hypothetical forensics event timeline
Forensics investigators/system administrator/operator (data acquisition layer)	Forensics acquisition objectives	On-site forensics data observation	Forensics acquisition/seizure procedures	Site network forensics data acquisition	Participants interviewing and hearing	Forensics acquisition timeline
Forensics investigators/forensics analysts (data analysis layer)	Forensics examination objectives	Event data reconstruction	Forensics analysis procedures	Network address extraction and analysis	Entity and evidence relationship analysis	Event timeline reconstruction
Legal prosecutor (legal presentation layer)	Legal presentation objectives	Legal presentation attributes	Legal presentation procedures	Legal jurisdiction location	Entities in litigation procedures	Timeline of the entire event for presentation

## **Appendix 12 Usability Evaluation Guide**

The following table contains Neilsons Usability Heuristics which will be used as a guideline to conduct an evaluation on the user interface.

### ***Appendix 12a Neilsons Heuristics***

Name of Heuristic	Description
Visibility of system status	The system should always keep users informed about what is going on, through appropriate feedback within reasonable time.
Match between system and the real world	The system should speak the users' language, with words, phrases and concepts familiar to the user, rather than system-oriented terms. Follow real-world conventions, making information appear in a natural and logical order.
User control and freedom	Users often choose system functions by mistake and will need a clearly marked "emergency exit" to leave the unwanted state without having to go through an extended dialogue. Support undo and redo.
Consistency and standards	Users should not have to wonder whether different words, situations, or actions mean the same thing. Follow platform conventions.
Error prevention	Even better than good error messages is a careful design which prevents a problem from occurring in the first place. Either eliminate error-prone conditions or check for them and present users with a confirmation option before they commit to the action.
Recognition rather than recall	Minimize the user's memory load by making objects, actions, and options visible. The user should not have to remember information from one part of the dialogue to another. Instructions for use of the system should be visible or easily retrievable whenever appropriate.
Flexibility and efficiency of use	Accelerators -- unseen by the novice user -- may often speed up the interaction for the expert user such that the system can cater to both inexperienced and experienced users. Allow users to tailor frequent actions.
Aesthetic and minimalist design	Dialogues should not contain information which is irrelevant or rarely needed. Every extra unit of information in a dialogue competes with the relevant units of information and diminishes their relative visibility.
Help users recognise, Diagnose, and recover from errors	Error messages should be expressed in plain language (no codes), precisely indicate the problem, and constructively suggest a solution
Help and documentation	Even though it is better if the system can be used without documentation, it may be necessary to provide help and documentation. Any such information should be easy to search, focused on the user's task, list concrete steps to be carried out, and not be too large.

Neilson(2005)

The following tables will also be used to calculate the severity and the amount of effort that would be required to repair the identified heuristic.

***Appendix 12b Severity of Heuristics***

Level of Severity	Description of severity
0	Violates a heuristic but is not a usability problem.
1	Superficial usability problem, not critical to system can be repaired before next release if time permits
2	Minor usability problem, low priority repair should be done before next release.
3	Major usability problem, high priority repair required
4	Disastrous

***Appendix 12c Repairing identified heuristic***

Effort Required to repair	Name of Heuristic
1	Problem is extremely easy to repair.
2	Problem is easy to repair.
3	Problem may require moderate effort to repair.
4	Problem requires significant amount of effort to repair.



## **Appendix 12d – Usability Evaluation Results**

	<b>Identified area</b>	<b>Problem</b>	<b>Violated Heuristic</b>	<b>Level of severity</b>	<b>Ease of correcting Heuristic</b>	<b>Proposed Solution</b>
1	Activities that requests information from the client.	There wasn't a clear indication of which fields were mandatory.	Error prevention	1	1	Use of an asterisk to identify which data fields are mandatory for progression to the next phase.
2	Uploading Photographs	If user changes mind, there is no exit or cancel button and user is forced to upload or exit screen and re-enter information on return	Visibility of system status	3	2	Insert a cancel button so user can cancel photograph upload.
3	There is no option for choosing the relevant time zone.	If user changes mind, there is no exit or cancel button and user is forced to upload or exit screen and re-enter information on return	Error Prevention	3	1	Implement data field to select time zone  Or  Implement automated time zone capturing.
4	User has to manually enter date and time when uploading evidence.	User can input fictional time by changing the time on the compute foreman is installed	Error Prevention	3	2	Implement necessary features to capture time and date automatically.

5	When viewing a specific case there are two options for close.	Two commands available for 1 action.	Error Prevention	3	1	Remove one of the buttons
6	Navigating through the different sections of the system	Issues relating to the location of the user. Feeling slightly lost when navigating further/deeper into different section	User control and freedom	2	3	Include a navigational tool which displays the current destination of the user.  Certain tasks such as adding evidence have already included a variation of this solution.
7	There is currently no help or guidance available throughout the system.	User may become unsure whether inputted information is relevant.	Help and documentation	3	3	Include a message that details the format and content of required information. To maintain minimalistic design the system could utilise mouse over messages which will appear once the mouse is scrolled over a particular title/link.
8	Accessing support or documentation whilst offline	Cant access the information without having an active internet connection	Help and documentation	4	2	Include the required information within the system. This will avoid the user having to refer to the online location for the required information.
9	There is currently no safeguard in place to ensure that work is not accidentally lost	Users can accidentally click back and lose all case notes	Error Prevention	3	2	Include an 'Are you sure?' Warning message for situations such as the back button being accidentally pressed.

## **Appendix 13 – Correspondence –Dr Alia Abdelmoty**

**RE: Question**  
Alia Abdelmoty (AbdelmotyA3@cardiff.ac.uk) [Add contact](#) 07/04/2015 11:11  
To: James Owen;

Hi James,

Essentially usability heuristics can be used in a "Heuristic Evaluation" usability test. This is an effective usability test that can be used several times in the development lifecycle and is complementary to a user test.

It should help you identify (and justify) major usability issues.  
You can focus the test on particular user tasks, do an overall review of the system interface or both.  
Essentially, you examine the system state when the user is executing a task and check for usability problems, identify the problem and describe it and justify it with a heuristic.  
To ensure you find most problems, you need to track and examine the user interaction carefully.

User tests are very valuable, but a heuristic evaluation may be sufficient in your case.

Regards,  
Alia

Hi James,





Essentially usability heuristics can be used in a "Heuristic Evaluation" usability test. This is an effective usability test that can be used several times in the development lifecycle and is complementary to a user test.

It should help you identify (and justify) major usability issues.  
You can focus the test on particular user tasks; do an overall review of the system interface or both.  
Essentially, you examine the system state when the user is executing a task and check for usability problems, identify the problem and describe it and justify it with a heuristic.  
To ensure you find most problems, you need to track and examine the user interaction carefully.

User tests are very valuable, but a heuristic evaluation may be sufficient in your case.

Regards,  
Alia

## Appendix 14 – Tabular Analysis

					Reccomendations
Name of System	<b>Foreman Forensic Suite</b>	<b>Case Notes</b>	<b>AD LAB</b>	<b>Lima Forensic Case Management</b>	
Website	<a href="https://bitbucket.org/lozmanio/foreman/">https://bitbucket.org/lozmanio/foreman/</a>	<a href="http://www.blackthorn.com/case-management/">http://www.blackthorn.com/case-management/</a>	<a href="http://accessdata.com/solutions/digital-forensics/ad-lab">http://accessdata.com/solutions/digital-forensics/ad-lab</a>	<a href="http://www.intaforensics.com/software/lima-product-suite/">http://www.intaforensics.com/software/lima-product-suite/</a>	Solution in recommendations
Operating systems	Linux, Windows and IOS. Supports most browsers	IPad, iPhone and windows pc	Microsoft Windows Server 2008 R	Windows XP,7,8 (32&64 bit systems) Supports any browser	Solution in recommendations
Database server					
Installation documentation	Provides 'wiki' with instructions for setting up system. Encountered issues regarding installation of python files which caused delays installing the system.	System can be installed by downloading app from relevant app store or website.	No installation guide online	Provides a step by step installation guide.	Solution in recommendations
Cost	Open source therefore £0	No costs	No costs	Dependant on version	Solution in recommendations
Free trial available	Free to download	Provides 14 day free trial	No	Free trial not available	Achieved ✓

ISO Compliance	Not yet. This project seeks to identify particular standards.	No information available for this system, however other Blackthorn systems are ISO compliant, (Mobile forensics)	No information available	ISO27001:2005 ISO 9001:2008 ISO 17025:2005 ISO 27037: ASCLD – Laboratory accreditation board	Discussed in further detail in ISO Analysis section
Training	No training available, develop will respond to email queries.	A system has been designed to minimise the need for training. Very simplistic design.  “intuitive product experience, reducing the need for onerous training sessions and ensuring stress-free user adoption”	Provide a knowledge base and discussion forum	Training course is available for new users. IntaForensics recommends users completing this course as system is considered to complex processes in certain parts.	Solution in recommendations
Support	Currently no support strategy in place, however Developer has provided an email address for any correspondence or queries.	Telephone number and email address.  Blog available on primary website however subjects do not cover training and support issues.	Access Data online portal  Email support  Telephone helpline	Monthly and quarterly updates  Requests feedback from users.  Promotes user recommendation for the addition of alternative features	Solution in recommendations

Available Versions/Mobile platforms	Foreman currently has one version which is run directly on single computer.	IPad, iPhone and windows pc	Windows	IntaForensics has 4 different versions that the user can choose from. 1. Lite 2. Standard 3. Portal 4. Enterprise 5. Each system offers different features for different organisations/level of involvement.	Solution in recommendations
Customisation	Addition, removal of types of evidence and cases.	Very simplistic design that does not possess options to customise the system.  Can integrate own form templates relevant to digital forensics.	Customisable interface	Allows users to customise the system in order to meet the needs of the organisation. The system can be modified in a manner to ensure that it adheres to the rules of digital forensics to ensure that it doesn't effect Customised reports can also be generated.	Achieved
Ability to export data	Bitbucket Website provides instructions for users to download case notes to RTF format or PDF.  Currently, no process in system to allow users to download case notes.	Capable of exporting cases in password protected ZIP archives Can also export to a range of additional systems Inc. Excel, PDF, RTF, TIFF, Information can also be printed	Data sent to centralised database so examiners can view/analyse.	Provide function to export data in XML format.	Achieved

Exhibit tracking	<p>Foreman has a feature that allows user to upload evidence. Uses a drop down menu with large range of evidence types including 'other'.</p> <p>Foreman also has feature that allows the user to generate a QR code for different evidence.</p> <p>Generates hash of note with date/time and name of author.</p>	<p>CaseNotes has a full audit trail; all entries are time stamped and geo-located where possible.</p> <p>Tamper proof notification system – red dots shows changes have been made to data</p> <p>System is tied to the iPod/iPhone specifications. When full, no further data can be added.</p> <p>Uses AES 512bit encryption for sensitive data</p> <p>Data is secured with hashing and encryption as it is uploaded to the system</p>	<p>Full logging of all electronic evidence</p> <p><u>Centralized</u> processing, indexing and data storage, with the ability to queue jobs into the distributed processing farm</p>	<p>The software allows full exhibit tracking and recording to maintain continuity of evidence for every case.</p> <p>Captures all forms of communication data and can be viewed as an audit log.</p> <p>Full log of use and activities of each case, important feature for forensics.</p>	Solution in recommendations
Search/query facility	<p>Foreman does not currently have a search option, instead it has an Evidence locker and is organised by date it was uploaded.</p>	<p>No search feature,</p>	<p>Sophisticated searching capabilities: Fuzzy, Stemming, Related Words, Phonic, Wildcard, Proximity and Concept</p>	<p>Provides the ability to search for relevant data. Large cases may develop a substantial amount of data; searches can be filtered to improve efficiency of retrieving evidence. Large cases can accrue a substantial amount of data; searches can be filtered to improve efficiency of retrieving evidence.</p>	Solution in recommendations

Contacts	N/A	N/A	N/A	Records all client information, ability to log all telephone calls, meeting notes.	Solution in recommendations
Sales modules	N/A	N/A	N/A	Includes an optional module that allows companies to manage sales processes. These processes include enquiries, quotations, invoicing and acquisition of client feedback	Solution in recommendations
Knowledge base.	Uses 'evidence locker' as central location retrieve evidence.	Uses a module called 'case' which stores all notes and uploaded data. This data is time stamped, includes name of person and if connected a geographical location for IPod.	Stores data in centralised location to stream line investigation activities.	Centralised repository for storing of data. Data can then be organised into different sections or categories	Achieved in different ways
Supports offline use	Does not require internet connection to use system.  Does not support multiple users connecting from different locations	Can be used off and online from any locations. (IPad/IPhone apps)	Requires connection to upload to centralised hubs	Supports offline activities particularly useful for those working 'on-site' or from multiple locations.	Solution in recommendations



Image and document attachments (evidence)	Foreman has a feature for uploading photographs; this feature was not operational at time of analysis.  No feature for videos or other file formats (documents.)	Can attach video, audio and documents.  Use own forms to write reports	Can upload evidence to centralised hub.	The ability to attach documents and images to securely.	Solution in recommendations
Allocation of tasks, distribute case work	Case managers can assign tasks to different user by using role based permission.	Manage teams and tasks.  Can allocate tasks to members of the teams.	Role based permissions to restrict who can access the content	Provides the function to complete these activities, also it uses a diary to record significant events. Users who have been assigned tasks receive an email to advise/remind them. Furthermore, tasks can be assigned by their security and permission level allowing cases to be prioritised.	Achieved
Time analysis	System displays times of activities (start/finish), however no tools provided for specific project time analysis.	Provides details on activities, however no analysis tool	Provides details on activities, however no analysis tool	System provides function that analyses time spent on cases	Solutions in recommendations

Resources management	Generic tasks can be inserted manually but no actual feature	Generic tasks can be inserted manually but no actual feature		Manages resources such as staff, hardware, software, suppliers and other locations.	Solutions in recommendations
Online portal	N/A	No portal, however app can be connected to internet	Simultaneous collaboration is enabled Through database backend.	Lima Forensics uses a secure online portal which enables communication with end clients throughout a case.	Discussed connecting to internet in recommendations
Firewall	N/A	No information available	No information available	Can be configured to be run through a secure firewall.	Not relevant if running on secured network
Portal Submissions Manager	N/A	Can upload data over a network.	Uses database backend for processing all submissions.	Enables authorised members to submit cases via the lima portal in order to request budgetary authorisation for a case submissions to be made.	Discussed connecting to internet in recommendations

## Sources

Access Data. 2015. *ADLAB* [Online]. Available at: <http://accessdata.com/solutions/digital-forensics/ad-lab/capabilities>

Blackthorn. No Date. *Blackthorn Case Notes*. [Online]. Available at: [http://assets-production.govstore.service.gov.uk/Giii%20Attachments/QCC%20Information%20Security/Bids/Archive2/CaseNotes\\_v1%200.pdf](http://assets-production.govstore.service.gov.uk/Giii%20Attachments/QCC%20Information%20Security/Bids/Archive2/CaseNotes_v1%200.pdf)

Foreman Forensic. 2007. *ReadMe* [Online]. Available at: <https://bitbucket.org/lowmanio/foreman/>

IntaForensics2 2015. Lima Enterprise [Online]. Available at: [www.intaforensics.com/index.php/download\\_file/view/223/214/](http://www.intaforensics.com/index.php/download_file/view/223/214/)

IntaForensic.2015 *Lima Product* [Online]. Available at: <http://www.intaforensics.com/software/lima-product-suite/standard/>

SC Magazine. 2013. [Online]. Available at: <http://www.scmagazine.com/intaforensics-lima-forensic-case-management-software/review/3874/>

**Appendix 15**  
**Email from SARAH Holmes (Developer)**

**Re: Foreman analysis**

Sarah Holmes (sarah\_fonduelover@yahoo.com) [Add contact](#)

26/04/2015 2

To: James Owen;



Findings for  
FF - Sarah  
Comment...

Hi James,

You've done a really great job and come up with some excellent suggestions. Many of which are on my to-do list, and some are new ideas which I will add onto the list! I have tried to add a comment for each recommendation I've found. Let me know if they don't make sense or you need any further clarification.

Thanks,  
Sarah

## **Appendix 16**

### **Developers Comments for Recommendations**

*\*Note\* - Wording may differ slightly to the original section in report as additional proof reading was conducted on all report prior to submission.*

### **Findings**

The primary purpose of this section is to provide the reader with an overview of one's findings and present them as recommendations for FF implement in the future; furthermore this section also aims to fulfil the requirements of the final stages of the SSM process.

FF is still in its early stages of development, therefore many of these recommendations may have already been considered by the developer but not yet been implemented.

#### ***Neilsons Heuristics evaluation***

As previously discussed, the developer of FF has a wealth of experience in Digital Forensics and is an experienced practitioner. The developer has also acquired feedback from multiple personnel in the digital forensic community and has utilised feedback from live demonstrations in conferences. Furthermore, the developer has also stated that she is also aware of Neilson's usability heuristics, therefore one did not expect to identify a substantial amount of violated heuristics. However by completing this evaluation, it ensured that the design of the user interface was examined by someone who may possess a different perspective to the developer of the system.

#### ***Recommendations***

The following recommendations have been determined by referring to Neilson's usability Heuristics (1995) and analysing the system's user interface. Furthermore, one did appreciate that the system is not fully functional and is still in its early stages of development.

1. The inclusion of an asterisk on all mandatory data fields would provide the user with the knowledge of what information is required to progress to the next stage. Alternatively, if all fields are mandatory then it would also be advisable to inform the user of this requirement.

Yes, perfectly reasonable

2. Whilst uploading images for the evidence, if the users wish to cancel the upload after selecting an image, the user will have to press the back button to cancel that process which will also cancel any recorded information. Alternatively, the user will have to choose a different file to load instead of the initially file. It is recommended that a 'cancel' process is included to provide the user with the opportunity to cancel the current task without exiting that section.

Yes, I would like to add more JavaScript which is more interactive with the user.

3. In the event that this system becomes available to users residing in different time zones particularly Europe, there is currently no feature that would allow the user to state their current time zone. Therefore, it is recommended that the system includes additional information to account for such time zones or implement a feature that automatically determines the time zone by pairing the location with its IP address otherwise known as Geolocation.

Good point, I can add timezone option in the overall options

4. There are currently security concerns regarding the addition of evidence. The system identifies the time and date when a user uploads evidence, however one was able to manipulate this time by adjusting ones laptop to a fictional time. This may contravene or degrade the reliability of the audit trail.

Hadn't thought of that; I will include timestamps in hashes

5. On inspection of a case there is currently two options available that allows the user to 'close' that case. It is recommended that this be reduced to one.

Can you give me further details; not sure I understand this one. You can close and also archive a case, which are different?

6. When the user visits the different sections on the system due to the number of shortcuts and quick links, the user could potentially lose track of their location within the system. This recommendation suggests that each screen provide a navigational feature to inform user of their current location. However, this has currently been achieved in some of the areas particularly in the addition of evidence as there is a notification stating that the user is at 'section 1 of 2'.

Yes, I can add breadcrumbs

7. The user is only advised of their actions when they fail to comply with any necessary requirements e.g. missing data from required fields. However, one has chosen a recommendation for this system to provide additional assistance without affecting its minimalistic design. This recommendation is to implement a feature that displays brief snippets of information when a mouse is rolled over a particular area/text. This ensures that the design isn't affected whilst also providing the user with valuable information.

*As mentioned above I haven't added any javascript interaction. I plan to add something like hover-over help*

8. In the event that a user requires assistance or referral to documentation, the link currently listed on FF directs the user to the Bitbucket website. If the user did not have access to the internet they would not be able to retrieve the required information they desire. Therefore, it is recommended that the documentation/support be made available without having to connect to the internet.

*Yes, I've not made a user guide yet but it's on the list to do.*

9. The system has implemented warning and success screens; however these are not fully consistent throughout the whole system. This may result in users losing substantial amount of evidence if they accidentally click the backspace button on keyboard. Consequently one recommends that a warning sign be included on all key areas where the user has to input any case notes or other forms of information.

*Yes certainly can do that*

### **Tabular Analysis**

Due to one being unable to acquire copies of each Case management system, one referred to the online brochures and documentation that each company provided. This analysis has revealed that there were many similarities amongst all of the systems, however one has identified the following recommendations and suggestions for future implementation that one believes will improve the current system.

### ***Recommendations***

The following recommendations have been formulated by researching and comparing FF and other leading digital forensic case management systems in order to identify the main features by performing tabular analysis on each system.

1. All three of the leading systems have a dedicated website that provides users with information. Although, the system is linked with a blog and Bitbucket, one would recommend considering developing a website specifically for FF system. This is due to the belief that a website may attract additional support from others programmers which will effectively reduce the development time and share the workload for this project.

As with comment regarding the link to bitbucket above, I have no user documentation yet. Foreman has a website that I can easily add a user guide section to once I've written it

2. This analysis has identified that each system is capable of being run on a Windows system; some can run on Linux and others such as Blackthorn has a mobile application that can be run on iPad's and iPhones. Mobile devices can be used in any location and would be highly valuable and convenient if the investigator was able to log their work by using such devices. Although this recommendation is not considered to be critical for the success of the current system it may be worth considering for future implementation.

Because Foreman is written in Python with standard libraries..in theory it should run on all systems – Mac and Linux. I hope eventually to create an android app for logging evidence and creating notes on the go

3. The current installation for this system requires the installation of Python files. Although the installation of FF was undemanding, one did experience difficulties with the initial setup of Python tools. In comparison the other systems appeared to be more user friendly as they were executed in a windows environment, furthermore they provided videos and detailed installation guides. This issue could potentially be improved by;
  - c. Providing additional resources such as videos with demonstrations to reduce installation technical problems.
  - d. As the system is open source and users won't be charged to acquire a copy, FF could generate revenue by charging for the installation and initial setup for their future clients

Ultimately these are just suggestions; however the current process of setting up the system in Python requires more technical knowledge than the rival systems.

I may be able to create a windows installer package but not made one before;  
so no idea how easy that is!

4. Throughout this project one did not consider FF to be a system that required enhanced in-depth training. However, each person has different levels of skills and abilities, consequently one would recommend providing some means of training particularly as the leading companies have developed online videos and detailed how to guides. Furthermore, IntaForensics has developed a course that users can attend in order to use the system to its full potential. This may also be an opportunity how FF can generate additional revenue to support further development.

Yeah that would a great idea once it's a finished product – couple of youTube videos on how to do things. I don't think this is appropriate just yet until it's more complete.

5. The leading systems have ensured that they have considered the support requirements in depth by providing several different means to provide user assistance. Currently the developer of FF has stated that this project receives minimum attention during the working week as she has employment commitments. As the system is currently not fully operational this does not cause any significant concern at present. However, once the system becomes operational FF must ensure that a support strategy is developed to ensure that their potential customers can receive support within a satisfactory timescale.

The main point of Foreman is that it is open source, therefore if someone really wanted a feature – they could add it themselves. If they thought others would want it too then I would be happy to review their code and add it to the master copy. I don't (at the moment!) foresee myself working on foreman full time or even generating any money out of it, so unfortunately getting support for customers will have to be best effort. This hopefully is clear to those who download foreman. I have had several emails about foreman already and have managed to respond to them all.

6. Each system has the option of exporting the data from the system into pdf, rtf, Tiff, and many other file formats. This appears to be a key feature as each system has included the tools to complete this task. FF does provide this service but it would need



to install additional packages. This recommendation suggests additional resources for those who are unsure of installing third party packages.

The process is the same as the initial foreman installation, so this should be easy for users; however perhaps it is not obvious. I can update the wiki to give better clarity.

7. The logging of evidence to maintain the chain of custody is also one of the key requirements for a digital forensic case management system. FF has utilised QR codes for the logging of evidence, this feature is unique to FF as no other system currently utilises this technology. Although, hashing of evidence is included, one would consider implementing an onscreen notification to inform the user if any tampering or modification of evidence has occurred. This can be completed similarly to Blackthorns system by displaying a red dot if data has been changed or modified in any way.

Yes, definitely on the to do list and I plan on adding more hashing to further areas

8. The current setup for FF's evidence locker is that it stores evidence by date/time. This may suffice for smaller amounts of evidence; however large investigations over a long period of time may result in a substantial amount of evidence and result in the user having to scroll through a large list. The inclusion of a search feature is popular amongst the rival systems; therefore one believes that this feature would be a valuable inclusion to the FF system.

Search is definitely a feature I will be adding later. It's actually quite a hard feature to add, so want to get the content added first before I do this.

9. Intaforensic's considers itself to be an end to end system that covers all aspects of Case management. There are currently two features that have been incorporated into this system which no other system has implemented; these are features that record sales and client data. Therefore, if FF wishes to be considered as an end to end system such as Intaforensic's Lima, it may need to consider additional features that are outside the scope of digital forensic operations such as these or similar management features.

Certainly something I could consider as bolt-ons or extra things to add

10. The current system does not utilise networking technologies, therefore this prohibits the sharing of information to different members involved in the investigation. Therefore, the system should consider implementing a network infrastructure whilst ensuring that information security principles are considered in great depth considering the sensitivity of some cases/evidence.

Not sure this is correct or I fully understand. Foreman on a PC or laptop runs locally, but it has the full capability of running on an internal network or website (see <http://university.foreman-forensics.org/> - a working example of foreman online which multiple users can user at the same time)

11. The photograph uploader is currently not in operation, however one would recommend a feature that would allow other media file formats to support audio recordings and videos. Although the system is capable of uploading such files in other areas, having these options in the same location as the photograph uploader would improve the design and continuity of the system.

I had not thought of audio and video, certainly something to add in

12. Intaforensic's system has also included an additional feature that monitors and 'analyses' the amount of time that is spent on different aspects of a case, this would allow the organisation to generate an enhanced understanding of the areas that may require additional support. Although, this data can be retrieved manually and may not be considered a primary concern at present, this feature could improve the efficiency of a case and reduce user's expenditures. Furthermore, the inclusion of a system that could potentially save the organisation money is a highly sought feature and highly marketable.

Something that would not be too hard to do and may be valuable to those who are paid by the hour per investigation.

13. A potential future recommendation for FF would to be to consider developing or amalgamating FF with an Open source FTK platform. Blackthorn has successfully implemented this, and as a result offers a full comprehensive digital forensic package that forensic investigators can use to conduct and manage their investigations.

On my to do list eventually. I'd like to provide an API for the other way round too; i.e. people can plug into foreman from whatever system they use.

### **Research of relevant ISO Standards**

In order to identify the relevant standards that may be applicable to digital forensic case management one required in-depth knowledge of the activities that took place throughout the lifecycle of an investigation. Therefore, once one had gained this knowledge of the investigation frameworks particularly FORZA (Leong 2006) and the ACPO guidelines (ref), one was then capable of identifying the relevant standards that would be applicable. Furthermore, one was able to identify some of the relevant ISO standards by referring to the results generated in the tabular analysis, these results highlighted the relevant standards that the competitor systems were utilising.

Although one did not receive many responses from ones initial attempts of communicating with many case management companies, one did receive some guidance from a director at Intaforensic regarding which standards that one should consider when carrying out this analysis (Appendix 10).

The next step was the acquisition of the relevant ISO standards, one discovered that these standards are not free and purchasing several of these documents would be expensive. Fortunately one was able to acquire copies through the University as they had copies in the library and allowed access to these standards whilst logged on to a university system.

On successfully acquiring copies of these ISO standards, it was identified would not be feasible within the time scales of this project to individually analyse each clause and statement within each of the standards. However, one still had aspirations of achieving the objective of identifying relevant standards for the developer of the system. Consequently, with the acceptance and guidance from ones supervisor, it was decided that this analysis would only consider the chosen standards at a high level and only include the salient points of each standard.

In addition, currently there are approximately 19500 different ISO standards available for various aspects of business and technology. Although many of these standards may be unsuitable or irrelevant, it was determined that one would review the recommended standards and only discuss the three most significant. This was due to one's belief that the chosen standards would be sufficient in capturing all of the main aspects and processes that an effective digital forensic case management system must possess.

An ISO standard is a written document that provides a range of information on the requirements, guidelines or characteristics that are necessary to ensure the materials, products or services are sufficiently met to achieve its purpose (ISO No Date). These documents can

be accessed and purchased online by visiting the International standards website. (ISO No date).

### ***ISO 9001 – Quality management systems***

The ISO 9001 Standard is currently under review; however it belongs to the group of standards whose purpose is to consider issues relating the management of quality. The standard aims to provide guidance and the necessary tools for companies and organisations to ensure that their products or services are satisfying their customers' needs. Furthermore this standard ensures that they engage in ongoing improvement to maintain levels of quality in their products or services, this is then measured on an ongoing basis by conducting audits and inspections.

The standard is built on eight quality management principles that it must consider in order for it to achieve the objectives of the standard. These principles consist of the following

9. Customer focus
10. Leadership
11. Involvement of people
12. Process approach
13. System approach to management
14. Continual improvement
15. Factual approach to decision making
16. Mutually beneficial supplier relationships

The standard has been created to be applicable across multiple organisations and is not specific to industry or organisation size. This is achieved by describing a quality management system, this system provides the requirements for that organisation to engage and complete certain documented procedures. In addition these procedures must adhere to specific requirements that are included in each of these clauses

- Clause 4.2.3 Control of documents
- Clause 4.2.4 Control of records
- Clause 8.2.2 Internal audit
- Clause 8.3 Control of nonconforming product
- Clause 8.5.2 Corrective action
- Clause 8.5.3 Preventative action

In addition, this standard states the requirement for the organisation to produce a quality policy and manual prior to considering becoming accredited.

According to the ISO standard website, the main objective of this standard is to ensure that the system is functioning in the correct manner. Therefore, it is ones belief, that even if the developer does not wish to proceed and gain accreditation for this standard, the identification

of any factors that violate the quality of the system still needs to be identified and resolved. Therefore, if the developer chooses not to proceed with accreditation, it is recommended that a strategy is still implemented to acquire feedback relating to the functionality and quality of the system. This can be achieved by requesting feedback from users of the system or by engaging in an analysis similar to ones heuristic evaluation completed previously

### ***ISO17025 - General requirements for the competence of testing and calibration laboratories***

This standard was developed for any organisation that is required to perform testing or sampling during its daily activities.. This standard does not state a minimum and maximum number of personnel that are required to be engaging in laboratory activities and does not state to what extent such activities must achieve. Therefore, the primary purpose of this standard is to assist laboratories in the managing and maintaining quality, administrative and technical operations.

The following describes the prominent clauses stated in the ISO 17025 that are specific to the different activities and processes that occur during a digital forensic investigation.

#### **Technical records (ISO 17025:2005, 4.13.2)**

This clause states the requirement of ensuring that a record of all seized evidence is completed, this may consist of the recording of all items that have been seized according to their bag number. Additionally an audit trail must always be completed to monitor the activities that take place throughout the lifespan of the investigation.

#### **Selection of methods (ISO 17025:2005, 5.4.22)**

This clause ensures that the best methods are used to conduct the investigation by considering the needs of the customer and the investigation itself. In the event that the customer does not state a desired method, then the investigator must make the decision based on the knowledge he/she possesses. This may involve decisions on what items are required to be seized based on that specific type of case they are investigating.

#### **Handling of test items (ISO 17025:2005, 5.8)**

This clause ensures that the integrity of the evidence is not violated; it details those procedures that must be followed to ensure that the evidence does not get compromised during the different stages of the investigation. Furthermore this clause also specifies the

requirements of how the evidence is to be transported, packaged and sealed. The clause further describes the requirements for the protection of evidence whilst transporting from unauthorised personnel and environmental factors such as shock and heat damage.

To summarise, one believes that FF must ensure that it can support those who are conducting the investigations as much as reasonably practicable. Furthermore, one believes that each of these activities should be completed if a system is to be considered a case management system specifically for digital forensics. However despite reports in ones feedback that this standard may become mandatory in the near future, one believes that a digital forensic case management system should be proficient in supporting laboratories by supporting these activities regardless. Therefore, it is recommended that once the system has been completed, that the developer considers the requirements previously discussed in finer detail and make the required modifications to the system should they be required.

### ***ISO/IEC 27001 - Information security management***

One determined this standard to be particularly important and relevant to case management systems. The primary objective of this standard is to assist organisations with the management of sensitive information. This aspect is particularly relevant for FF as it is likely that this system will be used to store sensitive images or documents. This standard utilises an information security management system (ISMS) in order to ensure that a system remains up to date with ever changing external threats. This standard is not industry, size or technology specific; therefore it covers a substantial amount of information to ensure it is relevant on a wider scale.

Certification for this standard can be acquired but it is also not mandatory, although becoming certified could demonstrate that a company uses best practices to ensure the safety of its data/information. Furthermore if a system has not considered the requirements included in this standard, it is likely that their information system is not appropriately protected. Conversely just becoming accredited to this ISO standard doesn't guarantee the safety of the system either, once accredited the organisation is responsible for maintaining and ensuring the system is kept up to date and protected against emerging threats.

On initial analysis of the system it is believed that the system does not possess networking facilities; as a result one would recommend the developer of FF to consider this standard in greater depth prior to enabling any networking features.

### ***Overview of iso standards***

To summarise ones findings of this analysis, one had determined that although the standards represent the best practice methods, FF should endeavour to implement and support these requirements regardless. One also believes that FF may experience difficulties in justifying the costs of accreditation due to it being open source software and still being in its early stages of development. Therefore, one would recommend that FF utilise specific aspects from each ISO standard that one has previously discussed and concentrate on building the system prior to acquiring accreditation for any of these standards. This will ensure that FF captures some of the criteria for these standards, and the remaining can be included at a later stage if accreditation becomes mandatory or if the developer chooses.

Yes sounds sensible to me

## **Comparison of foreman forensic and the forza framework**

The following section will provide ones recommendations from analysing the current system alongside the FORZA Framework designed by Leong (2006). The recommendations will be structured in order of their roles previously discussed in the Implementation section.

### ***Case Leader***

According to Leong (2006) the case leader is considered to be the person who plans and orchestrates the entire digital investigation process. This person will responsible for making the decisions on whether the case has scope for further progression or whether it should be discontinued.

On examining the case leader/manager section would recommends that the developer implements a feature that records the key personnel that have an involvement in the case. This could include the suspects, witnesses, system owner, victim and the reporting person. The possession of this information could save significant amount of time when other members of the team require knowledge on the involved parties. Furthermore, this information can be used to identify any relationships between the personnel involved in the case e.g. did the owner report the case or was it someone else.

The framework recommends that the case manager should acquire specific timings related to the case. These timings should include the time that the incident occurred, the time it was reported, the start time and time that the activity finished (if relevant). Although this can be inserted manually into the 'case background' section, one believes that as this is important information and it should have its own section in order to retrieve the information more efficiently.

There is no currently no feature on FF that requests geographical positions/locations where the crime/incidents took place. The inclusion of this information could be beneficial to identify whether there are any particular patterns emerging particularly if there are a large number of incidents/crimes involved in a single case located in a specific area of a company.

I can certainly add this in as fields for the case manager to fill out



### ***System or business owner***

Leong (2006) considers the system or business owner to be the victim or sponsor of the case, alternatively depending on the type of case, this person can also be considered as the main suspect of the investigation.

Therefore this phase of the investigation would require the case leader to develop his or hers understanding of the situation that they are required to investigate. This can be completed by carrying out initial interviews with the system/business owner or their representative (Leong 2006).

One could not determine any missing or potential features that FF could include to improve this phase of the framework. This is due to the belief that the case manager does not need to follow a rigid framework in order to develop a basic understanding.

### ***Legal Advisor***

Leong (2006) states that once the background of the case has been determined, the next step in the FORZA investigation framework would be for the case leader/case manager to determine the legal requirements of that particular investigation/incident.

A legal advisor is considered to be the initial advisor who provides the case manager with legal assistance in order to determine the course of the case/investigation (Leong 2006). Therefore, on examining the proposed activities that this phase of the framework entails, one has generated the following recommendations:

Foreman Forensic already possesses an option that allows the systems administrator to create user profiles and assign role based permissions. However, one would recommend implementing a 'signing off' feature that would enable law practitioners to approve or decline different aspects relevant to the case/investigation i.e. evidence/next steps.

**Sounds interesting, can you give me some details such as an example?**

Currently, the role titles 'authoriser' is primarily used to respond to 'requesters' at the very initial stages of an investigation. This modification would assist and improve the efficiency and quality of evidence retrieval as it will improve the communication between the IT and legal divisions of an investigation/case. Furthermore, this could also reduce the time that is spent processing ineffective evidence or leads as any evidence that possess no legal value can be disregarded earlier in the investigation.

According to Leong (2006), in order for the legal advisor to provide a recommendation whether to proceed, he/she will need to consider a substantial amount of legal constraints about the case/ investigation. The required information is as follows;

- Identify the objectives of the investigations i.e. have a crime been committed?
- Identify the legal background and preliminary issues that have arisen i.e. what information should be collected, determine information regarding the relevant law
- Identification of what procedures the investigation must follow i.e. require warrants, injections
- Identify participants of the investigation.
- Identify the maximum and minimum timeframe of the investigation

(Leong 2006)

Once this information has been acquired, the case manager would be able to determine the next steps in order to satisfy the legal aspects of the case.

Therefore, one believes that FF should create a feature that could record or install a process that ensures that all of the above factors are considered in order to ensure all required information regarding the legal aspects of the case is secured earlier in the investigation. This information should then be accessible on the system so that the case manager can ensure that the correct procedures can be deployed. Although this feature is not an essential requirement, one believes that this would evolve the current system as it would be incorporating the legal aspects into the system. Furthermore, this addition would also assist FF becoming a more comprehensive 'end-to-end' case management system.

Interestingly at both companies I have worked for it has been the case manager who decides whether the case is 'legal' or not and the authoriser who verifies this. I can think about how I would add in the feature mentioned here, without over complicating it for teams who wouldn't use it.

### ***Security/system Architect/Auditor***

The next step in the FORZA investigation framework is to examine and explore the involved system in greater detail. This process would seek to identify information regarding the design of the system that is being investigated. This could be considered as the stage in the framework that is responsible for acquiring specific technical information from the victims or from the technical staff employed by the business/system owner.

Whilst considering the number of potential offences and the substantial amount of relevant information that would need to be captured, it is likely that the case manager may not capture each fact regarding the case. Therefore, in order to assist with the retrieval of information, the system could propose an automated list of questions which can be accessed by the

investigator. The results can then be uploaded to the system and accessed by all personnel involved in the case/investigation.

I can certainly add the ability for foreman to display information on certain pages that have been uploaded by the administrator.

### ***Technical Presentation Level and Data acquisition layer***

Once the relevant information is captured from the previous phase, the next two steps are related to the planning and execution of the procedures required carrying out the case/investigation.

The FF system currently allows the case manager to assign principle and secondary forensic investigators for specific tasks. In addition the investigator is able to upload notes that will be hashed on submission and relevant files in support of the investigation/case.

Although the current system is able to log the required events/evidence, it may not be as suitable as rival competitor's mobile applications. Therefore in order to improve the functionality of the system whilst in the field, one recommends implementing a system that can be used on mobile devices similar to Blackthorns Case Notes mobile app. Furthermore, this is not an essential requirement as the system can be used effectively on a laptop.

Finally, this recommendation may not be feasible for implementation at present. However, one believes if this feature is desired for future implementation, the developers of the system can begin considering some of the background functions that may be required to host a mobile application.

Yes exactly. It's a lovely idea but firstly I've never developed for Android or iOS and requires a huge learning curve before I can even begin this.

### ***Data analysis layer***

This stage of the framework requires the evidence that has been transported to the lab to be further analysed and reviewed to determine its relevance and importance to the case. The current system has successfully provided the means to document and record such evidence. One of the key features of this phase in the FORZA framework (2006) is the ability for the investigators to identify the chain of custody and timeline of the proposed incident. During examination of FF system, one noticed that there is not option to include the date or time for the addition of evidence. One believes that if the system was able to generate graphical

timelines for the addition of evidence in the reports section of the system, this feature would assist all those involved in the investigation as it would organise the events in a manner than can be understood easily.

Nice idea. I intend to get foreman to auto-generate whole case timelines, so show when all notes where done, QA completed, evidence added etc.

### ***Legal presentation layer***

The final phase of the FORZA framework is to reevaluate the full details of the incident/event from a legal perspective and determine whether there is a requirement for further evidence or investigation. The current system has a feature which supports this requirement as it provides a Quality assurance feature. The purpose of this feature is to determine whether the case has achieved the required objectives. Alternatively if the quality assurance is not passed this investigation will return to the previous stage and the process will be repeated until a pass is achieved. As discussed previously user profiles can be created in the administrator section of this system, therefore it is feasible that user profiles for legal teams to be manually created and achieve the requirements of this phase.