DIGITAL FORENSIC AUTOMATION MODEL

FOR ONLINE SOCIAL NETWORKS

HUMAIRA ARSHAD

UNIVERSITI SAINS MALAYSIA

2019

DIGITAL FORENSIC AUTOMATION MODEL

FOR ONLINE SOCIAL NETWORKS

by

HUMAIRA ARSHAD

Thesis submitted in fulfillment of the requirements
for the degree of
Doctor of Philosophy

September 2019

ACKNOWLEDGEMENT

All praise and gratitude be to Allah, the most merciful and the most beneficent.

I could not have imagined having to do my work without the blessings of Allah Subhanahu Wa Ta'ala. I am incredibly grateful to Allah for giving me the energy and an opportunity to finish my work.

I must express my genuine thanks to my supervisor Dr. Aman Jantan, for his constant support of my Ph.D. study and related research, for his motivation, patience, and vast knowledge. His supervision has continuously helped me during the research and writing of this thesis.

My sincere thanks also go to Dr.Gan Keng Hoon for her encouragement and insightful comments, but also for the tough questions that motivated me to broaden my research from various perspectives.

At the same time, I like to acknowledge my fellow doctoral students for their feedback, cooperation, and of course friendship. I thank them for the stimulating discussions, and for all the fun we have had in recent years.

Last but most importantly, I would like to give my gratitude to my family; my husband Muhammad Ashfaq and my kids Eshaal Ashfaq and Muhammad Mahd, who always supported me during my studies and are a constant source of happiness and motivation. I am in great debt to my loving parents who always make supplications to Allah for me. I am also thankful to my brothers, who have always supported me during my study and my life in general.

TABLE OF CONTENTS

LIST OF TABLES

Page

LIST OF FIGURES

Page

LIST OF EQUATIONS

Page

LIST OF ABBREVIATIONS

API	Application programming interface
CSV	Comma-separated values
DIALOG	Digital Investigation Ontology
EFIOSN	Event-based Forensic Integration Ontology for Online Social
FIG	Frequency of Interaction Graph
FIMOSN	Forensic Investigation Model for Online Social Networks
HTC	Hashtag cloud
HTML	Hypertext Markup Language
HTTP	HyperText Transfer Protocol
IEF	Internet Evidence Finder
IEZ	Information Extraction Zone
IG	Interaction Graph
IoT	Internet of Things
IZ	Incident Zone
JSON	JavaScript Object Notation
MD5	Message-digest algorithm 5
MHT	MIME encapsulation of aggregate HTML documents
OSN	Online Social Network

OWL	Web Ontology Language
PDF	Portable Document Format
PIEZ	Primary information extraction zone
PNG	Portable Network Graphics
RDF	Resource Description Framework
RDFS	RDF Schema
SG	Social Graph
SIEZ	Secondary information extraction zone
SIOC	Semantically Interlinked Online Communities
SM	Social Media
SN	Social Network
SPARQL	Semantic query language for RDF
TAG	Temporal Activity Graph
TDB	Trivial database
UTC	Coordinated Universal Time
W3C	World Wide Web Consortium
WARC	Web ARChive archive
XML	Extensible Markup Language
xsd	XML Schema Definition

LIST OF SYMBOLS

!	NOT, logical negation
$\|O_e\|$	Number of Objects
$\|S_e\|$	Number of Subjects
~	Roughly similar
×	Cross product
∀	For all , For each
∃	There exists , existential quantification
∈	Is an element of
∑	Summation
∧	logical AND
∪	Union
≡	Numerical equality
≤	Less or equal to
⊆	is a subset of
⊢	is derived from
Ec'	The set of events that are not correlated
Ec	The set of correlated events
Ei	The set of all events that are related to the incident
Ei'	The set of all events that are not related to the incident
E_p	Primary Event
fn	Interaction rate, Number of interactions
O	Object
S	Subject

T	Time
α	Is related to
σ	Relation
∨	Logical OR

LIST OF APPENDICES

MODEL AUTOMASI FORENSIK DIGITAL UNTUK RANGKAIAN SOSIAL DALAM TALIAN

ABSTRAK

Pada masa ini, agensi penguatkuasa undang-undang dan pengamal undang-undang kerap menggunakan rangkaian sosial untuk mengakses maklumat yang berkaitan dengan para peserta sebarang insiden haram. Walau bagaimanapun, proses forensik secara teknikalnya rumit kerana rangkaian sosial dalam talian yang heterogen dan tidak berstruktur dan mencabar secara undang-undang. Oleh itu, mencipta cabaran kognitif dan beban kerja yang besar untuk penyiasat. Oleh itu, adalah penting untuk membangunkan penyelesaian automatik dan boleh dipercayai untuk membantu penyiasat. Walaupun, automasi bukan merupakan masalah teknikal sepenuhnya dalam forensik digital. Keperluan undang-undang selalu menuntut teori yang dijelaskan untuk kesimpulan yang dihasilkan oleh kaedah automatik. Kerja ini memperkenalkan model automasi; yang menangani isu-isu automasi daripada pengumpulan kepada analisis keterangan dalam forensik rangkaian sosial dalam talian. Kajian ini mula-mula menggambarkan model pengetahuan formal untuk menerangkan proses forensik untuk rangkaian sosial. Model pengetahuan ini diformulasikan untuk menerangkan hasil yang diperolehi oleh analisis automatik. Kedua, ia menjelaskan model penyiasatan forensik yang khusus menangani isu penyiasatan automatik pada rangkaian sosial dalam talian. Model ini mencadangkan satu proses penyiasatan untuk menjalankan siasatan forensik separa automatik pada rangkaian sosial dalam talian. Komponen ketiga pendekatan ini adalah model ontologi hibrid yang melibatkan pelbagai ontologi untuk menguruskan data yang tidak tersusun ke dalam koleksi teratur. Akhirnya, kerja ini mencadangkan satu set operator analisis yang berada di korelasi domain.

Pengendali ini boleh dibenamkan dalam alat perisian. Pengendali ini diuji dengan menggunakan ontologi Twitter dalam kajian kes. Kajian ini menggambarkan pendekatan konsep-konsep untuk automasi forensik pada rangkaian sosial dalam talian.

DIGITAL FORENSIC AUTOMATION MODEL FOR ONLINE SOCIAL NETWORKS

ABSTRACT

Presently, law enforcement agencies and legal practitioners frequently utilize social networks to quickly access the information related to the participants of any illicit incident. However, the forensic process is technically intricate due to heterogeneous and unstructured online social networks and legally challenging. Hence, creating intellectual challenges and enormous workloads for the investigators. Therefore, it is critical to developing automated and reliable solutions to assist investigators. Though automation is not an entirely technical issue in digital forensics. Legal requirements always demand an explainable theory for the conclusions generated by automated methods. This work introduces an automation model; that addresses the automation issues from collection to evidence analysis in online social network forensics. This study first describes a formal knowledge model to explain the forensic process for the social network. This knowledge model is formulated to explain the results obtained by an automated analysis. Second, it explained a forensic investigation model that specifically addresses the issue of automated investigations on online social networks. This model suggested an investigation process to carry out a semi-automated forensic investigation on online social networks. The third component of this approach is a hybrid ontology model that involves multiple ontologies to manage the unstructured data into an organized collection. Finally, this work proposed a set of analysis operators that are on domain correlations. These operators can be embedded in software tools. These operators are tested by using

Twitter ontology on a case study. This study has described a proof-concept approach for forensic automation on online social networks.

CHAPTER 1
INTRODUCTION

1.1 General Overview

Social media forensics is a new frontier in digital forensics. Social media is an endless source of information about potential suspects, victims, and witnesses. Social network sources are now commonly used by law enforcement agencies to reveal the details of a crime. The social media profile of a suspect or victim, their friend lists, photos of their activities and communications can help to uncover the details of the specific event and give an insight to the investigator about the personality and way of life of individuals. Defense attorneys also use social media evidence to defend their clients in courts. A criminal defendant's lawyer can use social media to gain knowledge through the public profile of the victim, their friends or family, and to find any excuse or to catch the plaintiff or witness in a lie. However, law enforcement officers can access even to private information on social media profiles through warrant and subpoena, and they often do that, but lawyers are limited to access only public data on social media. Court order can also compel social media sites such as Facebook or Twitter to provide private data about the specific user. Social media data could give exceptional support to investigators in the criminal investigation process if it is explored rightly. Published content on social media along with associated timestamps could be used to find the whereabouts of a person, could help to corroborate an alibi, or it might be suggestive of some prior or recent criminal activity.

Trials involving social media evidence are increasing rapidly. In cases like State of Louisiana v.Smith (State Court of Louisiana, 2016) and the United States v. Vayner (US vs Vayner, 2014), social media evidence are used by defense and prosecution in murder and fraud cases The use of social media evidence is relatively

common in insurance, custody, and divorce cases such as case ("Zimmerman v. Weis Markets, Inc., PICS Case No. 11-0932 (C.P. Northumberland May 19, 2011)," 2011) is a personal injury case.

Furthermore, social media evidence is the only source of evidence available for cybercrimes on social media such as cyberbullying, cyberstalking, identity theft, and defamation attacks. In 2012, 689 cases with social media evidence were reported (Patzakis, 2012). The use of social media evidence is increasing rapidly since 2015 (John Patzakis, 2016). As in 2016, 14,000 decisions, which mentioned social media evidence, were reported for 12 months in the United States only (John Patzakis, 2016); and among them, 9500 cases are significantly reliant on social media evidence, and these numbers represent a 50% increase from the previous year (GibsonDunn 2015; John Patzakis 2016). Currently, social media is a prevalent source of evidence in criminal and civil lawsuits.

Despite the noticeable standing of social media evidence in legal proceedings, electronic discovery, the process of evidence collection from social media is not reliable. It is observed that the procedure frequently skipped a crucial piece of evidence or sometimes wholly ignore entire volumes of social media content which are relevant to the investigation. It happens because the forensic examiners and legal practitioners do not have a sophisticated solution at their disposal, which enables them to successfully address diverse, vast, and technically intricate, electronically stored data.

Likewise, in legal proceedings, it is a usual practice to search, extract, and document social media evidence. In substantially larger cases it usually takes several weeks of paralegal and lawyer time and assistance of a forensic expert to gather and preserve the relevant evidence efficiently. This exercise costs a significant amount of

money to the client. In fact, according to (Edmond Burnett, 2016), the courts acknowledged the cost, complexity and time consumed for the electronic discovery of data and ordered electronic discovery only if it is critical for the case and if the price and burden are justified. Therefore, sometimes social media evidence are ignored in the judicial process due to high acquiring cost.

Furthermore, the current proliferation of digital devices in combination with extensive usage and online, activities resulted in massive volumes of electronic data created by a single person on digital devices and social media profiles. Examining and investigating this data to figure out a crime or to find evidence became a challenging and time-consuming task for investigators. Furthermore, the vast volumes of unrelated and unconnected of information acquired by these tools, fail to reveal the significant knowledge about the subject and logical order of events in the absence of appropriate tools for analysis. There are no standard and sophisticated tools to manage their task, and the use of limited and inappropriate tools affect further slow down their progress.

As a result, the workloads for investigators and backlog of cases are exponentially increasing, which is severely affecting the objectivity of the forensic process. As mentioned by (Lillis, Becker, O'Sullivan, & Scanlon, 2016) (Adam Belsher, 2016), the digital forensics case backlog was between 6–12 months in 2004 which became 18–24 months in 2010 and 1-3 years in 2016. It is still difficult to handle the substantial, dispersed, heterogeneous, and unstructured content on social media platforms. Therefore, despite a vast and promising set of information, it is tough for investigators to get enough support from social media evidence.

Social media platforms provide a variety of information on human behaviors and relationships. This information is explored in various studies observe business trends, psychological behaviors it is even used to study for the indication of medical

conditions such as depression. Multiple features of social media data provide supports in different fields. These features are categorized as User, Activity Network, and Content. User data mostly profile data which shows individual,s information like name, date of birth, email address, city. Network information is represented by data such as the number of contacts, who follow whom. Social media Content is actual content posted by the user such as posts, tweets, likes, images, and videos and mostly indicate info about a user's daily life.

User activity is recorded by social media sites for every action performed by the user, such as time and location of any work, and this information is critical in legal practice. It is essential to capture all of the data, with context and accompanying data to gain maximum insights from social media. In a study based in Malaysia, Balakrishnan observed a direct relationship between online activity and cyberbullying, according to it, the people who are more active in the online environment are more likely to engage in cyberbullying behaviors (Balakrishnan, 2015). Likewise, another study suggested a strong correlation among the sociability of users in an online environment and cyberbullying (Navarro & Jasinski, 2012). Sociability in online environments can be measured by the network part of social media data, which includes the number of followers, follower ratios and account validation (K. Lee, Mahmud, Chen, Zhou, & Nichols, 2014). Although, it is possible to capture all that information from the online social network by combining a few techniques. However, to store and manage all the aspects of that information in a practical way, which can later be associated with each other, and searched in a sophisticated way for potential evidence, is a challenging task in the domain. Mostly, activity and network features and metadata are either omitted or viewed out of context in such collections. If these components are correctly managed and examined in the context of each other, they

could potentially reveal a fair amount of valuable information. In a single social media investigation, often hundreds and thousands of disparate information pieces are forensically acquired. This information is used to establish a relationship with the suspect, crime, and victim. This information does not make much sense to the investigator and offer no investigative aids until the data could be managed into a single and cohesive representation.

Automation seems a reasonable solution to handle the heterogeneous, distributed, and massive data source of social network forensics. However, automation in digital forensic domains is not a straightforward issue. Digital forensics technique is useless if they do not qualify to meet the legal criteria of acceptance. For Instance, currently, several data mining approaches are being used for content analysis to identify a suspect or predict a crime (Alami & Elbeqqali, 2015; Liu et al., 2013; Zafarani & Liu, 2013; Zhou, Liang, Zhang, & Ma, 2016). These approaches are suitable for automatic detection systems but not for legal use as needed in forensics because they are based on statistics and probability analysis.

Furthermore, most of these approaches lost the provenance of data processing and pre-processing computations; hence, they cannot be used as evidence. Provenance denotes to the origin and history of an object, in forensic analysis, it is essential to manage the provenance of data regarding people, entities, and activities involved in producing related data objects. Otherwise, the results produced by the methods which failed to maintain and provide the provenance of data, like data mining techniques, would be rejected in a court of law.

The goal of this work is to study the feasibility of using automated techniques for online social network forensics. At present, automated techniques are necessarily needed to manage the massive volumes of digital data and their complexity on online

social networks. Otherwise, the investigation process would become inefficient. The inability to deal with the complexities of data might lead to errors in the process that would severely affect the subjectivity of the process. Furthermore, this work will address the problem of conducting an automated but legally acceptable forensic investigation on Online social networks. The proposed work presents a forensic investigation model and a formal knowledge model for the online social network to explain the collection and analysis of the evidence through automated methods.

1.2 Problem Statement

In general, forensic collection and analysis are time intensive and multi-dimensional phases in the digital forensic process (Casey & Rose, 2010). Forensic gathering phase collects the data from potential sources of evidence, and analysis phase interprets the factual information gathered in the collection phase. The interpretation involves the integration and correlation of extracted artifacts; to know the linkage such as who interacted with whom and to find the order of the event what happened when. This linkage and sequence would lead to attribution, who did this. Expert knowledge is needed to get these shreds of evidence and to create and test a different hypothesis about the crime, and correlate separate seemingly irrelevant pieces of information together to arrive at some plausible conclusion by judgment and deduction process.

In traditional crimes, the investigators manually sift through all the materials involved in an investigation to find the relevant information and potential evidence. While in digital inquiries, keyword search replaces this sifting process to find the relevant information and evidence from digital data quickly. Keyword search is an essential and efficient tool to quickly locate some relevant information from the massive bulk of digital data, which would be impossible by manual sifting. However,

improperly formulated keywords can miss vital information, or they may result in too much information with high false positives which would need to process again.

Investigators use some specialized such as Encase, CacheBack, Internet Evidence Finder (IEF) (Van Buskirk & Liu, 2006)(Cusack & Son, 2012). Some more recent software which claimed that they are specifically designed for social media forensics, like Informatica Enterprise Data Integration tool and X1 Social discovery (Patzakis, 2011). Though it is observed that this software perform faster large-scale legal extraction and legally preserve the data to ensure the data integrity, they are considered suitable for forensic acquisition, and early case assessment only as these tools provide data sorting and keyword searching features, i.e., keyword searching or date filter options. Such as Aleph Archives and Hanzo Archives, store data in the WARC Web archive format, X1, save data in the MHT Web archive format and can export to Concordance, CSV and HTML. Other like NextPoint store it as PDF, HTML, and PNG files it also exports data to Concordance and XML (Fasching, Kaliner, & Karel, 2012).

Their searching and sorting features, needed for analysis of data, becomes limited to keyword search; due to the storage formats and underlying data organization (Al Mutawa, Al Awadhi, Baggili, & Marrington, 2011; James Billingsley, 2016). Just keyword search is not enough for current social media investigations due to the enormous size and intricate nature of social media content which include text, reactions and multimedia content in the form of images and videos this fact is also acknowledged by (James Billingsley, 2016; Turnbull & Randhawa, 2015). The investigator must filter the data with customized and advances querying mechanism to get an insight into a particular sequence of events. For instance, the investigator must

be able to sort the communication frequency of the subject with a specific contact, usage patterns of time and location or social graph.

Automation of forensic techniques and processes is not entirely a technical issue. The conclusions produced as a result of automated methods are intended to be used as evidence in a court of law. Therefore it is necessary for the automated methods that they must fulfill all the legal requirements to gain the admissibility for the produced evidence. Fully automated forensic systems are strongly criticized both by legal and academic communities. Only the process that can demonstrate the provenance and explain the results through a logical explanation is acceptable in legal proceedings (Bates, Pohly, & Butler, 2016; Katilu, Franqueira, & Angelopoulou, 2015; Lu, Lin, Liang, & Shen, 2010; Ma, Zhang, & Xu, 2016) Due to this reason, most data mining methods, that are currently used for OSN content analysis are not suitable for forensic purposes (Glavic, Siddique, Andritsos, & Miller, 2013; Viviani & Pasi, 2017). In other forensic disciplines, formal theories are used to explain the conclusions. However, in digital forensics, formal theories are very few; even the theoretical models that exist are not suitable for OSN.

This study examines the potential areas of a forensics investigation where automation can be applied without contradicting the legal requirements on online social networks. This work intends to propose an automation model to address the automation issues at several phases of social network forensics. This works identifies the key process areas for automation and classify them into distinct layers. Then this works suggest appropriate automated solutions for each layer. This study aims to propose separate models for managing the collection, analysis, and interpretation of evidence.

1.3 Research Questions

The primary goal of this study is to identify the critical process areas in social network forensics suitable for automation and provide a legally acceptable solution to automate those processes.

RQ1: Is it possible to formally explain the theory of forensic analysis on OSNs, needed to explain the automated results in court?

RQ2: Is it useful to explicitly preserve the associations among the social network contents and accompanying metadata?

RQ3: Is the formal modeling of the domain knowledge would provide a suitable theoretical background to explain the automated results?

RQ4: Why is a generic digital forensic process model not suitable for Social network forensics?

RQ5. Does forensic investigation for OSN need a specialized process model?

RQ6: Is it feasible to define the crime scene boundaries on OSNs by using quantifiable parameters?

RQ7. Is it possible to automate a few phases of forensic investigation process model?

RQ8: Is it possible to propose a semantic data model for OSNs that can manage the complete data components (network, activity, interactions, multimedia?

RQ9: Is it suitable to use semantic data modeling to support automated analysis for OSN forensics?

RQ10: Is it feasible to propose automated analysis operators for social network forensics?

RQ11: Do the automated analysis operators can help in reducing the investigation time and decrease the effort needed to conduct the OSN investigation.

1.4 Research Objectives

Respectively, the study aims to achieve the following objectives.

RO1. To present a formal knowledge model for online social network forensic that can interpret and correlate information for automated analysis.

RO2. To propose a forensic investigation process model for supporting automated online social networks investigations.

RO3. To formulate a semantic data model, for social networks, to provide a structured representation of social network content that is suitable for automated analysis.

RO4. To design automated analysis operators, to evaluate the suitability of the proposed models for automated analysis.

1.5 Research Scope

The suggested framework is designed for the use of automated or semi-automated social media forensics. It explores the suitable features for automated or semi-automated forensics on social media. Current work is providing proof-of the concept ontologies for proposed knowledge model and Twitter platform to demonstrate the concept. Ontology of any social network platform, if available, can also be used in the suggested approach. Forensic archiving or preservation of social network data is also an open research area. In this work, some literature highlights the forensic preservation issues; however, this work does not provide any solution for that problem.

1.6 Research Methodology

This work aims to propose a multi-layer model to achieve automation in digital forensics for the online social network. Fully automated forensic analysis systems are sharply criticized both in academic and legal communities. However, the manual

forensic process is not suitable to with the massive volumes and diversity of the current digital infrastructures like OSNs. Therefore this work is focused on finding the optimum automated solutions, for OSN forensics, that are legally acceptable and technically achievable.

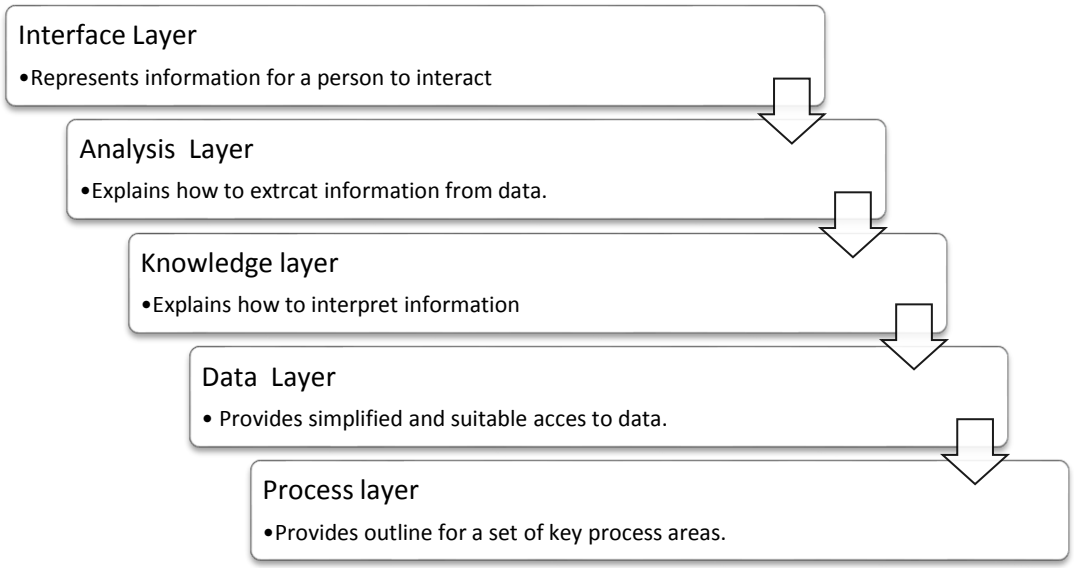

Figure 1.1 Overview of Research Methodology

The proposed methodology is consisting of a five-layer model to support forensic automation on OSN; it is outlined in the following diagram.

Process layer is the lowest layer. Process layer highlights the critical process areas for automation. These process areas include incident identification and evidence acquisition. This layer is also responsible for stating the parameters such as the scope and type of data extraction, specifying significant actors involving in an incident. The parameters specification is a must for the automation of the whole investigation process. A forensic investigation process model for online social networks is proposed to address the requirements of this layer.

Data layer provides simplified access to the data that is related to the incident and extracted from OSNs. The data layer is implementing the knowledge model by using semantic web methods and ontologies. Therefore, this layer is responsible for

normalizing the extracted data and saving it in persistent storage. The persistent storage is designed and implemented by using the semantic web schema and RDF stores.

Knowledge layer will provide a suitable theory that acts as a scientific foundation in digital forensic science is always mentioned in the literature. This theory is supposed to satisfy the legal and scientific demands to justify the facts derived as evidence. The use of a formal theory would help to explain the logical sequence and reasoning used to find and interpret the evidence by automated methods in a court of law. The proposed model is based on the event-based knowledge that is specifically designed for automated social media forensics and analysis. This detailed representation will allow constructing automated analysis methods.

The analysis of such a large and varied dataset requires sophisticated tools. In this work, we aim to propose some automated analysis methods. This layer aims to present automated analysis operators. As the approach presented in this work is supporting a semi-automated approach, therefore the purpose of these operators is to quickly sort and analyze the data and present the results to the human examiners for evaluation. The decision-making process is delegated to human examiners due to an infinite number of scenarios and the variety of crimes that are investigated through social network evidence.

Interface layer allows the investigators to interact with the data and analysis layer. This layer aims to present the data, filtered or sorted by the analysis layer, in a reader-friendly manner. The results produced by analysis operators would be presented through appropriate visualizations such as cluster graphs, relative or cumulative frequency histograms.

1.7 Research Contributions

This work has offered the following contributions in the domain.

1.7.1 Formal Knowledge model

This study is presenting a large-scale, consistent, and formal knowledge representation for social media forensic collection and evidence extraction process. It provides a formal description of the structure and semantics of online social networks and forensics, and the information is encoded into ontologies. The formal model will help in explaining the process and deductions made through automated analysis operators.

1.7.2 Forensic Investigation Process Model

This work proposes a forensic investigation process model for online social networks. Because it is observed that the existing process models are not suitable for automated forensic investigations OSNs.

1.7.3 Structured Data Representation

This work is implementing techniques to overcome the heterogeneity existing among social media content and sources to achieve a consistent and structured data representation. The structured information allows the execution of automated analysis methods to process the data to get useful knowledge. Structured data is also needed for forensic data sharing and interoperability among tools.

1.7.4 Automated Analysis

This model is providing a proof-of-concept implementation of automated analysis operators that can be incorporated into software tools to assist in forensic analysis and interpretation. These operators are finding the relatedness among the entities and events and use them for analysis. These operators will sort and filter the data by using the correlations and present the deduced information through appropriate

visualizations. More importantly, the results produced by proposed methods are logically explainable through knowledge model; hence, they are justifiable for legal acceptance.

1.7.5 Forensic and Social Network Ontologies

This study is providing the proof-of-the concept implementation of two Ontologies. One is a high-level ontology to explain the shared forensic concepts of the domain. The forensic ontology is a detailed ontology modeled for the Twitter schema to provide a comprehensive analysis of Twitter data. The Twitter ontology is a general-purpose ontology that can be used in any domain using Twitter data analysis.

1.8 Thesis Organization

Chapter 2 provides a review of literature and research gaps in relevant areas of the problem under study. This chapter concludes by finding the research gaps from existing literature.

Chapter 3 is a complete description of the proposed model. Furthermore, this section will describe the choice and construction of a case study that is based on a hypothetical cybercrime.

Chapter 4 is explaining the implementation of all the research objectives. That include knowledge layers which present a formal knowledge representation and forensic investigation model for social media forensic collection and analysis. Analysis layer presented in this chapter provide the generic algorithms for automated analysis operators. In the data layer, this chapter explains the data and relationships involve in micro-blogging social networks such as Twitter. Also, it presents the formal representation of the data model through ontology and describes the semantics of the model. The process layer describes the forensic investigation model for online social networks (FIMOSN).

Chapter 5 discusses the implementation of the analysis operators on the proposed study and presenting the results obtained by the experiments. The analysis operators will be evaluated on the case study dataset. This chapter will focus on evaluating the practicality of automated analysis operators and supporting knowledge and data models. This chapter also explains how to conduct an OSN investigation by using FIMOSN.

Chapter 6 is presenting the research conclusion and research contributions. It also explains the potential future works.

CHAPTER 2
LITERATURE REVIEW

Social media forensics research is an entirely new branch of digital forensics. Although, the digital forensic practices and techniques are in practice and continually improved over time. However, the new sub-fields of digital forensics such as cloud and social media forensics, are presenting entirely new challenges in the domain. These challenges are due to the size, distributed architecture, dynamic nature, and heterogeneities involved in structure and data of social media and cloud domains.

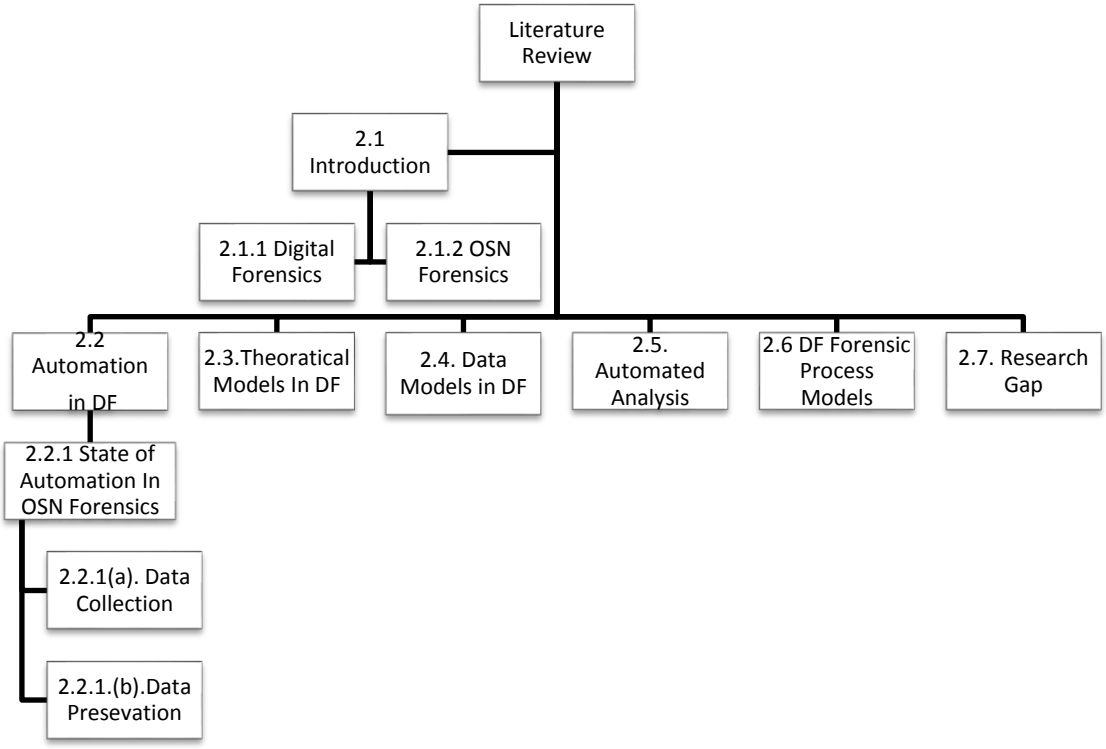

Figure 2.1. Outline of Literature Review

Very few related works are existing in social media forensic domain. Therefore, after finding the research gap, we also did a study of associated areas such as digital forensics and cloud forensics to see the feasibility of various probable solutions. The components of the literature review are outlined in Figure 2.1.

2.1 Introduction

2.1.1 Digital Forensics

Digital forensics is a field of forensic science comprehending the retrieval and investigation of the content found in digital devices after a crime that involves digital devices (Carrier, 2003).

Digital forensics investigations are applied in various scenarios. Commonly they are used to refute or validate a hypothesis in criminal or civil trials. Criminal trails encompass the suspected violations of laws that are prosecuted by the state and enforced by law enforcement agencies, such as theft, kidnap, murder, or assault against an individual. While, civil cases deal with defending the property rights of individuals or contractual disputes between commercial organizations (Casey & Altheide, 2010). Digital forensic also used in the private sector, such as intrusion detection and internal audits.

The typical digital forensic process involves the confiscation, forensic imaging (acquisition), and analysis of digital content. A report is also documented to report and present the collected evidence in legal proceedings.

The digital forensic process identifies the direct or indirect (circumstantial) evidence of a crime to link the perpetrators to the victim or the crime. The process may be also be used to attribute evidence to a suspect, verifying alibis or confirming statements to find the purpose of crime, to locate the evidence or validate documents (Casey & Altheide, 2010). Digital investigations are more wide-ranging in scope than other fields of forensic analysis. In other areas, the usual aim is to provide answers to a series of more straightforward questions while digital investigations usually involve complicated timelines or hypotheses.

2.1.1 (a). Digital Evidence Admissibility Criteria

When utilized in a court of law, computerized prove digital evidence are judged with laws as other forms of evidence; courts do not ordinarily require more rigid rules. Laws managing with digital evidence are concerned with two issues: integrity and authenticity. Integrity is guaranteeing that the act of seizing and securing electronic media does not modify the evidence. Authenticity refers to the capacity to confirm the integrity of information; such as the copied media matches the original evidence. The ease with which digital media can be altered implies that maintaining the chain of custody from the crime scene, through analysis and, ultimately, to the court, is imperative to prove the authenticity of the evidence.

2.1.1 (b). Digital Forensic Investigation Phases

A generic digital forensic investigation is usually comprised of three phases: acquisition and preservation, analysis, and reporting (Adams, Hobbs, & Mann, 2017; Jones, 2004; Michael B. Mukasey ;Jeffrey L. Sedgwick ;David W. Hagy, 2008). Preferably, the acquisition phase consists of capturing the digital media in an exact copy of the original content(Sammons, 2012). The process often uses write blocking mechanisms or devices to avoid any alteration in original content. However, currently, the immense size of the storage media and latest digital manifestations such as cloud computing and social network tends to generate large volumes of data have led to the use of a logical replica of the data is instead of a complete and identical copy of the physical storage (Adams et al., 2017). The extracted copy and original content are hashed by using algorithms like SHA-1 or MD5, and the generated values are used for comparison to ensure the integrity of data (Jones, 2004).

Analysis of evidence is a complex process and may among investigations, but generally, it includes keyword searches to locate specific information from retrieved

digital media, salvaging deleted files and extracting registry information and logs to list processes or user accounts involved in a task(Eoghan Casey and Curtis W. Rose, 2010).

The recovered evidence is analyzed to reconstruct the events or tasks to find the plausible sequence of action and participants that lead to a crime. On completion, the conclusions based on data is presented in a court of law; usually, as a written document to present the evidence most understandably (Carrier, 2003).

2.1.2 Social Network Forensics

Social media (SM) evidence is a new appearance in digital forensics. In 2017, 2.8 billion active users were reported; they are actively engaged in sharing their everyday activities on social media sites. The information published on social media, about an individual, his actions, and dealings is used from time to time as a potential tool, by investigators to backtrack a crime.

Although the use of social media evidence is not a straightforward process due to technical and legal issues, related to evidence gathering, admissibility, and the defendant's constitutional rights, presentation of social media evidence is still another issue. Despite all the problems, social media evidence is already being used, for the trials of custody, divorce, and insurance cases, mostly as direct evidence.

Social Media Forensics as a discipline is still in the infancy stage. Although, the first conviction based on social media evidence was reported in 2009, when the district court in California, United States convicted a Missouri woman who had created a false MySpace profile and allegedly caused the suicide of a teenage girl, United States v. Drew, (Cal., 2009). However, Potential use of social media evidence in litigation is formally highlighted in 2011 by (Browning, 2011). This concept is supported by (Zainudin, Merabti, & Llewellyn-jones, 2011), which also presented a

social media forensics investigation model. However, Social media forensics was not notably identified as a discrete sub-domain of digital forensics until 2013. A study (Damshenas, Dehghantanha, & Mahmoud, 2014) surveyed for a 2008-13 time interval to determine emerging trends and their extent in digital forensics research and community, and they did not list social media forensics as a discrete trend because they did not find more than five publications on the topic in a given interval.

Presently it is reported that 91% of adult users are using various social media platforms. This progression is offering unique and diverse opportunities for the individual. However, unfortunately, this evolution also provides many prospects to the criminals, to discover sophisticated ways of committing traditional crimes with the aid of digital technologies. Such as Christopher James Dannevig became friend with 18-year-old Nona Belomesoff on Facebook in 2012. He created another fake account to prey on her. Later, he kidnapped and killed her. The investigators observed the connection at Facebook and traced to preparator after her disappearance.

The criminal is also inventing altogether new crimes like, identity theft, cyberstalking, ransomware, which are labeled as cyber-crimes and are associated explicitly with digital infrastructure. While the digital systems became supportive tools of criminal activities due to their prevalence and ease of access, the positive aspect of digital incidence is that it likewise suggested a new set of opportunities for investigators to backtrack the crimes. Investigators could track and spot criminals by following the digital footprints are left behind.

2.1.2 (a) . Criminal cases

The use of social media evidence is reasonably every day in criminal cases. Prosecution and defense criminal layers equally use it. However, defense lawyers face more hurdles to seek a subpoena to social media companies for accessing nonpublic

social media data. However, still, they have access to a massive amount of social media public data. Several criminal cases are now routinely investigated, prosecuted, and defended through social media evidence.

For instance, 18year-old Kimberly Proctor was tortured and killed by her two classmates in March 2010 at British Columbia. Two teenage boys Kruse Wellwood and Cameron Moffat who are identified through the digital traces of the sick plot they left on a site World of Warcraft. Similarly, in the trial of State of Louisiana v.Smith, which is an aggravated assault case in 2015, suspected posted a picture of himself carrying a firearm and threating messages for the victim on Facebook. Later, printouts of photo and Facebook posts were presented as evidence which is rejected by the court due to lack of proper authentication (State Court of Louisiana, 2016).

In Hoffman v. State, an 18-year old female was convicted of vehicular manslaughter. Her photos from MySpace, which reveal her alcohol abuse, were presented to increase her sentence. In US v. Anderson, a pedophile was identified and convicted who used Facebook to lure victims.

2.1.2 (b) . Custody and Divorce Cases

Social media evidence provides a significant effect on alimony, Divorce, and child custody cases. Usually, in those cases, one of the partners is purposefully less honest with the court. For instance, a person who wrongly claims an incapability to work to receive spousal support or insurance claim may be proved wrong if opposing counsel provide photos from his or her profiles social media profiles, in which indicate active physical activity.

Dorothy McGurk won a settlement of $850 a month for life and home at the time of divorce by convincing a court three years ago, and a car accident left her incapable of working. The decision is reversed; when the husband Brian McGurk

presented her photos, she posted on a blog. The images showed her doing belly dancing, which invalidates her excuse for physical disability (Martoche, Smith, Centra, & Peradotto, 2010). Posts about traveling, shopping, or leisure activities are used in cases involving disputes over child support or alimony. Likewise, LinkedIn profiles are used to describe how someone is advertising himself to probable employers, and they are also used as evidence to access a person in cases involving child support or maintenance.

Child Custody is frequently a contentious issue when divorcing. People regularly used to share photographs of children and information about their activities on Facebook, Instagram, and other social media sites. These posts and photos can influence a court's decision in custody cases. For instance, images or posts indicating a parent's drug use or inappropriate behavior is usually enough to convince the judge to deny the custody of children to that person.

Social media posts can be used to confirm the activities of a person on a specific date or time. Facebook check-ins, Twitter geolocation tags, and posts to Foursquare can be easily applied to track the whereabouts of an individual. The social media content reveals that at what time or date a person was at a specific location and may also show who is spending time with that person. This type of information can ordinarily use in custody and divorce cases.

2.1.2 (c). Fraud and Personal Injury Cases

In personal injury cases, the appellant filed a lawsuit to claim financial compensation for his damage and emotional distress, caused directly or indirectly by the accused party. The plaintiff used to demand settlements from accused of two things: first, the actual expenses associated with the injury, and second, for loss and stress caused by the physical damage. In some instances, the insurance companies are

supposed to make that compensation. In these cases, the defendants seek to find information about the appellant, which help to disprove the appellant's claim or minimize the extent of that claim. Before the advent of social media, defendants use private investigators to take photographs and record videos of the day to day activities of the defendant to prove him healthy and enjoying life. Presently social media content is commonly used to disprove the severity of physical injuries and emotional distress by using photographs and posts from social media. The posts which demonstrate the presence of healthy physical activities and hobbies in appellants life. Tracking apps are also used to discredit the plaintiff's version of the events leading up to the accident.

Romano v. Steelcase is another example of a personal injury case where social media evidence is used for decision in a Suffolk County Supreme Court (Supreme Court Suffolk County, 2010). An office worker filed a product liability claim when her chair collapsed. She accused that the injuries caused by that faulty product had restricted her outdoor activities and socializing with friends, leading to considerable emotional distress. In response, the defense presented her pictures of smiling outside her home, the content of her posts, which show her happy. The defense counsel succeeded to demonstrate to the jury that the extent of her mental stress id not as severe as she claimed.

In another trial, the suspect Aliaksandr Zhyltsou was charged and later evicted on social media evidence (769 F.3d 125 (2014), 2014). He was convicted on a sole instance of illegal use of false identification documents, and he then appealed against the decision. At trial, Vladyslav Timku, he was a Ukrainian citizen living in Brooklyn, testified that Zhyltsou provided him with a bogus a birth certificate which presented that Timku was the father of a daughter. The initial conviction was based on expert

testimony that the email originated in New York, although there was no material proof for that statement. A web page of a Russian social media profile was also presented, and the prosecution claimed was Zhyltsou's profile page on VK.com, and that page connected him to the email address. In the end, the suspect Zhyltsou was charged only with Timku'a testimony was used to associate the Zhyltsou to the Gmail address used to send the fake birth certificate to Timku. However, later, the court overturned the ruling and stated that the prosecution failed to prove beyond doubt that the suspect creates this page as everything on it is public knowledge.

2.1.2 (d). Violation of Restraint Orders

Text messages and social media posts are also used as evidence of a violation in case of any restraining order in place. Social media check-ins to specific locations, in addition to or contact information with the other individuals through social media, is used as evidence. This evidence is also proved helpful in stalking and violating the restraining order. Such as, in the trial of People v. Mincey, the defendant violated the probation by communication on social media sites (People v. Mincey, 2013).

2.1.2 (e) . Cyber Crimes

The progression of social media has introduced new ways altogether and ease to commit crimes. Such as Cyber Bullying, or Cyber Harassment is a form of bullying or harassment using electronic forms of contact. Bullying is not something new. In the past, children were bullied at school or in their locality. However, it has certainly evolved with time and is much more common. Now not only children but adult individuals are bullied all the time on social media by their peers and even strangers sometimes. It is reported that nine in 10 teenagers in the United States acknowledged that they had observed bullying by their peers on social networks (Cecilia Kang, 2011). Cyber Bullying on social media involves, posting foul comments on pictures, posting