A picture containing clock

Description automatically generatedSchool of Information Technology

Department of Computer Science

**Thesis Title (TBD)**

**R. Domingues st.no. 9339876**

Table of Contents

[Introduction 3](#_Toc68032887)

[1.1 Introduction 3](#_Toc68032888)

[1.1.1 Criminal Investigations 3](#_Toc68032889)

[1.1.2 Digital Forensic Investigations 4](#_Toc68032890)

[1.1.3 Email as Digital Evidence 5](#_Toc68032891)

[1.1.4 Problem Statement 5](#_Toc68032892)

[1.2 Motivation 5](#_Toc68032893)

[1.3 Objectives/methodology 5](#_Toc68032894)

[1.4 Layout 5](#_Toc68032895)

[1.5 Conclusion 5](#_Toc68032896)

[Chapter 2: 6](#_Toc68032897)

# Introduction

(5 – 6 pages)

The typical modern business contains a lot of information in a semi-structured electronic format due to increasing reliance on electronic means for planning, transacting and communicating. Documents pertaining to many aspects of the daily business are prepared electronically and stored on network or local storage. Almost all financial transactions are through electronic funds transfers, and as a consequence all book keeping is in electronic form. Communication in written form includes documents like contracts[[1]](#footnote-1), email and short text communication on services like Whatsapp. Business discussions take place by means of telephonic conversations, meetings which are sometimes recorded electronically, and minutes of meetings often distributed in electronic format. As a consequence it can be expected that any fraudulent activity leaves traces in semi-structured electronic records.

This chapter explores the challenges in investigating potential fraud in a business where large volumes of semi-structured data may contain evidence. The basic principles followed in criminal investigations are explored. Digital forensic investigations principles are described which is often in support of the criminal investigation. The focus is narrowed to only one of the potential source of evidence namely emails. This is sufficient to formulate a problem statement for the research presented in the rest of this thesis. The work is motivated and the methodology to address the problem statement is described.

## Criminal Investigations

Criminal investigations involve the reconstruction of the most likely event that led to a crime. The reconstruction of the sequence of events rely on data available to the investigator like witness statements, financial transactions, camera footage, correspondence and forensic data [1]. The investigator keeps a case file with all the potential sources of evidence in it.

A case file is similar to a database. The investigator classifies information relevant to the reported crime in the form of witness statements, forensic evidence, intelligence and interviews. This provides structure to the evidence or data which the investigator use to develop lines of enquiry.

Ultimately the investigator wants to answer the following three basic questions during an investigation [1]:

• What crime was committed?

• Who are the suspects?

• What evidence exist to support a line of enquiry?

As much as possible evidence material is collected that might be applicable to the investigation [3]. This allows for the formulation of many lines of enquiries. The multiple lines of enquiry assists the investigator to gather more evidence, classify and order the evidence in the case file. New evidence may become available which opens more lines of enquiry. The investigator will have to revisit evidence previously examined with new lines of enquiry in mind [3]. Some lines of enquiry are eliminated which lead to an attrition of relevant material for prosecution [3].

All material gathered has to be preserved even if it is not used in the prosecution. Legislation in some countries require the police service to record all relevant evidence material gathered, retain the material and reveal all material relevant to a prosecution to the defence even if such material is not used in the prosecution [3]. Evidence presented in court needs to stand up to scrutiny of all alternative hypothesis so that there is no reasonable doubt the presented evidence points to the accused [3].

## Digital Forensic Investigations

Digital forensics has its roots in the observation that digital devices such as computers are utilized in committing crimes [2], and often the crime only takes place in the virtual or cyber world. Examples of such crimes are child pornography, theft of personal data, ransomware encrypting a person’s data which will only be released for a fee, etc.

A major source of forensic evidence in the context of business fraud is digital forensic evidence [2]. Digital forensics is a highly specialized field which often requires technical knowledge of the inner workings of digital devices, communication protocols and networks to find and extract evidence leading to catching the perpetrator [2]. A digital forensic investigator is therefore a specialist investigator supporting general investigators in investigating crimes, similar to e.g. a forensic pathologist or a forensic financial investigator [2]. Some of specialist aspects the digital forensic investigator is well equipped to deal with are [2]:

• Reconstructing network communication events through log analysis to determine how a hacker gained access to a computer system.

• Identifying and analysing deleted files with the purpose of reconstructing such files as evidence.

• Analysing malware to determine the purpose of the malware, how it was installed and what possible crime was committed by executing the malware.

• Extracting information from files, metadata, communications like email to assist the investigator in finding evidence for lines of enquiry.

A special relationship exists between an investigator and a forensic investigator. Each has its own focus and is complimentary. The forensic investigator must be able to present evidence to the investigator and the court in an understandable manner. The investigator needs to understand all relevant detail presented to him or her with-out becoming a forensic investigator. Investigators should not hesitate to question what the forensic investigator presents to him/her [3].

Increasingly crime is committed through digital channels and it often results in large volumes of data that needs to be analysed. The Enron case is one such case where prosecution was successful due to evidence uncovered in over 200 000 emails that was seized on company servers [2]. Emails contain both metadata in the form of email headers and routing information, attachments in the form of photographs, in-voices and other documents, and natural language information in the form of the email itself. The processing of such a large number of emails requires skills from both the investigator as well as the digital forensic investigator.

## Email as Digital Evidence

## Problem Statement

## Motivation

## Objectives/methodology

## Layout

## Conclusion

# 

Appendix A: Bibliography

[1] S. Tong, R. P. Bryant, and M. A. H. Horvath, Eds., *Understanding Criminal Investigation*. Oxford, UK: Wiley-Blackwell, 2010.

[2] X. Lin, *Introductory Computer Forensics: A Hands-on Practical Approach*. Cham: Springer International Publishing, 2018.

[3] National Centre for Policing Excellence (NCPE) United Kingdom, *Practice advice on core investigative doctrine 2005*. 2005.

1. A contract can be viewed as the communication of agreement between two parties. [↑](#footnote-ref-1)