COMPUTER CRIME INVESTIGATION PROCESS IN SRI LANKA: COMPARATIVE ANALYSIS WITH UK AND EU LAWS

D.Siyumi Sandarenu Dayananda

209104X

Degree of Master of Business Administration in Information Technology

Department of Computer Science and Engineering

Faculty of Engineering

University of Moratuwa

Sri Lanka

July 2022

COMPUTER CRIME INVESTIGATION PROCESS IN SRI LANKA: COMPARATIVE ANALYSIS WITH UK AND EU LAWS

D.Siyumi Sandarenu Dayananda

209104X

Thesis submitted in partial fulfillment of the requirements for the

Degree of Master of Business Administration in Information Technology

Department of Computer Science and Engineering

Faculty of Engineering

University of Moratuwa

Sri Lanka

July 2022

DECLARATION

I declare that this is my own work and this thesis does not incorporate without acknowledgement any material previously submitted for a degree or diploma in any other university of institute of higher learning and to the best of my knowledge and belief it does not contain any material previously published or written by another person except where the acknowledgement is made in the text.

Also, I hereby grant to the University of Moratuwa the non-exclusive right to reproduce and distribute my thesis, in whole or in part in print, electronic or other medium. I retain the right to use this content in whole or part in future works (such as articles or books).

UOM Verified Signature .. 2022.07.15 .....

D.S.S.Dayananda Date:

Signature of the Candidate

The above candidate has carried out research for the Master's thesis under my supervision.

..... UOM Verified Signature 17th July 2022 .....

Dr. Thusitha B. Abeysekara Date:

Senior Lecturer in Law,

Head-Legal Studies Unit,

Faculty of Management Studies and Commerce,

University of Sri Jayawardenepura

COPYRIGHT STATEMENT

ABSTRACT

The rapid advancements in the field of Information Technology have rendered several positive impacts for carrying out normal daily tasks easily and successfully. As a result of that, the usage of computer related systems have grown fast by attracting more people. Despite all the advantages that can be gained through such computer systems, negative impacts have also started to emerge in the form of "Computer Crimes". Since these crimes are making challenges in various ways it is utmost important to prevent and control them. The Computer Crime Investigation is the procedural and systematic way that is used to conduct legal investigations on computer crimes in preventing and controlling such crimes through revealing the real criminals behind any offence. Thus it is crucial of having a strong legal framework that consists of validated laws which render a proper investigation process for any computer related crime. This study focused on addressing the sufficiency level of existing laws related to Computer Crime Investigation in Sri Lanka in combatting the computer related crimes through strengthening out the process of computer forensic which used to present legally admissible evidence to the court. For identifying any loophole the research was conducted as a comparative analysis with UK and EU laws in the same context. The qualitative research approach has been adopted as a combination of interviews and library based research to gather data. Key findings were extracted based on the analysis. Thus, the research reached out to the implication that the existing laws in Computer Crime Act are not sufficient to conduct proper investigations. According to the data gathered via interviews and library research, this study has provided recommendations to strengthen the current legal framework. Meanwhile the research pointed out EU and UK law areas which have the possibility of adopting into existing Sri Lankan laws.

Keywords: Computer Crimes Investigation, Computer Crime Act, Computer Forensic, Legally Admissible Evidence

ACKNOWLEDGEMENT

This research has become a successful outcome as a result of support, guidance & courtesy received from many individuals. I would like to thank them all for assisting me in making my efforts into a reality.

First and foremost, I would like to express sincere gratitude to my supervisor Dr. Thusitha B. Abeysekara for his continuous engagement and support given throughout the research to make it effective. It was my privilege to work under his invaluable guidance.

I wish to thank Dr. Kutila Gunasekera, my internal supervisor and the course coordinator of MBA in IT for providing guidance and assistance to carry out the research study smoothly and productively. Also I like to acknowledge Dr. Adeesha Wijayasiri for his feedback given in various stages of this study and related presentations.

My special thanks should be extended to all the academic and non-academic staff members in Department of Computer Science and Engineering at University of Moratuwa as well as to all the visiting lecturers associated with MBA in IT degree course.

I owe an extra special gratitude towards all those who participated in my interviews including the members from Sri Lanka Police, University of Moratuwa, Centre for Digital Forensics in University of Colombo School of Computing and SLCERT. Highly appreciate the facts that could be extracted through their discussions as this study would not be able to finish successfully without their corporation.

Also I am extremely grateful to my family members for their patience, encouragement and unconditional support. Without them, achieving this goal would not be possible.

Last but not least I thank all of my fellow batch mates in MBA in IT program and all those who supported me directly or indirectly for the last two years to reach until this stage.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF ABBREVIATIONS

CCA	Computer Crime Act no 24 of 2007
EC3	European Cyber Crime Centre
ENISA	European Network and Information Security Agency
EUROJUST	European Union Agency for Criminal Justice Cooperation
EUROPOL	European Union Agency for Law Enforcement Cooperation (European Police Office and Europol Drugs Unit)
EU	European Union
GAD	Government Analyst Department
ISP	Internet Service Provider
NCA	National Crime Agency
NCCU	National Cyber Crime Unit
NPIA	National Policing Improvement Agency
SLCERT	Sri Lanka Computer Emergency Readiness Team
SL	Sri Lanka
SOP	Standard Operating Procedure
UK	United Kingdom

1 INTRODUCTION

1.1. Background of the study

This research examines the sufficiency level of existing laws related to Computer Crime Investigation process in Sri Lanka (SL) by comparing with United Kingdom (UK) and European Union (EU) laws. The study has a high relevancy and importance at this time because of the current situation in the society. Today with this digital era, most of the people have to use and rely on systems related to Information Technology in order to carry out day to day tasks successfully. With the rapid advancements in the field of Information Technology novel trends are emerging fast. During past few decades the field of Information Technology has gained the ability to make positive impacts for the normal day to day life of the people by making lot of things easier and faster than before. Computer and computer related systems are one such advancement which has changed the way things were carried out previously. Due to that, the usage of computer related systems have grown fast while creating new reasons to attract more people towards using such computer related devices and systems. Even though there are many benefits that reached out to the society as a result of using such computer related technologies, some negative outcomes have also emerged. Computer crimes are one such major disadvantage that affect for multiple aspects of the society. Along with this evolution in technology, there is a considerable growth in computer based and online crimes all over the world (Mshana, 2015).

This situation is same for Sri Lankan context as well. As stated by Annual Activity Report 2020 of Sri Lanka Computer Emergency Readiness Team (SLCERT), there is a significant increase in reported incidents in 2020 where it reported 16,376 compared to the 2019 where it had reported only 3566 incidents. It is nearly a 460% increase (Annual Activity Report, 2020, p.3).

These crimes and their rapid increase are posing challenges to multiple fields while making it difficult to prevent and control. Therefore it has become crucial of having a legal framework that has the ability to provide a strong backbone to conduct a proper investigation on such computer related crimes. As a result of that, it will be able to provide a more systematic way to find out the crime sources and the criminals by giving an advanced logical interpretation to those cases.

The computer crime investigation process is considered as the procedural mechanism that is used to conduct the legal investigations on such computer related crimes. Through that, it recovers and produces legally admissible evidence to the courts in order

to proceed with such court cases. This is carried out by appointed investigators. Due to the complexity and the fast growing trends in computer technologies, investigating on such computer crimes have become challenging and critical (Borges, 2020).

When considering the stages of a computer crime investigation, computer forensics plays a major role within that process. It helps for collecting and presenting legally admissible evidence to the court along with an analysis by adhering to the scientific knowledge standards (Wickramasinghe & Hettiarachchi, 2016).

To combat against the emerging computer crimes, it is essential to have a strong and a comprehensive legal framework for the investigation process. Most importantly it should contain specifications to certain areas when needed based on the type of the crime.

With the purpose of figuring out the law aspects which need further improvements, this research will be addressing computer crime investigation process of SL. In order to make the identification of loopholes easier, this study focuses on a comparison between the existing laws in SL related to the computer crime investigation along with the UK and EU laws in the same aspect.

The reason for including UK and EU laws into the comparison is that both those laws have similarities with the existing SL laws and hence comply up to a certain extent. The current Computer Crime Act in SL is based on the Computer Misuse Act 1990 of UK. In various scenarios EU cases are being taken as guidance principles by SL legal system. Also through ratifying the Budapest convention and implementing it within the country, the Sri Lankan laws related to cybercrime are showing an inherent with the EU laws. Due to those reasons it was decided to focus on the EU and UK laws so that it will enable convenient adaptation of Sri Lankan computer crime investigation laws in the future.

1.2. Significance of the Study

As discussed above, there is a significant importance of having a proper and adequate legal background to carryout investigation of computer related crimes. There are many studies carried out to find the loopholes in computer crimes in general with regard to the current legal framework of SL. But a very few studies specifically focused on finding out whether there are any loopholes in the existing laws for the investigation process in such crimes. Due to the inadequate discussions on that phenomena, through this research it is planning to focus on identifying areas stated in the computer crime investigation

process in SL, which need to be addressed further by having a comparative analysis with EU and UK laws.

1.3. Limitations

The study is basically focusing on the investigation process stated in the Computer Crime Act No 24 of 2007 (CCA) in SL since it acts as the reference laws for conducting investigations of computer related crimes. The comparison of the research has narrowed down into two legal frameworks as UK and EU to maintain the clarity throughout the study when identifying any gap in the existing laws and addressing recommendations more conveniently. Also the qualitative study in this research is limited to reviewing and analyzing of journal articles, books, thesis, acts, and websites along with data gathering through interviews since the research is employed as a mix of doctrinal research and interviews. Under interviews, data have been gathered from three types of investigators as SL Police, IT experts assigned from Universities and forensic investigators. The number of participant for interviews under the category of Police officer is 1 whereas for IT experts from universities and forensic investigators from SLCERT are 4 and 3 respectively.

1.4. Chapter Outline

Chapter one mainly consists of introductory information of the research while emphasizing the significance and the limitations of it. Research problem, respective research objectives, research questions along with research approach and methodology have been elaborated in chapter two. Chapter three is used to implement the theoretical and conceptual foundation while identifying the literature gap to proceed with the study. Chapter four is depicting the analysis and discussion on collected data while the findings and recommendations are being described in chapter five. Implications to be reached out along with the opportunities for future research have been discussed in chapter six by commenting on the conclusion.

2 RESEARCH METHODOLOGY

2.1. Chapter Introduction

This chapter depicts and justifies the methodology used to conduct this study and it consists of two main sections as,

- Research and
- Data

The Research section explains the research problem, research questions, objectives and assumptions (As this is an IT Law research, this does not carry out a hypothesis. However this consists of assumptions on which will be commented after the discussion and analysis). Meanwhile the Data section provides a detailed explanation on primary and secondary data which have been used in this study. As well it contains the information about the qualitative research approach that has been adopted throughout the study. Under data collection system, it elaborates data collection tools and methods which have been used in collecting necessary data.

2.2. Research

2.2.1. Research Problem

Even though Sri Lankan Computer Crime Act is based on the Computer Misuse Act in UK 1990, nowadays, western countries are performing more successful computer crime investigations with sufficient legal background when comparing with SL (Ekanayake, 2019). As of today there are very few court cases at higher courts for computer crimes in SL and due to that no case laws to refer on that context. Therefore, to get more exposure it is necessary to refer cases and solutions from laws in other countries like UK and EU. Even though the legal situation related to computer crimes investigation is in such a situation, the rate in which computer crimes are affecting to the SL society has been increased in several ways as stated by SLCERT Reports (Kulathunga, 2019; Annual Activity Report, 2020). In fact, computer related crimes throw the biggest threatening problems not only to the law enforcement entities but also to the entire society as a whole (Jayasekara, 2015). That adds more weight on the existing laws which are responsible in handling investigations on such crimes.

Thus there is a reasonable question about the sufficiency level of the existing Computer Crimes Investigation laws in SL for handling that process properly (Tharindu, 2020; Perera & Mahanamahewa, 2017). Moreover there is a doubt whether those laws are getting updated in a timely manner so that they facilitate a valid investigation process. According to some studies, number of court cases is remaining open without proper interpretation and unjustified for years due to the lack of necessary provisions within SL legal system for computer crime investigation (Perera & Mahanamahewa, 2017). Therefore it is essential to explore and address the adequacy of the existing provisions within computer crime investigation since it is the standard process that supports to produce and present reliable facts to the court in order to proceed with such cases.

In order to fulfill that need, this research focuses on the computer crime investigation process in SL while comparing the existing UK and EU laws in the same aspect. Through that analysis, it is intended to extract the lessons and solutions from UK and EU laws while addressing Sri Lankan computer crime investigation process to identify loopholes and areas which require further improvements.

2.2.2. Research Questions

The aim of this study is to identify the sufficiency level of the existing laws and any loopholes and areas to be improved further, in order to support the computer crime investigation process in SL through a comparative analysis with UK and EU laws. Computer crime investigation process consists of several stages and among those, computer forensics holds a special place. Therefore it is expected to search and address the current legal background for that area as well.

To respond to the above mentioned research problem, this research is intended to address the following research questions.

1. What is the investigation process in computer crimes?
2. What is the role of computer forensics in computer crime investigation process?
3. What are the main categories of challenges in computer crime investigation process?
4. What are the loopholes that can be identified in computer crime investigation in Sri Lankan legal framework, compared to the UK and EU Laws?

2.2.3. Assumptions

According to the type of the study this has two initial assumptions. The existing laws for Computer Crime Investigation are **sufficient** to conduct a proper investigation or else those are **not sufficient.** This research intends to proceed with the second assumptions until it is accepted or rejected based on the data analysis and discussions.

2.2.4. Objectives

In this research, it is expected to identify the areas that need further revisions or improvements within computer crime investigation process stated in CCA in SL. The study is planning to achieve that, through a comparison of UK and EU laws. In order to address the above mentioned research problem and the research questions, this study aims to achieve following research objectives.

1. To identify and understand the investigation process in computer crimes in preventing and controlling such crimes.
2. To understand the important role of computer forensics within the computer crime investigation process.
3. To examine the main categories of challenges that the computer crime investigation process face.
4. To explore and identify the loopholes in computer crime investigation in Sri Lankan legal framework compared to the UK and EU Laws and provide respective recommendations.

2.3. Data

2.3.1. Primary and Secondary Data

The source materials used in legal researches can be divided into two main categories as primary data sources and secondary data sources (“Introduction to Law”, n.d).

The actual law which is coming under the forms of Acts, Regulations, Court cases, Interviews, Press Release and Statutes are considered as primary legal sources. The data contain in such primary legal sources cannot be changed or modified easily (“Introduction to Law”, n.d.; “What are the different”, 2020).

Since this research requires the exploration of solid basement concepts related to the computer crime investigation process, it is decided to proceed with the above mentioned set of primary data sources.

Secondary legal sources are considered as the resources which help to locate the primary sources of law while permitting to describe, evaluate and analyze the actual law. Therefore such sources can be considered as the background resources which restate the law but argue and critique it at the same time. Books, Journal Articles, Newspapers, Web sources are coming under Secondary data sources in law research ("Introduction to Law", n.d.; "What are the different", 2020). .

The secondary data sources are one of the best places to start this type of a research as they can provide appropriate references to primary data sources. Also they include opinions and arguments about a particular law, mostly presented by a third party (Nemanja, 2021). Therefore, it is decided to include such type of secondary data sources in this study.

2.3.2. Qualitative Research Approach

This study intends to find out the gaps exist in laws related to the computer crime investigation process that comes under CCA. As it requires the exploration and discovery of underlying reasons, opinions and insights to proceed with this type of a research work, it is decided to apply the qualitative approach under empirical category using a combination of library (doctrinal) research and interviews to collect data. With the adaptation of qualitative research approach, it is able to gain an in-depth understanding about the problem (P. Gill, K. et al.,2008) while exploring and evaluating the existing legal framework of SL,UK & EU as a comparative analysis.

2.3.3. Data Collection System

Normally the qualitative data is more subjective since they are related to non-quantifiable data such as thoughts, insights and deep understandings etc. As a result of that, in a qualitative research the range of the data collection system can vary from unstructured to semi-structured (P. Gill, K. et al.,2008). Accordingly the data collection system of this research has been developed.

2.3.3.1. Data Collection Tools

Most commonly used qualitative data collection techniques consist of questionnaires, interviews, focus groups, observation, case studies (Nemanja, 2021). This study gathers a part of the primary data by conducting 1:1 interviews with investigators who are currently dealing with computer crime investigation process in SL. By contacting the experts who have good knowledge on this area, it is able to collect unique information which cannot be gathered from elsewhere. Apart from those interviews, a greater part of data is collected based on the doctrinal research method.

Depending on the need of the study the interviews have been conducted as structured and semi-structured by following a list of predetermined key questions (refer Appendix-A). Under interviews, information has been gathered from below mention three types of investigators.

- A Police officer who works attaching to the IT department.
- IT experts who has been assigned for such investigation via universities
- Forensic experts from SLCERT

The reason for selecting those investigators is that, they are the ones who are currently engage in Computer Crime Investigation process. Therefore, they experience any limitation or gap in the existing legal framework, which acts as barriers to perform the investigation successfully.

According to the request came through most of the investigators, their identities should not be revealed during the study. Therefore, only the role of each investigator and the organization they are working have been included in the research.

The details related to the held interviews have been stated in the table (see Table 2.1: Interview Details).

Table 2.1: Interview Details

Role/Type of the investigator	**Organization**	**Date of the interview and time**	**Number of participants**	**Participant Name**
Police officer	SL Police – IT Department	2021.07.17 4.30p.m – 5.30 p.m	1	X

IT Expert	University of Moratuwa	2022.02.07 8 p.m – 9 p.m	1	Y (All 4 members have denoted using Y)
	Centre for Digital Forensics in University of Colombo School of Computing	2022.06.28 10 p.m – 11.30 p.m.	3	
Forensic Investigator	SLCERT	2022.05.14 10 a.m – 11. 30 a.m	3	Z (All 3 members have denoted using Z)

Source: Constructed by Researcher

From this chapter onwards the "Participant Name" will be used in order to denote each interviewee.

Library (Doctrinal) research (McConville & Chui, 2017; Gawas, 2017) has been used as the main source for secondary data collection in this study. The secondary data includes sample sources from SL, UK & EU, related to the Computer Crime Investigation process.

2.3.3.1. Data Collection Methods

This research consists of a combination of interviews and library research. One of the primary data collection methods which have been used in this study is the interviews. The form of these interviews differed from structured to semi-structured as the way the discussions were conducted. The set of key questions used in interviews have been listed under Appendix A. Apart from the interviews the other sources for primary data collection includes Acts and Regulations.

The library research has been used to gather all the secondary data and a part of the primary data of this study. Therefore under library research, the study has gathered primary data by referring to the Acts and Regulations of the three jurisdictions; SL, UK & EU. The secondary data has been gathered by refereeing to the relevant journal articles, books, newspaper articles and web sources.

2.4. Chapter Summary

This chapter has described the research problem, research questions and the objectives of the study in detail while exposing the determined research approach and the methodology through which the research is going to be employed. Accordingly all the Primary and Secondary data collection methods and the respective data collection tools have been included with it.

3 LITERATURE REVIEW

3.1. Chapter Introduction

The purpose of this section is to find out the literature gap exist in relation to the research problem specified. In order to achieve that, a continuous search has carried out to find and extract existing literature related to the context of the research problem. Through that, it is able to identify, compare and contrast the available knowledge for figuring out the literature gap in order to proceed with the study. Also this chapter provides a theoretical background for the research problem while facilitating a path to build up a rich conceptual backbone to the research.

3.2. Computer Crime Investigation Process and Computer Forensics

The investigation of crime has been defined as "the process of legally gathering evidence of a crime that has been or is being committed" (Brown, 2001). Even though the underlying concept is same, there is a considerable difference between the traditional investigation process and the computer crime investigation due to the incredible capabilities of the information systems. As a result of that it requires additional amount of efforts for successfully carrying out the prosecutions of perpetrators (Hinduja, 2007).

According to Borges (2020) computer crime investigation process consists of common steps such as background check, information gathering, tracking & identifying the authors and computer forensics etc. In Background check, the background of the crime is created and defined by the investigators in order to establish the starting point for the process. Through the information gathering stage, they try to extract information as much as possible for the crime incident by clarifying multiple questions. They try to figure out facts about the attack such as whether they are automated one or human based targeted one, any open opportunities that caused the attack, the scope and the impact of the attack, the skill level needed to perform the attack, the possible suspects, the evidence and where they can be found and the accessibility to such sources etc. Tracking & identifying the authors is the slowest phase since it requires legal permissions and court orders to acquire necessary data. Through this phase they try to gather details from the Internet Service Providers (ISP) and other networking companies to find out log information of the connections used for the crime incident.

Among those stages in the investigation process, computer forensics performs an important part. One definition has been given for the computer forensics as "the science

of acquiring, preserving, retrieving, and presenting data that has been processed electronically and stored on computer media" (Noblett et al., 2000). But according to many experts this definition will not cover the precise meaning since nowadays digital evidence can also be extracted from the devices which are not traditionally considered as "computers"(Allen, 2005). Another acceptable definition has given as the "process of identifying, preserving, analyzing and presenting digital evidence in a manner that is legally acceptable" (McKemmish, 1999).

According to the Digital Forensics Workshop Model, computer forensics includes seven major steps as identification, preservation, collection, examination, analysis, presentation and decision. In identification, it is recognizing the need to conduct a forensic investigation. By maintaining a suitable chain of custody, necessary data is acquired in a forensic manner during the preservation. Through the use of needed software & hardware along with necessary legal authorities, evidence is gathered in collection stage. By using data extraction techniques and filtering mechanisms, the artifacts of interest are identified through the examination. In analysis, link all the artifacts and events and try to understand their chronology for getting a complete picture of the scenario. During the presentation, findings are documented and presented in a suitable way. The decision stage is used to determine the sufficiency of the available evidence in order to proceed with the legal procedures for a criminal case. (Clarke, 2010, p.20).

Depending on the type of the investigation and the nature of the digital evidence, the in-depth analysis for computer forensics varies. Therefore, standard operating procedures (SOP) cannot be established for carrying out forensic analysis for all kinds of computer related crimes. (Casey, 2001,p.8).

3.3. The main categories of challenges in Computer Crime Investigation process

Many experts all over the world have pointed out key challenges that are prevailing in the field of computer crime investigation. All those challenges can be grouped into 3 main categories as, Technical, Legal and Resources in terms of skills and knowledge (Husain & Khan, 2020).

The root challenge for the field of law is the difficulty of the law enforcement authorities to keep going with the rapid growing changes in the technology. The existing laws and terms cannot be updated as fast as the technology demands and changes are growing. The main challenge comes under resources category is the requirement of

standard knowledge and high skills needed to find, gather, preserve and transport the computer crime related evidence which is in the form of intangible. Lack of consistent standards and protocols to carry out the investigation becomes another challenging area (Hinduja, 2007).

When considering the computer forensics, it is dealing with same kind of issues related to the lack of skillful resources, unavailability of procedures & policies and the trainings that are needed to enhance the required skills and knowledge of relevant personnel (Radu, 2020). Moreover it is fighting over the technical challenges including the preservation of digital evidence, improving processing power and encryption of data (McKemmish, 1999 ; Allen, 2005 ; De Hert et al., 2006). Also, the large volume of data that can be stored within hard disks and ensuring that the gathered digital data are preserved during the forensic process have become a challenging task due to their perishability nature (Allen, 2005).

According to Allen (2005) the reliability of the digital evidence extracted via the forensic process and proving its solidness is another tough point. As well the privacy rights of the accused person along with the unreasonable search and seizure add more weight towards the challenges in computer forensics.

The technology gap between the emerging technologies used by cyber criminals in their activities and the forensics tools or software used by the investigators is another main challenge (Harbawi & Varol, 2016 ; Allen, 2005).

The relationship and the agreements between the law enforcement and ISPs or telecom companies also plays demanding when making the necessary data available while preserving them for a longer period (Perera & Mahanamahewa, 2017).

The jurisdictional issues related to obtaining digital evidence and the scopes of the warrants they can issue are also impacting heavily for the computer crime investigation process. Due to the unavailability of sufficient legal norms, it raises practical infeasibilities when obtaining the access to a computer system that is needed for an investigation and seizing or shutting down such systems (Azad et al., 2017 ; Radu, 2020). The lack of harmonization related to the investigation processes in the field has become another combating issue (Radu, 2020).

Having multiple jurisdiction for cybercrimes is another key challenging point (Guinchard, 2007). As a result of that, in some cases, a questionable area is created when trying to figure out whether to apply local or state or national or international law or a combination of them for investigating an online crime that is affected for overseas (Allen, 2005).

Most of the countries including EU, North Africa are experiencing several issues due to the lack of international collaboration they have gained in order to exchange the needed information related to any computer crime. This becomes worse since there are very less number of international treaties for mutual assistance and extradition(Sarrab et al., 2013 ; Radu, 2020). As the remedy, in order to address legal challenges, the existing laws should be updated and transformed in a practical manner by overcoming the language barriers and lack of knowledge in foreign legal matters (De Hert et al., 2006).

When it comes to Sri Lankan context, there are some categorizations done for the challenges coming under computer crime investigation. According to Geethal et al. (2020) challenges coming under cybercrime investigation in Sri Lankan social network, can be categorized under multiple areas such as Multiple Jurisdiction Challenges, Legal Challenges, Technical Challenges and Privacy Challenges. Similarly the field of computer forensics is also going through issues which can be grouped under Technical challenges, Resource challenges and Legal challenges (De Alwis, 2017).

3.4. The loopholes in Sri Lankan legal framework for Computer Crime Investigation, compared to the laws in UK and EU

Computer crime investigation process across the world is facing multiple challenges and this is same for the Sri Lankan context as well. Due to the absence of clear and precisely defined rules and laws applicable to this area, it has created several challenges to the law enforcement entities within SL when compared to the western countries.

CCA contains the laws related to computer crimes investigation. But there are several issues emerged due to the inadequate legal background that requires further review and improvements as per the numerous research and academic work have pointed out.

According to several studies there is a questionable area related to the appointment of expertise to conduct the investigation process (Ariyadasa, 2019a; Ariyadasa, 2019b; Ekanayake, 2019; Fernando, 2019; Iroshan, 2019; Perera & Mahanamahewa, 2017).

The Computer Crime Act Section 17 specifies the required qualification and experience of an expertise by defining broader fields such as electronic engineering or software engineering. But the act does not mention a specific field of specialization for each of the required qualification levels (Ariyadasa, 2019a; Fernando, 2019; Iroshan, 2019).

Iroshan (2019) has described how European Union Agency for Law Enforcement Cooperation (EUROPOL) has given a precise description about the qualifications which need to be fulfilled in order to be appointed as professional cybercrime investigators.

According to those terms, need to have exposure in investigating cybercrimes through two years of experience in cybercrime and related laws. The law enforcement knowledge in the field of cybercrime is expected in the international level. As well it requires having the experience and the capability to draft operational and strategic reports. Further, as the essential qualification, it expects to have the knowledge and skill in open source intelligence. As well, it has specifically pointed out the knowledge areas that are highly needed in terms of database and programming languages. The knowledge related to the web technology is expected as professional qualifications. Apart from those essential eligibilities, competencies related to administrative, problem solving, analyzing are also required along with good communication skills for both writing and speaking of English language. Therefore he has emphasized the importance of updating the qualification levels required for being appointed as computer crime investigator in SL.

Tharindu (2020) and Fernando (2019) have also pointed out the facts regarding the appointment of computer crime investigators in SL vs EU. There they have highlighted how the investigations for cybercrimes are carried out by EU through special agencies like EUROPOL and European Union Agency for Criminal Justice Cooperation (EUROJUST) which are maintained dedicatedly for serving and fulfilling the objectives of cybercrime investigations. On the other hand, they have indicated about the Sri Lankan context. Due to the unavailability of a dedicated agency type, the police officers have to be appointed for carrying out the cybercrime investigations irrespective of the fact that the needed technical skills and qualification levels are actually fulfilled or not by the respective officers. Iroshan (2019) and Ekanayake (2019) have also emphasized this matter and hence they have shown the importance of having a separate department like European Cyber Crime Centre (EC3) belonged to the EUROPOL to proceed with these types of investigations. This study will also identify the areas to be updated regarding the qualification levels of the computer crime investigators as well as their appointments and propose a precise set of specifications on that aspect.

According to Computer Crime Act section 17 (4), an expert with the mentioned qualifications is appointed in order to assist the police officer who has been granted all the necessary powers for the investigation. But this can be a difficult task for an ordinary police officer in SL since a proper technical knowledge is essential to carry out the work within this field. This is in contrast to the Council of Europe where it uses a separate knowledgeable expert and the police to assist that person. Therefore this should be the practical approach that is needed for Sri Lankan context as well (Ariyadasa, 2019a; Iroshan, 2019; Tharindu, 2020; Kulathunga, 2019; Ekanayake, 2019). Upon the assertion on that context, this study will also have the same intention.

Ekanayake (2019) and Fernando (2019) have pointed out another fact which others have not paid much consideration. Since the Computer Crime Act mentions that the expert

should be from “any other public institution”, they have indicated this point as an updateable section. As per their point of view, they have considered this as a break of equity and justice while elaborating how EU is appointing “Joint Investigation Teams and “Joint Customs Operations” in their investigating authorities. Further, they have described about the collaboration between the public authorities & state departments with EUROPOL and EC3 when obtaining necessary information. Through this study it is planning to address this fact further because this can be a debatable point as to which extent the collaboration should be made available in order to gain the best out of an investigation work.

As stated in Computer Crime Act, if the relevant officer thinks that there is any risk or danger for the useful information related to the investigation, that officer needs to notify the corresponding person who possesses the evidence to safeguard them for a period of seven days through a written notice. This is an impractical approach since it has ignored the volatility of the data as well as the questionable areas regarding the trustworthiness of the other party. Also this cannot be applied to scenarios where the particular device or information has being hacked or the system resides outside the Sri Lankan geography. Therefore having this kind of loopholes in the legal system is like giving better opportunities for the criminals to commit more crimes without any punishment. When implementing laws for this kind of scenarios, it should always align with the real world practical scenarios. Hence for the preservation of data related to cybercrime, should obtain backups as soon as possible without waiting days and hours. If compare this situation with EU, they have mechanisms implemented to address the gathering and preservation of evidence which is residing inside any computer or device across the world through the assistance of member states and the service providers of non-EU states. Therefore this area specified in the Computer Crime Act requires special attention and update. (Ariyadasa 2019a; Ekanayake, 2019; Fernando, 2019; Iroshan, 2019; Tharindu, 2020). This study will also have the same objective on that matter.

According to Fernando (2010) many experts are reluctant to be called upon to provide evidence by exposing them to any cross examination in a court. Due to that, those experts hesitate to be designated under that. Therefore as a remedy he is suggesting to update the existing laws by including the facility to submit an affidavit evidence regarding the sensitive investigations. As well he has mentioned concerns related to the admissibility of computer based evidence which is going to be dependent on several stringent criteria. Since the existing Computer Crime Act does not contain specific terms on this matter, need to refer and get help from the terms coming under Electronic Transaction Act. As per his point of view, before applying those terms, it requires further reviews.

Since Preservation of digital evidence is a main factor in computer forensics, preservation period has a direct impact on the investigations. But currently that

preservation period is differ based on the service provider due to the fact that it is not defined by the existing legislation. But when considering the Australian Attorney General's department, they have specifically mentioned a minimum of two years period for the service providers to retain their subscriber and transaction data. Therefore this factor should be included in the act with some necessary updates. (Perera & Mahanamahewa, 2017). Going with the intention of those researchers, this study will also assert the same.

As per the Section 18 (4) of Computer Crime Act, the interception and retention of data and information for the purposes of an investigation need to be handled under the procedures prescribed by the minister. But in this case, it has ignored the fact about the competency level of the minister with regard to the knowledge he or she has on the subject matter. Since computer crime investigation is a very critical area, that decision making should be handled by a highly skilled and experienced expert in the field of cyber-crime with a broader exposure at the international level. This issue has been addressed by several studies (Ariyadasa, 2019a, Ekanayake, 2019; Iroshan, 2019). By agreeing to the above point made through those research works, this exploration will also emphasize similar analysis on that matter.

According to Ekanayake (2019) the legislation states that the intention is sufficient to commit an offense. But it does not consist of valid procedures to prove the intention. But when considering the EU laws they are using methods like "evidence audience". Therefore this becomes another area to be improved as per his study. Similarly this research will also have the same intention.

Even though the current Computer Crime Act has granted permissions for the necessary officers to obtain a warrant or to intercept any communication of a service provider, it has not considered the privacy policies that the particular service provider needs to adhere to. As a result of that, the investigative officers may have to face some practical limitations which have been neglected by the laws when try to obtain the needed data to proceed with the case. Therefore this area also falls into the updateable law category (Iroshan, 2019). Since this can make a direct impact when carrying out investigation work practically, this study will also share the same intention as Iroshan.

As Ariyadasa (2019a) and Perera & Mahanamahewa (2017) mention in their studies, there is a lack in international collaborative law enforcement mechanisms in SL. As a result of that, issues occurred when trying to gather electronic evidence of the sources which are located outside Sri Lankan geography. As well such barriers make restrictions when proceeding with the prosecution of the suspects who are not Sri Lankan citizens. Also they assert that even though the section 27 of Computer Crime Act enables the

extradition of computer criminals among the states, in order to effectively execute this provision of law, the collaboration plays a vital role.

According to the section 26 of Computer Crime Act, the proof of document that needs to be issued by a police officer or the expert, should be produced as “Prima facie evidence”. Ekanayake (2019) and Ariyadasa (2019a) have commented on this in their studies. Due to the intangible nature of the data or the evidence associated with information technology, there will be nothing to present physically. For an instance, in a signal interception, there is not a properly defined way to endorse it under the existing document way of evidence. Also the act does not mention any mechanism to authenticate such crimes.

There is a challenge for preventing and mitigating cybercrimes in Sri Lankan society due to the unbalance between the process of investigating such crimes and the rights of the users who use variety of networks and related technologies. Therefore it is essential that the existing legal system should be reviewed by identifying areas that need further modifications. As well these updates should be carried out in a coordinated manner in which investigators, judges and prosecutors are involved. Moreover, SL can refer other developed jurisdictions like UK, USA, Australia and even India for taking the lessons and understanding new approaches of cybercrimes and preventing them. (Indrakumara & Fernando, 2022). This study will assert the same objective on that context.

According to Samarakoon (n.d.) UK has taken steps to limit the computer crimes in an appreciable level by introducing more provisions not only in investigation context but also in prevention of such computer related crimes. Therefore he is suggesting to update the existing Sri Lankan legal system in a manner in which it aligns and compatibles with the international law related to the computer crimes. In order to carry out computer crime investigation work successfully, this study will also share the same opinion as Samarakoon.

3.5. Literature Gap

The existing literatures on computer crime investigation have not focused on the law areas that should be updated based on the experience and challenges faced by actual investigators who are dealing with computer crime investigation process at the moment. Also most of the literatures are unable to provide practical and long term strategic recommendations according to any identified challenge that can be addressed conveniently through legal system. Therefore, this study plans to discuss those

untouched law areas to facilitate sufficient and appropriate legal background for SL to carryout computer crime investigation successfully.

3.6. Chapter Summary

This chapter has established the theoretical and conceptual foundation through comprehensive literature review related to the subject matter of Computer Crimes Investigation process in SL in relation to the existing legal framework. Also the chapter has identified the literature gap that exists within the context of the research problem.

4 DISCUSSION AND ANALYSIS

4.1. Chapter Introduction

The purpose of this study is to explore the sufficiency of laws related to computer crime investigation in SL, with a comparison of EU and UK laws. In order to achieve that aim, four objectives have been developed in chapter two by specifying the research approach and the data collection in detail. This chapter is providing the answers to the research questions by showing how the relationship among each research question has established.

4.2. The Investigation Process in Computer Crimes

When considering the current Sri Lankan legal framework, CCA and the Code of Criminal Procedure Act, No. 15 of 1979 use as the two main reference instruments for conducting investigations on computer related crimes (Janaha, 2013).

According to the interviews conducted with three types of investigators (X,Y,Z), they all emphasized on the importance of carrying out a proper investigation by following proper procedures, standard practices, and generally accepted guidelines according to the existing laws. According to Y and Z, if the responsible parties are unable to conduct a valid investigation process, that can be a motivation for those who involve in frauds or illegal activities in cyber space to continue such computer related crimes.

The computer crime investigation process starts with receiving the complaint to the Police. Then the particular complaint is verified by the Police through preforming a background check. Next the tools used in the crime are identified. Therefore the SL Police acts as the first responder in computer crimes related cases by being responsible for the initial stage tasks including analyzing the crime scene, seizing the items etc. (X, Y, Z).

Next, computer forensics comes into the play. After getting an official request from a court or Police or CID, an expert is allocated by a university in order to carry out the necessary investigation process related to the considered computer crime. This is same if getting help from any other organization such as SLCERT, TECHCERT which conduct forensic investigations (Y). According to Z, generally those organizations are contacted if it is unable to find an expert from university level to get technical assistance for the investigation.

As Y mentioned, the expert then follows a particular forensic process model based on the considered computer related crime. Even though there are multiple forensic process models available to address different incidents, all of those models consist of the following basic process.

1. Official starting up
2. Evidence extraction
3. Evidence preservation
4. The chain of custody
5. Analysis
6. The report

The allocated experts are providing only the analysis of the result since they are unable to provide the conclusion. Therefore, generally there are no conclusions in a forensic process as those will be drawn by the lawyers and the judges (Y).

According to Y and Z, protecting the concept of Chain of Custody becomes really important as long as the collected items reside with any expert. Also maintaining the integrity during the forensic investigation plays a vital role.

Generally during an investigation, following steps are carried out as mentioned by Y and Z.

- Collecting any external data or evidence (Ex – taking photos, videos, recordings and any notes) need for the case.
- Verify whether the tested device/system is the original one that is related to the crime as mentioned in the court order to be used in the investigation work.
- Safely remove the hard disk or any other device by maintaining the integrity and make it write protect so that any modification would not affect to the original data. This becomes essential for the investigators otherwise the court can question experts regarding data writing in the evidence.
- If it is a computer, then the hard disk is imaged through a write blocker in order to avoid any changes to the original data within it.
- Keep the original device in a safe mode.
- Duplicate the first image so that we have three copies/images at last.
- Calculate the hash values to maintain the integrity and to start the investigation. Verify whether the images taken are same as the original one by calculating the hash values.
- Take the clones or the bitwise image to proceed with the analysis without conducting the investigation using the actual evidence.
- Start the report preparation, in parallel to the investigation.
- Gather evidence to CDs/DVDs or as printed materials (based on the request)

- Conclude the analysis by calculating hash values again to maintain the integrity.
- Review, verify and check the report thoroughly and hand it over to the relevant case officer after a knowledge sharing of the case.
- By preserving the chain of custody, hand over the items to the relevant officer.

As per Z, SLCERT maintain ten year storage of evidence, if in any case, court or SL Police request them later. After 10 years those evidence are archived.

4.3. The role of Computer Forensics in Computer Crime Investigation process

According to three types of interviewees (X, Y, Z), the computer forensic becomes a must within a computer crime investigation process even though it represents only one part of the whole process. The computer forensic process is used to verify and prove the real scenario by presenting computer based evidence in a legally admissible way. Without having valid and acceptable evidence, a computer crime case will not proceed as there is an issue with the interpretation and presentation of evidence.

Through computer forensics it is able to disclose the content of metadata associated with any files which then help to reveal past user activities related to those files. That is why the outcome of this process plays a vital role in identifying the real criminals behind any computer crime (Wickramasinghe & Hettiarachchi, 2016).

According to Y and Z, the characteristics of digital evidence differ from traditional evidence. Since the evidence reside inside a system cannot be verified straight away like a physical element, computer forensic component becomes mandatory to deal with computer crime investigation. Also when there is digital evidence, in order to protect and maintain the integrity, conducting computer forensic becomes a must. Computer forensic is a combination of analysis, conclusion and drafting the report.

As Z mentioned currently in SL we don’t have any guidelines when performing digital forensics. But in UK they have. Therefore in order to work in that area, SLCERT has developed a SOP for that. According to Y, the Centre for Digital Forensics in UCSC is conducting the forensic work by adhering to the guidelines specified by The National Policing Improvement Agency (NPIA) in UK. This means currently there is not a generally accepted standard to follow when performing technical investigation on computer crimes within SL.

Generally the forensic team should consist of different expertise which needs to be there to cover up the forensic process. Apart from that, legal clearance and certain tools including both software & hardware are needed (Y).

4.4. The main categories of challenges in Computer Crime Investigation process

According to the conducted interviews with three types of investigators, some barriers could be identified as the challenges they are facing when conducting computer crime investigations. Each challenge could be grouped into three main categories (see Table 4.1: Challenges in Computer Crime Investigation Process).

Table 4.1: Challenges in Computer Crime Investigation Process

Investigator	X	Y	Z
Technical Challenges	Unavailability of proper mechanisms to backup data	Preventing modification of data or evidence	Difficulties in getting access to the data by handling all the security and privacy setups in each device
		Copying data as an image not as files which can cause things to be changed	Storage issues when maintaining backup data
		Need of high storage capacity to make several clones and to keep backups of evidence	Mistakes from first responders affecting negatively to the forensic investigation
		Need of performing lot of analysis that may take time	Forensic investigation being time consuming
		Unclear evidence leading to challenges	
		Unclear questionnaire provided via court orders (without mentioning what exactly they are looking for) leading to time wastage	

		Inability of accessing the low level resources that the cloud providers have	
		Inability to extract enough evidence due to the unavailability of forensic ready systems	
Legal Challenges	Unavailability of a defined preservation period for ISP related data	Getting the legal clearance of the data along with the witnesses so that it will be a transparent process	Unavailability of laws to address cloud related crimes
		Inability to apply the existing laws for the cloud related things	
		Inability to narrow down the responsibility towards one investigator when the given report is challenged by the court as (most of the time) the report is an outcome of panel of investigators	
		Unavailability of properly specified standards to follow during the technical investigation	
Resource Challenges	Unavailability of skillful resources within the Police	Having a dedicated forensic team with necessary expertise	Difficulty in finding qualified professionals for digital forensic area due to the less job market.
	The cost for investigating some computer crimes being higher than the fine charged for such	Unavailability of enough budget to maintain any certification/ renew the licenses or to	Difficulty in affording the required software and hardware

	crimes	purchase needed equipment	
	Determining what tool to be used for the forensic work	Unavailability of skillful resources which have knowledge on both technical and legal fields.	Officers being reluctant to be appointed and work if the report presented was challenged by the court

Source: Constructed by Researcher

4.4.1. Technical Challenges

Since computer forensic work requires lot of analysis and searching of large amount of data, an increased storage space is an utmost need (Wickramasinghe & Hettiarachchi, 2016). But still a proper long term mechanism is not available for fulfilling that (X). For some of the data, taking images of everything becomes difficult as well as impractical. Due to that, need to make several clones in order to keep the forensic image of the particular disk or multiple disks. This requires lot of storage which acts as a challenge. In order to protect evidence from being tampered need to take precautions (ex- Use of Write Blockers) during the investigation process. Due to the unavailability of large storage and necessary tools & equipment, it has become a challenge (Y). As Z mentioned since the organizations like SLCERT need to keep 10 year backup storage for every evidence, maintaining such a huge storage has thrown practical difficulties.

Meta data of the evidence being modified due to the use of certain tools has become challenging. In order to preserve Meta data of the files, it is necessary to copy data as images not as files which then requires certain tools. Even though those tools are used to copy data as images, some tools cause certain Meta data of the evidence to be changed and that becomes a challenge. Also some of the free tools used to extract evidence are very primitive and more sophisticated & convenient tools are quite expensive. Due to that, it has created several challenges when performing forensic work (Y).

As Z mentioned there are difficulties in getting access to the data during an investigation. Most of the existing devices can be locked using a pin or password. Due to that, getting the access to the data lies within a particular hard disk has become more difficult. Also it is hard to read data which has been protected based on the concept of 'Encryption and Decryption'. In order to decrypt, relevant keys are needed. This acts as

a technical limitation which impacts the investigation (Z, Wickramasinghe & Hettiarachchi, 2016).

Forensic investigation requires lot of analysis that may take time. From the place where items are handed over to the experts, to where they are handed over back to the police, the time it requires to complete the investigation will depend on the number of items that need to be analyzed and the evidence or the answers requested by the court via the court order. The investigation is a combination of tools and the human factor. Therefore even though tools are used to get some help, they also require lot of time to process data. Investigator also needs a considerable time to gather evidence and prepare the report as requested (Z). For some cases unable to predict a time since it is hard to know whether it is able to find a path without further investigation. This leads to a challenge. Also when try to proceed with intelligent guesses, proving that other paths are redundant and not necessary to consider, becomes difficult (Y). In some cases, unclear questionnaire provided as court orders leads to time wastage of the investigator as those documents do not specifically mention what exactly they are expecting as the outcome of the forensic stage. Because of that, the investigator has to contact the respective Police officers to get clarifications in order to proceed with further investigation work (Y).

As well if the evidence is not clear, forensic process becomes difficult when try to recreate the crime scene through time traversal into the past by considering each possible state (Y).

Currently there is no ability to access the low level resources that the cloud providers have. Because of that, in order to prove that the data is not tampered, need to use the available surface level evidence. If the cloud service provider is not providing those data, need to go with a court order which will take lot of time. That may lead to a loss of evidence (Y).

According to Y, when conducting investigations, sometimes it is unable to extract sufficient evidence because the existing systems not being forensic ready. In such cases, absence of necessary logs and audit trails affect negatively for carrying out a proper investigation.

As Y and Z mentioned, the mistakes from first responders affect negatively to the forensic investigation. Most of the time Police officers act as first responders. Since they do not possess proper skills and understanding on this subject matter, they do some mistakes when collecting and handing over the evidence to the experts. Those mistakes sometimes affect negatively for the investigation work and hence cannot proceed with further investigations. Also as Y mentioned, due to the lack of knowledge of the Police officers regarding this field, they are not able to prepare a valid questionnaire or to ask the required questions in a way that the expected answers can be filtered through a

proper forensic work. They ask broader questions such as to provide a detailed report on all the data available inside the computer. In such cases, since the investigator cannot understand the limit, conducting the forensic process for such broader area becomes very difficult with the increased capacities in hard drives and any other devices.

4.4.2. Legal Challenges

According to Y, currently there are no properly specified standards to follow during the computer forensic stage within SL (refer section4.3). Due to that, the specifications and the way the process is carried out differ based on the organization or the type of the investigator. (Ex – The way the computer forensic process is performed in University of Moratuwa is differ from the process followed in Forensic unit of UCSC or SLCERT or any other organization like Government Analyst's Department (GAD))

Unavailability of defined preservation period for maintaining (ISP) data that directly affect for investigation work has created several difficulties for the people who involved in such investigations (Perera & Mahanamahewa, 2017). When considering an ISP, the laws coming under any existing act or regulatory body do not specify a date limit to store data. As a result of that, even though they keep billing data, no background or transaction related data or application level data are kept for a considered period of time and this affect directly for the investigation work (X, Y, Geethal et al., 2020).

According to Y, gathering data along with the legal clearance is a must but also a challengeable task within an investigation process. It is really important to have a transparency throughout the forensic process as otherwise if the accused made an argument, the expert who provided the evidence should be present in the court. But generally the experts are not revealed as it should be kept anonymous. Therefore, for the betterment of all, it is required to get data with legal clearance which becomes a challenge.

Also as Y mentioned, in any case, if the given report is challenged by the court, it is difficult to narrow down the responsibility towards one investigator as most of the time the report is rendered as an outcome of panel of investigators. According to Y and Z, in such scenario, the current legal system does not support necessary facilities for the technical investigators to provide their expert witness separately by incorporating anonymities. Since they have to come to the court and provide the evidence publicly, sometimes it creates life threats for these types of IT professionals.

Currently in SL there are no laws defined to apply for the cloud related crimes. That acts as a loophole since modern society is moving fast to rely on cloud computing services

(Y, Z). Also the cloud related things are belonged to different countries which are governed according to different jurisdictions (Perera & Mahanamahewa, 2017). Therefore, when become cross boarders it is leading to multiple challenges since what has defined as legal and illegal can differ from one country to another (Y). Similarly unsupportive social networks which fall under multiple jurisdictions create severe threat for perusing computer crime investigations in a country like SL (Geethal et al., 2020).

More over the anonymization techniques which are used to hide identity of cyber criminals including dark web act as biggest challenges related to computer crime investigations (X, Geethal et al., 2020; Perera & Mahanamahewa, 2017).

4.4.3. Resource Challenges

According to Perera & Mahanamahewa (2017) it has become difficult to have a set of digital forensic experts who are updating their technical competencies in order to deal with the modern technologies used by cyber criminals in their activities. Also not having a proper qualified regulatory body which can guarantee on competency level of the forensic professionals is leading to create negative view on their tasks (Wickramasinghe & Hettiarachchi, 2016).

As mentioned by X unavailability of skillful resources within the SL Police acts as a major barrier to perform proper investigation for computer related crimes. There is very low number of police officers who are well knowledgeable and expertise to work on this area. Even though the officers who are dealing with computer crime investigation process have the ability to understand the severity of data or evidence related to this area, still most of the others including top executives do not understand that. Especially due to the absence of knowledge for following a proper mechanism when the evidence are being transported and seized, SL Police are struggling. As a result of that, sometimes it affects negatively for the continuation of investigation work. In most of the cases, SL Police do not have the required knowledge to deal with this work. Due to that, when they have to work with an expertise team allocated from a university or any other investigation organization, it becomes difficult for the Police officers. According to X, even though some training sessions were conducted to educate on technical investigation area, those have been conducted focusing on top-executive levels of SL Police instead of sharing the knowledge for the Police officers who are actually dealing with Computer Crime Investigation process.

Also it has become a challenge that the cost for investigating some computer crimes being higher than the fine charged for such crimes. When considering a computer hacking incident, the fine amount charge (Rs.1.5 LKS) is very less compared to the cost

incur for the Police to investigate such crime. Therefore it has become difficult to carry on investigation work with such a less gain (X).

According to Z, there is a difficulty in finding qualified professionals for digital forensic area due to the less job market. Most of the IT professionals are paid well within the IT industry. So they do not tend to join a government organization like SLCERT. Thus they are dealing with some issues in their organizational structure side. As well, some of the professionals are being reluctant to be appointed and work as investigators in SLCERT. The reason is sometimes the court asks the officers to be present at court when challenging the report. Since an organization like SLCERT has IT professionals not the legal officers, such situations become difficult and due to that also most of the officers are reluctant to be work at this area.

Having a forensic team with necessary expertise is an utterly important fact to proceed with the proper computer crime investigation. The team should consist with required expertise along with the hardware and software tools. But having a team with all these necessities has become a challenge as Y mentioned. Further Z was also emphasizing on difficulty in affording the required software and hardware. The Software tools which should be used for forensic work are very expensive. Those advance tools and license are not in a level which some government organizations can afford. Purchasing licenses and renewing them annually have become difficult in that case by adding a heavy weight to the operational cost. According to Y, currently no separate budget allocation is done by the SL government for the universities to conduct computer crimes investigation tasks. Therefore they are experiencing difficulties in maintaining any certifications or purchasing needed equipment.

As X mentioned, when conducting any investigation by SL Police, it becomes difficult to determine what tool to be used for the forensic work. Since the law or any existing regulatory body do not specify particular tools to be used during computer forensic stage of an investigation process, deciding what to be used has become an issue (Perera & Mahanamahewa, 2017). Most of the times open source software and tools are being used since it is difficult to purchase the commercial ones by the Police.

According to Y and Z, there are very less number of professionals who possessed knowledge on both technical and legal fields. But in order to provide solutions for the issues exist in current computer crime investigation process, it is important to have opinions from that kind of expertise in terms of executing the case and presenting & interpretation of digital evidence. Moreover they emphasized the fact that due to the lawyers and judges being unable to understand some of the technical aspects of the Computer Crime Investigations, sometimes it affects negatively for the final conclusion of such cases.

4.5. The loopholes that can be identified in computer crime investigation in Sri Lankan legal framework, compared to the UK and EU Laws

Based on the studies carried out for addressing the sufficiency or insufficiency of existing laws related to computer crime investigation, below facts were highlighted.

According to Y and Z, the laws specified in current Computer Crime Act are playing a vital role to conduct an investigation. Due to the way the act has drafted, it is providing definitions for most of the aspects related to the investigation of computer crimes. But meantime, based on their experiences they pointed out various points which require further updates with the time being. According to them, those areas should be amended. Similarly the doctrinal research also pointed out several law aspects that need further revisions in handling computer crime investigations.

Existing Computer Crime Act does not provide a proper detailed level definition that addresses the qualification level regarding the appointment of panel of investigators (Perera & Mahanamahewa, 2017; Ariyadasa, 2019a, p.16; Fernando, 2019, p.8; Iroshan, 2019,p.10). It defines only the broader fields without going into specific details. Even though the section 17 (3) specifies that the conditions related to the appointment of experts are described by regulations, those are not getting updated in timely manner. EU is conducting investigations by allocating relevant investigators for the tasks through special agencies such as EUROPOL, EUROJUST, European Network and Information Security Agency (ENISA), and EC3 (Directive 2013/40/EU). For each investigator position they maintain an updated list of qualifications with precise descriptions. EUROPOL specifies necessary qualification for each position in a more precise manner when they are publishing any vacancy (EUROPOL, 2022). This way they are ensuring that the people they hire for any given position are the most suitable ones.

Similarly UK is also having separate regulatory entities and agencies for cybercrime investigations. National Crime Agency (NCA) acts as the primary law enforcement entity which bears the responsibility of investigating cybercrimes in UK (Nikolić, 2020). As stated by NCA, its officers work within a broader range from investigations to intelligence and crime analysis to commercial procurement. Therefore its people are having different backgrounds and cultures with different experiences and skills. They even speak various languages. That diversification is acting as an added value to carry on their tasks.

According to the section 17 (4) in Computer Crime Act, an expert is called upon to assist any police officer who may not have competency level and technical knowledge needed for the investigation. Computer crime investigation is a different field which

includes collecting and handling of volatile and sensitive digital data. The experts have better understanding to deal with those scenarios. But most of the Police officers do not possess that knowledge. Therefore, it does not make much sense to assign experts for investigation tasks under the supervision of police officer especially during the forensic investigation period. But when it comes to UK and EU the responsibility of conducting the investigation has been handed over to specific knowledgeable investigators in related agencies. Based on the request of such agency, they have given the power to call for the assist from Police to proceed with the investigation work. According to Nikolić (2020), the director general of the National Cyber Crime Unit (NCCU) authority, has been given the powers when needed to make any order to any police chief in UK for assisting the agency to proceed with its investigation work.

In most of the cases, the resource and knowledge gap between Police officers and experts act as a highlighted barrier when performing investigations under this act. The existing Computer Crime Act is not presenting any mechanism or procedure to address that, through an appointed regulatory entity. But when it comes to UK and EU they have addressed them. The UK has recognized the need for a public-private partnership in combating the cybercrimes because majority of the Police officers are lack of expertise in conducting the investigations in cyberspace. Also the limited capacity and resources have emerged as one of the biggest hole when it comes to public organizations which work in investigation for combatting cybercrime. But it has increased the amount of private companies that provide security in cyberspace with the necessary skills and resources available within them. By considering the opportunities which can be gained through a public private collaboration, the UK has taken an important step. The National Cyber Security Centre has been established by using the collaboration between government agencies and private sector to provide protection from cybercrime threats. Not only UK but EU also has taken necessary steps towards it. With the introduction of EU Cyber security Act that forces since 2019, ENISA was redesigned and given a permanent mandate for contributing the EU cyber security. Through that, EU is indicating the commitment to maintain the public-private partnership in preventing and combatting against cybercrime (Akdemir et al., 2020).

Under section 18 (1), Computer Crime Act specifies the ability of an expert or a Police officer to obtain relevant information and traffic data possess by service providers. Generally service providers have their own privacy policies to be adhered to and followed in such situations. Therefore when try to collect information from them practical limitations can be experienced by officers. The current Act does not address this situation (X). When considering EU, they have provided provisions to improve corporation between law enforcement bodies, service providers and judicial authorities in preserving evidence and helping to identify offenders by understanding its importance. Also some of the EU Member States have established their legislations in

such a way that the ISPs keep their data, in case those data should be provided to the law enforcement entities to carryout investigation work conveniently. Therefore, other than the billing data and commercial data all the transactional related data are kept to effectively seek any criminal activity (Directive 2013/40/EU).

Computer Crime Act Section 18 (4) defines the ability of Minister in Charge of Science and Technology to prescribe the procedures to be followed regarding the retention and interception of data on behalf of any investigation. Also under section 32 (1), it states that the Minister has the ability to make regulations under this act when needed in order to carry out principles and provisions of the act. When considering the current Sri Lankan society, here it has ignored the fact about the competency level and the skill of the minister with regard to the knowledge he or she has on the subject matter.

According to the section 19 (1) in Computer Crime Act, if the expert or the police officer thinks that there is any risk of losing information related to the investigation, the corresponding person who possesses the evidence should be notified to safeguard them for a period of seven days through a written notice. This becomes a very impractical approach since it has ignored the volatility of the data reside inside any computer or any other related system. It is not recommended to wait for hours or days to get data in such scenario and the standard practice to preserve data is obtaining backups as soon as possible. Moreover there are issues related to the trustworthiness of the other party who actually possess the data. Also this cannot be applied when the computer or computer system is under the control of a hacker or if it is outside of the country.

Section 22 (1) of Computer Crime Act states that the police officer should issue a complete list of seized or non-accessible items, if there is any, to the owner of the computer system during the investigation. This provision cannot be applied when the system or part of it exists outside of SL.

According to section 25, jurisdiction to hear offences under Computer Crime Act is High court. Also it states that only the High court at Colombo has the exclusive jurisdiction under this act even though there are several high courts within the country. This becomes impractical in some situations since the relevant parties have to wait longer time until the case is executed with only one high court being available to hear offences (X).

In section 35 (1) it explains how the provisions of Mutual Assistance in Criminal Matters Act No. 25 of 2002 are applied for a case coming under Computer Crime Act. For a computer crime investigation that requires international level involvement, it is essential to take necessary actions to share electronic data immediately in between the relevant parties. But the existing Act does not provide sufficient provisions on that, at least by considering the volatility of digital data (Perera & Mahanamahewa, 2017).

But UK and EU have developed necessary legal background on that basis. In order to tackle cross broader crimes, improving the ways in which the information can be exchanged plus the international corporations play vital roles. The Crime Overseas Production Orders Act 2019 (COPOA) has been enacted by UK to address the above necessity through facilitating immediate sharing of electronic data between UK's law enforcement entities and the countries which the UK has arrangement corporations in international level. COPOA provides ways to overcome unnecessary delays experienced in mutual legal assistance processes (Michael, 2021).

According to Calderoni (2010) in EU, the two legal instruments, Council of Europe Convention on Cybercrime and European Union Framework Decision, provide solutions to address and combat computer related crimes in international level. It introduces novel way and tools that help investigating such crimes and then open paths to harmonize the national definitions related to various computer related crimes. As a result of that, it enables improvement of International Corporation regarding criminal matters.

As mentioned by X and Z, the current Computer Crime Act does not provide definitions on some modern cybercrimes including cloud related crimes and some social media related things. Therefore the judicial system is not yet ready to conduct investigations on those areas. But when it comes to EU, they have implemented necessary laws and policies to compliance with their data and digital strategies (European Commission, 2022).

The existing Sri Lankan legislation states that the intention is sufficient to commit an offense. But it does not consist of valid procedures to prove the intention. But when considering the EU laws they are using methods like "evidence audience" (Ekanayake, 2019).

According to the data analysis and discussion, it is indicated that some gaps exist in current computer crime investigation process stated in CCA when comparing it with EU and UK laws which provide better provisions to handle crimes related to cyber space. Even though the Act has provided better definitions on computer crimes, it is missing some major provisions needed to address computer crime investigation process.

4.6. Chapter Summary

This chapter focused on how to achieve the research objectives developed in earlier chapters of the study. Data Analysis and discussion was completed by using the primary and secondary data gathered as a combination of interviews and library research method. Also the study was conducted as a comparative analysis with EU and UK laws.

Next chapter will be focusing on the findings and recommendations which could be extracted based on the points discussed in this chapter.

5 FINDINGS AND RECOMMENDATIONS

5.1. Chapter Introduction

The analysis and discussion was described in the last chapter to assert the stated objectives of the study. It was able to successfully analyze the objectives while reaching out for commenting on the initially selected assumption. This chapter depicts inferences considering the assumption while pointing out findings and recommendations hand in hand.

5.2. Identified insufficiency in existing laws and Recommendations

As mentioned in the dissuasion and analysis chapter, even though there are plus points in the Computer Crime Act due to the way it has been drafted, it still requires further updates with the time being. Below facts have been extracted based on the study carried out using interviews and library research method. Further following points focus on identified insufficiency in existing laws and hence provide respective recommendations hand in hand.

For fulfilling the existing gaps in the current legal framework this study is suggesting to have a collaboration between law enforcement entities, investigators and judicial authorities when implementing necessary laws. Further, it emphasizes on ensuring the reliability and legality of any appointed regulatory bodies as discussed below.

I. Implementing provisions to make forensic ready systems

As per the discussions had, one important point was highlighted by forensic investigators (Category Y). When considering an organization that might have the ability to get affected from computer crimes, it is necessary to make its systems forensic ready so that it provides a better and feasible background for conducting proper investigations when needed. In order to address the needful, certain things should be fulfilled by the IT services and infrastructure of the organization including following,

- Maintaining proper tamperproof logs
- Enabling audit trails and specific security logs
- Having proper account assignment process

- Following certain standard practices like ISO 27001

To achieve that, an organization can implement certain policies to ensure that all the computer systems are forensic ready and they comply with standard practices specified by the IT services and Infrastructure of the organization. While necessary provisions should be added to the Computer Crime Act so that the Act should force to setup necessary infrastructure. Then all the organizations will adhere to that law when following the standards to comply with.

II. The appointment of investigators & their qualification level

As implied through data analysis and discussion (section 4.5) there is an issue in the existing Computer Crime Act in relation to the appointment of investigators & their qualification level. The act is providing only a broader range of qualifications to be appointed as an expert. By considering EU and UK legal systems, if the Act can point out to a separate regulatory body from where all the appointment of investigators are carried out by setting out more specific and in detail description for each investigative position, that will work well. But, in order to reach out to that point also an amendment should be added to the existing Act for addressing any missing segment related to the qualification levels especially by including a mandatory training period under the supervision of a charted engineer. Also this can be regulate through standards as the qualifications are going to be depend on standardization (Y). In that way it is able to present an updated set of qualifications rather than trying to add amendments for every time a modification is required for any appointment. Then the qualifications specified in the Act can be used as the higher level while the responsible regulatory body can be used to publish in detail description of each position along with required qualification levels. Also as Y suggested, there should be an accepted organization or an institute which provides trainings and is responsible for the qualification levels of professionals within computer crime investigation process.

III. Having knowledgeable first responders at the crime scene

As stated in section 4.4.1, currently SL Police acts as the first responders for computer related crimes. But most of the police officers do not possess basic knowledge on computer crimes or handling data related to such cases. But it should be mandatory for the SL Police to gain basic knowledge on how to capture evidence without crashing them as in some cases they have to acquire and handle evidence themselves without the help of experts. In order to facilitate that knowledge, it is suggesting to appoint police officers who comes with an IT background for investigating computer crimes or else

need to provide better trainings in practical manner so that some certification will be offered for the trained Police officers to add an additional value to their profiles to be highlighted as officers dedicated for Computer Crime Investigation. In EU and UK this is different since starting from the very beginning the investigation work is handled by appointed investigators by calling the police for any assistance when needed.

IV. An expert being called upon to assist the police officer

As mentioned in section 4.5, since the process carried out for a computer crime investigation, differ from other traditional investigations it is mandatory to get help from an expert. It is true that due to the safety issues an expert may not be able to present in almost all the crime scenario to extract evidence. Only the police officers have the ability to do so. But after extracting the evidence, only the experts have the ability to proceed with further investigations. That process is anyway needs to be supervised under those experts since the SL Police do not have knowledgeable resources. Therefore, mainly during the forensic investigation period, the Act should grant necessary powers on experts. Not the other way around where the experts should be guided according to the orders of the Police. In that way based on the requirement, they will be able to make orders to police officers in getting necessary assistance for investigation work.

V. Implementing necessary public-private partnership

According to the study it is indicated that most of the public organizations including SL Police are struggling to perform proper investigations due to various drawbacks (refer section 4). Lack of resources and skills is the major barrier. Meanwhile private organizations are successfully operating security in cyberspace as they possess a rich level of capacity and skills to handle such scenario. Therefore through a public-private partnership, multiple positive impacts can be achieved for combating cybercrime by following similar ways which UK and EU have already adopted (as stated in section 4.5). Therefore, to manage any gap between public and private sectors when performing computer crime investigation tasks, it is suggesting to implement necessary public private partnership.

VI. Improving corporation between law enforcement bodies, ISPs & Judicial authorities

The current Computer Crime Act has granted powers for the experts and SL Police officers to obtain necessary information from ISPs. But it does not include a specific provision that implement corporation between law enforcement entities and ISPs. As a result of that when collecting information or evidence, officers experience some practical limitations as the ISPs have their own policies to follow. As mentioned in section 4.5, in EU and UK, necessary corporations between each entity have been implemented by law in such a way that they minimize such practical limitations. By incorporating similar kind of laws, SL can also improve the corporation between law enforcement authorities, ISPs and judicial authorities. Also it is recommending to develop laws to ensure that ISPs are storing necessary transactional/background and application level data for a considered period of time to be used in any investigation work conveniently.

VII. Appointing a minister who has necessary competency level on the subject

As mentioned in section 4.5, the Minister in charge of Science and Technology has given the authority in defining procedures related to the retention and interception of data needed for any investigation. Also the Act has allocated powers for the Minister in making relevant regulations for facilitating provisions coming under this Act. But the Act has ignored the fact about the knowledge and the competency level of the Minister since in SL when appointing Ministers it is not considering their knowledge level or experiences related to the subject. Therefore this study is suggesting to appoint said Ministers from those who are coming from an IT background with relevant skills and experiences. Else, the powers to make relevant regulations should be granted to a responsible party like a regulatory entity which consists of necessary resources and skills.

VIII. Need of revisiting some sections in Computer Crimes Act

Based on the points discussed in section 4.5, the study has identified following areas which require further revisions.

As mentioned in section 19(1) of Computer Crime Act, it is impractical to make a written notice to the person who possesses the evidence to protect them for a period of seven days. As discussed in the previous chapter due to the volatility of digital data the standard practice is obtaining backups as soon as possible without waiting for hours and days. Also there is a question related to the trustworthiness of the party who possess the

data. Moreover, this section cannot be applied to computer crimes when the computer is under the control of a hacker or it locates outside of the country. Therefore this section should be re-visited so that it will include separate provisions to handle above mentioned situations. Therefore it is suggesting to provide a specific sub section regarding the protection of data when the corresponding computer system is under the control of a hacker or if it resides outside SL. Also it should update the way of making the request since now there are multiple options to make an immediate and reliable notification.

According to the study, section 22 (1) becomes impractical when the computer system or the part of it exists outside SL. In such scenarios the police officer is not capable of issuing a list of seized or non-accessible items that are relating to any investigation work. Therefore this research is proposing to re-visit the section while another sub section should be included to handle the situation when the system resides out of the country.

By having only one High court that is available to hear cases coming under Computer Crime Act, the related parties have to wait longer until the case is executed. According to multiple researches this becomes impractical. Therefore it is recommended to provide necessary resources and background factors so that other high courts would be capable of hearing cases coming under this Act. On that note, this study is recommending to re-visit section 25.

IX. Provisions for mutual assistance in Criminal Matters Act

Section 35 (1) in CCA specifies how the provisions of Mutual Assistance in Criminal Matters Act are going to be applied to a computer crime along with the conditions and terms in various conventions. But it has omitted the fact of digital data being volatile and hence the relevant international corporation should be implemented for immediate share of those data. Therefore necessary sections should be added to the respective Acts to facilitate immediate share of digital data between international parties. To achieve that, necessary examples can be extracted from EU and UK legal system as mentioned in the previous chapter (refer section 4.5). Further the existing Act should force entities to setup necessary infrastructure to support required international collaborative activities.

X. Provisions for addressing crimes related to cloud services and social media

As indicated through multiple discussions (refer 4.4 & 4.5 sections), current Computer Crime Act is not providing clear definitions and procedures that address investigation process on cloud related or social media related crimes. But in current society, most of the systems are now relying on cloud services. Therefore it is mandatory to implement laws regarding those areas. This study is suggesting to take necessary example provisions from EU and UK as mentioned in the previous chapter (refer section 4.5) when developing laws for investigating crimes associated with cloud services or social media.

XI. Implementing proper standards for conducting computer forensic

As Z and Y mentioned (refer section 4.3 & 4.4.2), the specifications and the way the computer forensic process is conducted differ based on the type of the investigator and the organization, due to the unavailability of proper standards specified to follow in that stage. Therefore it is necessary to establish a general standardization that all the computer crime investigators and such investigation organizations can adhere to when conducting computer crime investigation within SL. This study recommends implementing the standardization as required associated with a responsible regulatory body so that the Act can then point to that particular entity.

XII. Educating lawyers and judges regarding necessary technical related areas while sharing law related knowledge for (technical) investigators

As per Y and Z, it is a highlighted fact that the lawyers and judges do not possess technical knowledge regarding Computer Crime Investigation process and hence it leads to some issues when providing interpretations to the digital evidence and executing some court cases (refer section 4.4.3). Since the final decision is taken by the judges and lawyers, it is important that they possess sufficient knowledge on these aspects. As Y mentioned, even though they have started to conduct technical sessions for law related people, that has not continued in a proper manner. Therefore this study recommends conducting those types of sessions in a more practical manner so that they get the necessary technical knowledge.

Also according to Y and Z, when considering (technical) investigators, they also have very less knowledge on law areas related to the Computer Crime Investigation. Since they are involved in this process it becomes essential to gain that knowledge because then only they can contribute productively and meaningfully for producing the legally

admissible evidence to the court. Therefore this research suggests to conduct law related sessions for respective technical investigators as required. Also it recommends to establish certain certification levels so that it will add an additional value to the profile of the investigators.

XIII. Developing necessary legal facilities for the technical investigators to provide expert witness in a convenient manner when their report is being challenged in the court

As Y and Z mentioned, the existing legal system does not facilitate necessary legal background for the IT experts to provide expert evidence separately instead of presenting them publicly which then leads to reveal their identities and risk their lives (refer section 4.4.2). Therefore this study suggests to implement necessary legal background so that these type of investigators have the ability to go to the court separately and meet the judges and lawyers directly to provide the expert witness without providing them publicly.

The initial assumption made in chapter three was that "the existing legal framework for conducting computer crime investigations in SL is not sufficient to handle them in a proper manner". Based on these findings, now it has the ability to comment on the assumption. Therefore after considering the analysis and the findings this research study accepts the above stated assumption.

5.3. Chapter Summary

This chapter focused on rendering the findings based on the data analysis done while providing proposed recommendations hand in hand. Also based on the findings it has commented on the initial assumption made earlier and ensured that the study proceed with that. The next chapter will draw the concluding remarks of this study.

6 CONCLUSION

6.1. Chapter Introduction

Previous chapter elaborated the key findings of the research along with the recommendations. This chapter presents concluding remarks of the study while highlighting important implications with regard to the current Computer Crime Investigation process in SL. In addition, this chapter depicts the limitations of the study by pointing out the proposed opportunities for future research.

6.2. Implications and their significance

As a result of the development in the field of Information Technology, it opens up novel opportunities to commit crimes easily using computer related systems. Computer Crime Investigation process is the procedural and systematic way to identify such crimes along with related criminals. Any difficulty in conducting valid investigations would be an encouragement for the criminals to commit more crimes. The three types of investigators used for conducting interviews in this study are the ones who are currently dealing with computer crimes investigation process in SL. Therefore they experience any burning challenges within the process. Even though the challenges fall into different categories they are interconnected with each other. Therefore the purpose of this study was to find out those areas and investigate whether the existing legal system is capable of providing solutions for them to conduct proper investigations on computer related crimes. Meanwhile the research identified areas that require further revisions especially with regard to the Computer Crime Act and hence provided recommendations on how to address them.

Through the interviews it was able to find out some unique facts that have not been stated in previous researches. Hence it was able to add significant findings to this study.

According to the findings the existing laws pertaining to the computer crimes investigation in SL is not sufficient to proceed with a successful investigation. The main loophole is that the necessary provisions not being updated in timely manner to address important aspects.

According to the key findings there are mandate provisions to be updated in the Computer Crime Act to ensure an efficient computer crime investigation process. Hence this study suggests making amendments as necessary to address them. It is impractical

to make legal changes within an existing Act, as fast as the changes take place in the field of technology. Therefore, as a remedy for that, based on the key findings, this study suggests amending only the necessary provisions to the existing Act as stated in the previous chapter. Meanwhile this proposes to implement needed policies through appointed regulatory bodies to which the Computer Crime Act can then point in order to ensure smooth operation of investigation process. Through that, this study is recommending a significant way to make the computer crime investigation more efficient and effective. Also this emphasizes on the importance of having a corporation between law enforcement entities, investigators and judicial authorities when implementing necessary laws and policies including the appointment of aforementioned regulatory entities.

6.3. Opportunities for Future Research

The scope of this study included focusing on the investigation process stated in the Computer Crimes Act No 24 of 2007. In future research, interesting follow up studies could expand their scope to identify the sufficiency level of existing laws in SL for computer crimes as a whole instead of focusing on the investigation process.

This study consisted of a comparison between the computer crime investigation process in SL with UK and EU laws in same context. A comparative analysis facilitates proper identification regarding sufficiency level of existing legal system in combatting computer related crimes. Therefore the legal systems which are complying with the existing laws in SL were given prioritized when selecting them for the comparison. The future studies could be extended by adding more legal systems into the comparison so that it would render more comprehensive research results which helps to draw better recommendations for existing gaps.

Also the data collection in this qualitative study was limited to reviewing and analyzing of primary & secondary data extracted from the combination of interviews and library research method. Based on the resources used for the interviews in this study any interested party can continue this research further by including not only the investigators but also officers from law enforcement and judicial authorities who are responsible in drafting and executing laws related to computer crime investigations.

Bibliography

Acts and Directives

Sri Lanka

Computer Crime Act No 24 of 2007

UK

Computer Misuse Act 1990

EU

Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union (**2000/C 197/01**)

Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision **2005/222/JHA**

Regulation (EU) 2018/1727 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for Criminal Justice Cooperation (Eurojust), and replacing and repealing Council Decision **2002/187/JHA**

Books

Brown, M. F. (2001). *Criminal investigation: Law and practice*. Butterworth-Heinemann.

Casey, E. (Ed.). (2001). *Handbook of computer crime investigation: forensic tools and technology*. Elsevier.

Clarke, N. (2010). Computer Forensics. *New york: IT Governance Ltd*.

McConville, M., & Chui, W. H. (Eds.). (2017). *Research methods for law* (Second edition). Edinburgh University Press.

Journal Articles

Abeysekara, T. B., & Elkaduwa, S. (2015). A Game of Thrones: Law V Technology: A Critical Study on the Computer Crimes Legislation in Sri Lanka. Second International Conference on Interdisciplinary Legal Studies 2015, Sri Lanka

Abeysekara, T. B., & Ranasinghe, A. E. (2022). Holistic Approach in Introducing Proper Legal Framework to Regulate Data Protection and Privacy in Sri Lanka. Vidyodaya Journal of Management, 8(I).

AKDEMİR, N., SUNGUR, B., & BAŞARANEL, B. U. (2020). Examining the challenges of policing economic cybercrime in the UK. Güvenlik Bilimleri Dergisi, (International Security Congress Special Issue), 113-134.

Allen, W. H. (2005). Computer forensics. *IEEE security & privacy*, *3*(4), 59-62.

Ariyadasa, A. (2019a). Computer Crime Legislation in Sri Lanka: Comparative Analysis. *Available at SSRN 3382666*.

Ariyadasa, A. (2019b). Harassment Beyond Borders: Sexting, Cyber Bullying and Cyber Stalking in Social Media. Can Sri Lanka Protect Victims?. *Can Sri Lanka Protect Victims*.

Azad, M. M., Mazid, K. N., & Sharmin, S. S. (2017). Cyber crime problem areas, legal areas and the cyber crime law. *International Journal of New Technology and Research*, *3*(5), 1-6.

Calderoni, F. (2010). The European legal framework on cybercrime: striving for an effective implementation. Crime, law and social change, 54(5), 339-357.

De Hert, P., Fuster, G. G., & Koops, B. J. (2006). Fighting cybercrime in the two Europes. *Revue internationale de droit penál*, *77*(3), 503-524. – Book/Report

Ekanayake, I. (2019). Are the Sri Lankan Cyber-Crime Laws Sufficient to Safeguard IT Professionals and the Victims of Cyber-Attacks in Sri Lanka?. *Available at SSRN 3379904*.

Elkaduwa,S., Abeysekara,T.B. (2015). A Game of Thrones: Law V Technology: A Critical Study on the Computer Crimes Legislation in Sri Lanka. Second International Conference on Interdisciplinary Legal Studies 2015, Sri Lanka

Fernando, E. D. S. (2019). Are the Sri Lankan Cyber Laws Sufficient to Safe Guard the IT Professionals and Victims of Cyber Attacks. *Available at SSRN 3743590*.

Gawas, V. M. (2017). Doctrinal legal research method a guiding principle in reforming the law and legal system towards the research development.

Guinchard, A. (2007). Criminal Law in the 21st Century: The Demise of Territoriality?. *Available at SSRN 1290049*.

Harbawi, M., & Varol, A. (2016, April). The role of digital forensics in combating cybercrimes. In *2016 4th International Symposium on Digital Forensic and Security (ISDFS)* (pp. 138-142). IEEE.

Hinduja, S. (2007). Computer crime investigations in the United States: leveraging knowledge from the past to address the future. *International Journal of Cyber Criminology*, *1*(1), 1-26.

Indrakumara, M., & Fernando, L. (2022). Stalking and Cyber Stalking: A Comparative Analysis of the Legislative Responses in Sri Lanka, Canada, the United Kingdom and Australia.

Iroshan, A. (2019). Sufficiency of Sri Lankan Cyber Crime Laws to Safeguard the IT Professionals and Victims of Cyber Attacks. *Available at SSRN 3514806*.

Janaha, S. (2013). Has Sri Lanka worked out effective ways of fighting computer crime?-An analysis in respect of investigations under the Computer Crime Act of 2007.

Jayasekara, D. (2015). Internet and law (special reference to Sri Lanka). The Social Sciences, 10(6), 841-844.

Kharel, A. (2018). Doctrinal legal research. Available at SSRN 3130525.

Kulathunga, A. (2019). A Comparative Study on Sri Lankan v. European Cybercrime Law in Protecting IT Professionals and Victims of Cyber-attacks. *European Cybercrime Law in Protecting IT Professionals and Victims of Cyber-attacks (January 8, 2019)*.

Laksiri Geethal, K. G., De Zoysa, K., Thilakarathna, K., Wijesekera, P., & Keppitiyagama, C. (2020). Challenges in investigating Cybercrime in social networks: A Sri Lankan Perspective.

McKemmish, R. (1999). What is forensic computing? (pp. 1-6). Canberra: Australian Institute of Criminology.

Mshana, J. A. (2015). Cybercrime: An Empirical Study of its Impact in the Society-A Case Study of Tanzania. Huria: Journal of the Open University of Tanzania, 19(1), 72-87.

Noblett, M. G., Pollitt, M. M., & Presley, L. A. (2000). Recovering and examining computer forensic evidence. *Forensic Science Communications*, *2*(4).

Pandey, A. K., Tripathi, A. K., Kapil, G., Singh, V., Khan, M. W., Agrawal, A., ... & Khan, R. A. (2020). Current Challenges of Digital Forensics in Cyber Security. *Critical Concepts, Standards, and Techniques in Cyber Forensics*, 31-46.

Perera, P., & Mahanamahewa, P. (2017). Analysis of Dependencies & Legal Barriers on Digital Forensic Investigations in Sri Lanka.

Radu, S. (2020). The Concept of Computer Crime. EIRP Proceedings, 15(1).

Samarakoon, A. S. (n.d.). Law Relating To Computer Crimes; Is it Equal in Sri Lanka and United Kingdom?9.

Sarrab, M., Aldabbas, H., & Elbasir, M. (2013). Challenges of Computer Crime Investigation In North Africa's Countries. In *The International Arab Conference on Information Technology (AaCIT'2013)*.

Tharindu, S. (2020). Sufficiency of Sri Lankan Cyber Crime Law 'Critically Analysis of the Legal Frame Work Applicable to the IT Industry Comparing With European Union Law'. *Available at SSRN 3522038*.

Wickramasinghe, S., & Hettiarachchi, S. (2016). Use of Computer Forensics and Its Implications.

Reports

Annual Activity Report 2020 Sri Lanka CERT|CC, The National CERT of Sri Lanka.

Fernando, J. (2010). "e-Enabling legislation" A catalyst for ICT based banking and financial sector growth in Sri Lanka. *Sri Lanka ICT Agency, Colombo*.

Nikolić, G. (2020). NATIONAL CRIME AGENCY-NCA. International Journal of Economics & Law, 10(30), 17-30.

Web Sources

Borges, E., (2020). Cyber Crime Investigation Tools and Techniques Explained. Retrieved June 24, 2021, from https://securitytrails.com/blog/cyber-crime-investigation

Cybercrime. European Commission website. Retrieved August 02, 2021, from https://ec.europa.eu/home-affairs/what-we-do/cybercrime_en

De Alwis, W.C.(2017). An Introduction To Challenges In Digital Forensics. Retrieved June 28, 2021, from https://www.forensicfocus.com/articles/an-introduction-to-challenges-in-digital-forensics/

European Commission. (2022, February 24). Cloud Computing. Shaping Europe's digital future. (2022). Retrieved from May 15, 2022 from https://digital-strategy.ec.europa.eu/en/policies/cloud-computing

EUROPOL. (2022). Careers & Procurement. Retrieved May 13, 2022, from https://www.europol.europa.eu/careers-procurement/open-vacancies/vacancy/584

Michael, D., & Julian, H. (2021). Investigations in England and Wales: A Practitioners' Perspective. Retrieved May 06, 2022, from https://globalinvestigationsreview.com/guide/the-guide-cyber-investigations/second-edition/article/investigations-in-england-and-wales-practitioners-perspective

nationalcrimeagency.gov.uk. (2022). National Crime Agency. Retrieved May 14, 2022 from https://nationalcrimeagency.gov.uk/

Nemanja Jovancic. (2021). 5 Data Collection Methods for Obtaining Quantitative and Qualitative Data. Retrieved December 21, 2021, from https://www.leadquizzes.com/blog/data-collection-methods/

P. Gill, K. Stewart, E. Treasure & B. Chadwick. (2008). Methods of data collection in qualitative research: interviews and focus groups. Retrieved December 21, 2021, from https://www.nature.com/articles/bdj.2008.192

Introduction to Law: Primary and Secondary Sources. (n.d.). Retrieved December 22, 2021, from https://library.highline.edu/c.php?g=344547&p=2320319

What are the different primary and secondary sources of Law UK research?. (2020). Retrieved December 21, 2021, from https://www.phdassistance.com/blog/what-are-the-different-primary-and-secondary-sources-of-law-uk-research/

APPENDIX A: INTERVIEW QUESTIONS

Objective to address	**Question**
Objective 1	How would you engage with existing Computer Crime Investigation Process in Sri Lanka? What is the role you play within the Investigation Process?
Objective 1	In relation to your role (overall as an investigator), how do you see the importance of carrying out a proper investigation on computer crimes within the current Sri Lankan society?
Objective 1	What are the main steps carried out in existing Computer Crime Investigation Process in Sri Lanka?
Objective 3	What are the practical challenges faced when performing each step (in relation to your role)?
Objective 2	What is the role of computer forensics in Computer Crime Investigation Process?
Objective 3	What are the challenges faced when using various tools in data capturing and forensic analysis (in relation to your role)?
General Question	How do you see the importance of computer evidence/digital evidence to proceed with a court case that is related to any computer crime?
General Question	As per your point of view, what are the actions that should be taken for proving the legal admissibility of computer related evidence?
Objective 4	Do you have any knowledge related to the laws specified for Computer related crime investigations in EU and UK?
Objective 4	Is the existing law for Computer Crime Investigation Process stated in Computer Crime Act No 24 of 2017 and Criminal Procedure Act, sufficient to perform a proper investigation in current Sri Lankan society? OR else Do you identify any loopholes to update the areas with regard to the existing legal framework for Computer Crime Investigation Process in Sri Lanka, compared to the laws in EU and UK?
Objective 4	If so, what are the loopholes identified in order to update the areas in computer crime investigation within Sri Lankan legal framework, compared to the laws in EU and UK?

APPENDIX B: RESEARCH METHODOLOGY DIAGRAM